ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΙΡΑΙΩΣ – ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ

Πρόγραμμα Μεταπτυχιακών Σπουδών
«Πληροφορική»

Μεταπτυχιακή Διατριβή

Τίτλος Διατριβής	**Λογισμικό Ανίχνευσης Εισβολής (ΛΑΕ) κατά των επιθέσεων Crypto - Ransomware** **Crypto - Ransomware Detection Software (CRDS)**
Ον/μο Φοιτητή	**Τσατταλιός Άρης – Σταύρος**
Πατρώνυμο	**Νικόλαος**
Αριθμός Μητρώου	**ΜΠΠΛ18065**
Επιβλέπων	**Πατσάκης Κων/νος, Αναπληρωτής Καθηγητής**

Ημερομηνία Παράδοσης: **Δεκέμβριος 2022**

Τριμελής Εξεταστική Επιτροπή

(υπογραφή)	(υπογραφή)	(υπογραφή)
Πατσάκης Κων/νος	**Αλέπης Ευθύμιος**	**Σακκόπουλος Ευάγγελος**
Αναπληρωτής Καθηγητής	Αναπληρωτής Καθηγητής	Αναπληρωτής Καθηγητής

Περιεχόμενα

1. Περίληψη

Στην παρούσα διατριβή παρουσιάζεται ένα Λογισμικό Ανίχνευσης Εισβολής (ΛΑΕ) για Windows λειτουργικό σύστημα, το οποίο παρακολουθεί τις αλλαγές στο σύστημα αρχείων (filesystem monitoring) και ακολούθως ενημερώνει τον χρήστη για τυχόν μόλυνση από επίθεση crypto-ransomware. Το λογισμικό δημιουργήθηκε χρησιμοποιώντας την γλώσσα προγραμματισμού Python (ver. 3.9).

Αρχικά, γίνεται μια εισαγωγή παρουσιάζοντας το πρόβλημα, δηλαδή τις επιθέσεις ransomware και την ραγδαία αύξησή τους παγκοσμίως τα τελευταία χρόνια, που στόχο έχουν οργανισμούς αλλά και ιδιώτες, φαινόμενο που οδήγησε στην ανάγκη δημιουργίας εργαλείων ικανών στην πρόληψη και αντιμετώπιση τέτοιων επιθέσεων. Ακόμα γίνεται αναφορά στις σημαντικότερες επιθέσεις ransomware.

Στην συνέχεια ακολουθεί το θεωρητικό μέρος όπου γίνεται μια ανάλυση του τί ακριβώς είναι το ransomware, τα χαρακτηριστικά του, πως λειτουργεί αλλά και ποια είναι τα διακριτά είδη του.

Στο πρακτικό μέρος, αναλύεται εκτενώς ο τρόπος λειτουργίας του λογισμικού (ΛΑΕ), καθώς και ο κώδικας που χρησιμοποιήθηκε.

Τέλος στα δύο τελευταία κεφάλαια, παρουσιάζονται τα αποτελέσματα των μετρήσεων που πραγματοποιήθηκαν, και ακολούθως εξάγονται συμπεράσματα για την αποτελεσματικότητά του λογισμικού (ΛΑΕ) όσον αφορά την ακρίβεια αλλά και την ταχύτητα εντοπισμού της επίθεσης.

2. Abstract

In this dissertation, we will present our version of a Crypto-Ransomware Detection Software (CRDS), coded in Python (ver. 3.9), for Windows OS. This CRDS monitors the filesystem, specifically the file operations, and alerts user if a crypto-ransomware infection is detected.

Namely, at first, we will examine the ever-growing phenomenon of ransomware attacks worldwide, against organizations and individuals, which led to building software tools capable of spotting and preventing such attacks.

Consequently, in “theory” section, we will analyze ransomware’s characteristics, it’s working mechanism and discrete variants – families, while in “practical” section will analyze our CRDS (working logic & code).

Finally in last two chapters, titled “Results” and “Conclusions”, will measure the precision and speed of alerting during an attack, which will lead us in conclusions regarding the effectiveness of this CRDS, together with some proposals for further optimization.

3. Εισαγωγή

Τα τελευταία χρόνια η αντίληψή μας για τον κόσμο έχει αλλάξει. Για παράδειγμα, ένα σημαντικό κομμάτι της καθημερινότητας μας, το περνάμε μέσα σε έναν «ψηφιακό κόσμο» είτε μέσω των κοινωνικών δικτύων (social networks) είτε μέσω των δικτύων εικονικών κόσμων (virtual world networks). Ταυτόχρονα, η πλειονότητα των εργασιών που εκτελούμε καθημερινά, εμπεριέχει - απαιτεί είτε την χρήση Η/Υ, είτε άλλων «έξυπνων συσκευών» (smartwatches, smart home appliances κλπ.) με δυνατότητα σύνδεσης στο διαδίκτυο (Internet of Things, IoT), φαινόμενο που έρχεται ως απόρροια της εξέλιξης της τεχνολογίας σε τομείς όπως αυτός των ημιαγωγών (semiconductors), των Τηλεπικοινωνιών, της Μηχανικής Μάθησης (Machine Learning), αλλά και ανάδυσης νέων, όπως η Υπολογιστική Νέφους (Cloud Computing).

Επεκτείνοντας τον συλλογισμό αυτό και λαμβάνοντας υπόψιν πως σε αυτό το «Διαδίκτυο των Πραγμάτων» προστίθενται και συσκευές κρίσιμων υποδομών (πχ. Νοσοκομεία, Υπηρεσίες Παροχής Ενέργειας, Υπηρεσίες Ύδρευσης, Εργοστάσια κλπ.) (Liviu 2022) (Fortinet 2022), που παλαιότερα δεν υπήρχε η ανάγκη σύνδεσης τους στο Internet, καταλήγουμε αβίαστα στο συμπέρασμα πως, η προστασία των συσκευών, και κατ' επέκταση των υποδομών αυτών, από κυβερνοεπιθέσεις είναι ζωτικής σημασίας.

3.1. Ransomware: Το πρόβλημα

Η ραγδαία ανάπτυξη του IoT αλλά και η χρήση τεχνολογιών όπως το Blockchain, τα ψηφιακά νομίσματα - κρυπτονομίσματα (cryptocurrencies) αλλά και η ύπαρξη ισχυρών πρωτοκόλλων κρυπτογράφησης, κάποια μάλιστα ειδικά σχεδιασμένα για το IoT (πχ. AES, LWC) (Cryptography 2022), δίνει νέες δυνατότητες στους κυβερνοεγκληματίες και ένα νέο πεδίο δράσης, ώστε μέσω διαφόρων μεθόδων (attacking vectors) να καταφέρουν την απόκτηση πρόσβασης σε δίκτυα συστημάτων (attacking surfaces) ιδιωτών, οργανισμών, κρίσιμων υποδομών, ή του Δημοσίου Τομέα, με απώτερους οικονομικούς, πολιτικούς ή κοινωνικούς σκοπούς (Shacklett 2021).

3.1.1. Ransomware as a Service (RaaS)

Οι επιθέσεις ransomware αποτελούν την δημοφιλέστερη μέθοδο κυβερνοεπίθεσης, κυρίως λόγω του μοντέλου – συστήματος διανομής τους, δηλαδή το "Ransomware as a Service" (RaaS) (Strom 2021). Με βάση το συγκεκριμένο μοντέλο, το οποίο μοιάζει με άλλα μοντέλα υπηρεσιών που συναντάμε στο Cloud Computing (Iaas, PaaS, SaaS), ο ενδιαφερόμενος - επιτιθέμενος νοικιάζει την υπηρεσία (subscription) από τους δημιουργούς, οι οποίοι ως αντάλλαγμα χρεώνουν προμήθεια ως ποσοστό επί των λύτρων.

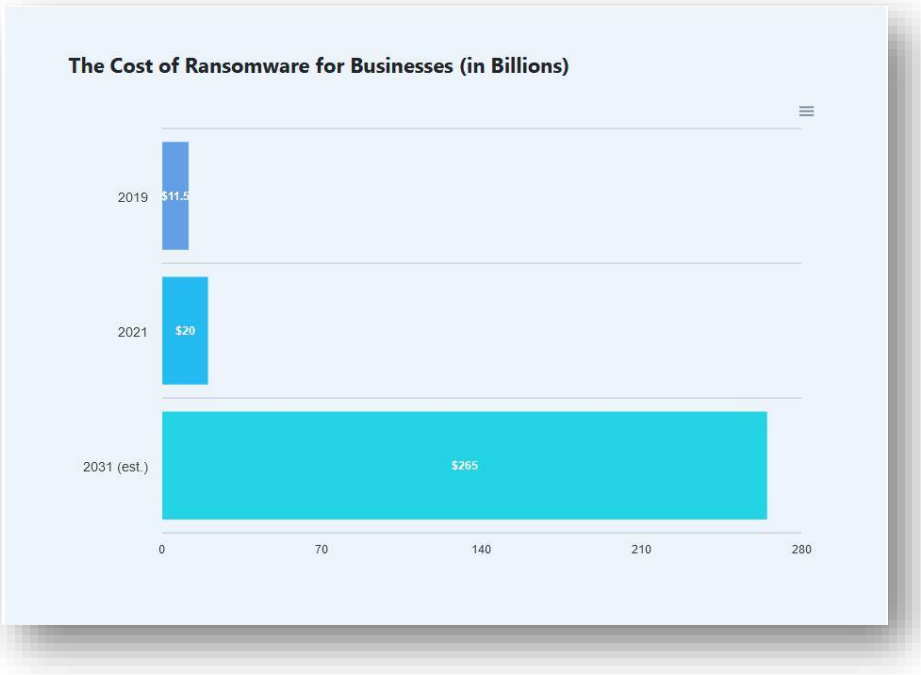
Έτσι, το μοντέλο RaaS παρουσιάζει 2 βασικά πλεονεκτήματα:

- Οι δημιουργοί του ransomware δεν χρειάζεται πια να καταπιάνονται με το να εκτελούν επιθέσεις. Αντ' αυτού λαμβάνουν, συνήθως 10% - 40%, προμήθεια επί των λύτρων.
- Οι επιτιθέμενοι δεν χρειάζεται να κατέχουν τις τεχνικές δεξιότητες για την δημιουργία ενός ransomware. Η "plug and play" ιδιότητα του RaaS μοντέλου, τους επιτρέπει να επικεντρωθούν αποκλειστικά στην, όσο το δυνατόν, μεγαλύτερη αποτελεσματικότητα των επιθέσεων και στην συλλογή των λύτρων. (Belcic 2022)

3.1.2. Στατιστικά Στοιχεία

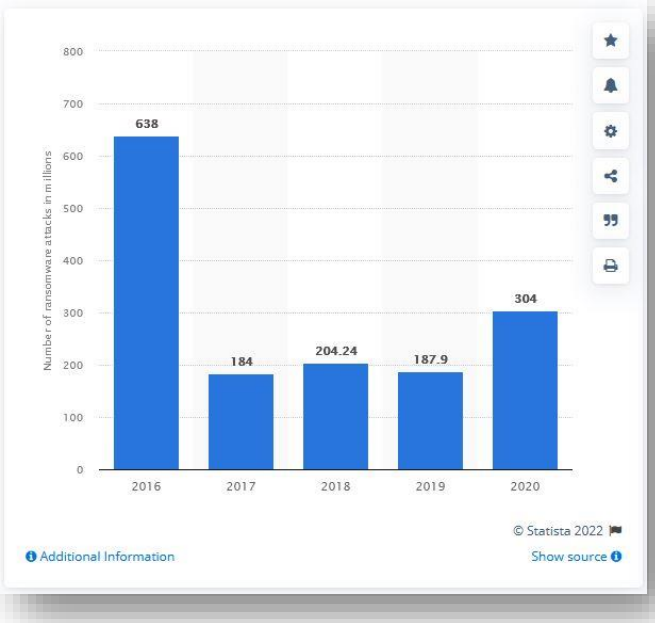
Οι επιθέσεις ransomware παρουσιάζουν δραματική άνοδο τα τελευταία χρόνια ξεκινώντας από το γεμάτο προκλήσεις, από πλευράς πλήθους κυβερνοεπιθέσεων, 2016 (638 εκ.) (Εικόνα 2) και φτάνοντας έως το 2021 όπου ο συνολικός όγκος των επιθέσεων παγκοσμίως έφτασε τα **623,3** εκ. (Sonicwall 2022). Οι συνολικές απώλειες για το 2021 φτάνουν τα **$20 δισ**., και προβλέπεται να φτάσουν τα **$265 δισ.** μέχρι το 2032, αν αυτή (η άνοδος) διατηρηθεί (Εικόνα 1).

Στην 1η θέση των λειτουργικών συστημάτων που μολύνθηκαν περισσότερο από τις επιθέσεις βρίσκονται τα Windows, κυρίως λόγω της δημοφιλίας τους (market share - 80,63 %) (Εικόνα 4), ακολουθούμενο από το Mac OS (12,99 %) (Εικόνα 3).

