

ΙΟΝΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ



IONIAN
UNIVERSITY

-- Πτυχιακή Εργασία --

Δημιουργία Playbook για την διαχείριση περιστατικών
ασφαλείας ransomware

Άγγελος Βαρότσης

Επιβλέπων Καθηγητής: – Εμμανουήλ Μάγκος –

Επιβλέπων

Εμμανουήλ Μάγκος, Καθηγητής,
Ιόνιο Πανεπιστήμιο

Τριμελής Επιτροπή

Εμμανουήλ Μάγκος, Καθηγητής,
Ιόνιο Πανεπιστήμιο

Χριστόφορος Νταντογιάν, Επίκουρος Καθηγητής,
Ιόνιο Πανεπιστήμιο

Αγγελική Τσώχου, Αναπληρώτρια Καθηγήτρια,
Ιόνιο Πανεπιστήμιο

Περίληψη

Σε μια εποχή που χαρακτηρίζεται από το χάος των απειλών ransomware και την επιτακτική ανάγκη για προληπτικά μέτρα κυβερνοασφάλειας, η δημιουργία ενός εγχειριδίου ransomware αναδεικνύεται ως απαραίτητο εργαλείο για τη διασφάλιση της ασφάλειας ενός οργανισμού. Η παρούσα πτυχιακή περιγράφει την ανάπτυξη και την εφαρμογή ενός ολοκληρωμένου εγχειριδίου προσαρμοσμένου για τις επιχειρήσεις. Αξιοποιώντας βασικά εργαλεία κυβερνοασφάλειας, σε συνδυασμό με τεχνική ανάλυση, με στόχο την ενίσχυση της οργανωτικής ανθεκτικότητας έναντι επιθέσεων ransomware.

Στο επίκεντρο της, βρίσκεται το εγχειρίδιο ransomware, το οποίο παρέχει αναλυτικές διαδικασίες σχολαστικά σχεδιασμένες για να ακολουθηθούν σε κάθε περιστατικό ασφαλείας ransomware. Το εγχειρίδιο όχι μόνο διευκρινίζει την ανατομία των περιστατικών ransomware, αλλά και δίνει στους οργανισμούς τη δυνατότητα να προσαρμόσουν και να χρησιμοποιούν πλαίσια τακτικής αντιμετώπισης προσαρμοσμένα στο μοναδικό προφίλ απειλών τους.

Τέλος, η παρούσα πτυχιακή υπογραμμίζει τη δυναμική φύση του εγχειριδίου για το ransomware, τονίζοντας το ρόλο του ως ένα έγγραφο που πρέπει να εξελίσσεται παράλληλα με το διαρκώς μεταβαλλόμενο τοπίο απειλών. Μέσω επαναλαμβανόμενων ενημερώσεων που ενημερώνονται από περιστατικά του πραγματικού κόσμου και τεχνικές αναλύσεις, το εγχειρίδιο πρέπει να παραμένει έτοιμο να αντιμετωπίσει τις αναδυόμενες παραλλαγές και τακτικές ransomware, εξασφαλίζοντας την ετοιμότητα και την ανθεκτικότητα του οργανισμού.

Πρόλογος και Ευχαριστίες

Με τις ραγδαίως αυξανόμενες απειλές στον κυβερνοχώρο, η ανάγκη για αποτελεσματικές αμυντικές στρατηγικές είναι πιο έντονη από ποτέ, ιδίως έναντι επιθέσεων Ransomware οι οποίες έχουν καταστροφικές συνέπειες. Κεντρικό σημείο της παρούσας πτυχιακής εργασίας είναι η δημιουργία ενός εγχειριδίου Ransomware Playbook προσαρμοσμένο σε επιχειρηματικό περιβάλλον για τον μετριασμό αυτών των επιθέσεων, το οποίο παρέχει πρακτικές, βήμα προς βήμα οδηγίες για τους οργανισμούς ώστε να ενισχύσουν την άμυνά τους και να αντιμετωπίζουν επιθέσεις Ransomware. Επιπλέον, αξιοποιούνται jupyter notebooks για την δημιουργία ενός εργαλείου ανάλυσης κακόβουλου λογισμικού το οποίο περιλαμβάνει ασκήσεις οι οποίες έχουν σχεδιαστεί για την περαιτέρω αξιοποίηση των δυνατοτήτων του εργαλείου.

Περιεχόμενα

1	Εισαγωγή	1
1.1	ΠΑΡΟΜΟΙΕΣ ΕΡΓΑΣΙΕΣ	2
1.2	ΣΥΝΕΙΣΦΟΡΑ	3
1.3	ΜΕΘΟΔΟΛΟΓΙΑ	4
1.4	ΔΟΜΗ ΤΗΣ ΕΡΓΑΣΙΑΣ	6
2	Συμπληρωματικά Έργα κυβερνοασφάλειας	7
2.1	ΤΙ ΕΙΝΑΙ ΤΑ SECURITY PLAYBOOKS?	7
2.1.1	Ορισμός και Επισκόπηση	7
2.1.2	Σκοπός και σημασία	8
2.1.3	Εξέλιξη	10
2.1.4	Προκλήσεις και περιορισμοί	11
2.2	MITRE ATT&CK FRAMEWORK	12
2.2.1	Επισκόπηση	12
2.2.2	Προσέγγιση στη δημιουργία εγχειριδίων με βάση το framework	14
2.2.3	Βασικές Συνεισφορές του MITRE	15
2.2.4	Αξιοποίηση του framework στην ανάπτυξη εγχειριδίων ransomware	16
2.3	SPLUNK	17
2.3.1	Επισκόπηση	17
2.3.2	Splunk και Security Playbooks	18
2.3.3	Το Splunk σε συνδυασμό με το Ransomware Playbook	20
2.4	THE HIVE PROJECT	22
2.4.1	Επισκόπηση	22
2.4.2	Βασικές Λειτουργίες	23

2.4.3	Ο Ρόλος του TheHive για την διαχείριση περιστατικών Ransomware	25
2.5	MISP	26
2.5.1	Overview	26
2.5.2	Αξιοποίηση του MISP στη δημιουργία εγχειριδίων και στον μετρισμό πιθανών IoCs και επιθέσεων.	27
2.5.3	Το MISP σε διαχείριση περιστατικού ασφαλείας Ransomware	29
3	Ransomware Playbook	30
3.1	ΠΕΔΙΟ ΕΦΑΡΜΟΓΗΣ ΚΑΙ ΣΤΟΧΟΣ	30
3.2	ΤΙ ΕΙΝΑΙ ΤΟ RANSOMWARE?	30
3.3	ΠΩΣ ΣΥΜΒΑΙΝΟΥΝ ΟΙ ΕΠΙΘΕΣΕΙΣ RANSOMWARE?	31
3.4	ΚΟΙΝΕΣ ΜΕΘΟΔΟΙ ΔΙΑΝΟΜΗΣ RANSOMWARE	33
3.5	ΔΙΑΔΙΚΑΣΙΑ ΔΙΕΡΕΥΝΗΣΗΣ	35
3.5.1	Προσδιορισμός του τύπου Ransomware	35
3.5.2	Scope and Impact	38
3.5.3	User Actions σε περίπτωση ενδείξεων Ransomware	39
3.6	ΜΕΤΡΑ ΑΠΟΚΑΤΑΣΤΑΣΗΣ	40
3.6.1	Στρατηγικές περιορισμού	40
3.6.2	Διαδικασία εξάλειψης	41
3.7	ΔΙΑΔΙΚΑΣΙΑ ΑΝΑΚΤΗΣΗΣ	42
4	Τεχνική Ανάλυση Κακόβουλου Λογισμικού	44
5	Συμπεράσματα	57
	Συντμήσεις	62
	Γλωσσάρι Ξενικών Όρων	64

Κατάλογος Σχημάτων

1.1	Methodology	4
2.2	AWS incident response principles and design goals	9
2.3	ATT&CK Matrix for Enterprise	13
2.4	Wannacry Ransomware, Techniques Used	16
2.5	Splunk Enterprise Security	18
2.6	List of Splunk Response Playbooks	19
2.7	Splunk Ransomware Playbook	21
2.8	TheHive Dashboard	22
2.9	TheHive Alert management	24
2.10	MISP — Current Threats	27
3.11	Ενδεικτικός κύκλος ζωής Ransomware	31
3.12	Ransom note, after the attack	32
3.13	MITRE ATT&CK Enterprise tactics	34
3.14	Ransom Note on a text file, Abysslocker	36
3.15	Uploading ransom note and chat URL	37
3.16	Detected as BlackMatter Ransomware	38
4.17	Key Validated	47
4.18	Δημιουργία YARA Rule	54
4.19	Τελικό Report με όλα τα ευρήματα	56

Κεφάλαιο 1

Εισαγωγή

Στον τομέα της κυβερνοασφάλειας, η ενσωμάτωση μιας φιλοσοφίας σχεδιασμού με επίκεντρο τον άνθρωπο είναι επιτακτικής ανάγκης για την αύξηση της αποτελεσματικότητας και της προσβασιμότητας των πρωτοκόλλων ασφαλείας. Μια τέτοια μεθοδολογία εκτείνεται πέρα από την απλή οχύρωση των υποδομών του κυβερνοχώρου έναντι τεχνικών ευπαθειών, δίνει έμφαση στην κρίσιμη αλληλεπίδραση μεταξύ ανθρώπινων παραγόντων και τεχνολογικών συστημάτων. Η διασφάλιση ότι τα μέτρα ασφαλείας δεν εξαρτώνται αποκλειστικά από τεχνολογικές λύσεις, αλλά είναι επίσης προσαρμοσμένα ώστε να προβλέπουν την ανθρώπινη αλληλεπίδραση και συμπεριφορά, είναι θεμελιώδους σημασίας για τη διαμόρφωση ενός ασφαλέστερου και προσαρμοσμένου στο χρήστη κυβερνοπεριβάλλοντος [16].

Επιπλέον, η σημασία της εμπειρίας του χρήστη στο πεδίο της κυβερνοασφάλειας είναι ύψιστης σημασίας. Ο στόχος είναι να αναπτυχθούν πρωτόκολλα ασφαλείας που δεν είναι απλώς ισχυρά και αξιόπιστα, αλλά και απλά και συναρπαστικά για τον χρήστη. Δανειζόμενοι καινοτόμες προσεγγίσεις από διάφορους κλάδους, όπως η μετεωρολογία και ο φαρμακευτικός τομέας, η ασφάλεια στον κυβερνοχώρο μπορεί να υιοθετήσει πρωτοποριακές στρατηγικές, όπως οι διαδραστικές οπτικοποιήσεις απειλών και οι αυτόνομοι μηχανισμοί προστασίας δεδομένων. Αυτές αποσκοπούν στο να προσφέρουν στους χρήστες μια πιο ολιστική και προσιτή εμπειρία ασφαλείας. Η απώτερη φιλοδοξία είναι να δημιουργηθούν λύσεις ασφαλείας που να συγχωνεύονται ευέλικτα με την καθημερινή ρουτίνα των χρηστών, ενισχύοντας την ευκολία τους και το συλλογικό πλαίσιο ασφαλείας, ενώ παράλληλα τους θωρακίζουν διακριτικά από τις πανταχού παρούσες απειλές στον κυβερνοχώρο[10].

Η συμβολή μας σε αυτόν τον τομέα έγκειται στην καινοτόμα προσέγγισή μας προς τον σχεδιασμό και την ανάπτυξη εγχειριδίων για την κυβερνοασφάλεια. Παρουσιάζουμε ένα ολοκληρωμένο πλαίσιο, το οποίο διασφαλίζει ότι δεν είναι απλώς ευανάγνωστα και γρήγορα εφαρμόσιμα, αλλά επίσης ενσωματώνονται αποτελεσματικά σε ευρύτερα σχέδια επιχειρησιακής συνέχειας, απευθυνόμενα τόσο σε τεχνικούς όσο και σε λιγότερο τεχνικούς ενδιαφερόμενους.

1.1 Παρόμοιες Εργασίες

Τα εγχειρίδια για την ασφάλεια στον κυβερνοχώρο έχουν σημειώσει μία σταθερή εξέλιξη από την ίδρυση τους, καθώς λειτουργούν ως πυξίδα στο συχνά αποπροσανατολιστικό τοπίο των περιστατικών ασφάλειας στον κυβερνοχώρο. Έχουν μετατραπεί από εξαντλητικά έγγραφα κειμένου σε πιο βελτιωμένους, πρακτικούς οδηγούς, με έμφαση στην προσβασιμότητα και τη χρησιμότητα σε πραγματικό χρόνο. Κατά τη διαδικασία αυτή, όχι μόνο έχουν μετριάσει την πολυπλοκότητα της αντιμετώπισης περιστατικών, αλλά και έχουν επιτρέψει στους οργανισμούς να ενεργούν γρήγορα και αποφασιστικά σε περιόδους κρίσης.

Τα πρώτα έργα, όπως το βιβλίο των Killcrece et al (2003) "Incident Management Playbooks: Μια νέα μέθοδος για αποτελεσματική αντιμετώπιση" έθεσαν τις βάσεις επισημαίνοντας την ανάγκη για μια συντονισμένη δομή στην αντιμετώπιση περιστατικών[13]. Αντίστοιχο έργο επαναλήφθηκε στις εργασίες των Tøndel et al. (2014) και Werlinger et al. (2009), δίνοντας έμφαση σε προσιτά και ρεαλιστικά σχέδια αντιμετώπισης συμβάντων[24][26].

Περίπου την ίδια εποχή, επικεντρώθηκαν γύρω από τη χρηστικότητα αυτών των εγχειριδίων σε σενάρια πραγματικού χρόνου. Οι εργασίες των Todorov και De Decker (2015) και του Bishop (2015) άρχισαν να υπαινίσσονται αυτή την αλλαγή [23][5]. Αυτοί οι πρώτοι κυματισμοί εξελίχθηκαν με την παρουσίαση από την Ομάδα Ετοιμότητας Έκτακτης Ανάγκης Υπολογιστών των Ηνωμένων Πολιτειών (US-CERT) του Εργαλείου Αξιολόγησης Κυβερνοασφάλειας (CSET) το 2016, το οποίο περιλάμβανε μια σειρά από προκαθορισμένα εγχειρίδια για διάφορες καταστάσεις στον κυβερνοχώρο[9].

Μέχρι το 2017, η προσέγγιση αυτή είχε αποκτήσει δυναμική. Όπως υποδηλώνει η εργασία των O’Gorman και McDonald, η εστίαση είχε σαφώς μετατοπιστεί προς την κατεύθυνση να καταστούν τα εγχειρίδια πιο φιλικά προς τον χρήστη και αποτελεσματικά[18]. Αυτό το κύμα συναντήθηκε σύντομα με ένα άλλο: την έλευση της αυτοματοποίησης στη δημιουργία

εγχειριδίων. Όπως φαίνεται στις εργασίες των Bertino και Ferrari (2018) και Barnum (2019), η αυτοματοποίηση αναγγέλθηκε ως εργαλείο για τη βελτίωση των χρόνων απόκρισης και τη μείωση του ανθρώπινου λάθους[3][2].

Στο τέλος της δεκαετίας, υπήρξε μια έξαρση των συζητήσεων γύρω από την ευρύτερη εφαρμογή και προσβασιμότητα των εγχειριδίων. Οι εργασίες των Haas et al. (2019), Lowe (2019) και Cortada and Gordon (2020) συνέβαλαν σημαντικά σε αυτές τις συζητήσεις[11][15][8]. Ο διάλογος άρχισε να εξετάζει τη δημιουργία εγχειριδίων από πολλαπλές οπτικές γωνίες, περιλαμβάνοντας τόσο τεχνικούς όσο και μη τεχνικούς ενδιαφερόμενους.

Ταυτόχρονα, η ιδέα της προσαρμογής των εγχειριδίων στις συγκεκριμένες ανάγκες ενός οργανισμού και της ενσωμάτωσής τους στα σχέδια επιχειρησιακής συνέχειας έγινε πιο διαδεδομένη, όπως φαίνεται στις εργασίες των Rajivan και Gonzalez (2020), Morgan (2020) και Shedden et al. (2020)[19][17][22]. Αυτή η ιδέα αντιπροσώπευε ένα ακόμη βήμα προς την κατεύθυνση της αύξησης της προσβασιμότητας και της προσαρμοστικότητας των εγχειριδίων στις μοναδικές ανάγκες ενός οργανισμού.

Πλεον, ο διάλογος γύρω από τα εγχειρίδια κυβερνοασφάλειας είχε φυσικά προχωρήσει ώστε να δοθεί προτεραιότητα στην προσαρμοστικότητα και τη διαισθητικότητα. Οι εργασίες των Bhattacharjee et al. και Scambray αποτελούν παράδειγμα αυτής της κατεύθυνσης[4][20]. Η πρόκληση ήταν τώρα να επινοηθούν εγχειρίδια που θα μπορούσαν να καλύψουν αποτελεσματικά και αποδοτικά διάφορες καταστάσεις, προσαρμόσιμα σε κάθε είδους απειλή.

Ο σταδιακός μετασχηματισμός των εγχειριδίων κυβερνοασφάλειας με την πάροδο των χρόνων αναδεικνύει την αυξανόμενη έμφαση στην προσβασιμότητα, την πρακτικότητα και την προσαρμοστικότητα. Η παρούσα πτυχιακή εργασία σκοπεύει να προωθήσει αυτόν τον συλλογισμό, με στόχο να προωθήσει τη δημιουργία και τη χρήση των εγχειριδίων.

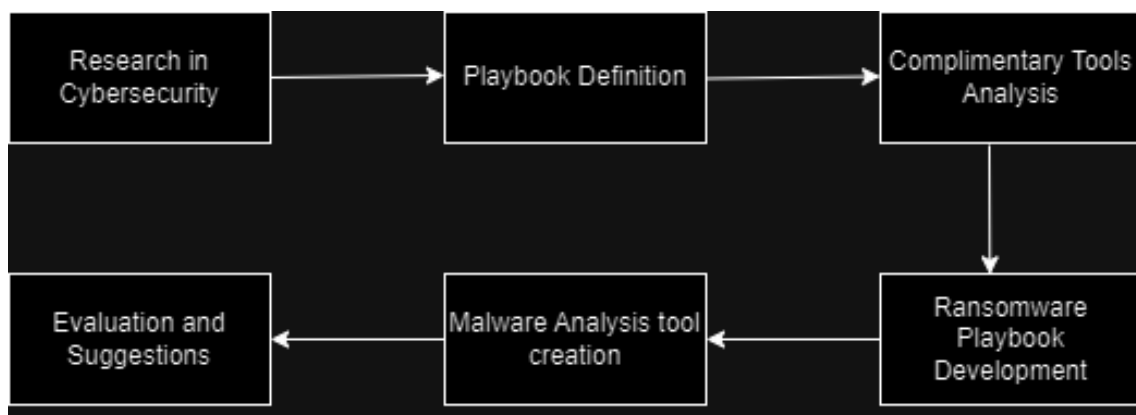
1.2 Συνεισφορά

Η παρούσα πτυχιακή συμβάλει σημαντικά στον τομέα της κυβερνοασφάλειας, αναφέροντας προβλήματα και περιορισμούς που προκύπτουν κατά την δημιουργία εγχειριδίων ασφαλείας, αναλύοντας συμπληρωματικά έργων που μπορούν να αξιοποιηθούν για τον μετρίασμό επιθέσεων σε συνδυασμό με τα εγχειρίδια ασφαλείας, με την δημιουργία ενός αναλυτικού *Ransomware Playbook* εξειδικευμένο για επιχειρησιακό περιβάλλον, με την ανάλυση κακόβουλου λογισμικού αξιοποιώντας *Jupyter notebooks* και τέλος με ασκήσεις που έχουν ως στόχο να

επεκτείνουν το συγκεκριμένο εργαλείο.

1.3 Μεθοδολογία

Η μεθοδολογία που αξιοποιήθηκε για την παρούσα πτυχιακή επικεντρώνεται βασικά στην αντιμετώπιση ενός συγκεκριμένου προβλήματος κυβερνοασφάλειας μέσω της δημιουργίας του εγχειριδίου Ransomware Playbook και την ανάπτυξη ενός αρχικού εργαλείου ανάλυσης κακόβουλου λογισμικού.



Σχήμα 1.1: Methodology

Αρχικά, η έρευνα ξεκίνησε με την οριοθέτηση της έννοιας των εγχειριδίων ασφαλείας και του αναπόσπαστου ρόλου τους στα πλαίσια της κυβερνοασφάλειας. Η κριτική εξέταση της υπάρχουσας βιβλιογραφίας αποκάλυψε τόσο τη σημασία όσο και τους περιορισμούς των σημερινών εφαρμογών των εγχειριδίων. Αυτή η θεμελιώδης κατανόηση έφερε στην επιφάνεια την ανάγκη να αναλύσουμε την ενσωμάτωση πρόσθετων πλαισίων, ιδίως του MITRE ATT&CK¹ και του MISP². Αυτά τα πλαίσια είναι αναπόσπαστα για την αναλυτική περιγραφή των τεχνικών των επιτιθέμενων και για τη συλλογή δεδομένων που σχετίζονται με απειλές.

