ENCRYPT 4.0

Joint Cyber Workforce Development Initiative to Enable the European Industry to Overcome the Shortage of Cybersecurity Professionals,

No. 2020-1-RO01-KA202-079983

O3: Documental battery on cyber-attacks

ΠΕΡΙΕΧΟΜΕΝΑ

Co-funded by the
Erasmus+ Programme
of the European Union

ΕΙΣΑΓΩΓΗ

Με την έλευση της πληροφορικής και την άνοδο της τέταρτης βιομηχανικής επανάστασης, οι επιχειρήσεις αντιμετωπίζουν νέες προκλήσεις που συνδέονται με την ασφάλεια στον κυβερνοχώρο και την προστασία των δεδομένων. Αυτό ισχύει ιδιαίτερα για τις μικρομεσαίες επιχειρήσεις παραγωγής, οι οποίες συχνά δεν διαθέτουν τους εσωτερικούς πόρους και την ικανότητα να αξιολογήσουν αποτελεσματικά τους κινδύνους κυβερνοασφάλειας που αντιστοιχούν στις νέες τεχνολογίες που βασίζονται στη βιομηχανία 4.0. Ταυτόχρονα, οι ΜΜΕ γίνονται όλο και συχνότερα θύματα διαφόρων εγκλημάτων στον κυβερνοχώρο. Σύμφωνα με την τελευταία έκθεση Verizon 2021 Data Breach Investigations Report *(Verizon, 2021)*, οι ΜΜΕ πέφτουν θύματα και είναι πολύ πιο ευάλωτες σε κυβερνοεπιθέσεις σε σύγκριση με τις μεγάλες επιχειρήσεις, καθώς δεν διαθέτουν πόρους, ανθρώπους, πληροφορίες και γενικότερα ικανότητα να αποτρέψουν τους κινδύνους μιας κυβερνοεπίθεσης.

Ταυτόχρονα, οι απειλές στον κυβερνοχώρο έχουν διαφορετικές πηγές και γίνονται ολοένα και πιο εξελιγμένες, για παράδειγμα, εάν οι ομάδες δεν έχουν βιώσει παρόμοια τρωτά σημεία και δεν έχουν σαφείς οδηγίες για το πώς να αντιδράσουν σε αυτά, μπορεί να χρειαστούν ημέρες ή και εβδομάδες για να αντιδράσουν σωστά, γεγονός που μπορεί να αποβεί μοιραίο για ορισμένες διαδικασίες παραγωγής. Σύμφωνα με την έκθεση 2021 SMB IT Security Report οι εργαζόμενοι που δεν ακολουθούν τις κατευθυντήριες γραμμές θεωρούνται ως το κορυφαίο εμπόδιο για την ασφάλεια στον κυβερνοχώρο και η τάση αυτή έχει επιδεινωθεί με την αύξηση της απομακρυσμένης εργασίας λόγω της πανδημίας COVID-19 *(Untangle, 2021).* Ωστόσο, όταν υπάρχει παραβίαση της ασφάλειας στον κυβερνοχώρο, δεν επηρεάζει μόνο τους ανθρώπους, αλλά μπορεί επίσης να προκαλέσει οικονομικές απώλειες, απώλεια της εμπιστοσύνης των πελατών και βλάβη της φήμης *(Acronis, 2021).*

Λαμβάνοντας υπόψη τα προαναφερθέντα, η κοινοπραξία Encrypt 4.0 ανέπτυξε το παρόν έγγραφο για να χρησιμεύσει ως εργαλείο τεχνογνωσίας που παρέχει πρόσβαση σε κρίσιμες αναλύσεις πραγματικών επιθέσεων στον κυβερνοχώρο και διδάγματα που αντλήθηκαν, καθώς και χάρτες πορείας για τον τρόπο πρόληψης, εντοπισμού, αντιμετώπισης και ανάκαμψης από αυτές.

Το «Encrypt 4.0 Documental battery on cyber-attacks» είναι ειδικά προσαρμοσμένο στις ανάγκες των μεταποιητικών ΜΜΕ της ΕΕ που δραστηριοποιούνται στο πλαίσιο της Βιομηχανίας 4.0 και αποτελεί μελέτες περιπτώσεων σχετικά με τις κυβερνοεπιθέσεις, η οποία αποσκοπεί στην υποστήριξη των ΜΜΕ για την ενίσχυση της κυβερνοασφάλειάς τους και την πρόληψη των κυβερνοεπιθέσεων.

ΔΟΜΗ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΑ

Το «Encrypt 4.0 Documental battery» περιέχει συνολικά **18 μελέτες περιπτώσεων**. Καθένας από τους εταίρους του ENCRYPT 4.0 έχει εκπονήσει 3 πραγματικές μελέτες περιπτώσεων κυβερνοεπιθέσεων, οι οποίες βασίζονται σε έρευνα γραφείου, προσωπική εμπειρία και παρατηρήσεις και σε εις βάθος συνεντεύξεις με διευθύνοντες συμβούλους, επαγγελματίες της κυβερνοασφάλειας και ειδικούς της πληροφορικής, οι οποίες καλύπτουν διάφορους τύπους κυβερνοεπιθέσεων και παρέχουν κριτική ανάλυση των λόγων των παραβιάσεων ασφαλείας, του τρόπου αντιμετώπισής τους και των συνεπειών τους.

Η κοινοπραξία ENCRYPT 4.0 δημιούργησε ένα ειδικό μοντέλο "PREVENT-IDENTIFY-RESPOND-RECOVER" (PIRR) που βασίζεται στο μοντέλο "Identify, Protect, Detect, Respond and Recover" του Εθνικού Ινστιτούτου Προτύπων και Τεχνολογίας (NIST). Ο τύπος των κυβερνοεπιθέσεων βασίζεται στο μοντέλο STRIDE[1] καθώς και στο πλαίσιο MITRE ATT&CK. Η ανάλυση του μοντέλου PIRR περιλαμβάνει 4 κύριες κατηγορίες/ενότητες με βάση τα κύρια βήματα για την καταπολέμηση ενός προβλήματος ασφάλειας στον κυβερνοχώρο, καθώς και ενότητες με τα διδάγματα που αντλήθηκαν (βλ. Σχήμα 1.).

Σχήμα 1. Κατηγορίες του μοντέλου "Πρόληψη - Εντοπισμός - Ανταπόκριση - Ανάκτηση" (PIRR)

[1] Μπορείτε να διαβάσετε περισσότερα για το μοντέλο STRIDE εδώ: Benjamin, P., 2018. Απομυθοποίηση των μοντέλων απειλών STRIDE [online]. DEV Community. Διαθέσιμο στη διεύθυνση: https://dev.to/pbnj/demystifying-stride-threat-models-230m

ΠΡΟΛΗΨΗ

Αυτή η ενότητα επικεντρώνεται στη μείωση του κινδύνου έκθεσης σε κυβερνοεπιθέσεις και στα προληπτικά μέτρα και για κάθε μελέτη περίπτωσης περιλαμβάνει τα εξής:

- Συγκεκριμένες πρακτικές ασφαλείας που τέθηκαν σε εφαρμογή και είχαν αποδεδειγμένα αποτελέσματα σε πραγματικές επιθέσεις στον κυβερνοχώρο,
- Παρανοήσεις για την ασφάλεια στον κυβερνοχώρο: πρακτικές που εφάρμοσε κάθε εταιρεία και είχαν μηδενικό ή και αρνητικό αντίκτυπο σε πραγματικά περιστατικά.

ΑΝΑΓΝΩΡΙΣΗ

Ο κύριος στόχος αυτής της ενότητας είναι να βοηθήσει τις ΜΜΕ να διακρίνουν μεταξύ των διαφόρων τύπων επιθέσεων στον κυβερνοχώρο που κατηγοριοποιούνται χρησιμοποιώντας το μοντέλο STRIDE και τα πλαίσια MITRE ATT&CK. Το μοντέλο STRIDE αντιπροσωπεύει ένα συστημοκεντρικό μοντέλο απειλών υψηλού επιπέδου που επικεντρώνεται στον εντοπισμό γενικών κατηγοριών επιθέσεων. Διαθέτει τις ακόλουθες 6 κατηγορίες:

+Spoofing

+Tampering

+Repudiation

+Information disclosure

+Denial of service

+Elevation of privilege

Για τους σκοπούς των μελετών περίπτωσης ENCRYPT 4.0 χρησιμοποιήθηκε το STRIDE για τον προσδιορισμό των απειλών σε υψηλότερο επίπεδο, ενώ το πλαίσιο MITRE ATT&CK εφαρμόστηκε για τον λεπτομερέστερο προσδιορισμό των επιθέσεων. Το πλαίσιο ATT&CK υιοθετεί σκόπιμα την οπτική γωνία του επιτιθέμενου για να βοηθήσει τους οργανισμούς να κατανοήσουν τον τρόπο με τον οποίο οι αντίπαλοι προσεγγίζουν, προετοιμάζονται και εκτελούν επιτυχώς τις επιθέσεις.