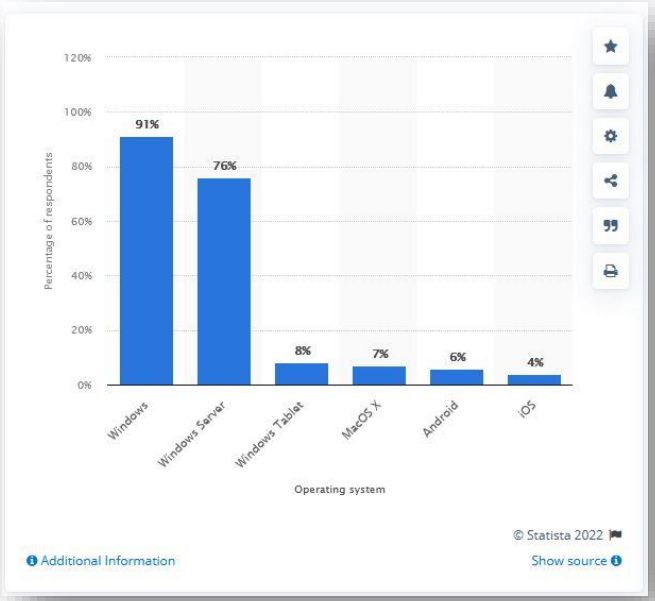


Εικόνα 1: Κόστος των επιθέσεων ransomware για τις Επιχειρήσεις

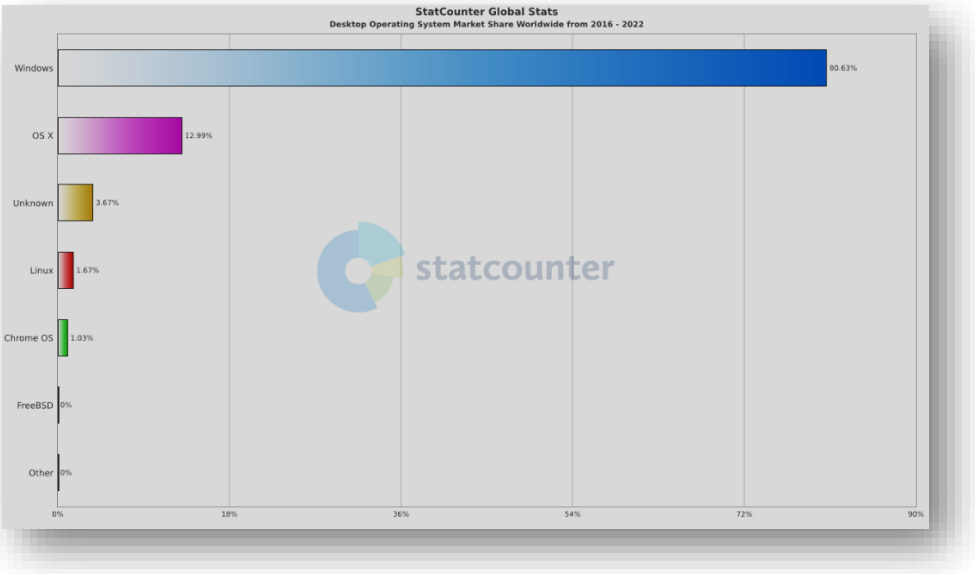
(cloudwards.net)



Εικόνα 2: Πλήθος επιθέσεων ransomware (σε εκ.) παγκοσμίως, ανά χρονιά (statista.com)



Εικόνα 3: Τα Windows στο «στόχαστρο» των επιθέσεων (statista.com)



Εικόνα 4: Windows – Το δημοφιλέστερο Λ.Σ (2016 - 2022)

(statcounter.com)

3.2. Ιστορική Αναδρομή

Η πρώτη γνωστή επίθεση ransomware ήταν αυτή του “AIDS Trojan” (PC Cyborg virus) το 1989, του Joseph Popp. Το συγκεκριμένο malware ουσιαστικά έκρυβε τα αρχεία στον δίσκο, ενώ κρυπτογραφούσε μόνο τα ονόματά τους, βασιζόμενο σε συμμετρική κρυπτογράφηση, το οποίο αργότερα αποδείχτηκε και η αχίλλειος πτέρνα του, από τους Young and Yung το 1996 (wikepidia.org 2021).

Για περισσότερο από μια δεκαετία μετά την επίθεση του “PC Cyborg”, οι επιθέσεις ransomware δεν ήταν τόσο διαδεδομένες, κυρίως λόγω της αδυναμίας ασφαλούς – ανώνυμης συλλογής των λύτρων. Αυτό έμελλε να αλλάξει με την εμφάνιση των κρυπτονομισμάτων, όπως το Bitcoin, το 2010 (Nakamoto 2008), καθώς και της τεχνολογίας του Blockchain (wikipedia 2022) τα οποία προσέφεραν εύκολο και ανώνυμο τρόπο συλλογής των λύτρων (Crowdstrike 2021).

Το 2013 κάνει την εμφάνισή του το “CryptoLocker”, το 1ο νέας γενιάς ransomware, απαιτεί πληρωμή σε Bitcoins, και μέσα σε λίγους μήνες (τέλη του 2013 – μέσα του 2014) καταφέρνει να συγκεντρώσει 27 εκ. δολάρια από 234.000 θύματα παγκοσμίως (Crowdstrike 2021).

Το 2016 θεωρείται η «χρονιά του ransomware» αφού κάνουν την εμφάνισή τους μερικά από τα ransomware που ευθύνονταν για τις μεγαλύτερες επιθέσεις στην ιστορία, όπως τα Locky και Petya[1], τα οποία εξαπλώνονται με ρυθμό περίπου 500.000 phishing[2] emails την

[1] Το “**SamSam”** ήταν ένα ακόμα ransomware που εμφανίστηκε το 2016. Στόχευε κυρίως JBoss (μετέπειτα WildFly) application servers και χρησιμοποιούσε επίθεση brute-force κατά του πρωτοκόλλου RDP, ώστε να μαντέψει αδύναμους κωδικούς. Θύματα της επίθεσης ήταν, μεταξύ άλλων, το υπουργείο μεταφορών του Κολοράντο και η κομητεία Davidson στην Β. Καρολίνα. (Ransomware 2022)

[2] **Phishing,** ό όρος αναφέρεται στην απόπειρα κλοπής ευαίσθητων πληροφοριών (διαπιστευτήρια χρήστη, αριθμό πιστωτικής κάρτας κ.α.) από εγκληματία ο οποίος μιμείται μια αξιόπιστη οντότητα, με σκοπό την χρήση τους σε επίθεση ή την πώλησή τους. (Phishing 2022)

ημέρα[3], συγκεντρώνοντας συνολικά 1 δις. δολάρια σε λύτρα. Και σαν να μην έφταναν αυτά, το μέλλον προβλεπόταν ζοφερό, αφού λίγους μήνες αργότερα, τον Μάιο του 2017 έχουμε την επίθεση του ransomware "WannaCry" (EternalBlue exploit), το οποίο εκμεταλλευόμενο μια ευπάθεια του πρωτοκόλλου SMBv1 (CVE-2017-0144) η οποία επέτρεπε την εκτέλεση κώδικα απομακρυσμένα (RCE attack), είχε ως αποτέλεσμα την μόλυνση 230.000 Η/Υ σε 150 χώρες, μέσα σε μια μέρα, αντίκτυπο σχετικά χαμηλό σε σχέση με άλλες επιθέσεις του ίδιου είδους, το οποίο όμως θα μπορούσε να είναι σημαντικά μεγαλύτερο, αν η επίθεση είχε ως στόχους «εξαιρετικά κρίσιμες υποδομές» όπως πυρηνικά εργοστάσια, σιδηροδρομικά δίκτυα ή φράγματα, με τις οικονομικές απώλειες, σε μια τέτοια περίπτωση, να φτάνουν σύμφωνα με τις εκτιμήσεις έως και τα 4 δις δολάρια. Η επίθεση σταμάτησε από την ανακάλυψη του ερευνητή ασφαλείας Marcus Hutchins, ο οποίος παρατήρησε πως το ransomware ήταν φτιαγμένο ώστε να ελέγχει αν μια διεύθυνση URL «οδηγούσε» σε ενεργή σελίδα. Ο Hutchins κατοχύρωσε το συγκεκριμένο domain, το οποίο ήταν το «σήμα» για το "WannaCry" να σταματήσει να εξαπλώνεται (WannaCry 2022) (The NHS cyber attack 2022). Θύματα του "WannaCry" ήταν το Εθνικό Σύστημα Υγείας της Αγγλίας (NHS), η "Nissan Motor Manufacturing UK", παραρτήματα της αυτοκινητοβιομηχανίας "Renault" καθώς και τα παραρτήματα των "FexEx" και "Deutsche Bahn" στην Ισπανία (wikipedia.org 2022).

Επίσης το 2017 έχουμε την επίθεση του "Not Petya"[4] (EternalBlue & mimikatz exploit) (Arntz 2018) (NotPetya 2022), μια παραλλαγή του "Petya" ransomware, το οποίο αρχικά ξεκίνησε από την Ουκρανία και γρήγορα εξαπλώθηκε σε όλη τη Ευρώπη, στοχεύοντας τράπεζες, αεροδρόμια και εταιρείες ενέργειας, με συνολική οικονομική ζημιά 10 δισ. δολαρίων, μια από τις πιο καταστροφικές επιθέσεις στην ιστορία (Melnyczuk 2021) (NotPetya 2022). Κάποια από τα θύματα της επίθεσης ήταν η Εθνική Τράπεζα της Ουκρανίας (NBU), ο ναυτιλιακός κολοσσός "Maersk Line", η Αμερικανική φαρμακευτική εταιρεία "Merck & Co.", η Γερμανική εταιρεία logistics "DHL",η Ρωσική εταιρεία πετρελαιοειδών "Rosneft", καθώς και το μεγαλύτερο λιμάνι εμπορευματοκιβωτίων της Ινδίας, το JNPT (Εικόνα 5). Τέλος για τις επιθέσεις του "Not Petya" κατηγορήθηκε η ομάδα "Sandworm", η οποία φέρεται να είναι μέλος της Ρωσικής Υπηρεσίας Πληροφοριών (GRU) (Petya and NotPetya 2022).

Το 2019 αποτελεί σημείο καμπής για την εξέλιξη των ransomware, αφού τότε εμφανίζεται για πρώτη φορά το φαινόμενο του «διπλού εκβιασμού» (double extortion)[5], από το "Maze" ransomware. Σύμφωνα με την τακτική αυτή, οι δημιουργοί του ransomware, πριν την κρυπτογράφηση των δεδομένων του θύματος, εξαγάγουν μεγάλο όγκο αυτών, και αργότερα απειλούν πως θα τα δημοσιοποιήσουν. Στην περίπτωση του "Maze", το θύμα ήταν η εταιρεία security "Allied Universal", και τα δεδομένα που κλάπηκαν αποτελούνταν από κυρίως email και πιστοποιητικά ονόματος τομέα (domain name certificates), τα οποία οι δημιουργοί του "Maze", η ομάδα γνωστή ως "TA2101", θα χρησιμοποιούσαν σε μια εκστρατεία phishing παριστάνοντας την "Allied Universal". Προς απόδειξη των προθέσεων τους δημοσιοποίησαν ένα δείγμα των κλεμμένων δεδομένων, που αποτελούνταν από συμβόλαια, ιατρικά αρχεία, πιστοποιητικά κρυπτογράφησης κ.α. (Ransomware Evolved: Double Extortion 2020) . Παρακάτω παρατίθεται ένας πίνακας με τις οικογένειες ransomware που χρησιμοποίησαν την τεχνική του «διπλού εκβιασμού» από τον Νοέμβριο 2019 έως τον Μάρτιο 2021 (Agcaoili, και συν. 2021).

[3] Τον ίδιο δηλαδή αριθμό mails, που στέλνονται σε μια μέση εκστρατεία phishing εν έτη 2020, ολόκληρη την χρονιά.

[4] Το **"Bad Rabbit"** ήταν ένα ακόμα ransomware που έκανε την εμφάνισή του το 2017, χρησιμοποιώντας παρόμοιο μοτίβο – τεχνική επίθεσης με τα WannaCry & Petya. Μάλιστα χρησιμοποιούν και τον ίδιο κώδικα, σε ποσοστό 67%. (Ransomware 2022)

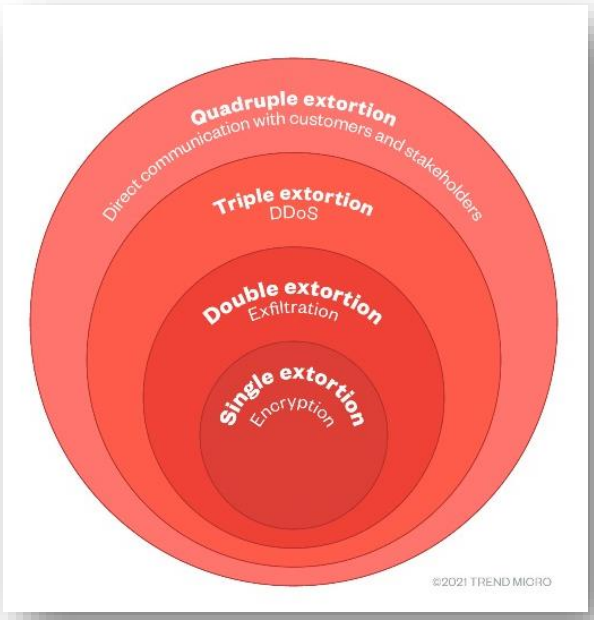
[5] Σε συνέχεια του φαινόμενου του «διπλού εκβιασμού», οι κυβερνοεγκληματίες εφαρμόζουν και «τριπλό» ή «τετραπλό εκβιασμό» (Triple / Quadruple extortion), όπου καταφεύγουν σε επιθέσεις DDoS (triple extortion) ή και απευθύνονται κατευθείαν στους πελάτες ή μετόχους, αυξάνοντας έτσι την πίεση στο θύμα (qadruple extortion).
(Agcaoili, και συν. 2021)

Εικόνα 5: Φορτηγά φορτωμένα με κοντέινερ παρατάσσονται έξω από ένα τερματικό σταθμό στο Jawaharlal Nehru Port Trust στη Βομβάη, Ινδία, Πέμπτη, 29 Ιουνίου 2017. Οι λειτουργίες στον τερματικό σταθμό του πιο πολυσύχναστου λιμανιού εμπορευματοκιβωτίων της Ινδίας έχουν σταματήσει λόγω του κακόβουλου λογισμικού που ξαφνικά εμφανίστηκε την Τρίτη σε οθόνες υπολογιστών σε όλο τον κόσμο, ένα άλλο παράδειγμα της αναστάτωσης που συνεχίζει να γίνεται αισθητή παγκοσμίως. (AP Photo/Rajanish Kakade) (hypr.com)

AgeLocker	CryLock	Hades	NetWalker	REvil/Sodinokibi
Ako/MedusaLocker	DarkSide	LockBit	Pay2Key	Ryuk
AlumniLocker	DoppelPaymer	Maze	ProLock	Sekhmet
Avaddon	Egregor	Mespinoza/Pysa	RagnarLocker	Snatch
Babuk Locker	Ekans	MountLocker/AstroLocker	Ragnarok	SunCrypt
Clop	Everest	Nefilim	RansomExx	Thanos
Conti	Exx/Defray777	Nemty	RanzyLocker/ ThunderX	Xinof

(Trend Micro™ Smart Protection Network™ infrastructure)

Εικόνα 5: Οικογένειες ransomware που χρησιμοποίησαν την τεχνική του «διπλού εκβιασμού» από τον Νοέμβριο 2019 έως τον Μάρτιο 2021.



