University of Piraeus

School of Information and Communication Technologies
Department of Digital Systems

Master Thesis

"Spyware technologies"

Valatsos Vasileios
ID: MTE2204

Supervisor:
Gritzalis Stefanos, Professor

Piraeus

April,2024

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία πραγματεύεται τα κατασκοπευτικά λογισμικά που εμφανίστηκαν το τελευταίο χρονικό διάστημα και κατάφεραν να μολύνουν ψηφιακές συσκευές ανυποψίαστων θυμάτων με απώτερο σκοπό- στόχο την υποκλοπή ευαίσθητων πληροφορίων. Η μελέτη της δράσης των παραπάνω λογισμικών ύστερα από την παραβίαση εξετάζεται από την επιστήμη της Ψηφιακής Εγκληματολογίας. Οι αναλυτές αναζητούν το τρωτά σημεία των ψηφιακών συσκευών, καθώς και τα ίχνη που αποτυπώνονται καθ' όλη την διαδικασία της υποκλοπής. Τα ίχνη που παρατηρήθηκαν πολλαπλές φορές, δύναται να αποτελέσουν ενδείξεις για το αν μια συσκευή έχει μολυνθεί από τα εν λόγω κατασκοπευτικά λογισμικά. Τέλος, εξετάζεται η χρήση μεθόδων παραπλάνησης ή απόκρυψης των λειτουργιών που εμπεριέχονται στα κακόβουλα λογισμικά καθώς και οι τρόποι που οι αναλυτές καταφέρνουν να διεξάγουν την έρευνας τους αποφεύγοντας τις προαναφερθείσες μεθόδους.

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Κυβερνοασφάλεια

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Spyware, Digital Forensics, Anti-Forensics, IoCs, Espionage

ABSTRACT

The present thesis deals with the spy software that appeared in the last period of time and managed to infect digital devices of unsuspecting victims with the ultimate goal of stealing sensitive information. The study of the action of the above-mentioned software following a breach is examined by the science of digital forensics. Analysts look for the vulnerabilities of the digital devices, as well as the traces that are captured throughout the interception process. Traces observed multiple times may provide clues as to whether a device has been infected by the spyware in question. Finally, the use of methods to deceive or conceal the functions contained in the malicious software and the ways in which analysts manage to conduct their research while avoiding the aforementioned methods are discussed.

SUBJECT AREA: Cybersecurity

KEYWORDS: Spyware, Digital Forensics, Anti-Forensics, IoCs, Espionage

Acknowledgements

I would like to say a special thanks to my supervisor Dr. Gritzalis Stefanos for his dedicated advice and support during the whole procedure. Dr. Gritzalis is always willing to guide young students in every aspect of their life, making him a great academic inspiration figure. I would also like to thank my family for their unconditional support throughout my study years.

Table of Contents

List of figures

List of tables

Prologue

The recent disclosure regarding the use of Spyware technologies to eavesdrop on Greek citizens private communications has forced the community to find answers. This Thesis is conducted in the context of the internet, the social media and the smart devices growth that people operate every day. With the intensively use of electronic devices, many traditional tasks such as a phone call, can be over the Internet without the local communications operator has an indication that a call occurred. Some people although based on Laws are suspects and have to be spied, for evidence gathering, but if a call cannot be logged from the communications operator no evidence will be collected. Technologies as spywares are developed to tackle that issue and provide to those who willing to pay the solution to have full access in the individuals' devices by spreading the malicious applications. Thus, there is need for analysis that identifies the malicious apps that spy on individuals.

1. Introduction

The stealthy and ever-evolving world of spyware provides an enduring challenge for digital forensics experts in the delicate area of modern cybersecurity. Spyware, as pernicious as it is, hides within digital ecosystems, capturing information and passing it to hostile actors invisibly. The constant evolution of these covert tools necessitates the pursuit of cutting-edge forensic procedures to uncover their presence and intent. However, while digital forensics works to shine light on clandestine operations, the shadowy world of anti-forensics arises, in which cybercriminals use advanced tactics to hinder investigation attempts. A continual cat-and-mouse game in the digital world unfolds in this complicated interaction of spyware, digital forensics, and anti-forensics, underscoring the crucial need of remaining one step ahead in the battle for information security.

2. Spyware Technologies

Spyware technologies is quickly becoming one of the most serious risks to Internet users' security. Those technologies' primary objective is to infiltrate devices invisibly with the goal of collecting valuable information ranging from login credentials and credit card details to personal documents and sensitive data. Furthermore, spyware is widely used for surveillance, acting as a digital spy that observes a user's online and offline actions. It accomplishes this by secretly monitoring email correspondence, chats, and social media activities in the name of espionage, this data is subsequently transmitted back to the spyware distributors. In less malicious forms, spyware, also known as adware, is used for marketing purposes. This more benign kind seeks to track user behavior to offer tailored adverts, but it occasionally oversteps its bounds by gathering more data than necessary, prompting privacy issues. Spyware comes in a variety of forms, each precisely tailored to suit a specific function. Among them are keyloggers, which quietly record every keystroke on a computer, thereby providing attackers access to a treasure of sensitive information such as usernames, passwords, and any textual input from the user. Adware, on the other hand, may appear less dangerous at first glance, but it expertly harvests data on a user's surfing patterns and tailors a bombardment of adverts appropriately. However, adware frequently teeters on the verge of being intrusive, collecting more data than it should. Trojans, which typically wear the guise of respectability, may have spyware elements that allow data theft and malicious backdoor access. Tracking cookies, those innocuous bits of code that websites surreptitiously plant in a user's device, methodically track browsing behaviors and preferences. Finally, more modern spyware employs screen recorders, meticulously gathering visual reports of a user's every interaction with their device, leaving no digital stone unturned in its pursuit of data, but system performance suffers because of the frequent improper coding.

Installing software from untrustworthy sites can lead to the installation of spyware in the user's device. Many freeware and shareware apps install malware in the background. Most people will click OK without fully understanding what they are installing and that can lead to the installation of malicious spyware programs which they install alongside other software. Some may even use features or weaknesses in certain operating systems or Web browser software to install themselves when specific websites are visited. This is known as a drive-by download. The bulk of spyware is not intended to harm the devices. Spyware aims to track user activity and share it with third parties and in this way is considered malicious since it is installed without knowledge or consent from the end user. These are but a handful of the sneaky things spyware may do to a compromised device such as the of use of system resources and alteration of system settings.

The main way that spyware varies from viruses is that it does not spread by itself. A virus is able to reproduce itself and spread to infect further machines. Spyware only installs when the user gives the authority to do so, either by consenting to install it, downloading, and installing it automatically from a website, inadvertently installing it as a component of another software, or it can also hide in corrupted hardware, such as a USB drive. It does not look for new devices to

infect or try to replicate itself once it is on the target system. This greatly relies on the individuals who have been impacted. For example, if a toddler has been exposed to this spyware software, there won't be anything to filter, making the program completely pointless. Using spyware to track a variety of situations in which governments are compelled to act—such as bomb threats, evidence of guilt, harassment, intimidation, and even the leakage of government information—is an extreme functionality that is typically employed by governments.

Many anti-spyware programs have been created, with the aim of locating and eliminating undesired software. The majority of the technology behind these programs is the same as that found in antivirus software. In other words, they compare the binary image of these programs with a variety of distinctive signatures to identify known spyware occurrences. These signatures are created by hand by examining previously released spyware samples. Because of this, these anti-spyware programs have the same shortcomings as signature-based anti-virus programs, such as the requirement for constant signature set updates and the incapacity to handle basic obfuscation strategies. Some of the Indications of Compromise will be later examined. [1][2][3][4][5][6][7][8][9][10][11]

2.1. Ethics

It may be deemed unethical for a user to install a packed application without receiving any kind of notification. The retrieval and/or recording of personal information from the user by an application is another unethical feature of spyware-specific software. This could involve anything from accessing and monitoring email accounts to actually retrieving additional personal data that is kept on the user's device. Passwords, credit card numbers, and other items kept in memory are a few examples. Packaged software can perform any function when it is installed automatically along with the accompanying application. The fact that some spyware programs perform functions other than information retrieval and transmission raises yet another ethical concern. They are incredibly difficult to find and track down on the user's device, and one of their possible actions is to take full control of a device. This brings up another intriguing—and highly unethical—feature regarding some spyware programs, namely the fact that they can be exceedingly challenging to get rid of. Programs that automatically reinstall themselves after the user uninstalls the original application have occasionally been reported. A program that reinstalls after being removed from a device violates the user's right to uninstall any software. Thus, if consent and authorization from the user are gathered. For example, breaking down the software and setting it up on several computers.[12][13]

2.2. Characteristics

Spyware distribution methods can be extremely misleading and covert. Bundled software is a frequent approach for malicious software to infiltrate systems. When downloading and installing what appear to be legal software packages, especially free or pirated software, users may unwittingly install spyware. Another entry point is via email attachments, where malware might be hidden, or via links in phishing emails. Visiting a compromised website can potentially result in an insidious attack by triggering automatic malware downloads onto a user's device, a tactic known as drive-by downloads. Malvertisements, or malicious adverts, are another covert distribution method because they can carry spyware and infect a user's device when they innocently click on them. It is critical to remain attentive and use strong security measures to protect against these shady distribution methods. Spyware, a type of malicious software with particular properties, is a major danger to cybersecurity. Its covert installation, frequently via misleading techniques, and capacity to capture personal and sensitive information without user consent are particularly concerning. This data is then silently sent to remote servers controlled by cybercriminals, who can later exploit it for harmful reasons. The longevity of spyware on the

infected system, even after reboots, ensures that data collecting, and unauthorized access continue. Furthermore, its versatility and continual evolution, designed to outwit security systems, make it difficult to identify and eradicate. Because of its breach of privacy, spyware, whether used for targeted attacks or widespread distribution, remains unlawful and unethical.

Events are produced, for instance, when a resource download is finished, a new URL is opened, or a requested website cannot be located. The spyware component's main utility is to send the data to a third party after it has extracted the desired information. In order to achieve this, the data must be saved locally, for instance, in a file on disk or in the Windows Registry, transferred directly over the network, or passed to a collaborating process running on the same host. In any event, to send the data to the designated destination, the spyware component needs to communicate with the operating system. Data eventually needs to be leaked by invoking an operating system service, even when it is just momentarily stored in memory. The operating system services that a spyware component reuses must be analyzed since the component has to interface with the operating system. It is possible to obtain information from the running process by using specific API calls to a third-party online application. Therefore, the only places where information may be safely leaked are in event handling code. By launching a second thread or setting up a timer with the proper callback function, a spyware component can try to create an extra pathway via which events might be leaked. The gathered user data would initially be saved in a globally available data structure before being released in response to a browser event. It is possible for the timer callback function or the second thread to flush out this data thereafter without being noticed. This chance of avoiding discovery was eliminated by using a cautious approach. In other words, if a component could generate a thread or a timer. A component might, for instance, download software updates upon startup, write entries to a log file, or read some configuration values from a file. The important takeaway from this is that while neither of the two traits by itself usually raises red flags, when combined, they strongly suggest malevolent activity.

A spyware operates very quickly since it can be activated by a simple error, such as adding unfamiliar hardware to a system. This means that the software can attack the device first by giving permissions without the user's knowledge in order to track all the movements a user makes within a device. Once inside, the spyware starts gathering and extracting data from the device, including cards, videos, images, photos, messages, histories, and screenshots, among other things. As was previously indicated, the very specific operation of this is the infiltration and theft of any information that can be obtained, but it is important to consider any potential negative impacts as well. As a result of spyware's constant operation as a scanner, the compromised device may become slower. End users can tell when something is amiss because the device’s speed and power drastically drop. Memory overload is causing programs and executions to run slower and slower, as well as more crashes and freezes. Other Internet connectivity issues or unusual device behavior are possible indications. Both individuals and businesses analyze this kind of software to find them and develop procedures for getting rid of them. It can be challenging for users to determine who to report spyware. Typically, people report spyware to computer technicians or antivirus providers. [14][15][16][17][18]

2.3. Windows

Over the years, several well-known spyware programs and families have targeted Windows users.

- Zeus (Zbot): Zeus is a Trojan horse designed to steal banking information. For years, it has posed a significant threat to Windows users.
- Keylogger software: Keyloggers are programs that record keystrokes and collect sensitive information such as usernames and passwords. SpyEye and DarkTequila are two well-known keyloggers.
- Remote Access Trojans (RATs): RATs are programs that provide remote access and control of a victim's computer. Poison Ivy, DarkComet, and njRAT are examples of popular RATs.
- SpyEye was a banking Trojan that became well-known for stealing financial information from compromised PCs. It was used to steal banking credentials as well as other sensitive information.
- FinFisher (also known as FinSpy) is a spyware software promoted as a law enforcement and government surveillance tool, however it has been utilized in several espionage efforts. It has the ability to infect Windows systems and track numerous actions.
- Hacking Team's Remote Control System: This surveillance software, designed by an Italian business, was reported to be utilized by governments for monitoring and surveillance.
- Superfish was an adware program that came pre-installed on some Lenovo laptops. While it was not classic spyware, it posed serious security and privacy threats by injecting unwelcome advertisements into web traffic and potentially capturing secure communications.
- WebcamSpy: Some spyware applications are designed to steal a computer's webcam, allowing an attacker to capture video and audio in the background. Webcams of many types of spyware have been discovered targeting Windows users.[19]

2.4. MacOS

Over the years, several well-known spyware programs and families have targeted MacOS users.

- FruitFly: FruitFly is a macOS spyware. It enabled attackers to gain control of a victim's computer, including the ability to capture screenshots and webcam footage.
- OSX/Proton: Proton is a macOS malware family that has been used to steal sensitive information, such as login passwords, via phishing attacks.
- Eleanor: Eleanor is yet another macOS malware that masquerades as a file converter application while granting attackers backdoor access to the affected system.
- KeRanger: was one of the first cases of macOS-specific ransomware. It encrypts user files and demands a payment to decrypt them.
- Silver Sparrow: Silver Sparrow was identified on macOS systems. While its particular intent and payload were unknown, it demonstrated the potential for widespread macOS malware spreading.
- Shlayer is adware that targets Mac users by diverting web traffic and displaying unwanted advertisements. It spreads by way of rogue websites and bogus software updates.
- CrescentCore was a macOS virus that masqueraded as an Adobe Flash Player update. It has the ability to circumvent macOS security mechanisms and infect users' PCs.
- MacDownloader: This macOS malware masqueraded as a security update while actually stealing personal information from users.[20]

2.5. Linux

Due to its open-source nature and significant community support, Linux is sometimes seen as a more secure operating system than Windows and macOS. However, it is not totally immune to spyware and viruses. While Linux malware is uncommon, there are a few well-known examples.

- BadBash is a Linux malware strain that targets vulnerable servers, notably those that are running obsolete versions of the Exim mail server. It is typically used to provide attackers with a backdoor.
- Linux.Rex.1 stands for Linux.Rex.1 is a remote access Trojan that was identified. Attackers can use it to obtain unauthorized access to Linux computers.
- Hand of Thief was a banking Trojan that targeted Linux users. Its goal was to steal financial information from the victim's computer.
- Linux.BackDoor.Irc.16: This Linux backdoor was created to allow attackers to take control of affected systems.
- Linux.Linux serves as the encoder.Encoder is a ransomware family that targets Linux systems, encrypting files and demanding a fee to recover them.
- Rootkits: Rootkits are a type of spyware since they are designed to disguise themselves on a compromised machine. Some Linux-specific rootkits have previously been discovered.
- Linux.Wifatch (a.k.a. Ifwatch): While not malicious in the traditional sense, Linux.Wifatch was a piece of self-replicating malware that aimed to improve the security of IoT devices by patching vulnerabilities and removing other malware.[21]

2.6. Android

Because Android is the most prevalent mobile operating system in the world, it is a frequent target for spyware and malware.

- HummingBad: HummingBad was a mobile virus family that predominantly affected Android smartphones via malicious apps. It obtained control over infected devices and earned false advertising money.
- Judy virus was distributed mostly through malicious apps on the Google Play Store. It generated cash for its operators by repeatedly clicking on advertisements without the user's permission.
- SpyDealer is a powerful Android spyware that can monitor and steal sensitive information such as call records, SMS messages, and even audio from a device's microphone.
- Chrysaor: Chrysaor is Android malware that was thought to be related to the iOS Pegasus spyware. It has the ability to take control of a user's device, record chats, and access sensitive data.
- Ztorg is a malware that was spread via malicious apps on the Google Play Store. It was capable of rooting infected devices, giving attackers complete control.
- Gooligan: a malware variant named Gooligan was discovered that targeted Android devices. It gained access to Gmail, Google Photos, Google Docs, and other Google services by compromising Google accounts and stealing authentication credentials.
- BankBot is a mobile banking Trojan designed particularly for Android users. It is capable of stealing banking credentials by displaying bogus login pages on legitimate banking apps.
- DressCode is a mobile malware family that created a botnet by infecting devices. It could be used for a variety of harmful reasons, including DDoS assaults.

- Joker (Bread): Joker is a sort of malware designed to steal SMS messages, contact lists, and device data. It has been discovered in a number of apps on the Google Play Store.
- X-Note: X-Note is Android malware capable of intercepting text messages, recording phone calls, and stealing sensitive data from affected devices.[22]

2.7. iOS

When compared to other platforms, iOS is noted for its excellent security protections, which make it more difficult for spyware and malware to access the system.

- Pegasus: The NSO Group created Pegasus, a very complex and notorious spyware. It can infect iOS devices by taking advantage of operating system flaws. Pegasus is capable of recording phone calls, capturing keystrokes, monitoring communications, and tracking the user's position. It has been used to target journalists, activists, and government officials.
- Predator: Cytrox created the spyware known as Predator, which is designed to target the iOS and Android operating systems.
- Xsser mRAT: Xsser mRAT is an iOS remote access Trojan that can steal a variety of data, including text messages, call records, contacts, and location information. It was mostly available in China and Taiwan.
- Pangu: While the Pangu jailbreak tool is not spyware in and of itself, it is worth noting that jailbreaking your iOS device (removing software restrictions) can possibly expose it to spyware and other security concerns. Users who jailbreak their handsets must take extreme caution.
- AceDeceiver: AceDeceiver is a family of iOS malware that infects non-jailbroken iOS devices by exploiting Apple's FairPlay mechanism. It has the ability to deceive consumers into downloading dangerous programs.
- KeyRaider is a type of iOS malware that targets jailbroken devices. It stole Apple account passwords, disabled unlock functions, and encrypted iTunes backups for users.
- YiSpecter is an iOS malware family that mostly targeted devices in China and Taiwan. It has the ability to download and install dangerous programs without the user's knowledge.
- Dendroid is a remote access Trojan that can infiltrate Android and iOS devices. While it predominantly targets Android smartphones, it is also capable of infecting iOS devices.[23]

2.8. Spyware similarities

Spyware, regardless of its precise type or source, shares numerous remarkable operational commonalities. To begin with, spyware is covert in nature, meant to operate without the user's agreement or awareness. It usually infiltrates a target system covertly, using deceptive methods such as phishing emails or malicious downloads. Once entered, spyware has a common goal: to collect sensitive data, monitor user behaviors, and send this data to a distant party, usually for harmful intentions. Spyware usually employs complex evasion strategies to prevent detection by security software and communicates over a variety of channels, including command and control servers. Furthermore, it can keep its presence on the infected machine indefinitely, making removal difficult. While spyware can take various forms, these common traits highlight the fundamental harm it poses to individual privacy and cybersecurity.[24][25][26]

Table 1 - Differences of malicious software	
Spyware	❖ **Unauthorized software known as spyware "spies" on computer activities and relays information back to its owner.** ❖ **Usually, the computer owner is unaware of or does not consent to its installation.** ❖ **Spyware has the ability to capture keystrokes and is useful for identity theft.** ❖ **Spyware tries to conceal or disguise its operations and files.** ❖ **Spyware can impede a computer's performance or make it operate slowly by consuming more memory and CPU power.**
Malware	❖ **The phrase malware is a compound word that combines the terms malicious and software.** ❖ **It can be used to refer to several threat classifications, including Trojan horses, worms, and viruses.** ❖ **Sometimes, the word "virus" is used to refer to any kind of malware.** ❖ **A virus works by changing or modifying files to infect them; it then needs the user's help to keep spreading.** ❖ **In order to propagate without human interference, worms operate in memory and look for other victims.** ❖ **A Trojan horse is a malevolent software concealed within a legitimate executable file.** ❖ **The majority of contemporary threats lack distinction between the various classifications and are better characterized as malware.**
Adware	❖ **Similar to shareware and freeware, adware is a valid software distribution method that makes money from embedded advertisements.** ❖ **Adware providers log users' online browsing behaviors and show personalized advertisements by utilizing tracking cookies and additional monitoring tools.** ❖ **A lot of adware programs don't make it obvious that they will track and**

	report back on any activity on your computer. ❖ **Adware has the potential to impact system performance by inadvertently using processor and memory resources.**
Parasiteware	❖ **Parasiteware has the ability to change the default search engine and/or home page of a web browser.** ❖ **Affiliate advertising links are hijacked or overwritten by parasites in order to divert legitimate ad revenue.** ❖ **Redirected websites are very annoying, even when parasiteware doesn't directly harm the user of the machine.** ❖ **Legitimate websites may face closure due to insufficient revenue.**
Phishing	❖ **Phishing schemes consist of two parts: social engineering and spam.** ❖ **The former is carried out through spam emails that entice the recipient to visit a malicious phishing website or provide personal information.** ❖ **Phishing scammers aim to gather as much personal data as possible about their target to get access to their accounts or steal their identity.** ❖ **Phishing emails sometimes have poor writing quality, including misspelled words and improper language.**
Botnets	❖ **Originally designed for IRC channel maintenance, bots are utilities.** ❖ **Malicious bots have infected tens of thousands of computers, causing them to become inactive without the owner's knowledge.** ❖ **Thousands of hacked bot PCs can be controlled by botnet masters to carry out the same malicious operation simultaneously.** ❖ **DDoS attacks and spam dissemination are frequently carried out via botnets.**

2.9. Spyware statistics

Table 2 - Statistics based on Spyware activity

Figure 1 - Percentage of targeted people by occupation

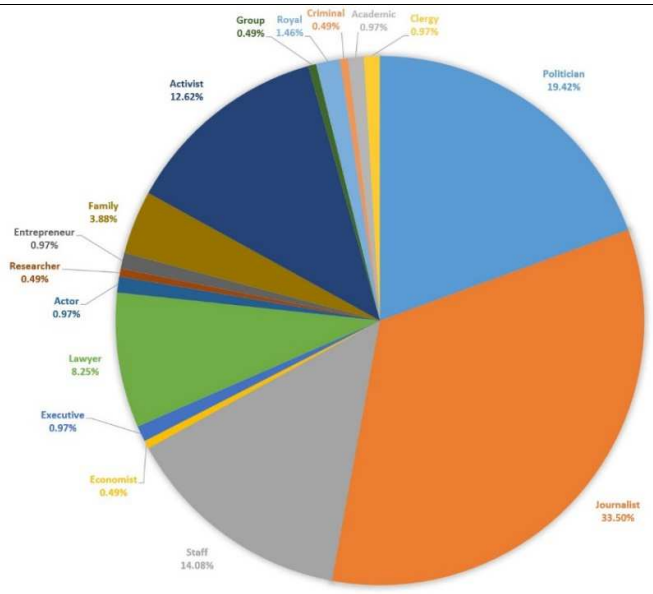


Figure 2 - Percentage of targeted operating systems

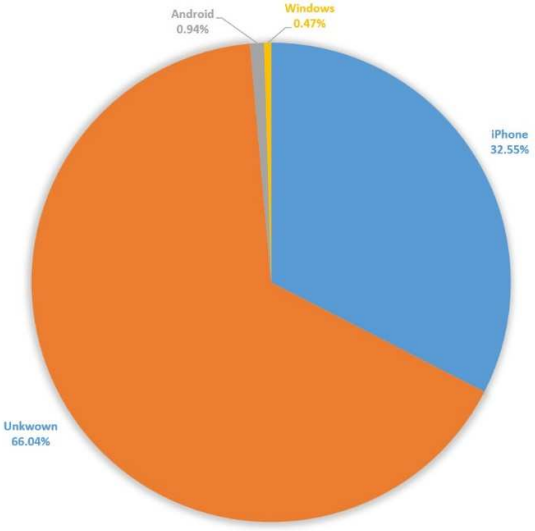


Figure 3 - Ways of exploitation

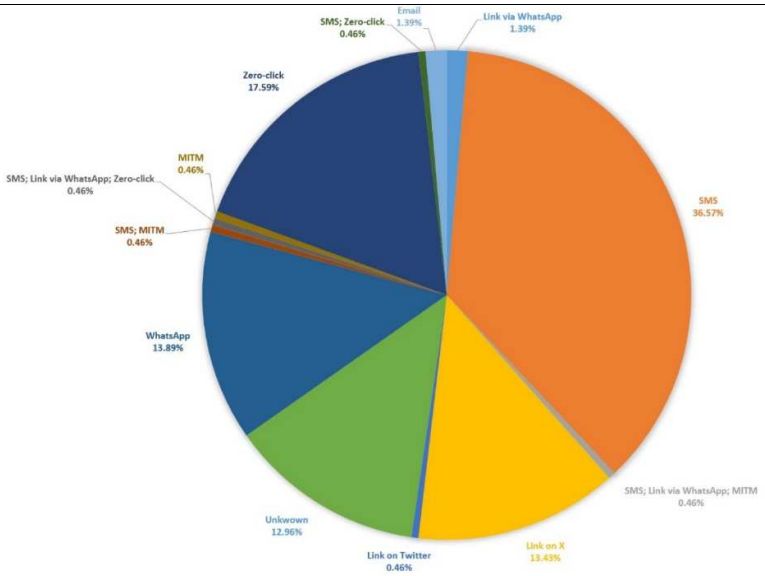


Figure 4 - Exploit methods by name or CVE

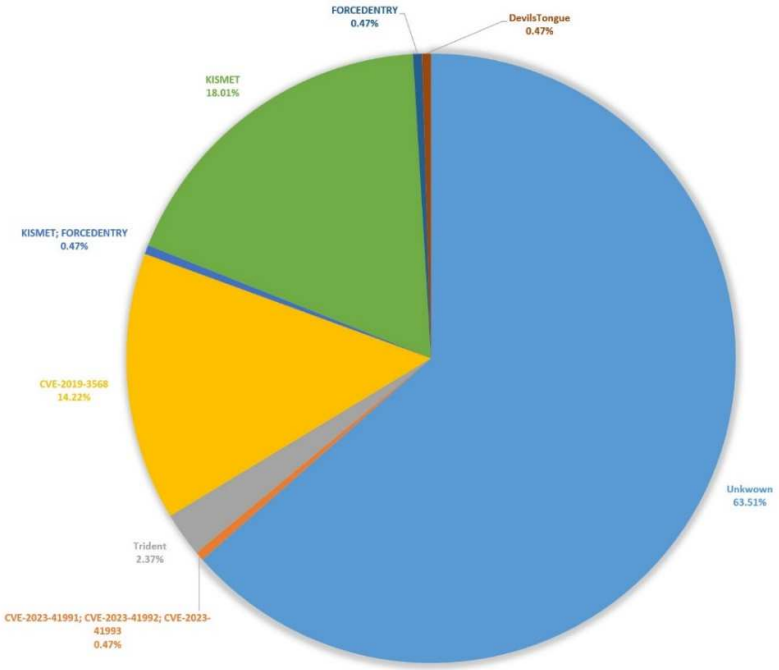


Figure 5 - Percentages of targeted people by country

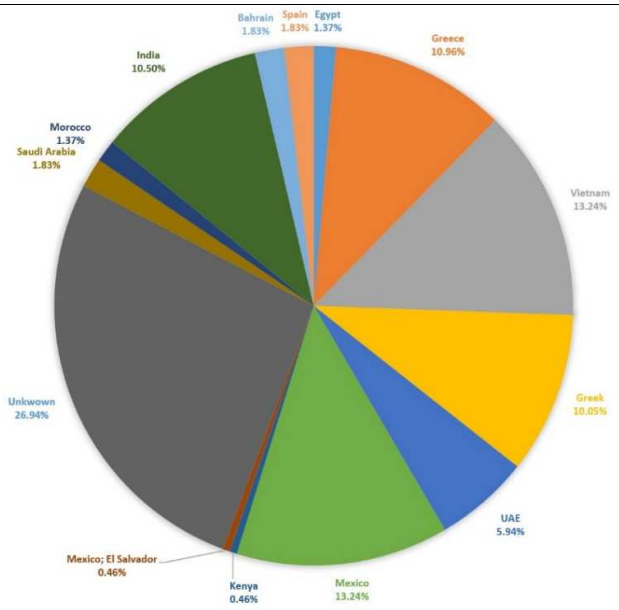


Figure 6 - Percentages of the three most known

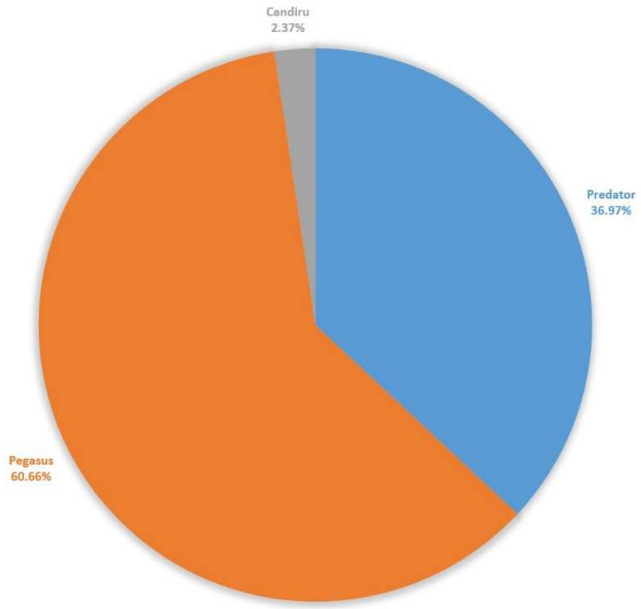
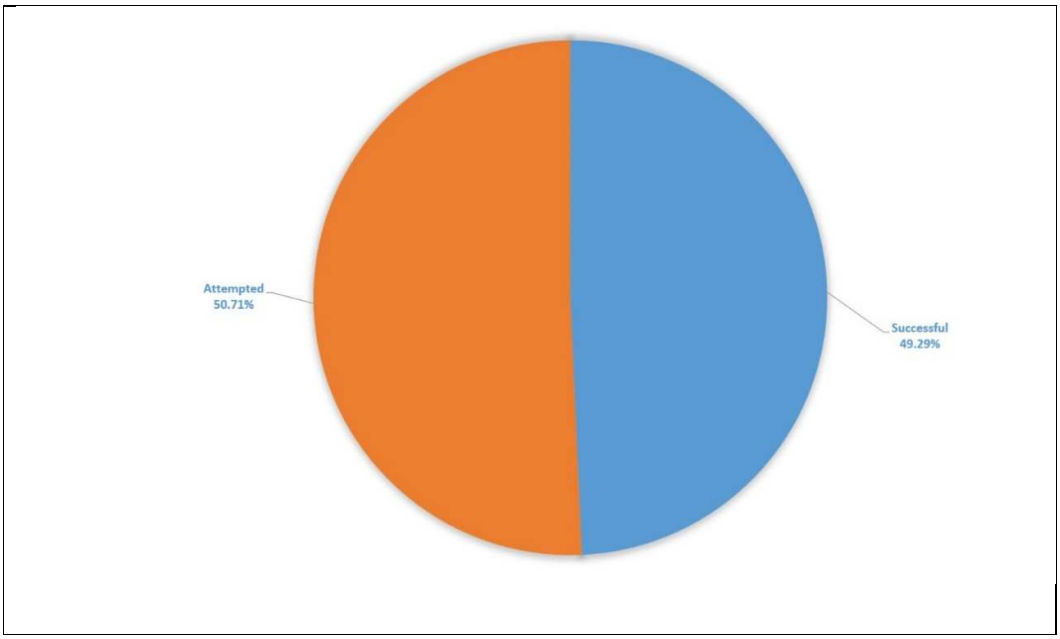


Figure 7 - Percentage of successful exploitation



[27][28][29]

2.10. Impact on encrypted communications

In today's interconnected world, encrypted communication applications are an important part of digital privacy and security. Advanced encryption techniques are used in these applications to ensure the secrecy and integrity of communications and data transmitted between users. They provide end-to-end encryption, which ensures that only the sender and recipient can decode and read the content, making it extremely difficult for eavesdroppers or third parties, including service providers, to access the data. Signal, WhatsApp, and Telegram are all popular encrypted communication apps, each with its own approach to security and features. Signal, for example, is well-known for its open-source technology and dedication to anonymity, making it a popular choice among activists and security-conscious users. WhatsApp, which is owned by Facebook, delivered end-to-end encryption to a large user base, boosting the privacy of daily communications. While Telegram provides strong encryption, it is most recognized for its emphasis on group chats, media sharing, and the option for self-destructing communications. These apps are regarded not only for protecting individual privacy, but also for facilitating safe communication in business, journalism, and political activism. However, its use has raised disputes over law enforcement's ability to investigate criminal activity and the balance between privacy and national security, highlighting the ever-changing nature of this essential part of the digital landscape.