ΑΠΑΝΤΗΣΗ

Αυτή η ενότητα απεικονίζει τις καταστάσεις στις οποίες η απειλή είναι ήδη παρούσα, παρέχοντας ανάλυση πραγματικών επιθέσεων στον κυβερνοχώρο και συμβουλές για τον τρόπο αντίδρασης σε παρόμοιες περιπτώσεις μετά τον εντοπισμό τους. Οι επιθέσεις στον κυβερνοχώρο στο πλαίσιο των περιπτωσιολογικών μελετών περιγράφονται με την ακόλουθη μορφή:

- ΠΟΙΟΣ: ο επιτιθέμενος
- ΣΕ ΠΟΙΟΝ: ο οργανισμός-στόχος
- ΓΙΑΤΙ: τα κίνητρα πίσω από την επίθεση (ήταν τυχαία ή στοχευμένη)
- ΤΙ: η στοχοθετημένη ιδιοκτησία
- ΠΩΣ: περιγραφή της επίθεσης και ποιες ήταν οι τεχνικές που χρησιμοποιήθηκαν.
- ΣΤΡΑΤΗΓΙΚΗ: πώς αντιμετωπίστηκε η απειλή και τα μέτρα που είχαν μηδενικό ή αρνητικό αποτέλεσμα.

ΑΝΑΚΑΜΨΗ

Η ενότητα παρέχει πληροφορίες σχετικά με τις συνέπειες της επίθεσης, καθώς και ανάλυση σχετικά με τον τρόπο αποκατάστασης του συστήματος μετά την καταστροφή ορισμένων διεργασιών και την ανάκτηση της πρόσβασης στα δεδομένα που χάθηκαν, με βάση τις πραγματικές περιπτώσεις επίθεσης που περιγράφονται στην ενότητα ΑΝΤΙΜΕΤΩΠΙΣΗ. Η ενότητα ακολουθεί τα μοντέλα STRIDE & MITRE ATT&CK περιγράφοντας πρακτικές ανάκτησης με βάση κάθε συγκεκριμένη ομάδα απειλών στον κυβερνοχώρο που παρουσιάζονται στην ενότητα ΑΝΑΓΝΩΡΙΣΗ.


ΜΕΛΕΤΕΣ
ΠΕΡΙΠΤΩΣΕΩΝ

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 1: THE REVERSE SHELL

Ο ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Η Innovalia Association είναι ένα ιδιωτικό και ανεξάρτητο τεχνολογικό κέντρο που δημιουργήθηκε από τον όμιλο Innovalia προκειμένου να διαμορφώσει μια κρίσιμη μάζα ικανή να επιτύχει με επιτυχία τις μακροπρόθεσμες ερευνητικές φιλοδοξίες και τους στρατηγικούς στόχους του. Η Innovalia είναι μια συμμαχία για τεχνολογικές ΜΜΕ με έδρα την Ισπανία. Έχει διεθνή παρουσία με γραφεία στη Χώρα των Βάσκων, τη Μαδρίτη, την Καταλονία, τις Κανάριες Νήσους, την Ευρώπη, την Ασία, τη Μέση Ανατολή, την Κεντρική και τη Νότια Αμερική. Από την ίδρυσή της, η Ένωση Innovalia έχει αναπτύξει ιδιαίτερη ευαισθησία και επίγνωση των ιδιαίτερων χαρακτηριστικών των ΜΜΕ που βασίζονται στην τεχνολογία. Σήμερα, έχει καταστεί ηγέτης στον τομέα της E&A από και για τις ΜΜΕ στην Ισπανία. Προσφέρει επίσης λύσεις για τη διευκόλυνση των διεθνών διαδικασιών καινοτομίας που απευθύνονται σε ΜΜΕ. Ως τεχνολογικός παράγοντας του τεχνολογικού δικτύου της Χώρας των Βάσκων (Innobasque), η Innovalia συγκεντρώνει τις δεξιότητες, τα εργαστήρια και τους πόρους των εταιρειών που ίδρυσαν την ένωση.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Οι πληροφορίες για την παρούσα μελέτη περίπτωσης συγκεντρώθηκαν μέσω συνέντευξης σε βάθος με τον τεχνικό πληροφορικής της επιχείρησης. Κατά τη διάρκεια της αλληλεπίδρασης ο ερευνητής έθεσε τις αρχικές ερωτήσεις, έτσι ώστε ο ερωτηθείς να ενθαρρυνθεί να απαντήσει. Οι πληροφορίες που έλειπαν συμπληρώθηκαν εκ των υστέρων με τα στοιχεία που παρείχε ο ερωτηθείς.

ΠΡΟΛΗΨΗ

Η πρακτική που εφάρμοζε η Innovalia πριν από το περιστατικό ήταν η εγκατάσταση ενός **λογισμικού τείχους προστασίας**.

Ειδικές πρακτικές ασφαλείας:

- ☑ **την ευαισθητοποίηση των εργαζομένων σχετικά με τα αναξιόπιστα μηνύματα**. Σε αυτή την περίπτωση, ένας χάκερ έστειλε ένα φαινομενικά νόμιμο μήνυμα ηλεκτρονικού ταχυδρομείου ζητώντας από τους υπαλλήλους μας να κάνουν κλικ σε έναν σύνδεσμο στο μήνυμα για να επαναφέρουν τον κωδικό πρόσβασης, με το

"Η έγχυση εντολών είναι μια επίθεση στον κυβερνοχώρο κατά την οποία ένας εισβολέας αναλαμβάνει τον έλεγχο του λειτουργικού συστήματος του κεντρικού υπολογιστή εισάγοντας κώδικα σε μια ευάλωτη εφαρμογή μέσω μιας εντολής. Αυτός ο κώδικας εκτελείται ανεξάρτητα από οποιονδήποτε μηχανισμό ασφαλείας και μπορεί να χρησιμοποιηθεί για την κλοπή δεδομένων, την κατάρρευση συστημάτων, τη ζημιά σε βάσεις δεδομένων, ακόμη και την εγκατάσταση κακόβουλου λογισμικού που μπορεί να χρησιμοποιηθεί αργότερα". (StackHawn, 2022)

πρόσχημα ότι είχαν καταγραφεί αρκετές ανεπιτυχείς προσπάθειες σύνδεσης.

☑ **την εγκατάσταση εσωτερικών τειχών προστασίας** για την ενίσχυση του τυπικού εξωτερικού τείχους προστασίας. Όταν το προσωπικό εργαζόταν από το σπίτι του κατά τη διάρκεια της πανδημίας COVID-19, έπρεπε να εγκαταστήσει τείχος προστασίας στο οικιακό του δίκτυο.

ΑΝΑΓΝΩΡΙΣΗ

Ο τύπος και η φύση της κυβερνοεπίθεσης ήταν: **Apache web server της εταιρείας μέσω απομακρυσμένης εκτέλεσης εντολών**. Αυτός ο τύπος επίθεσης μπορεί να περιγραφεί λεπτομερώς σύμφωνα με το MITRE ATT&CK framework, όπως φαίνεται παρακάτω.

☑ Αναγνώριση: Ενεργή σάρωση: Σάρωση μπλοκ IP και σάρωση ευπαθειών

☑ Αρχική πρόσβαση: Εξωτερικές απομακρυσμένες υπηρεσίες

☑ Εκτέλεση: Διερμηνέας εντολών και σεναρίων: Shell

☑ Κλιμάκωση προνομίων:

- Έγχυση διαδικασίας: Έγχυση Βιβλιοθήκης δυναμικής σύνδεσης, Έγχυση φορητού εκτελέσιμου αρχείου, Παρακώλυση εκτέλεσης νήματος, Ασύγχρονη κλήση διαδικασίας, Τοπική αποθήκευση νήματος, Κλήσεις συστήματος Ptrace, Μνήμη Proc, Εγχυση μνήμης επιπλέον παραθύρου,
- Εκτέλεση με ενεργοποίηση συμβάντος: Unix Shell Τροποποίηση παραμέτρων,

☑ Αμυντική αποφυγή: Διαδικασία και template Injection

☑ Διείσδυση: Μεταφορά δεδομένων σε λογαριασμό Cloud.

☑ Επιπτώσεις:

- Χειραγώγηση δεδομένων: Χειρισμός δεδομένων κατά τη διάρκεια εκτέλεσης
- Στάση υπηρεσίας
- Τερματισμός λειτουργίας/επανεκκίνηση συστήματος

ΑΠΑΝΤΗΣΗ

☑ **ΠΟΙΟΣ:** Ο επιτιθέμενος δεν μπόρεσε να αναγνωριστεί με ακρίβεια. Μόνο ο τόπος καταγωγής, η Κίνα, ήταν γνωστός.

☑ **ΣΕ ΠΟΙΟΝ:** Σύλλογος Innovalia

- ☑ **ΓΙΑΤΙ:** Ήταν τυχαίο
- ☑ **ΤΙ:** Σύστημα της οργάνωσης Innovalia
- ☑ **ΠΩΣ:** Έγχυση διαδικασίας με απομακρυσμένη εκτέλεση εντολών.
- ☑ **ΣΤΡΑΤΗΓΙΚΗ:** Η απειλή αντιμετωπίστηκε με το τείχος προστασίας που είχε ο διακομιστής εκείνη τη στιγμή. Ακολουθήστε τα βήματα που περιγράφονται στην ακόλουθη ενότητα, σχετικά με τον τρόπο αποκλεισμού των Ips

ΑΝΑΚΑΜΨΗ

Οι κύριες συνέπειες της επίθεσης ήταν:

- ☑ Συμβιβασμός του συστήματος
- ☑ Έρευνα και ανάλυση
- ☑ Ενημέρωση της έκδοσης του διακομιστή
- ☑ Αλλαγή διαπιστευτηρίων

Η **στρατηγική αποκατάστασης** επικεντρώθηκε στον αποκλεισμό της IP μέσω του τείχους προστασίας:

Πρώτα απ' όλα, συνδεθείτε στο διακομιστή στον οποίο πρέπει να μπλοκάρετε τη διεύθυνση IP. Στη συνέχεια, κάντε κλικ στο κουμπί Έναρξη, πληκτρολογήστε Τείχος προστασίας των Windows με προηγμένη ασφάλεια και πατήστε Enter. Στο αριστερό παράθυρο, κάντε κλικ στην επιλογή Εισερχόμενοι κανόνες για να εμφανιστούν οι τρέχουσες ρυθμίσεις κανόνων στο μεσαίο παράθυρο.