(trendmicro.com)

Εικόνα 6: Οι 4 φάσεις της τεχνικής του «εκφοβισμού» σε μια επίθεση ransomware (Agcaoili, et al. 2021)

Το 2020 και το 2021 παρατηρείται μια στροφή από ομάδες κυβερνοεγκληματιών προς μεγάλες επιχειρήσεις ή οργανισμούς κρίσιμων υποδομών (Critical Infrastructures), από τους οποίους μπορούν να απαιτήσουν υψηλό ποσό λύτρων. Ένα τέτοιο παράδειγμα αποτελεί η επίθεση στην εταιρεία αγωγών Colonial Pipeline από την ομάδα DarkSide μέσω της RaaS υπηρεσίας τους, ζημιώνοντας τελικά την εταιρεία περίπου 2εκ δολάρια σε κρυπτονομίσματα . Επίσης την ίδια χρονιά έχουμε τις επιθέσεις της (εδρεύουσας επι Ρωσικού εδάφους) ομάδας " REvil" , γνωστή και ως " Sodinokibi", στην Βραζιλιάνικη εταιρεία επεξεργασίας κρέατος "JBS S.A."[6] (JBS S.A. cyberattack 2021), και στο λογισμικό απομακρυσμένης διαχείρισης και εποπτείας "VSA", της Αμερικανικής εταιρείας "Kaseya Limited" (Managed Service Provider). Μάλιστα η τελευταία από τις δυο επιθέσεις ώθησε τον Πρόεδρο των Η.Π.Α Joe Biden, μετά από τηλεφωνική επικοινωνία που είχε με τον Ρώσο ομόλογό του Vladimir Putin να δηλώσει[7] (Ransomware 2022):

"I made it very clear to him that the United States expects when a ransomware operation is coming from his soil even though it's not sponsored by the state, we expect them to act if we give them enough information to act on who that is."

(9 Ιουλίου 2021)

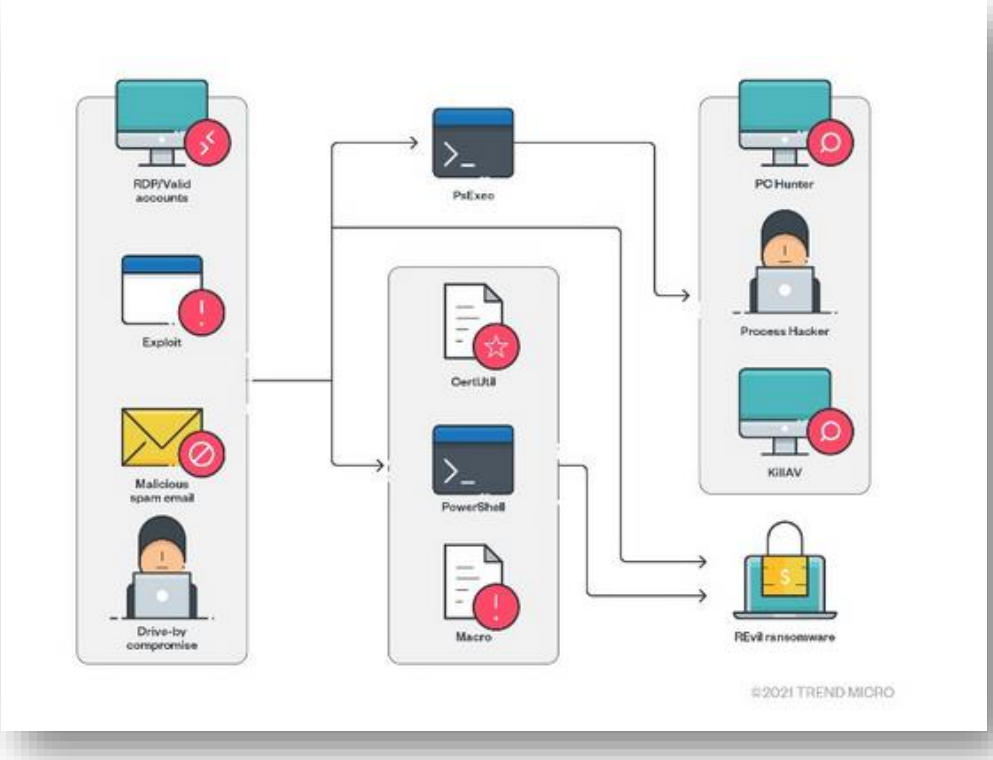
[6] Τον μεγαλύτερο παραγωγό βοδινού, χοιρινού και κοτόπουλου κρέατος, υπεύθυνο για το 1/5 της παγκόσμιας παραγωγής.

7 Τέσσερις ημέρες μετά την δήλωση του Joe Biden, οι ιστοσελίδες της ομάδας "REvil", έπαψαν την λειτουργία τους.

Το “REvil” ransomware συγκαταλέγεται στα λεγόμενα “*Human-operated ransomware”*, δηλαδή εκείνα τα ransomware των οποίων ο χειρισμός γίνεται από τον επιτιθέμενο, και όχι αυτοματοποιημένα. Αυτού του είδους οι επιθέσεις μπορεί να είναι καταστροφικές για τους οργανισμούς, αφού απαιτούν καθολικό αποκλεισμό του επιτιθέμενου από το δίκτυο του οργανισμού, χωρίς να είναι απίθανο το ενδεχόμενο μιας μελλοντικής επίθεσης. (microsoft.com 2022)

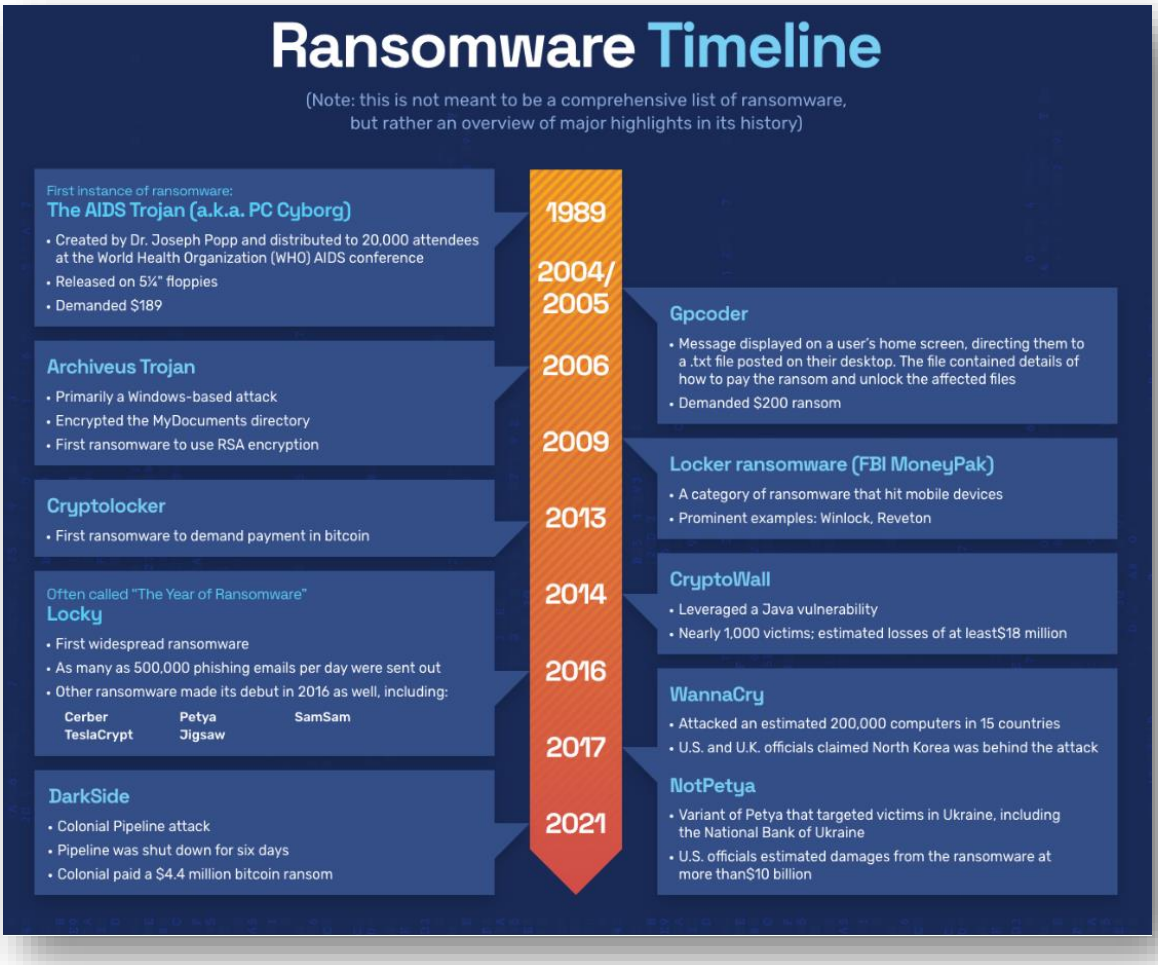
Μια τυπική επίθεση του “ REvil” ransomware, όπως φαίνεται στην παρακάτω εικόνα (Εικόνα 7), χωρίζεται σε 3 διακριτά στάδια:

1. **Αρχική πρόσβαση (initial access)**, μέσω εκμετάλλευση διαφορετικών ευπαθειών πχ. σε πρωτόκολλα απομακρυσμένης πρόσβασης (RDP), Spam emails μέσω της τεχνικής “spear-phishing” ή παραβιασμένες ιστοσελίδες (trendmicro.com n.d.).
2. **Λήψη και εκτέλεση του REvil ransomware (Download and Execution),** μέσω πχ. μακροεντολών από μολυσμένα emails ή εκμετάλλευση ευπαθειών σε διακομιστές (servers) (CVE-2019-2725), τείχη προστασίας (firewalls) ή VPNs (CVE-2018-13379, CVE-2018-13379) (Agcaoili, et al. 2021)
3. **Αποφυγή αναγνώρισης (discovery – defense evasion),** στα πλαίσια των ενεργειών του επιτιθέμενου μετά την είσοδό του στο δίκτυο του οργανισμού (lateral movement) (crowdstrike.com 2022). Αυτές (οι ενέργειες) μπορεί να περιλαμβάνουν πχ. την απενεργοποίηση των λογισμικών Antivirus ή και Antimalware των Η/Υ.



(trendmicro.com)

Εικόνα 7: Σχηματική αναπαράσταση μιας τυπικής επίθεσης του REvil ransomware. (Agcaoili, et al. 2021)



Εικόνα 8: Χρονοδιάγραμμα των επιθέσεων ransomware. (The History of Ransomware 2022)

4. Θεωρητικό Μέρος - Ransomware

4.1. Τι είναι

Αν θέλαμε να δώσουμε έναν ορισμό του τι είναι το ransomware, θα λέγαμε ότι αποτελεί ένα είδος malware (συνθ. mal-icious + soft-ware), δηλαδή ένα λογισμικό σχεδιασμένο να προκαλεί επιτήδεια διακοπή της κανονικής λειτουργίας ενός (ή ολόκληρου δικτύου) Η/Υ, διακομιστών (servers), με σκοπό την διαρροή πληροφοριών, την απόκτηση πρόσβασης στα συστήματα των θυμάτων και εν τέλη την απαίτηση λύτρων, σε αντίθεση με το σφάλμα λογισμικού (software bug) το οποίο οδηγεί σε αντίστοιχο αποτέλεσμα (διακοπή ομαλής λειτουργίας) αλλά προέρχεται συνήθως από ανθρώπινο λάθος. (Malware 2022) (Software bug 2020)

4.2. Πως Λειτουργεί

Οι κύριες φάσεις μιας επίθεσης ransomware, με βάση το μοντέλο “cyber kill chain”[8], είναι οι κάτωθι (Spitzner 2019) (DeGonia 2020):

I. Αναγνώριση - Reconnaissance

Κατά την φάση της «Αναγνώρισης», ο επιτιθέμενος συλλέγει πληροφορίες σχετικά με το δίκτυο του θύματος. Αυτές μπορεί να είναι είτε πληροφορίες δημόσια διαθέσιμες (πχ. Κοινωνικά Δίκτυα), είτε μέσω τεχνικών «Κοινωνικής Μηχανικής» (Social Engineering) (Social engineering (security) 2022), είτε ακόμα ψάχνοντας, κυριολεκτικά, στα σκουπίδια για έγγραφα της εταιρείας που μπορεί να φανούν χρήσιμα (Dumpster diving) (Michael 2006) (Dumpster Diving/Trashing 2021).