Spyware can have a major negative influence on the privacy and security of encrypted communications. Malicious software intended to penetrate and observe a user's device or internet activities without authorization is referred to as spyware. The security of encrypted communication apps can be jeopardized by spyware infection in several ways:

Table 3 - Spyware infection features	
Keylogging	Keystrokes may be recorded by spyware to obtain the passphrases or encryption keys needed to protect encrypted communications. Despite the encryption being in place, this enables the attacker to decrypt and read the messages.
Screen Capture	Certain spyware has the ability to record or take snapshots of the screen, which could lead to the content of encrypted messages being seen as they are shown.
Message Intercept	Bypassing the encryption protection, sophisticated spyware can intercept messages either before or after they are decoded on the recipient's device.
Metadata Collection	Spyware can still gather metadata, such as who is chatting with whom and when, even while the content of encrypted communications is protected. This metadata might provide important details about a user's social network and activities.
Backdoor Creation	Spyware occasionally uses flaws to open backdoors in encrypted communication apps, giving the attacker direct access to messages and circumventing encryption.
Data Exfiltration	Malicious actors that wish to decrypt the information at their own discretion can obtain encrypted data or encryption keys through the exfiltration of this data by spyware.

By using trustworthy and frequently updated encryption programs, installing apps with caution, and keeping their devices and software up to date, users can reduce the negative effects of spyware on encrypted conversations. The security of encrypted communications can also be improved by using extra security measures like two-factor authentication and routine virus detection. But it's important to realize that no system is impervious to focused and sophisticated spyware attacks, so it's critical to remain vigilant and up to date on new dangers.[30][31][32]

2.10.1. EncroChat

EncroChat was an encrypted chat platform that became well-known for being used by criminal groups and people involved in unlawful operations. It was a subscription-based encrypted messaging service that promised customers anonymity and security. To secure its users' privacy and communications, EncroChat provided end-to-end encryption, self-destructing messages, and other security measures. However, law enforcement organizations in several nations thought that it was being used by criminals to coordinate and plan unlawful activities like as drug trafficking, money laundering, and other organized crime. Several countries' law enforcement agencies, including the European Union's law enforcement agency Europol, collaborated to infiltrate the service and decode messages, resulting in several arrests and the collapse of criminal networks. The EncroChat case exemplified the persistent conflict between privacy and security concerns. While encryption is an important tool for protecting people's privacy and security, it may also be used to conceal illegal activity. The EncroChat case highlighted the difficulties that law enforcement organizations confront in balancing these interests.

EncroChat phones were advertised as providing users with complete anonymity, discretion, and non-tracking capabilities. It also included features that made sure communications would automatically be deleted and a unique PIN that would allow you to erase everything on the device. This would enable users to delete compromising messages fast, say at the moment of a police arrest. Furthermore, the reseller or support desk could remotely wipe the gadget. On a global scale, EncroChat offered crypto telephones for approximately EUR 1,000 per. Additionally, it provided memberships with 24/7 assistance and global coverage for 1,500 EUR over the course of six months. Judiciary and law enforcement authorities throughout the European Union continue to pay close attention to the illicit use of encrypted communications. In March 2021, OCGs using encryption suffered yet another setback when the SkyECC tool was taken down.

The EncroChat service catered to devices known as "carbon units," which were intentionally meant to deactivate GPS, camera, and microphone features for privacy reasons. These devices, which frequently used modified Android hardware, came pre-installed with applications such as EncroChat, an OTR-based messaging app that routed conversations through a central server in France, EncroTalk, a ZRTP-based voice call service, and EncroNotes, which allowed users to create encrypted private notes. Dual boot modes were available on several handsets, notably those based on the BQ Aquaris X2 and Samsung devices, as well as non-Android BlackBerry phones. hitting merely the power button launched a false Android home screen, while simultaneously hitting the power and volume buttons triggered a secret, encrypted partition that enabled confidential communication via EncroChat's French servers. A "panic button" feature enabled users to wipe all phone data by entering a specified PIN from the unlock screen. EncroChat's server IP address was assigned to the French web hosting business OVH, while its SIM card was provided by the Dutch telecoms corporation KPN. Despite being available in the Middle East and other locations, EncroChat devices gained special appeal in Europe, becoming the "industry standard" among criminals, with reported pricing of €1,000 per and €1,500 for a six-month contract.[33][34]

2.10.2. Sky ECC

Sky ECC, also known as Sky Secure E-Communications, is a secure communication solutions provider with a primary focus on encrypted messaging and mobile device security. Their solutions are intended to give individuals and businesses with a high level of security and privacy in their electronic communications. Sky ECC's major features include encrypted communications, which ensures that messages are jumbled and only readable by the intended receiver with the right decryption key, protecting the message's confidentiality. Sky ECC also offers secure mobile devices that have been designed and fortified to protect against a variety of threats such as hacking, malware, and surveillance. Because the company emphasizes the significance of user anonymity and privacy, it is an appealing option for anyone looking to protect critical information and communications from potential breaches. However, Sky ECC, like other encrypted communication platforms such as EncroChat, has been under attention from law enforcement agencies around the world owing to worries that it could be used by persons or organizations engaged in unlawful activity. The balance between privacy and security is a point of contention in the context of such platforms, and the legal position and reputation of organizations such as Sky ECC might change over time. As a result, it is vital to stay current on any legal or regulatory developments pertaining to such services, particularly if considering their usage.

Authorities have been able to keep an eye on the information flow of about 70 000 Sky ECC customers as of mid-February. Several EncroChat users migrated to the well-liked Sky ECC platform following EncroChat's launch. The tool was the subject of investigations that began in Belgium after mobile phones found during searches revealed that suspects were using Sky ECC. The tool, which is run from the United States and Canada using computer servers located in Europe, has its own architecture and applications, and is utilized by about 170,000 people globally. Approximately three million messages are sent and received with Sky ECC every day on a global basis. Belgium and the Netherlands are home to more than 20% of the users. Claiming to be the “most secure messaging platform you can buy,” Sky ECC is so sure of the strength of its systems that it is willing to pay a hefty sum to anyone who can crack one of its phones' encryption. "Sky ECC did not authorize or cooperate with the authorities conducting the investigation or with the individuals distributing the phony phishing application," the business stated. According to the company, the Sky ECC software is kept safe on the phone in a secure container that guards against malware like keyloggers and surveillance tools like the popular Pegasus spyware from Israeli company NSO Group. While 2,048-bit SSL encryption protects network connections, 512-bit elliptical curve cryptography encrypts all messages. The fact that the company does not save encrypted messages on its servers is one of its selling features. It states: "We hold the encrypted communication for up to 48 hours before deleting it if your contact isn't reachable (for example, if their device is off). The communication is lost if they do not read it inside that window of time. In a statement released late Friday night, the corporation stated that it strictly rejects any claim that it serves as the "platform of choice for criminals" and that any illegal conduct is forbidden on its platforms. It stated, "Any accounts used for criminal activity are deactivated immediately.". In a statement, Sky ECC stated that it was "actively investigating and pursuing legal action against the offending individuals for defamation, fraud, injurious falsehood, trademark infringement, and impersonation." "A much clearer understanding of the inner workings of the criminal organizations, their global character, unlimited financial means, their unscrupulousness and their aggressiveness" was provided by the decoded texts. The goal of the investigation was to demonstrate that Sky ECC phones were only ever used for illegal conversations and that Sky ECC was aware of this.[35][36]

2.10.3. ANOM

ANOM was a secure messaging platform that enabled encrypted communication. It rose to prominence, however, as part of a large-scale multinational law enforcement operation aimed at destroying organized crime networks. Law enforcement authorities, particularly the Federal Bureau of Investigation (FBI) in the United States and the Australian Federal Police (AFP), created and distributed ANOM. The ANOM operation began after law enforcement authorities infiltrated and compromised other encrypted communication systems used by criminals to plan illegal acts, such as EncroChat and Sky ECC. Following the demise of these platforms, the criminal underworld sought new encrypted communication channels, resulting in the promotion of ANOM by undercover officers and informants. ANOM offered its users a safe and encrypted messaging service, leading them to feel that their discussions were private and secure. However, they were unaware that law enforcement authorities had access to the platform's messages. This operation resulted in many arrests and the dismantling of various criminal networks. ANOM exemplifies how law enforcement agencies use a variety of ways to combat organized crime, even in the digital age, and the balance between privacy and security remains a point of contention in the context of such operations. ANOM, which was created to target worldwide organized crime, drug trafficking, and money laundering networks, included attractive features like remote wipe and duress passwords. Using intelligence from 27 million messages exchanged between ANOM's criminal users, the FBI and the international coalition carried out a series of large-scale law enforcement actions across 16 countries, resulting in over 700 house searches, 800 arrests, and the seizure of significant amounts of contraband, including cocaine, cannabis, synthetic drugs, firearms, luxury vehicles, and more than $48 million in various currencies and cryptocurrencies. The success of Operation Trojan Shield/Greenlight positions Europol to expand its intelligence architecture, aiding in the continuous identification and targeting of high-value criminal groups on a global scale.

How it works

The ANOM devices were built with a messaging app running on Android cellphones that was modified to disable common functions such as voice calling, email, and location services. Additional security features included scrambling the PIN entry screen to randomize number layouts, deleting all phone information when a specific PIN was entered, and an option for automated deletion if left unused for a specified length of time. To access the app, users performed a unique calculation within the calculator app, a method dubbed "security theater" by GrapheneOS's developer. Each user was granted a fixed identification number, which made it easier to link messages from the same person. Initially beta-tested in Australia with approximately 50 devices in October 2018, the gadgets were then supplied to the United States in 2020. The app's popularity grew thanks to word of mouth and encouragement by undercover agents, with Hakan Ayik, a trusted figure in the criminal underworld, unknowingly promoted to distribute and sell the gadgets on the illegal market. Following user requests for smaller and newer phones, the company manufactured and sold new devices, giving customer service and technical assistance. The app's most popular languages were Dutch, German, and Swedish. Despite a slow beginning, ANOM's dissemination increased dramatically beginning in mid-2019, reaching several hundred users by October 2019 and 11,800 devices with ANOM installed by May 2021, with around 9,000 in active usage spanning more than 100 countries. Europol said that it had collected 27 million texts from ANOM devices.
The FBI's operation, which involved collecting messages from thousands of encrypted phones worldwide, used a homemade code. Motherboard discovered this code and is disclosing bits of it that reveal how the FBI created its honeypot. The code reveals that

messages were discreetly replicated and delivered to a "ghost" contact who did not appear on users' contact lists. This phantom account effectively represented the FBI, and its law enforcement allies, allowing them to covertly monitor organized criminals' talks. Last year, the FBI and its international partners announced Operation Trojan Shield, which revealed their clandestine administration of Anom, an encrypted phone firm, spanning several years. Anom was intentionally marketed to criminals, reaching the hands of over 300 crime syndicates worldwide. This historic operation resulted in over 1,000 arrests, including accused high-level drug traffickers, as well as significant seizures of firearms, cash, narcotics, and luxury cars. Motherboard obtained the Anom app's core code and shared pieces of it to address public interest in understanding how law enforcement organizations are dealing with the "Going Dark" phenomenon, in which criminals use encryption to hide their conversations from police. The code reveals the hastened development process, the use of freely available web tools by Anom's developers, and how a specific code piece duplicated messages as part of one of the most thorough law enforcement operations ever conducted. The program communicates via XMPP, a well-established standard for transmitting instant messages. In addition, Anom added an extra layer of encryption surrounding messages. XMPP works by issuing each contact a handle that resembles an email address. In the instance of Anom, this featured an XMPP account for the customer service channel, which consumers could utilize. Another account was identified as the "bot." Unlike the visible help channel, the bot stayed hidden from Anom users' contact lists, operating quietly in the background, as evidenced by the code and photos of live Anom devices obtained by Motherboard. In practice, the program examined the user's contact list and, when it found the bot account, filtered it out and hidden it from view. This discovery is confirmed by law enforcement papers obtained by Motherboard, which confirm that the bot operated as a hidden or "ghost" contact, copying communications sent by Anom users.The code also discloses that in the message-sending section, the software adds location information to any message sent to the bot. Furthermore, the app's AndroidManifest.xml file, which lists the app's accessed permissions, contains the "ACCESS_FINE_LOCATION" permission. This backs up Motherboard's prior conclusions, which came from a thorough analysis of police files relating to Anom investigations. Many of the intercepted Anom messages in those documents had the GPS coordinates of the devices at the time of message transmission. While some cases reported by law enforcement indicated flaws in recording GPS locations inside the Anom system, authorities typically regard the coordinates as reliable, especially when cross-referenced with additional data such as pictures, as shown in police files. A large chunk of the code for managing conversations appears to have been borrowed from an open-source messaging app. The code is somewhat disorganized, with significant chunks commented off, and the app frequently logs debug messages directly to the phone. Motherboard has decided not to publish Anom's whole code due to fears that it may contain personally identifying information about those involved in the app's development. The majority of Anom app contributors were unaware of its covert use as an FBI tool for surveilling organized crime, and disclosing their identities may put them in danger. Motherboard has chosen against making the app public or sharing it further. Motherboard previously purchased one of the Anom phones from the secondary market following the disclosure of the law enforcement operation. In that particular example, the phone had a locked bootloader, making it more difficult to retrieve files from it. For the current code study, a source submitted a standalone copy of the Anom APK, which Motherboard then decompiled. To protect individuals from potential retaliation, Motherboard has provided anonymity to certain sources cited in this article. Decompiling an app is a routine process used by reverse engineers to gain access to the code used to create the app. It serves a variety of objectives, including fixing software faults, discovering vulnerabilities, and conducting study on how the program was created. Motherboard's analysis of the app was confirmed and expanded upon by two reverse engineering experts.[37][38][39]

3. Digital Forensics

Digital Forensics is a branch of forensics focusing on digital devices. According to National Institute of Standards and Technology (NIST) "Digital forensics is the field of forensic science that is concerned with retrieving, storing, and analysing electronic data that can be useful in criminal investigations. This includes information from computers, hard drives, mobile phones, and other data storage devices." [40]

Digital forensics utilizes a set of techniques with which digital crimes can be investigated. Such crimes are ransomware attacks against corporations that are performed to steal and encrypt valuable data until ransom is paid. Another example is Phishing campaigns where the attacker redirects users to different custom website, thereby stealing their information. Digital Forensics Analysts need to collect evidence and through their investigation are able to provide helpful evidence to indicate a suspect or to validate which malicious actions where performed and what was the attack result. Nowadays, unfortunately a lot of electronically committed crimes such as child pornography and terrorism are made known to the public. For this reason, Digital Forensics become a needed field and all people that are working on it must have the appropriate knowledge and expertise in order to do not undergo deterioration. Qualified researchers are considered experts in their field and their opinion can be used to investigate simple cases of fraud even murder.

3.1. Types of Digital Forensics

Digital forensics is applied to every digital device with stored information that when. evidence gets collected can be used by a court for example to strengthen the evidence process.

- Network Forensics: Network forensics is an important subfield of digital forensics that focuses on the investigation and analysis of network-based evidence to reveal malicious actions, security breaches, and cybercrimes. It entails collecting, preserving, and analyzing network traffic, logs, and digital artifacts to recreate and comprehend the sequence of events that led to a security incident. Network forensics experts use a variety of tools and techniques to detect and analyze network anomalies, intrusions, and unauthorized access, assisting organizations and law enforcement agencies not only in determining the scope of a breach but also in developing strategies to prevent future incidents. Network forensics plays a critical role in boosting cybersecurity and successfully responding to cyber threats by thoroughly inspecting network data.

- Computer Forensics: Computer forensics is a subfield of cybersecurity and forensic science that entails the analysis of digital devices and data to unearth evidence linked to criminal acts, data breaches, or legal issues. Computer forensic experts acquire, preserve, and analyze electronic data from computers, servers, storage devices, and digital media using a methodical approach. This procedure entails recovering deleted files, reviewing system logs, and looking for indicators of manipulation or unauthorized access. Computer forensics can help identify cybercriminals, data breaches, intellectual property theft, and fraud in criminal investigations, litigation, and corporate cybersecurity. It is critical in assuring the integrity and admissibility of digital evidence in a court of law, as well as contributing to the security and accountability of digital systems in our increasingly interconnected world.

- Memory Forensics: Memory forensics is a kind of digital forensics that focuses on the study and analysis of a computer's volatile memory (RAM) to elicit valuable information about security incidents, malware infections, and cyberattacks. Memory forensics, as opposed to typical disk-based forensics, allows investigators to access real-time data and

volatile artifacts that may not be preserved on disk, providing insights into ongoing processes, open network connections, and evidence of criminal activity that would otherwise go undiscovered. Memory forensics tools and techniques allow experts to identify malware, extract encryption keys, uncover attacker tactics, and recover critical evidence, making memory forensics an indispensable resource for cybersecurity professionals and digital investigators in understanding and responding to modern cyber threats.

- Mobile Forensics: Mobile forensics is a subfield of digital forensics that focuses on extracting, analysing, and preserving digital evidence from mobile devices such as smartphones, tablets, and other portable devices. This discipline is critical in criminal investigations, cybersecurity incidents, and legal matters. Mobile forensic professionals use a number of techniques and tools to recover data such as text messages, call logs, photographs, and application usage history, as well as unearth deleted or concealed data. With the rising prevalence of mobile devices, mobile forensics is becoming increasingly important in solving cases involving cybercrime, missing persons, corporate espionage, and other issues. It not only assists in the discovery of vital evidence but also in the preservation of such evidence for use in judicial processes, making it an essential component of modern investigative and security efforts.

- Cloud Forensics: Cloud forensics is a new area of digital forensics that focuses on investigating cloud-based services and data storage. Cloud forensics is critical for reacting to security events, legal investigations, and compliance needs in an age where enterprises and individuals rely on cloud platforms for data storage and processing. Documents, email messages, logs, and metadata are examples of digital evidence kept in remote cloud settings that must be collected, preserved, and analyzed. Experts in cloud forensics utilize specialized tools and procedures to track user activity, detect security breaches, and uncover potential data breaches or illegal access. Because cloud services are dynamic and frequently geographically distant, the complexity of cloud forensics necessitate a distinct skill set and understanding of cloud architecture, making it a key component in modern digital investigations and cybersecurity efforts.

- Smartphone Forensics: Smartphone forensics is a subset of digital forensics that focuses on the extraction, analysis, and preservation of digital evidence from mobile devices, specifically smartphones. Call logs, text messages, photographs, location data, application usage history, and other data are stored on these devices. Smartphone forensic experts recover this data using specific tools and procedures, even if it has been erased or encrypted, making it a valuable resource in criminal investigations, cybersecurity events, and legal actions. Mobile devices are an essential part of modern life, and their use in illegal actions or as potential sources of evidence is growing. As a result, smartphone forensics has evolved into a critical discipline in the field of digital investigations, ensuring that valuable information is gathered and preserved with integrity for use in legal proceedings or cybersecurity initiatives.

- IoT Forensics: IoT (Internet of Things) forensics is a subfield of digital forensics that investigates and analyses digital evidence created by interconnected IoT devices. As the IoT ecosystem grows, with smart devices ranging from home appliances to industrial sensors becoming more common, the need for IoT forensics becomes more crucial. Experts in IoT forensics collect, review, and preserve data from these devices to unearth evidence of security breaches, cyberattacks, and other digital crimes. This could include analysing data sent between IoT devices, examining device logs, and discovering vulnerabilities in the IoT ecosystem that can be exploited. IoT forensics is critical to understanding and addressing the unique security issues provided by networked devices, as well as assisting in detecting the source of security breaches and assuring compliance

in a variety of sectors, including healthcare, transportation, and industrial control systems.

- Wearable Forensics: Wearables forensics is a subfield of digital forensics that focuses on the study of data generated by wearable devices such as smartwatches, fitness trackers, and augmented reality glasses. These little gadgets, which are commonly worn on the body, collect a wide range of personal data, such as health indicators, location data, and conversation logs. Wearables forensics professionals use novel approaches and technologies to extract and analyze data, revealing significant evidence in a variety of scenarios such as criminal investigations, health-related occurrences, and workplace disputes. These devices' insights can provide a comprehensive perspective of an individual's activities and interactions, making wearable forensics a critical component in understanding the digital footprint left by wearable technology and its potential ramifications in legal or investigative proceedings.[41][42][43][44][45][46]

3.2. Evidence

Digital Evidence can be found after malicious activities. According to National Institute of Justice (NIJ) “Digital evidence is information stored or transmitted in binary form that may be relied on in court.” [47]

Here is a more comprehensive list of the kinds of evidence that digital forensics investigators collect, which includes additional context and details:

- Digital Documents and Files: As part of their investigation, digital forensics experts painstakingly gather a variety of digital documents and files. Text documents, spreadsheets, PDFs, pictures, and videos can all be among them. These kinds of files frequently have vital information that clarifies a variety of cybercrimes and digital catastrophes.

- Email correspondence: In many investigations, email correspondence is a veritable gold mine of information. The text, timestamps, and metadata of sent and received messages—as well as any attachments—are examined by investigators in order to gather useful evidence.

- Chat and Instant Messaging records: Analysts examine chat and instant messaging records from well-known applications like as Facebook Messenger, Slack, and WhatsApp. These logs are carefully examined for hints, linkages, and pertinent case-related conversations.

- History of Web Browsing: A wealth of evidence may be found in the historical records of web browsing habits. It can help investigators put together a whole story by offering information into a suspect's internet behavior, interests, and any connections to illegal activity.

- Social Media Data: Digital forensics may learn a great deal from social media sites. Posts, private messages, buddy lists, and comments are among the information gathered by investigators that might provide light on a suspect's activities, motivations, and connections to online harassment or wrongdoing.

- Metadata: Frequently disregarded yet extremely important, metadata includes data like the creation date of files, modification history, and geographical information. These particulars help create chronologies and comprehend the background of digital evidence.

- Registry and System Logs: Windows registry entries and system logs are carefully examined by digital detectives. These logs provide important information for the investigation since they document system events, user activity, and possible security breaches.

- Network Traffic and Packet Captures: Tracking data exfiltration, determining network infrastructure vulnerabilities, and tracking the source of cyberattacks all depend heavily on the data gathered from these sources. In trials involving cybersecurity, this evidence may be crucial.

- File System Metadata: Information on the characteristics of files and folders, access times, and permissions can be used to build a thorough picture of the chronology and order of events surrounding the inquiry.

- Data Extraction from Mobile Devices: Data extraction from smartphones and tablets is a common task in mobile forensics. Call logs, SMS messages, contact lists, images, and data from other apps could all be included in this data. Data from mobile devices can be essential to comprehending the relationships and activities of the suspect.

- Database Records: Digital forensics specialists examine the data kept in relational or NoSQL databases when databases are involved. These documents may include vital details that are relevant to the case.

- Cloud Services Data: Another interesting source of data is information kept in cloud services like Dropbox, iCloud, and Google Drive. Legal procedures may be followed in order to obtain access to this data, which might include evidence that is pertinent to the investigation.

- Malware and malicious code: When faced with cases involving malicious software or code, investigators analyze the malware's behavior and code to understand how it affects the system and identify where it came from. This information is crucial for cybersecurity investigations.

- Data and File Recovery from Deleted Files: Digital forensic techniques are used to recover data and files from deleted files. Recovery of deleted data is crucial because it frequently contains important evidence that suspects may have purposefully hidden.

- Server Logs: When conducting an investigation into a server attack or a network breach, server logs are essential. These logs assist investigators put the puzzle pieces together by providing information about the tactics used by attackers and the sources of the breaches.

- Geolocation Data: This information can be very useful in situations involving location-based crimes or alibis. It is typically obtained from mobile devices and specific applications. It can reveal a suspect's precise location during particular occurrences.

- Disk images and virtual machines: Digital forensics specialists make disk images of storage media to retain evidence in its original condition. As frozen snapshots of the digital world, these photos allow for in-depth examination without changing the original data.

- Digital signatures and hash values: These two elements are essential to preserving the integrity of digital evidence. They are used to ensure that no tampering has occurred with the evidence while it is being investigated.

- Memory Analysis: Memory analysis is used to find open connections, active processes, and indications of intrusion in situations involving live systems. Real-time insights into ongoing digital incidents can be obtained from this analysis.

- Audio and Video Recordings: In cases involving cyberbullying, harassment, or digital crimes containing multimedia content, multimedia evidence in the form of audio and video recordings is frequently crucial. These recordings are painstakingly gathered, and their applicability to the inquiry is evaluated.[48][49][50][51][52][53][54]

To ensure the integrity of the evidence they gather, digital forensics investigators must follow certain protocols. To make sure that no digital stone is overlooked in the hunt for justice, the precise kinds of evidence that are gathered depend on the particulars of each case.

3.2.1. Collecting digital evidence

As more people utilize the Internet, a lot of documented proof on each user can be found. Evidence for cybercrimes can be gathered from a variety of sources. ISPs typically keep copious logs of user activities that include access points, IP addresses utilized, start and finish times of connections, etc. These logs are typically retained for a few days, but recently, because storage media is becoming less expensive, log retention periods have been extended to one or even 10 days. The majority of ISPs are also able to provide router data for use in cybercrime investigations. It is anticipated that law enforcement would want even more data from ISPs about Internet users in the near future. There are currently forensics techniques in place that require tapping particular sessions and real-time access to communication data. System logs from firewalls, DHCP servers, mailers, and even currency files are additional sources of proof. However, it should be mentioned that forensics techniques can be used to discover evidence unrelated to criminal activity. It is possible to gather details about someone's tastes, way of life, friends, and relationships with other people, which raises privacy considerations.[55]

3.2.2. Technical challenges

The demand for developing Digital Forensics methods and tools to identify assaults has increased due to the rise in cybercrimes. There has also been a contention that investigators in Digital Forensics ought to possess the same skill sets as their adversaries, or hackers. In addition to the requirement for investigators to create and implement appropriate protocols and tools for conducting digital investigations, a variety of technical, social, procedural, and legal concerns must also be addressed. Both the absence of theoretical framework and lack of standards in the field of digital forensics lead to procedural issues. Ad hoc techniques and instruments for extracting digital evidence might reduce the evidence's dependability and trustworthiness, particularly in a criminal prosecution when the evidence and the procedures used to gather it can be contestable. Practitioner bodies and organizations have recently begun working to offer recommendations for standardizing forensics processes to address this challenge. Technical obstacles include physical impediments that prevent investigators from accessing the sources of evidence, such as routing tables in routers, and the diversity and heterogeneity of the infrastructure. Analyzing dates and timelines on gathered data is made more challenging when evidence is tracked over the Internet. Furthermore, to apply specific methods in an effort to find and gather pertinent traces, it is necessary to assume that an attack has occurred in order for most forensics models to be applied. Thus, when the forensic inquiry is initiated, the kind and attributes of the attack must be recognized and comprehended. On the other hand, risks stemming from the Internet are increasing rapidly. Furthermore, gathering, storing, and analyzing a sizable amount of data is usually necessary for forensics techniques. This places a lot of demands on the systems in use, particularly when it comes to cybercrimes. Another problem is that when investigators are faced with a large amount of material, they frequently struggle to select the most important or pertinent portions from the rest. Often, data mining techniques are used to

make the analysis easier. Additionally, information must be gathered while computers and servers are still operational to investigate cybercrimes. Under these circumstances, carrying out a "live" discovery procedure involves much more difficult technical obstacles. In addition to the difficulties that come with doing Digital Forensics, cybercriminals frequently use a variety of strategies to obstruct inquiries and legal actions. These include of taking steps to obstruct investigations, remove or obscure evidence, or even cast doubt on the evidence gathered during the prosecution process. Changing file extensions, using swap space, disk wiping software, physically destroying media, anonymizing techniques, using free anonymous email accounts and internet access, using other people's access, cryptography, and steganography are examples of traditional anti-forensic techniques. Particularly, the use of encryption creates major obstacles for the forensics procedures. The usage or export of powerful cryptography is prohibited in many nations, yet retrieving evidence is nevertheless hampered by even weak cryptography. It should be highlighted, however, that one of the best ways to combat cybercrime is to employ encryption. A further challenge facing Digital Forensics is anonymous online data storage. A lot of online retailers provide storage services, which thieves can take advantage of by utilizing credit card information that has been stolen. Criminals also frequently decide to carry out their illegal acts from nations with lax regulations pertaining to cybercrime and computer crime. Lastly, people who engage in offensive online behavior frequently obstruct investigations by using compromised computers in other nations, taking advantage of disparate or contradictory laws, legal codes, and procedures.[56][57]

3.2.3. Legal challenges for Digital forensics

The legal aspects of cybercrime investigation and prosecution involve jurisdictional disparities, digital evidence management, requirements for legitimate investigations, and privacy protection.