Η πτυχιακή ενσωματώνει επίσης ενδελεχή ανάλυση των εργαλείων Splunk³ και TheHive-Project⁴. Το Splunk, ως εργαλείο διαχείρισης πληροφοριών και συμβάντων ασφαλείας

¹<https://attack.mitre.org>

²<https://www.misp-project.org>

³<https://www.splunk.com>

⁴<https://github.com/TheHive-Project/TheHive>

(SIEM), είναι απαραίτητο για την παρακολούθηση και την αντιμετώπιση πιθανών απειλών στον κυβερνοχώρο, ενώ το TheHiveProject χρησιμεύει ως πλατφόρμα αντιμετώπισης συμβάντων ασφαλείας (SIRP), διευκολύνοντας τη συντονισμένη αντιμετώπιση συμβάντων ασφαλείας. Η επιλογή αυτών των εργαλείων βασίστηκε στο αποδεδειγμένο ιστορικό τους και στις δυνατότητες συνέργειάς τους όταν ενσωματώνονται με το Ransomware Playbook.

Η φάση ανάπτυξης του Ransomware Playbook περιελάμβανε έναν σχολαστικό ορισμό του ransomware, παρακολουθώντας την πορεία τέτοιων επιθέσεων από την έναρξη έως την κλιμάκωση. Το εγχειρίδιο είναι δομημένο για να καθοδηγήσει τους επαγγελματίες της κυβερνοασφάλειας μέσω μιας συστηματικής αντιμετώπισης περιστατικών ransomware, που περιλαμβάνει την ανίχνευση, τη διερεύνηση, τον περιορισμό και την ανάκτηση. Αυτός ο ολοκληρωμένος οδηγός διαδικασιών αναπτύχθηκε μέσω ανάλυσης, διασφαλίζοντας ότι το εγχειρίδιο είναι πρακτικό και βασισμένο στην εφαρμογή στον πραγματικό κόσμο.

Στη συνέχεια, η πτυχιακή περιγράφει τη δημιουργία ενός εργαλείου αρχικής ανάλυσης κακόβουλου λογισμικού με τη χρήση σημειωματάρων Jupyter. Αυτό το εργαλείο ενσωματώνει διάφορες τεχνολογίες, συμπεριλαμβανομένων των VirusTotal⁵ και YARA⁶ Rules, και χρησιμοποιεί πρακτικές όπως το defanging και οι συναρτήσεις κατακερματισμού (hashes) για την ανάλυση ύποπτων αρχείων. Το εργαλείο αυτό αναπτύχθηκε ακολουθώντας μια προσέγγιση κατά την οποία η διαδικασία ανάπτυξης περιελάμβανε επαναληπτικούς κύκλους όπου αντιμετωπίστηκαν προκλήσεις όπως ζητήματα ενσωμάτωσης των τεχνολογιών, αναδεικνύοντας τις δεξιότητες επίλυσης προβλημάτων και προσαρμόζοντας το εργαλείο ώστε να ανταποκρίνεται καλύτερα στις ανάγκες της ανάλυσης. Να σημειωθεί ότι κάθε λειτουργία του κώδικα συνοδεύεται από μία ανάλογη άσκηση η οποία παρέχει εκπαιδευτικά οφέλη και δυνατότητες επέκτασης του εργαλείου με περισσότερες λειτουργίες.

Η αξιολόγηση αυτής της έρευνας παρουσιάζεται στο τελευταίο κεφάλαιο, αναλογιζόμενη την αποτελεσματικότητα των επιλεγμένων μεθοδολογιών και εργαλείων. Εκτιμάται κατά πόσον επιτεύχθηκαν οι στόχοι και πώς τα ευρήματα συμβάλλουν στον τομέα. Αυτό περιλαμβάνει μια κριτική ανάλυση του Ransomware Playbook και του εργαλείου ανάλυσης κακόβουλου λογισμικού, συζητώντας τις πρακτικές εφαρμογές τους και προτείνοντας μελλοντικές βελτιώσεις για την περαιτέρω επέκταση των δυνατοτήτων τους.

⁵<https://www.virustotal.com/gui/>

⁶<https://www.picussecurity.com/resource/glossary/what-is-a-yara-rule>

1.4 Δομή της Εργασίας

Στην ενότητα 2 ορίζουμε τι είναι τα security playbooks, τον σκοπό, τις προκλήσεις και περιορισμούς, και αναλύουμε τα συμπληρωματικά frameworks MITRE ATT&CK, MISP, Splunk και TheHiveProject. Στην συνέχεια στο κεφάλαιο 3 υπάρχει μια εξονυχιστική ανάλυση του Ransomware Playbook που δημιουργήσαμε, ξεκινώντας από τον ορισμό του μέχρι και την διαδικασία ανάκτησης από μία επίθεση. Στο κεφάλαιο 4 αναλύουμε και δημιουργούμε ένα εργαλείο αρχικής ανάλυσης κακόβουλου λογισμικού, το οποίο συνοδεύεται με ασκήσεις οι οποίες επεκτείνουν το εργαλείο με περαιτέρω λειτουργίες. Τέλος, στο κεφάλαιο 5 καταλήγουμε σε συμπεράσματα και δίνουμε ιδέες και μελλοντικές προοπτικές εξέλιξης.

Κεφάλαιο 2

Συμπληρωματικά Έργα κυβερνοασφάλειας

2.1 Τι είναι τα Security Playbooks?

2.1.1 Ορισμός και Επισκόπηση

Ένα εγχειρίδιο ασφάλειας στον κυβερνοχώρο είναι ένας γραπτός οδηγός που παρέχει σαφείς οδηγίες για τον τρόπο χειρισμού διαφόρων περιστατικών ασφάλειας. Τα εγχειρίδια σχεδιάζονται ώστε να διασφαλίζεται ότι μπορούν να ανταποκρίνονται σε περιστατικά με συνέπεια, ταχύτητα και αποτελεσματικότητα. Χρησιμοποιούν ως εγχειρίδια που περιγράφουν βήμα προς βήμα τις διαδικασίες για την αντιμετώπιση διαφόρων απειλών ασφαλείας, επιτρέποντας στην ομάδα να ανταποκρίνεται άμεσα και αποτελεσματικά[1].

Ο κύκλος ζωής περιλαμβάνει την προετοιμασία, την ανίχνευση, τον περιορισμό, την εξάλειψη, την αποκατάσταση και την εξαγωγή διδαγμάτων. Κάθε φάση περιλαμβάνει συγκεκριμένα καθήκοντα και τις απαραίτητες πληροφορίες για την εκτέλεση αυτών των καθηκόντων. Αξίζει να σημειωθεί ότι τα εγχειρίδια δεν είναι γενικά, είναι προσαρμοσμένα στην υποδομή κυβερνοασφάλειας ενός οργανισμού. Λαμβάνουν υπόψη τα μοναδικά εργαλεία, τις τεχνολογίες και τις διαδικασίες που χρησιμοποιεί ο οργανισμός, καθοδηγώντας ανάλογα τις δραστηριότητες αντιμετώπισης περιστατικών[7].

Τελικός στόχος για ένα εγχειρίδιο ασφαλείας είναι να παρέχει ένα ακριβές σχέδιο για τη διαχείριση και την ελαχιστοποίηση ενός περιστατικού ασφαλείας, συμβάλλοντας στη μείωση

του ανθρώπινου λάθους, εξασφαλίζοντας άμεσες αντιδράσεις και τελικά μειώνοντας τη ζημία και τον χρόνο αποκατάστασης που προκαλούν οι παραβιάσεις ασφαλείας, καθορίζοντας εκ των προτέρων τις αντιδράσεις.

2.1.2 Σκοπός και σημασία

Σε αυτή την εποχή των διαρκώς εξελισσόμενων απειλών στον κυβερνοχώρο, οι οργανισμοί έχουν ανάγκη από ισχυρές, αξιόπιστες και απολύτως αποτελεσματικές στρατηγικές για να αντιμετωπίσουν το ενδεχόμενο περιστατικών.

Τα εγχειρίδια, στην ουσία τους, έχουν ως στόχο να είναι κάτι περισσότερο από ένα σύνολο κανόνων- προσπαθούν να αποτελέσουν τους οδηγούς στο τεράστιο και ενίοτε μπερδεμένο χάος των περιστατικών κυβερνοασφάλειας. Φανταστείτε τους ως οδικό χάρτη, που σας βοηθά να περιηγηθείτε στον ψηφιακό κόσμο όταν έρχεστε αντιμέτωποι με πιθανές παραβιάσεις ή απειλές. Είναι σαν τους καθοδηγητές του τοπίου της κυβερνοασφάλειας, επισημαίνοντας τα σημάδια του προβλήματος και δείχνοντας το δρόμο για άμεσες και επακόλουθες ενέργειες.

Αποτελούν τη βάση στην αντιμετώπιση περιστατικών ασφαλείας. Ουσιαστικά, οποιοδήποτε μέλος μιας ομάδας ασφαλείας, ανεξάρτητα από το επίπεδο της εξειδίκευσής του, συμβουλευέται το εγχειρίδιο και βρίσκεται σε γνώριμο έδαφος, γνωρίζοντας τα ακριβή βήματα για να αντιμετωπίσει ένα περιστατικό. Αυτό όχι μόνο διασφαλίζει ότι όλοι βαδίζουν στο ίδιο μονοπάτι, αλλά μειώνει επίσης σημαντικά τις πιθανότητες να παραλείπονται κρίσιμα βήματα, ειδικά όταν το άγχος και η αβεβαιότητα ξεκινούν κατά τη διάρκεια μιας κρίσης.

Επόμενο θέμα συζήτησης είναι η ενίσχυση της αποτελεσματικότητας που παρέχουν τα εγχειρίδια ασφαλείας στη διαδικασία αντιμετώπισης συμβάντων. Ο χρόνος αποτελεί κρίσιμο παράγοντα κατά τη διάρκεια περιστατικών ασφαλείας και η άμεση εκτέλεση των ενεργειών αντιμετώπισης είναι υψίστης σημασίας. Με σαφώς περιγραφόμενα βήματα και διαδικασίες, τα εγχειρίδια μειώνουν σημαντικά τον χρόνο που δαπανάται για τον προσδιορισμό της βέλτιστης πορείας δράσης. Αυτό έχει ως αποτέλεσμα τον ταχύτερο περιορισμό και την ταχύτερη επίλυση των περιστατικών ασφαλείας.

Τα εγχειρίδια διαδραματίζουν καθοριστικό ρόλο στον μετριασμό των κινδύνων και στη μείωση των πιθανών απωλειών που σχετίζονται με περιστατικά ασφαλείας. Διατυπώνοντας τις διαδικασίες βέλτιστης πρακτικής για διάφορα σενάρια συμβάντων, τα εγχειρίδια αυτά επιτρέπουν στους οργανισμούς να προετοιμάζονται προληπτικά για τα συμβάντα και να τα αντιμετωπίζουν, ελαχιστοποιώντας έτσι τις συνολικές επιπτώσεις τους.

Για παράδειγμα, όπως φαίνεται και στην εικόνα 2.2, το incident response guide της amazon για το AWS (Amazon Web Services)[21] σε αυτό το σημείο δίνει μία λίστα με προληπτικά βήματα και βέλτιστες πρακτικές για την ελαχιστοποίηση των απειλών στον κυβερνοχώρο μέσω γενικών διαδικασιών οι οποίες είναι εξιδικευμένες για τις cloud υπηρεσίες.

- **Establish response objectives** – Work with stakeholders, legal counsel, and organizational leadership to determine the goal of responding to an incident. Some common goals include containing and mitigating the issue, recovering the affected resources, preserving data for forensics, returning to known safe operations, and ultimately learning from incidents.
- **Respond using the cloud** – Implement response patterns within the cloud, where the event and data occurs.
- **Know what you have and what you need** – Preserve logs, resources, snapshots, and other evidence by copying and storing them in a centralized cloud account dedicated to response. Use tags, metadata, and mechanisms that enforce retention policies. You'll need to understand what

AWS incident response principles and design goals
4

AWS Security Incident Response Guide
AWS Technical Guide

services you use and then identify requirements for investigating those services. To help you understand your environment, you can also use tagging, which is covered later in this document in the [the section called “Develop and implement a tagging strategy”](#) section.

- **Use redeployment mechanisms** – If a security anomaly can be attributed to a misconfiguration, the remediation might be as simple as removing the variance by redeploying resources with the proper configuration. If a possible compromise is identified, verify that your redeployment includes successful and verified mitigation of the root causes.
- **Automate where possible** – As issues arise or incidents repeat, build mechanisms to programmatically triage and respond to common events. Use human responses for unique, complex, or sensitive incidents where automations are insufficient.
- **Choose scalable solutions** – Strive to match the scalability of your organization's approach to cloud computing. Implement detection and response mechanisms that scale across your environments to effectively reduce the time between detection and response.

Σχήμα 2.2: *AWS incident response principles and design goals*

Επιπλέον, συμβάλλουν στην κανονιστική συμμόρφωση, παρέχοντας σαφή τεκμηρίωση των προληπτικών προσπάθειών ενός οργανισμού για τη διατήρηση της συμμόρφωσης με τους κανονισμούς για την ασφάλεια δεδομένων και την αντιμετώπιση παραβιάσεων. Πολλοί κλάδοι υπόκεινται σε αυστηρές κανονιστικές απαιτήσεις, και ένα καλά σχεδιασμένο εγχειρίδιο μπορεί να χρησιμεύσει ως απόδειξη της δέσμευσης ενός οργανισμού για την τήρηση αυτών των

προτύπων.

Τέλος, τα εγχειρίδια διευκολύνουν την οργανωτική μάθηση και τη συνεχή βελτίωση των πρακτικών κυβερνοασφάλειας. Πέρα από την καθοδήγηση της άμεσης απόκρισης σε ένα περιστατικό, βοηθούν στον εντοπισμό κενών και περιοχών προς βελτίωση μετά το περιστατικό, προωθώντας έναν συνεχή κύκλο μάθησης και βελτίωσης των πρακτικών κυβερνοασφάλειας.

2.1.3 Εξέλιξη

Ακριβώς όπως το τοπίο των απειλών κυβερνοασφάλειας έχει εξελιχθεί σημαντικά με την πάροδο του χρόνου, έτσι έχουν εξελιχθεί και τα εγχειρίδια που χρησιμοποιούνται για τον μετριασμό αυτών των απειλών.

Στα πρώτα στάδια της ασφάλειας στον κυβερνοχώρο, η αντιμετώπιση περιστατικών ήταν συχνά μια αντιδραστική διαδικασία. Οι εταιρείες βασιζόνταν σε μεγάλο βαθμό σε *ad hoc* μέτρα, διαχειρίζοντας τα περιστατικά ανάλογα με την εμφάνισή τους, χωρίς να υπάρχουν τυποποιημένες διαδικασίες. Κατά τη διάρκεια αυτής της περιόδου, τα εγχειρίδια ασφαλείας ήταν ουσιαστικά ανύπαρκτα ή, στην καλύτερη περίπτωση, πολύ υποτυπώδη[14].

Καθώς το τοπίο των απειλών στον κυβερνοχώρο γινόταν όλο και πιο σύνθετο, με την εμφάνιση προηγμένων μόνιμων απειλών, ransomware και εξελιγμένων επιθέσεων, έγινε εμφανής η ανάγκη για μια πιο δομημένη και οργανωμένη προσέγγιση στην αντιμετώπιση περιστατικών. Αυτό σηματοδότησε τη γέννηση του σύγχρονου εγχειριδίου ασφαλείας[25].

Ως απάντηση στην ταχεία εξέλιξη των απειλών στον κυβερνοχώρο, τα εγχειρίδια ασφαλείας έπρεπε να γίνουν πιο δυναμικά, προσαρμόσιμα και ολοκληρωμένα. Καλύπτοντας πλέον ένα ευρύτερο φάσμα πιθανών περιστατικών, με ευέλικτες διαδικασίες που μπορούν να προσαρμόζονται με βάση τις ιδιαιτερότητες της απειλής. Τα εγχειρίδια έχουν γίνει πλέον πιο λεπτομερή, καλύπτοντας όχι μόνο τεχνικά θέματα αλλά και στοιχεία όπως η επικοινωνία, η λήψη αποφάσεων και η κανονιστική συμμόρφωση.

Με την άνοδο της αυτοματοποίησης, τα σημερινά προηγμένα playbooks μπορούν να ενσωματωθούν με πλατφόρμες ενορχήστρωσης, αυτοματοποίησης και απόκρισης ασφάλειας (SOAR). Αυτό επιτρέπει την αυτοματοποίηση ορισμένων καθηκόντων ρουτίνας, ενισχύοντας την ταχύτητα και την αποτελεσματικότητα της αντιμετώπισης περιστατικών. Η εξέλιξη των εγχειριδίων ασφαλείας αποτελεί απόδειξη της προσαρμοστικότητας και της ανθεκτικότητας του τομέα της ασφάλειας στον κυβερνοχώρο[12].

2.1.4 Προκλήσεις και περιορισμοί

Παρόλο που τα εγχειρίδια ασφαλείας αποτελούν κρίσιμο στοιχείο αποτελεσματικών στρατηγικών κυβερνοασφάλειας, η δημιουργία και η εφαρμογή τους δεν είναι χωρίς προκλήσεις και περιορισμούς[6]. Πιο συγκεκριμένα:

1. **Εξελισσόμενες απειλές:** Μία από τις μεγαλύτερες προκλήσεις στη δημιουργία εγχειριδίων ασφαλείας είναι η διατήρησή τους σε επαφή με το διαρκώς εξελισσόμενο τοπίο απειλών. Νέες απειλές και φορείς επιθέσεων εμφανίζονται τακτικά και τα εγχειρίδια πρέπει να ενημερώνονται αναλόγως για να διασφαλιστεί ότι παραμένουν αποτελεσματικά. Αυτό απαιτεί συνεχή παρακολούθηση και ευαισθητοποίηση σχετικά με τις τελευταίες απειλές, καθώς και τακτική αναθεώρηση και ενημέρωση των εγχειριδίων.
2. **Πολυπλοκότητα και σαφήνεια:** Ένα καλό εγχειρίδιο ασφάλειας πρέπει να επιτυγχάνει μια λεπτή ισορροπία μεταξύ λεπτομέρειας και απλότητας. Πρέπει να είναι αρκετά λεπτομερές ώστε να καλύπτει όλες τις απαραίτητες ενέργειες και απρόβλεπτες καταστάσεις, αλλά αρκετά σαφές και απλό ώστε να μπορούν να το κατανοήσουν και να το ακολουθήσουν μέλη της ομάδας με διαφορετικά επίπεδα εξειδίκευσης. Η επίτευξη αυτής της ισορροπίας μπορεί να αποτελέσει πρόκληση.
3. **Περιορισμοί πόρων:** Η ανάπτυξη, η ενημέρωση και η συντήρηση των εγχειριδίων ασφαλείας μπορεί να είναι πιεστική σε πόρους. Απαιτείται σημαντική επένδυση χρόνου και εμπειρογνωμοσύνης, η οποία μπορεί να αποτελέσει πρόκληση για οργανισμούς με περιορισμένους πόρους κυβερνοασφάλειας.
4. **Ενσωμάτωση με υφιστάμενα συστήματα και διαδικασίες:** Ένα εγχειρίδιο πρέπει να ευθυγραμμίζεται με τις υπάρχουσες τεχνολογίες, τα εργαλεία, τις διαδικασίες και τη συνολική στρατηγική κυβερνοασφάλειας ενός οργανισμού. Αυτό απαιτεί βαθιά κατανόηση της υποδομής του οργανισμού και μπορεί να είναι ένα πολύπλοκο έργο, ιδίως σε μεγάλους οργανισμούς ή σε οργανισμούς με πολύπλοκα περιβάλλοντα IT.
5. **Δοκιμές και επικύρωση:** Για να διασφαλιστεί ότι ένα εγχειρίδιο είναι αποτελεσματικό, πρέπει να δοκιμάζεται τακτικά μέσω ασκήσεων, όπως προσομοιώσεις περιστατικών. Αυτό μπορεί να είναι χρονοβόρο και απαιτεί συνεχή δέσμευση από όλα τα εμπλεκόμενα μέρη.

6. **Ανθρώπινος παράγοντας:** Ακόμη και το καλύτερα σχεδιασμένο εγχειρίδιο μπορεί να αποτύχει εάν δεν εκτελεστεί σωστά. Αυτό μπορεί να οφείλεται σε έλλειψη εκπαίδευσης ή ευαισθητοποίησης, σε αντίσταση στην τήρηση των διαδικασιών ή σε απλό ανθρώπινο λάθος. Η διασφάλιση ότι όλα τα μέλη της ομάδας είναι επαρκώς εκπαιδευμένα και ασχολούνται με τα εγχειρίδια είναι ζωτικής σημασίας, αλλά μπορεί να αποτελέσει πρόκληση.

Παρά τις προκλήσεις αυτές, τα οφέλη από την ύπαρξη ενός καλά σχεδιασμένου εγχειριδίου ασφαλείας είναι τεράστια. Είναι σημαντική η προσέγγιση στην ανάπτυξη και την εφαρμογή των εγχειριδίων ασφαλείας ως μια συνεχή, εξελισσόμενη διαδικασία με την απαραίτητη επένδυση στους απαραίτητους πόρους για την αντιμετώπιση αυτών των προκλήσεων, ώστε να δημιουργηθεί ένα αποτελεσματικό, αξιόπιστο εργαλείο για την αντιμετώπιση περιστατικών.