Υπάρχουν δυο είδη Αναγνώρισης:

1) **Παθητική Αναγνώριση** (Passive Recon.), όταν ο επιτιθέμενος συλλέγει πληροφορίες σχετικά με τον στόχο – θύμα, χωρίς να αλληλεπιδρά απευθείας με αυτό, χρησιμοποιώντας δημόσια διαθέσιμες πληροφορίες, το λεγόμενο “Open Source INTelligence” (OSINT), μέσω διαφόρων εργαλείων – τεχνικών (πχ. Google Hacking – Google Dorks, Shodan, Maltego) (Brathwaite 2022) (Zelleke 2021)

2) **Ενεργητική Αναγνώριση** (Active Recon.), όταν ο επιτιθέμενος αλληλεπιδρά απευθείας με το σύστημα/τα του θύματος, ώστε να συλλέξει πληροφορίες για τις συσκευές που είναι συνδεδεμένες στο δίκτυο, τις (δικτυακές) πόρτες επικοινωνίας που είναι ανοικτές, τα λειτουργικά συστήματα των Η/Υ και τις υπηρεσίες (services) που «τρέχουν» σε αυτά κλπ. Το βασικό μειονέκτημα μιας ενεργητικής αναγνώρισης είναι η πιθανότητα ενεργοποίησης των IDS/IPS[9] συστημάτων του θύματος. Εργαλεία που χρησιμοποιούνται, μεταξύ

[8] Τα διακριτά στάδια – φάσεις αυτά, είναι παρόμοια σε όλους τους τύπους – είδη κυβερνοεπιθέσεων. Το μοντέλο αρχικά αναπτύχθηκε από την εταιρεία Lockheed Martin το 2011. (7 Stages of Cyber Kill Chain 2022)

[9] Intrusion Detection System (IDS), αναλύει την κίνηση του δικτύου ή των Η/Υ (endpoints) για ύποπτες ενέργειες και ειδοποιεί τους αναλυτές ασφαλείας. Αντίστοιχα ένα Intrusion Prevention System (IPS), πχ. Firewall, μπορεί και να αποτρέψει κακόβουλες ενέργειες όπως επιθέσεις “brute force” ή “Denial of Service” (DoS).
(Intrusion Prevention System – IPS 2022) (Intrusion Detection System (IDS) 2022)

άλλων, σε μια ενεργητική αναγνώριση είναι: “Nmap”, “Nessus”, “Nikto”. (Brathwaite 2022)

II. Οπλοποίηση - Weaponisation

Στην φάση αυτή, ο επιτιθέμενος προετοιμάζει την επίθεσή του, Μπορεί για παράδειγμα να δημιουργήσει ένα phishing mail ή ένα malware το οποίο θα διανεμηθεί μέσω ενός USB flash drive.

III. Διανομή - Delivery

Όπως λέει και το όνομά της, πρόκειται για την φάση όπου ο επιτιθέμενος διανέμει – εφαρμόζει την μέθοδο που έχει επιλέξει ώστε να μεταφέρει το malware μέσα στο δίκτυο της εταιρείας - οργανισμού. Στην φάση αυτή, ο ανθρώπινος παράγοντας παίζει καθοριστικό λόγο, αφού πρόκειται για την πρώτη γραμμή άμυνας κατά τέτοιων επιθέσεων, αλλά και πολλές φορές, τον αδύναμο κρίκο της αλυσίδας (τεχνικές Social eng. έχουν και εδώ πεδίο εφαρμογής).

IV. Εκμετάλλευση (ευπάθειας) – Exploitation

Στην φάση αυτή ξεκινάει η «πυροδότηση» της επίθεσης, με την εκμετάλλευση της ευπάθειας που έχει ανιχνευθεί από τον επιτιθέμενο, και λαμβάνοντας τελικά τον έλεγχο του συστήματος (compromised system).

V. Εγκατάσταση – Installation

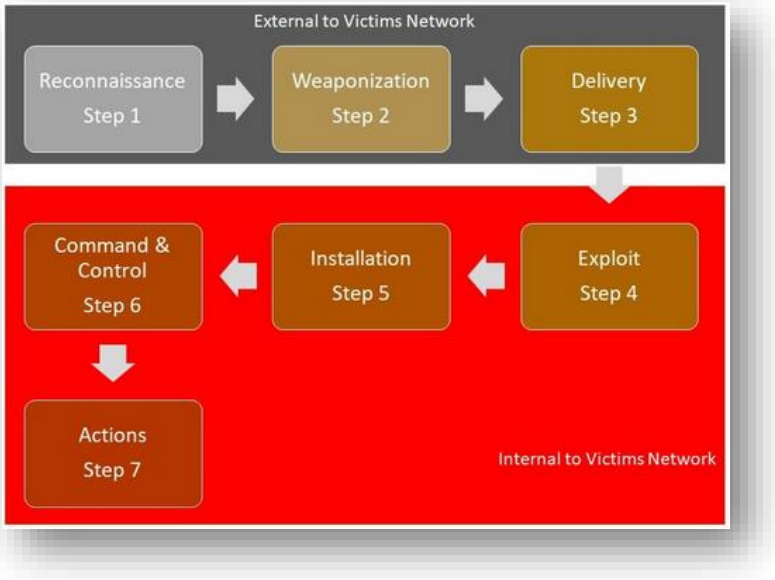
Το κακόβουλο λογισμικό (ransomware) εγκαθίσταται στον Η/Υ. Οι χρήστες, άθελα τους, μπορεί να εξαπλώσουν το ransomware και σε άλλους Η/Υ στο δίκτυο, στέλνοντας μολυσμένα email σε άλλους χρήστες του οργανισμού.

VI. Διοίκηση & Έλεγχος - Command & Control

Ο επιτιθέμενος πια έχει τον έλεγχο του συστήματος. Το ransomware επικοινωνεί με τον server του hacker, από τον οποίο θα λάβει και οδηγίες.

VII. Ενέργειες προς την επιτεύξη του στόχου - Actions on Objectives

Πρόκειται για την τελευταία φάση της επίθεσης. Αναλόγως τον στόχο της, οι κινήσεις που μπορεί να γίνουν είναι πχ η κρυπτογράφηση των δεδομένων και η εμφάνιση μηνύματος για λύτρα, να σταλούν τα συλλεχθέντα δεδομένα πίσω στον server, ώστε να πουληθούν αργότερα κ.α. (Seqrite 2019)



Εικόνα 9: Οι 7 φάσεις μιας επίθεσης Ransomware. (DeGonia 2020)

4.3. Είδη – Οικογένειες

Τα ransomware χωρίζονται σε πέντε είδη, βάση του τρόπου λειτουργίας τους, με τις δύο πρώτες να είναι και οι σημαντικότερες:

1. **Crypto-Ransomware:** Κρυπτογραφεί τα αρχεία του Η/Υ, χωρίς όμως να εμποδίζει την λειτουργία του συστήματος

2. **Locker Ransomware:** Δεν επηρεάζει τα αρχεία του χρήστη αλλά τον εμποδίζει να έχει πρόσβαση στην συσκευή. Το μήνυμα για πληρωμή λύτρων εμφανίζεται συνήθως σαν ειδοποίηση από κάποια αστυνομική αρχή.

3. **Doxware / Leakware:** Απειλεί τον χρήστη / εταιρεία για δημοσιοποίηση των δεδομένων αν δεν ικανοποιηθούν τα αιτήματα (πληρωμή των λύτρων).

4. **Scareware:** Εμφανίζει ψευδή μηνύματα στον χρήστη, για δήθεν μόλυνση από ιό, προτρέποντας τον να πληρώσει ώστε να επιλυθεί το πρόβλημα. Ενώ κάποια από τα ransomware του είδους μπορεί να κλειδώσουν τον χρήστη εκτός της συσκευής, η πλειονότητα αυτών απλά «γεμίζει» την οθόνη με “pop-ups”.

5. **Ransomware as a Service (RaaS):** Υπηρεσία που παρέχεται στον κυβερνοεγκληματία έναντι αμοιβής και περιέχει όλες τις φάσεις μιας επίθεσης.

5. Πρακτικό Μέρος - Λογισμικό Ανίχνευσης Εισβολής (ΛΑΕ)

5.1. Εισαγωγή

Όπως αναλύσαμε και παραπάνω, οι επιθέσεις ransomware έχουν αυξηθεί εκθετικά τα τελευταία χρόνια, στοχεύοντας κυρίως μεγάλους οργανισμούς και κρίσιμες υποδομές, με απώτερο σκοπό το κέρδος ή με πολιτική σκοπιμότητα, όπως είδαμε στην πρόσφατη Ρωσική εισβολή στην Ουκρανία (Gatlan 2022) (Constantinescu 2022) (Trendmicro 2022) (Kaduri 2022).

Το Λογισμικού Ανίχνευσης Εισβολής (ΛΑΕ) δημιουργήθηκε με σκοπό την έγκαιρη (μέσα σε μερικά δευτερόλεπτα) διάγνωση και ενημέρωση του χρήστη για εν εξελίξει επίθεση crypto-ransomware, μια υποκατηγορία malware το οποίο κρυπτογραφεί τα αρχεία του Η/Υ που μολύνει. Στόχος είναι μέσω της παρακολούθησης των προσβάσεων στα αρχεία του σκληρού δίσκου, να εντοπισθεί «η κίνηση» (movement) - το μοτίβο που χρησιμοποιεί το crypto-ransomware κατά την εκτέλεσή του.

5.2. Τρόπος Λειτουργίας

Όπως αναφέρθηκε παραπάνω, ένα crypto-ransomware θα ακολουθήσει ένα συγκεκριμένο μοτίβο σχετικά με τον τρόπο που διαβάζει και στην συνέχεια κρυπτογραφεί τα δεδομένα. Πιο συγκεκριμένα, θα διαβάσει – κρυπτογραφήσει με την σειρά, όλα τα αρχεία που υπάρχουν σε έναν φάκελο (folder path) και στην συνέχεια θα προχωρήσει στον επόμενο, ακολουθώντας δηλαδή μια «Αναζήτηση Κατά βάθος» (DFS – Depth First Search).

Το συγκεκριμένο RDS βασίζεται στο έλεγχο, σε πραγματικό χρόνο, των προσβάσεων (file accesses) που πραγματοποιούνται στα αρχεία του δίσκου, από τις διεργασίες του Λειτουργικού Συστήματος (ΛΣ) και την ειδοποίηση του χρήστη (alert) όταν υπάρχει η υποψία απειλής crypto-ransomware. Με βάση την σχεδίαση του αλγορίθμου, δημιουργείται αρχικά ένα alert για τις παρακάτω τέσσερις διακριτές ενέργειες, μαζί με την σχετική χρονοσφραγίδα (timestamp):

i. Δημιουργία - “Created”
ii. Μεταβολή – “Modified”
iii. Μετακίνηση – “Moved”
iv. Διαγραφή – “Deleted”

Από τις 4 αυτές ενέργειες μας ενδιαφέρει κυρίως η μεταβολή (modified) και η μετακίνηση του αρχείου (moved)[10], αφού αυτές είναι που παρατηρούνται σε μια επίθεση crypto-ransomware κατά την ανάγνωση και κρυπτογράφηση των δεδομένων αντίστοιχα.

Για την κατηγοριοποίηση μιας σειράς ενεργειών (μοτίβο) ως επίθεση, πρέπει να συντρέχουν, καθολικά, οι παρακάτω παράγοντες:

1. Η προς έλεγχο διαδρομή να είναι αρχείου (file path)
2. Η εντροπία του αρχείου να είναι κοντά στην τιμή **7.999**

[10] Ουσιαστικά πρόκειται για αλλαγή της κατάληξης (κρυπτογράφηση?) του αρχείου αφού έχει προηγηθεί ανάγνωσή του.

5.3. Ανάλυση του Αλγορίθμου

Προετοιμασία για την εκτέλεση του αλγορίθμου.

Το ΛΑΕ αποτελείται από δύο ξεχωριστά αρχεία, το 1ο περιέχει τον κώδικα (κλάσεις, συναρτήσεις κλπ.) ενώ το 2ο περιέχει τις (global) μεταβλητές. Η επιλογή αυτή έγινε για την ευκολότερη πρόσβαση στις (global) μεταβλητές από όλα τα modules (Siddiqui 2022)[1], αλλά και για την αποφυγή του φαινομένου του "*Circular Importing*" (Robinson 2017). Τέλος, μαζί με τα αρχεία αυτά υπάρχει και το "*requirements.txt*" μέσω του οποίου θα εγκατασταθούν οι απαραίτητες βιβλιοθήκες (dependencies) για την σωστή λειτουργία του ΛΑΕ. Περισσότερες οδηγίες στον σύνδεσμο.

Η εκτέλεση του κώδικα θα πρέπει να γίνει από το root directory με δικαιώματα διαχειριστή (administrator).