Digital data as evidence

Conventional and cybercrime differ greatly in terms of commission and prosecution. Because present legal systems are designed to handle traditional forms of crime, it is particularly challenging to identify, investigate, and prosecute cybercriminals. Cybercrime does not require the criminal to be physically present, there are no fingerprints and/or no physical presence at all. Offenders can also select a location that is convenient for them. The method of conducting a Digital Forensic investigation is scrutinized closely for the integrity of the investigation process as well as the evidence, which is defined as the data used to support facts. Any information gleaned from an electronic device or digital medium that supports the veracity of an act is referred to as electronic evidence. The fragility and transience of many sorts of computer evidence pose concerns rather than e-evidence's inherent differences from other forms of evidence. Whether and to what degree digital footprints and computer data can be viewed as documentary evidence is a basic subject that needs to be taken into consideration. Analysts must gather and analyze massive amounts of data as part of their information-intensive process. Following a significant criminal incidence, Digital Forensic investigations are frequently employed as a post-event reaction. Information acquired and reported determines how well laws are enforced and prosecuted. Although the evidence must be taken into account and assessed, the majority of cybercrimes lack tangible proof. Data can easily erased or vanished, making them volatile even though they may later be categorized as evidence. Without leaving evident signs, it is undoubtedly simpler for a culprit to erase or change cyber evidence. The digital evidence is brittle as careless access and handling can quickly destroy it. Evidence derived from networks needs to meet all the requirements of traditional evidence. It must first and foremost be admissible, that is, it must adhere to the legal standards and guidelines in the criminal justice system. E-evidence needs to be unquestionably real, meaning that it needs to be able to be positively linked to the incident and gathered in compliance with formal guidelines to prove its validity. Information security procedures can be applied to protect the dependability and caliber of data that has been gathered. Standard procedures and methods for gathering, preserving, and

presenting stored content are necessary to demonstrate the validity and integrity of the material in court. Considering the close relationship between standardization and the use and handling of data and information gathered by detection tools, the European Commission highlights the necessity of developing technical standards to guarantee that the data gathered complies with legal requirements for its use in court proceedings. Additionally, it has been suggested that independent testing and certification be applied to the technical means and procedures. Particular criminal procedure regulations deal with the sources of evidence that law enforcement can access. The applicable law governs the procedures that can be used to establish facts in court. Nonetheless, several questions about the applicability of these regulations are brought up by cyberspace. The guiding principles of evidence in the relevant nation have a significant impact on whether computer record evidence is admissible in court. [58][59][60]

Search for evidence and jurisdiction

In a traditional setting, a search entails obtaining tangible evidence that has previously been documented or registered. The need for acquiring legal authorization to conduct an offline search is the presence of reasonable suspicion that the data in question is present in a certain location and could provide evidence of a particular criminal offense. The geographic reach of a warrant issued by a judge or court granting access to digital data is one consideration when using search and seizure warrants in a cyberspace setting. Digital Forensic autopsies are no longer carried out on lone computers with limited storage. Rather, networks of linked computers are already within the purview of possible evidence. Any connected systems that fall under the investigating authority's purview may be subject to a legally permitted search warrant that starts at one location. To expeditiously extend the search or similar access to the other system when its investigating authorities search a particular computer system or a portion of it and have reason to believe that the data sought is stored in another computer system and such data is lawfully accessible from or available to the initial system. This will require the adoption of legislative measures in addition to other measures as may be required. The equipment used to store the data under search is frequently situated in another state or jurisdiction. National borders are crossed by network boundaries. The investigation and prosecution of electronic crime, despite the global nature of the Internet, are closely tied to territorial sovereignty and jurisdiction that is clearly defined. The international community has established well-established procedures for both receiving and offering legal aid. But these procedures take time, and there are frequently restrictions on the kind of help that can be provided. The Convention on Cybercrime's drafters extensively deliberated over the topic of when an investigative authority may unilaterally access data maintained in another state without requesting reciprocal help. Trans-border access to stored computer data in two circumstances: first, if the data being accessed is publicly available; and second, if the investigating authority has used a computer system under its jurisdiction to access or receive data located outside of its borders and has obtained the person's consent, which is voluntary and lawful, to disclose the data to the investigation unit through that system. The definition of a "person" who is "lawfully authorized" to divulge data varies based on the situation, the individual, and the relevant legal framework. Some have claimed that in a multinational internet environment, the extraterritorial extension of criminal procedure jurisdiction could reinforce sovereignty. Nevertheless, it is indisputable that this clause is a compromise that attempts to combat cybercrime while undermining a state's generally recognized sovereign rights.[61][62]

Impact in privacy

The application of forensic techniques can potentially violate a citizen's basic right to privacy. Therefore, compliance with the legal restrictions and privacy-related legal assurances outlined in legislation is necessary for the lawfulness and, by extension, admission of electronic evidence in court. The gathering and subsequent processing of electronic evidence must adhere to the provisions ensuring data privacy and communication secrecy, as mandated by material and procedural standards. Legislators must outline the steps to take and standards to be met to

investigate a cybercrime occurrence in compliance with the principles of necessity and proportionality. One important concept of European law, proportionality, also calls for evaluating the measure's necessity and fitness for achieving its objectives. The goal must be weighed against the gravity of the interference, which is to be assessed by considering, among other things, the quantity and kind of individuals impacted and the severity of the adverse consequences. Most European nations control the admissibility of general or sector-specific data protection regulations. However, there are significant differences in the applicable legal framework, particularly when compared to common law nations. These differences include the constitutional background, the legal context, the legislative approach used to enact the relevant provisions, and the substantive law requirements. The Fourth Amendment and how the courts, particularly the US Supreme Court, have interpreted it provide the fundamental constitutional underpinning for communication and informational privacy in the US. The Fourth Amendment upholds everyone's right to be free from arbitrary searches and seizures of their person, residence, papers, and belongings. Generally speaking, forensics techniques used during a criminal investigation are subject to rather stringent procedural assurances and controls, including a court warrant.[63][64][65][66]

Windows

The related logs can be found under the path “C:\Windows\System32\winevt\Logs” and an examiner will start by sorting the files by size. The size indicates which file has the most records written as a candidate to contain the most valuable information. The files are EVTX and can be examined by using the default windows app Event Viewer or with a third-party solution.

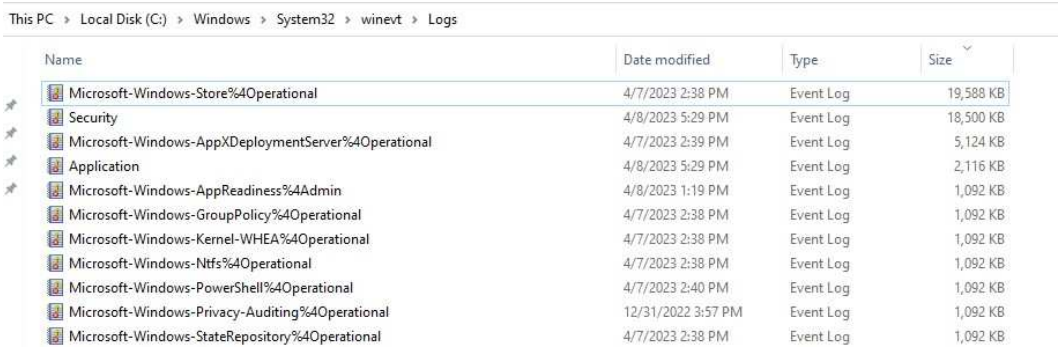


Figure 8 - Default logs location on Windows.

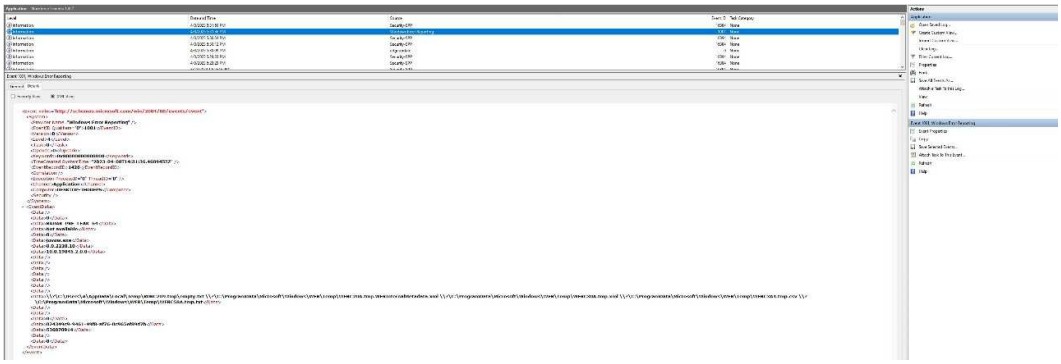


Figure 9 - Event Viewer example.

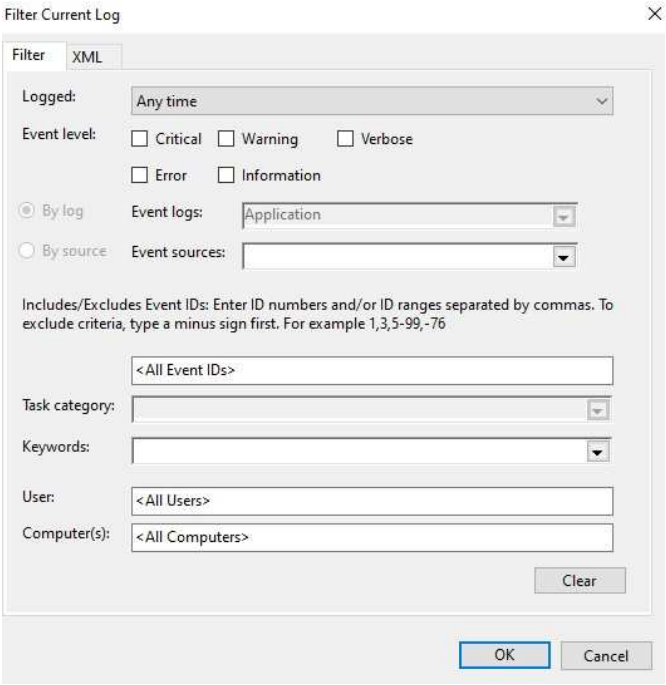


Figure 10 - Event Viewer filter example.

Windows logs play a crucial role in system management and troubleshooting. The Application Log records events related to applications, offering insights into errors, warnings, and software installations. The System Log provides information on system events, including hardware issues, driver problems, and critical errors. For security-related insights, the Security Log is vital, capturing details on logins, account changes, and audit events. The Setup Log focuses on events related to the setup of the Windows operating system. Meanwhile, the DNS Server Log aids in diagnosing and resolving DNS-related issues. The Task Scheduler Log keeps track of scheduled task events, while the Windows PowerShell Log records events related to PowerShell script execution. The category of Application and Service Logs encompasses logs specific to various applications and services, offering detailed information about their performance and issues. Lastly, the Hyper-V-VMMS Log is essential for virtualized environments, capturing events related to Hyper-V virtual machine management. These logs collectively empower administrators and analysts to monitor system health, troubleshoot problems, and enhance security. [67][68][69]

MacOS

MacOS maintains various logs that are valuable for troubleshooting and diagnosing issues on your system. Among these logs, the System.log (located at /var/log/system.log) contains general system messages and events. The Console application provides a graphical interface to view logs under different categories, such as system.log and diagnostic and usage information. The Unified Logging System (ULS), accessible through the log command in the Terminal, offers a centralized logging system for all logs on macOS, allowing filtering based on various criteria. Additionally, the Diagnostic Reports directory (located at /Library/Logs/DiagnosticReports/) contains crash reports and diagnostic information for applications, while the CrashReporter directory (located at /Library/Logs/CrashReporter/) holds details about application crashes. The Secure.log (located at /var/log/secure.log) records security-related messages, including authentication attempts, and the WiFi.log (located at /var/log/Wi-Fi.log) contains information about Wi-Fi connections and issues. For low-level system activity, the Kernel.log (located at /var/log/kernel.log) provides insights into the kernel, and the Installer.log (located at

/var/log/install.log) logs installation and removal of packages. The ASL (Apple System Logger) Database can be accessed using the log show command in the Terminal, allowing users to query and filter logs based on specific criteria. Finally, many applications maintain their own logs, often found in the ~/Library/Logs/ directory. When troubleshooting issues on your Mac, these logs collectively offer a comprehensive resource to identify the root causes of problems, with options ranging from the user-friendly Console application to more advanced command-line tools for log analysis.[70][71]

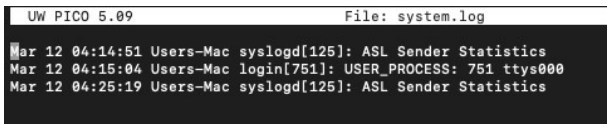


Figure 11 - MacOS system.log example.

Figure 12 - Default MacOS location using terminal.

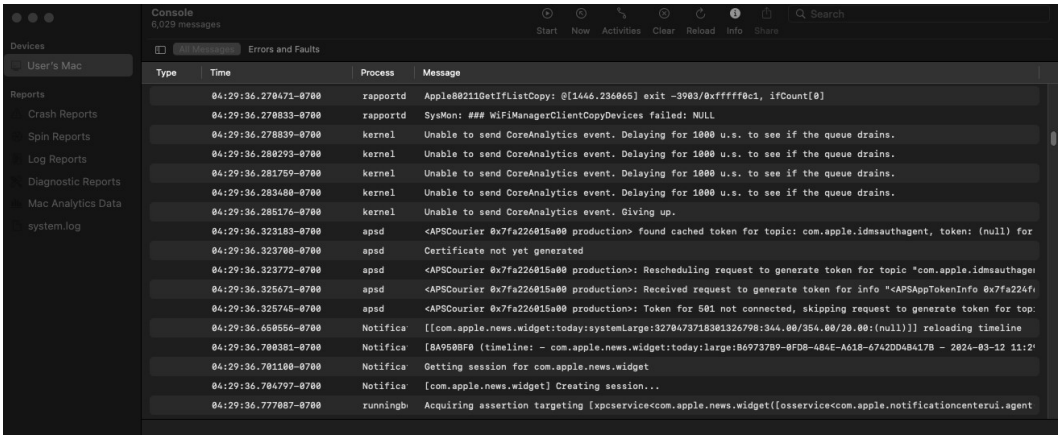


Figure 13 - MacOS event check using native Console application.

Linux

Linux logs are integral for system administration, troubleshooting, and security analysis. Key logs include Syslog (/var/log/syslog, /var/log/messages), crucial for general system troubleshooting by capturing messages from system processes and daemons. Kernel Logs (/var/log/kern.log) are essential for diagnosing hardware and kernel-related issues. Authentication Logs (/var/log/auth.log) and Secure Logs (/var/log/secure) provide vital information on authentication events, aiding in monitoring system access and security. Application-specific logs in directories like /var/log/apache2/, /var/log/nginx/, or /var/log/mysql/ are pivotal for diagnosing issues with web servers, databases, and applications. The Systemd Journal (journalctl) allows advanced filtering and querying of logs. Cron Logs (/var/log/cron.log, /var/log/cron) track scheduled task execution and related messages. Boot Logs (/var/log/boot.log) contain information about the system boot process. Network-related Logs (/var/log/daemon.log, /var/log/iptables.log) offer insights into network activities and firewall events. Package Management Logs (/var/log/dpkg.log, /var/log/yum.log) document package installation, removal, or upgrades. Xorg Logs (/var/log/Xorg.0.log) are crucial for troubleshooting graphics and display issues. Additionally, Security Logs (/var/log/security) may contain security-related information depending on the distribution. Analyzing logs requires a focus on system-specific requirements, with an emphasis on security, authentication, and system logs to maintain overall system health and security.[72][73]

```
user@user:~$ cd /var/log
user@user:/var/log$ ls
alternatives.log  dist-upgrade     hp          speech-dispatcher
apt               dmesg            installer   syslog
auth.log          dpkg.log         journal     ubuntu-advantage.log
boot.log          faillog          kern.log    unattended-upgrades
bootstrap.log     fontconfig.log   lastlog     wtmp
btmp              gdm3             openvpn
cups              gpu-manager.log  private
```

Figure 14 - Linux default logs location.

```
user@user: /var/log
 GNU nano 6.2                          syslog
Dec 10 13:06:26 user systemd-modules-load[375]: Inserted module 'lp'
Dec 10 13:06:26 user systemd-modules-load[375]: Inserted module 'ppdev'
Dec 10 13:06:26 user systemd-modules-load[375]: Inserted module 'parport_pc'
Dec 10 13:06:26 user systemd-modules-load[375]: Inserted module 'msr'
Dec 10 13:06:26 user systemd-modules-load[375]: Inserted module 'ipmi_devintf'
Dec 10 13:06:26 user systemd[1]: Starting Flush Journal to Persistent Storage.
Dec 10 13:06:26 user systemd[1]: Started Rule-based Manager for Device Events
Dec 10 13:06:26 user systemd[1]: Finished Coldplug All udev Devices.
Dec 10 13:06:26 user systemd[1]: Starting Show Plymouth Boot Screen...
Dec 10 13:06:26 user systemd[1]: Received SIGRTMIN+20 from PID 413 (plymouthd).
Dec 10 13:06:26 user systemd[1]: Started Show Plymouth Boot Screen.
Dec 10 13:06:26 user systemd[1]: Condition check resulted in Dispatch Password
Dec 10 13:06:26 user systemd[1]: Started Forward Password Requests to Plymouth
Dec 10 13:06:26 user systemd[1]: Reached target Local Encrypted Volumes.
Dec 10 13:06:26 user systemd[1]: Finished Flush Journal to Persistent Storage.
Dec 10 13:06:26 user systemd-udevd[419]: Using default interface naming scheme
```

Figure 15 - Linux syslog.log example.

Android

Android logs play a crucial role in troubleshooting and analyzing the performance of Android devices. Among the most valuable logs are Logcat, a comprehensive system log capturing messages from applications and the Android system, accessible through commands like 'adb logcat' or Android Studio. Kernel logs, found in '/proc/kmsg' or via 'dmesg', provide low-level system information. The Event Log, obtained with 'adb shell dumpsys eventlog' or 'logcat', records system, and application events. Bugreport, generated by 'adb bugreport' or through device settings, offers a detailed report for issue diagnosis. Radio logs in '/data/misc/radio/' and dumpsys, accessed via 'adb shell dumpsys', provide mobile network and system service information. ANR logs in '/data/anr/' capture app unresponsiveness, while battery stats in '/sys/class/power_supply/battery/' or 'dumpsys batterystats' detail battery usage. App-specific logs may reside in '/data/data/Package Name/logs/', and security logs in '/data/misc/securitylog/' cover security events. Interpretation requires an understanding of Android architecture, and some logs may require specific permissions or root access. Always prioritize privacy and security considerations when handling logs.[74]

```
user@user:~$ sudo adb connect 192.168.244.138:5555
connected to 192.168.244.138:5555
user@user:~$ sudo adb devices
List of devices attached
192.168.244.138:5555    device
```

Figure 16 - Android adb connection.

```
user@user:~$ adb shell
x86_64:/ $ su
:/ # cd /data/misc
:/data/misc # ls
adb           carrierid  logd             recovery       update_engine
apns          dhcp       media            shared_relro   update_engine_log
audioserver   ethernet   net              sms            user
bluedroid     gatekeeper network_watchlist stats-data     vold
bluetooth     gcov       perfprofd        stats-service  vpn
bootstat      incidents  profiles         systemkeys     wifi
boottrace     keychain   profman          textclassifier wmtrace
cameraserver  keystore   radio            trace          zoneinfo
:/data/misc #
```

Figure 17 - Android default system logs locations.

iOS

iOS logs provide valuable information for troubleshooting and diagnosing issues on Apple devices. Among the most significant logs are the Console Logs, offering a broad overview of system messages, errors, and warnings, as well as the ASL (Apple System Logger) Logs, which contain detailed system information. Crash logs, such as the CrashReporter Logs, are essential for understanding and addressing app crashes. Diagnostic and Usage Messages offer insights into system events, crashes, and usage patterns. Networking logs, like Wireless Diagnostics Logs, are helpful for resolving network-related issues. Security and Privacy Logs provide information about security-related events, while CoreLocation Logs offer details on location services. Application-specific logs and sync logs, like Sync Services Logs, can be crucial for debugging issues specific to certain apps or synchronization problems. Accessing and interpreting logs often requires technical expertise and can be done using tools like Xcode or the macOS Console app. Users should exercise caution regarding sensitive information in logs and only use them for diagnostic purposes or as directed by Apple Support. Keep in mind that Apple's security features may restrict access to certain logs.[75][76]

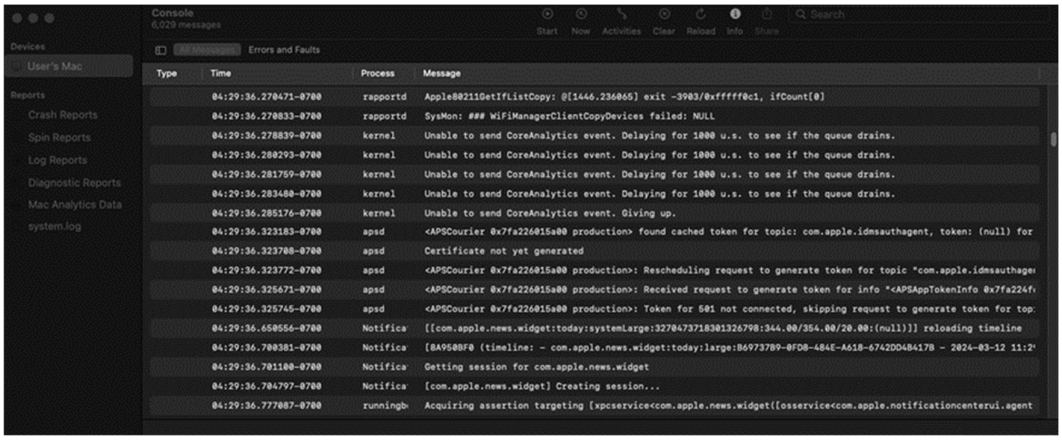


Figure 18 - iOS debugging logs on MacOS Console application.

3.3. IoCs

Indicators of Compromise (IoCs) are bits of information or patterns that are used to detect potentially malicious or suspicious activity in a computer system or network. IoCs play an important role in cybersecurity and threat detection since they assist security professionals and systems in identifying and responding to security incidents and breaches. Some examples of IoCs and their sources will be provided below.

- File hashes are cryptographic representations of files that are used to verify file integrity and detect known harmful files. MD5, SHA-1, and SHA-256 are examples of common hash types. IoCs relating to file hashes can be found in a variety of threat intelligence feeds.
- Suspicious or known malicious IP addresses associated with command-and-control servers or other malicious operations. Threat intelligence reports and feeds, as well as open-source threat feeds, contain IP IoCs.
- Suspicious or known harmful domain names that have been used in phishing, malware distribution, or other attacks. These IoCs are available in domain reputation databases, threat intelligence feeds, and domain blacklists.
- Malicious or suspicious URLs used in phishing campaigns or to distribute malware. IoCs connected to URLs are frequently provided by threat intelligence feeds and online security providers.
- Email addresses linked to phishing efforts, malicious actors, or spear-phishing activities. Email security solutions and threat intelligence reports contain IoCs tied to email addresses.
- Malware signatures or code patterns, such as YARA rules or Snort rules, that are used to detect malicious software or network traffic. These IoCs can be found in signature databases and threat intelligence sources.
- In a system, suspicious or malicious registry keys, artifacts, or configurations. These are available in a variety of threat intelligence reports and registry scanning programs.
- Anomalous or malevolent behavior patterns, such as anomalous network traffic, system operations, or user behavior, are examples of behavioral indicators. Security information and event management (SIEM) systems and network monitoring tools can detect these.
- Metadata from files that are File-related information, such as file creation dates, author information, or file type, can suggest suspicious activity. Various forensic techniques can be used to capture and evaluate metadata IoCs.
- A system's unusual or known harmful file names and paths. These can be gathered using file monitoring and analysis software.[77][78]

3.4. Use cases

3.4.1. Pegasus

iOS 10

The researchers for iOS 10 searched for the process “GoldenGate” of the service “com.apple.osanalytics.addaily.plist” or as a stored information in the database “DataUsage.sqlite” file. An extra evidence point would be the Pegasus process “pcsd”.

iOS 11

The researchers for iOS 11 searched for the service “com.apple.thumper” that it could communicate with malicious iCloud accounts retrieved from “IDStatusCache” file. Such iCloud accounts were used to transfer data between the interacting devices by using the Wi-Fi calling option that mobile providers offer. The Wi-Fi calling is also available to devices that share the same iCloud account as the mobile device.

iOS 12

The researchers for iOS 12 searched for the file “/private/var/root/Library/Preferences/roleaccountd.plist”. This file is available in an

iOS backup in the "RootDomain" and will appear after the first run of malicious code. Traces from "IDStatusCache" files shown that iMessage accounts used from Pegasus interacted with the target device before successful exploitation. This indicated that iMessage is a way to distribute the spyware. The "roleaccountd.plist" file was created and used by Pegasus on the initiative state against a target device. Also, the Apple Podcast app was launched after the first message content send from the malicious actor. Another method used by the malicious actors was opening the Apple Music app during the exploitation process. Significant evidence came from a jailbroken device which revealed a web request cache file tied to Apple Music. This cache file contained records of HTTP requests to a previously identified Pegasus infection domain. The URL contained an HTML exploit that was to be run as a subprocess of the Apple Music process.

iOS 13

The researchers for iOS 13 searched for the service "com.apple.mediastream.mstreamd" that it could communicate with malicious domain names and the service "com.apple.private.alloy.photostream idstatuscache" that could communicate with email addresses used by the malicious actors. The next exploiting attempts was performed to the photo sharing feature that iOS offers. Suspicious iCloud accounts in the "IDStatusCache" file used by the "com.apple.private.alloy.photostream" service. The photostream service is responsible for the shared camera content. A successful exploitation can trigger the
"bh" process. The exploit launched a WebKit instance in the "com.apple.mediastream.mstreamd" process. The WebKit instance then fetched JavaScript scaffolding from a known Pegasus infection domain. The scaffolding was fetched
"from /[uniqueid]/stadium/goblin" and from "/[uniqueid]/stadium/eutopia". The scaffolding includes a Pegasus infection domain name. The browser exploit was downloaded from a URL containing path "/[uniqueid]/stadium".

A new exploit method leaves traces in the file "IMTranscoderAgent.plist" which is visible in an iTunes backup. The new attack method utilized the iMessage app and especially the "IMTranscoderAgent" component that is used to create the previews for media in. The malicious actors this time found the way to force the "IMTranscoderAgent" component to automatically open a WebKit instance in the background and navigate to a Pegasus infection URL. Two attachment types were identified and the first seemed to work as the performing a stackoverflow and the second to be the one that contained the malicious code. After the successful exploitation of the predictable "IMTranscoderAgent" state traces of process "bh" were found.

iOS 14

The researchers for iOS 14 searched for "com.apple.coretelephony" cache files that could contain malicious domains. As in the above paragraph in the same way the component "IMTranscoderAgent" was the main target for the malicious actors. A different approach and the use of a custom Turing machine architecture implemented using JBIG2 segment commands. Multiple JBIG2 segment commands are chained in the
exploit to implement a sequence of logical bit operations on arbitrary memory. The logical bit operations are then abstracted to create a higher-level computer architecture to search memory and perform arithmetic operations. This computing environment is used to launch a sandbox escape and gain code execution outside the "IMTranscoderAgent" sandbox. The

sandbox escape uses only logic bugs, avoiding the need for further memory corruption bugs, and bypassing certain memory-corruption mitigations such as Pointer Authentication Codes (PAC) and Memory Tagging. After escaping the sandbox, the malicious code downloaded a payload from an infection server. Furthermore "Cache.db" is a precious database that can be found under the path "/private/var/wireless/Library/Caches/com.apple". An encrypted version of the malicious code found in the "fsCachedData" subfolder under the "com.apple.coretelephony" cache directory, to access the folder jailbreak is required. The code launched by the .gif files decrypts the malicious code via the "AES128DecryptWithPassword" method in "OpusFoundation.framework" using "coretelephony/Cache.db", which included the URL and headers of the HTTP GET request a key hard coded in the .gif files. The key appears to be randomized in each deployment of the exploit, meaning that decrypting the payload requires both a copy of the .gif files and the item from the "com.apple.coretelephony cache" directory. After the successful decryption the malicious code run and created a malicious process using the name "gatekeeperd". In the "/private/var/root/Library/Caches/ gatekeeperd/Cache.db" file contained a domain that probably checks for successful installation.