2.2 MITRE ATT&CK Framework

2.2.1 Επισκόπηση

Το MITRE ATT&CK Framework, αποτελεί αναπόσπαστο κομμάτι στον τομέα της κυβερνοασφάλειας, προσφέροντας μια ολοκληρωμένη βάση γνώσεων που βασίζεται σε πραγματικές παρατηρήσεις των τακτικών και τεχνικών των επιτηθέμενων. Το framework είναι σχεδιασμένο για να ενισχύει τις δυνατότητες ανίχνευσης επιτηθέμενων στον κυβερνοχώρο μετά την παραβίαση, παρουσιάζοντας μια τακτική πλεονεκτική θέση προς τις κακόβουλες συμπεριφορές, η οποία ενισχύει σημαντικά την ικανότητα των επαγγελματιών της κυβερνοασφάλειας να εντοπίζουν και να αντιμετωπίζουν τις επιθέσεις στον κυβερνοχώρο.

Το ATT&CK Matrix for Enterprise αναπτύχθηκε για να περιγράψει τις ενέργειες στις οποίες μπορεί να προβούν οι επιτιθέμενοι κατά την επίθεση τους σε ένα επιχειρησιακό δίκτυο. Χρησιμεύει ως ένα ολοκληρωμένο repository των τακτικών και τεχνικών των επιτιθέμενων που βασίζονται σε παρατηρήσεις του πραγματικού κόσμου.

Ο πίνακας χωρίζεται σε στήλες, καθεμία από τις οποίες αντιπροσωπεύει ένα διαφορετικό στάδιο του κύκλου ζωής ενός επιτιθέμενου ή τους διαφορετικούς στόχους που μπορεί να επιδιώκει να επιτύχει. Πιο συγκεκριμένα, περιλαμβάνει αλλά δεν περιορίζεται στα παρακάτω:

Reconnaissance: Τεχνικές που χρησιμοποιούνται για τη συλλογή πληροφοριών σχετικά με το δίκτυο ή τον οργανισμό-στόχο. Αυτό μπορεί να περιλαμβάνει δραστηριότητες όπως η

ATT&CK Matrix for Enterprise								
layout: flat ▾ show sub-techniques hide sub-techniques								
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques
Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (4) Search Closed	Acquire Access Acquire Infrastructure (8) Compromise Accounts (3) Compromise Infrastructure (7) Develop Capabilities (4) Establish Accounts (3) Obtain Capabilities (6)	Content Injection Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (4) Replication Through	Cloud Administration Command Command and Scripting Interpreter (9) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (3)	Account Manipulation (8) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Browser Extensions Compromise Client Software Binary	Abuse Elevation Control Mechanism (5) Access Token Manipulation (5) Account Manipulation (6) Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5)	Abuse Elevation Control Mechanism (5) Access Token Manipulation (5) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access	Adversary-in-the-Middle (3) Brute Force (4) Credentials from Password Stores (6) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2)	Account Discovery (4) Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object Discovery Container and Resource

Σχήμα 2.3: ATT&CK Matrix for Enterprise

ενεργή σάρωση ή η συλλογή πληροφοριών από δημόσια διαθέσιμες πηγές.

Resource Development: Τεχνικές που περιλαμβάνουν τη δημιουργία, την αγορά ή την κλοπή πόρων που μπορεί να χρησιμοποιήσει ο επιτιθέμενος στις επιχειρήσεις του, όπως η απόκτηση παραβιασμένων λογαριασμών.

Initial Access: Τεχνικές που επιτρέπουν στους επιτιθέμενους να αποκτήσουν αρχικό πάτιμα στο δίκτυο. Οι μέθοδοι μπορεί να περιλαμβάνουν την εκμετάλλευση τρωτών σημείων σε εφαρμογές με δημόσια πρόσβαση, τη χρήση spear phishing ή την εκμετάλλευση απομακρυσμένων υπηρεσιών.

Execution: Τεχνικές που χρησιμοποιούνται για την εκτέλεση κακόβουλου κώδικα σε ένα σύστημα. Περιλαμβάνει μεθόδους όπως η χρήση exploitation εργαλείων.

Persistence: Τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να διατηρήσουν τα πατίματα τους. Αυτό περιλαμβάνει μεθόδους όπως η δημιουργία νέων λογαριασμών χρηστών ή τροποποίηση αρχείων συστήματος.

Privilege Escalation: Τεχνικές που χρησιμοποιούνται για την απόκτηση δικαιωμάτων υψηλότερου επιπέδου σε ένα σύστημα. Οι μέθοδοι περιλαμβάνουν την παράκαμψη του ελέγχου λογαριασμού χρήστη ή την εκμετάλλευση ευπαθειών.

Defense Evasion: Τεχνικές που χρησιμοποιούν οι επιτιθέμενοι για να αποφύγουν την ανίχνευση. Αυτό περιλαμβάνει την απόκρυψη αρχείων, την απενεργοποίηση εργαλείων ασφαλείας ή τη χρήση obfuscated κώδικα.

Credential Access: Τεχνικές που χρησιμοποιούνται για την κλοπή κωδικών, όπως ονόματα χρηστών και κωδικούς πρόσβασης. Αυτό μπορεί να επιτευχθεί μέσω keylogging, credential dumping ή phishing.

Discovery: Τεχνικές που επιτρέπουν στους επιτιθέμενους να συλλέγουν πληροφορίες σχετικά με το σύστημα και το εσωτερικό δίκτυο. Αυτό περιλαμβάνει σάρωση δικτύου, αναζήτηση πληροφοριών συστήματος και εντοπισμό αρχείων και καταλόγων.

2.2.2 Προσέγγιση στη δημιουργία εγχειριδίων με βάση το framework

Στην αναζήτηση ισχυρών εργαλείων ασφάλειας, το πλαίσιο ATT&CK της MITRE αποτελεί ένα αναμφίβολα σημαντικό και ξεχωριστό μοντέλο ανίχνευσης και διαχείρισης απειλών συμπεριφοράς όπου τα βασικά χαρακτηριστικά του είναι τα εξής:

1. **Behavioral Insights:** Το κεντρικό στοιχείο της φιλοσοφίας του πλαισίου ATT&CK είναι η έμφαση στη συμπεριφορά των επιτιθέμενων, η μετάβαση από την παραδοσιακή ανίχνευση βάσει υπογραφής σε μια πιο διαφοροποιημένη κατανόηση της συμπεριφοράς των επιτιθέμενων. Επιτρέπει τον εντοπισμό κακόβουλων δραστηριοτήτων μέσω της αναγνώρισης προτύπων, ανεξάρτητα από την καινοτομία της επίθεσης.
2. **Χαρτογράφηση κύκλου ζωής για προληπτική άμυνα:** Το πλαίσιο προσφέρει ένα χρονολογικό σχεδιάγραμμα της εξέλιξης μιας κυβερνοεπίθεσης, επιτρέποντας στις ομάδες ασφαλείας να προβλέπουν και να αντιμετωπίζουν τις επόμενες φάσεις της επίθεσης. Αυτή η χαρτογράφηση του κύκλου ζωής χρησιμεύει ως θεμέλιο για τη δόμηση του εγχειριδίου, προσφέροντας μια σταδιακή στρατηγική αντιμετώπισης περιστατικών.
3. **Εξαντλητικός κατάλογος τακτικών και τεχνικών:** Με τη λεπτομερή συλλογή των τακτικών και τεχνικών των επιτιθέμενων, το ATT&CK παρέχει στις ομάδες αξιοποιήσιμες πληροφορίες σχετικά με τις στρατηγικές ανίχνευσης και μετριάσμού, προωθώντας μια ολοκληρωμένη αμυντική στάση.
4. **Εξέλιξη με γνώμονα την κοινότητα:** Η ζωτικότητα του πλαισίου διατηρείται μέσω των συνεχών συνεισφορών της κοινότητας, διασφαλίζοντας ότι τα εγχειρίδια εξακολουθούν να αντικατοπτρίζουν τις τελευταίες τακτικές των επιτιθέμενων στον κυβερνοχώρο.

5. **Ανάλυση στρατηγικών κενών:** Η αξιοποίηση του ATT&CK για την ανάλυση κενών φωτίζει τα τρωτά σημεία της άμυνας, επιτρέποντας στους οργανισμούς να προσαρμόσουν τα εγχειρίδια ασφαλείας τους ώστε να αντιμετωπίσουν και να ιεραρχήσουν αποτελεσματικά αυτές τις αδυναμίες.

Με την ενσωμάτωση αυτών των αρχών στον ιστό της ανάπτυξης εγχειριδίων ασφαλείας, το πλαίσιο ATT&CK της MITRE εφοδιάζει τους οργανισμούς με ένα στρατηγικό, συμπεριφορικό σχέδιο για την ενίσχυση της ανθεκτικότητας στον κυβερνοχώρο.

2.2.3 Βασικές Συνεισφορές του MITRE

Η επιρροή του πλαισίου ATT&CK της MITRE στην ασφάλεια στον κυβερνοχώρο είναι σημαντική και χαρακτηρίζεται από διάφορες καίριες συνεισφορές:

1. **Ενοποιημένη βάση γνώσης των επιθέσεων:** Η βάση του ATT&CK χρησιμεύει ως εγκυκλοπαιδική αναφορά των τακτικών και τεχνικών των επιτιθέμενων στον κυβερνοχώρο, ανεκτίμητη για τη διαμόρφωση τεκμηριωμένων αμυντικών στρατηγικών.
2. **Παγκόσμια συνεργατική πλατφόρμα:** Η MITRE έχει προωθήσει ένα παγκόσμιο δίκτυο επαγγελματιών της κυβερνοασφάλειας, εξασφαλίζοντας την ευελιξία και τη συνάφεια του πλαισίου, ώστε να συμβαδίζει με το εξελισσόμενο τοπίο των απειλών στον κυβερνοχώρο.
3. **Τυποποιημένο λεξικό κυβερνοασφάλειας:** Το ATT&CK έχει διαδραματίσει καθοριστικό ρόλο στην εναρμόνιση του λόγου για την κυβερνοασφάλεια, διευκολύνοντας την ενισχυμένη συνεργασία και κατανόηση μεταξύ των οργανισμών.
4. **Σχέδιο για συνεχή βελτίωση της ασφάλειας:** Το πλαίσιο χρησιμεύει ως οδικός χάρτης για τον εντοπισμό και την αντιμετώπιση των κενών στην κατάσταση ασφαλείας, καθοδηγώντας συστηματικές βελτιώσεις.
5. **Ενσωμάτωση εργαλείων και υπηρεσιών:** Η ενσωμάτωση του ATT&CK σε διάφορες λύσεις κυβερνοασφάλειας έχει ενισχύσει την αποτελεσματικότητά τους στον εντοπισμό απειλών και την ενορχήστρωση ενεργειών απόκρισης, αυξάνοντας τις συνολικές επιχειρήσεις ασφαλείας.

6. **Εκπαιδευτικός πόρος:** Πέρα από τις πρακτικές εφαρμογές του, το πλαίσιο ATT&CK εμπλουτίζει τα προγράμματα εκπαίδευσης και κατάρτισης για την κυβερνοασφάλεια, προσφέροντας πληθώρα γνώσεων σχετικά με τις απειλές και τις άμυνες στον κυβερνοχώρο μέσω λεπτομερών περιγραφών τεχνικών και πραγματικών περιπτώσι-ολογικών μελετών.

2.2.4 Αξιοποίηση του framework στην ανάπτυξη εγχειριδίων ransomware

Κατά τη δημιουργία ενός εγχειριδίου ransomware, το πλαίσιο ATT&CK της MITRE αναδεικνύεται ως ένα απαραίτητο εργαλείο, παρέχοντας μια δομημένη μεθοδολογία για την ανάλυση και κατανόηση καμπάνιας ransomware με απaráμιλλο βάθος και εύρος. Αυτό το πλαίσιο μας εφοδιάζει με μια λεπτή κατανόηση των φορέων επίθεσης ransomware, από την αρχική εισβολή έως τα τελικά στάδια κρυπτογράφησης δεδομένων και απαίτησης λύτρων, χαρτογραφώντας αυτές τις ενέργειες εντός του ολοκληρωμένου πίνακα τακτικών και τεχνικών του.

Initial Access 12 techniques	Execution 9 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 6 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System	Block Reporting Message	Spoof Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode	Change Credential	Unauthorized Command Message	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking	Valid Accounts		Spoof Reporting Message		Remote Services	Valid Accounts	Block Serial COM	Denial of Service	Denial of Service	Loss of Productivity and Revenue
Replication Through Removable Media	Native API						I/O Image	Data Destruction	Denial of Service	Denial of Service	Loss of Protection
Rogue Master	Scripting						Monitor Process State	Denial of Service	Device Restart/Shutdown	Device Restart/Shutdown	Loss of View
Spearphishing Attachment	User Execution						Point & Tag Identification	Manipulate I/O Image	Manipulate I/O Image	Manipulate I/O Image	Manipulation of Control
Supply Chain Compromise							Program Upload	Modify Alarm Settings	Rootkit	Rootkit	Manipulation of View
Transient Cyber Asset							Screen Capture	Service Stop	Service Stop	Service Stop	Theft of Operational Information
Wireless Compromise							Wireless Sniffing	System Firmware	System Firmware	System Firmware	

Σχήμα 2.4: Wannacry Ransomware, Techniques Used

Στο παραπάνω σχήμα, βλέπουμε αναλυτικά, όπως και νωρίτερα στο ATT&CK Matrix, for Enterprise, όλες τις τεχνικές που μπορεί να ακολουθήσει ένας επιτιθέμενος ή/και παρατηρούνται κατά την εκτέλεση του Wannacry Ransomware.

Η αξιοποίηση του πλαισίου ATT&CK επιτρέπει τον εντοπισμό μοτίβων συμπεριφοράς και τεχνικών που χρησιμοποιούνται συνήθως σε επιθέσεις ransomware, όπως το phishing, η εκμετάλλευση ευπαθειών, η πλευρική μετακίνηση εντός δικτύων και η διαρροή δεδομένων πριν

από την κρυπτογράφηση. Αυτή η διορατικότητα είναι ζωτικής σημασίας για την ανάπτυξη στοχευμένων στρατηγικών άμυνας και δράσεων απόκρισης που είναι ειδικά προσαρμοσμένες στη διαφοροποιημένη και εξελισσόμενη φύση των απειλών ransomware.

Επιπλέον, οι ενημερώσεις του πλαισίου διασφαλίζουν ότι το εγχειρίδιο για το ransomware παραμένει επίκαιρο με τις τελευταίες πληροφορίες για απειλές και τις τακτικές των επιτιθέμενων. Αυτή η δυναμική πτυχή του πλαισίου επιτρέπει τη συνεχή βελτίωση και εξέλιξη του εγχειριδίου, διασφαλίζοντας ότι παραμένει αποτελεσματικό έναντι νέων και αναδυόμενων παραλλαγών ransomware.

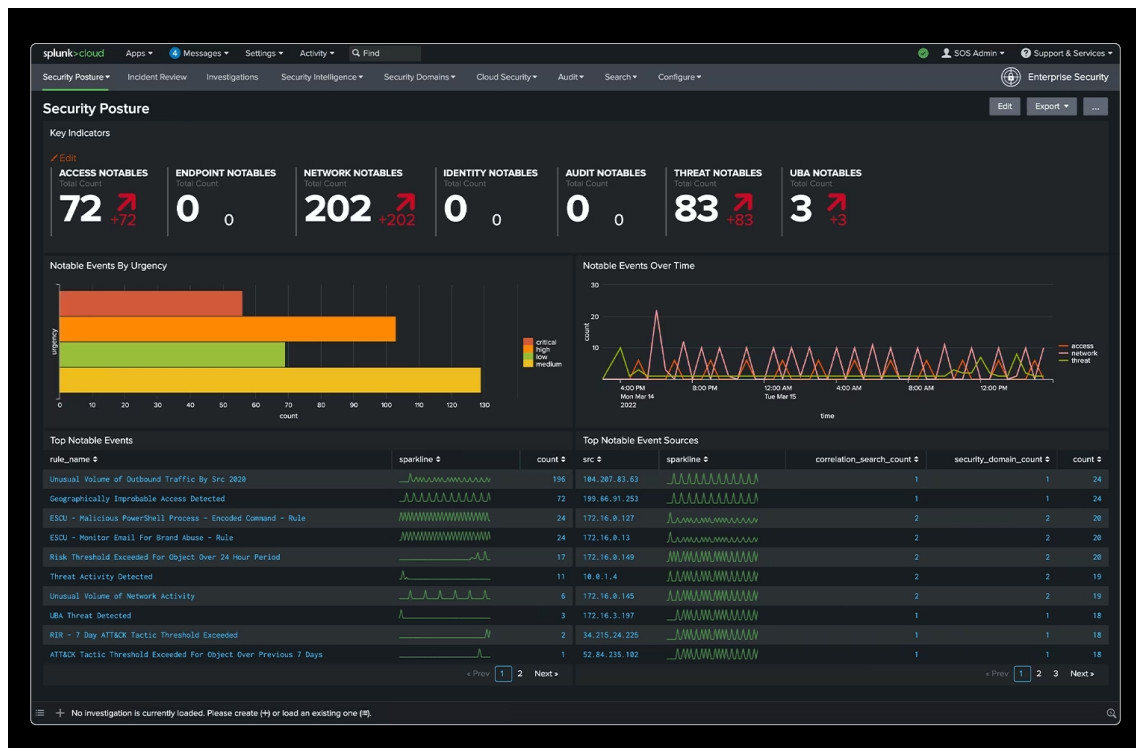
Στην ουσία, το πλαίσιο ATT&CK του MITRE όχι μόνο καθοδηγεί την ανάπτυξη ενός ολοκληρωμένου εγχειριδίου για το ransomware, αλλά και ενισχύει την αποτελεσματικότητά του μέσω λεπτομερών πληροφοριών σχετικά με τις τακτικές και τις τεχνικές των επιτιθέμενων. Αυτό διασφαλίζει ότι οι αμυντικές στρατηγικές μας δεν είναι απλώς αντιδραστικές αλλά προληπτικές, επιτρέποντάς μας να είμαστε ένα βήμα μπροστά από τους επιτιθέμενους ransomware και να μετριάσουμε τον κίνδυνο καταστροφικών κυβερνοεπιθέσεων.

2.3 Splunk

2.3.1 Επισκόπηση

Το Splunk¹ ξεχωρίζει στον τομέα της κυβερνοασφάλειας με τις ισχυρές δυνατότητες διαχείρισης πληροφοριών και συμβάντων ασφαλείας (SIEM). Ως κομμάτι της πλατφόρμας Splunk Enterprise, το Splunk ES αξιοποιεί τα δεδομένα μηχανής για να ενισχύσει τις διαδικασίες εντοπισμού, παρακολούθησης και αντιμετώπισης περιστατικών ασφαλείας. Εξασφαλίζει πληροφορίες σε πραγματικό χρόνο σχετικά με τις οργανωτικές στάσεις ασφαλείας, ενισχύοντας σημαντικά την ανίχνευση, τη διερεύνηση και τον μετριασμό τόσο των εσωτερικών όσο και των εξωτερικών απειλών ασφαλείας. Ειδικότερα, οι λειτουργίες του περιλαμβάνουν μια ολοκληρωμένη σουίτα εργαλείων, όπως το ταμπλό επισκόπησης συμβάντων, το πλαίσιο ανάλυσης κινδύνου και ένα πλαίσιο Threat Intelligence, τα οποία συναρμονίζονται για να παρέχουν μια διαφοροποιημένη λύση ασφάλειας που εκτείνεται από τον εντοπισμό απειλών έως την ολοκληρωμένη αντιμετώπιση και αποκατάσταση συμβάντων.

¹https://www.splunk.com/en_us/products/enterprise-security.html



Σχήμα 2.5: Splunk Enterprise Security

Η συγκεκριμένη εικόνα, δείχνει ένα security dashboard του Splunk, παρέχοντας βασικές μετρήσεις όπως ο αριθμός των περιστατικών που σχετίζονται με την πρόσβαση και το δίκτυο και τις απειλές, μπάρες που υποδεικνύουν το επίπεδο κρίσιμότητας αυτών των περιστατικών (κρίσιμα, υψηλά, μεσαία). Όλες αυτές οι πληροφορίες έχουν ως στόχο να δίνουν μία πρώτη εικόνα που αντιπροσωπεύει την υποδομή η οποία είναι υπό παρακολούθηση.