Στο δεξιό παράθυρο, κάντε κλικ στην επιλογή «Ενέργειες» > «Νέος κανόνας»: Για «τύπο κανόνα», επιλέξτε «Προσαρμοσμένο» και κάντε κλικ στο «Επόμενο», για «Πρόγραμμα», επιλέξτε «Όλα τα προγράμματα» και κάντε κλικ στο «Επόμενο», για «Πρωτόκολλο και θύρες», επιλέξτε «Οποιοδήποτε» από το αναπτυσσόμενο μενού «Τύπος πρωτοκόλλου» και κάντε κλικ στο «Επόμενο» και για «Πεδίο εφαρμογής»: στην περιοχή «Σε ποιες απομακρυσμένες διευθύνσεις IP εφαρμόζεται αυτός ο κανόνας», επιλέξτε την επιλογή «Ακτινική»: Αυτές οι διευθύνσεις IP: Κάντε κλικ στο κουμπί «Προσθήκη».

Στη συνέχεια, πληκτρολογήστε τη διεύθυνση IP που θέλετε να αποκλείσετε από το διακομιστή και κάντε κλικ στο κουμπί «OK». Μπορείτε επίσης να επιλέξετε να αποκλείσετε ένα εύρος διευθύνσεων IP επιλέγοντας την επιλογή «Εύρος της διεύθυνσης IP: ακτινική». Αφού ολοκληρώσετε την προσθήκη των διευθύνσεων IP, κάντε κλικ στο κουμπί Επόμενο. Για την επιλογή Ενέργεια, επιλέξτε Αποκλεισμός της σύνδεσης και κάντε κλικ στο κουμπί «Επόμενο». Για το «Προφίλ», αφήστε όλες τις επιλογές επιλεγμένες και κάντε κλικ στο κουμπί «Επόμενο». Για «Όνομα», δώστε στον κανόνα ένα περιγραφικό όνομα, όπως για παράδειγμα «Μαύρη λίστα Ips». Μπορείτε επίσης να εισαγάγετε μια προαιρετική περιγραφή του κανόνα. Κάντε κλικ στο κουμπί «Finish (Τέλος)». Ο πρόσφατα δημιουργημένος κανόνας με το συγκεκριμένο όνομα εμφανίζεται τώρα στο μεσαίο παράθυρο κανόνων εισερχομένων. Για να ταξινομήσετε τους κανόνες αλφαβητικά με βάση το όνομα, μπορείτε να κάνετε κλικ στην επικεφαλίδα της στήλης «Όνομα». Εάν πρέπει να απενεργοποιήσετε τον κανόνα, κάντε δεξί κλικ στον κανόνα στη λίστα και επιλέξτε «Disable Rule (Απενεργοποίηση κανόνα)». Εάν πρέπει να τροποποιήσετε το πεδίο εφαρμογής των διευθύνσεων IP για τον κανόνα, κάντε δεξί κλικ στον κανόνα στη λίστα και κάντε κλικ στην επιλογή «Ιδιότητες». Στη συνέχεια, κάντε

κλικ στην καρτέλα «Πεδίο εφαρμογής», κάντε τις απαραίτητες αλλαγές και κάντε κλικ στο κουμπί «Εφαρμογή».

ΔΙΔΑΓΜΑΤΑ

Μάθαμε ότι είναι καλύτερο να έχουμε ορισμένα προληπτικά και αμυντικά μέτρα, τα οποία είναι χρήσιμα για αυτού του είδους τις επιθέσεις, όπως:

- ☑ Για να διατηρείτε τον διακομιστή ενημερωμένο
- ☑ Για να προσθέσετε παρακολούθηση στο μηχάνημα διακομιστή
- ☑ Για την κατάτμηση του δικτύου σε VLANS και
- ☑ Για την απομόνωση μηχανημάτων που εκτίθενται στην ύπαιθρο.

"Το 2021, το 83% των οργανισμών ανέφεραν ότι δέχθηκαν επιθέσεις phishing. Το 2022, αναμένεται να σημειωθούν επιπλέον έξι δισεκατομμύρια επιθέσεις". (CyberTalk, 2022)

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 2: Η ΑΠΕΡΙΣΚΕΨΙΑ ΕΝΟΣ ΕΡΓΑΖΟΜΕΝΟΥ

ΠΡΟΛΗΨΗ

Ο οργανισμός εφάρμοσε Σύστημα Ανίχνευσης Εισβολών (IDS), το οποίο παρακολουθεί το δίκτυο της CARSA για κακόβουλη δραστηριότητα ή παραβιάσεις της πολιτικής. Η CARSA εφαρμόζει λογισμικό τείχους προστασίας για την προστασία του δικτύου και του συστήματός της από μη εξουσιοδοτημένη πρόσβαση.

Οι συγκεκριμένες πρακτικές ασφαλείας που τέθηκαν σε εφαρμογή και είχαν αποδεδειγμένα αποτελέσματα σε άλλες επιθέσεις στον κυβερνοχώρο είναι οι εξής:

Επικύρωση και εξυγίανση των εισόδων: Σαρώστε για χαρακτήρες διαφυγής και άλλα ειδικά σύμβολα για τη γλώσσα της εφαρμογής και το λειτουργικό σύστημα, όπως σήματα σχολίων, χαρακτήρες τερματισμού γραμμής και οριοθέτες εντολών. Εάν η εφαρμογή αναμένει μόνο ένα περιορισμένο σύνολο τιμών, αποδεχτείτε μόνο αυτές τις τιμές, για παράδειγμα, με λευκή λίστα ή με υπό όρους ενεργοποίηση.

Αποφυγή ευάλωτων δομών αξιολόγησης: αποφεύγουμε τη χρήση της "eval()" και ισοδύναμων συναρτήσεων σε ακατέργαστες εισόδους χρήστη. Το CARSA χρησιμοποίησε ειδικά χαρακτηριστικά της γλώσσας για την ασφαλή επεξεργασία των ορίων που παρέχονται από τον χρήστη.

Κλειδώστε τον διερμηνέα: Εάν έχετε τον έλεγχο της διαμόρφωσης του διακομιστή, είναι προτιμότερο να περιορίσετε τη λειτουργικότητα του διερμηνέα στο ελάχιστο που απαιτείται για την εφαρμογή, ώστε να αποτρέψετε την κλιμάκωση σε έγχυση εντολών συστήματος. Για

παράδειγμα, αν η εφαρμογή PHP σας δεν χρησιμοποιεί τη συνάρτηση system(), μπορείτε να απενεργοποιήσετε αυτή τη συνάρτηση στο αρχείο php.ini καθορίζοντάς την στην οδηγία disable_functions. Οι συνήθεις απενεργοποιημένες συναρτήσεις για την PHP περιλαμβάνουν: exec(), passthru(), shell_exec(), system(), proc_open(), popen(), curl_exec(), curl_multi_exec(), parse_ini_file() και show_source().

Ελέγξτε τον κωδικό μας: CARSA χρησιμοποίησε εργαλεία στατικού ελέγχου κώδικα για να ανιχνεύσει ευπάθειες που σχετίζονται με την επικύρωση εισόδου και την ανασφαλή αξιολόγηση.

Σάρωση των εφαρμογών: ο οργανισμός χρησιμοποίησε έναν σαρωτή για να διασφαλίσει ότι οι εφαρμογές είναι ασφαλείς από διάφορους τύπους επιθέσεων. Για παράδειγμα, η CARSA διαθέτει ένα σύστημα ανίχνευσης εισβολών.

ΑΝΑΓΝΩΡΙΣΗ

Η κυβερνοεπίθεση σημειώθηκε στο πλαίσιο της CARSA και ο τύπος της ήταν **"επίθεση ηλεκτρονικού ψαρέματος**". Η επίθεση phishing είναι ένας τύπος επίθεσης κοινωνικής μηχανικής που χρησιμοποιείται συχνά για την κλοπή δεδομένων χρηστών, συμπεριλαμβανομένων των διαπιστευτηρίων σύνδεσης.

Σύμφωνα με το μοντέλο STRIDE, αυτός ο τύπος επίθεσης έχει ως "Απειλή" την αύξηση των προνομίων, επειδή η ιδιότητα που παραβιάζεται είναι η "εξουσιοδότηση". Σε αυτόν τον τύπο κυβερνοεπίθεσης, ο χρήστης επιτρέπει σε κάποιον να κάνει κάτι που δεν έχει εξουσιοδότηση να κάνει.