Android

The researchers searched for segfaults of Android video calling functionality. A copy of WhatsApp's "com.whatsapp_preferences.xml" file on the phone indicated that a video call ended two seconds after the first crash. A fragment of the call_log table from an old copy of msgstore.db stored on the phone was found and shown six incoming calls that could had triggered the crashes.[79][80][81]

3.4.2 Candiru

Candiru spyware hold persistence with the registry key HKEY_LOCAL_MACHINE\Software\Classes\CLSID\ {CF4CC405-E2C5-4DDD-B3CE-5E7582D8C9FA}\InprocServer32. The registry key is related to wmiutils.dll file, but after the modification the malware does to the registry key a malicious DLL file, associated with the Japanese input method (IMEJP) C:\WINDOWS\ system32\ime\IMEJP\IMJPUEXP.DLL, is pointed. When Windows boots, the pointed from registry DLL files will be used. In this case the DLL differs from the one that comes by default with the Windows Installation. Although the DLL is altered and is used to run malicious code after loading the resources also the default wmiutils.dll will be used in order to keep the Windows to run stable. The spyware has to load the AgentService.dat file from the folder C:\WINDOWS\system32\config\spp\Licenses\curv\config\tracing\ and the KBDMAORI.dat in the same directory. A series of four new DLL files will appear vcruntime140.dll, msvcp140.dll, ucrtbase.dll, concrt140.dll and the spyware configuration which are needed to perform the malicious actions. All the code that can be reversed is obfuscated. The main functionality can exfiltrate files, export messages from encrypted messaging app Signal, stealing cookies and passwords from browsers. [82]

3.5. Practical analysis

Table 4 - Subdomains of GR.COM Domain				
212.vrapjiys.gr.com	cpcalendars.libra.gr.com	goldentriangletourpackage.gr.com	linkresearchtools.gr.com	postmaster.freshfingers.gr.com
4games.gr.com	cpcalendars.platon.gr.com	gpf85.365bet.gr.com	live.city.gr.com	postmaster.moneyamulet.gr.com
adidas-shoes.gr.com	cpcalendars.rotary.gr.com	gps.gr.com	localbitcoins.gr.com	protothema.gr.com
airbnb.gr.com	cpcalendars.seo.gr.com	gr.com	login.gps.gr.com	psychic.gr.com
alawyer.gr.com	cpcalendars.site.gr.com	greenevo.gr.com	login.piraeusbamk.gr.com	quetempo.gr.com
alemao.gr.com	cpcalendars.vassilikibloukou.gr.com	growl.gr.com	login.pireaus.gr.com	rae.gr.com
alhpa.gr.com	cpcalendars.ydravlikos.gr.com	gus-mod.gr.com	login.winbamk.gr.com	rakbank.gr.com
alibaba.gr.com	cpcontacts.companyformationbulgaria.gr.com	gw2.atl.gr.com	maccosmetics.gr.com	raybansunglasses.gr.com
allianz.gr.com	cpcontacts.domain.gr.com	gw2.dal.gr.com	mail.alpha.gr.com	rentberry.gr.com
alpha.gr.com	cpcontacts.freshfingers.gr.com	gw2.den.gr.com	mail.bitmain.gr.com	rivercity.gr.com
anousakielenicooking.gr.com	cpcontacts.geoplan.gr.com	gw2.min.gr.com	mail.cbd-premium-quality-gold.gr.com	rizoste.gr.com
api.gr.com	cpcontacts.gps.gr.com	hairkats.gr.com	mail.cbd-premium-quality.gr.com	rotary.gr.com
apleton.gr.com	cpcontacts.hairkats.gr.com	happy-new-year.gr.com	mail.city.gr.com	ru.ibeauty.gr.com
apofraxeis.gr.com	cpcontacts.helensvilla.gr.com	heatmax.gr.com	mail.companyformationbulgaria.gr.com	sam.gr.com
applyport.gr.com	cpcontacts.hiking.gr.com	helensvilla.gr.com	mail.dofus.gr.com	sansimera.gr.com
apps.sepenet.gr.com	cpcontacts.innocent.gr.com	hellenichomesitters.gr.com	mail.domain.gr.com	scoop.gr.com
astynomia.gr.com	cpcontacts.patrikios.gr.com	hifimagasinet.gr.com	mail.e-peiraias.gr.com	seo.gr.com.seo.gr.com
atl.gr.com	cpcontacts.rotary.gr.com	hiking.gr.com	mail.eshops.gr.com	sepenet.gr.com
autodiscover.companyformationbulgaria.gr.com	cpcontacts.seo.gr.com	hogan.gr.com	mail.gameflip.gr.com	server2019.gr.com
autodiscover.geoplan.gr.com	cpcontacts.site.gr.com	hostmaster.123movies.gr.com	mail.geoplan.gr.com	services.gr.com
autodiscover.hellenichomesitters.gr.com	cpcontacts.skechersgreece.gr.com	hostmaster.bmamodels.gr.com	mail.helensvilla.gr.com	shadowplay.gr.com
autodiscover.hiking.gr.com	cpcontacts.vassilikibloukou.gr.com	hostmaster.cbd-premium-quality-gold.gr.com	mail.hobbyness.gr.com	shaolin.gr.com
autodiscover.hobbyness.gr.com	cpcontacts.villakatia.gr.com	hostmaster.cloud.gr.com	mail.honey.gr.com	sirina.gr.com
autodiscover.patrikios.gr.com	cpcontacts.ydravlikos.gr.com	hostmaster.cpcalendars.seo.gr.com	mail.insta.gr.com	site.gr.com

autodiscover.platon.gr.com	craqc.365bet.gr.com	hostmaster.cpcalendars.site.gr.com	mail.libra.gr.com	skai.gr.com
autodiscover.pokerstars.gr.com	create-my-own-website.gr.com	hostmaster.cpcontacts.seo.gr.com	mail.localbitcoins.gr.com	skinbaron.gr.com
autodiscover.stonelite.gr.com	create-web-page.gr.com	hostmaster.cpcontacts.site.gr.com	mail.luminusjewels.gr.com	skinbid.gr.com
autodiscover.transaction.gr.com	crete.tournet.gr.com	hostmaster.dc-990f597ec7f3.seo.gr.com	mail.mediator.gr.com	skinscash.gr.com
autodiscover.vassilikibloukou.gr.com	cretion.gr.com	hostmaster.espressonews.gr.com	mail.misslavore.gr.com	slots.gr.com
autodiscover.video.gr.com	daniel.gr.com	hostmaster.estia.gr.com	mail.namaste.gr.com	smtp.seo.gr.com
bad.gr.com	david-avramidis.gr.com	hostmaster.fimes.gr.com	mail.orange.gr.com	smtp.site.gr.com
batterydepot.gr.com	dc-990f597ec7f3.seo.gr.com	hostmaster.ftp.seo.gr.com	mail.peggysvilla.gr.com	solusdesign.gr.com
belanjaalkes.gr.com	decoline.gr.com	hostmaster.ftp.site.gr.com	mail.scoop.gr.com	sourceforge.gr.com
beyou.gr.com	den.gr.com	hostmaster.imap.site.gr.com	mail.site.gr.com	spam1.gr.com
bi.tiny.gr.com	denbench.gr.com	hostmaster.inews.gr.com	mail.skechersgreece.gr.com	sparkasse.gr.com
bit.gr.com	dofus.gr.com	hostmaster.interlight.gr.com	mail.sparkasse.gr.com	sportit.gr.com
bittrex.gr.com	drawwebsite.gr.com	hostmaster.kranos.gr.com	mail.stark.gr.com	sportsneakers.gr.com
bmamodels.gr.com	dream-design.gr.com	hostmaster.login.alpha.gr.com	mail.stoiximan.gr.com	squeeze.gr.com
bmw.gr.com	dream.gr.com	hostmaster.mail.alpha.gr.com	mail.stonelite.gr.com	sr4wd.365bet.gr.com
bni.gr.com	e-amanda.gr.com	hostmaster.mail.site.gr.com	mail.transaction.gr.com	srv.gr.com
btc.gr.com	e7tgi.365bet.gr.com	hostmaster.mail.unisea.gr.com	mail.video.gr.com	ssilka.hydra.gr.com
btcturk.gr.com	eastmed.gr.com	hostmaster.my.alpha.gr.com	mail.villakatia.gr.com	sso.btcturk.gr.com
carent.gr.com	ecommerce.gr.com	hostmaster.newsbeast.gr.com	mail.winbankprivat.gr.com	st.gr.com
cbd-premium-quality-gold.gr.com	el.ibeauty.gr.com	hostmaster.nexus-international.gr.com	mail.xn--jxacfhdgduh6b1aul0ambko.gr.com	staging.fiorito.gr.com
celicaclub.gr.com	emeis.gr.com	hostmaster.nissan.gr.com	manavrecharge.gr.com	stoneflre.gr.com
chase.gr.com	emon.gr.com	hostmaster.per.gr.com	marsbet.gr.com	stonelite.gr.com
cheapuggboots.gr.com	en.ibeauty.gr.com	hostmaster.seo.gr.com	mediator.gr.com	storage.gr.com
china3m.gr.com	epipla.gr.com	hostmaster.seo.gr.com.seo.gr.com	memo.gr.com	store.ferrari.gr.com
chinammm.gr.com	escortbabes.gr.com	hostmaster.sepenet.gr.com	microsoftonline.gr.com	strongblock.gr.com
city.gr.com	escortgirls.gr.com	hostmaster.site.gr.com	min.gr.com	ta-nea.dolnet.gr.com
cloud.gr.com	escortsathens.gr.com	hostmaster.skechersgreece.gr.com	misslavore.gr.com	tagliatelleitalyana.gr.com
cloudcloud.gr.com	eshops.gr.com	hostmaster.smtp.seo.gr.com	moncler.gr.com	tanda.gr.com
co-devs.gr.com	espressonews.gr.com	hostmaster.smtp.site.gr.com	mta-1.marcin.gr.com	tax-art.gr.com

cpanel.companyformationbulgaria.gr.com	estia.gr.com	hostmaster.store.ferrari.gr.com	mta-1.testdomainformarus0508.gr.com	tele.gr.com
cpanel.culinaryco.gr.com	eth.gr.com	hostmaster.uniseа.gr.com	mta-sts.stonelite.gr.com	test.gr.com
cpanel.eshops.gr.com	euroibanking.gr.com	hostmaster.viva.gr.com	my.alpha.gr.com	uggboots.gr.com
cpanel.freshfingers.gr.com	europa.gr.com	hostmaster.webdisk.seo.gr.com	na.gr.com	uggoutlet.gr.com
cpanel.geoplan.gr.com	exoplismoi.gr.com	hostmaster.webdisk.site.gr.com	namaste.gr.com	uggsoutlet.gr.com
cpanel.gps.gr.com	ferrari.gr.com	hostmaster.webmail.seo.gr.com	neti.gr.com	www.3wisemonkeys.gr.com
cpanel.hairkats.gr.com	fimes.gr.com	hostmaster.webmail.site.gr.com	newslive.gr.com	www.burberryoutlet.gr.com
cpanel.helensvilla.gr.com	firewind.gr.com	hostmaster.winbanknprivat.gr.com	nexus-international.gr.com	www.cheapuggboots.gr.com
cpanel.hellenichomesitters.gr.com	flash.gr.com	hostmaster.www.alpha.gr.com	nissan.gr.com	www.drawwebsite.gr.com
cpanel.hobbyness.gr.com	football.gr.com	hostmaster.www.katalogos.gr.com	oakleysunglasses.gr.com	www.jit.gr.com
cpanel.honey.gr.com	forex.gr.com	hostmaster.www.seo.gr.com	odchudzaniejestproste.gr.com	www.maccosmetics.gr.com
cpanel.innocent.gr.com	fotoart.gr.com	hostmaster.www.sepenet.gr.com	okx.gr.com	www.massageprincess.gr.com
cpanel.institutfrancais.gr.com	fr.ibeauty.gr.com	hostmaster.www.unisea.gr.com	oliveoil.gr.com	www.metafores-metakomiseis.gr.com
cpanel.libra.gr.com	freepen.gr.com	hostmaster.xlamma.gr.com	omaze.gr.com	www.oakleysunglasses.gr.com
cpanel.moneyamulet.gr.com	freshfingers.gr.com	hotelsmeteora.gr.com	onlineservices.gr.com	www.outletuggs.gr.com
cpanel.newslive.gr.com	fromparistoparos.gr.com	house.gr.com	opap.gr.com	www.pdf-manual.gr.com
cpanel.orange.gr.com	ftp.seo.gr.com	icloud.gr.com	opskins.gr.com	www.pisines.gr.com
cpanel.patrikios.gr.com	ftp.site.gr.com	igro-gh.gr.com	orange.gr.com	www.psychic.gr.com
cpanel.peggysvilla.gr.com	g-a.gr.com	image.123movies.gr.com	papaki.gr.com	www.raybansunglasses.gr.com
cpanel.platon.gr.com	gabrielmenezes.gr.com	imap.seo.gr.com	patrikios.gr.com	www.spiti.gr.com
cpanel.pokerstars.gr.com	gameflip.gr.com	independentnews.gr.com	peggysvilla.gr.com	www.tvopen.gr.com
cpanel.rakbank.gr.com	gateway.gr.com	inews.gr.com	petness.gr.com	www.uggboots.gr.com
cpanel.skechersgreece.gr.com	gaylife.gr.com	insta.gr.com	phen375.gr.com	www.uggoutlet.gr.com
cpanel.stark.gr.com	gemmaco.gr.com	interchain.gr.com	phpmyadmin.memo.gr.com	www.uggsoutlet.gr.com
cpanel.transaction.gr.com	geoplan.gr.com	interlight.gr.com	piraeusbamk.gr.com	www.unfollow.gr.com
cpcalendars.companyformationbulgaria.gr.com	gidra-zerkalo.onion.gr.com	jit.gr.com	platon.gr.com	www.wehitch.gr.com
cpcalendars.domain.gr.com	givejoy.gr.com	kathimerini.gr.com	poker-online.gr.com	
cpcalendars.geoplan.gr.com	gleninnestourism.gr.com	kiriakopoulos.gr.com	poker.gr.com	
cpcalendars.hairkats.gr.com	goldcoastescorts.gr.com	libra.gr.com	pokerstars.gr.com	
cpcalendars.helensvilla.gr.com	goldenbeach.gr.com	linkedin.gr.com	polkastarter.gr.com	

Table 5 - IP Addresses related to found Predator domains				
1.118.120.77	18.213.250.117	198.144.157.126	46.40.200.204	64.95.64.219
103.224.182.208	18.215.128.143	198.54.114.171	47.245.8.67	64.95.64.223
103.224.182.242	184.168.131.241	198.54.116.178	47.74.9.12	64.98.145.30
103.224.182.246	184.168.221.1	198.54.117.197	47.91.170.222	66.150.161.140
103.224.182.248	184.168.221.10	198.54.117.198	5.182.206.6	66.150.161.141
103.224.182.251	184.168.221.11	198.54.117.199	5.183.95.151	67.222.7.35
103.224.212.213	184.168.221.12	198.54.117.200	5.183.95.152	67.222.7.35
103.224.212.215	184.168.221.15	198.54.117.210	5.2.81.16	68.178.232.100
103.224.212.217	184.168.221.16	198.54.117.212	5.2.81.166	68.178.232.143
103.224.212.220	184.168.221.2	198.54.117.212	5.230.67.206	68.178.232.143
103.224.212.222	184.168.221.20	198.58.118.167	5.230.68.136	68.65.121.150
104.18.42.205	184.168.221.22	199.115.116.43	5.230.78.27	69.163.185.150
104.18.44.171	184.168.221.23	199.184.144.27	5.255.103.157	69.172.201.153
104.18.45.171	184.168.221.24	199.184.144.27	5.255.103.162	69.172.201.218
104.18.62.243	184.168.221.26	199.188.201.129	5.255.103.165	69.25.27.170
104.18.63.243	184.168.221.27	199.27.134.71	5.255.97.82	69.25.27.173
104.21.21.72	184.168.221.28	199.59.243.120	5.255.97.85	69.43.161.178
104.21.49.58	184.168.221.3	199.59.243.120	50.63.202.10	69.64.147.10
104.21.52.99	184.168.221.31	199.59.243.222	50.63.202.11	69.64.147.242
104.21.52.99	184.168.221.32	199.59.243.223	50.63.202.12	69.64.147.37
104.217.8.102	184.168.221.35	199.59.243.224	50.63.202.13	70.32.1.32
104.238.177.225	184.168.221.36	199.59.243.225	50.63.202.14	70.32.1.32
104.24.122.56	184.168.221.38	2.58.14.241	50.63.202.15	72.14.178.174
104.24.123.56	184.168.221.39	2.58.15.120	50.63.202.16	72.14.178.174
104.24.126.190	184.168.221.4	203.170.87.12	50.63.202.17	72.14.185.43
104.24.98.248	184.168.221.40	204.13.160.107	50.63.202.18	72.34.38.64
104.24.99.248	184.168.221.43	204.13.162.116	50.63.202.2	72.52.179.174
104.27.150.203	184.168.221.44	205.251.130.241	50.63.202.20	72.52.4.119
104.27.151.203	184.168.221.48	207.180.226.111	50.63.202.21	72.52.4.89
104.27.164.76	184.168.221.49	208.43.167.119	50.63.202.22	72.52.4.90
104.27.165.76	184.168.221.50	208.73.211.177	50.63.202.24	72.52.4.91
104.27.180.58	184.168.221.51	208.73.211.208	50.63.202.27	74.36.25.44
104.27.181.58	184.168.221.52	208.73.211.230	50.63.202.28	75.126.101.235
104.27.186.245	184.168.221.53	208.73.211.244	50.63.202.33	75.126.101.239
104.27.187.245	184.168.221.53	208.73.211.249	50.63.202.34	75.126.101.244
104.28.237.168	184.168.221.54	208.87.32.69	50.63.202.34	75.126.102.231
104.31.94.121	184.168.221.55	208.87.32.75	50.63.202.35	75.126.102.232
104.31.95.121	184.168.221.58	208.87.35.100	50.63.202.36	75.126.102.237
107.161.23.204	184.168.221.58	208.87.35.101	50.63.202.37	75.126.104.228
107.161.23.204	184.168.221.59	208.87.35.103	50.63.202.38	75.126.104.228
107.20.81.21	184.168.221.59	208.87.35.104	50.63.202.39	76.223.54.146
108.161.136.111	184.168.221.6	208.87.35.105	50.63.202.40	78.47.98.51

108.162.192.130	184.168.221.60	208.87.35.106	50.63.202.41	79.130.116.113
108.162.192.176	184.168.221.61	208.91.197.64	50.63.202.42	79.130.116.117
108.162.192.40	184.168.221.63	208.91.197.87	50.63.202.43	79.137.112.21
108.162.192.85	184.168.221.65	208.91.197.91	50.63.202.44	79.98.24.223
108.162.194.118	184.168.221.69	209.141.38.71	50.63.202.45	8.5.1.34
108.162.194.163	184.168.221.75	209.141.38.71	50.63.202.47	8.5.1.41
108.162.194.229	184.168.221.76	209.250.235.211	50.63.202.47	8.5.1.51
108.162.198.57	184.168.221.77	209.99.40.222	50.63.202.48	8.5.1.58
108.179.213.68	184.168.221.8	209.99.40.224	50.63.202.49	80.208.224.105
108.59.12.100	184.168.221.82	213.186.33.87	50.63.202.5	80.208.227.132
108.61.103.152	184.168.221.84	216.139.213.144	50.63.202.50	80.208.230.56
109.68.33.64	184.168.221.86	217.160.0.22	50.63.202.52	80.208.231.23
109.70.26.37	184.168.221.87	23.227.38.32	50.63.202.53	80.209.226.15
112.140.180.23	184.168.221.9	23.229.216.0	50.63.202.53	80.209.229.94
112.213.97.31	184.168.221.96	23.234.27.209	50.63.202.55	80.240.16.147
13.248.169.48	184.168.221.96	23.253.58.227	50.63.202.55	81.171.22.4
13.248.213.45	185.134.114.118	3.124.194.15	50.63.202.56	81.171.22.7
135.181.39.23	185.134.114.119	3.124.194.15	50.63.202.57	81.177.6.142
142.4.18.44	185.134.114.70	3.126.58.91	50.63.202.59	82.102.16.39
146.70.20.224	185.134.114.75	3.130.253.23	50.63.202.59	82.196.9.113
15.197.148.33	185.150.117.30	3.141.96.53	50.63.202.6	82.98.86.161
15.197.192.55	185.176.43.62	3.20.137.44	50.63.202.61	82.98.86.168
15.235.110.39	185.199.108.153	3.248.195.240	50.63.202.62	82.98.86.172
15.236.204.129	185.199.109.153	3.33.130.190	50.63.202.62	82.98.86.173
154.12.253.85	185.199.109.153	3.64.163.50	50.63.202.63	82.98.86.174
154.12.253.85	185.199.110.153	3.64.163.50	50.63.202.67	82.98.86.176
157.230.40.185	185.199.110.153	34.160.209.102	50.63.202.7	82.98.86.176
159.8.40.54	185.199.111.153	34.160.73.230	50.63.202.70	83.125.22.211
161.35.169.213	185.234.72.147	34.201.37.74	50.63.202.71	85.13.161.235
162.213.255.27	185.234.72.26	34.242.71.176	50.63.202.75	85.17.164.183
162.242.150.89	185.243.112.247	34.244.102.249	50.63.202.76	87.236.19.102
162.254.39.7	185.243.115.97	34.244.239.200	50.63.202.78	88.119.161.127
162.254.39.7	185.26.239.241	34.255.136.127	50.63.202.8	88.80.148.133
162.255.118.194	185.28.21.86	34.98.99.30	50.63.202.81	88.85.110.34
162.255.119.106	185.53.178.9	35.156.92.159	50.63.202.83	88.85.110.38
162.255.119.107	185.53.179.24	35.169.58.188	50.63.202.9	89.252.182.3
162.255.119.12	185.53.179.6	35.186.238.101	50.63.202.91	89.35.39.50
162.255.119.122	185.61.154.56	35.209.183.198	50.63.202.93	91.195.240.117
162.255.119.153	188.120.225.21	37.140.192.178	50.87.249.35	91.195.240.12
162.255.119.155	188.120.225.21	43.251.105.120	51.195.73.143	91.195.240.126
162.255.119.199	192.161.187.200	44.227.65.245	51.195.80.31	91.195.240.87
162.255.119.206	192.161.187.200	44.227.76.166	51.210.132.37	91.195.240.94
162.255.119.214	192.169.7.252	44.230.85.241	52.213.114.86	91.200.102.174
162.255.119.248	192.169.7.252	44.230.85.241	52.213.213.245	91.200.102.182
162.255.119.249	192.187.111.221	45.155.173.184	52.33.207.7	91.206.200.14
162.255.119.52	192.241.129.7	45.33.18.44	52.4.209.250	91.206.200.150

163.172.84.107	192.30.252.153	45.33.2.79	52.58.78.16	91.206.200.201
165.22.80.21	192.30.252.154	45.33.20.235	52.87.165.213	91.206.200.43
166.62.121.235	192.34.57.172	45.33.23.183	54.153.56.183	91.206.200.92
166.62.27.56	192.34.63.175	45.33.30.197	54.154.120.159	91.219.236.148
167.114.94.188	192.64.112.173	45.56.79.23	54.161.222.85	91.219.236.235
167.235.242.21	192.64.119.10	45.56.79.23	54.205.101.85	91.219.237.39
167.86.66.125	192.64.119.117	45.79.19.196	54.208.77.124	91.219.238.181
170.178.168.203	192.64.119.151	45.79.19.196	54.72.130.67	91.222.137.170
170.64.161.135	192.64.119.16	45.86.162.120	59.188.232.88	91.222.137.84
172.67.139.90	192.64.119.191	45.86.162.121	62.162.5.58	91.231.86.19
172.67.152.118	192.64.119.192	45.86.162.160	62.77.155.55	93.86.50.218
172.67.156.46	192.64.119.207	45.86.162.23	62.77.159.107	93.86.50.218
172.67.159.55	192.64.119.21	45.86.162.37	63.141.254.146	94.176.31.34
172.67.175.142	192.64.119.223	45.86.162.7	63.250.32.4	94.176.31.34
172.67.197.2	192.64.119.229	45.86.163.125	63.251.171.80	95.216.144.25
172.67.198.15	192.64.119.36	45.86.163.128	63.251.171.81	96.126.123.244
173.245.60.113	192.64.119.67	45.86.163.143	64.202.189.170	98.124.243.32
173.245.60.194	193.183.99.135	45.89.127.252	64.29.151.218	99.81.40.78
173.255.194.134	193.29.56.63	45.95.168.70	64.70.19.203	99.83.154.118
176.223.137.173	193.70.79.57	46.137.81.221	64.70.19.34	99.83.154.118
176.34.241.253	194.58.56.134	46.30.188.164	64.74.223.32	
176.53.74.102	194.85.61.76	46.30.188.250	64.95.64.195	
178.157.82.65	195.43.82.170	46.30.188.56	64.95.64.197	
18.212.64.196	196.218.19.59	46.30.189.107	64.95.64.218	

Table 6 - Domains related to Predator activity

2y4nothing.xyz	cut.red	kathimerini.news	paok-24.com	tinyurl.cloud
5m5.io	cyber.country	kinder.engine.ninja	pastepast.net	tiol.xyz
actumali.org	danas.bid	koenigseggg.com	pdfviewer.app	tly.gr.com
addons.news	distedc.com	kohaicorp.com	plantastictab.com	tly.link
adibjan.net	download4you.xyz	koora-egypt.com	playestore.net	tovima.live
adservices.gr.com	dragonair.xyz	kormoran.bid	pocopoc.xyz	trecv.xyz
adultpcz.xyz	eagerfox.xyz	kranos.gr.com	politika.bid	trecvf.xyz
advertsservices.com	ebill.cosmote.center	lamborghini-s.shop	politique-koaci.info	tribune-mg.xyz
advfb.xyz	edolio5.com	landingpg.xyz	prmopromo.com	trkc.online
affise.app	efsyn.online	landingpge.xyz	pronews.gr.com	tsapp.me
almasryelyuom.com	eg-gov.org	leanwithme.xyz	protothema.live	tsrt.xyz
alpineai.uk	egyqaz.com	lexpress.me	proupload.xyz	tw.itter.me
alraeeenews.com	elpais.me	lexpress-mg.xyz	ps1link.xyz	twtter.net
alraeesnews.net	engine.ninja	lifestyleshops.net	ps2link.xyz	ube.gr.com
altsantiri.news	enigmase.xyz	limk.one	quickupdates.xyz	uberegypt.cn.com

amazing.lab	enikos.news	linkit.cloud	qwert.xyz	updates4you.xyz
ancienthistory.xyz	ereportaz.news	linkit.digital	qwxzyl.com	updateservice.center
android-apps.tech	espressonews.gr.com	link-m.xyz	redeitt.com	updatetime.zone
api-apple-buy.com	etisalategypt.tech	link-protection.com	redirecting.live	updatingnews.xyz
api-telecommunication.com	etisalatgreen.com	linktothisa.xyz	redirecting.page	updete.xyz
applepps.com	ewish.cards	liponals.store	safelyredirecting.com	url-promo.club
apps-ios.net	fastdownload.me	livingwithbadkidny.xyz	safelyredirecting.digital	url-tiny.app
aramexegypt.com	fastuploads.xyz	llinkedin.net	sepenet.gr.com	uservicescheck.com
arrefourmisr.com	fbc8213450838f7ae251d4519c195138.xyz	lnkedin.org	sephoragroup.com	uservicesforyou.com
atheere.com	ferrari.gr.com	localegem.net	servers-mobile.info	utube.digital
audit-pvv.com	ffoxnewz.com	lylink.online	serviceupdaterequest.com	utube.to
bank-alahly.com	fimes.gr.com	makeitshort.xyz	sextape225.me	viva.gr.com
bbcsworld.com	fireup.xyz	md-news-direct.com	shortely.xyz	vodafoneegypt.tech
bi.tly.gr.com	fisherman.engine.ninja	mifcbook.link	shorten.fi	vodafonegypt.com
bi.tly.link	flexipagez.com	miniiosapps.xyz	shortenurls.me	wavekli.xyz
bit-li.com	forwardeshoptt.com	mitube1.link	shortmee.one	weathear.live
bit-li.ws	getsignalapps.com	mlinks.ws	shortwidgets.com	weathernewz.xyz
bitlinkin.xyz	getsignalapps.live	mobnetlink1.com	shortxyz.com	weathersite.online
bitlly.live	getupdatesnow.xyz	mobnetlink2.com	simetricode.uk	webaffise.com
bit-ly.link	goldenscent.net	mobnetlink3.com	sinai-new.com	we-site.net
bit-ly.org	goldenscint.com	mozillaupdate.xyz	sitepref.xyz	wha.tsapp.me
bitlyrs.com	goldescent.com	msas.ws	smsuns.com	worldnws.xyz
bitt.fi	gosokm.com	museumviewstab.com	snapfire.xyz	wtc1111.com
bity.ws	guardian-tt.me	mycoffeeshop.shop	sniper.pet	wtc2222.com
bityl.me	guardnew.live	myfcbk.net	solargoup.xyz	wtc3333.com
blacktrail.xyz	guardnews.live	mytrips.quest	solargroup.xyz	xf.actor
bmw.gr.com	heaven.army	myutbe.net	speedy.sbs	xnxx-hub.com
bookjob.club	heiiasjournai.com	mywebsitevpstest.xyz	speedygonzales.xyz	xyvok.xyz
browsercheck.services	hellasjournal.company	nabd.site	speedymax.shop	yallakora-egy.com
bumabara.bid	hellasjournal.website	nabde.app	sports-mdg.xyz	yo.utube.digital
burgerprince.us	hellottec.art	nassosblog.gr.com	sportsnewz.site	yo.utube.to
businesnews.net	hempower.shop	nemshi.net	static-graph.com	youarefired.xyz
canyouc.xyz	hopnope.xyz	nemshi-news.live	stonisi.news	yout.ube.gr.com
carrefourmisr.com	icloudeu.com	nemshi-news.xyz	supportset.net	youtub.app

cbbc01.xyz	icloudflair.com	networkenterprise.net	suzuki.gr.com	youtube.gr.live
celebrnewz.xyz	iibt.xyz	newsbeast.gr.com	svetovid.bid	youtu-be.net
cellconn.net	ikea-egypt.net	newslive2.xyz	symoty.com	youtube.voto
charmander.xyz	ilnk.xyz	newzeto.xyz	syncservices.one	youtubesyncapi.com
chatwithme.store	infosms-a.site	newzgroup.xyz	synctimestamp.com	youtubewatch.co
citroen.gr.com	in-politics.com	niceonase.com	syncupdate.site	yuom7.net
ckforward.one	inservices.digital	niceonesa.net	telecomegy-ads.com	z2a.digital
clockupdate.com	insider.gr.com	nikjol.xyz	telenorconn.com	z2adigital.cloud
cloudstatistics.net	instagam.click	nissan.gr.com	teslal.shop	z2digital.cloud
cloudtimesync.com	instagam.in	novosti.bid	teslal.xyz	zougla.gr.com
cnn.gr.com	instagam.photos	oilgy.xyz	teslali.com	zougla.news
conlnk.one	instegram.co	olexegy.com	tesla-s.shop	
connectivitycheck.live	invoker.icu	olxeg.com	tgrthgsrgwrthwrtgwr.xyz	
connectivitycheck.online	ios-apps.store	omanreal.net	timestampsync.com	
connectivitychecker.com	iosmnbg.com	omeega.xyz	timeupdate.xyz	
contents-domain.com	itcgr.live	onlineservices.gr.com	timeupdateservice.com	
cosmote.center	itly.link	orangegypt.co	tiny.gr.com	
covid19masks.shop	itter.me	orchomenos.news	tinylinks.live	
crashonline.site	jquery-updater.xyz	otaupdatesios.com	tinyulrs.com	

Table 7 - Hashes related to Predator activity
8e4edb1e07ebb86784f65dccb14ab71dfd72f2be1203765b85461e65b7ed69c6
007b94fe3cf36aa1a3e01461fa261767

Table 8 - URLs related to Predator activity
ht[t]p://163.123.143.126/bins/dark.86_64
ht[t]p://163.123.143.126/bins/dark.arm4
ht[t]p://163.123.143.126/bins/dark.arm5
ht[t]p://163.123.143.126/bins/dark.arm6
ht[t]p://163.123.143.126/bins/dark.arm7
ht[t]p://163.123.143.126/bins/dark.m68k
ht[t]p://163.123.143.126/bins/dark.mips
ht[t]p://163.123.143.126/bins/dark.mpsl
ht[t]p://163.123.143.126/bins/dark.ppc
ht[t]p://163.123.143.126/bins/dark.sh4
ht[t]p://163.123.143.126/bins/dark.x86
ht[t]p://2.56.59.215/i.sh
ht[t]p://212.192.241.72/lolol.sh

ht[t]p://31.210.20.100/lolol.sh
ht[t]p://museumviewstab.com/
ht[t]p://plantastictab.com/
ht[t]ps://api.telegram.org/bot5943289606:AAGNEW2B3zDRhGDxY7E1tg7_m2BJcVkUJDw/sendDocument
ht[t]ps://museumviewstab.com/
ht[t]ps://pastebin.com/raw/3fS0MSjN
ht[t]ps://plantastictab.com/
ht[t]ps://redirecting.page/9cdfb439c7876e703e307864c9167a15/vsk/afile