Ο αλγόριθμος έχει σχεδιαστεί με βάση την αρχιτεκτονική "multithreading". Σύμφωνα με αυτή δημιουργούνται κατά την εκτέλεση δυο διακριτά νήματα (threads) τα οποία εκτελούνται ψευδό-παράλληλα. Στο 1ο thread εκτελείται η συνάρτηση **main**, για έλεγχο των αλλαγών σε επίπεδο αρχείων, ενώ στο 2ο thread με όνομα **"ransomCheckTrd"** εκτελείται μια ρουτίνα η οποία ελέγχει τις διαδρομές αρχείων που αποθηκεύονται σε λίστα μέσω της συνάρτησης **"buffer"** και υπολογίζει (αν χρειαστεί) την εντροπία αυτών. Τέλος, αν βρεθεί αρχείο με τιμή εντροπίας μεγαλύτερη από το καθορισμένο όριο (**"entropy_limit"**) καλεί ένα ξεχωριστό παράθυρο εντολών (terminal) το οποίο απεικονίζει και το σχετικό alert.

Ειδικότερα τα βήματα που ακολουθεί ο αλγόριθμος είναι τα παρακάτω:

1. Δημιουργεί ένα αντικείμενο (instance) της κλάσης "Listener" (pynput lib), το οποίο υλοποιεί την δυνατότητα τερματισμού του προγράμματος με πάτημα του "Esc"[11].

```
def main():
    # create a Listener for using 'Esc' to exit.
    with Listener(on_release=on_release) as listener:
```

Εικόνα 10: Το αντικείμενο της κλάσης "Listener"

[11] Κατά τον τερματισμό της συνάρτησης main, τερματίζονται και τα υπόλοιπα (daemon) threads.

```python
# Function for using 'Esc' to exit.
def on_release(key):
    if key == Key.esc:
        print("> 'Esc' key was pressed. Exiting ... !")

        return sys.exit(1)
```

Εικόνα 11: Η συνάρτηση "on_release", για τον τερματισμό της εκτέλεσης του προγράμματος πατώντας το "Esc".

2. Θέτει το προς παρακολούθηση directory ανάλογα το Λ.Σ, μέσω της συνάρτησης "**monitor_path**":

   - Windows: **C:**
   - Linux[12]: user's "**HOME"** folder path

```python
try:
    global mon_path
    mon_path = monitor_path()
    if os.path.exists(mon_path):
        print("Path to be monitored EXISTS!")
        print(f"Started Monitoring: {mon_path}")
    else:
        raise "Path to be monitored DOES NOT EXIST!"
```

```python
# Set monitoring path depending on the OS
def monitor_path():
    operSys = platform.system().lower()

    if operSys  == "windows":
        print(f"Detected OS: {operSys.capitalize()}")
        return os.getenv("SystemDrive") + "\\"

    elif operSys == "linux":
        print(f"Detected OS: {operSys.capitalize()}")
        return os.getenv("HOME") # set HOME dir


    else:
        raise Exception(f"Not supported OS: {operSys}")
```

Εικόνα 12: Κλήση και ορισμός της συνάρτησης "monitor_path", για τον ορισμό του προς παρακολούθηση directory.

[12] Η λειτουργία για Linux θα προστεθεί σε μελλοντική έκδοση.

3. Δημιουργεί τα δύο αντικείμενα των κλάσεων “Handler”, “Observer” (watchdog lib), ώστε μέσω της μεθόδου **“observer.start()”** να ξεκινήσει η παρακολούθηση του root directory για αλλαγές στο σύστημα αρχείων.

```
# create a Listener for using 'Esc' to exit.
with Listener(on_release=on_release) as listener:

    try:
        gv.monPath = monitor_path()
        if os.path.exists(gv.monPath):
            print(f"Path '{gv.monPath}' to be monitored EXISTS!")
        else:
            print(f"Path '{gv.monPath}' to be monitored DOES NOT EXIST!")
            sys.exit(1)
        patterns = ["*"]
        ignore_patterns = None
        ignore_directories = True
        case_sensitive = False  # Windows is case-insensitive
        event_handler = Handler(
            patterns, ignore_patterns, ignore_directories, case_sensitive)
        observer = Observer()
        observer.schedule(event_handler, gv.monPath, recursive=True)
```

Εικόνα 13: Τα αντικείμενα των κλάσεων “Handler” και “Observer”, για την παρακολούθηση του root directory.

4. Ανάλογα με τον τύπο της αλλαγής καλείται και η αντίστοιχη μέθοδος της κλάσης “Handler”, εμφανίζοντας ταυτόχρονα στην οθόνη και το αντίστοιχο timestamp:
   - **on_created**, για δημιουργία αρχείου
   - **on_modified**, για αλλαγή αρχείου
   - **on_deleted**, για διαγραφή αρχείου
   - **on_moved**, για μετακίνηση αρχείου

5. Αν έχουμε μεταβολή (**on_modified**) ή μετακίνηση (**on_moved**) αρχείου, καλείται η συνάρτηση “ **pattern_recognition**” με ορίσματά της την **αρχική** (file_src) και **τελική διαδρομή** (file_dest) του αρχείου (με κενή αρχική τιμή).

```python
# Inherits "PatternMatchingEventHandler" class
class Handler(PatternMatchingEventHandler):
    """monitors filesystem events"""

    def on_created(self, event):
        super().on_created(event)
        print(f"{strftime('%H:%M:%S')} - CREATED File: {event.src_path}")


    def on_modified(self, event):
        super().on_modified(event)
        print(f"{strftime('%H:%M:%S')} - MODIFIED File: {event.src_path}")
        pattern_recognition(event.src_path)


    def on_deleted(self, event):
        super().on_deleted(event)
        print(f"{strftime('%H:%M:%S')} - DELETED File: {event.src_path}")


    def on_moved(self, event):
        super().on_moved(event)
        print(f"{strftime('%H:%M:%S')} - File MOVED from {event.src_path} TO {event.dest_path}")
        pattern_recognition(event.src_path, event.dest_path)
```

Εικόνα 14: Οι συναρτήσεις της κλάσης "Handler", για την διαχείριση του εκάστοτε file access event.

6. Η συνάρτηση "**pattern_recognition**" υλοποιεί τα παρακάτω:

```python
def pattern_recognition(fileSrc, fileDest = ""):
    if fileDest == '':
        path = fileSrc
        suffix = pathlib.Path(fileSrc).suffix
    else:
        path = fileDest
        suffix = pathlib.Path(fileDest).suffix

    try:
        if not os.path.isdir(path):

            # Excluding known file extensions
            if suffix.lower() not in gv.knownExtList:
                if path not in gv.bufferCache:

                    print("Adding file path to Buffer!")
                    buffer(path)
                else:
                    print("File already in buffer")

            else:
                print("Known file extension or path is a directory")
        else:
            print(f"{path} is a directory!")

    except Exception as e:
        print("Error when analysing path:\n",e)
```

Εικόνα 15: συνάρτηση "pattern_recognition"

i. Ελέγχει αν προς έλεγχο (αρχική) διαδρομή είναι αρχείο μέσω της συνθήκης (Path lib): "**if not os.path.isdir(path)**"

ii. Ελέγχει αν η κατάληξη του αρχείου είναι στην λίστα **"knownExtList",** και άρα πρόκειται για γνωστή κατάληξη. Ουσιαστικά η λίστα αυτή λειτουργεί ως «φίλτρο» των file extensions που θέλουμε να αποκλείσουμε.

```
# Lists with know File Extensions and error Log
knownExtList = [".zip", ".rar", ".tmp", ".7z", ".tar.gz",".xlsx", ".jpeg", ".txt"]
errorLog = []
```

Εικόνα 16: Ο ορισμός της λίστας "knownExtList", για το «φιλτράρισμα» των γνωστών καταλήξεων αρχείων.

iii. Αν η κατάληξη αρχείου δεν είναι γνωστή, ο αλγόριθμος προχωράει στον υπολογισμό της εντροπίας του αρχείου (μέσω της συνάρτησης "**file_entropy**"), ώστε να διαπιστωθεί αν το αρχείο είναι κρυπτογραφημένο. Επίσης, υπολογίζει και τον συνολικό χρόνο που χρειάστηκε από την στιγμή εισαγωγής του 1ου προς έλεγχο αρχείου μέχρι την στιγμή της εύρεσης του 1ου «μολυσμένου» αρχείου. Η ρουτίνα ελέγχου τρέχει σε ξεχωριστό thread όπως φαίνεται παρακάτω.

```
# Calculate file entropy
def file_entropy(path):
    with open(path, "rb") as f:
        data = f.read()
    e = 0
    cnt = Counter(data)
    l = len(data)
    for c in cnt.values():
        p = c / l
        e += p * log2(p)
    return round(-e, 3)
```

Εικόνα 17: Η συνάρτηση "file_entropy", για τον υπολογισμό της εντροπίας του αρχείου.

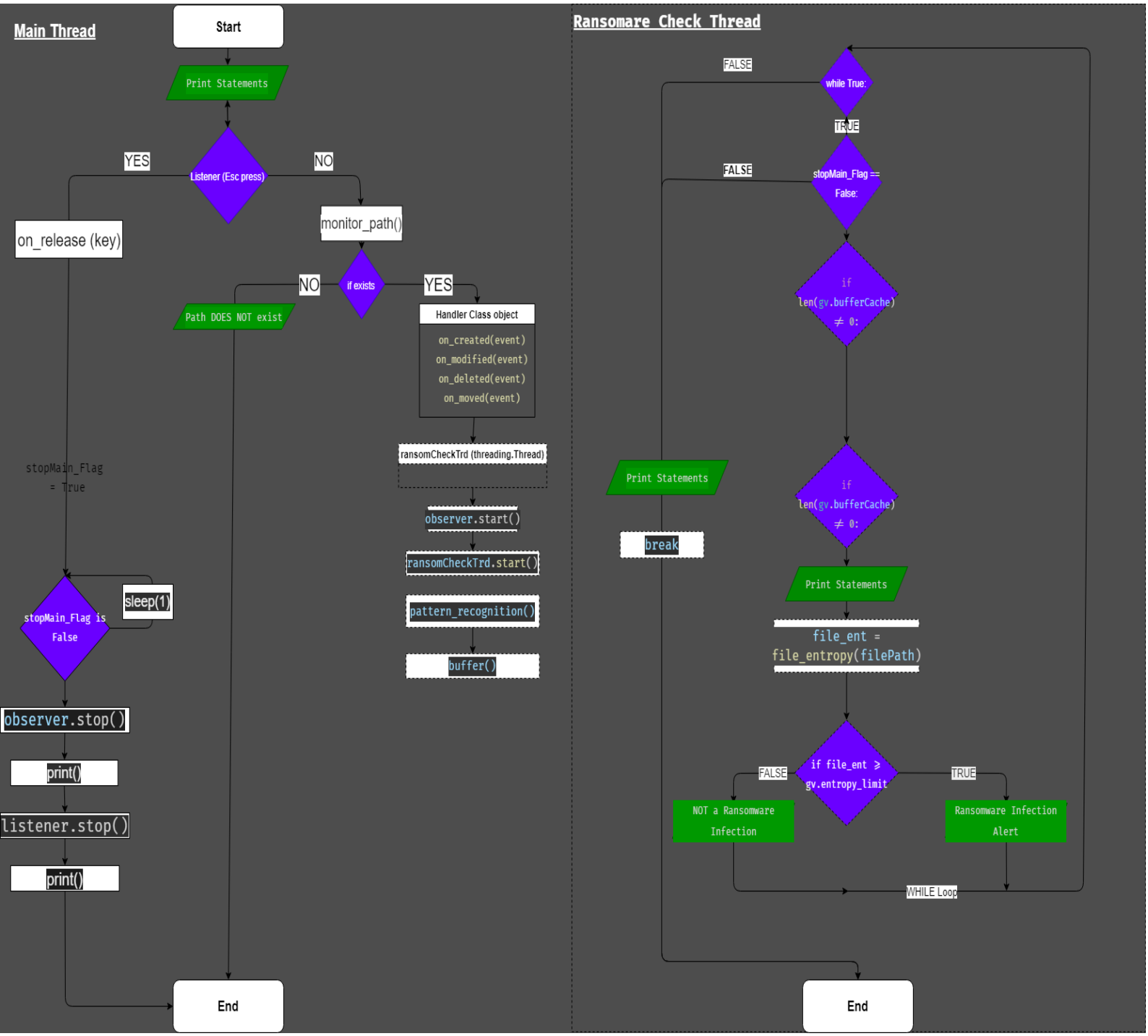
```
ransomCheckTrd = thrd.Thread(target=ransomware_check, name="Ransomware_Check_Thread", daemon=True)
gv.ransomCheckTrdName = ransomCheckTrd.name
```

Εικόνα 18: Η δημιουργία του ξεχωριστού thread στο οποίο θα εκτελείται η συνάρτηση "ransomware_check", για τον έλεγχο των αρχείων.

```
def ransomware_check():

    while True:
        if gv.stopMain_Flag == False:
            if len(gv.bufferCache) != 0:
                filePath = gv.bufferCache.pop()

                try:
                    print("Checking for Ransomware!")
                    print("Calculating Entropy ... !")
                    file_ent = file_entropy(filePath)
                    print(f"The entropy of {filePath} is: {file_ent}")
                    if file_ent >= gv.entropy_limit:
                        print("RANSOMWARE INFECTION")
                        ransTime = datetime.now()
                        winCmd = f"""start cmd.exe /K "echo '--ALERT--: RANSOMWARE INFECTION in file: {filePath}'; & echo '--ALERT--: Infection found after:
                        {(ransTime - gv.startTime).total_seconds(): 0.2f} seconds'" """
                        subprocess.run(winCmd, shell = True)

                    else:
                        print("NOT A Ransomware Infection")


                except Exception as e:
                    print("Could not calculate entropy with error:\n", e)
                    print("Writing Error to Log", gv.errorLog.append(e))

            else:
                print(f"{gv.ransomCheckTrdName}: Buffer is empty!")


        else:
            print(f"'{gv.ransomCheckTrdName}' thread has been stopped!")
            break
    return;
```

Εικόνα 19: Ορισμός της συνάρτησης "ransomware_check"

5.3.1. Διάγραμμα Κώδικα



Εικόνα 20: Διάγραμμα Κώδικα

6. Αποτελέσματα

Κατά την φάση των δοκιμών (testing), χρησιμοποιήθηκαν 4 πραγματικά Crypto-Ransomware της οικογένειας Conti (Rochberger 2021), τα hashes καθώς και η συνοπτική εικόνα (virustotal.com) των οποίων παρατίθενται παρακάτω **(Πίνακας 1) (Εικόνα 21) (Εικόνα 22) (Εικόνα 23) (Εικόνα 24)**.