Σύμφωνα με το MITRE ATT&CK framework, η επίθεση αυτή είναι:

- ☑ Αναγνώριση: Ψάρεμα για πληροφορίες: Spearphishing service, spearphishing attachment και spearphishing link.
- ☑ Αρχική πρόσβαση: Συνημμένα αρχεία, σύνδεσμος ή μέσω υπηρεσίας.
- ☑ Εκτέλεση: Οι αντίπαλοι μπορούν να στείλουν μηνύματα phishing για να αποκτήσουν πρόσβαση στα συστήματα των θυμάτων. Όλες οι μορφές του phishing είναι ηλεκτρονικά μεταδιδόμενη κοινωνική μηχανική. Το phishing μπορεί να είναι στοχευμένο, γνωστό ως spearphishing. Στο spearphishing, ο αντίπαλος στοχεύει ένα συγκεκριμένο άτομο, εταιρεία ή κλάδο. Γενικότερα, οι αντίπαλοι μπορούν να διεξάγουν μη στοχευμένο phishing, όπως σε μαζικές εκστρατείες spam με κακόβουλο λογισμικό.
- ☑ Ανακάλυψη: η ανίχνευση μπορεί να γίνει μέσω: ή την κυκλοφορία του δικτύου (περιεχόμενο ή ροή).
- ☑ Πλευρική κίνηση: Πλευρική κίνηση: Εσωτερικό spearphishing
- ☑ Διείσδυση: εξερχόμενο ταχυδρομείο, λήψεις σε μη ασφαλείς συσκευές, μεταφορτώσεις σε εξωτερικές υπηρεσίες και μη ασφαλής συμπεριφορά στο νέφος.
- ☑ Αντίκτυπος: απώλεια ευαίσθητων δεδομένων, βλάβη της φήμης, απομάκρυνση πελατών ή πελατών, κόστος διακοπής λειτουργίας κ.λπ.

ΑΠΑΝΤΗΣΗ

ΠΟΙΟΣ: Ο επιτιθέμενος ήταν ένα άγνωστο εξωτερικό πρόσωπο/οργανισμός, μέσω ενός υπαλλήλου της CARSA.
ΣΕ ΠΟΙΟΝ: Τα διαπιστευτήρια για την πρόσβαση σε ένα λογισμικό πληρωμής (όχι δημόσιο ή ανοικτού κώδικα).
ΓΙΑΤΙ: Η κλοπή διαπιστευτηρίων καθώς και ευαίσθητων πληροφοριών οντοτήτων.
ΤΙ: Δεδομένα και κωδικοί πρόσβασης
ΠΩΣ: Ενας εργαζόμενος εγκατέστησε λογισμικό που δεν επιτρεπόταν από την εταιρεία, όπως ορίζεται στην πολιτική της εταιρείας. Αυτό το είδος λογισμικού δεν επιτρεπόταν λόγω αμφιβόλου αξιοπιστίας και ασφάλειας. (Γενικά, όλο το λογισμικό που εγκαθίσταται στους υπολογιστές των εργαζομένων πρέπει να εποπτεύεται από το τεχνικό προσωπικό πληροφορικής της οντότητας). Αυτό το λογισμικό είχε ένα δικτυακό "δούρειο ίππο". υπάρχουν διάφοροι τρόποι με τους οποίους ένα δούρειο ίππο επιτίθεται σε ένα σύστημα, στη συγκεκριμένη περίπτωση, επρόκειτο για ένα "δούρειο ίππο infostealer", όπως ακούγεται, αυτό το δούρειο ίππο κυνηγάει τα δεδομένα του μολυσμένου υπολογιστή σας.
ΣΤΡΑΤΗΓΙΚΗ: Η στρατηγική που ακολουθήθηκε ήταν ο εντοπισμός της διεύθυνσης mac για τον εντοπισμό του μολυσμένου μηχανήματος και του υπεύθυνου υπαλλήλου. Αργότερα, αφαιρέθηκε το λογισμικό καθώς και ο ιός.

ΑΝΑΚΑΜΨΗ

ΕΠΙΠΤΩΣΗ: κλοπή διαπιστευτηρίων χρηστών σε τοπικό επίπεδο

ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ:

☑ Μέσω της διεύθυνσης MAC ξέραμε σε ποιον υπάλληλο γινόταν επίθεση, χωρίς ο ίδιος να το καταλάβει.
☑ Απεγκαταστάθηκε λογισμικό που δεν έπρεπε να έχει εγκατασταθεί
☑ εκτελέστηκαν προγράμματα antivirus και antimalware στο συγκεκριμένο μηχάνημα.
☑ Αλλαγή διαπιστευτηρίων χρήστη που έχουν παραβιαστεί

ΚΑΛΥΤΕΡΗ ΣΤΡΑΤΗΓΙΚΗ: θα μπορούσε να έχει διαμορφωθεί ολόκληρος ο υπολογιστής, επειδή ποτέ δεν μπορείτε να είστε σίγουροι για την πλήρη εξάλειψή του.

ΔΙΔΑΓΜΑΤΑ

Αύξηση της υπευθυνότητας των εργαζομένων μέσω:

- ☑ εκπαίδευση με σύντομες διαλέξεις σχετικά με τη σημασία της μη εγκατάστασης απροειδοποίητου λογισμικού και επιβεβαίωση της ασφάλειας από την ομάδα τεχνικής υποστήριξης και,
- ☑ να θυμάστε τις πολιτικές ασφαλείας της εταιρείας και τους κοινούς κανονισμούς ασφαλείας στην κυβερνοασφάλεια.
- ☑ Ενημέρωση του λογισμικού των μηχανημάτων της εταιρείας (λογισμικό: Windows και προγράμματα προστασίας από ιούς). Να υπενθυμίζει στους υπαλλήλους να εκτελούν αρκετές φορές τη σάρωση κατά των ιών.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 3: Η ΠΙΣΤΩΤΙΚΗ ΚΑΡΤΑ ΣΕ ΕΝΑ ΜΙΚΡΟΜΕΣΑΙΟ ΚΑΤΑΣΤΗΜΑ ΜΕΣΩ WIFI

Ο ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Το **Bodegas Monje** βρίσκεται σε έναν εξαιρετικό θύλακα του νησιού της Τενερίφης, στο μέρος που είναι γνωστό ως "La Hollera" στο δήμο El Sauzal με θέα τον Teide. Μια μακρά παράδοση οινοπαραγωγών συνοδεύει την οικογένεια Monje από το 1750. Τα δρύινα βαρέλια και τα σύγχρονα συστήματα εκχύλισης συνυπάρχουν για να προσδώσουν στους κόκκινους, λευκούς και ροζέ οίνους έναν ιδιαίτερο χαρακτήρα και γεύσεις, οι οποίες είναι απόλυτα προσαρμοσμένες στην καλύτερη γαστρονομία των Καναρίων Νήσων. Αυτό το οινοποιείο φιλοξενεί επίσης πολιτιστικές, γαστρονομικές και ψυχαγωγικές πρωτοβουλίες που διευρύνουν τα όρια του κρασιού και το επιστρέφουν στο κοινωνικό περιβάλλον από το οποίο ιστορικά προέρχεται, μια πραγματική δέσμευση για τον οινοτουρισμό: Wine&Tours.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ;

Η μέθοδος που εφαρμόστηκε για τη συλλογή των πληροφοριών για την παρούσα μελέτη περίπτωσης ήταν μια συνέντευξη σε βάθος.

ΠΡΟΛΗΨΗ

Ο οργανισμός δεν εφάρμοζε καμία πρακτική κυβερνοασφάλειας πριν από αυτό το συμβάν. Διαθέτει μόνο ένα τείχος προστασίας στον πάροχο υπηρεσιών διαδικτύου (Router Movistar).

Οι ειδικές πρακτικές ασφαλείας που εφαρμόστηκαν στο Bodegas Monje και είχαν αποδεδειγμένα αποτελέσματα στην πρόληψη τέτοιου είδους συμβάντων προγραμματίστηκαν μετά το συμβάν. Ειδικότερα, οι ενέργειες που ελήφθησαν ήταν επιτυχείς στην αποτροπή περαιτέρω επιθέσεων παρόμοιας φύσης.

ΑΝΑΓΝΩΡΙΣΗ

Ενας πελάτης της εγκατάστασης μπήκε στην εταιρεία για να καταναλώσει τα παραγόμενα προϊόντα και συνδέθηκε στο διαδίκτυο μέσω του δικτύου WIFI. Η κυβερνοεπίθεση εντοπίστηκε από τον ίδιο τον επηρεαζόμενο πελάτη. Το εν λόγω πρόσωπο εντόπισε κινήσεις στους τραπεζικούς του λογαριασμούς με ηλεκτρονικές πληρωμές που έγιναν με την πιστωτική του κάρτα αλλά όχι από τον ίδιο. Όλες αυτές οι κινήσεις έγιναν αμέσως μετά την επίσκεψή του στην εταιρεία "Bodegas Monje".
Ο πελάτης ειδοποίησε την τράπεζα να προσπαθήσει να ακυρώσει αυτές τις πληρωμές και να μπλοκάρει την κάρτα για να εμποδίσει τον εγκληματία του κυβερνοχώρου να συνεχίσει να τη χρησιμοποιεί.
Στη συνέχεια, ενημέρωσε την εταιρεία "Bodegas Monje", καθώς ήταν το τελευταίο μέρος όπου το χρησιμοποίησε πραγματικά.

ΑΠΑΝΤΗΣΗ

ΠΟΙΟΣ: ένας πελάτης της ίδιας της εταιρείας που είχε πρόσβαση στο τοπικό δίκτυο για παράνομους σκοπούς.
ΣΕ ΠΟΙΟΝ: σε άλλον πελάτη, μέσω της εταιρείας.
ΓΙΑΤΙ: για κλοπή χρημάτων
ΤΙ: υπεξαίρεση τραπεζικών στοιχείων και πραγματοποίηση χρεώσεων, επωφελούμενος από τα χρήματα κάποιου άλλου
ΠΩΣ: διείσδυση μέσω του δικτύου Wifi των πελατών
ΣΤΡΑΤΗΓΙΚΗ: Επανασχεδιασμός του δικτύου ώστε να διαχωριστεί η σύνδεση των πελατών που επισκέπτονται την επιχείρηση από το σύστημα πληρωμών και το εσωτερικό δίκτυο της επιχείρησης.