Table 9 - IP Addresses related to found Candiru domains

103.199.17.221	184.168.221.86	198.54.117.197	34.98.99.30	74.117.222.24
103.224.212.222	184.168.221.87	198.54.117.198	35.205.61.67	74.220.199.15
104.155.138.21	184.168.221.93	198.54.117.199	35.224.204.202	74.55.102.21
104.21.2.172	185.107.56.207	198.54.117.200	44.227.65.245	8.5.1.34
104.216.8.60	185.107.56.208	199.115.116.162	44.227.76.166	80.251.18.108
107.178.223.183	185.107.56.209	199.59.243.222	45.61.137.20	80.251.18.8
109.68.33.64	185.107.56.210	20.50.64.14	47.89.58.141	82.194.76.11
109.70.236.107	185.125.206.182	202.65.152.177	47.89.58.32	83.171.236.133
112.78.119.85	185.181.8.155	204.152.214.28	50.116.74.155	83.171.237.211
124.6.37.131	185.230.60.173	204.152.214.29	50.17.5.224	83.171.237.29
15.197.142.173	185.230.61.173	204.152.214.30	50.63.202.37	83.97.20.89
152.89.247.252	185.230.63.107	208.64.124.162	50.63.202.63	84.2.35.43
152.89.247.66	185.230.63.171	208.73.210.201	50.63.202.74	85.217.171.183
162.210.195.111	185.230.63.186	208.73.210.29	50.63.202.75	88.214.207.96
162.210.196.171	185.53.177.54	208.73.211.166	50.63.202.80	91.195.240.87
162.210.196.172	185.53.179.6	208.73.211.170	50.87.10.35	94.136.40.51
162.210.196.173	185.53.179.7	208.73.211.188	52.209.142.7	94.229.72.125
162.255.119.112	188.165.148.60	208.73.211.193	58.158.177.102	95.211.75.25
172.105.103.207	192.185.4.159	208.73.211.195	63.143.32.84	96.9.225.161
172.67.129.124	192.195.77.31	208.73.211.243	64.190.63.111	99.83.154.118
173.212.56.238	192.3.185.145	208.73.211.247	64.190.63.222	
173.212.56.239	192.52.166.55	208.73.211.249	64.74.223.39	
173.230.255.141	192.64.119.156	208.87.243.131	66.175.236.129	
174.137.132.45	192.64.119.157	209.200.154.51	68.178.232.100	
174.37.172.68	192.64.119.32	213.227.154.121	69.175.87.226	
184.154.21.218	192.64.147.171	217.70.184.38	69.43.160.144	
184.168.221.64	194.36.188.62	23.236.62.147	69.43.161.206	
184.168.221.69	195.140.215.243	3.33.152.147	69.58.188.49	
184.168.221.74	195.20.43.29	34.102.136.180	72.52.4.90	

Table 10- Domains related to Candiru activity				
adtracker.link	drpbx-update.net	konferenciya-zoom.com	pochtarossiy.info	winmslaf.xyz
amazon-cz.eu	dw-arabic.com	kupony-rohlik.cz	rasef22.com	womanstudies.co
amnestyreports.com	eulenformacion.com	lenovo-setup.tk	refugeeinternational.org	yeni-safak.com
apple-updates.online	euro-news.online	library-update.com	service-deamon.com	youtubee.life
armenpress.net	faceb00k-live.com	linkedin-jobs.com	tehrantimes.org	zcombinator.co
backxercise.com	fbcdnads.live	llink.link	total-slovenia-news.net	
bitly.tel	france-24.news	lwaeh-iteham-alasra.com	twitt-live.com	
blacklivesmatters.info	genderconference.org	mbsmetoo.com	un-asia.co	
cdnmobile.io	googlplay.store	minstagram.net	url-tiny.co	
cnn24-7.online	grayhornet.com	msstore.io	useproof.cc	
codeingasmylife.com	hilocake.info	noc-service-streamer.com	vesteldefnce.io	
colorpallatess.com	indoprogress.co	oiip.org	vfsglobal.fr	
cortanaupdates.com	instagrarn.co	online-affiliate-mon.com	weathercheck.digital	
cyprusnet.tk	johnshopkin.net	online-source-validate.com	whoint.co	
dl.nmcyclingexperience.com	kenoratravels.com	osesgy-unmissions.org	wikipediaathome.net	

Table 11 - CVE related to Candiru activity
CVE-2021-21166
CVE-2021-30551
CVE-2021-31979
CVE-2021-33742
CVE-2021-33771

Table 12 - Hashes related to Candiru activity
c299063e3eae8ddc15839767e83b9808fd43418dc5a1af7e4f44b97ba53fbd3d
9a964e810949704ff7b4a393d9adda60

Table 13 - IP Addresses related to found Pegasus domains				
103.114.75.1	176.223.111.231	185.94.189.198	3.12.87.58	63.141.242.43
103.138.151.26	176.31.83.118	185.94.189.204	3.140.13.188	63.141.242.44
103.199.16.11	176.32.100.193	185.94.189.207	3.141.96.53	63.141.242.45
103.199.16.111	176.32.100.196	185.94.189.208	3.18.7.81	63.141.242.46
103.199.16.12	176.32.100.202	185.94.189.214	3.19.116.195	63.143.32.90
103.199.16.15	176.32.100.244	185.94.189.219	3.33.130.190	63.143.32.94
103.199.16.153	176.32.101.132	185.94.190.203	3.33.152.147	64.190.63.222
103.199.16.47	176.32.101.68	185.94.191.114	3.64.163.50	64.202.189.170
103.199.16.88	176.32.101.76	185.94.191.120	3.94.41.167	64.74.223.37
103.199.17.206	176.32.102.68	185.94.191.123	3.96.23.237	64.74.223.8
103.224.212.212	176.32.97.204	185.94.191.124	31.13.72.8	64.99.80.30
103.224.212.217	176.32.98.237	185.94.191.14	31.13.92.10	65.108.111.241
103.224.212.221	176.32.99.100	185.94.191.23	31.13.93.19	65.9.66.108
103.224.212.222	176.32.99.123	185.94.191.59	31.15.13.101	65.9.66.110
103.30.127.13	176.32.99.156	185.94.191.67	31.15.13.146	65.9.66.126
103.90.220.11	176.32.99.172	185.94.191.69	31.184.198.149	65.9.66.57
104.130.165.10	176.32.99.180	185.94.191.73	31.184.198.150	66.160.146.2
104.130.165.114	176.32.99.212	185.94.192.101	31.3.232.108	66.172.10.189
104.130.165.234	176.32.99.37	185.94.192.106	31.3.232.116	66.85.157.71
104.130.166.123	176.32.99.45	188.166.176.58	31.3.232.125	66.85.157.83
104.130.166.86	176.32.99.49	188.166.184.217	31.3.232.126	66.85.157.84
104.155.138.21	176.74.176.167	188.166.184.78	34.102.136.180	66.96.147.159
104.171.16.31	176.74.176.178	188.215.229.205	34.196.164.216	66.96.162.145
104.171.21.200	176.74.176.179	188.215.229.212	34.205.242.146	67.225.218.50
104.200.22.130	178.62.16.70	188.215.229.213	34.98.99.30	67.228.171.237
104.200.23.95	178.62.212.205	188.215.229.214	35.172.94.1	68.178.232.100
104.21.12.249	179.43.125.194	188.215.229.215	35.205.61.67	68.178.232.143
104.21.14.210	179.43.169.36	188.215.229.216	35.241.18.84	68.178.232.68
104.21.22.143	179.43.169.41	188.215.229.222	37.139.10.119	68.178.232.99
104.21.31.18	179.43.169.8	188.226.191.238	37.220.31.107	68.178.246.253
104.21.40.49	18.119.154.66	188.40.155.240	37.220.31.108	68.66.248.15
104.21.41.75	18.165.122.45	190.97.165.115	37.220.31.114	68.66.248.32
104.21.49.229	18.165.122.69	191.101.31.114	37.220.31.19	69.171.250.15
104.21.56.120	18.165.122.76	191.101.31.118	37.220.31.28	69.172.201.208
104.21.69.196	18.165.122.98	191.101.31.21	37.220.31.46	69.43.161.161
104.21.78.107	18.65.39.120	191.101.31.213	37.220.31.78	69.64.147.10
104.21.91.142	18.65.39.123	191.101.31.214	37.220.31.80	69.64.147.242
104.216.8.34	18.65.39.5	191.101.31.222	37.48.65.148	69.64.147.28
104.216.8.38	18.65.39.92	191.101.31.25	37.48.65.149	70.32.1.32
104.219.248.95	18.66.112.108	191.101.31.29	37.48.65.151	72.14.178.174
104.219.53.104	18.66.112.33	192.121.23.183	37.48.65.152	72.14.185.43
104.239.143.7	18.66.112.64	192.155.108.149	37.48.65.153	72.21.194.146
104.239.157.210	18.66.112.79	192.161.187.200	37.48.65.154	72.21.194.20
104.239.162.22	180.215.67.139	192.161.48.122	37.48.65.155	72.21.195.167

104.239.169.57	184.168.131.241	192.185.131.113	37.72.175.143	72.21.195.72
104.239.169.58	184.168.221.34	192.187.111.219	37.72.175.179	72.21.203.159
104.247.162.122	184.168.221.38	192.187.111.220	38.132.114.167	72.21.211.197
104.247.82.53	184.168.221.40	192.187.111.221	38.132.114.168	72.52.178.23
104.27.136.90	184.168.221.44	192.187.111.222	38.132.118.107	72.52.4.90
104.27.137.90	184.168.221.47	192.52.243.110	38.132.118.108	74.117.114.80
104.28.18.154	184.168.221.58	192.64.119.113	38.132.118.110	74.208.2.190
104.28.19.154	184.168.221.62	192.64.119.135	38.132.118.111	74.208.236.136
104.28.30.120	184.168.221.64	192.64.119.155	38.132.118.114	74.208.236.70
104.28.31.120	184.168.221.66	192.64.119.191	38.132.118.116	74.53.234.130
104.37.35.119	184.168.221.67	192.64.119.204	38.132.118.117	74.53.234.148
104.37.35.65	184.168.221.69	192.64.119.231	38.60.88.108	75.2.18.233
104.37.35.67	184.168.221.70	192.64.119.51	38.84.132.165	75.2.37.224
104.37.35.68	184.168.221.71	192.64.119.99	38.84.132.168	76.223.67.189
107.149.180.159	184.168.221.75	192.64.151.240	38.84.132.172	77.245.76.109
107.149.180.57	184.168.221.76	193.201.35.20	38.84.132.174	77.245.76.110
107.149.180.59	184.168.221.78	193.203.185.128	43.139.248.205	77.245.76.113
107.161.23.204	184.168.221.79	194.187.249.106	44.227.65.245	77.247.179.82
107.178.223.183	184.168.221.83	194.195.211.98	44.227.76.166	77.247.179.83
107.180.51.22	184.168.221.85	194.195.220.41	45.176.188.29	77.247.179.84
107.21.207.1	184.168.221.90	194.244.56.186	45.33.122.153	77.247.179.85
107.22.166.27	184.168.221.91	194.58.112.174	45.33.126.185	77.247.179.86
108.157.214.100	184.168.221.92	194.58.56.113	45.33.18.44	77.247.179.87
108.157.214.22	184.168.221.93	194.58.56.158	45.33.2.79	77.247.179.88
108.157.214.26	184.168.221.94	194.58.56.50	45.33.20.235	77.247.179.89
108.157.214.73	184.168.221.95	195.110.124.133	45.33.23.183	77.247.179.90
108.157.229.10	184.168.221.96	195.12.48.42	45.33.30.197	77.247.179.91
108.157.229.104	185.106.120.130	195.12.50.176	45.33.4.29	77.247.183.146
108.157.229.121	185.106.120.173	195.12.50.177	45.33.9.234	77.247.183.147
108.157.229.129	185.106.120.246	195.12.50.179	45.55.28.80	77.247.183.148
108.157.4.101	185.106.120.34	195.149.84.100	45.55.55.31	77.247.183.149
108.157.4.113	185.106.120.35	195.149.84.101	45.56.69.72	77.247.183.150
108.157.4.32	185.107.56.197	195.245.112.107	45.56.72.12	77.247.183.152
108.157.4.41	185.107.56.198	195.245.112.96	45.56.79.23	77.247.183.153
108.170.31.100	185.107.56.199	195.35.39.197	45.76.42.111	77.247.183.154
108.186.135.237	185.107.56.200	198.185.159.144	45.77.139.78	77.73.65.199
109.200.24.10	185.109.168.12	198.252.105.22	45.79.19.196	77.73.65.210
109.200.24.102	185.109.168.18	198.49.23.144	46.101.1.140	77.73.65.47
109.200.24.104	185.109.168.29	198.49.23.145	46.101.119.3	77.73.65.48
109.200.24.106	185.117.72.10	198.54.117.197	46.101.142.156	77.73.68.160
109.200.24.11	185.117.72.113	198.54.117.198	46.101.16.63	78.142.25.30
109.200.24.112	185.117.72.117	198.54.117.199	46.101.196.252	78.142.25.37
109.200.24.121	185.117.72.120	198.54.117.200	46.101.215.198	79.141.160.2
109.200.24.122	185.117.75.165	198.54.117.210	46.183.216.141	8.28.175.71
109.200.24.126	185.117.75.169	198.54.117.212	46.183.219.79	8.28.175.73
109.200.24.14	185.117.75.228	198.54.117.244	46.183.221.149	8.28.175.78

109.200.24.15	185.117.75.82	198.58.118.167	46.183.221.185	8.39.147.100
109.200.24.18	185.117.75.84	199.115.115.102	46.183.221.187	8.5.1.32
109.200.24.19	185.117.89.145	199.115.115.116	46.183.223.249	8.5.1.33
109.200.24.2	185.117.89.198	199.115.115.118	46.21.147.123	8.5.1.35
109.200.24.20	185.117.89.220	199.115.115.119	46.21.147.14	8.5.1.38
109.200.24.32	185.117.89.231	199.115.116.216	46.21.147.141	8.5.1.39
109.200.24.48	185.117.89.251	199.115.116.43	46.21.147.173	80.211.250.229
109.200.24.58	185.117.89.252	199.16.129.222	46.21.147.196	80.211.254.70
109.200.24.59	185.117.89.253	199.195.142.109	46.21.147.197	80.255.12.246
109.200.24.64	185.130.184.35	199.34.228.59	46.21.147.21	80.255.3.107
109.200.24.66	185.134.29.144	199.59.242.150	46.21.147.224	80.255.3.111
109.200.24.7	185.134.29.146	199.59.242.151	46.21.147.237	80.255.6.24
109.200.24.71	185.14.29.17	199.59.242.153	46.21.147.46	80.67.28.104
109.200.24.72	185.14.31.48	199.59.243.200	46.21.147.65	81.169.145.149
109.200.24.73	185.141.25.210	199.59.243.224	46.21.150.144	81.17.18.194
109.200.24.76	185.141.25.30	199.59.243.225	46.22.223.209	81.17.18.195
109.205.180.8	185.141.26.18	199.80.53.28	46.22.223.252	81.17.18.196
109.248.222.20	185.141.26.39	200.7.105.24	46.246.1.12	81.17.18.197
109.68.33.64	185.141.26.49	200.7.105.3	46.246.1.14	81.17.18.198
109.70.26.36	185.141.26.50	200.7.105.39	46.252.18.146	81.17.29.146
128.199.157.230	185.141.27.116	200.7.111.102	46.38.243.234	81.17.29.147
128.199.227.0	185.141.27.123	200.7.111.11	46.4.96.16	81.17.29.148
128.199.81.37	185.141.27.124	200.7.111.118	47.91.170.222	81.17.29.149
13.225.78.108	185.144.83.114	200.7.111.124	5.102.145.113	81.17.29.150
13.225.78.111	185.144.83.116	200.7.111.125	5.102.145.12	81.17.30.45
13.225.78.34	185.156.173.104	200.7.111.154	5.102.145.122	81.171.22.4
13.225.78.37	185.156.173.118	200.7.111.155	5.102.145.130	81.171.22.5
13.226.153.128	185.156.173.70	200.7.111.156	5.102.145.14	81.171.22.6
13.226.153.15	185.156.175.219	200.7.97.167	5.102.145.169	81.171.22.7
13.226.153.76	185.181.10.64	200.7.97.168	5.102.145.17	81.19.154.98
13.226.153.89	185.183.107.43	200.7.97.212	5.102.145.180	81.22.255.180
13.248.169.48	185.183.107.44	200.7.97.213	5.102.145.183	81.31.145.134
13.248.213.45	185.183.107.49	200.7.97.214	5.102.145.248	81.92.202.215
13.32.121.18	185.183.96.131	200.7.97.215	5.102.145.26	81.92.202.222
13.32.121.21	185.183.96.139	200.7.97.216	5.102.145.37	81.95.101.8
13.32.121.59	185.183.96.140	200.7.97.225	5.102.145.39	81.95.5.144
13.32.121.6	185.183.96.149	200.7.97.228	5.102.145.64	81.95.5.147
13.33.243.12	185.183.96.150	200.7.97.229	5.102.145.72	81.95.5.164
13.33.243.21	185.183.96.169	200.7.97.230	5.102.145.8	81.95.5.165
13.33.243.38	185.183.97.117	200.7.97.238	5.102.145.90	81.95.5.168
13.33.243.79	185.183.97.194	200.7.97.242	5.102.145.98	81.95.7.58
130.185.250.199	185.183.97.196	200.7.97.248	5.102.145.99	81.95.96.29
130.185.250.200	185.189.112.199	200.7.97.254	5.102.146.116	82.165.66.161
130.185.250.201	185.189.112.200	200.7.98.117	5.102.146.123	82.211.30.122
137.175.73.23	185.193.38.159	200.7.98.133	5.102.146.124	82.211.31.177
138.59.17.76	185.195.200.38	203.170.190.21	5.102.146.126	82.80.202.200

139.162.128.141	185.195.200.43	204.11.56.37	5.102.146.128	82.98.86.165
139.162.148.172	185.195.200.44	204.11.56.48	5.102.146.184	82.98.86.166
139.162.156.11	185.195.200.46	204.16.169.54	5.102.146.237	82.98.86.169
139.162.219.164	185.195.200.47	205.251.242.131	5.102.146.241	82.98.86.179
139.162.231.74	185.195.200.51	205.251.242.147	5.102.146.49	83.166.133.69
139.162.239.235	185.195.200.56	205.251.242.151	5.102.146.59	83.221.132.104
139.162.247.90	185.198.164.119	205.251.242.190	5.102.146.64	83.221.132.157
139.162.253.66	185.198.57.144	205.251.242.252	5.102.146.66	84.200.32.211
139.162.255.76	185.198.57.200	205.251.243.100	5.102.146.72	84.32.84.33
141.255.161.88	185.198.57.43	205.251.243.116	5.102.146.82	84.38.129.195
141.8.225.63	185.198.58.143	205.251.243.196	5.102.146.85	84.38.130.107
143.95.246.100	185.198.58.144	205.251.243.220	5.102.146.87	85.13.131.111
143.95.43.131	185.198.58.151	205.251.243.68	5.102.146.90	85.13.157.122
148.135.48.58	185.198.58.154	205.251.243.84	5.102.146.91	86.105.18.11
149.255.35.106	185.198.58.158	206.189.108.245	5.102.146.93	86.105.18.121
149.255.35.115	185.198.58.177	206.189.51.151	5.102.147.105	86.105.18.212
149.255.36.132	185.198.58.178	207.171.163.139	5.102.147.106	86.105.18.222
149.255.36.138	185.198.58.182	207.171.163.149	5.102.147.114	87.121.98.38
15.197.130.221	185.198.58.195	207.171.163.159	5.102.147.13	87.121.98.39
15.197.148.33	185.198.58.196	207.171.163.193	5.102.147.138	88.119.179.102
15.197.210.240	185.206.224.41	207.171.163.223	5.102.147.162	88.119.179.105
150.95.255.38	185.225.68.123	207.244.67.215	5.102.147.163	88.119.179.134
151.106.5.166	185.225.68.124	207.244.67.216	5.102.147.172	88.119.179.140
151.106.5.168	185.225.68.125	207.244.67.218	5.102.147.219	88.119.179.156
151.106.5.172	185.225.68.126	208.87.35.103	5.102.147.234	88.119.179.164
153.122.19.55	185.225.68.127	208.91.197.197	5.102.147.235	88.119.179.165
154.16.37.105	185.225.68.128	208.91.197.241	5.102.147.236	88.119.179.166
154.16.37.11	185.225.68.129	208.91.197.44	5.102.147.250	88.119.179.168
154.16.37.35	185.225.68.130	208.91.197.46	5.102.147.254	88.119.179.169
154.16.37.39	185.225.68.131	208.91.197.54	5.102.147.41	88.119.179.176
154.16.37.40	185.225.68.132	208.91.197.87	5.102.147.51	88.119.179.205
154.197.157.153	185.225.68.133	208.91.197.91	5.102.147.73	88.119.179.226
154.26.238.46	185.225.68.134	209.126.81.34	5.102.147.82	88.150.138.106
154.7.60.56	185.225.68.135	209.141.38.71	5.104.105.200	88.150.138.111
154.80.164.162	185.225.68.136	209.17.116.163	5.135.199.22	88.150.138.66
155.94.160.126	185.225.68.141	209.250.247.96	5.149.248.193	88.150.138.69
156.250.5.59	185.225.68.158	209.85.51.152	5.149.248.2	88.150.138.74
156.251.228.56	185.225.68.159	209.99.40.222	5.149.248.27	88.150.138.78
157.240.0.13	185.225.68.160	209.99.40.223	5.149.249.174	88.150.138.82
157.240.194.18	185.225.68.176	209.99.64.18	5.149.249.189	88.150.138.83
157.240.195.17	185.225.68.177	209.99.64.25	5.149.249.19	88.150.138.85
157.240.196.17	185.225.68.198	209.99.64.52	5.149.250.18	88.150.138.99
157.240.2.20	185.225.68.199	209.99.64.53	5.149.250.19	88.150.189.106
157.240.20.15	185.225.68.2	212.237.249.16	5.149.250.2	88.150.189.108
157.240.201.17	185.225.68.200	212.32.237.101	5.149.252.157	88.150.189.111
157.240.205.1	185.225.68.201	212.32.237.90	5.149.252.241	88.150.189.121

157.240.21.16	185.225.68.202	212.32.237.91	5.149.254.12	88.150.227.103
157.240.221.18	185.225.68.203	212.32.237.92	5.149.254.14	88.150.227.104
157.240.236.15	185.225.68.204	213.171.195.105	5.149.254.18	88.150.227.105
157.240.251.6	185.225.68.205	213.202.100.29	5.149.254.2	88.150.227.110
157.240.252.10	185.225.68.206	216.21.239.197	5.149.254.20	88.150.227.115
157.240.253.13	185.225.68.207	216.239.32.21	5.149.254.24	88.150.227.116
157.240.9.18	185.225.68.229	216.245.197.41	5.149.254.5	88.150.227.117
159.89.193.231	185.225.68.3	216.245.197.42	5.149.255.16	88.150.227.118
159.89.8.195	185.225.68.5	216.245.197.43	5.149.255.18	88.150.227.119
159.89.84.252	185.225.68.6	216.245.197.44	5.149.255.19	88.150.227.120
160.153.128.24	185.225.68.60	216.245.197.46	5.149.255.198	88.150.227.121
162.209.103.68	185.225.68.61	216.245.214.81	5.149.255.3	88.150.227.122
162.210.195.111	185.225.68.64	216.245.214.82	5.149.255.69	88.150.227.125
162.210.196.166	185.225.68.65	216.245.214.83	5.79.68.103	88.150.227.77
162.210.196.167	185.225.68.68	216.245.214.84	5.79.79.209	88.150.227.83
162.210.196.168	185.225.68.69	216.245.214.85	5.79.79.211	88.150.227.98
162.241.224.215	185.225.68.75	216.245.214.86	50.116.15.71	88.150.227.99
162.241.253.111	185.225.68.77	217.112.131.103	50.63.202.36	88.99.107.18
162.241.62.217	185.225.68.86	217.112.131.106	50.63.202.45	89.107.57.53
162.241.62.49	185.225.68.97	217.112.131.108	50.63.202.55	89.107.57.62
162.242.231.231	185.225.74.114	217.112.131.109	50.63.202.59	89.117.139.95
162.254.207.52	185.230.124.228	217.112.131.111	50.63.202.60	89.238.132.249
162.254.207.55	185.230.124.233	217.112.131.120	50.63.202.63	89.238.138.136
162.254.207.58	185.230.124.234	217.112.131.136	50.63.202.64	89.238.138.141
162.254.207.59	185.230.124.235	217.112.131.137	50.63.202.67	89.249.65.138
162.254.207.60	185.230.124.241	217.112.131.146	50.63.202.68	89.249.65.146
162.255.119.119	185.230.60.173	217.112.131.147	50.63.202.69	89.249.65.148
162.255.119.143	185.230.61.173	217.112.131.150	50.63.202.73	89.249.65.149
162.255.119.171	185.230.63.107	217.112.131.156	50.63.202.75	89.249.65.165
162.255.119.199	185.230.63.171	217.112.131.158	50.63.202.76	89.249.65.193
162.255.119.207	185.230.63.186	217.112.131.16	50.63.202.77	89.249.65.206
162.255.119.215	185.234.73.10	217.112.131.176	50.63.202.79	89.249.65.234
162.255.119.248	185.236.202.184	217.112.131.189	50.63.202.80	89.33.246.112
162.255.119.254	185.243.112.77	217.112.131.20	50.63.202.81	89.33.246.113
162.255.119.36	185.243.115.100	217.112.131.207	50.63.202.82	89.33.246.118
162.255.119.61	185.244.150.68	217.112.131.208	50.63.202.85	89.33.246.119
163.172.140.159	185.29.11.165	217.112.131.227	50.63.202.86	89.34.111.212
163.44.197.147	185.29.11.200	217.112.131.39	50.63.202.93	89.40.181.124
164.132.138.55	185.29.11.203	217.112.131.42	50.63.202.94	89.40.181.125
165.3.107.227	185.38.151.11	217.112.131.58	50.63.202.95	89.43.60.103
167.172.228.26	185.44.105.35	217.112.131.61	50.87.144.12	89.43.60.104
167.88.5.222	185.45.192.134	217.112.131.67	50.87.148.122	91.195.240.117
167.99.136.207	185.45.192.144	217.112.131.90	51.255.109.179	91.195.240.82
170.178.168.203	185.45.192.231	217.112.131.91	52.20.84.62	91.195.240.87
170.178.183.18	185.45.193.210	217.112.131.95	52.203.208.133	91.195.240.94
172.104.57.40	185.53.178.50	217.160.0.104	52.25.69.130	91.213.50.73

172.121.113.173	185.53.178.8	217.160.0.123	52.41.243.83	91.216.245.56
172.234.25.151	185.53.178.9	217.160.0.7	52.42.91.180	91.219.238.77
172.67.136.127	185.53.179.170	217.182.242.101	52.45.169.12	91.219.28.21
172.67.150.213	185.53.179.6	217.61.104.60	52.54.37.95	91.90.192.176
172.67.160.146	185.53.179.7	217.61.4.34	52.58.78.16	92.222.208.251
172.67.160.65	185.53.179.8	217.61.5.131	52.71.57.184	93.158.200.205
172.67.174.165	185.60.216.15	217.61.7.152	52.73.71.73	93.158.203.140
172.67.176.38	185.60.218.19	217.61.96.219	52.77.227.164	93.158.203.142
172.67.196.200	185.68.16.188	217.61.96.247	52.8.153.44	94.177.234.8
172.67.205.80	185.73.37.131	217.64.113.250	52.8.52.166	94.177.236.235
172.67.208.210	185.73.37.19	217.64.113.251	52.86.108.145	94.177.239.30
172.67.212.202	185.73.37.207	217.64.113.252	52.86.6.113	94.52.85.185
172.67.220.96	185.73.37.218	217.64.113.254	54.161.222.85	95.183.51.199
172.67.222.21	185.73.37.49	217.64.114.179	54.186.251.233	95.213.188.35
172.93.103.100	185.73.38.107	217.70.184.38	54.187.191.4	95.213.193.40
172.93.103.101	185.77.129.103	23.107.197.107	54.187.40.241	96.126.123.244
172.93.103.102	185.77.129.136	23.227.207.174	54.191.52.61	98.124.204.16
172.93.103.99	185.77.131.10	23.227.38.32	54.201.71.208	98.124.243.34
173.192.56.250	185.77.131.103	23.227.38.65	54.209.32.212	98.124.243.38
173.193.212.4	185.77.131.109	23.23.88.25	54.224.163.221	98.124.243.39
173.212.192.14	185.80.53.199	23.230.62.149	54.227.98.220	98.124.243.40
173.245.5.106	185.81.113.105	23.236.62.147	54.231.1.228	98.124.243.41
173.254.248.104	185.81.113.81	23.253.126.58	54.231.1.252	98.138.19.88
173.254.248.105	185.82.200.143	23.253.126.7	54.231.16.36	98.139.135.21
173.254.248.115	185.82.200.164	23.253.238.196	54.251.49.214	99.81.40.78
173.255.194.134	185.82.200.187	23.253.238.232	54.37.104.101	99.83.154.118
174.120.189.99	185.82.200.233	23.253.241.66	54.72.130.67	99.83.175.80
174.122.27.24	185.82.202.29	23.82.12.29	54.72.9.51	99.83.248.67
176.223.111.137	185.82.202.32	23.82.12.30	62.113.232.197	
176.223.111.159	185.82.202.42	23.82.12.31	62.113.232.207	
176.223.111.206	185.93.183.231	23.82.12.32	62.113.232.221	

Table 14 - Domains related to Pegasus activity

123tramites.com	cryptocurrecny.com	hundredsofdesigns.net	novosti247.com	somuchrain.com
14-tracking.com	cryptokoinz.com	icecreamlovesme.com	now-online.net	sparepresence.com
1minto-start.com	cryptopcoinz.com	icloudcacher.com	nsoqa.com	specialgifts4all.com
1place-togo.com	csomagodjott.com	icrcworld.com	nuevaidea.co	speechenforce.com
24-7clinic.com	cssgraphics.net	ideas-telcel.com.mx	objectreduction.com	speedservicenow.com
301-redirecting.com	cupscars.net	igiheonline.com	odnoklass-profile.com	spiritualbrakes.com