2.3.2 Splunk και Security Playbooks

Τα εγχειρίδια ασφαλείας αποτελούν βασικό μέρος του πλαισίου αντιμετώπισης περιστατικών του Splunk. Το Splunk τα αποκαλεί "εγχειρίδια εκτέλεσης" ή "σχέδια δράσης" και παρέχουν βήμα προς βήμα διαδικασίες για τον χειρισμό διαφόρων τύπων συμβάντων ασφαλείας. Αυτά τα εγχειρίδια ενσωματώνονται απευθείας στο περιβάλλον εργασίας του Splunk ES, παρέχοντας στις ομάδες ασφαλείας εύκολη πρόσβαση στις διαδικασίες που χρειάζονται όταν ανταποκρίνονται σε μια ειδοποίηση. Επιπλέον, η πρωτοβουλία Adaptive Response Initiative του Splunk επεκτείνει περαιτέρω τις δυνατότητες αυτών των εγχειριδίων. Η πρωτοβουλία

αυτή αποσκοπεί στην αυτοματοποίηση και τον συντονισμό των απαντήσεων σε διάφορες τεχνολογίες ασφαλείας, γεγονός που μπορεί να συμβάλει στη μείωση του χρόνου μεταξύ της ανίχνευσης απειλών και της αντίδρασης.

Το Splunk, με την επιχειρησιακού επιπέδου τεχνολογία της, έχει αναπτύξει μια μοναδική προσέγγιση στα εγχειρίδια ασφαλείας, που τη διακρίνει ως ηγέτη στο τοπίο της κυβερνοασφάλειας.

Name	SOAR App	D3FEND	Use Case
AD LDAP Account Unlocking	AD LDAP		
AWS Disable User Accounts	AWS IAM		
AWS IAM Account Unlocking	AWS IAM	Restore User Account Access	
Active Directory Enable Account Dispatch	AD LDAP, Azure AD Graph, AWS IAM		
Active Directory Reset password	AD LDAP		
Azure AD Account Unlocking	Azure AD Graph	Restore User Account Access	
Block Indicators	Palo Alto Networks Firewall, Carbon Black Response, Cisco Umbrella		
Cisco Umbrella DNS Denylisting	Cisco Umbrella	DNS Denylisting	Phishing, Endpoint
Crowdstrike Malware Triage	CrowdStrike OAuth API		
DNS Denylisting Dispatch		DNS Denylisting	Phishing, Endpoint
Delete Detected Files	Windows Remote Management		

Σχήμα 2.6: *List of Splunk Response Playbooks*

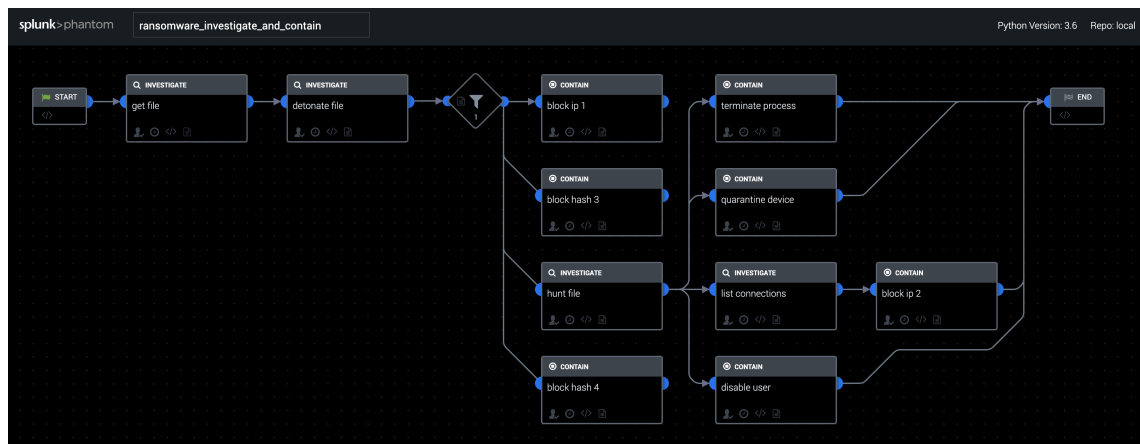
Όπως φαίνεται και στο σχήμα, το Splunk παρέχει στους χρήστες της μία λίστα από response και investigation playbooks οι οποίες στοχεύουν στην ανταπόκριση σε περίπτωση καθώς και στην διερεύνηση με στόχο να εντοπιστεί πρόωρα κάποιο pattern πριν το alert. Για κάθε είδος επίθεσης υπάρχει ένα αντίστοιχο playbook το οποίο μπορεί να ενσωματωθεί και να εκτελεστεί αυτόματα από το Splunk SOAR.

Βασικές από τις λειτουργίες των playbooks οι οποίες τα διαφοροποιούν είναι οι εξής:

1. **Integration into Splunk ES Interface:** Ένα βασικό χαρακτηριστικό της προσέγγισης του Splunk είναι η ενσωμάτωση των εγχειριδίων ασφαλείας απευθείας στη διεπαφή του Splunk ES. Αυτή η ενσωμάτωση διευκολύνει την άμεση πρόσβαση σε αυτά τα εγχειρίδια όταν ενεργοποιείται μια συγκεκριμένη ειδοποίηση. Αυτή η λειτουργία επιτρέπει στους αναλυτές ασφαλείας να ανατρέχουν γρήγορα στα απαιτούμενα βήματα για τη διαχείριση περιστατικών, μειώνοντας το χρόνο απόκρισης και εξασφαλίζοντας συνεπή χειρισμό περιστατικών.
2. **Προσαρμόσιμα playbooks:** Τα playbooks ασφαλείας του Splunk είναι ιδιαίτερα προσαρμόσιμα, προσφέροντας τη δυνατότητα προσαρμογής των βημάτων με βάση το συγκεκριμένο επιχειρησιακό περιβάλλον και τα πρωτόκολλα αντιμετώπισης συμβάντων ενός οργανισμού. Η πτυχή της προσαρμογής επιτρέπει τη συνεχή βελτίωση των εγχειριδίων ως απάντηση στην εξελισσόμενη κατάσταση ασφαλείας και το τοπίο των απειλών, καθιστώντας τα ένα δυναμικό εργαλείο στο οπλοστάσιο ασφαλείας ενός οργανισμού.
3. **Αυτοματοποίηση των απαντήσεων:** Η πρωτοβουλία Adaptive Response Initiative της Splunk ενισχύει τις δυνατότητες των εγχειριδίων ασφαλείας με την αυτοματοποίηση ορισμένων βημάτων. Αυτή η δυνατότητα σημαίνει ότι η ομάδα ασφαλείας μπορεί να ρυθμίσει προκαθορισμένες ενέργειες που θα ενεργοποιούνται αυτόματα ως απάντηση σε ορισμένους τύπους ειδοποιήσεων. Η αυτοματοποίηση απελευθερώνει πολύτιμο χρόνο για τους αναλυτές ασφαλείας, επιτρέποντάς τους να επικεντρωθούν σε σύνθετα ή ασυνήθιστα περιστατικά που απαιτούν ανθρώπινη επαφή.
4. **Συνεργατική διαχείριση συμβάντων:** Το Splunk δίνει έμφαση στη συνεργατική διαχείριση συμβάντων με τα εγχειρίδια ασφαλείας του. Τα playbooks χρησιμεύουν ως ένας κοινός οδηγός στον οποίο έχουν πρόσβαση όλα τα μέλη της ομάδας ασφαλείας. Αυτή η κοινή κατανόηση διασφαλίζει μια εναρμονισμένη ανταπόκριση σε περιστατικά ασφαλείας, ελαχιστοποιώντας τη σύγχυση και τα λάθη που θα μπορούσαν να προκύψουν από κακή επικοινωνία ή διαφορετικές διαδικασίες.

2.3.3 Το Splunk σε συνδυασμό με το Ransomware Playbook

Στην εικόνα 2.7, φαίνεται η σειρά εκτέλεσης ενός playbook σχεδιασμένο για ανταπόκριση σε ενδείξεις Ransomware. Μας δείχνει ότι αρχικά βρίσκει και αναλύει το αρχείο, προχωρώντας

Σχήμα 2.7: *Splunk Ransomware Playbook*

περιορίζοντας τον κίνδυνο με τον αποκλεισμό κάποιων hashes και IP Addresses από τα συστήματα ασφαλείας.

Αντιμετωπίζοντας τις επιθέσεις ransomware, είναι απαραίτητο να αναφερθεί η συμβολή του Splunk στις ποικίλες τακτικές που απαιτούνται για την αποτελεσματική απόκρουση τέτοιων απειλών. Το Splunk λάμπει με την περίπλοκη ικανότητά του για εξέταση και ανάλυση των δεδομένων συστήματος και δικτύου, ανοίγοντας το δρόμο για τον ταχύ εντοπισμό οποιωνδήποτε ενδείξεων εισβολής ransomware. Αυτή η ικανότητα εντοπισμού των προβλημάτων αλλάζει τα δεδομένα, δίνοντας τη δυνατότητα στις ομάδες να αναλάβουν δράση γρήγορα και με σύνεση, αμβλύνοντας το πιθανό πλήγμα από μια επίθεση.

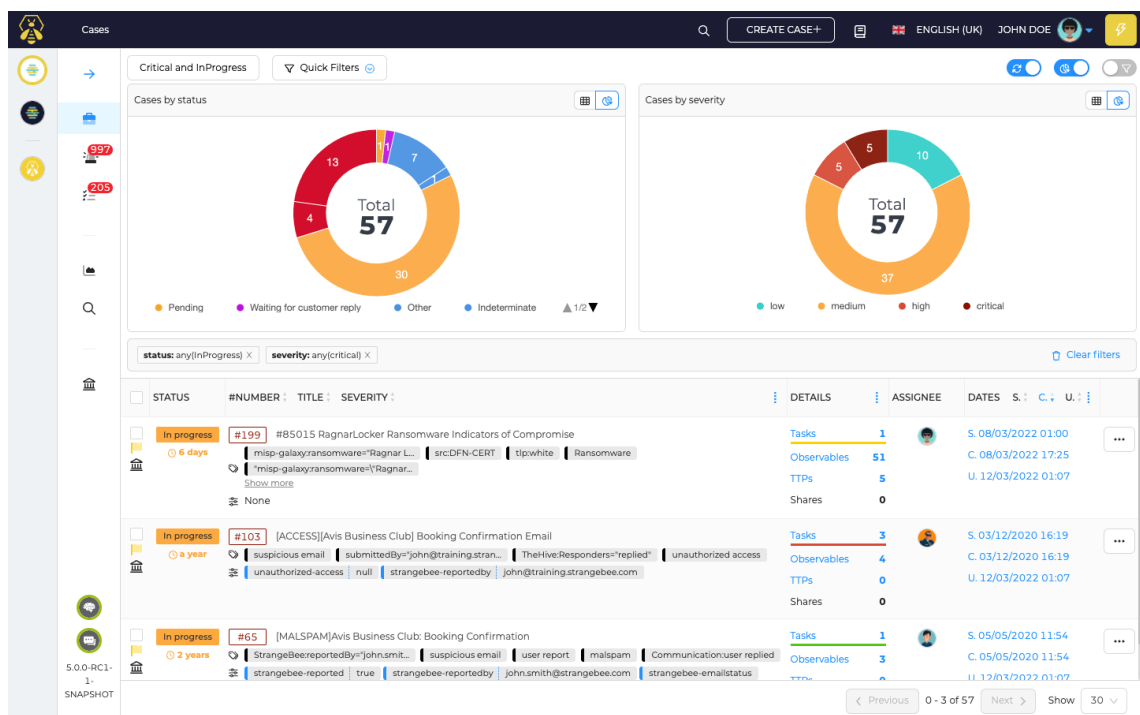
Με την ενσωμάτωση του Splunk στον ιστό της ευρύτερης εγκατάστασης ασφαλείας, ουσιαστικά ενισχύονται οι αμυντικοί μηχανισμοί. Είναι σαν να συγκεντρώνεται μια ενωμένη αμυντική ομάδα ασφαλείας έτοιμη να εντοπίσει, να αναλύσει και να αντιμετωπίσει κατά μέτωπο περίπλοκες απειλές.

Εξοπλίζοντας το με ένα ισχυρό εγχειρίδιο, ενισχυμένο από την ικανότητα του Splunk, σημαίνει ότι η ομάδα δεν είναι απλώς προετοιμασμένη για να αντιμετωπίσει μία επίθεση ransomware, αλλά επίσης ενισχύει τις άμυνες ενάντια στις απειλές που διαφαίνονται. Αυτή η ολοκληρωμένη προσέγγιση, που συνδυάζει προληπτικά βήματα με στιβαρές αμυντικές τακτικές, υπογραμμίζει πραγματικά τον ρόλο του Splunk στην πλοήγηση στον πολύπλοκο και συνεχώς μεταβαλλόμενο λαβύρινθο των κινδύνων ransomware.

2.4 The Hive Project

2.4.1 Επισκόπηση

Το έργο TheHive² αντιπροσωπεύει μια ολοκληρωμένη πλατφόρμα αντιμετώπισης συμβάντων ασφαλείας (SIRP), η οποία είναι απαραίτητη για τις ομάδες αντιμετώπισης συμβάντων ασφαλείας πληροφοριών και τους ειδικούς στην ψηφιακή εγκληματολογία. Ο σχεδιασμός του είναι σχολαστικά σχεδιασμένος για να υποστηρίξει τη διαχείριση, την ανάλυση και την αντιμετώπιση περιστατικών ασφαλείας, δίνοντας έμφαση στις συνεργατικές προσπάθειες και τη λειτουργική αποτελεσματικότητα.



Σχήμα 2.8: TheHive Dashboard

Το παραπάνω dashboard (2.8) παρέχει μια ολοκληρωμένη επισκόπηση των περιστατικών κυβερνοασφάλειας. Συνοψίζει οπτικά την κατάσταση και τη σοβαρότητα ενεργών cases χρησιμοποιώντας διαγράμματα. Ο κατάλογος κάτω από τα διαγράμματα αναλύει κάθε case με συγκεκριμένες πληροφορίες, όπως το status, ο αριθμός του case, ο τίτλος, η σοβαρότητα, οι λεπτομέρειες, σε ποιον είναι assigned και οι σχετικές ημερομηνίες.

²<https://thehive-project.org>

Κεντρικό ρόλο στη χρησιμότητα του TheHive παίζει η ικανότητά του να διευκολύνει τη μεθοδική διαχείριση περιστατικών ασφαλείας. Επιτρέπει τη δημιουργία ολοκληρωμένων φακέλων υποθέσεων για κάθε περιστατικό, επιτρέποντας τη συγκέντρωση και διαχείριση όλων των σχετικών πληροφοριών, όπως διευθύνσεις IP, διευθύνσεις URL και hashes αρχείων. Αυτή η συστηματική προσέγγιση εγγυάται τη σύλληψη και την προσβασιμότητα όλων των σχετικών δεδομένων, προωθώντας έτσι μια διεξοδική διαδικασία διερεύνησης και ανταπόκρισης.

Η συνεργασία αποτελεί θεμελιώδη πτυχή του TheHive, επιτρέποντας σε πολλά μέλη της ομάδας να ασχολούνται ταυτόχρονα με την ίδια υπόθεση. Αυτό το χαρακτηριστικό είναι ιδιαίτερα επωφελές σε περιβάλλοντα όπου η άμεση, συντονισμένη δράση είναι υψίστης σημασίας. Η πλατφόρμα φιλοξενεί ενημερώσεις σε πραγματικό χρόνο, ανάθεση καθηκόντων και ανταλλαγή πληροφοριών, ενισχύοντας έτσι τη συλλογική αποτελεσματικότητα της ομάδας.

Επιπλέον, η δυνατότητα ενσωμάτωσης του TheHive με ένα ευρύ φάσμα εργαλείων και υπηρεσιών ασφαλείας ενισχύει περαιτέρω την αξία του. Η ενσωμάτωση αυτή επιτρέπει την αυτοματοποίηση διαφόρων εργασιών, όπως η ανάλυση των παρατηρήσεων και η ενίσχυση των περιπτώσεων με εξωτερικές πληροφορίες για απειλές, μειώνοντας σημαντικά το χειροκίνητο φόρτο των ομάδων ασφαλείας και επιταχύνοντας τη διαδικασία απόκρισης.

Στο πλαίσιο των εγχειριδίων ransomware, το TheHive Project αναλαμβάνει κρίσιμο ρόλο στην οργάνωση και την εκτέλεση των μέτρων αντιμετώπισης. Προσφέρει ένα δομημένο πλαίσιο για την τεκμηρίωση της αλληλουχίας των ενεργειών, από την αρχική ανίχνευση, τον περιορισμό και την εξάλειψη, έως την ανάλυση μετά το συμβάν. Η έμφαση που δίνει η πλατφόρμα στη συνεργασία διασφαλίζει την ευθυγράμμιση και την ενημερωμένη συμμετοχή όλων των μελών της ομάδας, διευκολύνοντας έτσι την ενιαία και αποτελεσματική αντιμετώπιση των απειλών ransomware.

2.4.2 Βασικές Λειτουργίες

1. **Διαχείριση ειδοποιήσεων:** Το project περιλαμβάνει μια λεπτομερή σελίδα ειδοποιήσεων, όπως φαίνεται και στην εικόνα 2.9 σχεδιασμένη για ολοκληρωμένη διαχείριση. Οι χρήστες μπορούν να αλληλεπιδράσουν με την πλατφόρμα σχολιάζοντας τις ειδοποιήσεις, αναγνωρίζοντας μοτίβα μεταξύ τους και αλλάζοντας το status και τα πεδία. Με βάση αυτές τις αλληλεπιδράσεις, λαμβάνονται αποφάσεις σχετικά με την κλιμάκωση των ειδοποιήσεων σε στάδια διερεύνησης ή άμεσες ενέργειες αντιμετώπισης συμβάντων.
2. **Case Management Framework:** Το σύστημα επιτρέπει τη δημιουργία cases, μαζί με

The screenshot displays the TheHive web interface for managing alerts. At the top, there's a navigation bar with 'TheHive' logo, '+ New Case', 'My tasks' (6), 'Waiting tasks' (41), 'Alerts' (288), and 'Statistics'. A search bar is on the right. Below the navigation bar, the main content area shows 'List of alerts (288 of 302)'. There are filters (No event selected), sorting (Quick Filters), and pagination (15 per page). A filter is applied: 'Status: New, Updated'. The alert list has columns: Reference, Type, Status, Title, Source, Severity, Attributes, and Date. Three alerts are visible:

Reference	Type	Status	Title	Source	Severity	Attributes	Date
648	misp	New	#648 OSINT - Similarities Between Carbanak and FIN7 Malware Suggest Actors Are Closely Related <code>src:CIRCL</code> <code>verisactor:motive="Financial"</code> <code>circitopic="finance"</code> <code>misp-galaxy:threat-actor="Anunak"</code>	MISP-DEMO	H	19	Fri, Apr 28th, 2017 2:14 -04:00
650	misp	New	#650 Dridex 2017-04-11 : botnet 7200/7500 campaigns <code>src:CIRCL</code> <code>misp-galaxy:tool="Dridex"</code>	MISP-DEMO	H	59	Thu, Apr 27th, 2017 5:57 -04:00
647	misp	New	#647 OSINT - Threat Spotlight: Mighty Morphin Malware Purveyors: Locky Returns Via Necurs <code>src:CIRCL</code> <code>Type:OSINT</code> <code>malware_classification:malware-category="Ransomware"</code>	MISP-DEMO	H	259	Wed, Apr 26th, 2017 9:31 -04:00

Σχήμα 2.9: TheHive Alert management

τα σχετικά tasks και τα παρατηρήσιμα στοιχεία. Διευκολύνει τον εντοπισμό ομοιοτήτων μεταξύ cases και alerts και επιτρέπει τον ορισμό του Permissible Actions Protocol (PAP) level για κάθε παρατηρήσιμο στοιχείο. Επιπλέον, προσφέρει ένα template engine για την ενίσχυση της διαδικασίας αντιμετώπισης περιστατικών.

- Προηγμένη προσαρμογή προφίλ χρήστη:** Η πλατφόρμα παρέχει τη δυνατότητα ορισμού και προσαρμογής προφίλ χρηστών, ανάθεσης αυτών σε μέλη οργανισμών και διασφάλισης συγχρονισμού μέσω της ενσωμάτωσης LDAP ή Active Directory (AD).
- Σχεδιασμός συστήματος ειδοποίησης:** Υλοποιείται ένα ευέλικτο σύστημα ειδοποιήσεων, το οποίο επιτρέπει τον ορισμό κανόνων για την ενεργοποίηση διαφόρων μορφών ειδοποιήσεων, συμπεριλαμβανομένων των Webhooks³, emails, των μηνυμάτων Slack⁴ και Mattermost⁵ ή των προσαρμοσμένων αιτημάτων HTTP.
- Χρήση μετρήσεων και ταμπλό:** Το project ενσωματώνει ένα σύστημα για τη συγκέντρωση και συσχέτιση δεδομένων από διάφορες πηγές, όπως cases, tasks και observables, για τη δημιουργία key performance indicators (KPI) και management by objectives (MBO) μέσω μιας δυναμικής μηχανής dashboard.