Τα Ransomware εκτελέστηκαν σε εικονική μηχανή (VM) με **Windows 10** ΛΣ, και χαρακτηριστικά όπως παρουσιάζονται στην **Εικόνα 28**. Η εκτέλεση τους έγινε χειροκίνητα, αφού πρώτα ξεκίνησε να «τρέχει» το ΛΑΕ. Οι πόροι του συστήματος (resources) που απορροφούσε το ΛΑΕ κατά την εκτέλεση, αποτυπώνονται στην **Εικόνα 29**.

Στόχος ήταν, να υπολογισθούν τα παρακάτω:

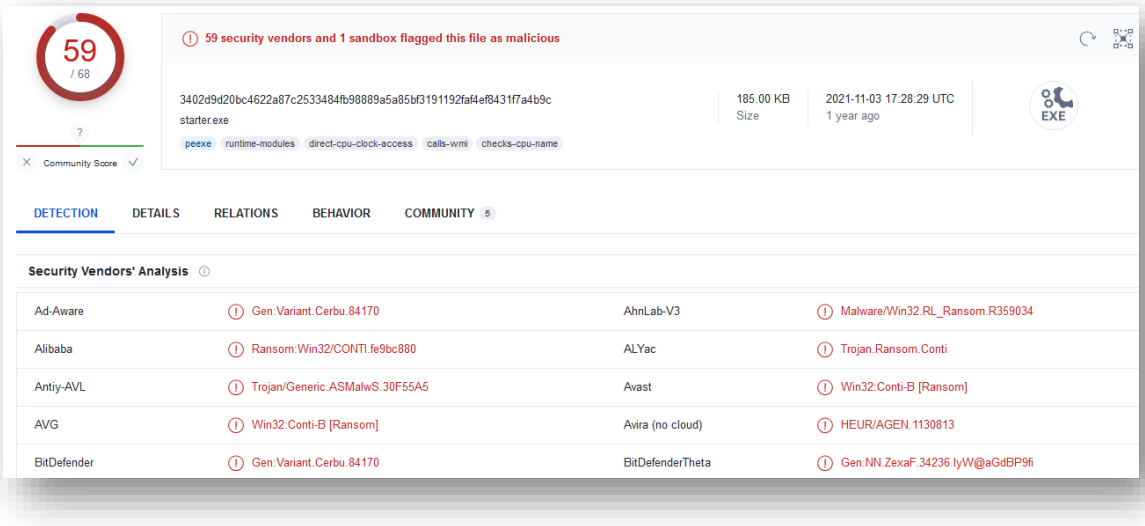
1. **Χρόνο Απόκρισης**, δηλαδή ο χρόνος που χρειάζεται το ΛΑΕ για να εντοπίσει το μοτίβο – «κίνηση» του Ransomware.
2. **Απαιτούμενους Πόρους (resources)**, δηλαδή την υπολογιστική ισχύ (CPU) και μνήμη RAM που χρειάζεται το ΛΑΕ για να λειτουργήσει.

Όπως γίνεται εύκολα κατανοητό, ένας συνδυασμός χαμηλού (γρήγορου) χρόνου απόκρισης, με σχετικά λίγους απαιτούμενους πόρους, καθιστά το ΛΑΕ μια λύση που μπορεί να χρησιμοποιηθεί σε ένα ευρύ φάσμα συστημάτων.

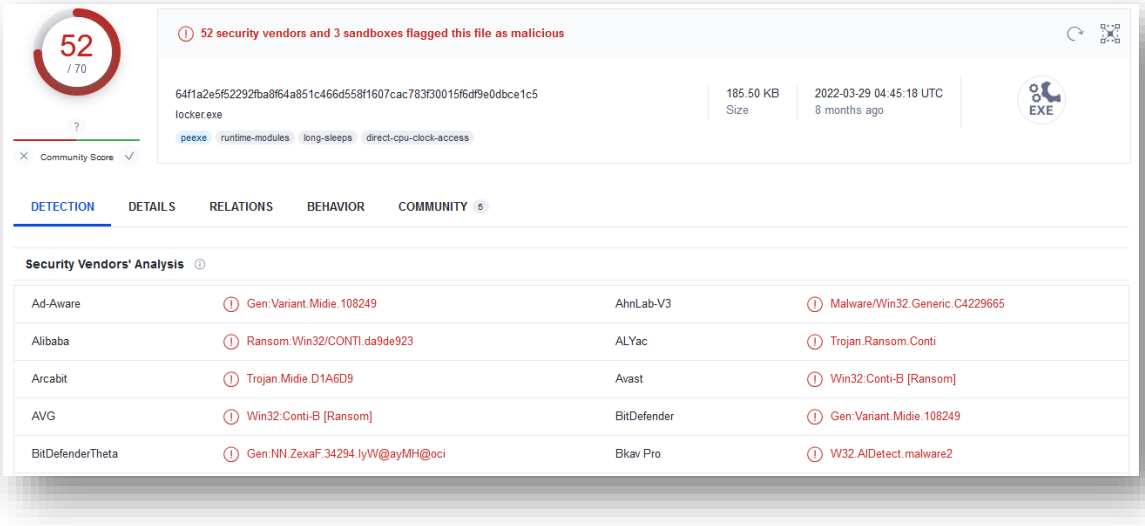
Παρακάτω παρατίθενται μερικά στιγμιότυπα κατά την εκτέλεση του κώδικα **(Εικόνα 25)**. Παρατηρούμε ότι ο χρόνος απόκρισης, δηλαδή ο χρόνος που χρειάζεται ο αλγόριθμος από την στιγμή που ξεκίνησε ο έλεγχος του 1ου αρχείου της λίστας (buffer list) , μέχρι και την ταυτοποίηση του 1ου κρυπτογραφημένου αρχείου, εξαρτάται κυρίως από την σειρά προσπέλασης των αρχείων από το ransomware, άρα και το πότε θα αρχίσει η κρυπτογράφησή τους. Ένας τυπικός χρόνος απόκρισης είναι περίπου τα **35 sec**. **(Εικόνα 26)(Εικόνα 27)**

File Hash	Ransomware Family	Virustotal.com
3402d9d20bc4622a87c2533484fb98889a5a85bf3191192faf4ef8431f7a4b9c	Conti	Link
64f1a2e5f52292fba8f64a851c466d558f1607cac783f30015f6df9e0dbce1c5	Conti	Link
bc413e02defccc55f1c9925e9cf4fde4a714db1e06c6e021ddbd4b15cf2613d7	Conti	Link
53b1c1b2f41a7fc300e97d036e57539453ff82001dd3f6abf07f4896b1f9ca22	Conti	Link

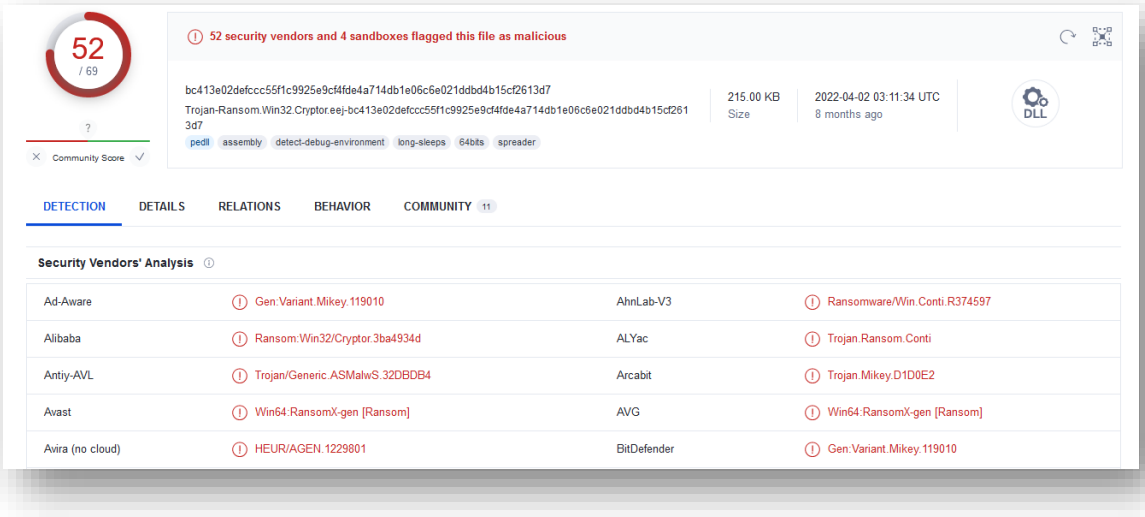
Πίνακας 1: Τα χαρακτηριστικά των Ransomware που χρησιμοποιήθηκαν κατά την φάση των δοκιμών (testing)



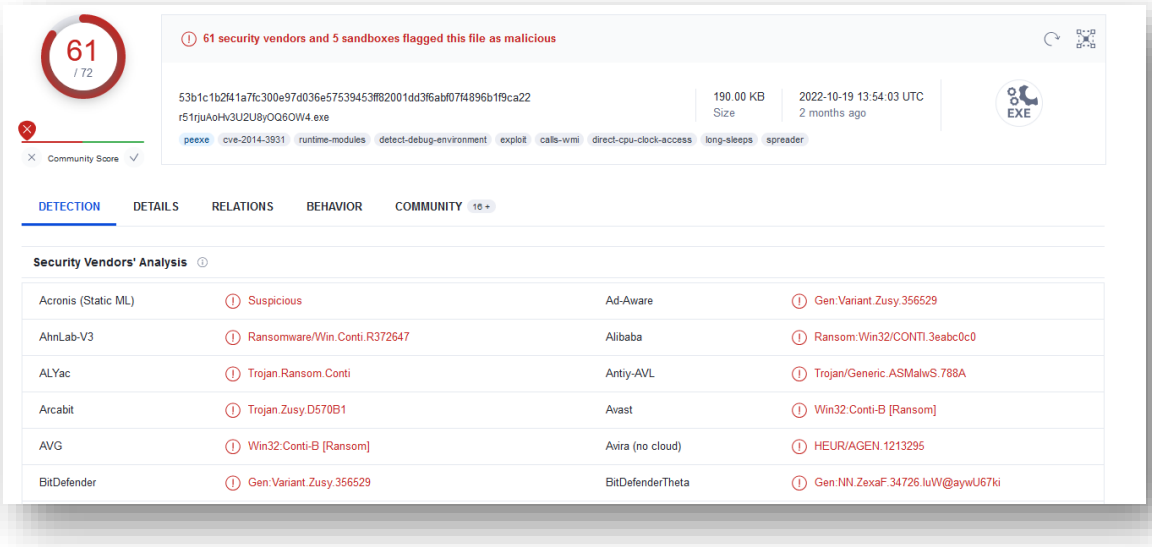
Εικόνα 21: Συνοπτική εικόνα 1ου Ransomware στο virustotal.com