365redirect.co	curiousrabbitgame.com	ikomek.info	offresimmobilier.com	sportssaint.net
3driving.com	currentscan.net	ilovemybeatifulnails.com	offspringperform.net	sportupdates.info
456h612i458g.com	currentwestpeople.com	ilovemymilf.com	ok-group.org	sportupdates.online
7style.org	daily-sport.news	img565vv6.holdmydoor.com	old-glasses.net	sputnik-news.info
800health.net	damanhealth.online	in-weather.com	oldmywater.com	squaretables.net
911hig11carcay959454.com	dancersing.net	in2date.com	one-isnot-enough.com	sslbind.com
9jp1dx8odjw1kbkt.f15fwd322.regularhours.net	dancinglife.co	inbox-messages.net	oneadjump.com	standartsheet.com
a-redirect.com	dashboardprompt.com	income-tax.online	oneleadingchat.com	standstock.net
a-resolver.com	data-formula.com	indrive.info	onetreeinheaven.com	starbuckscoffeeweb.com
aalaan.tv	databasemeans.net	industry-specialist.com	online-dailynews.com	starreturned.com
access.dynamic-dns.net	deadwordsstory.com	ineediscounts.com	online-loading.com	stars4sale.co
accomodation-tastes.net	deal4unow.com	info24.live	onlinefreework.com	start2playnow.com
accountant-audio.com	dearlegendseed.com	infoquiz.net	onlineshopzm.com	starting-from0.com
accountcanceled.com	defencepk.email	informados24h.cominfo-urbano.com	only-news.net	startupsservices.net
accountnotify.com	delivery-24-7.com	infospotpro.com	onlycart.net	stationfunds.net
accounts-unread.com	dental-care-spa.net	infospress.com	onlygossip.info	statisticsdb.net
accounts.mx	deportes24-7.com	insertfilters.net	onlytoday.biz	statsads.co
accountsections.com	deportesinfo.com	insta-foto.net	onlywebsite.org	statsupplier.com
accountsecurities.org	derinaydogan.com	instangram.com.mx	onthegoodtime.com	stayallalone.com
activate-discount.com	designednetwork.com	internetmobilespeed.com	ooredoodeals.com	staysystem.net
active-folders.com	destinytool.net	intim-media.net	openingquestion.org	sterlingpetcare.com
actorsshop.net	detailrush.net	investigationews.com	opera-van.com	stilloak.net
actu24.online	deter-individuals.com	investormanage.net	operatingnews.com	stopmysms.com
ad-generator.net	devicer.co	ipjackets.com	operations-delivery.com	stopsms.biz
ad-switcher.com	dhcpserver.net	ipurlredirect.com	operations-shifts.com	storageseminar.net
add-client.com	diagram-shape.com	islam-today.info	oplata-shtraf.info	storelive.co
additional-costs.com	diaspora-news.com	islam-world.net	opposedarrangement.net	strangegloom.net
addmyid.net	diningip.com	islamic-news-today.com	optionalshift.online	strategyroles.com
addresstimeframe.com	dinneraroundyou.com	islamiyaat.com	optionstoreplace.com	suitcasesmellnice.com

adeal4u.co	directbegins.com	ispr.email	orange-updates.com	summermover.com
adjust-local-settings.co	directlyforuse.com	istgr-foto.com	organicdiamonds.net	sunday-deals.com
adjust-local-settings.com	directurl-loading.com	itsthebrowser.com	ourorder.info	sunnydaylight.com
adjustlocalsettings.net	discountads.net	iusacell-movil.com.mx	ourperfume.net	sunrise-brink.net
adscreator.net	discountmarkets.info	iwantitallnow.com	outgoingurl.com	sunsetdnsnow.com
adsload.co	discountstores.info	jaimelire.net	outletsaroundme.com	superlinks4u.com
adsmetrics.co	discoveredworld-news.com	jeeyarworld.com	outletstore.tech	support-team.tech
advert-time.com	displaytag.net	judgeauthority.com	page-host.net	supportonline4me.com
advert-track.com	dns-1.co	judo-genlis.com	page-info.com	surprising-sites.com
afriquenouvelle.com	dns-analytics.com	just-one-left.com	pageisloading.net	sweet-water.org
afternicweb.net	dns-direct.net	kaidee.info	pageredirect.co	sweetcup.co
agilityprocessing.net	dns-upload.com	karbalaeyat.com	pageupdate.co	sync-cdn.com
aircraftsxhibition.com	dnsclocknow.com	kaspi-payment.com	painruncart.com	syncingprocess.com
ajelnews.net	dnslogs.net	keepiptext.com	painting-walls.com	syncmap.org
akhbar-aliqtisad.com	dnsmachinefork.com	keepthiseasy.com	pakistanarmy.email	systemtrees.com
akhbar-almasdar.com	dnsprotector.net	kenyasms.org	panelbreed.com	t-support.net
akhbar-arabia.com	dnsroof.com	keyindoors.com	papers2go.co	tablereservation.info
akhbar-islamyah.com	do-itonyour-own.com	keynotepalm.com	papervoice.net	tahmilmilafate.com
akhbara-aalawsat.com	documentpro.org	khaleejtimes.online	parinari.xyz	tahmilmilafate.info
akhbarnew.com	dogfoodstorage.net	khilafah-islamic.com	park4free.info	takecarhomes.com
al-nusr.net	dogopics.com	kingdom-deals.com	particularmechanic.net	takemallelectric.com
al-taleanews.net	doitformom.com	kingdom-news.com	parties-fun.com	takethat.co
al-taleanewsonline.net	doitforthefame-now.com	klientuserviss.com	passwd.privo7799add.net	talabatt.net
al7erak247.com	domain-control.net	knowingfun.com	pastesbin.com	tastyteaflavors.com
al7eraknews.com	domain-redirect.com	knowseminar.com	pathtogo.net	teachskate.com
alawaeltech.com	domain-resolver.net	koramaghreb.com	pay-city.com	techhelping.net
albumphotopro.biz	domain-routing.com	kra.center	pay-penalty.info	telangana-news24.com
alignmentdisabled.net	domain-security.org	kruseswiss.com	paynfly.info	telecom-info.com
alive2plunge.com	domainloading.net	kurjerserviss.com	paywithcrytpo.com	telephonequality.com

all-sales.info	domainport.net	labonneforme.net	pc-views.net	template-iso.net
allaboutwrightwood.com	domains-resolver.net	lamyterie.com	pemra.email	tengrinews.co
allafricaninfo.com	domainsearching.net	landflatheart.com	performinghost.com	tentrosegain.com
allbeautifularts.com	domesticwindow.com	landstofree.com	permalinking.com	thainews.asia
alldaycooking.co	donateabox.co	laptop-parts.org	phonemetrics.co	thankstossl.com
allergiesandcooking.com	donateaflower.com	last-chainleash.net	phonering4you.com	the-only-way-out.com
allfadiha.co	donateyouroldclothes.net	latest-songs.com	phonestats.net	theappanalytics.com
alljazeera.co	done.events	lawlowvat.net	photo-afisha.net	theastafrican.com
allladiesloveme.com	donefordeal.com	layerprotect.com	photo-my.net	thebestclassicalmusic.net
allthecolorsyoulike.com	doorcoffeebrown.com	layoutfill.com	physicalcheetah.com	thecoffeeilove.com
allthegamesyouneed.com	dotroomeight.com	leadersnews.org	pi.license-updater.com	thefuturearticle.net
allthemakeupyouneed.com	dowhatyouneed.com	leavehomego.com	pickcard.info	thehighesttemple.com
allthesongsyoulike.com	downgradeproduct.com	leggingsjustforyou.com	pickuchu.com	thehoteloffers.com
alluneed4home.net	download.fbr.tax	legsfriesears.com	picture4us.com	theredirect.net
alpharythme.com	dramatic-challenge.com	legyelvodas.com	pincattape.com	theshopclub.org
alrainew.com	driventicket.com	legyelvodas.net	pine-sales.com	thesimplestairs.com
android-core.org	e-loading.biz	leleader.org	pirnaram.xyz	thespaclub.net
android-updates.net	e-prokuror.info	leprotestant.com	pizzatoyourplace.com	theway2get.com
animal-politico.com	e-sveiciens.com	lesbonnesaffaires.online	planeocean.com	thoughtfulbundle.com
api.priveetalk.com	eardooraround.com	leshutchins.com	playfantasticsplastic.com	thtube.video
apiapple.com	earsstrawsfive.com	lesportail.biz	playwithusonline.com	tibetnews365.net
apigraphs.net	easy-pay.info	letyoufall.com	pleaseusenew.com	ticket-aviata.info
apiwacdn.com	easybett.online	levelsteelwhite.com	pleaseusenew.net	ticket-selections.com
appleleaveit.co	ecommerce-ads.org	liam-ryan.co	pmogovpk.email	tiketon.info
applicationcreation.net	economic-news.co	license-updater.com	pochta-info.com	timelesscelebrity.com
appointments-online.com	editorscolumn.net	lifedonor.net	politica504.com	timeofflife.com
appsgratis.com.mx	effectivespeech.net	lifenoonkid.com	politicalpress.org	tinyurler.com
appsjuegos.com.mx	egov-online.com	like-the-rest.com	politicoportales.org	tlgr-me.org
ar-tweets.com	egov-segek.info	limitedfeature.com	politiques-infos.info	tobepure.com
arab-share.com	egov-sergek.info	link-crawler.com	popagency.net	todaysdeals4u.com

arabia-islamion.com	ehistorybooks.com	link-scan.net	popularmessages.net	todoinfonet.com
arabnews365.com	elementscart.com	linking-page.com	port-connection.com	toggletools.com
arabworld.biz	eliminateadjust.com	linksnew.info	portredirect.net	tommyfame.com
arabworldnews.info	eliteautosaloninc.com	littlefrogalarm.com	possibilitytotransfer.com	tomorrowpastno.com
around-theglobe.co	elitecarz.net	live-once.net	posta.news	tookcheckout.com
arrowowner.com	eltiempo-news.com	lizzardsnail.com	postainf.net	top100vidz.com
asrararabiya.co	email-plans.com	loading-ads.net	pourcentfilers.com	top10gifts4men.com
asrararablya.com	emiratesfoundation.net	loading-domain.com	poweredbycpanel.com	top10leadsgen.com
asrarrarabiya.com	emonitoring-paczki.pl	loading-images.com	poweredlock.com	topadblocker.net
assembled-battery.com	energy-dispatch.net	loading-pag.net	ppcisdead.com	topbraingames4u.com
atlaslions.info	enoughtoday.org	loading-page.net	pprocessor.net	topcontactco.com
audienceflake.com	entertainmentinat.com	loading-url.net	practical-basis.net	topoems.com
auditorcast.com	entire-cases.com	loadingpage1.net	practicehazard.com	topten-news.info
authenticangry.com	equal-gravity.com	loadingpage4.net	preferenceviews.com	touristvaca.com
authenticated-origin.com	erty.online	loadingurl.net	preferring.org	towebsite.net
authlovebirth.com	estatearea.net	loadthatpage.com	presidentialagent.com	track-your-fedex-package.com
autodiscount.info	eura-cell.com	localgreenflowers.com	preventadmission.com	track-your-fedex-package.online
autoredirect.net	eurasianupdate.com	login-service.net	preventsusing.com	track-your-fedex-package.org
av-scanner.com	eurosportnews.info	loginverify.net	pride-industry.com	trackyourfedexpackage.net
avocadofight.com	event-reg.info	loisiragogo.com	pride-industry.net	trade-agreement.com
awardpractice.com	everycolor-inside.com	lonely-place.com	pridetomyself.net	tradeexchanging.com
awizo.info	everyuse.org	look-outsidenow.com	prikol-girls.com	traffic-pay.com
axis-indication.net	ex-forexlive.com	looking-for-two.com	primarystrike.net	traffic-updates.info
babies-bottles.com	exchangenames.net	lookitupnow.website	prioritytrail.net	transfer-rate.com
bahrainsms.co	exchangenerate.com	looklifewhite.com	priveetalk.com	transferbase.co
balancewreckpoint.com	existingpass.com	loschanquetes.com	privo7799add.net	transferkeep.com
bananakick.net	exoticsendurance.com	loschismescalientes.com	productsall.net	transferlights.com

banca-movil.com	expired-getway.net	losnegocios.biz	productsview.co	travel-foryou.online
banca-movil.net	expiredsession.com	lost-n-found.net	produitsjpcote.com	travelcrimea.info
bankportal.net	expiringdate.com	loveandhatenow.com	projectgoals.net	travelight.online
baramije.net	exploreemail.net	lowervalues.com	promosderevee.com	traveltogether.link
bargainservice.online	extend-list.net	m-resume.com	promotionlove.co	trendsymbol.net
bbc-africa.com	externalprivacy.com	macmaclaren.com	proudmorale.com	trialvariable.net
bdaynotes.com	externaltransfers.com	maghrebfoot.com	pub-dns.com	trianglerank.net
beanbounce.net	extractsight.com	maghrebfunny.biz	publishbig.net	tricksinswiss.com
beautifulhousesaroundme.com	extrahoney.net	magicalipone.com	puffyteddybear.com	trililihihi.com
becomeiguana.com	eyestoip.com	mailappzone.com	purchaseusingcoins.com	tripleclickpays.com
beethoventopsymphonies.com	eyesunderspray.com	mailerservice.directory	purple-enveloppe.com	tunnelprotocol.net
behindaquarium.com	ezdropshipping.net	maingreatessay.com	puttylearning.com	turismo-aqui.com
benjamin-taganga.info	f15fwd322.regularhours.net	mainredirecter.com	qaintqa.com	turkeynewsupdates.com
bestadventures4u.com	fabric-shops.com	mamba-live.com	qaoffers.net	turkishairines.info
bestcandyever.com	face-image.com	managedsnap.com	qualityfeeling.net	tvshowcusting.com
bestday-sales.com	facebook-accounts.com.mx	management-help.com	quitmyjob.xyz	twiitter.com.mx
bestfoods.co	fadewallwine.com	managingincluded.com	quota-reader.net	uaenews.online
bestfriendneedshelp.com	fadi7apress.com	mangoutlet.net	quran-quote.com	uidebol.info
bestheadphones4u.com	fallround.com	manoraonline.net	rainingcats.net	umbrellacover.net
besthotelsaroundme.com	fallsjuice.com	manydnsnow.com	raininscreen.com	un-limitededitions.com
bestperfumesnow.com	familyabroad.net	maphonortea.com	randomlane.net	un0noticias.com
bestpresents4all.net	fantastic-gardens.com	mapupdatezone.com	rapidredirecting.com	un0noticias.net
bestsalesaroundme.com	fashion-live.net	martinipicnic.com	raresound.org	unavailableentry.com
beststores4u.com	fashion-online.net	massagetax.co	raw-console.com	unionofteenagers.com
bestsushiever.com	fashioncontainer.net	masternicherights.com	reachcomputer.com	uniquesite.co
better-deal.info	fashionpark.info	masterpolishformula.com	readingbooksnow.com	universopolitico.net
betterapplesearch.com	fastdirect.net	matlauinlondon.com	readirectly.com	univision.click
betterhandsblack.com	fastfixs.net	maymknch2026.co	realmythtrend.com	unlockaccount.net

bicyclerentalnow.com	fatpop.net	mcel-update.com	receiptpending.net	unonoticias.net
biggunsarefun.com	fb-accounts.com	mcel.info	reception-desk.net	unsubscribe-now.net
bigseatsout.net	fbr-update.com	mealrentyard.com	recepzihni.com	unsubscribed.co
billednorth.com	fbr.news	meanspursuit.com	recordinglamping.com	unsubscribeinhere.com
bingoblitzvippro.com	fbr.tax	medical-updates.com	redcrossworld.com	untoldinfo.net
birdbathmorning.com	fbsecurity.co	medicalcircle.net	redemptionphrase.com	unusualneighbor.com
biscuit-taste.net	feature-publish.net	megacenter.info	redirect-connection.com	updateapps.net
bitanalysis.net	feelbonesbag.com	megaticket.info	redirect-link.com	updatedchargers.com
bitfadepens.com	feeltrail.com	mercedesbenz-vip.com	redirect-net.com	updatedcharges.net
bitforeat.net	femmedaffaire.com	merchant-businesses.com	redirect-protocol.com	updating-link.com
bl33pon6373.com	fetchlink.net	mergeandcenter.com	redirect-service.net	updating-url.com
black-bricks.net	fiestamaghreb.com	methodslocal.com	redirect-systems.com	updating-url.net
blackberry.org.mx	file-dnld.com	mgifweb.com	redirect-traffic.net	updatingpage.com
blackwhitebags.com	files-downloads.com	mideast-today.com	redirect-tunnel.net	updatingwebpage.com
blcheck.utensils.pro	filingwarranty.com	mijn-vgz-overzicht-nl.info	redirect-webpage.net	upgrade-sim-card.com
blindlydivision.com	financecomments.net	miles-club.com	redirect2url.net	upkeepno.com
blockedsituation.net	findavoucher.online	miralo-rapidamente.com	redirectchannel.net	upload-now.net
blogreseller.net	findgoodfood.co	mirrorgossip.com	redirectcheck.net	uptownfun.co
blue.911hig11carcay959454.com	findgroupon.com	mixershake.net	redirectconnection.net	urbestfriends.com
boldconclusion.com	finditout-now.com	mixsinger.com	redirectdoor.com	url-configure.com
booking-tables.com	findmyass.org	mobi-up.net	redirecteur.net	url-direct.com
bottlehere.com	findmyfriendsnow.com	mobile-analytics.netweb-cloud-services.com	redirectgate.com	url-hoster.com
boxes-mix.net	findmylunch.org	mobile-softs.com	redirecting-url.com	url-loading.com
boysrbabies.co	findmymind.co	mobile-update.online	redirectingpage.net	url-redirect.com
br-hashtags.com	findmyplants.com	mobile-updates.info	redirectingurl.net	url-redirect.net
br-travels.com	findouthere.org	mobilebrowsing.net	redirectingurl.org	url2all.net
brand-tech.net	firebulletfan.com	mobilephonesme.com	redirection-url.net	urlconfig.net

brandttoyota.com	fishingtrickz.com	mobiles-security.net	redirectit.net	urlconnection.net
breakfastisgood.com	fitness-for-ever.com	mobileweatherweb.com	redirectking.net	urldefender.net
breaking-extranews.online	flashobligation.com	modifytimezone.net	redirectload.com	urlpage-redirect.com
breaking-news.co	flashtraininggoal.com	moh-followup.com	redirectmotion.org	urlpush.net
breakingnewsasia.com	flights-report.com	moh-online.com	redirectnet.net	urlredirect.net
breakthenews.net	flights-todays.com	monawa3ate.org	redirectool.com	urlregistrar.net
brighttooth.net	flowersarrows.com	mondaymornings.co	redirectprotocol.net	urlreload.net
brookviewpetgrooming.com	flying-free.online	moneycheesecolor.com	redirectshare.com	urlscanner.net
brownandblueeyes.com	flynewfries.com	moneycoincurrency.com	redirectweburl.com	urlsync.com
browser-update.online	fofopiko.org	moneydigitalcurrency.com	redirigir.net	urlupdates.com
bubblesmoke.net	foodeveryhour.com	moneyxchanges.com	redirstats.com	urlviaweb.com
bubblesweetcake.com	foodforyou.info	moregatesthere.com	redstarnews.net	urspanishteacher.net
buildingcarpet.com	foodiez.online	morning-maps.com	reflectextension.net	user-registration.com
buildurlife.net	forgetjustit.com	mosque-salah.com	regionews.net	utensils.pro
buildyourdata.com	formatpainter.net	mosque-salah.net	regularhours.net	vamizi.info
bulbazaur.com	formattingcells.com	mosquesfinder.com	reklamas.info	vanillaandcream.com
bulk-theft.net	forward-page.com	motiontastebad.com	related-ads.com	varietyjobspaid.org
bulksender.info	forward5costume.com	motivation-go.com	relatedspams.net	varietyregistrar.com
bulktheft.com	foto-top.info	motordeal.info	reload-url.com	vastdealsnow.com
bullgame.net	foudefoot.live	movie-tickets.online	reload-url.net	vault-encryption.com
bun54l2b67.get1tn0w.free247downloads.com	free-local-events.info	moyfoto.net	reloading-page1.com	verify-app.online
bunchi.club	free247downloads.com	moz-noticias.com	reloadinput.com	videosdownload.co
bundlestofear.com	freedominfo.net	mozillaname.com	reloadpage.net	videotubbe.net
business-today.info	freelancers-team.org	mozsafety.com	remove-client.com	vider-image.com
businesssupportme.com	freeshoemoon.com	mp3.ucrazy.org/music/	remove-from-mailing-list.com	vie-en-islam.com
bussybeesallover.com	freshandsoftbread.com	muftyat.com	remove-from-mailinglist.com	viedechretien.org
bustimer.net	freshsaladtoday.com	multiplecurrencies.com	remove-subscription.co	viewhdvideos.com

butterdogchange.com	functionalcover.com	music-electric.org	remove-subscription.com	viewstracker.com
buymanuel.co	fundum8430.com	music-headphones.org	renewal-control.net	vipmasajes.com
buypresent4me.net	funinat.com	muslim-world.info	rentalindustries.com	viva-droid.com
bytlo.com	funinthesun4u.com	muzicclips.com	rentmotors.net	vivrechezsoi.info
cablegirls.net	funintheuk.com	muziclovers.org	research-archive.com	vkan-profile.com
calculatesymbols.com	funnytvclips.com	my-privacy.co	reseausocialsolutions.co	volcanodistance.com
calendarsapp.com	funtifu.live	mybrightidea.co	reservationszone.com	volcanosregion.com
candlealbum.com	fwupdating.com	mydailycooking.net	reseufun.com	waffleswithnutella.com
captcha.bl33pon6373.com	gadgetproof.net	mydarkarms.com	resolutionsbox.com	waitingtoload.com
carpetdignity.com	gadgetsshop.info	myfiles.photos	restaurantsstar.com	walkerpost.net
carrefour-des-affaires.com	garrigareptiles.com	myfreecharge.online	results-house.net	walkhatclock.com
cars-to-buy.com	gate-sync.net	myfundsdns.com	revoke-dashboard.com	wallagainsthall.com
cartsafer.com	gdfr.online	mygreathat.com	revolution-news.co	walltome.com
cashandlife.com	gearstereotype.com	mygummyjelly.com	rewards-club.info	wasted-nights.com
cashtowebmail.com	getagift.info	myheartbuild.com	rhymeshey.com	waterforplants.net
casia-news.info	getoutofyourmind.com	mykaspi.com	righttriangle.net	watersport4u.net
casusbocekler.com	getphotosinstant.net	mylogfrog.com	roadwide.net	weakdistance.com
catbrushcable.com	getpoints.net	mylovelypet.net	robotscan.net	weather4free.com
catfoodstorage.net	getspeednows.com	mymanagement-service.com	rockbreakdown.com	weatherapi.co
catsndogsproducts.com	gettingchances.com	mymensaje-sms.com	rockmusic4u.com	web-check.co
cdnupdateweb.com	gettingurl.com	mymobile-cell.com	rockstarpony.com	web-config.org
cdnwa.com	gherboshop.com	mynewbesttime.com	rosegoldjewerly.com	web-developper.net
celebrateyourdaynow.com	girlimstill.com	mypostservice.online	rosesforus.com	web-domain.net
cell-abonnes.com	girlsyoulike.com	mysadaga.com	rotaryimports.com	web-hoster.co
cell-mcel.info	glassesofwine.com	myseesea.com	rss-me.com	web-loading.com
cellphone-inside.org	glasstaken.com	myself-dns.com	russian4u.net	web-loading.net
cellphonesprices.com	glittercases.net	myshoesforever.com	sabafon.info	web-only.net
cellular-updates.com	global-redirect.net	myshop4u.net	safe-mondays.net	web-page.co

cellular-updates.online	globalcoverage.co	mystulchik.com	safecrusade.com	web-scanner.co
cellularupdates.info	globalnews247.net	mysuperheadphones.co	saladsaroundme.com	web-spider.net
centersession.com	globalsupporteam.com	myukadventures.com	sale-2019.com	web-url.net
centrasia-news.com	go-trip.online	mywebbargains.com	saltyapplepie.com	web-viewer.online
cerfcube.com	golf-news.live	mz-vodacom.info	same-old.net	webadv.co
changesstarted.net	good-games.org	nation-news.com	savemoretime.co	webexaminer.net
chatresponses.com	goodcookingonline.com	nation24.info	savephotos.net	webpageupdate.co
cheapapartmentsaroundme.com	goodflowersinside.com	nationalleagues.net	saveurday.net	webprotector.co
cheapcardonline.com	goodthoughts4u.com	natural-ice.com	scannerservices.net	webprotocol.net
cheaphostingtoday.com	googleplay-store.com	navywalls.com	scaryaudience.com	webresourcer.com
cheapmotelz.net	goroskop.co	nbrowser.org	scriptincluded.com	websconnector.co
cheapsolutions4u.com	gossipsbollywoods.com	nerdtvfan.com	scriptsinstallers.com	websiteconnecting.com
cheaptransporting.net	gostatspro.com	net-protector.com	seacoastkaraoke.com	websiteeco.com
check-my-internetspeed.com	greatcitymore.com	netstatistics.net	searchjustdont.net	websitereconnecting.com
checkboxcart.com	greenbusnoise.com	nettprofile.com	searchunit.net	websites4yourhost.com
checkboxfee.com	greensmallcanvas.com	netvisualizer.com	sec-checker.com	websitetosubmit.com
checkinonlinehere.com	greenwatermovement.com	netweb-cloud-services.com	secretgirlfriend.net	webstrings.net
chickenwaves.com	grevejeunesmedecins.com	network-bots.com	secure-access10.mx	websupporter.co
chistedeldia.mx	growstart.net	network190.com	secured-url.net	webtunnels.net
chocolateicecreamlovers.com	guardnotes.com	networkinfo.org	securedloading.com	webupdater.net
chocollife.me	gulf-financials.com	networkingloading.com	securedlogin.org	webview-redirect.com
chormnet3.com	gulf-news.info	networkingproperty.com	securesmsing.com	wedding-strategy.com
chretiendaujoudhui.com	gulfca.net	neutralpages.com	secureyourad.com	weddingbandsoft.com
chubaka.org	gumclockberry.com	neverwayneck.com	securisurf.com	welcomehosting.net
classic-furnitures.com	hairdresseraroundme.com	newandfresh.com	securlaw.com	welovebigcakes.com
classstylemap.com	halal-place.com	newandroidapps.net	select-edition.net	welovelollipops.com
cleanmiddle.com	handcraftedformat.com	newarrivals.club	send2url.com	welovemorningcoffees.com
clickrighthere.online	handcreamforyou.com	newcooking.org	sendhtml.net	wewantflowersnow.com
clicktrack247.com	handymanwood.com	newdailycoupons.com	sendingurl.com	whatcanidowithbirds.com

clients-access.com	happiness4us.com	newenvelope.net	sendingurl.net	whats-new.org
clockmarkcoffee.com	hardthinmetal.com	newip-info.com	sergek.info	whatsapp-app.com
closefly.com	hatsampledc.com	newipconfig.com	seriousprotection.net	whatsappsupport.net
cloudads.net	hdsoccerstream.com	newmodel.online	service-update.online	whereismybonus.com
cloudbiggest.com	health-club.online	newnhotapps.com	services-sync.com	whereismyhand.com
clubloading.net	healthyguess.com	newredirect.net	servingshade.com	whereismytree.net
clubmovistar.com	healthykids-food.com	news-alert.org	severalheroes.com	whereisthehat.com
clubsforus.net	hearsmugglergarden.com	news-flash.net	sexxclip.com	whynotyesterday.com
cnic-ferify.live	heavy-flood.com	news-gazette.info	sharepassageset.com	whypillyellow.com
cnic-update.com	hellomydaddy.com	news-news.co	shia-voice.com	willpurpleshe.com
cnn-africa.co	hellomymommy.com	newscurrent.info	shipment-status.org	windyone.net
coffecups.online	henrietta-commerce.com	newsdirect.online	shoppingdailydeals.net	winfoxflip.com
coffee2go.org	highclassdining.net	newsofficial.info	short-address.com	winter-balance.com
colorfulnotebooks.com	hillsaround.com	newsofgames.com	shortfb.com	wintertimes.co
colorsoflife.online	hitrafficip.com	newsofthemoment.net	shortredirect.com	wishdownget.com
columbus-parking.com	hmizat.co	newsportal24.online	shtraf.info	without-additional.com
com-reports.net	holdingspider.com	newtarrifs.net	shuturl.com	witness-delay.com
cominfo-urbano.com	holdmydoor.com	newworld-news.com	siamha.info	wonderfulinsights.com
companybreakfast.net	holdstory.com	nicevibezaction.net	signpetition.co	woodhome4u.com
computer-set.com	holecatorange.com	nightevents.info	silverodgone.com	wordstore.net
conditionalcell.com	holiday-sun.net	nightscloudwant.com	simplycode.co	working-online.net
conference-ballroom.com	holiday4u.work	nnews.co	site-lock.net	workshopmanager.net
confusedmachine.com	homeishere.co	noextramoney.com	site-redirecting.com	wraptext.net
connecting-to.com	homemadecandies.net	noloveforyou.com	skillsforest.net	xchange4u.net
contacting-customer.com	hona-alrabe3.com	nomorewarnow.com	smallperfumerain.com	xchangerates247.net
content-blocking.net	horsefingercoffee.com	noodlegray.com	smallridebar.com	xn--nissn-3jc.com
contentsbycase.com	host-one-more.com	noonstore.sale	smarttarfi.com	xn--noki-t5b.com
convertedversion.com	host-redirect.net	noor-alhedaya.com	smokeshowshoe.com	xn--telegrm-qbd.com
cookiescom.com	hot-motors.com	normal-brain.com	smoothurl.com	xtremelivesupport.com

cookiesoutthere.com	hotels-review.org	normal-strength.com	sms-center.info	y0utube.com.mx
cool-smartphone-apps.com	hotelsauto.co	normalseason.com	sms-sending.net	youaresostupid.net
coolasiankitchen.com	hotelstax.co	northridgebest.com	sms-zone.org	youcantpass.com
coolbbqtools.net	hotelsurvey.info	nosalternatives.com	sms.webadv.co	youintelligence.com
coolmath4us.net	hothdwallpaperz.com	nosemorningnine.com	smscentro.com	youliehow.com
cornclean.com	hotinfosource.com	nothernkivu.com	smser.net	yourbestclothes.com
cottondecay.com	housesfurniture.com	noti-global.com	smsmensaje.mx	yourbestefforts.com
countrytrips.net	housing-update.com	noti-hot.com	snoweverywhere.com	yourbestvaca.com
coupedumondepro.com	howisurday.com	noti-hoy.co	so-this-is.com	yourgreatestsmartphone.com
couponshops.info	howtoexplorebirds.com	noticiaspoliticos.com	soccerstreamingstars.com	yourhotelreservation.info
cozmo-store.net	howtomakeavocadotoastandegg.com	notificationsneeded.com	social-artist.net	yourlastchance.net
cpr-appointments.com	hracingtips.com	notisms.net	social-exercise.com	yousunhard.com
crashparadox.net	htmlmetrics.com	notresante-infos.com	social-life.info	yummyfoodallover.com
crimebackfire.com	htmlstats.net	nouveau-president.com	social-rights.com	zednewszm.com
crosslocated.net	httpaccess.com	nouvelles247.com	sockstubename.com	zm-banks.com
crowndecoration.net	humandiven.com	noveletters.com	solo-hoy.com	zm-weather.com
crownsafe.net	humblebenefit.com	novoicenoprob.net	somewarmremember.com	zsports-info.com

Table 15 - Hashes related to Pegasus activity
316fac5ae2d4e250b1c0f10b4388fa2c6c3407b118e539a7d865613e373628d9
9fae5d148b89001555132c896879652fe1ca633d35271db34622248e048c78ae
ade8bef0ac29fa363fc9afd958af0074478aef650adeb0318517b48bd996d5d5
bd8cda80aaee3e4a17e9967a1c062ac5c8e4aefd7eaa3362f54044c2c94db52a
fa538fc20af8aa198db5e932b2afaf9710633a49cf3e19b7465175520e3e8b47

Table 16 - Emails related to Pegasus activity
ameliehaggart@gmail.com
arvidamelia1@gmail.com
bakkere268@gmail.com
bekkerfredi@gmail.com
benjiburns8@gmail.com
bergers.o79@gmail.com

bogaardlisa803@gmail.com
emmadavies8266@gmail.com
emmaholm575@gmail.com
filip.bl82@gmail.com
herbruud2@gmail.com
jessicadavies1345@outlook.com
kleinleon1987@gmail.com
krystynajasinska86@gmail.com
k.williams.enny74@gmail.com
lee.85.holland@gmail.com
linakeller2203@gmail.com
martin.vdm78@gmail.com
meliastahl@gmail.com
mitchkremer14@outlook.com
naomiwerff772@gmail.com
oskarschalcher@outlook.com
smithsonrobert080@gmail.com
sylianosliatsos84@gmail.com
taylorjade0303@gmail.com
vincent.dahl76@gmail.com
weertlaura1@outlook.com
yvonne.wechsler61@gmail.com
natalymarinova@proton.me

Table 17 - Processes related to Pegasus activity
ABSCarryLog
accountpfd
actmanaged
aggregatenotd
appccntd
bfrgbd
bh
bluetoothfs
boardframed
brstaged
brfstagingd
bundpwrd
cfprefssd
ckeblld
ckkeyrollfd
com.apple.Mappit.SnapshotService
com.apple.rapports.events
CommsCenterRootHelper
comnetd

comsercvd
confinstalld
contextstoremgrd
corecomnetd
ctrlfs
dhcp4d
Diagnostic-2543
Diagnosticd
Diagnostics-2543
eventfssd
eventsfssd
eventstorpd
faskeepd
fdlibframed
fmld
frtipd
fservernetd
gatekeeperd
GoldenGate
gssdp
JarvisPluginMgr
jlmvskrd
launchafd
launchrexd
libbmanaged
libtouchregd
llmdwatchd
lobbrogd
locserviced
logseld
misbrigd
mobileargd
MobileSMSd
mptbd
msgacntd
natgd
neagentd
nehelprd
netservcomd
otpgrefd
passsd
payload
pcsd
PDPDialogs
pstid
ReminderIntentsUIExtension

rlaccountd
roleaboutd
roleaccountd
rolexd
seraccountd
setframed
smmsgingd
stagegrad
stagingd
vm_stats
keybrd
xpccfd
fnotifyd
tisppd
updaterd
wifip2ppd

edolio5.com Domain Hosting History - HosterStats.com

Old Hoster	New Hoster	Month / Year	Zone Date	Transaction
ABOVEDOMAINS.COM	N/A	September 2023	2023-10-01	Deleted
ABOVE.COM	ABOVEDOMAINS.COM	May 2023	2023-06-01	Transfer
N/A	ABOVE.COM	August 2022	2022-09-01	New
REGISTRAR-SERVERS.COM	N/A	April 2022	2022-05-01	Deleted
N/A	REGISTRAR-SERVERS.COM	March 2021	2021-04-01	New

Figure 19 - Example of domain provider history

ViewDNS.info

Tools | API | Research | Data

ViewDNS.info > Tools > **IP History**

Shows a historical list of IP addresses a given domain name has been hosted on as well as where that IP address is geographically located, and the owner of that IP address.