³<https://www.redhat.com/en/topics/automation/what-is-a-webhook>

⁴<https://slack.com>

⁵<https://mattermost.com>

6. **Ολοκληρωμένη προσβασιμότητα API:** Παρέχεται πλήρης πρόσβαση σε τεκμηριωμένα APIs, διευκολύνοντας την ενσωμάτωση workflows ή την automation scripts που χρησιμοποιούν δεδομένα από το TheHive.
7. **Δυνατότητα ενσωμάτωσης MISP:** Το σύστημα προσφέρει λειτουργικότητα για την ταχεία εισαγωγή και ετοιμότητα των shared Indicators of Compromise , καθώς και την κοινή χρήση αυτών των δεικτών εντός των κοινοτήτων χρηστών, συνδέοντας το TheHive με το MISP.
8. **Ενσωμάτωση του πλαισίου MITRE ATT&CK:** Το project ενσωματώνει το Πλαίσιο MITRE ATT&CK, επιτρέποντας την εισαγωγή των TTPs στο σύστημα διαχείρισης συναγερμών του TheHive, ειδικά για συναγερμούς, ή την εξαγωγή τους σε ένα συμβάν MISP.

2.4.3 Ο Ρόλος του TheHive για την διαχείριση περιστατικών Ransomware

Η διαχείριση ενός ransomware περιστατικού απαιτεί όχι μόνο άμεση δράση, αλλά και μια διαφοροποιημένη, συντονισμένη αντίδραση που αξιοποιεί όλο το φάσμα των διαθέσιμων πόρων και της τεχνογνωσίας. Το σύστημα διαχείρισης alert, το οποίο χρησιμεύει ως το αρχικό σημείο επαφής με πιθανές απειλές, επιτρέπει στις ομάδες να σχολιάζουν, να αξιολογούν και να κατηγοριοποιούν τις ειδοποιήσεις με ακρίβεια. Αυτό το λεπτομερές επίπεδο ανάλυσης είναι απαραίτητο για τη διάκριση των ψευδών συναγερμών από τις πραγματικές απειλές, επιτρέποντας έτσι μια εστιασμένη και αποτελεσματική αντίδραση στις ενδείξεις ransomware.

Μόλις μια ειδοποίηση ransomware επαληθευτεί ως πραγματική απειλή, οι δυνατότητες διαχείρισης cases του TheHive παίζουν σημαντικό ρόλο, διευκολύνοντας την ταχεία συγκρότηση cases, tasks και observables. Αυτή η δομημένη προσέγγιση διασφαλίζει ότι διερευνάται και τεκμηριώνεται κάθε πτυχή της απειλής, προωθώντας μια ενδεδειγμένη κατανόηση που είναι απαραίτητη για την αποτελεσματική λήψη αντιμέτρων. Η ικανότητα της πλατφόρμας να παραλληλίζει τρέχοντα και προηγούμενα περιστατικά είναι ιδιαίτερα πολύτιμη, προσφέροντας γνώσεις που μπορούν να βελτιώσουν τη στρατηγική αντιμετώπισης και να αποτρέψουν μελλοντικές παραβιάσεις.

Ο συνεργατικός χαρακτήρας του TheHive, που υποστηρίζεται από το multi-tenant environment, ξεχωρίζει ως σημαντικό πλεονέκτημα για την αντιμετώπιση περιστατικών ransomware.

Επιτρέποντας την απρόσκοπτη συνεργασία μεταξύ διαφορετικών ομάδων και οργανισμών, διασφαλίζει ότι η τεχνογνωσία και οι πόροι συγκεντρώνονται αποτελεσματικά, μεγεθύνοντας τη συλλογική ικανότητα αντιμετώπισης. Το προηγμένο σύστημα διαχείρισης χρηστών ενισχύει περαιτέρω αυτή τη συλλογική προσπάθεια, διασφαλίζοντας ότι ο ρόλος και η πρόσβαση κάθε συμμετέχοντα είναι σαφώς καθορισμένα, διατηρώντας τόσο την αποτελεσματικότητα όσο και την ασφάλεια.

Τα συστήματα ειδοποίησης στο TheHive διασφαλίζουν ότι όλοι οι ενδιαφερόμενοι ενημερώνονται, επιτρέποντας την ταχεία λήψη αποφάσεων και δράση. Αυτό συμπληρώνεται από τις ισχυρές μετρήσεις και τις λειτουργίες του, οι οποίες παρέχουν πληροφορίες σε πραγματικό χρόνο σχετικά με το τοπίο των απειλών και την αποτελεσματικότητα των προσπαθειών αντιμετώπισης, καθοδηγώντας τις τρέχουσες και μελλοντικές ενέργειες.

Επιπλέον, η ενσωμάτωση του TheHive με εξωτερικά εργαλεία και πλαίσια, όπως το MISP για sharing indicators of compromise και το πλαίσιο MITRE ATT&CK για την κατανόηση των τακτικών και τεχνικών επίθεσης, εμπλουτίζει την αντιμετώπιση περιστατικών ransomware. Αυτές οι ενσωματώσεις προσφέρουν ευρύτερο πλαίσιο και βαθύτερη πληροφόρηση, δίνοντας τη δυνατότητα στις ομάδες όχι μόνο να ανταποκριθούν στην άμεση απειλή αλλά και να ενισχύσουν την άμυνα έναντι παρόμοιων μελλοντικών επιθέσεων.

2.5 MISP

2.5.1 Overview

Η πλατφόρμα Malware Information Sharing (MISP) αναδεικνύεται ως μια καίρια λύση στο πεδίο των πληροφοριών σχετικά με τις απειλές στον κυβερνοχώρο, παρέχοντας ένα ολοκληρωμένο πλαίσιο για την αποτελεσματική ανταλλαγή, αποθήκευση και διάδοση βασικών δεδομένων σχετικά με απειλές στον κυβερνοχώρο. Κεντρική θέση στην αρχιτεκτονική του MISP κατέχει η δέσμευσή της να ενισχύσει τις συλλογικές αμυντικές ικανότητες των οργανισμών, επιτρέποντας την απλουστευμένη ανταλλαγή κρίσιμων πληροφοριών σχετικά με τις ενδείξεις παραβίασης (Indications Of Compromise - IoC) χρησιμοποιούν οι επιτιθέμενοι στον κυβερνοχώρο.

Το MISP είναι σχολαστικά σχεδιασμένο ώστε να ανταποκρίνεται στις πολύπλευρες απαιτήσεις των επαγγελματιών της κυβερνοασφάλειας, προσφέροντας μια σειρά εργαλείων και λειτουργιών που έχουν σχεδιαστεί για την επιδέξια διαχείριση των πληροφοριών σχετικά

με τις απειλές. Το MISP απευθύνεται σε οντότητες διαφορετικής κλίμακας, από μικρότερες επιχειρήσεις έως οργανισμούς μεγάλης κλίμακας, και διευκολύνει την ανταλλαγή πληροφοριών σχετικά με τις αναδυόμενες απειλές, ενισχύοντας έτσι την ανθεκτικότητα των υποδομών κυβερνοασφάλειας σε διάφορους τομείς. Διαδραματίζει κρίσιμο ρόλο στην ενίσχυση της άμυνας έναντι εξελεγμένων επιθέσεων στον κυβερνοχώρο, καθιερώνοντας τον εαυτό του ως απαραίτητο στοιχείο στο σύγχρονο τοπίο της πρόληψης του εγκλήματος.

Στο παρακάτω σχήμα, βλέπουμε ένα overview από τις τρέχουσες απειλές κυβερνοασφάλειας που σχετίζονται με μια συγκεκριμένη ευπάθεια στην πλατφόρμα MISP. Περιλαμβάνει διάφορες λεπτομέρειες, όπως για παράδειγμα, πληροφορίες για την συγκεκριμένη ευπάθεια, συναφή συμβάντα, ένα γράφημα δικτύου που απεικονίζει τις συνδέσεις που σχετίζονται με την απειλή, παρέχοντας ένα ολοκληρωμένο στιγμιότυπο για την ανάλυση και την ανταλλαγή απειλών.



Σχήμα 2.10: MISP — Current Threats

2.5.2 Αξιοποίηση του MISP στη δημιουργία εγχειριδίων και στον μετριασμό πιθανών IoCs και επιθέσεων.

Η αρχιτεκτονική και τα χαρακτηριστικά του MISP συμβάλλουν σημαντικά στη δημιουργία εγχειριδίων κυβερνοασφάλειας και στον μετριασμό πιθανών δεικτών παραβίασης (IoCs). Η εν λόγω πλατφόρμα διευκολύνει μια ολοκληρωμένη και διαφοροποιημένη προσέγγιση της πληροφόρησης σχετικά με τις απειλές, προσφέροντας εργαλεία και λειτουργίες που συμβάλλουν καθοριστικά στην ανάπτυξη αποτελεσματικών στρατηγικών για την αντιμετώπιση και την πρόληψη απειλών.

1. Automated Indicator Extraction and Enrichment: Η δυνατότητα του MISP να εξάγει και να εμπλουτίζει αυτόματα IoCs από shared Threat Intelligence απλοποιεί τη

διαδικασία εντοπισμού πιθανών απειλών. Αυτή η αυτοματοποιημένη λειτουργία επιτρέπει τη γρήγορη εξαγωγή διευθύνσεων IP, διευθύνσεων URL, hashes αρχείων και άλλων IoCs από κοινές αναφορές, διευκολύνοντας την ενσωμάτωση αυτών των δεικτών στα εγχειρίδια ασφαλείας. Η διαδικασία εμπλουτισμού παρέχει περαιτέρω πληροφορίες σχετικά με το πλαίσιο αυτών των IoCs, όπως η συσχέτισή τους με γνωστές απειλές, η ιστορική τους συμπεριφορά και ο αντίκτυπός τους, οι οποίες είναι απαραίτητες για την ανάπτυξη στοχευμένων στρατηγικών μετριασμού.

2. Integration with Security Tools and Workflows: Το εκτεταμένο API και οι δυνατότητες ενσωμάτωσης του MISP επιτρέπουν τον απρόσκοπτο συγχρονισμό με ένα ευρύ φάσμα εργαλείων και πλατφορμών ασφαλείας, συμπεριλαμβανομένων των συστημάτων SIEM, των συστημάτων ανίχνευσης εισβολών και των εργαλείων ανάλυσης απειλών. Αυτή η ολοκλήρωση εξασφαλίζει ότι τα IoC και άλλα σχετικά δεδομένα απειλών μπορούν να τροφοδοτούνται απευθείας σε ροές εργασίας ασφαλείας, διευκολύνοντας την αυτοματοποίηση των ενεργειών απόκρισης, όπως περιγράφονται στα εγχειρίδια κυβερνοασφάλειας. Επιτρέπει ενημερώσεις και ειδοποιήσεις σε πραγματικό χρόνο, διασφαλίζοντας ότι οι ομάδες απόκρισης μπορούν να ενεργούν γρήγορα για τον μετριασμό των απειλών.

3. Προσαρμοσμένες ταξινομήσεις για Incident Classification: Οι προσαρμοσμένες ταξινομήσεις του MISP επιτρέπουν στους οργανισμούς να κατηγοριοποιούν τις απειλές και τα περιστατικά με τρόπο που ευθυγραμμίζεται με τις εσωτερικές τους διαδικασίες και τις δομές των εγχειριδίων τους. Αυτή η κατηγοριοποίηση βοηθά στον γρήγορο προσδιορισμό της φύσης και της σοβαρότητας των περιστατικών, επιτρέποντας μια πιο δομημένη και αποτελεσματική απόκριση με βάση τις κατευθυντήριες γραμμές του εκάστοτε εγχειριδίου. Η δυνατότητα προσαρμογής στις συγκεκριμένες οργανωτικές ανάγκες διασφαλίζει ότι οι απαντήσεις στο εγχειρίδιο είναι σχετικές και αποτελεσματικές.

4. Συσχέτιση συμβάντων για προληπτική άμυνα: Η λειτουργία συσχέτισης συμβάντων του MISP επιτρέπει στους οργανισμούς να εντοπίζουν μοτίβα και συνδέσεις μεταξύ διαφορετικών IoC και συμβάντων. Αυτή η δυνατότητα είναι καθοριστική για την πρόβλεψη πιθανών απειλών και την προληπτική ενσωμάτωση σχετικών στρατηγικών μετριασμού στα εγχειρίδια. Με την κατανόηση του τρόπου με τον οποίο συνδέονται διαφορετικοί δείκτες και περιστατικά, οι οργανισμοί μπορούν να αναπτύξουν πιο ολοκληρωμένα και προληπτικά μέτρα αντιμετώπισης.

2.5.3 Το MISF σε διαχείριση περιστατικού ασφαλείας Ransomware

Όταν εντοπίζεται μια ένδειξη απειλής ransomware, το MISF χρησιμεύει ως κεντρικό αποθετήριο και κόμβος επικοινωνίας, όπου μπορούν να διαμοιραστούν και να προσπελαστούν σε πραγματικό χρόνο λεπτομερείς πληροφορίες σχετικά με τις απειλές, συμπεριλαμβανομένων των υπογραφών, των τακτικών, των τεχνικών και των διαδικασιών που χρησιμοποιούν οι επιτιθέμενοι.

Όταν υπάρχει ένδειξη ransomware, οι ομάδες κυβερνοασφάλειας μπορούν να αξιοποιήσουν το MISF για την ταχεία διάδοση πληροφοριών σχετικά με τη συγκεκριμένη παραλλαγή ransomware, τη συμπεριφορά της, τις μεθόδους διάδοσης και τυχόν γνωστά τρωτά σημεία που εκμεταλλεύεται. Αυτή η άμεση ανταλλαγή πληροφοριών είναι κρίσιμη για την προληπτική λήψη μέτρων, επιτρέποντας στους οργανισμούς εντός του δικτύου να εφαρμόσουν γρήγορα αμυντικές στρατηγικές, όπως η ενημέρωση των τειχών προστασίας, το patching ευπαθειών και η ενίσχυση της ασφάλειας των τελικών σημείων, μειώνοντας έτσι τον κίνδυνο διείσδυσης.

Ταυτόχρονα, το MISF επιτρέπει την ενσωμάτωση αυτών των πληροφοριών απειλών σε πραγματικό χρόνο στο ευρύτερο εγχειρίδιο αντιμετώπισης του ransomware. Αυτό το εγχειρίδιο, ένας ολοκληρωμένος οδηγός που περιγράφει βήμα προς βήμα τις διαδικασίες για τον εντοπισμό, τον περιορισμό, την εξάλειψη και την ανάκαμψη από περιστατικά ransomware, εμπλουτίζεται από τις λεπτομερείς και ενημερωμένες πληροφορίες που παρέχει το MISF. Για παράδειγμα, εάν το MISF μοιραστεί δείκτες μιας νέας τεχνικής κρυπτογράφησης ransomware, το εγχειρίδιο μπορεί να ενημερωθεί άμεσα ώστε να περιλαμβάνει συγκεκριμένες μεθόδους εντοπισμού και αντίμετρα για την τεχνική αυτή, εξασφαλίζοντας έτσι μια έγκαιρη και αποτελεσματική αντιμετώπιση.

Επιπλέον, ο ρόλος του MISF επεκτείνεται πέρα από την αρχική απόκριση και διευκολύνει την ανάλυση και την αποκατάσταση μετά το συμβάν. Συγκεντρώνοντας δεδομένα σχετικά με τις επιθέσεις ransomware από διάφορες πηγές, το MISF βοηθά στον εντοπισμό μοτίβων, στην κατανόηση των φορέων επίθεσης και στην εκπόνηση πιο ισχυρών αμυντικών μέτρων.

Αυτή η διαδικασία υποστηρίζει όχι μόνο την τελειοποίηση των υφιστάμενων ενεργειών, αλλά βοηθά επίσης στην ανάπτυξη στρατηγικών πρόβλεψης, ενισχύοντας τη συνολική ανθεκτικότητα των οργανισμών έναντι μελλοντικών απειλών ransomware.

Κεφάλαιο 3

Ransomware Playbook

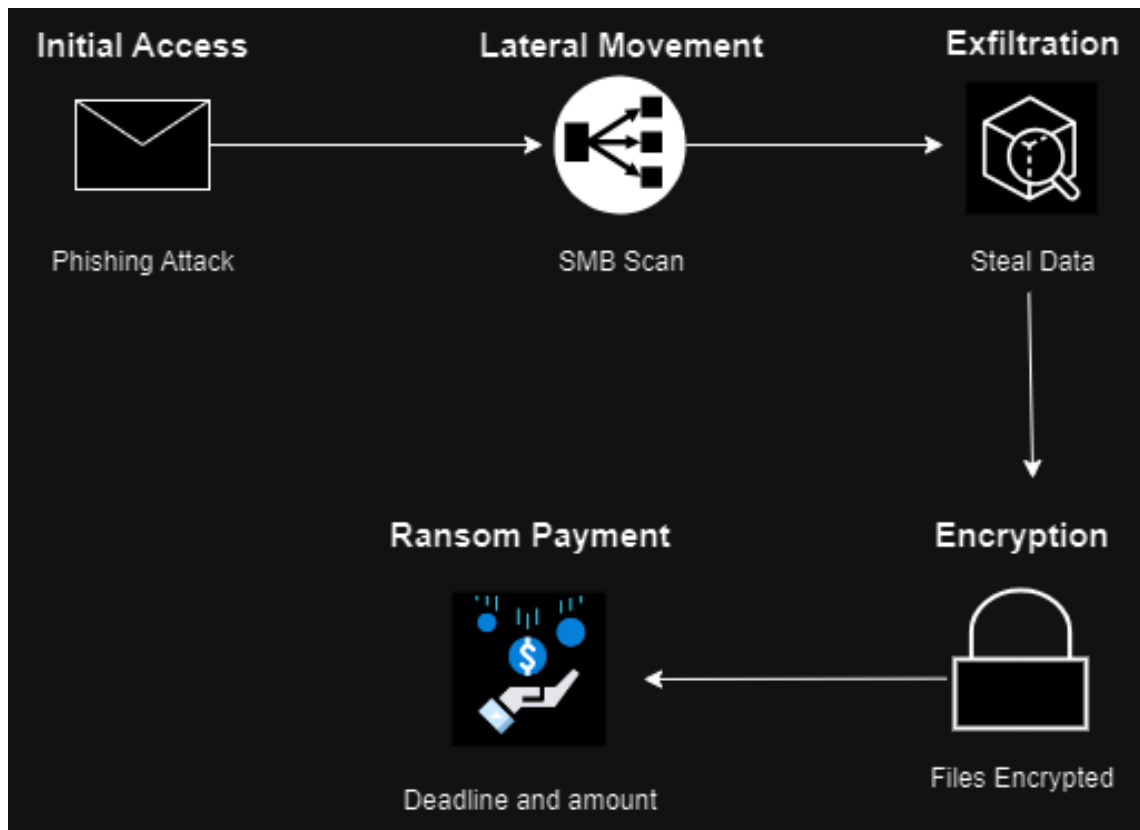
3.1 Πεδίο εφαρμογής και Στόχος

Το παρόν κεφάλαιο περιγράφει την προσέγγιση για τη διαχείριση και τον μετριασμό των απειλών ransomware με επιχειρησιακές διαδικασίες για ένα εταιρικό περιβάλλον. Προσφέρει πληροφορίες σχετικά με την ανίχνευση και την ανάλυση περιστατικών ransomware, εξοπλίζοντας τους ενδιαφερόμενους με εφαρμόσιμες στρατηγικές για τη διασφάλιση των δεδομένων και τον περιορισμό των πιθανών απειλών.

3.2 Τι είναι το Ransomware?

Το Ransomware εμπίπτει στην ευρύτερη έννοια του κακόβουλου λογισμικού, το οποίο περιλαμβάνει διάφορα επιβλαβή λογισμικά που αποσκοπούν στην πρόκληση ζημιών σε υπολογιστές ή δίκτυα. Το ransomware είναι ένας διαρκώς προσαρμοζόμενος τύπος κακόβουλου λογισμικού που κλειδώνει ή κρυπτογραφεί αρχεία σε μια συσκευή, καθιστώντας αυτά και τυχόν εξαρτώμενα συστήματα μη λειτουργικά. Στη συνέχεια, οι επιτιθέμενοι ζητούν λύτρα σε αντάλλαγμα για το ξεκλείδωμα των πληροφοριών. Συχνά απειλούν να πουλήσουν ή να απελευθερώσουν κλεμμένα δεδομένα ή διαπιστευτήρια σύνδεσης, εάν δεν ικανοποιηθούν οι απαιτήσεις τους.

Ένας ενδεικτικός κύκλος ζωής (3.11) μιας επίθεσης με λύτρα ξεκινά με τον επιτιθέμενο να αποκτά αρχική πρόσβαση, για παράδειγμα μέσω ενός phishing email, εξαπατώντας κάποιον να κάνει κλικ σε έναν κακόβουλο σύνδεσμο ή συνημμένο αρχείο. Μόλις εισέλθει, ο επιτιθέμενος



Σχήμα 3.11: Ενδεικτικός κύκλος ζωής *Ransomware*

κινείται πλευρικά σαρώνοντας το δίκτυο για να βρει περισσότερα συστήματα για να μολύνει. Στη συνέχεια, κλέβει πολύτιμα δεδομένα από το δίκτυο και προχωρά στην κρυπτογράφηση των αρχείων, καθιστώντας τα μη προσβάσιμα από το θύμα. Τέλος, ο επιτιθέμενος απαιτεί την καταβολή λύτρων, καθορίζοντας μια προθεσμία και ένα ποσό, σε αντάλλαγμα για την αποκρυπτογράφηση των αρχείων.