ΑΝΑΚΑΜΨΗ

ΕΠΙΠΤΩΣΗ:

- ☑ Η πιστωτική κάρτα ενός πελάτη του καταστήματος που εκτίθεται σε κίνδυνο
- ☑ Η εμπιστοσύνη των πελατών στην ασφάλεια της εταιρείας θα μπορούσε να διακυβευθεί και δεν θα μπορούσαν να βασίζονται τόσο εύκολα στην πραγματοποίηση πληρωμών με αυτή τη μέθοδο.
- ☑ Εάν περισσότεροι πελάτες επηρεάζονταν από αυτή την κυβερνοεπίθεση, αυτό θα είχε άμεσο αντίκτυπο στη φήμη της εταιρείας.

ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ:

Η στρατηγική που εφάρμοσε ο ιδιοκτήτης της εταιρείας, από τη στιγμή που έλαβε γνώση του περιστατικού, ήταν να απενεργοποιήσει το Wi-Fi ή/και να αποσυνδέσει το δίκτυο επισκεπτών. Στη συνέχεια, επικοινώνησε με μια εταιρεία κυβερνοασφάλειας για την επίλυση του προβλήματος.

Η νέα στρατηγική ανάκαμψης που εφάρμοσε η ομάδα κυβερνοασφάλειας ήταν ο επανασχεδιασμός του δικτύου ώστε να διαχωριστεί το δίκτυο πελατών από το εσωτερικό δίκτυο της εταιρείας, όπου αποθηκεύονται τα πιο ευαίσθητα δεδομένα (δεδομένα των εργαζομένων και των πελατών, όπως τα δεδομένα του συστήματος πληρωμών).

Μετά τον επανασχεδιασμό του δικτύου δεν μπόρεσαν να ανακτηθούν τα χρήματα που είχαν κλαπεί. Ο πελάτης έπρεπε να αλλάξει την παλιά πιστωτική κάρτα που "έκλεψε" με μια άλλη νέα. Το πρόσωπο που πραγματοποίησε την κυβερνοεπίθεση δεν μπόρεσε να ταυτοποιηθεί. Δεν κατέστη δυνατή η ανάληψη νομικών ενεργειών.

Υπάρχει μια καλύτερη στρατηγική που πρέπει να ακολουθηθεί σε αυτή την περίπτωση. Αντί να αποσυνδεθεί το δίκτυο Wi-Fi της εταιρείας, θα μπορούσε επιπλέον:

- ☑ Να καταρτιστεί ένας κατάλογος όλων των πληροφοριών που έχουν τεθεί σε κίνδυνο, με όλα τα στοιχεία επικοινωνίας των πιθανών πελατών που θα μπορούσαν να επηρεαστούν (με βάση το χρονοδιάγραμμα - όσοι βρίσκονταν στην επιχείρηση την ίδια στιγμή με τον επηρεαζόμενο πελάτη).
- ☑ Να ενημερώνουν τους άλλους πελάτες για τυχόν περίεργες κινήσεις στους τραπεζικούς τους λογαριασμούς που πραγματοποιούνται με ηλεκτρονικές πληρωμές που γίνονται με την πιστωτική τους κάρτα.
- ☑ Να συλλέξουν όσο το δυνατόν περισσότερες πληροφορίες για να μπορέσει όχι μόνο να εντοπίσει τον ένοχο της κυβερνοεπίθεσης, αλλά και να προειδοποιήσει καλύτερα τους πελάτες που ενδέχεται επίσης να επηρεαστούν.
- ☑ Να αλλάξουν αμέσως τους κωδικούς πρόσβασης για να αποφύγετε μια ξαφνική διακοπή λειτουργίας της εταιρείας, επειδή εκείνη τη στιγμή το δίκτυο δεν ήταν χωρισμένο, λειτουργούσε για τους πελάτες και για τους υπαλλήλους ταυτόχρονα.

ΔΙΔΑΓΜΑΤΑ

Μεταξύ των διδαγμάτων που αντλήθηκαν, ξεχωρίζουν τα ακόλουθα:

- ☑ ότι είναι προτιμότερο το δίκτυο να είναι τμηματοποιημένο
- ☑ ότι πρέπει να εφαρμόζονται πολιτικές μηδενικής εμπιστοσύνης
- ☑ ότι δεν χρειάζεται να είσαι μεγάλη εταιρεία για να υποστείς κυβερνοεπίθεση

ότι είναι απαραίτητο να διαθέτουν σύγχρονο εξοπλισμό και ενεργά συστήματα κυβερνοασφάλειας (με επαγγελματικό τείχος προστασίας, IPS, antivirus κ.λπ.).

CASE STUDY 4: INFORMATION DISCLOSURE HANESBRANDS INC.

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Η Hanesbrands Inc. (HBI) είναι πολυεθνική εταιρεία ένδυσης που ιδρύθηκε το 1901 και εδρεύει στο Winston-Salem των ΗΠΑ. Διαθέτει πάνω από 250 καταστήματα σε 47 χώρες. Μεταξύ των πιο γνωστών εμπορικών σημάτων της εταιρείας είναι οι Hanes, Champion, Playtex, Bali, L'eggs, Just My Size, Barely There, Wonderbra, Duofold, Celebrity, Maidenform, Zorba κ.λπ. Ενα από τα ανταγωνιστικά πλεονεκτήματα της Hanesbrands είναι ότι το 70% των ενδυμάτων που πωλεί κατασκευάζεται στις δικές της εγκαταστάσεις καθώς και σε εγκαταστάσεις συνεργαζόμενων εργολάβων. Με αυτόν τον τρόπο, η εταιρεία καταφέρνει να ελέγχει το μεγαλύτερο μέρος της αλυσίδας εφοδιασμού, γεγονός που επιτρέπει επίσης την καθιέρωση ισχυρών πρακτικών βιωσιμότητας και συμβάλλει στην παγκόσμια επιτυχία της. Το 2021, η HBI ανακηρύχθηκε μία από τις πιο ηθικές εταιρείες του κόσμου από την Ethisphere και έγινε μέρος της λίστας Barron's 100 Most Sustainable Companies για τρία συνεχόμενα έτη. Για να διασφαλίσει ότι η εταιρεία ακολουθεί μια μακροπρόθεσμη πολιτική βιωσιμότητας, έχει θέσει παγκόσμιους στόχους βιωσιμότητας για το 2030 (σύμφωνα με τους Στόχους Βιώσιμης Ανάπτυξης των Ηνωμένων Εθνών υπό τρεις πυλώνες: Ανθρωπος, Πλανήτης και Προϊόν) και ξεκίνησε έναν ιστότοπο για τη βιωσιμότητα.

Το 2019 η εταιρεία είχε έσοδα 7,0 δισεκατομμυρίων δολαρίων και περίπου 61 000 υπαλλήλους. Αναφέρεται ότι η HBI δαπανά πάνω από 100 000 δολάρια για την ασφάλεια στον κυβερνοχώρο, χρησιμοποιώντας κυρίως προϊόντα της Akamai, όπως υπηρεσίες cloud.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Η μέθοδος που εφαρμόστηκε για τη συλλογή των πληροφοριών για την παρούσα μελέτη περίπτωσης ήταν η έρευνα γραφείου, ενώ οι συγκεκριμένες πηγές πληροφοριών μπορούν να βρεθούν στην ενότητα "Αναφορές" του παρόντος εγγράφου.

ΠΡΟΛΗΨΗ

☑ **Πρακτικές που είχαν μηδενικό αποτέλεσμα:** Προκειμένου να παρακολουθήσει την παραγγελία των ρούχων του, ο χρήστης έλαβε έναν σύνδεσμο για να συνδεθεί ως επισκέπτης στον ιστότοπο. Ο επισκέπτης χρήστης είχε εκτεταμένα δικαιώματα για να αποκτήσει πληροφορίες για τις παραγγελίες που έκαναν όλοι οι άλλοι χρήστες απλά και μόνο αλλάζοντας τη διεύθυνση URL του επισκέπτη. Ως εκ τούτου, η βάση δεδομένων παραβιάστηκε μέσω του ιστότοπου, καθώς δεν ζητούσε έλεγχο ταυτότητας και θεωρούσε τον επισκέπτη χρήστη ως έγκυρο χρήστη. Τα δεδομένα που ήταν ορατά για τους άλλους πελάτες αποτελούνταν από ονόματα, τελευταία ψηφία των πιστωτικών τους καρτών, διεύθυνση, αριθμό τηλεφώνου κ.λπ.

☑ **Πρακτικές που είχαν αποδεδειγμένα αποτελέσματα σε πραγματικές κυβερνοεπιθέσεις αυτού του τύπου:**

1. Ανακάλυψη της έκθεσης δεδομένων (με χρήση εξωτερικών συστημάτων σάρωσης).

2. Ισχυρός έλεγχος ταυτότητας (ενιαία σύνδεση που επιτρέπει σε έναν χρήστη να συνδεθεί σε διάφορα συστήματα ή διαφορετικά ονόματα χρήστη/κωδικούς πρόσβασης για κάθε σύστημα).

3. Ιεράρχηση της πρόσβασης στα δεδομένα (π.χ., το τμήμα ανθρώπινου δυναμικού μπορεί να χρειάζεται πρόσβαση μόνο σε πληροφορίες για τους εργαζομένους και το λογιστήριο μπορεί να χρειάζεται πρόσβαση μόνο σε δεδομένα προϋπολογισμού και φόρων. Οι φιλοξενούμενοι χρήστες θα πρέπει να έχουν κατ' αρχήν ελάχιστη πρόσβαση σε δεδομένα).