Domain (e.g. *domain.com*):
GO

IP history results for edolio5.com.

IP Address	Location	IP Address Owner	Last seen on this IP
103.224.182.242	Australia	Trellian Pty. Limited	2023-09-21
70.32.1.32	Ashburn - United States	ASN-GIGENET	2023-06-19
199.115.116.43	Manassas - United States	LEASEWEB-USA-WDC	2023-06-16
103.224.182.242	Australia	Trellian Pty. Limited	2023-06-14
70.32.1.32	Ashburn - United States	ASN-GIGENET	2023-06-11
199.115.116.43	Manassas - United States	LEASEWEB-USA-WDC	2023-06-10
70.32.1.32	Ashburn - United States	ASN-GIGENET	2023-06-09
199.115.116.43	Manassas - United States	LEASEWEB-USA-WDC	2023-06-08
103.224.182.242	Australia	Trellian Pty. Limited	2023-06-07
70.32.1.32	Ashburn - United States	ASN-GIGENET	2023-04-18
170.178.168.203	Los Angeles - United States	SHARKTECH	2023-04-17
103.224.182.242	Australia	Trellian Pty. Limited	2023-04-06
199.115.116.43	Manassas - United States	LEASEWEB-USA-WDC	2022-10-06
103.224.182.242	Australia	Trellian Pty. Limited	2022-09-29

Figure 20 - Example of domain's IP address history

zougla.gr.com	Public	2 years		0 B	1	1	0	
viva.gr.com	Public	2 years		0 B	1	1	0	
suzuki.gr.com	Public	2 years		0 B	1	1	0	
sepenet.gr.com	Public	2 years		0 B	1	1	0	
tiny.gr.com/	Public	2 years		59 KB	2	2	2	
pronews.gr.com	Public	2 years		0 B	1	1	0	
onlineservices.gr.com	Public	2 years		0 B	1	1	0	
nissan.gr.com	Public	2 years		0 B	1	1	0	
newsbeast.gr.com	Public	2 years		0 B	1	1	0	
kranos.gr.com	Public	2 years		0 B	1	1	0	
fimes.gr.com	Public	2 years		0 B	1	1	0	
ferrari.gr.com	Public	2 years		0 B	1	1	0	
espressonews.gr.com	Public	2 years		0 B	1	1	0	
bmw.gr.com	Public	2 years		0 B	1	1	0	
adservices.gr.com	Public	2 years		0 B	1	1	0	
zougla.gr.com	Public	2 years		0 B	1	1	0	
viva.gr.com	Public	2 years		0 B	1	1	0	
suzuki.gr.com	Public	2 years		0 B	1	1	0	
sepenet.gr.com	Public	2 years		0 B	1	1	0	
tiny.gr.com/	Public	2 years		59 KB	2	2	2	
pronews.gr.com	Public	2 years		0 B	1	1	0	
onlineservices.gr.com	Public	2 years		0 B	1	1	0	
nissan.gr.com	Public	2 years		0 B	1	1	0	
newsbeast.gr.com	Public	2 years		0 B	1	1	0	
kranos.gr.com	Public	2 years		0 B	1	1	0	
fimes.gr.com	Public	2 years		0 B	1	1	0	
ferrari.gr.com	Public	2 years		0 B	1	1	0	
espressonews.gr.com	Public	2 years		0 B	1	1	0	
bmw.gr.com	Public	2 years		0 B	1	1	0	
adservices.gr.com	Public	2 years		0 B	1	1	0	

Figure 21 - Found scans of gr.com subdomains.

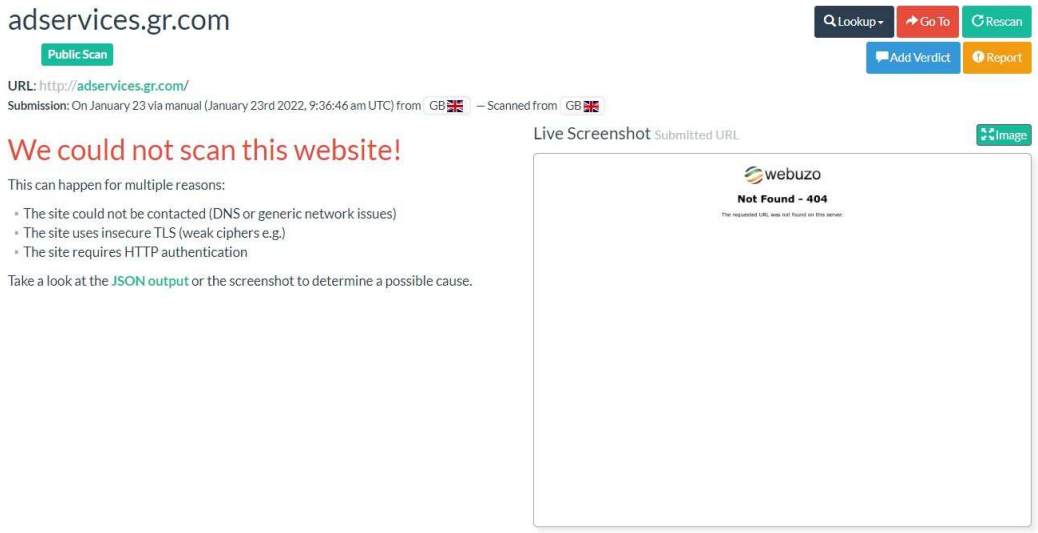


Figure 23 - First example of performed manual scan

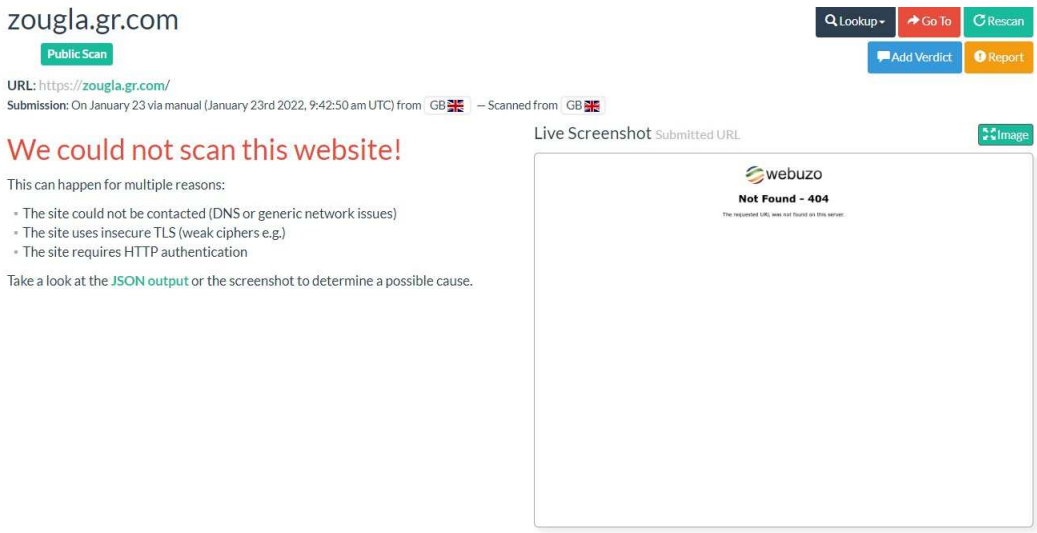


Figure 22 - Second example of performed manual scan.

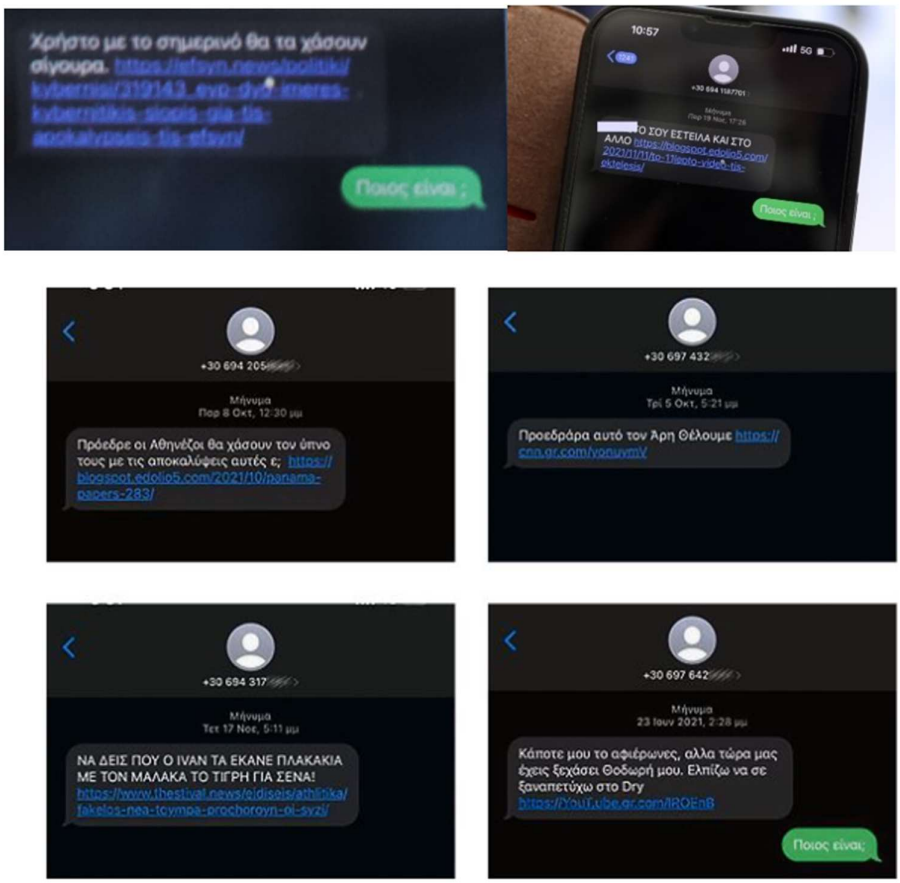


Figure 24 - Predator sent SMS on targeted Greek iPhone users

[83][84][85][86][87][88]

4. Anti-Forensics

Anti-forensics, commonly referred to as counter-forensics, is a set of strategies and methods used to obstruct or weaken digital forensic investigations. The practice of collecting, preserving, analyzing, and presenting digital evidence in a legal setting, often for the purpose of investigating cybercrime or other digital wrongdoing, is known as digital forensics. Anti-forensics, on the other hand, seeks to make gathering evidence or recovering data from a system or device difficult or impossible.

4.1. Usage

Anti-forensics refers to a set of strategies and practices used to undermine or dodge digital forensic examinations, most commonly in computer and cybercrime. These techniques are intended to remove, modify, or hide digital evidence, making it difficult for forensic analysts to identify and attribute criminal activity. Data wiping, encryption, file hiding, steganography, and the use of anonymity networks like Tor are all common anti-forensic techniques. Anti-forensics can be used by cybercriminals, hackers, and anyone looking to hide their tracks, but it can also be used as a lawful tool for privacy and protection by whistleblowers or activists under oppressive regimes. Balancing the requirement for investigative accountability with individual privacy rights is a difficult task, as anti-forensics can impede the pursuit of justice while safeguarding individuals from harm. One well-known application of anti-forensics is in privacy and security measures used by individuals and businesses to protect their digital conversations and data. When used to anonymize internet traffic and disguise a user's IP address, Virtual Private Networks (VPNs) are a type of anti-forensics. Encrypted messaging apps like Signal and encrypted email services can also be viewed as anti-forensic tools because they guarantee communication secrecy and make it difficult for other parties to obtain message content. While these tools are largely employed for legitimate privacy and security concerns, they share some concepts with anti-forensic strategies designed to hinder digital investigations. [89][90] [91]

Implications on forensic investigations

Entropy cannot be utilized as a countermeasure since encryption was used. However, pattern recognition can be achieved by statistical analysis if the encryption layer is disabled. This is a prototype implementation. When creating a workable solution, there shouldn't be any installation files, execution traces, or other evidence that an anti-forensic tool was used. For example, if one doesn't think to work around this, running the Python program may show up in the history file. Additionally, the language interpreter may leave relevant hints (log files, for example). Forensic investigators should be aware of invalid timestamp states, such as access or modification timestamps that occur prior to the creation time of a file, as well as change and modification timestamps that occur mere nanoseconds after the creation time. It is beneficial to verify that the chronological sequence of timestamps makes sense. We eliminated these anomalies in our implementation by appropriately adjusting timestamp values, which are less precise than nanoseconds. Furthermore, data should only be stored in memory by a legitimate anti-forensic instrument; no hard disk shifting allowed. Different timestamps can be used to indicate concealed information if the disk has backups. Further internal file system data structures (such the journal) could also be investigated to see if they are applicable in this situation. In the event that operating system files were utilized as carriers, discrepancies between the tampered creation timestamps and the installation files' chronological sequence can be demonstrated by comparing them using a timeline of the corresponding timestamps. Even while digital data is increasingly used in the investigation

and prosecution of numerous crimes, there is growing worry about the use of procedures and instruments that could compromise the efficacy of any testing techniques intended for this kind of evidence. Certain lawbreakers attempt to conceal their online activities since they are aware of the tactics that the authorities can use. Their procedures, referred to as anti-forensics, usually only come up in the most complicated circumstances. Many times, it seems too costly or time-consuming to conduct an inquiry using such countermeasure approaches. Frequently, a case may be dropped, leaving investigators feeling personally defeated. Though the extent to which such techniques are used is still unknown, the digital forensic community will naturally be concerned about any course of action that hinders an efficient investigation of a criminal crime. Perhaps because of using these procedures, there is still little media coverage of so-called anti-forensic techniques in the field of digital forensics; effective anti-forensic tactics might never be discovered to cause the potential concern. Furthermore, there is a dearth of empirical research that provides evidence regarding the existing perceptions and usage of so-called anti-forensic tools, as well as an evaluation of the degree to which the public and criminal use privacy-enhancing tools for anti-forensic reasons. Even while there may be little evidence to raise concerns, this should not be an excuse for ignoring the harm posed by programs and techniques meant to thwart a digital forensics inquiry. According to the broader field of forensic science, criminals frequently use "tools" to obtain a mechanical edge in a variety of illegal operations. It may not be acceptable to fail to find and retrieve impression evidence. This will obstruct a thorough forensic investigation and undoubtedly skew the interpretation of what actually happened. As a result, forensic science has written a great deal on the recovery, dependability, and identification of physical toolmarks. Comparable research, however, is scarce. The necessity for Digital Forensics to dedicate resources to the additional analysis and assessment of the risks posed by methods that impede workflow. The possibility exists that practitioners who come across such processes during an investigation may not completely comprehend the effects they have had on a device that is being investigated, which is why there is a need for more research in the anti-forensic field.[92][93]

There are three possible effects of poorly studied anti-forensic procedures:

- Neglecting to identify the presence of anti-forensic processes on a system could hinder a thorough examination of the device being investigated locally and, more importantly, external sources of data. Tools that exclude questionable content from the Internet, for instance, could lead a practitioner to believe that no illegal behavior has occurred. Thus, to determine the full scope of a criminal act, it may never be possible to request and question more sources of external evidence, such as saved Internet Service Provider (ISP) logs or other external service data.

- Inadequate anti-forensic practices might result in lost forensic opportunities because tools and processes can leave behind traces on a system that explain the tasks they may have completed and provide clues as to what data has been altered.

- Insufficiently investigated anti-forensic protocols create an obstacle to ascertaining the actual potential and efficacy of these attributes, so averting any constraints and vulnerabilities from being tapped into for the aim of obtaining evidence.

For simplification of arguments, those tools designed for AF purposes can be typically placed in one of the following six classifications.

Table 18 – Anti-Forensics techniques	
Data hiding	Techniques for hiding data are intended to conceal digital stuff from an individual's view. Given the forensic capabilities available to many analysts, data concealing might be the least effective anti-forensic tactic available to a potential criminal. For instance, a typical desktop computer generally allows users complete physical access to the operating system and digital material. Using straightforward methods like changing the file name and extension or putting content in unusual system locations can also be effective ways to hide data. In these situations, the effectiveness of data hiding tactics depends on the weakness of the investigating practitioner and their propensity to miss material or to process this data without applying the appropriate safeguards to ensure that content is not lost.
Data removal	The goal of data removal techniques is to obscure information that is stored on digital media from Digital Forensics' ability to retrieve it. Standard file deletion does not automatically do this; however, data removal entails the timely and deliberate removal.
Data obfuscation	Within the context of digital forensics, the term "obfuscation" refers to a broad range of methods and algorithms that are used to conceal data, rendering it unreadable until certain access protocols are begun. To decrypt data, this can just require providing the right authentication credentials. The capacity to reverse obfuscation techniques to guarantee that data can be retrieved by the right person is what sets them apart from removal techniques. The purpose of obfuscation techniques is to restrict content access to individuals who have been preselected.
Data manipulation /editing /masking	These techniques modify an existing system using meaningful data that a practitioner could use to accurately explain a collection of events. The accuracy of the event reconstruction is purposefully impaired if alterations are found. Inaccurate test results

	could be obtained if these procedures go unnoticed.
Data adding	When it comes to AF tools, the goal is frequently to erase any evidence of a user's implicating activities from their system. But certain instruments could try to present evidence that incriminates a person.
Physical destruction	Traditional AF methods, like as physical destruction, depend on a device reaching a point of destruction beyond the capabilities of specialized digital device recovery. These methods might work well in situations involving local device storage, but as more and more data is kept remotely by service providers, physical destruction might not always be a reliable anti-forensic method.

Disruptive technologies

Although disruptive technologies serve a legitimate primary purpose, they may also negatively affect any later investigation's ability to access pertinent digital data stored on a device. Using a disk defragging tool, which minimizes file defragmentation to increase system drive efficiency, is one example of such a problem. Although this feature is non-AF, using it may affect the recoverability of data stored on a drive in unallocated areas. Consequently, any such instrument or procedure is considered a disruptive technology that has anti-forensic applications. The tool itself is not AF, but it can be utilized in an AF manner if it can determine a suspect's necessary purpose. This brings up a problem in the context of a Digital Forensics investigation, which is how to tell the difference between a malicious and normal process. Disruptive technology use presents two challenges for Digital Forensics investigations:

- Identifying the use of disruptive technologies in a specific instance, given that their purpose is lawful system activity, which can occasionally be hard to discern from normal user behaviour.
- Identifying the use of disruptive technologies with the purpose to be AF and differentiating them from uses such as legitimate privacy or performance enhancements.

While the latter task of proving deliberate disruptive technology usage is arguably unachievable in many situations, the former may be achievable. When a suspect uses disruptive technology, it might be difficult to tell the difference between intentional attempts to erase potential behaviours that could document criminal activity from their system and legitimate system maintenance or PET usage. Such activities are probably impossible to differentiate, and attempting to do so runs the risk of undermining the responsible user. These behaviours draw attention to the challenges of defining AF in Digital Forensics. Because of this, it might not always be able to determine motive. However, in any case, identifying disruptive technology use might aid in explaining the lack of evidence or determining the validity of a certain piece of information on a particular system. Although certain AF tools are problematic, many users' everyday device usage exposes them to disruptive technologies that are used by watchful users. These technologies are thought to represent a greater concern. The problem with this explanation is that it makes the assumption that device passcodes, as well as any subsequent encryption and wiping, are AF. Although they can be utilized in an AF method, this is not the case. One could argue that one example of a

disruptive technology is the iPhone. On an iPhone device, password protection, encryption, and wiping are intended to improve privacy and safeguard personal data. Apple has indicated that these features are legitimately implemented in many cases, including when a device is sold later, and all personal content is deleted. Apple does not market any of these procedures with the intention of causing AF.[94][95]

Kinds of anti-forensics

- Destroying the proof, it entails destroying evidence to render it useless for use in the course of the investigation. Even if it is frequently fatal to remove evidence, it is important to note that the actions or instruments used to do so can leave behind evidence in the form of usage traces.
- Keeping evidence hidden methods used to undermine the analyst instead of a particular forensic analysis application in order to lessen or even completely eliminate the visibility of the evidence during the forensics study. The effectiveness of this method is related to the limitations of the individuals using it or, if any, the forensics equipment that was employed. Regarding the last point, the existence of any concealing implements may produce proof.
- Removing sources of evidence, it is the neutralization of the sources of evidence; this method focuses on preventing the development of evidence rather than its elimination.
- Falsifying proof to sabotage the forensic investigation, a phony version of the evidence is created and carefully designed to contain inaccurate or erroneous facts.[96]

Mobile anti-forensics

Because they retain so much personal data, mobile devices have become even more crucial in the field of forensics in recent years. Nevertheless, traditional forensic protocols and instruments frequently do not apply to mobile devices. The lack of direct access to such devices' internal memory is likely the biggest obstacle to overcome. Indeed, the internal memory volume cannot be detached from the device and subjected to an easy analysis, unlike the removable storage volumes (such as SIM cards and memory cards). As with any other commercial forensic tool, there are a number of well used commercial tools and suites available for use in such scenarios. The challenge is in delving into the tool's behaviour. Moreover, the internal memory appears to be a prime option for applying particular AF techniques because the volume is inaccessible.

Broad methods with an emphasis on Android devices

- Exploiting android features: With the introduction of the Sandbox execution paradigm, the robust Linux processes and users' management policies that underpin Android have been strengthened and fortified. Every application, each representing a distinct user, operates by default in a solitary secure region. Moreover, file permissions management guarantees the security of the application's files. In this case, the OS ensures and enforces the protection of any files or directories that a particular application request.
- A private folder: A specific program can build a directory in the appropriate storage volume that is unavailable to any other applications, thanks to the basic security capabilities of Android. This type of directory, sometimes known as a private directory, is generated during installation, and is deleted along with all of its contents when the corresponding application is uninstalled. It can be used to store any type of information, including text files and multimedia. It is simple to understand how these types of folders might be used to conduct various AF tactics; for example, the folder may include all the compromising data that the device's end user has specifically specified. While the automatic destruction of the folder contents upon uninstalling assures that the data is theoretically wiped, the folder's inaccessibility to other apps guarantees the safety of the stored data. The classified data will obviously be found if the volume containing the private folder is isolated and all physically stored data is obtained; however, if the private folder is created in the device's internal memory, both the isolation and the physical imaging are currently difficult tasks. Furthermore, any sensitive information moved to the private folder is essentially rendered invisible to the end-user and the default applications on the device, making it difficult to perform a cursory review of the device regardless of the amount of storage volume used. Furthermore, any type of compromising data can be transferred via the secret folder without the need for easily investigated detachable volumes. Lastly, it is important to note that the data kept in the private folder are not required to be encrypted; by doing this, certain cryptography-related problems are avoided in favour of a type of steganography that is guaranteed by the device's operating system.
- Anti-forensics by a common application: The AF techniques that rely on the private folder concept are explained in the following sections. These techniques have been successfully constructed and assessed on both a real device and a device emulator. It is important to note that a common Android application that can be downloaded and used on the device has adopted all the following strategies. For example, specific applications can create a private folder at execution time that allows finally the evidence export and import. The evidence destruction can also be a part of the application offered procedures. [97][98][99]

4.2. Techniques

- Data Deletion: The act of permanently removing or overwriting data in order to render it unrecoverable. This may entail the use of specialist software to delete files or the use of secure deletion procedures.

- Data Encryption: The process of encrypting sensitive data so that it is illegible without the encryption key. If the investigators are unable to obtain the key, the data stays protected. The simple solution to prevent data from being readily revealed is to encrypt it. Additionally, encryption shields the stored data from illegal access. Cybercriminals utilize encryption to impede investigations and data extraction. Therefore, decrypting lengthy keys that encrypt fake data would be a complete waste of time and resources. If there is no access key, encryption creates a barrier to prevent files from being accessed by employing an encryption algorithm. Nonetheless, the encrypted files' structure makes it easier to identify these harmful methods. Mobile forensics must be included into the legal and justice systems due to the rising use of smartphones in illegal activity and the use of mobile device evidence by legal professionals. anti-forensic apps for smartphones and shown their efficacy against two paid forensic tools.

- Data Hiding: The concealment of data within other files or regions of a system in order to make it more difficult to identify or recover. Steganography and encryption are primarily employed to obscure criminals' trails and conceal any evidence, thus complicating forensics investigations. This covers data encryption, disk encryption, data concealment in network traffic, and even data encoding within memory.

- Disk wiping: The process of overwriting the whole storage medium to ensure that no previous data can be restored. studied the "IconCache.db" file's characteristics to demonstrate its usefulness and the behavior of anti-forensics by introducing several methods. Traditionally, digital forensics have looked through storage devices for evidence. Commercial counter-forensic technologies, on the other hand, provide a challenge to digital forensics since they eliminate evidence from forensic investigations. Prefetch files, registry keys, installation folders, and other files are among the fingerprints of wiping tools. A collection of anti-forensic tools to determine their existence, their use, and the likelihood of recovering the evidence in relation to commercial products that erase data from disk drives.

- Anti-Memory Forensics: Techniques that change or obscure the contents of volatile memory (RAM) in order to obstruct investigation.

- Counterfeit Data: Using false or misleading information to divert or confuse investigators. A collection of anti-forensics obscures possible evidence of intrusions once a system is compromised. This type of anti-forensics has been found in a number of digital forensics topics, including mobile, hard drive, and memory forensics. One type of data contraceptive technology is a rootkit, which stops any evidence from being generated on the disk. Rootkits not only conceal the attacker's harmful code from operating systems and detection technologies, but they also allow malicious software to go undiscovered. Furthermore, by altering function pointers in the kernel's memory space, rootkits enable the execution of malicious routines. A mobile application can conceal evidence by abusing a security feature, and it can even conceptually erase data from the file system after being uninstalled.

- Rootkit Installation: Malicious software (rootkits) that can mask the presence of additional malicious software or change system behavior to escape discovery.

- Anonymous Communication: Using techniques such as Tor or VPNs to obscure the source of network communication, making it more difficult to track.

- Encrypting Disks: Various tools have been created to encrypt the entire volume of the hard drive. Disk encryption is therefore used by cybercriminals to safeguard any data that could be used against them as proof. This can be accomplished by transforming it into an unsupported format or an unintelligible, non-comprehensible form. making it challenging to interpret for digital forensics specialists. Furthermore, disk encryption depends on hardware and/or software encryption to encrypt all data on the hard disk.

- Encrypting Databases: Database encryption emerged as another widely used method of data hiding as a result of the ongoing growth in database usage. This encryption also targets the files and folders used by single users and many users. The foundation of database encryption is the transformation of data—including emails, apps, mobile devices, and cloud services—into a meaningless cipher text.

- Hardware Memory Encryption: The advancement of this kind of memory encryption makes it easier for criminals to evade typical memory access hierarchies. This will make it impossible for any known memory acquisition method to work.

- Steganography: Steganography is a tool used by cybercriminals to conceal data in digital multimedia components. Text, audio, video, and image files are some of these components. System files are included in this as well. Steganalysis techniques and attacks can be used to lessen the impact of steganography.

- Data Contraception: It is actually categorized as an anti-forensics action because it leaves little to no digital evidence that can be traced back to prevent its recovery. Data manipulation is actually capable of manipulating in-use hard drives and file systems by disguising any content on a particular system or network.

- Zero-Foot printing: Disk cleaner is a recently developed anti-forensics program that may be used to clear specific disk regions or erase all the original data on the drive. Consequently, the attack remains undetected. Because zero-foot printing can unlink files and replace them with nonsense data, it can be used for both legal and illegal purposes.
- Timestamp Modification: Establishing a forensics chain of events inquiry is necessary for the crucial work of timestamp extraction. But, to deceive investigators, hackers and cybercriminals were able to alter the timestamps on files and records.

- File Signature Manipulation: Every file has a file signature at the start to identify the sort of file it is. Typically, hackers may intentionally alter and corrupt a file signature using anti-forensics tools to deceive forensics investigators.

- Hiding Network: The attackers also exploited networks to conceal data. The goal of data concealing in networks is to make sure that the attackers leave no evidence behind. As a result, the forensics investigation is severely hampered, particularly when VPNs, proxies, or TOR are used.

- Artifact Wiping: The process of artifact wiping involves erasing important information that might be used as evidence. Numerous software solutions that can be used to remove several types of data and metadata have been discovered through the examination of artifact wiping. Files, drives, audits, logs, and registers are all included in this. A variety of technologies were created by fusing distinct data wiping formats. Although the

rewritten data will be permanently erased, this class of approaches has two drawbacks. The first is that it might overlook certain data, and the second is that it might leave behind evidence of previous wiping—most notably, the wiping tool itself. The focus of a significant amount of the current literature on Android anti-forensics is artifact wiping. A method for cleaning a phone by eliminating files that have been removed. Their method involves overwriting the entire internal memory, booting a customized recovery image, moving all the contents to an external drive, and then copying the files back. The recovery image is a stripped-down operating system image that can be installed on a rooted phone and was initially meant to be used for a full phone reset. This process has the drawback of being an offline process that takes a lot of time and human labour, but it will ensure that any data that was previously erased will now be permanently lost. Two ways have been employed to start the wipe: one is reading the system logs, and the other is looking for a USB connection. The drawback of reading system logs is that it is slow since action cannot be taken until the event that generated, wrote, and finally read back in the log message has occurred. Particularly with older Android versions, there is a lack of specificity when it comes to USB connection detection.