3.3 Πως συμβαίνουν οι επιθέσεις ransomware?

Ας εξερευνήσουμε μια κατάσταση όπου επιτιθέμενοι εκμεταλλεύονται ευπάθειες ενός δικτύου, εστιάζοντας συγκεκριμένα στο περιστατικό με το ransomware WannaCry. Η εικόνα 3.12 αποτελεί το σημείωμα που φαίνεται στο θύμα μετά την επίθεση, εκεί εξηγείται η διαδικασία πληρωμής των λύτρων και τα απαραίτητα βήματα για να ολοκληρωθεί η διαδικασία αποκρυπτογράφησης.



Σχήμα 3.12: Ransom note, after the attack

Η ακολουθία ξεκινά όταν οι επιτιθέμενοι εντοπίζουν και εκμεταλλεύονται μία ευπάθεια στο πρωτόκολλο SMB των Windows, γνωστό ως EternalBlue. Αυτή η παράβλεψη, που δεν έχει διορθωθεί σε πολλά συστήματα παγκοσμίως, επιτρέπει στους επιτιθέμενους να εκτελούν απομακρυσμένα επιβλαβή κώδικα στα επηρεαζόμενα συστήματα χωρίς να απαιτείται καμία αλληλεπίδραση του χρήστη. Το ransomware αναζητά και θέτει σε κίνδυνο συστήματα που είναι ευάλωτα λόγω απουσίας κρίσιμων ενημερώσεων ή επιδιορθώσεων.

Μετά τη μόλυνση ενός συστήματος, το WannaCry προχωρά στην κρυπτογράφηση αρχείων και παρουσιάζει απαίτηση λύτρων σε κρυπτονόμισμα για το κλειδί αποκρυπτογράφησης. Χρησιμοποιεί ισχυρές μεθόδους κρυπτογράφησης για να αρνηθεί στους χρήστες την πρόσβαση στα αρχεία τους.

Το WannaCry έχει σχεδιαστεί με χαρακτηριστικά που μοιάζουν με worm, επιτρέποντάς του να διαδίδεται γρήγορα μέσω δικτύων, στοχεύοντας άλλα συστήματα που δεν διαθέτουν τα απαραίτητα patches, μεγεθύνοντας έτσι τη συνολική διαταραχή της επίθεσης. Αυτή η ικανότητα αυτοαναπαραγωγής οδηγεί σε εκτεταμένες λειτουργικές διακοπές και διακοπές υπηρεσιών στους επηρεαζόμενους οργανισμούς.

Καθώς το WannaCry κλειδώνει βασικά αρχεία και παραλύει συστήματα, προκαλεί ευρεία

ανησυχία και σημαντικές επιχειρησιακές προκλήσεις. Πολλοί οργανισμοί βρίσκονται απροετοίμαστοι για την ταχύτητα και το εύρος της επίθεσης, με αποτέλεσμα να υπάρχουν σημαντικές οικονομικές απώλειες και απώλειες φήμης.

3.4 Κοινές μέθοδοι διανομής Ransomware

Όπως απεικονίζεται στο προηγούμενο παράδειγμα, η αρχική φάση σε κάθε επίθεση ransomware περιλαμβάνει την ανάπτυξη του κακόβουλου λογισμικού στο σύστημα-στόχο. Αυτό επιτυγχάνεται συνήθως μέσω ορισμένων στρατηγικών:

1. Στοχευμένες απάτες phishing, όπου ο ανυποψίαστος παραλήπτης κάνει κλικ σε ένα κακόβουλο συνημμένο αρχείο ή σύνδεσμο, όπου οι επιτιθέμενοι εκμεταλλεύονται ελαττώματα σε προγράμματα περιήγησης στο διαδίκτυο ή σε σχετικό λογισμικό
2. Εκμετάλλευση τρωτών σημείων, που επιτρέπουν στους επιτιθέμενους να έχουν πρόσβαση σε απομακρυσμένα συστήματα ή επιτρέπουν στο ransomware να εξαπλωθεί αυτόνομα.
3. Εξάπλωση μέσω αφαιρούμενων δίσκων, η οποία περιλαμβάνει επίσης δίσκους δικτύου τους οποίους το ransomware κρυπτογραφεί ταυτόχρονα καθώς θέτει σε κίνδυνο το σύστημα.

Στη συνέχεια, οι επιτιθέμενοι καταφεύγουν σε τυπικές μεθόδους εκτέλεσης (αναφέρονται από το MITRE ATT&CK - TA0002, το οποίο αποτελεί μέρος διάφορων τακτικών όπως φαίνεται στην εικόνα 3.13) που συνήθως περιλαμβάνουν:

1. Χρήση γραμμής εντολών
2. Χρήση του PowerShell
3. Χρήση των Processes

ID	Name	Description
TA0043	Reconnaissance	The adversary is trying to gather information they can use to plan future operations.
TA0042	Resource Development	The adversary is trying to establish resources they can use to support operations.
TA0001	Initial Access	The adversary is trying to get into your network.
TA0002	Execution	The adversary is trying to run malicious code.
TA0003	Persistence	The adversary is trying to maintain their foothold.
TA0004	Privilege Escalation	The adversary is trying to gain higher-level permissions.
TA0005	Defense Evasion	The adversary is trying to avoid being detected.
TA0006	Credential Access	The adversary is trying to steal account names and passwords.
TA0007	Discovery	The adversary is trying to figure out your environment.
TA0008	Lateral Movement	The adversary is trying to move through your environment.
TA0009	Collection	The adversary is trying to gather data of interest to their goal.
TA0011	Command and Control	The adversary is trying to communicate with compromised systems to control them.
TA0010	Exfiltration	The adversary is trying to steal data.
TA0040	Impact	The adversary is trying to manipulate, interrupt, or destroy your systems and data.

Σχήμα 3.13: MITRE ATT&CK Enterprise tactics

Γνωρίζοντας τις πιο κοινές μεθόδους διανομής ransomware, οι ενδιαφερόμενοι είναι προετοιμασμένοι είτε να ερευνήσουν την στρατηγική που χρησιμοποιήθηκε στην αρχική φάση της επίθεσης είτε να οχυρώσουν τα συστήματά τους με στόχο να αποτρέψουν πιθανές μελλοντικές επιθέσεις.

3.5 Διαδικασία Διερεύνησης

Αυτό το Playbook περιέχει διεξοδική ανάλυση για την διαχείριση περιστατικών ασφαλείας σε επιχειρησιακό περιβάλλον με στόχο να δημιουργούμε μια δομημένη προσέγγιση ώστε να διασφαλιστεί η ενδεδειγμένη και ολοκληρωμένη αντιμετώπιση για κάθε απαραίτητο βήμα στην διαδικασία της διερεύνησης.

3.5.1 Προσδιορισμός του τύπου Ransomware

Σε μία επίθεση ransomware, ο τύπος του ransomware που έχει μολύνει τα συστήματα είναι ύψιστης σημασίας. Παρά το γεγονός ότι στην βάση τους όλα τα ransomware έχουν παρόμοια στρατηγική, το καθένα έχει τις ιδιαιτερότητες του. Γι'αυτό το πρώτο βήμα κατά την διερεύνηση μίας τέτοιας επίθεσης είναι ο προσδιορισμός του τύπου του, με στόχο να εξειδικεύσουμε την ανάλυση μας προς την συμπεριφορά του εκάστοτε ransomware.

1. Αναζητήστε τυχόν σχετικά notes, (βλ. Σχήμα 3.10 Ransom Note) για πιθανές ενδείξεις. (text/ image files, pop-ups)
2. Επανεξετάστε τα εμπλεκόμενα αρχεία καθώς και νέα αρχεία που μπορεί να δημιουργήθηκαν.

Όπως φαίνεται στο παρακάτω παράδειγμα, ενώ ένας μεγάλος όγκος αρχείων έχουν κρυπτογραφηθεί, έχουμε πρόσβαση στο παρακάτω .txt αρχείο που μας δίνει πληροφορίες σχετικά με το είδος του ransomware.

Με βάση την εικόνα 3.14, μπορούμε να βγάλουμε το συμπέρασμα ότι ο συγκεκριμένος host έχει μολυνθεί με το abysslocker ransomware, με αποτέλεσμα να περιορίσουμε και να στοχοποιήσουμε την ανάλυση μας προς την ανάλογη συμπεριφορά του.

```
vboxuser@P2018118:~/Desktop$ cat abyss_ransomware.txt
We are the Abyss.

Your company Servers are crypted and your data has been stolen to our servers.

Good news for you:

1) We can restore your entire system.
2) We are not interested in publishing your information.
3) Our motivation is purely financial.
4) We are open to negotiations.
5) We are ready to maintain complete confidentiality of this incident.

Let's explain the further steps in the situation:

You can seek help from authorities - unfortunately, this path will not lead to a constructive resolution of the situation.
They will not assist you with decryption, seize your servers for OPsec, and your company's operations will be halted.
Subsequently, the date will be disclosed, leading to fines, legal actions, and reputational damage.

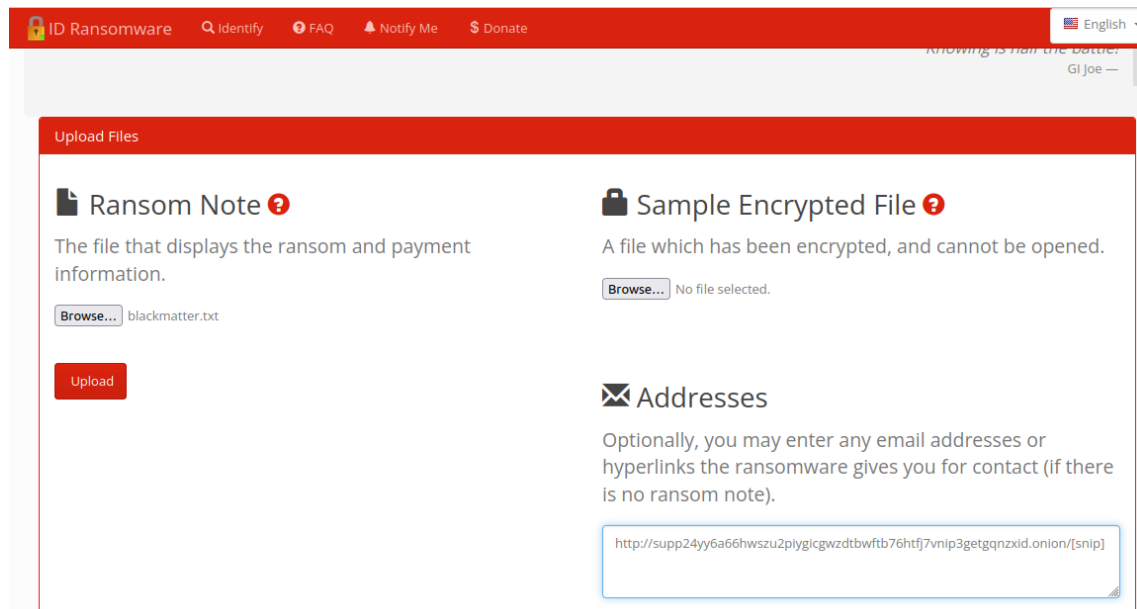
OR

You initiate negotiations with us, and we reach a mutually beneficial and constructive solution for both parties.
You pay a specified amount and receive the full decryption, support throughout the decryption process,
proofs that all information on our servers has been deleted, and a guarantee that it will never resurface,
ensuring no one learns about this incident.

To initiate negotiations, please download the Tor Browser using their official website: https://www.torproject.org/
use these credentials to enter the Chat for text negotiation: http://jqlcrn2fsfvxlngdq53rqyrwtwfrulup74xyle54bsvo3l2kgpeeljid.onion/\[snip\]
There will be no bad news for your company after successful negotiations for both sides. But there will be plenty of those bad news if case of failed negotiations, so
don't think about how to avoid it.
Just focus on negotiations, payment and decryption to make all of your problems solved by our specialists within 1 day after payment received: servers and data restor
ed, everything will work good as new.
```

Σχήμα 3.14: Ransom Note on a text file, Abysslocker

3. Χρησιμοποιήστε εργαλεία όπως το Crypto Sheriff¹ ή το ID Ransomware² για αυτοματοποιημένη ανάλυση των indicators.



The screenshot shows the ID Ransomware website interface. At the top, there is a red navigation bar with the logo and links for 'Identify', 'FAQ', 'Notify Me', and 'Donate'. A language dropdown menu is set to 'English'. Below the navigation bar, the main content area is titled 'Upload Files'. It is divided into two columns. The left column is for the 'Ransom Note', describing it as a file displaying ransom and payment information. It includes a 'Browse...' button (which shows 'blackmatter.txt' as the selected file) and an 'Upload' button. The right column is for the 'Sample Encrypted File', describing it as a file that cannot be opened. It includes a 'Browse...' button (showing 'No file selected'). Below these columns, there is an 'Addresses' section with a description and a text input field containing a long URL: 'http://supp24yy6a66hwszu2plygicgwzdtbwtb76htfj7vnip3getgqnxid.onion/[snip]'.

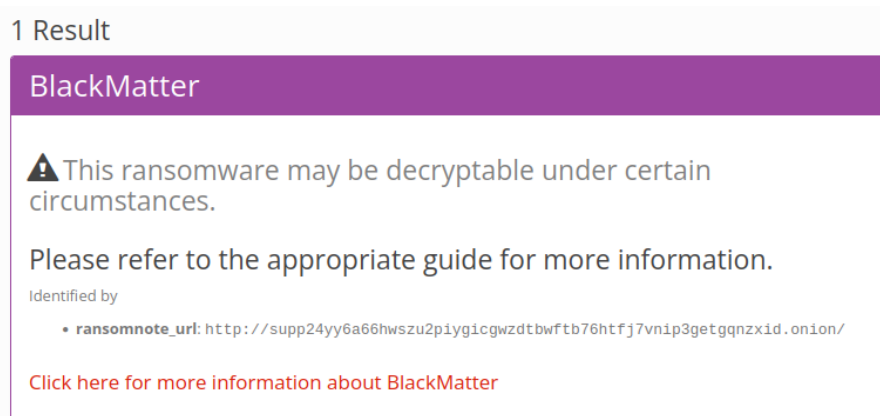
Σχήμα 3.15: *Uploading ransom note and chat URL*

Σε ένα άλλο παράδειγμα όπως φαίνεται παραπάνω(3.15, το ransom note σε πολλές περιπτώσεις δεν αρκεί για να εξακριβώσουμε το είδος του ransomware. Χρησιμοποιώντας ένα από τα αναφερόμενα εργαλεία, κάνουμε upload το Ransom note καθώς και άλλες σχετικές πληροφορίες.

Τέλος, το εργαλείο μας εξακριβώνει το είδος του Ransomware και μας παραπέμπει σε πληροφορίες για το σχετικό Ransomware 3.16.

¹<https://www.nomoreransom.org/crypto-sheriff.php?lang=en>

²<https://id-ransomware.malwarehunterteam.com>



Σχήμα 3.16: *Detected as BlackMatter Ransomware*

Αξιοποιώντας τις παραπάνω πληροφορίες οι ενδιαφερόμενοι μπορούν με ακρίβεια να εξακριβώσουν τον τύπο του ransomware, χρησιμοποιώντας τα αναφερόμενα εργαλεία και να αναλύουν τις ιδιαιτερότητες του. Αυτό καθιστά την διαδικασία διερεύνησης πιο εύκολη και προσιτή.

3.5.2 Scope and Impact

Το πεδίο εφαρμογής (Scope) αναφέρεται στην έκταση και τα όρια των μέτρων προστασίας εντός ενός οργανισμού, συμπεριλαμβανομένων των συστημάτων, των δεδομένων και των λειτουργιών που χρειάζονται προστασία από απειλές στον κυβερνοχώρο. Το impact αφορά τις πιθανές συνέπειες και τη σοβαρότητα μιας επίθεσης στον κυβερνοχώρο σε αυτά τα προστατευόμενα στοιχεία, όπως απώλεια δεδομένων, οικονομική ζημία, λειτουργική διαταραχή και βλάβη της φήμης. Μαζί, η κατανόηση του πεδίου εφαρμογής και του impact βοηθά τους οργανισμούς να ιεραρχήσουν τις προσπάθειές τους στον τομέα της κυβερνοασφάλειας και να κατανείμουν αποτελεσματικά τους πόρους για τον μετριασμό των κινδύνων. Στην δική μας περίπτωση, μας ενδιαφέρουν πιο συγκεκριμένα τα παρακάτω:

1. Προσδιορίστε ποια συστήματα έχουν μολυνθεί.
2. Καθορίστε το είδος των δεδομένων που μολύνθηκαν, όπως ο τύπος των αρχείων, το είδος του λογισμικού, ή το department που ανήκουν.
3. Μετρήστε το Impact που θα έχει στην επιχείριση.
4. Αξιολογήστε το Impact όσον αφορά το CIA (Confidentiality, Integrity, Availability).

Αυτή η διαδικασία επιτρέπει στους οργανισμούς να απομονώσουν αποτελεσματικά τα προσβεβλημένα συστήματα, αποτρέποντας την περαιτέρω εξάπλωση και ελαχιστοποιώντας τη ζημία. Από εκπαιδευτικής άποψης, η εκμάθηση της ανάλυσης του πεδίου εφαρμογής και των επιπτώσεων βοηθά στην ανάπτυξη κρίσιμων δεξιοτήτων στην αντιμετώπιση περιστατικών και στην αξιολόγηση κινδύνων. Βοηθά επίσης στην κατανομή των πόρων για την ασφάλεια στον κυβερνοχώρο, διασφαλίζοντας ότι μπορούν να αντιμετωπίσουν πρώτα τα πιο κρίσιμα τρωτά σημεία.

3.5.3 User Actions σε περίπτωση ενδείξεων Ransomware

Όταν παρατηρείται μια επίθεση ransomware, οι ενέργειες των χρηστών περιλαμβάνουν τα βήματα που πρέπει να λάβουν αμέσως, για να μετριάσουν την κατάσταση. Αυτές οι ενέργειες είναι κρίσιμες για την αποτελεσματική διαχείριση του περιστατικού ώστε να δωθεί ο απαραίτητος χρόνος στους ειδικούς να ανταπεξέλθουν στην τρέχον επίθεση χωρίς περισσότερες ζημιές. Πιο συγκεκριμένα:

1. Απομονώστε αμέσως το σύστημά σας από το δίκτυο για να αποτρέψετε την περαιτέρω εξάπλωση.
2. Καταγράψτε οπτικές αποδείξεις του περιστατικού χρησιμοποιώντας ένα smartphone.
3. Καταγράψτε όλες τις παρατηρήσεις και τις ενέργειες που έγιναν κατά τον εντοπισμό του περιστατικού, σημειώνοντας λεπτομέρειες όπως η ώρα, η τοποθεσία και τα στοιχεία του συστήματος.
4. Διατηρήστε αρχείο όλων των επικοινωνιών σχετικά με το περιστατικό για μελλοντική αναφορά.

Με τα παραπάνω βήματα που αναλαμβάνουν οι χρήστες, συμβάλλουν στον περιορισμό της επίθεσης και στην παροχή λεπτομερούς τεκμηρίωσης που θα βοηθήσει στην ανάκτηση και τη διερεύνηση. Για παράδειγμα, η απομόνωση του προσβεβλημένου συστήματος από το δίκτυο είναι ύψιστης σημαντικότητας για να αποτραπεί η εξάπλωση του κακόβουλου λογισμικού σε διασυνδεδεμένα συστήματα. Η καταγραφή οπτικών αποδεικτικών στοιχείων και η τεκμηρίωση κάθε λεπτομέρειας που σχετίζεται με το περιστατικό, συμπεριλαμβανομένης της ώρας εντοπισμού, της συγκεκριμένης τοποθεσίας και των λεπτομερειών του συστήματος, βοηθούν τους επαγγελματίες της κυβερνοασφάλειας να κατανοήσουν πώς συνέβη η επίθεση

και πώς να την αντιμετωπίσουν. Αναλύοντας και κατανοώντας αυτά τα βήματα, ο κάθε χρήστης είναι προετοιμασμένος ώστε να αντιδράσει σε μία τέτοια επίθεση, μετριάζοντας τον κίνδυνο και δημιουργώντας μία καλύτερη βάση για να προχωρήσουν σε διερεύνηση οι ειδικοί.

3.6 Μέτρα αποκατάστασης

3.6.1 Στρατηγικές περιορισμού

Για την αντιμετώπιση του ransomware, ο άμεσος περιορισμός είναι απαραίτητος. Δώστε μεγαλύτερη έμφαση στις στρατηγικές περιορισμού απ' ό,τι στις τυπικές αντιδράσεις περιστατικών.