4. Ανάπτυξη υποδομών παρακολούθησης και αυτοματοποιημένων λύσεων που μπορούν να εντοπίζουν γρήγορα πιθανά προβλήματα προτού μετατραπούν σε καταστάσεις έκτακτης ανάγκης, να απομονώνουν τις μολυσμένες βάσεις δεδομένων και να ενημερώνουν τις ομάδες υποστήριξης και πληροφορικής για τα επόμενα βήματα.

"Σύμφωνα με μια νέα έκθεση της Blumira και της IBM, ο μέσος κύκλος ζωής μιας παραβίασης διαρκεί 287 ημέρες, με τους οργανισμούς να χρειάζονται 212 ημέρες για να εντοπίσουν αρχικά μια παραβίαση και 75 ημέρες για να την περιορίσουν." (VentureBeat, 2022)

ΑΝΑΓΝΩΡΙΣΗ

Η επίθεση κατά της Hanesbrands Inc. ήταν **τύπου αποκάλυψης πληροφοριών**.

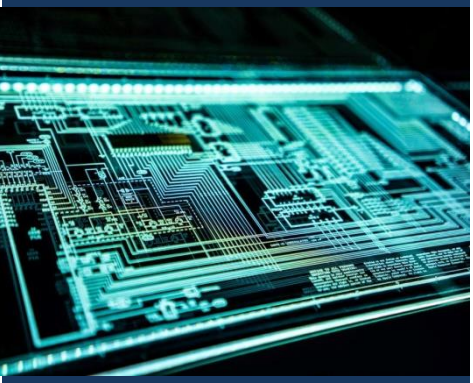
Την τελευταία εβδομάδα του Ιουνίου και την πρώτη του Ιουλίου 2015 η Hanesbrands Inc. έπεσε θύμα κυβερνοεπίθεσης. Μετά την κλοπή των δεδομένων η εταιρεία ενημερώθηκε από τους αντιπάλους για την παραβίαση χωρίς να δώσουν κίνητρο για την ενέργειά τους. Είναι πολύ πιθανό η αδυναμία της εταιρείας να ανακαλύφθηκε με σάρωση[1]. Οι χάκερ δημιούργησαν εντολή check-out "επισκέπτη" στον ιστότοπο της Hanesbrands[2] (χωρίς καν να εγγραφούν στον ιστότοπο). Με τον σύνδεσμο παραγγελίας που έλαβαν οι χάκερς κατάφεραν να αποστραγγίσουν τη βάση δεδομένων της εταιρείας που ήταν υπεύθυνη για την τήρηση των δεδομένων όλων των παραγγελιών των πελατών (παραγγελίες που έγιναν στον ιστότοπό τους ή μέσω τηλεφώνου) - όπως αποδείχθηκε, ο σύνδεσμος "guest" check-out ήταν σε θέση να έχει πρόσβαση σε κάθε άλλη παραγγελία χωρίς πιστοποίηση ταυτότητας. Σε διάστημα μιας εβδομάδας οι αντίπαλοι κατάφεραν να αποκτήσουν πληροφορίες για πάνω από 900 000 πελάτες. Για να μην εντοπιστούν οι χάκερς χρησιμοποίησαν πιθανότατα το Port Knocking[3] προκειμένου να κρύψουν τη δραστηριότητά τους. Σύμφωνα με την Hanesbrands, οι αντίπαλοι χρησιμοποίησαν Screenshots[4] για να αποσπάσουν τα δεδομένα, ωστόσο είναι πολύ πιθανό να χρησιμοποίησαν πιο αυτοματοποιημένο τρόπο - όπως σενάριο που θα αναλύει τα δεδομένα απευθείας[5].

Η επίθεση που περιγράφεται από το πλαίσιο ATT&CK της MITRE:

Με συγχρηματοδότηση από το
πρόγραμμα «Erasmus+»
της Ευρωπαϊκής Ένωσης

[1] Ενεργή σάρωση: T1592.002).
[2] Αρχική πρόσβαση: (T1190).
[3] Επιμονή: Σήμανση κυκλοφορίας: (T1205.001).
[4] Λήψη οθόνης (T1113).
[5] Αυτοματοποιημένη συλλογή (T1119).

Η επίθεση εντοπίστηκε από την εταιρεία μετά την ειδοποίησή της από τους αντιπάλους. Η Hanesbrands δεν γνώριζε ότι αυτό συνέβαινε μέχρι που τους ενημέρωσαν οι χάκερς.



ΑΠΑΝΤΗΣΗ

Τον Ιούνιο του 2015 η Hanesbrands Inc. ενημερώθηκε από τους αντιπάλους της για την παραβίαση. Μέσω του λογαριασμού επισκέπτη στον ιστότοπό τους, οι επιτιθέμενοι κατάφεραν να αποσπάσουν γενικές πληροφορίες χρήστη για 900.000 πελάτες. Αφού ενημερώθηκε για τη διαρροή, η Hanesbrands πρόσθεσε έλεγχο ταυτότητας στη βάση δεδομένων "παραγγελίες πελατών" και αφαίρεσε την επιλογή "check-out επισκεπτών" (παρόλο που το διόρθωσε).

ΠΟΙΟΣ: Άγνωστος.

ΣΕ ΠΟΙΟΝ: Hanesbrands Inc.

ΓΙΑΤΙ: Ήταν μια στοχευμένη επίθεση για την απόκτηση πληροφοριών σχετικά με τη βάση δεδομένων πελατών και τις λίστες πελατών, αλλά τελικά δεν ζητήθηκαν λύτρα από τους αντιπάλους. Απλώς ενημέρωσαν την Hanesbrands ότι απέκτησαν τα δεδομένα.

ΤΙ: Γενικές πληροφορίες πελατών για 900.000 πελάτες - ονόματα, διευθύνσεις, πληροφορίες για την κατάσταση της παραγγελίας του πελάτη, αριθμούς τηλεφώνου και τα 4 τελευταία ψηφία της πιστωτικής του κάρτας. Αλλά τα ονόματα χρήστη ή οι κωδικοί πρόσβασης των πελατών δεν αποκαλύφθηκαν. Οι χάκερ δεν έθεσαν σε κίνδυνο τα εταιρικά συστήματα της Hanesbrands.

ΠΩΣ: Οι αντίπαλοι δημιούργησαν μια παραγγελία μέσω check-out λογαριασμού επισκέπτη στην ιστοσελίδα της Hanesbrands. Παριστάνοντας τον "επισκέπτη" που ελέγχει μια παραγγελία (οι αντίπαλοι δεν ήταν εγγεγραμμένοι στον ιστότοπο) κατάφεραν να βρουν ρήγμα στη βάση δεδομένων της Hanesbrands εκμεταλλευόμενοι τον σύνδεσμο της παραγγελίας. Οι χάκερ κατάφεραν να αποκτήσουν πρόσβαση στα στοιχεία και την κατάσταση των παραγγελιών των πελατών και να εξάγουν τα

δεδομένα για περίπου μία εβδομάδα χρησιμοποιώντας την επιλογή "exploit with check-out" στον ιστότοπο.

ΣΤΡΑΤΗΓΙΚΗ: Μόλις η Hanesbrands ενημερώθηκε για την παραβίαση από τους αντιπάλους, πρόσθεσε έλεγχο ταυτότητας στη βάση δεδομένων της για να σταματήσει το κενό αποκάλυψης πληροφοριών. Επιπλέον, επιδιόρθωσαν το check-out "guest user" μέσω του οποίου διαχειρίζονταν τη διαρροή. Η Hanesbrands ενημέρωσε τους πελάτες της για την παραβίαση μέσω ηλεκτρονικού ταχυδρομείου και ταχυδρομείου. Από εκείνο το ατύχημα, η Hanesbrands επενδύει κάθε χρόνο όλο και περισσότερο στην ασφάλεια στον κυβερνοχώρο.

ΑΝΑΚΑΜΨΗ

☑ **ΕΠΙΠΤΩΣΕΙΣ: Οι** συνέπειες ήταν η διαρροή πληροφοριών για τους πελάτες. Δεν έχει γνωστοποιηθεί οποιαδήποτε αγωγή ή άλλη άμεση ζημιά.

☑ **ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ: Η** Hanesbrands ενημέρωσε τους πελάτες της σχετικά με την παραβίαση. Επισκευάστηκε ο σύνδεσμος "επισκέπτης χρήστης"[1] προκειμένου να μην έχει άμεση πρόσβαση στη βάση δεδομένων και συνολικά απενεργοποιήθηκε ως επιλογή[2]. Πρόσφερε εξυπηρέτηση πελατών για να απαντήσει εάν οι χρήστες έχουν ανησυχίες. Επιπλέον πραγματοποίησε έλεγχο ασφαλείας[3] και σάρωση ευπαθειών[4] στα υφιστάμενα συστήματά τους και επένδυσε σε εκπαιδεύσεις για την ασφάλεια στον κυβερνοχώρο[5].

Τα μέτρα μετριασμού που περιγράφονται από το πλαίσιο MITRE ATT&CK:

[1] Διαμόρφωση λογισμικού (M1054).
[2] Απενεργοποίηση ή κατάργηση λειτουργίας ή προγράμματος (M1042).
[3] Έλεγχος (M1047).
[4] Σάρωση ευπαθειών (M1016).
[5] Οδηγίες για τον προγραμματιστή εφαρμογών (M1013).