- Trail obfuscation: is a planned action intended to confuse and distract a forensics investigation. It is predicated on the same ideas as fake data injection, or steganography. Peer-to-peer protocols are used via trail obfuscation to conduct cybercrimes. This aids in the mitigation of cybercriminals' cyberbiometric fingerprints, enabling them to conceal evidence and evade detection. In the field of obfuscation, an automation system was created that may be used to simulate a user's presence on the phone, giving the impression that the user was there at the location where the phone was at a specific moment. They outline a number of solutions based on widely accessible software automation and testing technologies before creating their own system that records and replays user interactions. They use a USB debug connection to record events when the phone is connected to a computer. Playback can be done on the phone using a script file that has been uploaded from the PC, or from the recording PC. Tests reveal that this system can be used to send and receive SMS texts as well as publish messages to Facebook. Following the message transmission, forensic examinations were conducted, but the phone's automated system was not conclusively detected. The phone needed to be rooted for their system to function, and a general-purpose scheduling program needed to be installed for it to function without a PC. The researchers imply—but do not explicitly say—that the uploaded script is not a substantial trace because it is so remarkably simple. There were no traces at all because the controlling PC was running a Linux live CD exclusively in RAM.

- Virtual System Execution: Without leaving any trace on the device, malicious code or scripts can be led to execute remotely or from external disk storage. Additionally, other virtualization techniques, such as network and USB boot devices.

- Content Compression: The goal of content compression or saturation is to contaminate systems with erratic content. Delays and increased latency result from this, and the forensics investigation process is severely harmed. There are two types of content compression: standard compression, which takes advantage of regular compression implementations, and compression bombs, sometimes known as zip bombs, which are intended to expand significantly once decompressed.

- Data Pooling: Attackers want to maintain the activity of their digital media, such as USB keys, CDs and DVDs, smartphones, laptops, PCs, and hard drives, by employing data pooling. Investigators are enticed to sift through all the data gathered in this way. Because of this, conducting a search of this kind may take months or even years, and it may infringe upon the privacy of the victim or suspect, leading to legal issues. Consequently, this results in increased expenses and extended duration of the study.

- Loop References: are recognized as default file path lengths; because of the Windows API on NTFS, they are limited to 260 characters. Still, there are a number of ways to start lengthier journeys. The method that is most often used is LPT-based. There are other methods as well, such as using loop references, which allow symbolic links to point to a parent folder. As a result, a recursive path is created, allowing unscrupulous people to store their data in these layered recursive folders safely.

- Dummy Hard Disk: Using this technique, hackers and cybercriminals store an inoperable PC on its hard drive. This makes it possible to boot the computer without utilizing the hard drive by using a USB that contains the operating system. Data will thus be kept on cloud services. Hackers may also attempt to mimic random writes on disks to mislead investigators into believing that a particular disk has been used recently. As a result, time and resources would be wasted in doing this.

- Anti-Forensics Malware: They were also utilized to carry out an anti-forensics operation by erasing any pertinent information that is necessary proof to identify its origin, composition, and features.

- Attacks against processes and tools: Computer forensic analysts are expected to adhere to public guidelines established by central authorities in their procedures. Therefore, creating anti-forensic tools to target these processes is pertinent. One instance would be securing data so that only one software with a password could access it. In this situation, the analyst has the option of either rooting the phone and obtaining the data while breaking some rules, such not changing the data on the device, or following protocol and not acquiring the data. Because smartphones are intricate, integrated devices, the study frequently requires the usage of the complete original system. Comparatively speaking, personal computers are made up of separate parts that are connected by common interfaces and may be disassembled piece by piece, circumventing some security. Because of this, compared to PCs, the published standards allow for far more intrusive testing on mobile devices. Nevertheless, a lot of these inquiries are time-consuming, particular to phone models, necessitate specialized testing, and may call for lengthy justifications in court settings.

- iOS anti-forensic technique: Using case studies with iPhones Apple created a sophisticated, hierarchical scheme with multiple security layers linked to protect data on iOS devices. Typically, distinct encryption keys are used to safeguard distinct data blocks within the user partition. The metadata, file system structure, and special files (catalog, attributes, journal, etc.) are safeguarded by the data partition file system key, also known as the EMF key. To access the file system payload, you need to have the specific files. When a jailbreak is tethered, it implies that the device cannot restart in a jailbroken condition without being connected to the desktop. Since no permanent changes are performed to the OS or user data partition, tethered jailbreaking is acceptable for digital forensic practitioners and is only meant to be used temporarily. Conversely, an untethered jailbreak indicates that the status of being jailbroken is irreversible. integrated via characteristics, user files, and folders. Using the AES CBC mode, each file on the data partition is encrypted by the specialized AES cryptographic engine using a different 256-bit key. Each per-file key is saved in the file's metadata and wrapped with the key linked to the data protection class to which the file belongs.[100][101][102] [103][104][105][106] [107][108]

4.3. Examples

Timestamps
An attacker may be interested in **changing the timestamps of files** to avoid being detected. It's possible to find the timestamps inside the MFT in attributes $STANDARD_INFORMATION __ and __ $FILE_NAME. Both attributes have 4 timestamps: **Modification**, **access**, **creation**, and **MFT registry modification** (MACE or MACB).

$LogFile
- CTIME: File's creation time
- ATIME: File's modification time
- MTIME: File's MFT registry modification
- RTIME: File's access time

$STANDARD_INFORMATION and $FILE_NAME

Nanoseconds
NTFS timestamps have a **precision** of **100 nanoseconds**. Attackers
can modify both attributes $STARNDAR_INFORMATION and $FILE_NAME.

Data Hiding
NFTS uses a cluster and the minimum information size. That means that if a file occupies uses and cluster and a half, the **reminding half is never going to be used** until the file is deleted. Then, it's possible to **hide data in this slack space**.

Live Linux Distributions
These distros are **executed inside the RAM** memory. The only way to detect them is **in case the NTFS filesystem is mounted with write permissions**. If it's mounted just with read permissions, it won't be possible to detect the intrusion.

Windows Configuration
It's possible to disable several windows logging methods to make the forensics investigation much harder.

Disable Timestamps - UserAssist
This is a registry key that maintains dates and hours when each executable was run by the user. Disabling UserAssist requires two steps:

1. Set two registry keys, HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Start_TrackProgs and HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Start_TrackEnabled, both to zero in order to signal that we want UserAssist disabled.
2. Clear your registry subtrees that look like HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\<hash>.

Disable Timestamps - Prefetch
This will save information about the applications executed with the goal of improving the performance of the Windows system. However, this can also be useful for forensics practices.

- Execute regedit
- Select the file path HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\Memory Management\PrefetchParameters
- Right-click on both EnablePrefetcher and EnableSuperfetch
- Select Modify on each of these to change the value from 1 (or 3) to 0.
- Restart

Disable Timestamps - Last Access Time
Whenever a folder is opened from an NTFS volume on a Windows NT server, the system takes the time to update a timestamp field on each listed folder, called the last access time. On a heavily used NTFS volume, this can affect performance.

1. Execute regedit
2. Browse to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem.
3. Look for NtfsDisableLastAccessUpdate. If it doesn't exist, add this DWORD and set its value to 1, which will disable the process.
4. Close the Registry Editor and reboot the server.

Delete USB History
All the **USB Device Entries** are stored in Windows Registry Under the "USBSTOR" registry key that contains sub keys which are created whenever you plug a USB Device into your PC or Laptop. Key can be found here
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR.
Deleting this you will delete the USB history.
Another file that saves information about the USBs is the file setupapi.dev.log inside C:\Windows\INF. This should also be deleted.

Disable Shadow Copies
List shadow copies with vssadmin list shadowstorage.
Delete them via running vssadmin delete shadow.
To disable shadow copies:

1. Execute services.
2. From the list, find "Volume Shadow Copy", select it, and then access Properties by right-clicking.
3. Choose Disabled from the "Startup type" drop-down menu, and then confirm the change by clicking Apply and OK.

It's also possible to modify the configuration of which files are going to be copied in the shadow copy in the registry
HKLM\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot

Overwrite deleted files

- Windows tool: cipher /w:C This will indicate cipher to remove any data from the available unused disk space inside the C drive.

Delete Windows event logs

- Execute eventvwr.msc
- Right click each category and select "Clear Log"
- for /F "tokens=*" %1 in ('wevtutil.exe el') DO wevtutil.exe cl "%1"
- Get-EventLog -LogName * | ForEach { Clear-EventLog $_.Log }

Disable Windows event logs

- reg add 'HKLM\SYSTEM\CurrentControlSet\Services\eventlog' /v Start /t REG_DWORD /d 4 /f
- Disable the service "Windows Event Log"
- WEvtUtil.exec clear-log or WEvtUtil.exe cl

Disable $UsnJrnl

- fsutil usn deletejournal /d c:

[109]

In the realm of software protection and anti-reverse engineering, code packers are indispensable instruments that serve as a vital barrier against illegal access and manipulation of executable files. Code packing is the process of obfuscating or compressing executable files to increase their resistance to deciphering and analysis. This method uses a variety of cutting-edge strategies, including virtualization, encryption, and anti-debugging techniques, to mask the original code and obstruct reverse engineering attempts. The capacity of code packers to establish virtual machines, in which the actual code executes on such machines instead of the host, is one of their most notable features. For reverse engineers, this makes tracking down and examining the code flow more difficult. Furthermore, to make it harder for attackers to decode the original code, code packers frequently encrypt both the executable and runtime data using strong encryption methods. Code packers may come under fire for possible antivirus software compatibility problems and false positives, even if they are very effective. Even with greater difficulty, determined attackers might still manage to get past these defenses. In conclusion, code packers are essential for safeguarding software in the present day since they provide an effective barrier against illegal access and reverse engineering. To maintain the security and integrity of their software products, developers and security experts must strike a careful balance between providing strong protection and preserving compatibility as technology advances.[110]

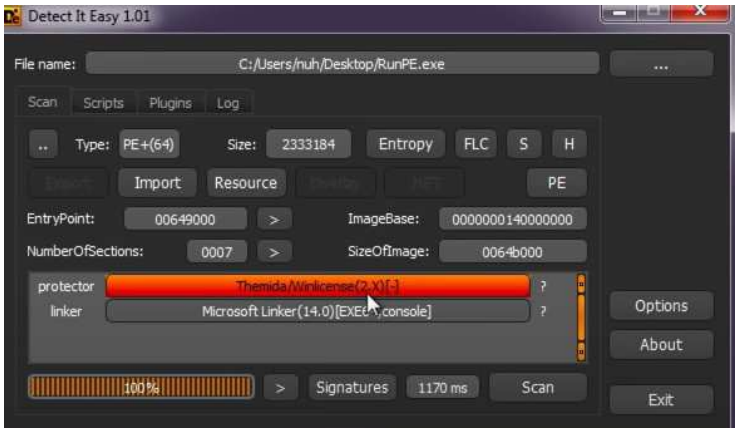


Figure 25 - Example of code packing detection.

Secure Deletion:

- shred command: Overwrite files with random data to make data recovery more challenging.
- srm command: Securely remove files, overwriting with patterns to prevent recovery.

Temporary and Volatile Storage:

- Store sensitive data in volatile memory (RAM) rather than on disk.
- Use tmpfs for temporary storage to ensure data is not persisted on disk.

ELK

- Inject processes
- Zero the header but program still runs

Sensors

Disable file system journaling

- Mount the volume without journaling capabilities

Journal file copy

- Analyze HFS+ volume header and journal_info_block to identify journal file and extract it

Data manipulation

- Concealment: get file contents without being detected or the action being logged
- Deletion: delete file contents without being detected or the action being logged
- Insertion: alter file contents without being detected or the action being logged

Clean up

- Remove traces that could lead to evidence which can lead to undo the anti-iOS forensics

Obfuscation[111]

```c
#include <stdio.h>

int main() {
    printf("Hello, World!\n");
    return 0;
}
```

Figure 26 - Code section before obfuscation.

```c
#include <stdio.h>

#define _ 0
#define __ 1
#define ___ 2
#define _0 3
#define _1 4
#define _2 5
#define _3 6
#define _4 7
#define _5 8
#define _6 9
#define _7 10
#define _8 11
#define _9 12
#define ____ 13

int main() {
    int ______ = _ + __ + ___ + _0;
    int _______ = _1 + _2 + _3 + _4 + _5 + _6;

    char _____[] = {
        'H' - _1, 'e' - __, 'l' - __, 'l' - __, 'o' - __,
        ',' - __, ' ' - __, 'W' - _2, 'o' - __, 'r' - __,
        'l' - __, 'd' - __, '!' - __, '\n' - __, '\0' - ____
    };

    for (int ________ = _; ________ < _______ - _1; ________++) {
        putchar(_____ + ________);
    }

    return _;
}
```

Figure 27 - First example of obfuscated code.

```c
#include <stdio.h>

#define _ 0
#define __ 1
#define ___ 2
#define ____ 3

int main() {
    char _[] = "\x48\x65\x6C\x6C\x6F\x2C\x20\x57\x6F\x72\x6C\x64\x21\x0A\x00";
    for (int __ = _; _[__] != ____; ++__) {
        putchar(_[__]);
    }
    return _;
}
```

Figure 28 - Second example of obfuscated code.

4.3. Anti anti-forensics

While anti-forensic techniques can be employed for lawful privacy and security purposes, they are frequently associated with illegal acts such as cybercrime, hacking, and data theft. When using these techniques, legal and ethical considerations come into play, as their usage is banned in many places and can have catastrophic consequences.

Digital forensic professionals are constantly evolving their ways to fight anti-forensic measures, creating a cat-and-mouse game between investigators and those attempting to disguise their digital trails.

- Data Recovery and Carving: Developing advanced data recovery and carving techniques to reconstruct and restore deleted or hidden data even when anti-forensic measures are present.
- Advanced Decryption: Accessing encrypted data using cutting-edge decryption methods such as brute force attacks, cryptanalysis, or exploiting weaknesses in encryption software.
- Implementing stringent chain of custody protocols to ensure the integrity of evidence and keeping a written record of who accessed the evidence and when.
- Best Practices for Evidence Preservation: Developing and adhering to best practices for evidence preservation to safeguard evidence against tampering or degradation.
- Malware Analysis: Using advanced malware analysis and reverse engineering techniques to understand and combat anti-forensic measures deployed by malware writers in the case of cyberattacks.
- Memory Forensics is the study of volatile memory (RAM) to recover data that may not be present in traditional storage, such as encryption keys or passwords.
- Legislative and Policy Changes: Advocating for legislative and policy changes that necessitate the retention of specific data or make anti-forensic measures illegal.

The conflict between anti-forensics and anti-anti-forensics is continuing and changing, with each side attempting to outwit the other. Even in the face of more sophisticated anti-forensic strategies used by hackers and other threat actors, digital forensic investigators strive to adapt and develop new tools and methods for recovering and analyzing data.[112][113]

The classification, identification, characterization, and distinction between digital forensics and anti-forensics tools and procedures are all included in the categorization of anti-anti-digital forensics.

Anti-Forensics Detection Techniques

A recently developed system called Anti-Anti-Forensics defends forensics from any attempt to undermine it. In order to guarantee a high detection rate of any anti-forensics activity or attack, it is crucial to maintain the appropriate anti-forensics countermeasures. The data on a machine may be encrypted, according to the file installation for cryptographic software, which could result in an anti-digital forensics incident. As a result, the hash data set was compared to NIST hashes; any discrepancies in the hashes could indicate the presence of anti-forensics files or software. This suggested that anti-digital forensics techniques might be used to completely hide all traces by erasing any evidence that is not recoverable. The suggested remedy is based on techniques for detecting anti-forensics already in use. The methods that are now in place that a forensics investigator could utilize to stop the malevolent yet persistent use of rootkits while also determining the potential anti-forensics uses that a rootkit could have. An improved protected forensics version is required to reduce the usage of anti-forensics operations. Therefore, the direction of change is towards an improved version of Anti-Anti-Forensics. to identify and notify digital investigators of any instances of the employment of anti-digital forensics tools. To defeat an anti-forensics attack, this strengthened and improved the digital forensics inquiry. The method showed that the recovery of the correct data with the required evidence was made possible by an incomplete wiping of unallocated space. a forensics tool that can both capture inaccessible forensics information and extract and analyse forensics data to enable the detection of anti-forensics attempts. This improved the digital forensics investigation and helped restore a system. Machine learning emerged as a novel early smart detection technique to sort out the shortcomings of earlier forensics and counter-forensics methods, notwithstanding the difficulties and restrictions that forensics domains face. To identify any anti-forensics activity, a new machine-learning counter anti-forensics-based branch was created. The significance of integrating and using AI/ML methods in the field of cybersecurity. maintaining the confidentiality and integrity of the information infrastructure through the application of artificial intelligence algorithms for offline intrusion analysis.[114]

Anti-forensics countermeasures

- Use of Multiple Tools: Utilize a variety of forensic tools and techniques to cross-verify findings and increase the chances of discovering hidden or obfuscated data.
- Timeline Analysis: Employ timeline analysis to reconstruct the sequence of events and identify any anomalies or inconsistencies.
- Hashing and Integrity Checks: Use cryptographic hashing to verify the integrity of acquired data, ensuring that it has not been tampered with during the investigation.
- Steganalysis: Employ steganalysis techniques to detect hidden information within files, images, or other media.
- User and Behavioral Analysis: Analyze user behavior patterns to identify any unusual or suspicious activities that may indicate attempts to cover tracks. [115][116]

Conclusion

A spyware is still a malware that exploits unknown vulnerabilities of digital devices to gain access to information of particular interest. Through this thesis, the action of such software can be seen which uses illegitimate techniques to influence digital devices and enforce the continuous operation of the software's internal processes. Analysts can identify vulnerabilities that malicious users have exploited to gain access and intercept data in a variety of ways, such as text messages, emails or even sending data to third-party applications. Although the creators of spyware use techniques to hide the source code, sometimes traces and evidence are captured that are not expected but indicate a strange interaction of the digital device with the internet or with the appropriate system functions. The network communication is carried out with specific addresses of web space providers or cloud computing services to conceal the real identity of the moral and physical perpetrators. The Internet is a space without beginning and end, but many elements such as IP addresses, software hashes as signatures, domains and common software processes limit the final search for the suspected perpetrators of the crime. Analysts are asked to link all the available data - which in many cases is already freely available online - and determine the final course of action. Obstacles are an integral part of the research process which, as mentioned above, are either placed by the malicious users or arise during. This piece of research has little material available which means that it could be studied to an even greater extent.

References

[1] Chapter 1 • An Overview of Spyware, http://www.syngress.com/
[2] A Holistic Approach for Managing Spyware, Xin Luo
[3] Spyware, Ms. Sakshi Sanklecha, Mr. Darshit Deotale, Ms. Jyoti Yadav, Ms. Dipti Mishra , Prof V.P. Yadav
[5] Spying on Spyware, C Matthew Curtin
[6] Spyware: What Influences College Students to Use Anti-Spyware Tools?, Michael R. Ward, D. Scott Hunsinger
[7] Rootkits, Spyware/Adware, Keyloggers and Backdoors: Detection and Neutralization, Oleg Zaytsev
[8] Spyware, https://csrc.nist.gov/glossary/term/spyware
[9] Spyware and Adware: How Do Internet Users Defend Themselves?, Rajendran Sriramachandramurthy, Siva K. Balasubramanian, Monica Alexandra Hodis
[10] Viruses, Hardware and Software Trojans, Anatoly Belous, Vitali Saladukha
[11] What Do Consumers Really Know About Spyware?, Xiaoni Zhang
[12] No Privacy Among Spies: Assessing the Functionality and Insecurity of Consumer Android Spyware Apps, Enze Liu, Sumanth Rao, Sam Havron, Grant Ho, Stefan Savage, Geoffrey M. Voelker, Damon McCoy
[13] Pegasus Spyware – "A Privacy Killer", Ajay Chawla
[14] A Data-driven Characterization of Modern Android Spyware, FABIO PIERAZZI, GHITA MEZZOUR, QIAN HAN, MICHELE COLAJANNI, V. S. SUBRAHMANIAN
[15] Techniques of Adware and Spyware, Eric Chien
[16] Differences and Similarities of Spyware and Adware, Chris Gutzman, Seth Sweep, Asong Tambo
[17] A Spyware Detection System with a Comparative Study of Spywares using Classification Rule Mining, Satya Narayan Tripathy, Sisira Kumar Kapat, Susanta Kumar Das and Binayak Panda
[18] СУЧАСНІ ТРЕНДИ ВИЯВЛЕННЯ ТА ПРОТИДІЇ ЗАСТОСУВАННЮ ШПИГУНСЬКИХ ТА ШКІДЛИВИХ ПРОГРАМ, ПОЛЯКОВ О.М.
[19] https://www.techtarget.com/whatis/definition/Top-10-Spyware-Threats
[20] https://www.macworld.com/article/672879/list-of-mac-viruses-malware-and-security-flaws.html
[21] https://www.scaler.com/topics/linux-malware/
[22] https://www.linkedin.com/pulse/best-spy-apps-android-without-access-target-phone-diana-moraa
[23] https://www.forbes.com/sites/kateoflahertyuk/2023/09/29/iphone-spyware-attacks-what-you-need-to-know/
[24] More Malware – Adware, Spyware, Spam and Spim. Australian Institute of Criminology
[25] Techniques of Adware and Spyware, Chien, E
[26] Spyware and Adware: How Do Internet Users Defend Themselves? American Journal of Business, Sriramachandramurthy, R., Balasubramanian, S. K., &Hodis
[27] https://github.com/GranittHQ/
[28] Οι 190 στόχοι του Predator στην Ελλάδα – Τα πρόσωπα, η πολιτική αστάθεια και οι θεσμικές πρωτοβουλίες της κυβέρνησης, https://www.parapolitika.gr/
[29] Νέα λίστα Predator: Παρακολουθούσε αρχηγό της ΕΛΑΣ, εισαγγελείς και υπουργούς – Όλα τα ονόματα, https://www.koutipandoras.gr/
[30] CHAMPING AT THE CYBERBIT Ethiopian Dissidents Targeted with New Commercial Spyware, Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert

[31] ARCHIBALD REISS DAYS, UNIVERSITY OF CRIMINAL INVESTIGATION AND POLICE STUDIES
[32] Investigating Factors Affecting the Adoption of Anti-Spyware Systems, Younghwa Lee and Kenneth A. Kozar
[33] On the lawfulness of the EncroChat and Sky ECC-operations, New Journal of European Criminal Law 2023
[34] Encrochat: Secret network messages can be used in court, judges rule, https://www.bbc.com/
[35] Police crack world's largest cryptophone network as criminals swap EncroChat for Sky ECC, https://www.techtarget.com/network/
[36] Cracking the covert app that exposed Europe's drug gangs, https://www.euractiv.com/
[37] The Criminals Thought the Devices Were Secure. But the Seller Was the F.B.I., https://www.nytimes.com/
[38] 800 criminals arrested in biggest ever law enforcement operation against encrypted communication, https://www.europol.europa.eu/
[39] FBI used encrypted Anom app in international crime bust, https://www.techtarget.com/network/
[40] https://www.nist.gov/itl/ssd/digital-forensics
[41] Digital Forensics and Cyber Crime, Frank Breitinger Ibrahim Baggili
[42] Fundamentals of Digital Forensics, Joakim Kävrestad
[43] Digital Forensics and Cyber Security, Kevin Mondy
[44] Cloud Forensic Artifacts: Digital Forensics Registry Artifacts discovered from Cloud Storage Application, Mohammed A. Bajahzar and Prof. Shailendra Mishra
[45] Internet Forensics: Legal and Technical Issues Maria Karyda and Lilian Mitrou
[46] Digital Forensics, Investigation, and Response, Chuck Easttom
[47] https://nij.ojp.gov/digital-evidence-and-forensics
[48] DIGITAL FORENSIC EVIDENCE, Marcello L. Busetto, Alberto Camon, Claudia Cesari, Enrico Marzaduri, Daniele Negri
[49] A Framework for Crime Detection and Diminution in Digital Forensics (CD3F), Arpita Singh, Sanjay K. Singh, Nilu Singh, and Sandeep K. Nayak
[50] Advances in Internet, Data and Web Technologies, Leonard Barolli · Fatos Xhafa · Zahoor Ali Khan · Hamad Odhabi
[51] Ambient Intelligence— Software and Applications, Juan F. De Paz, Vicente Julián Gabriel Villarrubia, Goreti Marreiros
[52] Information Security, Pierangela Samarati, Moti Yung, Fabio Martinelli, Claudio A. Ardagna
[53] Proceedings of International Conference on Deep Learning, Computing, and Intelligence, Gunasekaran Manogaran, A. Shanthini, G. Vadivu
[54] Cyber Security and Digital Forensics, Mangesh M. Ghonge, Sabyasachi Pramanik, Ramchandra Mangrulkar and Dac-Nhuong Le
[55] Technical and legal perspectives on forensics scenario, Fabrizio Solinas
[56] Technical Challenges and Directions for Digital Forensics, https://medium.com/@wisemonkeysoffpage/technical-challenges-and-directions-for-digital-forensics-21332e6f7335
[57] https://ieeexplore.ieee.org/document/1592529
[58] Crime Science and Digital Forensics: A Holistic View, Anthony C. Ijeh, Kevin Curran
[59] DIGITAL FORENSICS VS. ANTI-DIGITAL FORENSICS: TECHNIQUES, LIMITATIONS AND RECOMMENDATIONS, Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, and Ali Chehab
[60] Overview of Financial Fraud Digital Forensic Investigation Framework, Pei-Shan Choong, Yusnita Yusof
[61] Curbing cyber-crime and Enhancing e-commerce security with Digital Forensics, Israel D. Fianyi
[62] Technology and Internet Jurisdiction, Reidenberg, J.R.

[63] Consumer motivations in taking action against spyware: an empirical investigation, Anil Gurung, Xin Luo, Qinyu Liao
[64] Security, Privacy, and Digital Forensics in the Cloud, Lei Chen, Hassan Takabi, Nhien-An Le-Khac
[65] Privacy Concerns with Digital Forensics, Neil Rowe
[66] https://faculty.nps.edu/ncrowe/forensicpriv.pdf
[67] https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/view-the-security-event-log
[68] https://superuser.com/questions/847438/location-of-event-logs-in-windows
[69] https://learn.microsoft.com/en-us/shows/inside/event-viewer
[70] https://stackify.com/linux-logs/
[71] https://support.apple.com/guide/console/log-messages-cnsl1012/mac
[72] https://askubuntu.com/questions/186276/where-are-all-the-major-log-files-located
[73] https://linuxsecurity.com/features/linux-log-analysis
[74] https://www.xda-developers.com/how-to-take-logs-android/
[75] https://developer.apple.com/documentation/xcode/acquiring-crash-reports-and-diagnostic-logs
[76] https://support.apple.com/guide/console/locate-a-log-file-cnsl9361/mac
[77] iGen: Toward Automatic Generation and Analysis of Indicators of Compromise (IOCs) using Convolutional Neural Network, Anupam Panwar
[78] Malware Detection and Analysis, Namratha Suraneni
[79] THE PREDATOR FILES: CAUGHT IN THE NET, Amnesty International
[80] Technical Analysis of the NSO Group's Pegasus Spyware, JD Rudie, Zach Katz, Sam Kuhbander, Suman Bhunia
[81] Pegasus for Android Technical Analysis and Findings, Chrysaor
[82] Hooking Candiru Another Mercenary Spyware Vendor Comes into Focus, Bill Marczak, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert
[83] https://github.com/AmnestyTech/investigations
[84] https://www.virustotal.com/gui/collection/452597908679766ab49a60fb22c09cdfd2f86494ab87605369b973ce9f43f64b/iocs
[85] https://virustotal.com/gui/collection/f0daa825f90962fd303687d30fa92776f34d64f46de495b5a78d7723f92691a4/iocs
[86] https://www.virustotal.com/gui/collection/941213a51888c4d4cb97608982b7b29f268812537f56c05ae034ca367117a657/iocs
[87] https://www.hybrid-analysis.com/
[88] https://viewdns.info/
[89] Introduction to Cyberdeception, Neil C. Rowe, Julian Rrushi
[90] Blurring Intelligence CrimeA Critical Forensics, Willem Bart de Lint
[91] Anti-Forensics Techniques: An Analytical Review, Anu Jain, and Gurpal Singh Chhabra
[92] Open Source Intelligence Methods and Tools, Nihad A. Hassan, and Rami Hijazi
[93] Practical Cyber Forensics, Niranjan Reddy
[94] When finding nothing may be evidence of something: Anti-forensics and digital tool marks, Graeme Horsman, David Errickson
[95] Android anti-forensics through a local paradigm, Alessandro Distefano, Gianluigi Me, Francesco Pace
[96] Understanding digital image anti-forensics: an analytical review, Neeti Taneja, Vijendra Singh Bramhe, Dinesh Bhardwaj, Ashu Taneja
[97] A Novel Anti-Forensics Technique for the Android OS, Pietro Albano, Aniello Castiglione, Giuseppe Cattaneo, Alfredo De Santis
[98] Android Forensics and Anti-forensics techniques – A survey, Nemanja D. Macek, Perica Strbac, Dusan Coko, Igor Franc, Mitko Bogdanoski

[99] iOS anti-forensics: How can we securely conceal, delete, and insert data? Christian D'Orazio, Aswami Ariffin, Kim-Kwang Raymond Choo
[100] Wiping techniques and anti-forensics methods, Miroslav Ölvecký, Darja Gabriška
[101] Advanced digital forensics and anti-digital forensics for IoT systems: Techniques, limitations and recommendations, Jean-Paul A. Yaacoub, Hassan N. Noura, Ola Salman, Ali Chehab
[102] A survey and research challenges of anti-forensics: Evaluation of game-theoretic models in simulation of forensic agents' behaviour, Saeed Shafiee Hasanabadi , Arash Habibi Lashkari, Ali A. Ghorbani
[103] Anti-Forensics, LOCKHEED MARTIN
[104] Anti-Forensics: A Practitioner Perspective, Richard de Beer, Adrie Stander, and Jean-Paul Van Belle
[105] Detection and Mitigation of Anti-Forensics, Emre Caglar Hosgor
[106] A Survey on Anti-Forensics Techniques, Murat Gül, Emin Kugu
[107] IMPACT OF ANTI-FORENSICS TECHNIQUES ON DIGITAL FORENSICS INVESTIGATION, Tambue Ramine Etow
[108] iOS anti-forensics: How can we securely conceal, delete, and insert data? Christian D'Orazio, Aswami Ariffin, Kim-Kwang Raymond Choo
[109] https://book.hacktricks.xyz/generic-methodologies-and-resources/basic-forensic-methodology/anti-forensic-techniques
[110] https://www.linkedin.com/advice/3/what-best-tools-resources-learning-code-packing
[111] https://www.crowdstrike.com/cybersecurity-101/data-obfuscation/
[112] https://infocon.org/cons/DEF%20CON/DEF%20CON%2020/DEF%20CON%2020%20presentations/DEF%20CON%2020%20-%20Perklin-AntiForensics.pdf
[113] https://www.linkedin.com/pulse/combatting-anti-forensic-tools-how-law-enforcement-ahead-anil-more
[114] An Incident-Based Approach to Forensic Investigations, Niranjan Reddy
[115] Anti-Forensics: The Next Step in Digital Forensics Tool Testing, Martin Wundram, Felix C. Freiling, Christian Moch
[116] General Countermeasures of Anti-Forensics Categories, Mohammad Rasmi Al-Mousa, Nael A. Sweerky, Ghassan Samara, Mohammed Alghanim, Abla Suleiman Ismail Hussein, Braa Qadoumi