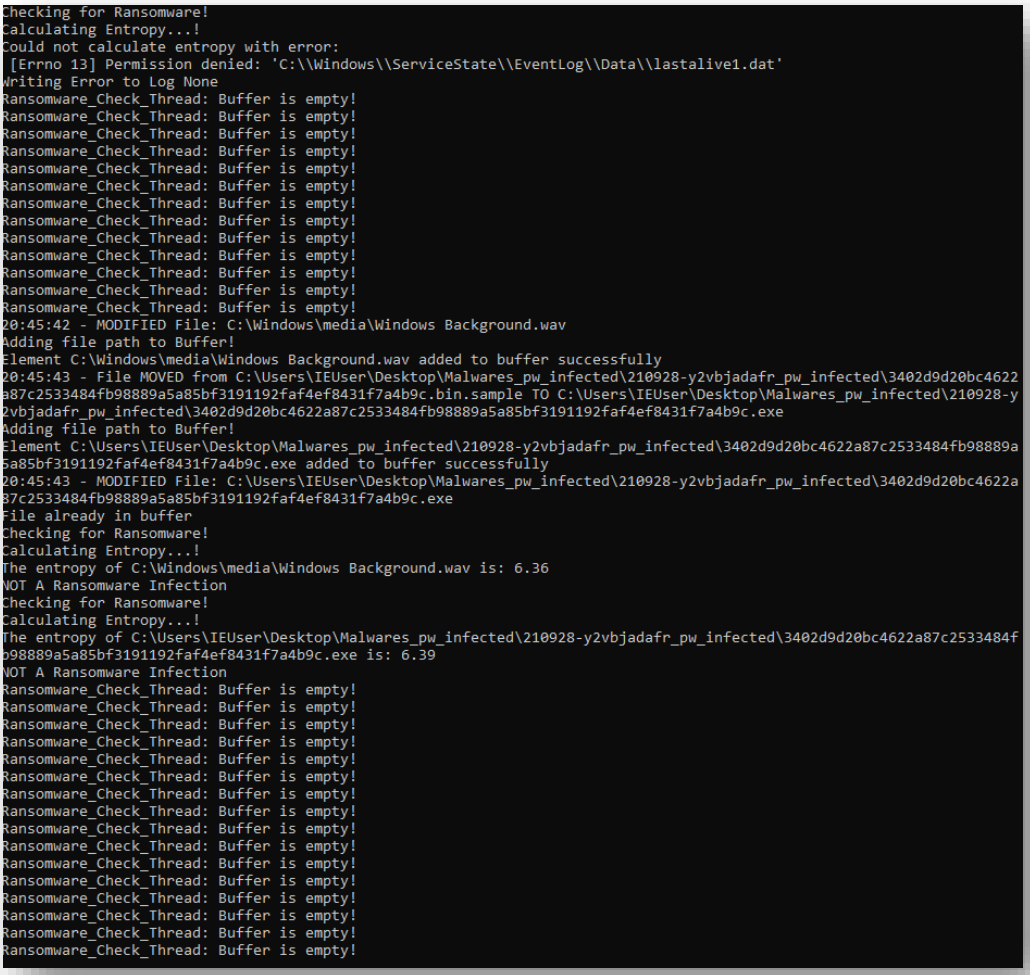
Εικόνα 22: Συνοπτική εικόνα 2ου Ransomware στο virustotal.com



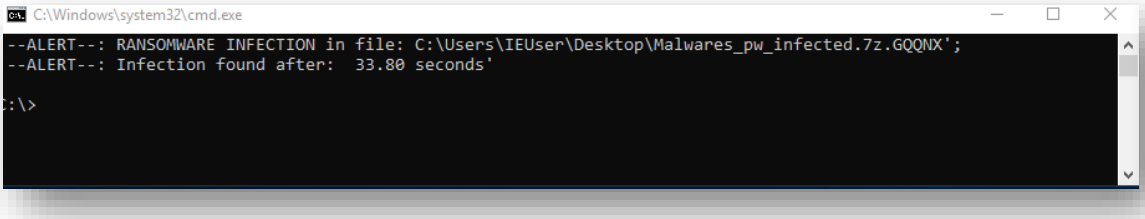
Εικόνα 23: Συνοπτική εικόνα 3ου Ransomware στο virustotal.com



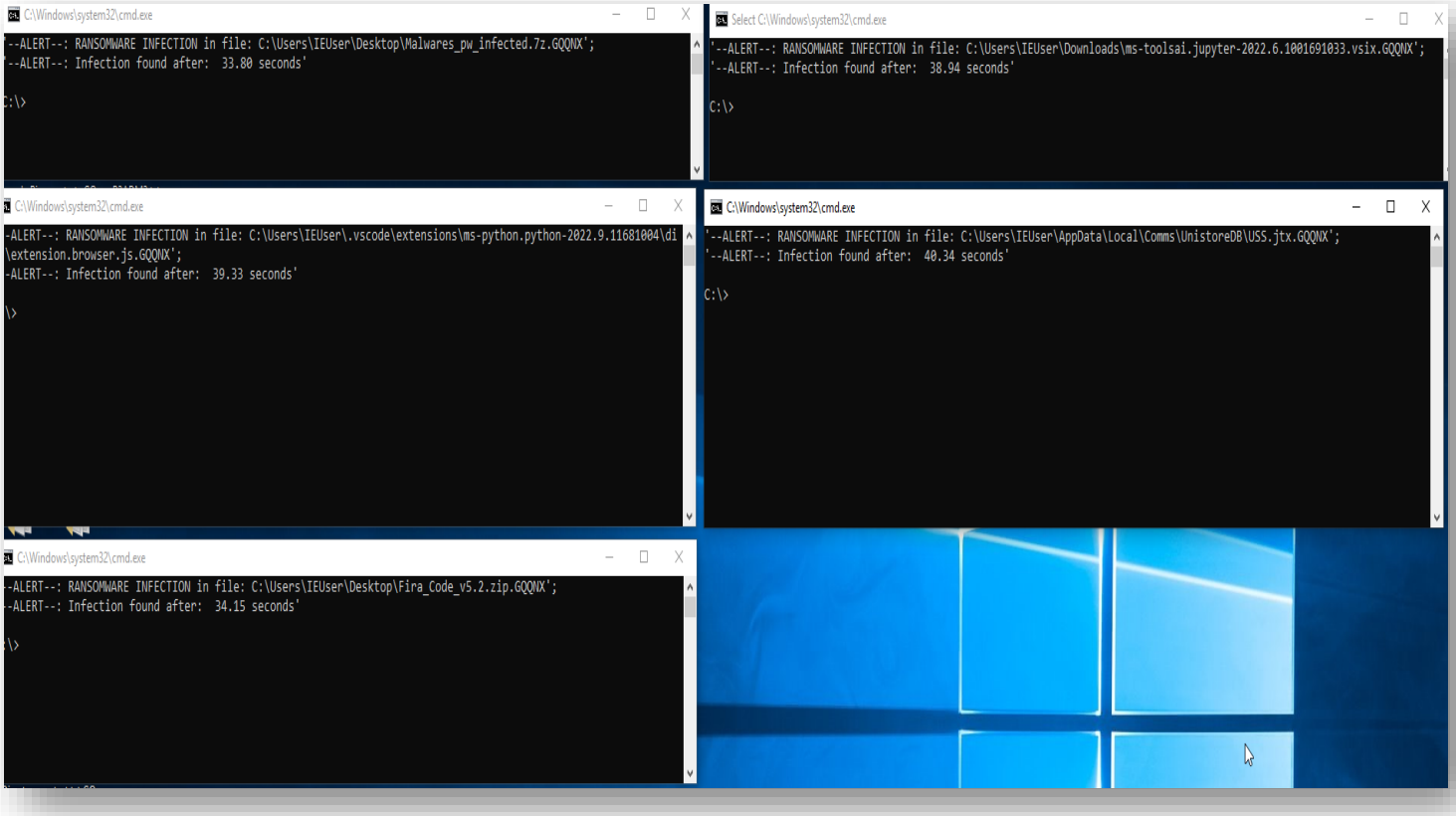
Εικόνα 24: Συνοπτική εικόνα 4ου Ransomware στο virustotal.com



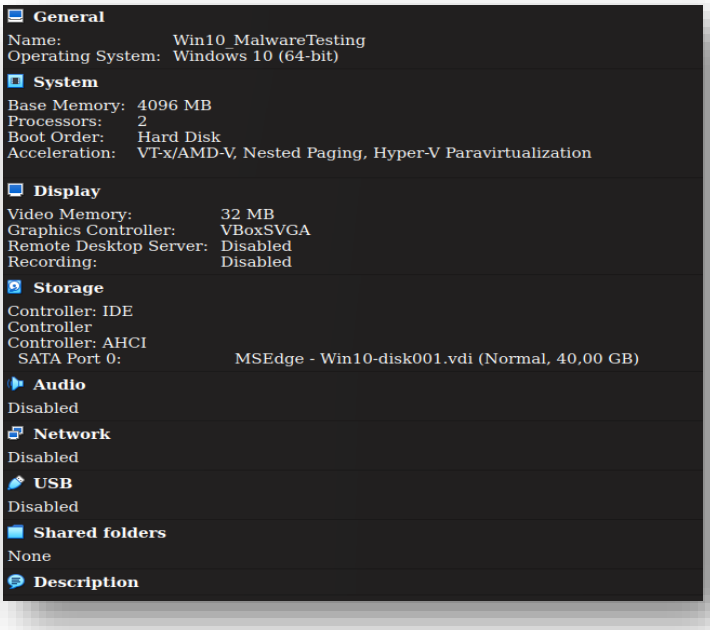
Εικόνα 25: Μια τυπική απεικόνιση της γραμμής εντολών (terminal), κατά την εκτέλεση του ΛΑΕ. Παρατηρούμε ότι η τιμή εντροπίας των ίδιων των ransomware (.exe), είναι κάτω του ορίου.



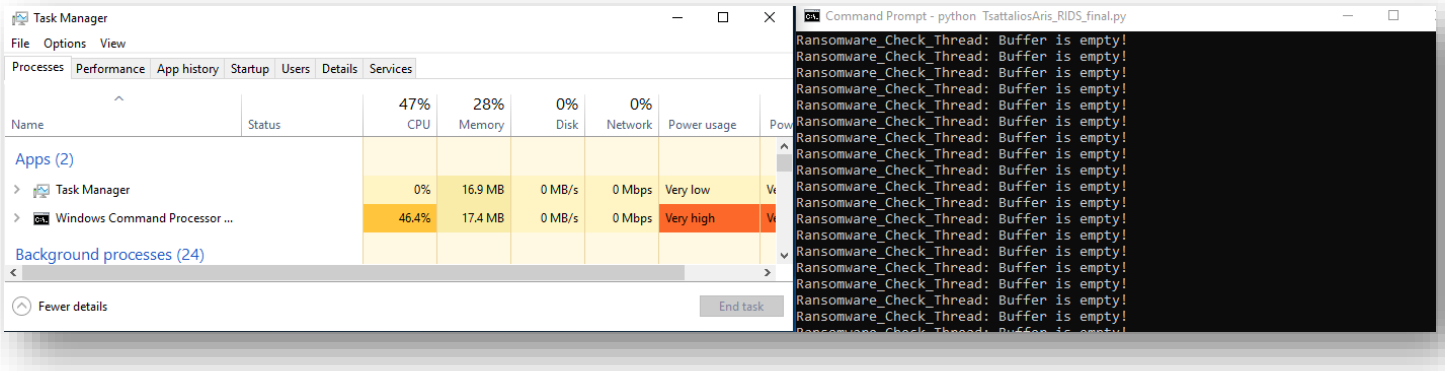
Εικόνα 26: Εύρεση του πρώτου κρυπτογραφημένου αρχείου μετά από 33,8 δευτ.



Εικόνα 27: Τα alerts που παράγονται από το ΛΑΕ.



Εικόνα 28: Τα χαρακτηριστικά της εικονικής μηχανής (VM) στην οποία πραγματοποιούνταν οι μετρήσεις.



Εικόνα 29: Τα resources που καταναλώνονται κατά την εκτέλεση του ΛΑΕ.

6.1. Δικαιολόγηση Επιλογών

- **Python ως η γλώσσα υλοποίησης**

  Επιλέχθηκε η Python ως γλώσσα υλοποίησης, αφού πρόκειται για μια δημοφιλή αντικειμενοστραφή γλώσσα με πολλά εργαλεία – βιβλιοθήκες, ιδιότητα ιδιαίτερα χρήσιμη σε ενδεχόμενη επεκτασιμότητα (scalability) του αλγορίθμου, και προσθήκης νέων λειτουργιών (features). Επίσης λόγω της ευκολίας του συντακτικού της, δίνει την δυνατότητα γρήγορης ανάπτυξης νέων δυνατοτήτων και ένταξής τους στον ήδη υπάρχον κώδικα, για τυχόν αντιμετώπιση νέων ειδών ransomware. Τέλος, είναι διαθέσιμη by default σε Linux OS.

- **Λειτουργικό σύστημα Windows**

  Επιλέχθηκε η σχεδίαση του ΛΑΕ καταρχήν για Windows, αφού αποτελεί το πιο διαδεδομένο ΛΣ για προσωπικούς ΗΥ, δίνοντας όμως ταυτόχρονα και την δυνατότητα επέκτασης των λειτουργιών του και για *nix λειτουργικά συστήματα (πχ. Mac OS, Linux).

- **Μέτρηση εντροπίας ως μέθοδο ταυτοποίησης**

  Επιλέχθηκε ο υπολογισμός της εντροπίας ως μέθοδος ταυτοποίησης ενός αρχείου ως «μολυσμένου», στα πλαίσια μιας λογικής “behavior-based detection”[13] αφού αυτή δεν προϋποθέτει την ύπαρξη κάποιας εξωτερικής βάσης δεδομένων για την αναγνώριση της απειλής, όπως συμβαίνει στην “signature-based detection” λογική. Ταυτόχρονα η μέτρηση εντροπίας αποτελεί μια γρήγορη και σχετικά απλή διαδικασία, η οποία δεν απαγορεύει την συνύπαρξή της με επιπλέον μεθόδους (πχ. υπολογισμός hash) εντοπισμού «μολυσμένων» αρχείων.

6.2. Ανάπτυξη – προσθήκη λειτουργιών

Σε μια μελλοντική έκδοση του ΛΑΕ, θα μπορούσαν να προστεθούν επιπρόσθετες λειτουργίες καθώς και επικουρικοί τρόποι εντοπισμού του μοτίβου των ransomware όπως οι παρακάτω:

- Επέκταση της λειτουργίας του ΛΑΕ και σε Linux ΛΣ. Απαιτεί την μικρή διαφοροποίηση στον εντοπισμό του root directory, καθώς και στην διαχείριση του file path string.

- Προσθήκη επιπλέον ελέγχων ώστε να αναγνωρίζει το ΛΑΕ αν στην συγκεκριμένη διαδρομή φακέλου (folder path) έχουν επηρεαστεί (σειριακά) και άλλα αρχεία, αποθηκεύοντας και στην συνέχεια ελέγχοντας τα folder paths.