1. Απομονώστε τα μολυσμένα συστήματα για να αποτρέψετε την περαιτέρω εξάπλωση. Περιορίστε την πρόσβαση για τους χρήστες και τις ομάδες που έχουν επηρεαστεί.
2. Ασφαλίστε τις υπηρεσίες κοινής χρήσης αρχείων, προστατεύοντας τόσο τα μολυσμένα όσο και τα μη μολυσμένα shares.
3. Απομονώστε τις κοινόχρηστες βάσεις δεδομένων, διασφαλίζοντας ότι οι μη μολυσμένες βάσεις δεδομένων παραμένουν ασφαλείς.
4. Ασφαλίστε τα αντίγραφα ασφαλείας για να αποτρέψετε την παραβίαση.
5. Αποκλεισμός γνωστών κακόβουλων domain και διευθύνσεων IP.
6. Καθαρίστε τα πιθανά phishing emails από τα γραμματοκιβώτια για να εξαλείψετε τις πηγές επαναμόλυνσης.
7. Διασφαλίστε ότι όλες οι λύσεις ασφάλειας των endpoints είναι τρέχουσες και ενεργές σε όλο το δίκτυο.
8. Εφαρμόστε τις απαραίτητες ενημερώσεις λογισμικού, δίνοντας προτεραιότητα στα κρίσιμα συστήματα και εφαρμογές.
9. Εφαρμογή προσαρμοσμένων μέτρων ασφάλειας με τη χρήση Indicators Of Compromise (IOC).

Με τα παραπάνω βήματα, εξασφαλίζουμε τον πλήρη περιορισμό του κινδύνου στα μολυσμένα συστήματα αξιοποιώντας βέλτιστες στρατηγικές. Τα περισσότερα από τα αναφερόμενα βήματα χρησιμοποιούνται για τον περιορισμό πολλών τύπων κακόβουλου λογισμικού και αποτελούν αναπόσπαστες στρατηγικές περιορισμού για τους ειδικούς ασφαλείας.

3.6.2 Διαδικασία εξάλειψης

Η διαδικασία εξάλειψης των μολυσμένων συστημάτων αποτελεί ένα από τα σημαντικότερα βήματα σε ένα περιστατικό ασφαλείας. Με την εξάλειψη, διασφαλίζουμε ότι τα συστήματα είναι καθαρά από οποιαδήποτε μόλυνση και εξασφαλίζουμε ότι το ίδιο συμβάν δεν θα επαναληφθεί στο μέλλον.

1. Ανακατασκευάστε τα παραβιασμένα συστήματα χρησιμοποιώντας αξιόπιστες πηγές για να εξαλείψετε τις κρυφές απειλές.
2. Διεξάγετε ενδεδεχείς σαρώσεις κακόβουλου λογισμικού για τον καθαρισμό των συστημάτων από κακόβουλα στοιχεία.
3. Αποκλείστε τους εντοπισμένους κακόβουλους τομείς και διευθύνσεις IP στις περιμέτρους του δικτύου.
4. Τερματίστε τυχόν κακόβουλες διεργασίες που εντοπίζονται στα επηρεαζόμενα τελικά σημεία.
5. Ασφαλίστε τους παραβιασμένους λογαριασμούς αλλάζοντας τους κωδικούς πρόσβασης και κλειδώνοντάς τους, εάν είναι απαραίτητο.
6. Διερευνήστε και απομακρύνετε παρόμοιες απειλές phishing από τα γραμματοκιβώτια άλλων χρηστών.
7. Αποκλείστε τις διευθύνσεις ηλεκτρονικού ταχυδρομείου που συνδέονται με τον επιτιθέμενο για να αποτρέψετε περαιτέρω επικοινωνίες.
8. Επαναφέρετε συστήματα από καθαρά αντίγραφα ασφαλείας για να διασφαλίσετε την ακεραιότητα των δεδομένων.
9. Επιβεβαιώστε ότι όλα τα εργαλεία και τα συστήματα ασφαλείας είναι ενημερωμένα και λειτουργικά.

10. Εφαρμόστε προσαρμοσμένες άμυνες με βάση τις ιδιαιτερότητες του περιστατικού για να αποτρέψετε την επανάληψη.
11. Διατηρήστε επαγρύπνηση για σημάδια επαναμόλυνσης, προσαρμόζοντας τις προτεραιότητες των ειδοποιήσεων ανάλογα με τις ανάγκες.
12. Προσαρμόστε τα προνόμια των χρηστών ώστε να ελαχιστοποιήσετε τον κίνδυνο, αφαιρώντας την περιττή διοικητική πρόσβαση.
13. Επιβολή πολιτικών για την απενεργοποίηση εκτελέσεων macros από μη αξιόπιστες πηγές για τον μετριασμό ενός φορέα επίθεσης.
14. Διασφαλίστε ότι οι κωδικοί πρόσβασης του τοπικού διαχειριστή είναι μοναδικοί για κάθε σύστημα, ώστε να παρεμποδίζεται το lateral movement.
15. Εξετάστε το ενδεχόμενο δημιουργίας whitelist εφαρμογών σε κρίσιμες υποδομές για τον αποκλεισμό μη εξουσιοδοτημένων εκτελέσεων.
16. Διαχωρίστε τους privileged λογαριασμούς από τους λογαριασμούς καθημερινής χρήσης για να μειώσετε τον κίνδυνο.
17. Επανεξετάστε και προσαρμόστε τις πολιτικές δικτύου για να αποκλείσετε την πρόσβαση σε κατηγορίες ιστοσελίδων υψηλού κινδύνου και να διασφαλίσετε ότι οι ρυθμίσεις ασφαλείας ευθυγραμμίζονται με τις βέλτιστες πρακτικές.
18. Λάβετε προληπτικά μέτρα για την απενεργοποίηση της εκτέλεσης πακέτων OLE στο Microsoft Word για να αποκλείσετε μια γνωστή μέθοδο εκμετάλλευσης.

Κάθε βήμα που έχει αναφερθεί παραπάνω, συμβάλλει είτε στην εξάλειψη του μολυσμένου συστήματος είτε στην οχύρωση του. Από την ανακατασκευή ενός συστήματος μέχρι και την χρήση καλών πρακτικών όπως ο διαχωρισμός privileged/καθημερινών λογαριασμών, όλα τα βήματα είναι απαραίτητα για την ομαλή λειτουργία του συστήματος και την εξασφάλιση ότι είναι οχυρωμένο κατάλληλα σε περίπτωση παρόμοιας επίθεσης.

3.7 Διαδικασία ανάκτησης

Η καταβολή λύτρων γενικά αποθαρρύνεται, καθώς δεν εξασφαλίζει την επίλυση του προβλήματος και μπορεί να ενθαρρύνει περαιτέρω επιθέσεις. Είναι σημαντικό να επικεντρωθείτε σε

προσπάθειες ανάκτησης που δεν συνεπάγονται παραχώρηση λύτρων.

1. **Αποκατάσταση δεδομένων:** Μόλις εξουδετερωθεί η απειλή, επαναφέρετε τα δεδομένα από επαληθευμένα καθαρά αντίγραφα ασφαλείας σε ασφαλή συστήματα που έχουν επιδιορθωθεί και βρίσκονται υπό συνεχή επιτήρηση.
2. **Χρήση εργαλείων αποκρυπτογράφησης:** Εξερευνήστε τα διαθέσιμα εργαλεία αποκρυπτογράφησης για τη συγκεκριμένη παραλλαγή ransomware που αντιμετωπίζετε. Το No More Ransom!³ Project παρέχει πολύτιμα εργαλεία που μπορεί να βοηθήσουν στην ανάκτηση κρυπτογραφημένων δεδομένων χωρίς την καταβολή λύτρων.
3. **Εξετάστε το ενδεχόμενο πληρωμής λύτρων μόνο ως έσχατη λύση:** Σε ακραίες περιπτώσεις όπου τα κρίσιμα δεδομένα είναι μη ανακτήσιμα και απαραίτητα για τη λειτουργία, μπορεί να εξεταστεί το ενδεχόμενο καταβολής λύτρων. Ωστόσο, αυτό θα πρέπει να είναι μια προσεκτικά σταθμισμένη απόφαση, λαμβάνοντας υπόψη:
 - (a) Διαβούλευση με όλους τους ενδιαφερόμενους φορείς για την κατανόηση των ευρύτερων συνεπειών.
 - (b) Αξιολόγηση των οικονομικών επιπτώσεων και των εκτιμήσεων στο πλαίσιο του οργανωτικού προϋπολογισμού.
 - (c) Νομικές, κανονιστικές και ασφαλιστικές επιπτώσεις που θα μπορούσαν να προκύψουν από μια τέτοια απόφαση.
 - (d) Κατανόηση της διαδικασίας και των τεχνολογιών που εμπλέκονται στην καταβολή των λύτρων, συμπεριλαμβανομένου του ρόλου τυχόν διαμεσολαβητών ή πλατφορμών.

Σε κάθε βήμα της διαδικασίας ανάκτησης, είναι ζωτικής σημασίας η τεκμηρίωση των ενεργειών, των αποφάσεων και των αποτελεσμάτων για την ενημέρωση των μελλοντικών μέτρων ασφαλείας και τη βελτίωση της ανθεκτικότητας έναντι παρόμοιων απειλών. Κατανοώντας τα παραπάνω βήματα, οι ενδιαφερόμενοι είναι κατάλληλα προετοιμασμένοι να ακολουθήσουν τις αναλυτικές διαδικασίες με στόχο την σωστή ανάκτηση των μολυσμένων συστημάτων.

³<https://www.nomoreransom.org/en/index.html>

Κεφάλαιο 4

Τεχνική Ανάλυση Κακόβουλου Λογισμικού

Στόχος του συγκεκριμένου κεφαλαίου είναι να χρησιμοποιήσουμε jupyter notebooks με σκοπό να δημιουργήσουμε ένα initial malware analysis kit. Όπως θα δούμε παρακάτω, ο κώδικας μας δίνει σημαντικές πληροφορίες αξιοπώντας εργαλεία όπως το VirusTotal και YARA rules με σκοπό να έχουμε μία αρχική εικόνα για το κακόβουλο λογισμικό. Μας καθοδηγεί βήμα-βήμα δίνοντας στην πορεία πληροφορίες και οδηγίες για την ορθή εκτέλεση του. Περιέχει επίσης διάφορες ασκήσεις μέσω των οποίων επεκτείνεται ο κώδικας με περισσότερες λειτουργίες.

Το πρώτο βήμα, είναι να κάνουμε import όλα τα απαραίτητα modules που θα χρειαστούν κατά την εκτέλεση του κώδικα, όπως φαίνεται παρακάτω.

Listing 4.1: *Importing libraries*

```
1
2 """
3 This notebook performs the initial stages of malware analysis.
4
5 ## How To
6 1. Place the malware samples into the malware directory
7 2. Walk through the steps on the notebook
8 3. Interact with the prompts
9 4. Perform the exercises along the way
10 """
11 import os
```

```

12 import hashlib
13 import requests
14 import YARA
15 from virustotal_python import Virustotal
16 from IPython.display import display, Markdown

```

File listing

Ξεκινώντας, διαλέγουμε τον φάκελο στον οποίο θα τοποθετήσουμε τα κακόβουλα αρχεία και θα τα εμφανίζουμε ώστε να επιβεβαιώσουμε ότι βρίσκονται στον κατάλληλο φάκελο.

```

1 """
2 Listing of the files in the Malware directory
3
4 ### Notes
5
6 Feel free to change the file directory and adjust it to your ↵
   environment. By default, it is set to ./malicious .
7
8 By default, the directory contains the EICAR file which is a harmless↵
   computer file that is used to test the effectiveness of ↵
   antivirus programs, it also contains another random test file.
9
10 """
11
12 file_directory_path = './malicious' # Directory containing files
13 files = [f for f in os.listdir(file_directory_path) if os.path.isfile(↵
   (os.path.join(file_directory_path, f)))]
14 print("Files found in the directory: \n")
15 for file in files:
16     print(file)

```

Με βάση τον κώδικα, όλα τα αρχεία πρέπει να τοποθετητούν στον φάκελο "malicious" όπου από εκεί θα αναλύονται με βάση τον υπόλοιπο κώδικα. Γενικότερα, είναι καλή πρακτική τα κακόβουλα αρχεία να είναι απομονωμένα σε έναν φάκελο ώστε να αποφύγουμε την ακούσια εκτέλεση τους.

VirusTotal API Key

Πριν προχωρήσουμε στην ανάλυση του αρχείου, πρέπει να δώσουμε το API key του VirusTotal ώστε να μπορέσουμε να επικοινωνήσουμε με το API. Αυτό θα μας χρειαστεί στη συνέχεια που θα αξιοποιήσουμε το hash του κάθε αρχείου ώστε να βρούμε αποτελέσματα μέσω του VirusTotal.

```

1
2 """
3 VirusTotal API Key Validation
4
5 Provide a valid VirusTotal key.
6
7 ### Notes
8
9 To get your VirusTotal API Key, you need to log in on the official ↵
    website, there, you can find the API Key in the upper right menu.
10
11 """
12
13 def validate_vt_api_key(key):
14     """ Validate the VirusTotal API key by making a test request. """
15     try:
16         vttotal_temp = Virustotal(API_KEY=key, API_VERSION="v3")
17         # Make a benign test call using a known file hash to check ↵
            the API key validity
18         response = vttotal_temp.request("files/908↵
            B64B1971A979C7E3E8CE4621945CBA84854CB98D76367B791A6E22B5F6D53↵
            ")
19         if response.status_code == 200:
20             return True
21         elif response.status_code == 403:
22             print("Invalid API key. Please re-enter.")
23             return False
24         else:
25             print(f"Failed to validate API Key: HTTP Status Code {↵
                response.status_code}. Response: {response.data}")
26             return False
27     except requests.exceptions.RequestException as e:

```

```

28         print(f"Network error during API request: {str(e)}")
29         return False
30     except Exception as e:
31         print(f"An error occurred: {str(e)}")
32         return False
33
34 # Loop to ensure the user enters a valid API key
35 valid_key = False
36 while not valid_key:
37     V_API_KEY = input("Enter your VirusTotal API key: ").strip()
38     valid_key = validate_vt_api_key(V_API_KEY)
39     if not valid_key:
40         print("Please enter a valid VirusTotal API key.")
41
42 print("API Key validated successfully.")

```

```

Enter your VirusTotal API key: 55b57b12c1a055bcc35c0a4064b45c061da59bb8cf5917
API Key validated successfully.

```

Σχήμα 4.17: *Key Validated*

Ασκηση: Με βάση την εικόνα 4.17, μπορούμε να δούμε ότι το κλειδί είναι σε clear text, είναι όμως καλή πρακτική τα κλειδιά και οι κωδικοί να μην είναι εμφανή κατά την πληκτρολόγηση τους ή αργότερα, ώστε να μην μπορούν να κλαπούν. Δοκιμάστε να κρύψετε το κλειδί ώστε να μην φαίνεται κατά την πληκτρολόγηση του ή σε οποιαδήποτε φάση εκτέλεσης του κώδικα.

Defanging

Στόχος του defanging που αναφέρεται παρακάτω, είναι να μετατρέψουμε τυχόν εκτελέσιμα αρχεία και URLs σε μη εκτελέσιμα, με στόχο να αποφύγουμε την ακούσια εκτέλεση τους. Στον κώδικα, αντικαθιστούμε την τελεία από κάθε αρχείο με "[dot]".

```

1  """
2  File defanging
3
4  Let's defang files to avoid misclicking them. The code provides ↵
    feedback based on your answer.

```

```
5
6 ## Notes
7
8 Defanging is a technique used to modify files or URLs in a way which ↵
9 makes them unclickable or executable.
10 """
11 def defang_filenames(directory, perform_defang, user_input):
12     files = os.listdir(directory)
13     all_defanged = True # Assume all are defanged unless proven ↵
14     otherwise
15     any_defanged = False # Track if any file has been defanged
16
17     for filename in files:
18         if not is_defanged(filename): # Check if the file needs ↵
19         defanging
20         all_defanged = False # Found a file that is not defanged
21         if perform_defang:
22             defanged_name = defang_filename(filename)
23             original_filepath = os.path.join(directory, filename)
24             new_filepath = os.path.join(directory, defanged_name)
25             os.rename(original_filepath, new_filepath)
26             any_defanged = True
27
28     if any_defanged:
29         return "DEFANGED"
30     elif all_defanged:
31         return "No actions needed, all files are already DEFANGED" #↵
32         All were already defanged
33     else:
34         return "NOT DEFANGED" if user_input.lower() == 'no' else "↵
35         INVALID INPUT"
36
37 def is_defanged(filename):
38     """Check if the filename is already defanged."""
39     return '[dot]' in filename or '[slash]' in filename or '[colon]' ↵
40     in filename
```

```

37 def defang_filename(filename):
38     """Defang the filename by replacing certain characters."""
39     defanged_name = filename.replace('.', '[dot]').replace('/', '[←
        slash]').replace(':', '[colon]')
40     return defanged_name
41
42 # User interaction for defanging decision
43 defang_choice = input("Do you want to defang the filenames? Yes/No: "←
    )
44 perform_defang = defang_choice.strip().lower() == 'yes'
45
46 # Directory containing files
47 file_directory_path = '/home/aggelos/Desktop/notebook/malicious'
48
49 # Execute defanging based on user choice and print the appropriate ←
    response
50 defanging_result = defang_filenames(file_directory_path, ←
    perform_defang, defang_choice)
51 print(defanging_result)

```

Ασκηση: Παρά το γεγονός ότι μετά την εκτέλεση του κώδικα τα αρχεία δεν είναι εκτελέσιμα, μπορεί ακόμη και απλά text αρχεία να περιέχουν κακόβουλα URLs που πιθανόν ακούσια να εκτελεστούν. Δοκιμάστε να επεκτήντε τον κώδικα ώστε να κάνει defang τα URLs ¹ που μπορεί να υπάρχουν εντός των αρχείων.

File Hash

Όταν διαχειριζόμαστε αρχεία, ένα από τα πιο χρήσιμα χαρακτηριστικά που μπορούμε να αξιοποιήσουμε στην διαδικασία διερεύνησης είναι το hash² του αρχείου. Μας δίνει την δυνατότητα να εξακριβώσουμε μέσω άλλων εργαλείων (βλ. VirusTotal) εάν πρόκειται για κάποιο γνωστό κακόβουλο αρχείο ή εάν απαιτείται περαιτέρω διερεύνηση.

```

1 """
2 Calculating the sha256 of each file
3

```

¹<https://isc.sans.edu/diary/Defang+all+the+things/22744>

²https://www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_Factsheet_FileHashings508C.pdf

```
4  ##Notes
5
6  Hashing gives us a unique fingerprint of a file , if a file is ↵
   slightly tempered with, the hash will change.
7
8  The hash can be used on the VirusTotal database to check if it is ↵
   malicious.
9
10 """
11
12 def sha256sum(filepath):
13     with open(filepath, 'rb') as file:
14         data = file.read()
15         h = hashlib.sha256(data)
16         return h.hexdigest()
17
18 hashes = {file: sha256sum(os.path.join(file_directory_path, file)) ↵
            for file in files}
19 for file, hash_val in hashes.items():
20     print(f"SHA256 of {file}: {hash_val}")
```

Άσκηση: Σε αυτό το σημείο, μπορούμε να αξιοποιήσουμε το strings command ώστε να δούμε εάν τα αρχεία περιέχουν συγκεκριμένες λέξεις που μας ενδιαφέρουν, όπως "password", "encrypt", κ.α.

Χρησιμοποιήστε την εντολή strings με στόχο να βρείτε πιθανά URLs, domains, IP Addresses ή συγκεκριμένα keywords. Αξιοποιώντας αυτό το εργαλείο, μπορούμε να χρησιμοποιήσουμε τις νέες πληροφορίες ώστε να εξειδικεύσουμε ακόμη περισσότερο την διερεύνηση μας, να αποκλείσουμε από συστήματα ασφαλείας IP Addresses ή/και domains ή να βρούμε κάποιο άλλο χρήσιμο στοιχείο.

VirusTotal Score

Το VirusTotal Score χρησιμοποιείται για τον προσδιορισμό του αριθμού των vendor που έχουν αναγνωρίσει ένα συγκεκριμένο αρχείο ως κακόβουλο. Αυτό το score ποικίλλει επειδή δεν χαρακτηρίζουν όλοι οι vendors τα ίδια αρχεία ως κακόβουλα. Οι λόγοι για αυτές τις αποκλίσεις συχνά περιλαμβάνουν διαφορές στους αλγόριθμους ανίχνευσης, όπως συστήματα

που βασίζονται σε υπογραφές έναντι συστημάτων που βασίζονται στη συμπεριφορά, ή διαφορές στην ευαισθησία των αλγορίθμων. Επιπλέον, η εστίαση της αγοράς ενός προμηθευτή - που απευθύνεται είτε σε επιχειρήσεις είτε σε καταναλωτές- μπορεί να επηρεάσει τα κριτήρια επισήμανσης των αρχείων. Τέλος, οι προσπάθειες μείωσης των false-positives αποτελεσμάτων συμβάλλουν επίσης στον τρόπο αξιολόγησης των αρχείων από τους προμηθευτές, επηρεάζοντας τη συνολική βαθμολογία του VirusTotal.

```

1  """
2  Check the files on VirusTotal
3
4  ### Notes
5
6  The VirusTotal Score indicates how many security vendors have flagged↵
   the specific file as malicious.
7
8  Not all vendors flag the same files as malicious for various reasons,↵
   most commonly:
9
10 - Variations in detection algorithms (Signature-based vs Behavioral↵
   based or algorithm sensitivity)
11 - Market focus (Enterprises vs Consumers)
12 - False positives mitigation
13 """
14
15 vttotal = Virustotal(API_KEY=V_API_KEY, API_VERSION="v3")
16 def check_virustotal(hash):
17     try:
18         resp = vttotal.request(f"files/{hash}")
19         score = f"{resp.data['attributes']['last_analysis_stats']['↵
           malicious']} / {sum(resp.data['attributes']['↵
           last_analysis_stats'].values())}" if resp.data['↵
           attributes']['last_analysis_stats']['malicious'] > 0 else↵
           "No detections"
20     except Exception as e:
21         score = "Not Found on VirusTotal"
22     return score
23
24 vt_scores = {file: check_virustotal(hash_val) for file, hash_val in ↵

```

```

        hashes.items() }
25 for file, score in vt_scores.items():
26     print(f"VirusTotal Score for {file}: {score}")

```

Οι πληροφορίες του VirusTotal είναι άκρως αξιόπιστες και χρησιμοποιείται από όλους τους ειδικούς. Μας δίνει μία ολοκληρωμένη εικόνα για την κατάσταση ενός αρχείου και αποτελεί ένα αναπόσπαστο κομμάτι στο οπλοστάσιο ενός ειδικού ασφαλείας.