☑ **ΚΑΛΥΤΕΡΗ ΣΤΡΑΤΗΓΙΚΗ:** Μετά την επισκευή του συνδέσμου "επισκέπτης χρήστης" μέσω του οποίου ένας πελάτης μπορούσε να αναθεωρήσει την αγορά του, η Hanesbrands απενεργοποιεί αυτή την επιλογή. Αντ' αυτού θα μπορούσαν να είχαν προσθέσει μια παρακολούθηση για ύποπτη δραστηριότητα και/ή πολιτικές για την επανεξέταση μόνο συγκεκριμένου ποσού αγορών.

ΔΙΔΑΓΜΑΤΑ

Οι επιθέσεις αποκάλυψης πληροφοριών είναι σπάνιες, καθώς πολλά σύγχρονα εργαλεία παρέχουν αυτόματη ασφάλεια στον κυβερνοχώρο και συμβουλεύουν τις εταιρείες σχετικά με το τι θα μπορούσε να αποτελέσει πιθανή διαρροή. Η επίθεση στη Hanesbrands δείχνει ότι το αδύναμο μονοπάτι ελέγχου των βάσεων δεδομένων και η έλλειψη τεχνογνωσίας σε θέματα ασφάλειας μπορούν να αξιοποιηθούν μάλλον εύκολα. Σε πολλές περιπτώσεις οι βάσεις δεδομένων παραβιάζονται εξαιτίας του ανεπαρκούς επιπέδου εμπειρογνωμοσύνης στον τομέα της ασφάλειας

στον κυβερνοχώρο και της έλλειψης σχετικής κατάρτισης/εκπαίδευσης των μη τεχνικών υπαλλήλων, οι οποίοι ως εκ τούτου μπορεί να παραβιάζουν βασικούς κανόνες ασφαλείας των βάσεων δεδομένων. Το προσωπικό πληροφορικής μπορεί επίσης να μην διαθέτει την απαιτούμενη τεχνογνωσία για την επιβολή πολιτικών ασφαλείας, τη διεξαγωγή κατάλληλων διαδικασιών και δράσεων αναφοράς περιστατικών.

Ένα άλλο σημείο είναι ότι η βάση δεδομένων στο Hanesbrand ήταν ευάλωτη λόγω λανθασμένων ρυθμίσεων - οι βάσεις δεδομένων συνήθως γίνονται εντελώς απροστάτευτες εξαιτίας αυτού. Συχνά ξεχνιέται ότι συνήθως οι αντίπαλοι είναι άκρως επαγγελματίες ειδικοί της πληροφορικής, οι οποίοι σίγουρα γνωρίζουν πώς να εκμεταλλεύονται τέτοιες ευπάθειες. Αυτό μπορεί να αντιμετωπιστεί με την απενεργοποίηση των προεπιλεγμένων λογαριασμών της βάσης δεδομένων σε συνδυασμό με εκπαιδευμένο και έμπειρο προσωπικό πληροφορικής.

Η Hanesbrands είχε την τύχη να διαρρεύσουν μόνο γενικές πληροφορίες, καθώς και ότι οι αντίπαλοι ενημέρωσαν την εταιρεία αφού απέσπασαν όλα τα δεδομένα που μπορούσαν. Επιπλέον, η Hanesbrands ενημέρωσε αμέσως τους πελάτες της για την παραβίαση, γεγονός που δείχνει ότι η εταιρεία θέλει να είναι ειλικρινής με τους πελάτες της και ότι το θέμα λαμβάνεται σοβαρά υπόψη

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 5: SPOOFING HUMANA

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Η Humana είναι εταιρεία ασφάλισης υγείας με έδρα το Louisville του Kentucky. Αρχικά ιδρύθηκε το 1961 ως φορέας εκμετάλλευσης οίκων ευγηρίας, η κύρια δραστηριότητα της εταιρείας μετατράπηκε στην ιδιοκτησία και διαχείριση νοσοκομείων και στη συνέχεια σε προγράμματα ασφάλισης υγείας τη δεκαετία του 1980. Τον Μάιο του 2015, το Forbes εκτιμούσε ότι η αξία της εταιρείας ανερχόταν σε 26,7 δισεκατομμύρια δολάρια. Το 2020 η Humana είχε έσοδα ύψους 77,155 δισ. δολαρίων και περίπου 48 000 υπαλλήλους. Μηνιαίως, η Humana δαπανά πάνω από 100.000 δολάρια για την ασφάλεια στον κυβερνοχώρο. Η Humana χρησιμοποιεί προϊόντα ασφάλειας στον κυβερνοχώρο όπως η "Akamai" (πλατφόρμα παροχής cloud) και η "Prolexic (λύσεις ασφαλείας για την προστασία δικτυακών τόπων, κέντρων δεδομένων και εταιρικών εφαρμογών IP από επιθέσεις Distributed Denial of Service (DDoS))", η "Proofpoint" (λύση για την προστασία των ανθρώπων και των κρίσιμων

δεδομένων σας από προηγμένες απειλές ηλεκτρονικού ταχυδρομείου), τα προγράμματα "Alert Logic" (white-glove managed detection and response) και άλλα.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ;

Η μέθοδος που εφαρμόστηκε για τη συλλογή των πληροφοριών για την παρούσα μελέτη περίπτωσης ήταν η έρευνα γραφείου, ενώ οι συγκεκριμένες πηγές πληροφοριών μπορούν να βρεθούν στην ενότητα "Αναφορές" του παρόντος εγγράφου.

ΠΡΟΛΗΨΗ

☑ **Πρακτικές που είχαν μηδενικό αποτέλεσμα:** Η Humana εφάρμοσε αυτή την πρακτική πριν από το περιστατικό. Δεν ήταν αποτελεσματική, καθώς ο οργανισμός χρειάστηκε περίπου μία ημέρα για να λάβει μέτρα ως απάντηση στις πολυάριθμες αποτυχημένες προσπάθειες σύνδεσης που έλαβε.

☑ **Πρακτικές που είχαν αποδεδειγμένα αποτελέσματα σε πραγματικές επιθέσεις στον κυβερνοχώρο:**

1. Κλείδωμα λογαριασμού μετά από αποτυχημένη προσπάθεια σύνδεσης.
2. Αποκλεισμός της κυκλοφορίας στο διαδίκτυο από ξένες χώρες με τις οποίες ο οργανισμός δεν συνεργάζεται.
3. Αναγκαστική επαναφορά κωδικού πρόσβασης.

ΑΝΑΓΝΩΡΙΣΗ

Η επίθεση κατά της Humana ήταν **τύπου Spoofing.**

Στις 3 Ιουνίου 2018 η Humana έγινε στόχος μιας εξελιγμένης επίθεσης κυβερνο-απομίμησης που σημειώθηκε στο Humana.com. Την ίδια ημέρα η Humana αντιλήφθηκε σημαντική αύξηση των προσπαθειών σφάλματος σύνδεσης από διευθύνσεις IP ξένων χωρών[1]. Προκειμένου να μην αποκαλύψουν την πραγματική τους τοποθεσία, οι αντίπαλοι χρησιμοποίησαν Multi-Hop Proxies[2]. Ο όγκος των προσπαθειών σύνδεσης στο Humana.com υποδήλωνε ότι είχε εξαπολυθεί μια μεγάλη και ευρείας κλίμακας επίθεση. Η φύση της επίθεσης και οι παρατηρούμενες συμπεριφορές έδειξαν ότι οι επιτιθέμενοι είχαν μια μεγάλη βάση δεδομένων με ταυτότητες χρηστών και αντίστοιχους κωδικούς πρόσβασης που εισάγονταν με σκοπό να εντοπίσουν ποιοι από αυτούς θα μπορούσαν να είναι έγκυροι στο Humana.com με "ωμή βία"[3]. Ο υπερβολικός αριθμός σφαλμάτων σύνδεσης υποδηλώνει ότι οι πληροφορίες πιστοποίησης δεν προέρχονταν από την Humana[4] (και πιθανότατα αγοράστηκαν από τον "σκοτεινό" ιστό). Στις 4 Ιουνίου η Humana μπλόκαρε τις IPs. Με βάση αυτά τα γεγονότα, η επίθεση αυτή μπορεί να περιγραφεί ως επίθεση εξαπάτησης ταυτότητας. Οι αντίπαλοι συνέλεξαν δεδομένα[5] για περίπου 65 000 χρήστες που περιλαμβάνει :

- ☑ Ιατρικές, οδοντιατρικές και οπτικές απαιτήσεις, συμπεριλαμβανομένων των υπηρεσιών που εκτελέστηκαν, του ονόματος του παρόχου, των ημερομηνιών παροχής υπηρεσιών, της χρέωσης και των καταβληθέντων ποσών κ.λπ.

- ☑ Πληροφορίες λογαριασμού δαπανών, όπως πληροφορίες για τις δαπάνες και το υπόλοιπο του λογαριασμού αποταμίευσης υγείας.

Μετά το περιστατικό, η Humana είχε λάβει πρόσθετα μέτρα, όπως το κλείδωμα του λογαριασμού μετά από αποτυχημένη προσπάθεια σύνδεσης, το μπλοκάρισμα της διαδικτυακής κίνησης από ξένες χώρες με τις οποίες ο οργανισμός δεν συνεργάζεται και την αναγκαστική επαναφορά του κωδικού πρόσβασης.

Η επίθεση που περιγράφεται από το πλαίσιο MITRE ATT&CK:
[1] Διερμηνέας εντολών και σεναρίων: (T1059.008).
[2] Πληρεξούσιος αντιπρόσωπος: T1090.003).
[3] Ωμή βία: (T1110.004).
[4] Συγκέντρωση πληροφοριών για την ταυτότητα του θύματος: (T1589.001).
[5] Αυτοματοποιημένη συλλογή (T1119).