- (Δειγματοληπτικός) Υπολογισμός hash των αρχείων στους φακέλους που υπάρχουν μετά το folder path που έχει εντοπιστεί παραπάνω, και σύγκριση των hashes πριν και μετά την αλλαγή του αρχείου. Αν αυτό συμβαίνει σε x πλήθος αρχείων από τον ίδιο γονικό φάκελο, τότε σηματοδοτεί πιθανή επίθεση.

[13] Με την μελλοντική προσθήκη και άλλων features.

- Εντοπισμός της/των διεργασιών (parent – child processes), τις οποίες χρησιμοποιεί το ransomware κατά την λειτουργία του, και τερματισμός (kill) αυτών.

7. Συμπεράσματα

Σύμφωνα με τα παραπάνω, θα μπορούσαμε να συνοψίσουμε τα πλεονεκτήματα και τα μειονεκτήματα της υπό εξέταση λύσης ως εξής:

7.1. Πλεονεκτήματα Αλγορίθμου

- **Ταχύτητα απόκρισης**

  Λόγω της σχετικά απλής διαδικασίας για τον υπολογισμό της εντροπίας κάθε αρχείου, αλλά και του αρχικού «φιλτραρίσματος» των καταλήξεων αρχείων που δεν αποτελούν απειλή, έχουμε ως αποτέλεσμα άμεση απόκριση στα file events της τάξεως μερικών δευτερολέπτων. Η συγκεκριμένη ιδιότητα, είναι κομβικής σημασίας αν λάβει κάνεις υπόψιν ότι μιλάμε για ένα λογισμικό το οποίο πρέπει να εντοπίζει εν εξελίξει επιθέσεις.

- **Μικρή ανάγκη σε επεξεργαστική ισχύ**

  Σε συνέχεια των παραπάνω, δηλαδή στην απλότητα σχεδίασης του αλγορίθμου, έχουμε και ένα ακόμα πλεονέκτημα, την μικρή ανάγκη σε επεξεργαστική ισχύ, παρόλο που η γλώσσα Python θεωρείται γενικά “resource-hungry”, λόγω της εξάρτησής της από βιβλιοθήκες γραμμένες σε άλλες, πιο χαμηλού επιπέδου, γλώσσες (κυρίως σε γλώσσα C). Η εικονική μηχανή στην οποία έγιναν οι μετρήσεις, επιλέχθηκε να είναι σχετικά «αδύναμη», πράγμα που αποτυπώνεται και στα χαρακτηριστικά της (**Εικόνα 28)** . Παρόλα αυτά η κατανάλωση CPU και μνήμης, περιορίζεται στο μισό και στο 1/3 της διαθέσιμης, αντίστοιχα. **(Εικόνα 29)**

- **Αρχιτεκτονική σχεδίασης πολλαπλών νημάτων (multithreading architecture)**

  Επιλέγοντας την multithreading αρχιτεκτονική έχουμε το πλεονέκτημα ότι τα διαφορετικά threads λειτουργούν (ψευδο)παράλληλα, με αποτέλεσμα αφενός την ταχύτερη διαχείριση των file access events, και αφετέρου την δυνατότητα μελλοντικής επεκτασιμότητας (scalability) του αλγορίθμου, αφού αρκεί η δημιουργία ενός καινούργιου νήματος ώστε να ενσωματωθεί μια καινούργια λειτουργία.

7.2. Μειονεκτήματα Αλγορίθμου

- **Μονοδιάστατος μηχανισμός ανίχνευσης της απειλής**

  Λόγω του ότι το ΛΑΕ, στην παρούσα έκδοση, βασίζεται μόνο στον υπολογισμό της εντροπίας για την κατηγοριοποίηση ενός αρχείου ως «μολυσμένου» ή όχι, υπάρχει μεγαλύτερη πιθανότητα σφάλματος, για παράδειγμα ψευδώς θετικών ειδοποιήσεων (false positive alerts), αλλά και η αδυναμία εντοπισμού του κακόβουλου λογισμικού, πριν αυτό εκτελεστεί, αφού η τιμή της εντροπίας του είναι κατώτερη του θεσπισμένου ορίου. **(Εικόνα 25)**

- **Λειτουργία μόνο σε Windows OS.**

  Η παρούσα έκδοση του ΛΑΕ, υποστηρίζει μόνο Windows ΛΣ, αφού η ενσωμάτωση και των *nix λειτουργικών συστημάτων απαιτεί διαφορετική διαχείριση των συμβολοσειρών (strings) για τις διαδρομές των αρχείων (file paths), λειτουργία που μπορεί να προστεθεί σε μελλοντική έκδοση.

Βιβλιογραφία

2022. «7 Stages of Cyber Kill Chain.» *crowdstrike.com.* 14 October. Πρόσβαση 10 11, 2022. https://www.crowdstrike.com/cybersecurity-101/cyber-kill-chain/.

Agcaoili, Janus, Miguel Ang, Earle Earnshaw, Byron Gelera, και Nikko Tamaña. 2021. *Ransomware Double Extortion and Beyond: REvil, Clop, and Conti.* 15 June. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti.

Arntz, Pieter. 2018. *How threat actors are using SMB vulnerabilities.* 14 December. https://blog.malwarebytes.com/101/2018/12/how-threat-actors-are-using-smb-vulnerabilities/.

Belcic, Ivan. 2022. *The Destructive Reality of Ransomware Attacks .* 24 February. https://www.avast.com/c-biggest-ransomware-attacks.

Brathwaite, Shimon. 2022. «Active vs Passive Cyber Reconnaissance in Information Security.» *securitymadesimple.org.* 06 January. https://www.securitymadesimple.org/cybersecurity-blog/active-vs-passive-cyber-reconnaissance-in-information-security.

Clark , Jen. 2016. *Internet Of Things.* 17 November. https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/.

2021. *Colonial Pipeline Incident: Ransomware Impacts and Mitigation Strategies.* 13 05. https://www.cyber.nj.gov/garden_state_cyber_threat_highlight/colonial-pipeline-incident-ransomware-impacts-and-mitigation-strategies.

Constantinescu, Vlad. 2022. *Russian Hacktivists Infect Ukrainian Targets with New Somnia Ransomware.* 15 November. Πρόσβαση 11 2022, 20. https://www.bitdefender.com/blog/hotforsecurity/russian-hacktivists-infect-ukrainian-targets-with-new-somnia-ransomware/.

Crowdstrike. 2021. *History of Ransomware.* 21 June. https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/.

crowdstrike.com. 2022. *Lateral Movement.* 18 02. https://www.crowdstrike.com/cybersecurity-101/lateral-movement/.

2022. *Cryptography.* 26 February. https://en.wikipedia.org/wiki/Cryptography.

DeGonia, Tony. 2020. *Cyber Kill Chain model and framework explained.* 13 March. https://cybersecurity.att.com/blogs/security-essentials/the-internal-cyber-kill-chain-model.

2021. *Dumpster Diving/Trashing.* 28 November. https://www.geeksforgeeks.org/dumpster-diving-trashing/.

Fortinet. 2022. *What Is Critical Infrastructure Protection (CIP)?* 7 March. https://www.fortinet.com/resources/cyberglossary/critical-infrastructure-protection.

Gatlan, Sergiu. 2022. 10 11. Πρόσβαση 11 20, 2022. https://www.bleepingcomputer.com/news/security/russian-military-hackers-linked-to-ransomware-attacks-in-ukraine/.

2022. «Intrusion Detection System (IDS).» *checkpoint.com.* 28 March. https://www.checkpoint.com/cyber-hub/network-security/what-is-an-intrusion-detection-system-ids/.

2022. «Intrusion Prevention System – IPS.» *checkpoint.com.* 28 March. https://www.checkpoint.com/cyber-hub/network-security/what-is-ips/.

2021. *JBS S.A. cyberattack.* 21 September. https://en.wikipedia.org/wiki/JBS_S.A._cyberattack.

Johnson, Joseph. 2021. *Ransomware - statistics & facts.* 09 September. https://www.statista.com/topics/4136/ransomware/#topicHeader__wrapper.

Kaduri, Bar. 2022. *Cyber Attacks in Russia's Invasion of Ukraine: Orca Security Research Pod Perspectives.* 11 March. Πρόσβαση November 20, 2022. https://orca.security/resources/blog/ukraine-orca-security-research-pod-perspectives/.

Kurt, Baker. 2022. *Ransomware as a Service (RaaS) Explained.* 7 February. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/.

Liviu, Arsene. 2022. *The Importance of Critical Infrastructure Security.* 7 March. https://www.cipsec.eu/content/importance-critical-infrastructure-security.

2022. *Malware.* 19 March. https://en.wikipedia.org/wiki/Malware.

Melnyczuk, Fred. 2021. *Famous Ransomware Attacks.* 24 December. https://antivirus.com/2021/12/24/famous-ransomware-attacks/.

Michael, Gregg. 2006. «Layer 8: The People Layer.» Στο *Hack the Stack*, 362. Elsevier.

Micro, Trend. 2017. *Massive WannaCry/Wcry Ransomware Attack Hits Countries.* 12 May. https://www.trendmicro.com/en_us/research/17/e/massive-wannacrywcry-ransomware-attack-hits-various-countries.html.

microsoft.com. 2022. *What is ransomware.* 27 10. https://learn.microsoft.com/en-us/security/compass/human-operated-ransomware.

Nakamoto, Satoshi. 2008. «Bitcoin: A Peer-to-Peer Electronic Cash System.» https://bitcoinwhitepaper.co/bitcoin.pdf.

2022. *NotPetya.* 13 March. https://www.hypr.com/notpetya/.

2022. *Petya and NotPetya.* 11 March. https://en.wikipedia.org/wiki/Petya_and_NotPetya.

2022. *Phishing.* 20 March. https://www.eset.com/gr/phishing/.

2022. *Ransomware.* 08 March. https://en.wikipedia.org/wiki/Ransomware.

2020. *Ransomware Evolved: Double Extortion.* 16 April. https://research.checkpoint.com/2020/ransomware-evolved-double-extortion/.

Robinson, Scott. 2017. *Python Circular Imports Module: Solving Circular Import Problem.* 17 October. Πρόσβαση 11 20, 2022. https://stackabuse.com/python-circular-imports/.

Rochberger, Lior. 2021. *cybereason.com.* 12 01. Πρόσβαση 12 01, 2022. https://www.cybereason.com/blog/research/cybereason-vs.-conti-ransomware.

Seqrite. 2019. «What is the kill chain and the seven steps involved in it? .» *seqrite.com.* 11 October. https://www.seqrite.com/blog/seven-phases-of-a-cyberattack/.

Shacklett, Mary E. 2021. *Definition: Attack Vector .* 1 April. https://www.techtarget.com/searchsecurity/definition/attack-vector.

Siddiqui, Naila Saad. 2022. *Use Global Variables Across Multiple Files in Python.* 16 September. Πρόσβαση 11 20, 2022. https://www.delftstack.com/howto/python/python-global-variable-across-files/.

2022. *Social engineering (security).* 18 March. https://en.wikipedia.org/wiki/Social_engineering_(security).

2020. *Software bug.* 02 March. https://el.wikipedia.org/wiki/Software_bug.

Sonicwall. 2022. *2022 Cyber Threat Report.* https://www.sonicwall.com/2022-cyber-threat-report/.

Spitzner , Lance. 2019. *Applying Security Awareness to the Cyber Kill Chain.* 31 May. https://www.sans.org/blog/applying-security-awareness-to-the-cyber-kill-chain/.

Stouffer, Clare. 2021. «Types of ransomware to recognize + ransomware protection tips.» *norton.com.* 24 November. https://us.norton.com/internetsecurity-malware-types-of-ransomware.html.

Strom, David. 2021. *The rise of ransomware as a service.* 25 March. https://blog.avast.com/ransomware-as-a-service-avast.

2022. *The History of Ransomware.* 20 March. https://ransomware.org/what-is-ransomware/the-history-of-ransomware/#locky-and-friends.

2022. *The NHS cyber attack.* 12 March. https://www.acronis.com/en-us/articles/nhs-cyber-attack/.

Trendmicro. 2022. *trendmicro.com.* 03 March. Πρόσβαση 11 20, 2022. https://www.trendmicro.com/en_us/research/22/c/cyberattacks-are-prominent-in-the-russia-ukraine-conflict.html.

trendmicro.com. χ.χ. *Spear phishing.* https://www.trendmicro.com/vinfo/us/security/definition/spear-phishing.

2022. «Types of Ransomware.» *geeksforgeeks.org.* 06 March. https://www.geeksforgeeks.org/types-of-ransomware/.

2022. *WannaCry.* 12 March. https://www.hypr.com/wannacry/.

wikepidia.org. 2021. *AIDS Trojan_horse.* 19 October. https://en.wikipedia.org/wiki/AIDS_(Trojan_horse).

Wikipedia. 2022. *2022 Ukraine cyberattacks.* 02 November. Πρόσβαση 11 20, 2022. https://en.wikipedia.org/wiki/2022_Ukraine_cyberattacks.

wikipedia. 2022. *Blockchain.* 09 March. https://en.wikipedia.org/wiki/Blockchain.

wikipedia.org. 2022. *WannaCry ransomware attack.* 10 March. https://en.wikipedia.org/wiki/WannaCry_ransomware_attack.

Zelleke , Liku. 2021. «The 8 Best OSINT Tools.» *comparitech.com.* 05 February. https://www.comparitech.com/net-admin/osint-tools/.