Άσκηση: Προσπαθήστε να αξιοποιήσετε το VirusTotal ώστε να ελέγχει τυχόν URLs που μπορεί να εμφανιστούν, όπου επιστρέφει παρομοίως μία τιμή η οποία μας δείχνει την επικινδυνότητα του εκάστοτε URL. Με αυτόν τον τρόπο θα έχουμε μία πιο ολοκληρωμένη εικόνα, αξιοποιώντας όλες τις λειτουργίες του εργαλείου.

YARA Rules

Οι κανόνες YARA χρησιμοποιούνται κυρίως για τον εντοπισμό και την ταξινόμηση κακόβουλου λογισμικού. Λειτουργούν επιτρέποντας στους χρήστες να δημιουργούν προσαρμοσμένους κανόνες που περιγράφουν συγκεκριμένα patterns, τα οποία είναι τυπικά για κακόβουλα λογισμικά.

Όταν ένας κανόνας YARA εφαρμόζεται για τη σάρωση αρχείων, αναζητά αυτά τα καθορισμένα μοτίβα. Εάν ένα μοτίβο από έναν κανόνα εντοπιστεί σε ένα αρχείο, υποδηλώνει ότι το αρχείο μπορεί να είναι κακόβουλο ή να σχετίζεται με μια συγκεκριμένη οικογένεια κακόβουλου λογισμικού, ανάλογα με τα κριτήρια του κανόνα.

```

1 """
2 Load YARA rules and Scan Files
3
4 ## Notes
5
6 YARA rules are a tool used in cybersecurity to identify and classify ↵
   malware based on textual or binary patterns.
7
8 The default file path for YARA rules is ./YARA .|
9 """
10
11 YARA_rule_directory_path = './YARA'
12 rules = {}

```

```

13 for file in os.listdir(YARA_rule_directory_path):
14     if file.endswith('.yar'):
15         path = os.path.join(YARA_rule_directory_path, file)
16         with open(path, 'r') as f:
17             rules[file] = f.read()
18
19 compiled_rules = YARA.compile(sources=rules)
20 def scan_with_YARA(filepath, rules):
21     matches = rules.match(filepath)
22     return ", ".join([match.rule for match in matches]) if matches ←
        else "No matches"
23
24 YARA_results = {file: scan_with_YARA(os.path.join(file_directory_path←
    , file), compiled_rules) for file in files}
25 for file, result in YARA_results.items():
26     print(f"YARA Matches for {file}: {result}")

```

Άσκηση:

Δοκιμάστε να αξιοποιήσετε ή να δημιουργήσετε ένα YARA rule το οποίο θα έχει ως στόχο να ελέγχει εάν ένα συγκεκριμένο αρχείο ανήκει σε μία ομάδα κακόβουλου λογισμικού της επιλογής σας.

Δημιουργία YARA Rule για την ανίχνευση του EICAR αρχείου

Για την δημιουργία του YARA rule θα αξιοποιήσουμε το εργαλείο hexyl³ που θα χρησιμοποιηθεί για την απόκτηση του hex sequence του EICAR αρχείου. Τέλος, θα δημιουργήσουμε το YARA rule το οποίο θα ελέγχει κατά την εκτέλεση του εάν το hex sequence ταιριάζει με κάποιο από τα αρχεία.

Χρησιμοποιώντας το hexyl, μπορούμε να δούμε το hexadecimal sequence του EICAR αρχείου. Στην συνέχεια, τοποθετούμε το sequence εντός του YARA rule το οποίο κατά την εκτέλεση του θα συγκριθεί με το EICAR και θα μας δώσει την ανάλογη πληροφορία.

³<https://github.com/sharkdp/hexyl>

```

aggelos@aggelos:~/Desktop$ hexyl eicar
00000000  58 35 4f 21 50 25 40 41 50 5b 34 5c 50 5a 58 35 X50!P%@A P[4\PZX5
00000010  34 28 50 5e 29 37 43 43 29 37 7d 24 45 49 43 41 4(P^)7CC )7}$EICA
00000020  52 2d 53 54 41 4e 44 41 52 44 2d 41 4e 54 49 56 R-STANDA RD-ANTIV
00000030  49 52 55 53 2d 54 45 53 54 2d 46 49 4c 45 21 24 IRUS-TES T-FILE!$
00000040  48 2b 48 2a 0a 0a H+H*__

aggelos@aggelos:~/Desktop$ cat yara_eicar_rule
rule EICAR_Detection {
  meta:
    description = "EICAR pattern detection"
    author = "Aggelos"

  strings:
    $eicar_hex = { 58 35 4F 21 50 25 40 41 50 5B 34 5C 50 5A 58 35 34 28 50 5E 29 3
7 43 43 29 37 7D 24 45 49 43 41 52 2D 53 54 41 4E 44 41 52 44 2D 41 4E 54 49 56 49 52 5
5 53 2D 54 45 53 54 2D 46 49 4C 45 21 24 }

  condition:
    $eicar_hex
}

aggelos@aggelos:~/Desktop$ yara yara_eicar_rule eicar
EICAR_Detection eicar
aggelos@aggelos:~/Desktop$

```

Σχήμα 4.18: Δημιουργία YARA Rule

Στην προκειμένη περίπτωση, εκτελώντας το YARA Rule, έχουμε εξακριβώσει την ομάδα κακόβουλου λογισμικού που ανήκει το αρχείο και πιο συγκεκριμένα με το EICAR αρχείο.

Report

Τελειώνοντας, έχουμε ένα τελικό report με όλα τα ευρήματα μας ώστε να έχουμε μία ολοκληρωμένη εικόνα.

```

1
2 # Final Summary Report for Each File
3 print("\nFinal Summary Report:")
4 print("↵
      ↵
      ")
5 for file in files:
6     file_path = os.path.join(file_directory_path, file)
7     file_hash = hashes[file]
8     vt_score = vt_scores[file]
9     YARA_result = YARA_results[file]

```

```
10     defanged_status = "DEFANGED" if is_defanged(file) else "NOT ↵
    DEFANGED"
11
12     print(f"File Name: {file}")
13     print(f"File Hash: {file_hash}")
14     print(f"VirusTotal Score: {vt_score}")
15     print(f"YARA rule Matches: {YARA_result}")
16     print(f"Defanged: {defanged_status}")
17     print("↵
    n")
```

Final Summary Report:

```
-----  
File Name: eicar[dot]exe  
File Hash: e038b5168d9209267058112d845341cae83d92b1d1af0a10b66830acb7529494  
VirusTotal Score: 60 / 74  
Yara rule Matches: eicar  
Defanged: DEFANGED  
-----
```

```
File Name: text[dot]sh  
File Hash: 5b5b114edabdcdf33ad1dcc78f7c2e5be0ad3412a0c97afaaee2f2d585bc581bf  
VirusTotal Score: Not Found on VirusTotal  
Yara rule Matches: No matches  
Defanged: DEFANGED  
-----
```

Σχήμα 4.19: Τελικό Report με όλα τα ευρήματα

Όπως φαίνεται και στο 4.19, έχουμε μία ολοκληρωμένη εικόνα. Βλέπουμε για παράδειγμα ότι το EICAR αρχείο, έχει χαρακτηριστεί από πολλούς βέντορες ως κακόβουλο, έγινε επιτυχημένα defanged, το οποίο σημαίνει ότι επιτυχημένα άλλαξε την τελία σε [dot] (π.χ. EICAR.exe → EICAR[dot]exe) και έκανε match το YARA rule με το EICAR. Με αυτές τις πληροφορίες, μπορούμε να προχωρήσουμε σε περαιτέρω διερεύνηση, στοχευμένα με τη συμπεριφορά του εκάστοτε κακόβουλου αρχείου.

Κεφάλαιο 5

Συμπεράσματα

Στη παρούσα πτυχιακή διερευνήσαμε την ολοκληρωμένη ανάπτυξη και στρατηγική εφαρμογή ενός ειδικού playbook για ransomware και την δημιουργία ενός initial malware analysis kit, αποδεικνύοντας τον κρίσιμο ρόλο τους στην ενίσχυση της άμυνας της κυβερνοασφάλειας. Η επισκόπηση των διαφορετικών, αλλά συμπληρωματικών, πλαισίων και εργαλείων κυβερνοασφάλειας - συγκεκριμένα των MITRE ATT&CK, The Hive Project, Splunk και MISP – αποτελούν εργαλεία ανεκτίμητης αξίας τόσο στην πρόβλεψη όσο και στην αντιμετώπιση απειλών ransomware.

Το πλαίσιο MITRE ATT&CK αποτελεί ένα θεμελιώδες στοιχείο στην αντιμετώπιση κάθε περιστατικού, προσφέροντας ένα καλά τεκμηριωμένο και συνεχώς ενημερωμένο λεξικό τακτικών και τεχνικών απειλών. Η συμβολή του Splunk σε συνδυασμό με τα υπόλοιπα εργαλεία, περιστρέφεται γύρω από τις ισχυρές δυνατότητες ανάλυσης δεδομένων, οι οποίες ενισχύουν την ανίχνευση και την αντιμετώπιση περιστατικών. Η ενσωμάτωση του Splunk, αξιοποιεί την επεξεργασία δεδομένων σε πραγματικό χρόνο για τον γρήγορο εντοπισμό ενδείξεων δραστηριότητας ransomware, επιτρέποντας έτσι την ταχύτερη και αποτελεσματικότερη λήψη αποφάσεων κατά τη διάρκεια ενός περιστατικού ασφαλείας. Το TheHive έχει επίσης καθοριστικό ρόλο στην αντιμετώπιση ενός συμβάντος. Αξιοποιώντας τις δυνατότητες του TheHive για το συντονισμό των δραστηριοτήτων απόκρισης και τη διαχείριση πολλαπλών πτυχών των περιστατικών ασφαλείας,, η οποία είναι απαραίτητη για τη διαχείριση των πολύπλοκων επιθέσεων ransomware. Έπειτα από την επισκόπηση του MISP, φάνηκε ότι ο ρόλος του επικεντρώνεται γύρω από τη δύναμή του στην ανταλλαγή πληροφοριών σχετικά με απειλές. Η ενσωμάτωση του MISP διευκολύνει τη συγκέντρωση και τη διανομή πληροφοριών που

σχετίζονται με IoCs και τακτικές ransomware, το οποίο όχι μόνο ενισχύει την πρόληψη αλλά και εμπλουτίζει τη συλλογική βάση γνώσεων. Σε συνδυασμό με το ransomware playbook, το οποίο αναλύει διεξοδικά όλα τα βήματα αντιμετώπισης ενός τέτοιου περιστατικού, από την προετοιμασία και την αναγνώριση έως τον περιορισμό, την εξάλειψη και την ανάκτηση από το περιστατικό έχουμε μια ολοκληρωμένη λύση αντιμετώπισης περιστατικών. Τέλος, το initial malware analysis kit, μας παρέχει πολλές δυνατότητες στην φάση της αναγνώρισης και του περιορισμού μίας επίθεσης ransomware, αξιοποιώντας τα διάφορα εργαλεία που αναφέρθηκαν. Τέλος, ο κώδικας συμπεριλαμβάνει διάφορες ασκήσεις με στόχο να επεκτείνουν περαιτέρω τις λειτουργίες του και να βοηθήσουν τους ενδιαφερόμενους να κατανοήσουν καλύτερα τον στόχο του συγκεκριμένου εργαλείου.

Καθώς οι απειλές στον κυβερνοχώρο συνεχίζουν να εξελίσσονται, ιδίως στον τομέα του ransomware, η ανάγκη για συνεχείς ενημερώσεις και βελτιώσεις του εγχειριδίου είναι σαφής. Η μελλοντική έρευνα θα πρέπει να διερευνήσει την ενσωμάτωση αναδυόμενων τεχνολογιών και μεθοδολογιών, όπως η τεχνητή νοημοσύνη και η μηχανική μάθηση, για την πρόβλεψη πιθανών συμπεριφορών ransomware και την αυτοματοποίηση ενεργειών αντιμετώπισης. Αυτή η συνεχής βελτίωση θα διασφαλίσει ότι το εγχειρίδιο για το ransomware θα παραμείνει ένα ισχυρό, προληπτικό εργαλείο της κυβερνοασφάλειας, έτοιμο να προσαρμοστεί στις μεταβαλλόμενες τακτικές των επιτιθέμενων στον κυβερνοχώρο.

Βιβλιογραφία

- [1] Cyber Management Alliance. “How to Create NIST-Compliant Incident Response Playbooks”. In: *Cyber Management Alliance* (2023). URL: <https://www.cma-alliance.com/cybersecurity-blog/how-to-create-nist-compliant-incident-response-playbooks>.
- [2] S. Barnum. “Common Attack Pattern Enumeration and Classification: A General Schema and its Applications”. In: *Cyber Threat Intelligence*. Vol. 70. Advances in Information Security. Springer, Cham, 2019.
- [3] E. Bertino and E. Ferrari. “Big Data Security and Privacy”. In: *Big Data: Concepts, Methodologies, Tools, and Applications*. IGI Global, 2018.
- [4] Y. Bhattacharjee et al. “Designing Cybersecurity Playbooks for Strategic Decision Making”. In: *Designing Interactive Systems Conference 2021 (DIS ’21)*. Association for Computing Machinery. New York, NY, USA, 2021.
- [5] M. Bishop. “About Penetration Testing: A Review of Methods and Techniques”. In: *Foundations of Security Analysis and Design VIII*. Vol. 9808. Lecture Notes in Computer Science. Springer, Cham, 2015.
- [6] Jeimy J. Cano M. “Managing Uncertainty and Complexity: Emerging Challenges in Cyber Security”. In: *Information Systems and Technologies*. 2022. URL: https://link.springer.com/chapter/10.1007/978-3-031-04826-5_19.
- [7] Paul Cichonski et al. *Computer Security Incident Handling Guide*. Special Publication 800-61. National Institute of Standards and Technology. 2012. URL: <https://csrc.nist.gov/pubs/sp/800/61/r2/final>.
- [8] J.W. Cortada and M. Gordon. *Understanding Cyber Risk: Protecting Your Company and Society*. Wiley, 2020.

- [9] *Cybersecurity Evaluation Tool*. United States Computer Emergency Readiness Team. 2016.
- [10] Deloitte. *Cybersecurity, user interface, and you: Sugarcoating the security pill*. Deloitte Insights. <https://www2.deloitte.com/us/en/insights/topics/risk/cybersecurity-user-interface.html>. 2015.
- [11] H. Haas, M. Teixeira, and K. Geers. “The Janus Face of the ‘New Ways of War’ and the Role of Cyber Operations in the Framework of the Jus ad Bellum”. In: *Cyberthreats and International Law*. SpringerBriefs in Cybersecurity. Springer, Cham, 2019.
- [12] Angela Horneman and Justin Ray. “Benefits and Challenges of SOAR Platforms”. In: *SEI Insights* (2021). URL: <https://insights.sei.cmu.edu/blog/benefits-and-challenges-of-soar-platforms/>.
- [13] G. Killcrece et al. “Incident Management Playbooks: A New Method for Effective Response”. In: *Proceedings of the Conference*. Carnegie Mellon University, Pittsburgh. 2003.
- [14] Rick Van der Kleij, Geert Kleinhuis, and Heather Young. “Computer Security Incident Response Team Effectiveness: A Needs Assessment”. In: *Frontiers in Psychology* (2017). DOI: 10.3389/fpsyg.2017.02179. URL: <https://www.frontiersin.org/articles/10.3389/fpsyg.2017.02179/full>.
- [15] D. Lowe. “Cyber-Risk Management”. In: *Successful Cybersecurity Risk Management*. Auerbach Publications, CRC Press, 2019.
- [16] Surya Nepal Marthie Grobler Raj Gaire. “User, Usage and Usability: Redefining Human Centric Cyber Security”. In: *Frontiers* (2021). <https://www.frontiersin.org/articles/10.3389/fpsyg.2020.567905/full>.
- [17] C. Morgan. *Cybersecurity Program Development for Business*. Wiley, 2020.
- [18] G. O’Gorman and G. McDonald. *Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents*. Wiley, 2017.
- [19] P. Rajivan and C. Gonzalez. “Creative Persuasion: A Study on Adversarial Behaviors and Strategies in Phishing Attacks”. In: *Frontiers in Psychology* 11 (2020), p. 56.
- [20] J. Scambray. *Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions*. McGraw Hill, 2021.

- [21] Amazon Web Services. *AWS Security Incident Response Guide*. 2023. URL: <https://docs.aws.amazon.com/whitepapers/latest/aws-security-incident-response-guide/develop-incident-response-playbooks.html>.
- [22] P. Shedden et al. *Managing Cybersecurity Risk: Cases Studies and Solutions*. Routledge, 2020.
- [23] V. Todorov and B. De Decker. “On the Real-time Incident Response”. In: *Theory and Engineering of Complex Systems and Dependability. DepCoS-RELCOMEX 2015*. Vol. 365. Advances in Intelligent Systems and Computing. Springer, Cham, 2015.
- [24] I.A. Tøndel et al. “Security Practitioners in Context: Their Activities and Interactions with Other Stakeholders within Organizations”. In: *11th Workshop on Security and Trust Management (STM)*. Wrocław, Poland, 2014.
- [25] Yuntao Wang et al. “Combating Advanced Persistent Threats: Challenges and Solutions”. In: *arXiv* (2023). URL: <https://arxiv.org/abs/2309.09498>.
- [26] R. Werlinger, K. Hawkey, and K. Beznosov. “An integrated view of human, organizational, and technological challenges of IT security management”. In: *Information Management & Computer Security* 17.1 (2009), pp. 4–19.

Συντμήσεις

SIEM	Security Information and Event Management
ATT&CK	Adversarial Tactics, Techniques and Common Knowledge
IoC	Indicator of Compromise
US-CERT	United States Computer Emergency Readiness Team
MISP	Malware Information Sharing Platform
SOAR	Security Orchestration, Automation, and Response
SIRP	Security incident response planning
URL	Uniform Resource Locator
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
HTTP	HyperText Transfer Protocol

AD	Active Directory
KPI	Key Performance Indicator
MBO	Management by Objectives
API	Application Programming Interface
TTP	tactics, techniques, and procedures
UEBA	User and Entity Behavior Analytics
PAP	Permissible Actions Protocol
SMB	Server Message Block

Γλωσσάρι Ξενικών Όρων

Incident Management	Διαχείριση περιστατικών
Complimentary	Συμπληρωματικά
Repository	Αποθετήριο
Reconnaissance	Αναγνώριση
Resource Development	Ανάπτυξη πόρων
Initial Access	Αρχική πρόσβαση
Execution	Εκτέλεση
Persistence	Επιμονή
Privilege Escalation	Κλιμάκωση δικαιωμάτων
Defense Evasion	Αποφυγή Άμυνας
Behavioral Insights	Συμπεριφορικές γνώσεις

Dashboard	Ταμπλό
Threat Intelligence	Γνώση Απειλών
Adaptive Response Initiative	Πρωτοβουλία προσαρμοστικής απόκρισης
Integration	Ενσωμάτωση
lateral movement	Πλευρική Κίνηση
initial malware analysis kit	αρχικό κιτ ανάλυσης κακόβουλου λογισμικού
playbook	Εγχειρίδιο
Notebook	Σημειωματάριο
complimentary	Συμπληρωματικά
Security	Ασφάλεια
exploitation	Εκμετάλλευση Ευπαθειών
obsfucated	Απόκρυψη
keylogging	Καταγραφή πλήκτρων
credential dumping	Απόκτηση κωδικών πρόσβασης
Credential Access	Απόκτηση κωδικών πρόσβασης

investigation	Έρευνα
template engine	Μηχανή Προτύπων
multi-tenant environment	περιβάλλον πολλαπλών παρόχων
Automated Indicator Extraction and Enrichment	Αυτοματοποιημένη εξαγωγή και εμπλουτισμός δεικτών
Threat Analysis and Attribution	Ανάλυση απειλών και απόδοση ευθυνών
Patches	Ενημερώσεις
Vendor	Βέντορας