Η επίθεση εντοπίστηκε από ειδοποιήσεις για σφάλματα πολλαπλών προσπαθειών σύνδεσης.

ΑΠΑΝΤΗΣΗ

- ☑ **ΠΟΙΟΣ:** Άγνωστος
- ☑ **ΣΕ ΠΟΙΟΝ:** Humana
- ☑ **ΓΙΑΤΙ:** Κλοπή ταυτότητας (που πιθανώς θα πωληθεί σε τρίτους)
- ☑ **ΤΙ:** ευαίσθητες πληροφορίες για τους χρήστες (ιατρικές, οδοντιατρικές και οπτικές απαιτήσεις, συμπεριλαμβανομένων των υπηρεσιών που εκτελέστηκαν, του ονόματος του παρόχου, των ημερομηνιών παροχής υπηρεσιών, της χρέωσης και των καταβληθέντων ποσών κ.λπ.)
- ☑ **ΠΩΣ:** Οι αντίπαλοι συνέλεξαν μεγάλες ποσότητες λογαριασμών και διαπιστευτηρίων. Στη συνέχεια, χρησιμοποιώντας διακομιστές μεσολάβησης πολλαπλών βημάτων, ανάγκασαν με ωμό τρόπο να συνδεθούν με τους λογαριασμούς που είχαν. Μετά την επιτυχή είσοδο οι αντίπαλοι συνέλεξαν δεδομένα χρηστών μέσω μεταφοράς δεδομένων μικρού μεγέθους.
- ☑ **ΣΤΡΑΤΗΓΙΚΗ:** Μόλις η Humana παρατήρησε τη σημαντική αύξηση του αριθμού των σφαλμάτων στις απόπειρες σύνδεσης, οι υπεύθυνοι για την ασφάλεια στον κυβερνοχώρο μπλόκαραν τις ξένες διευθύνσεις IP από τις οποίες γίνονταν οι πολλαπλές προσπάθειες σύνδεσης. Μετά από αυτό η Humana επέβαλε την επαναφορά κωδικού πρόσβασης σε όλους τους λογαριασμούς που ήταν γνωστό ότι είχαν παραβιαστεί και μάλιστα κυκλοφόρησε ένα προϊόν - προσφέροντας στα μέλη προστασία από κλοπή ταυτότητας για ένα έτος.

ΑΝΑΚΑΜΨΗ

- ☑ **ΕΠΙΠΤΩΣΗ: Η** συνέπεια ήταν η διαρροή εμπιστευτικών πληροφοριών των χρηστών (ιατρικές, οδοντιατρικές και οπτικές απαιτήσεις, συμπεριλαμβανομένων των υπηρεσιών που πραγματοποιήθηκαν, του ονόματος του παρόχου, των ημερομηνιών παροχής υπηρεσιών, της χρέωσης και των καταβληθέντων ποσών κ.λπ.) Πολλές αγωγές αμέλειας κατατέθηκαν προς την Humana μετά από αυτό. Δεν υπάρχουν πληροφορίες για το αν οι αγωγές κερδήθηκαν από την εταιρεία, γεγονός που υποδηλώνει ότι τα αποτελέσματα ήταν μάλλον αρνητικά.

- ☑ **ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ: Η** Humana ειδοποίησε αριθμό μελών για να τους ενημερώσει σχετικά με την παραβίαση των δεδομένων μετά την παρέλευση ενός μήνα. Έλαβαν επίσης μια σειρά από μέτρα για να αυξήσουν την ασφάλεια στον κυβερνοχώρο, μεταξύ των οποίων: 1) επιβολή επαναφοράς κωδικού πρόσβασης[1]- 2) ανάπτυξη νέων ειδοποιήσεων για επιτυχείς και αποτυχημένες συνδέσεις[2] και 3) κλείδωμα λογαριασμών που συνδέονταν με ύποπτη δραστηριότητα[3]. Επιπλέον, ανέπτυξαν μια σειρά από τεχνικούς ελέγχους για την ενίσχυση της ασφάλειας της διαδικτυακής πύλης (αποκλεισμός επιθέσεων ωμής βίας, άμυνα κατά της έγχυσης SQL[4], εγκατάσταση πιστοποιητικού ασφαλείας SSL[5] κ.λπ.) Η εταιρεία μπλόκαρε επίσης όλες τις ξένες διευθύνσεις IP που δεν είχαν σχέση με τις δραστηριότητές της[6].

  Τα μέτρα μετριασμού που έλαβε η Humana περιγράφονται από το πλαίσιο MITRE ATT&CK:

  [1] Πολιτικές κωδικών πρόσβασης (M1027).
  [2] Πρόληψη εισβολών στο δίκτυο (M1031).
  [3] Πολιτικές χρήσης λογαριασμού (M1036).
  [4] Διαμόρφωση λογισμικού (M1054).
  [5] Επιθεώρηση SSL/TLS (M1020).

[6] Φίλτρο κίνησης δικτύου (M1037).

☑ **ΚΑΛΥΤΕΡΗ ΣΤΡΑΤΗΓΙΚΗ:**

Η Humana θα μπορούσε να είχε ενημερώσει τους χρήστες νωρίτερα. Θα μπορούσαν επίσης να είχαν προσθέσει πρόσθετα μέτρα ασφαλείας, όπως:

- Χρήση ελέγχου ταυτότητας με βάση την ανταλλαγή κλειδιών μεταξύ των μηχανημάτων στο δίκτυο ενός οργανισμού ή έλεγχο ταυτότητας πολλαπλών παραγόντων για απομακρυσμένη πρόσβαση,
- Χρήση μιας λίστας ελέγχου πρόσβασης για την άρνηση ιδιωτικών διευθύνσεων IP σε διασυνδέσεις downstream,
- Εφαρμογή φιλτραρίσματος τόσο της εισερχόμενης όσο και της εξερχόμενης κυκλοφορίας,
- Διαμόρφωση δρομολογητών και μεταγωγέων - αν είναι δυνατόν - ώστε να απορρίπτουν πακέτα που προέρχονται από το τοπικό δίκτυο ενός οργανισμού και ισχυρίζονται ότι προέρχονται από το εσωτερικό του,
- Ενεργοποίηση των συνόδων κρυπτογράφησης στο δρομολογητή ενός οργανισμού, έτσι ώστε οι αξιόπιστοι κεντρικοί υπολογιστές εκτός του δικτύου του να μπορούν να επικοινωνούν με ασφάλεια με τους τοπικούς κεντρικούς υπολογιστές του.

ΔΙΔΑΓΜΑΤΑ

Τα διδάγματα που αποκομίστηκαν θα μπορούσαν να προσδιοριστούν ως η ανάγκη να δοθεί μεγαλύτερη έμφαση στην ασφάλεια των προσωπικών δεδομένων των χρηστών, η διοργάνωση εκπαιδεύσεων του προσωπικού προκειμένου να αυξηθεί η ευαισθητοποίηση σχετικά με τις απειλές στον κυβερνοχώρο, η ενημέρωση των χρηστών για τη διαρροή δεδομένων λόγω των πολυάριθμων αγωγών αμέλειας κατά της Humana μετά το περιστατικό (η Humana δεν αποκάλυψε καμία πληροφορία ότι συνέβη τέτοια επίθεση παρά μόνο ένα μήνα αργότερα).

Οι επιπτώσεις της επίθεσης δεν σχετίζονταν μόνο με τα έξοδα για την αντιμετώπιση της επίθεσης και των αγωγών, αλλά και με τη μεγάλη ζημία στη φήμη της Humana και την αξιοπιστία της. Δεδομένου ότι η εταιρεία δραστηριοποιείται στον τομέα της ασφάλισης υγείας, είναι ζωτικής σημασίας για αυτήν να έχει τα υψηλότερα μέτρα ασφαλείας και την εμπιστοσύνη των πελατών της, καθώς τα δεδομένα που αποθηκεύονται στα συστήματά της είναι πολύ ευαίσθητα και εμπιστευτικά. Αυτός είναι ο λόγος για τον οποίο η Humana ήταν και παραμένει κορυφαίος στόχος για κυβερνοεπιθέσεις πολύ πριν από αυτή που προσδιορίζεται στην παρούσα υπόθεση αλλά και μετά. Λαμβάνοντας υπόψη τα παραπάνω, το λάθος στην εκτίμηση της σοβαρότητας της επίθεσης αυτής θα μπορούσε να θεωρηθεί εκπληκτικό.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 6: ΑΡΝΗΣΗ ΥΠΗΡΕΣΙΩΝ WILLIAM HILL

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Η William Hill είναι μια εταιρεία διαδικτυακών τυχερών παιχνιδιών με έδρα το Λονδίνο της Αγγλίας, η οποία ιδρύθηκε αρχικά το 1934 από τον William Hill. Η εταιρεία άλλαξε χέρια πολλές φορές - αγοράστηκε για πρώτη φορά το 1971 από τη Sears Holdings. Αφού πουλήθηκε πολλές φορές, τον Απρίλιο του 2021 εξαγοράστηκε από την Ceasars Entertainment. Το 2020 η εταιρεία είχε έσοδα 1.324,3 εκατ. στερλίνες και 12000 υπαλλήλους (8000 στο Ηνωμένο Βασίλειο). Το 2021 η εταιρεία είχε περισσότερα από 1400 καταστήματα στοιχημάτων, αλλά το 2019 άρχισε να κλείνει περισσότερα από 800 καταστήματα λόγω χαμηλών κερδών, αλλά ισχυριζόμενη ότι θα διατηρήσει το προσωπικό της ανέπαφο.

Μηνιαίως, η William Hill δαπανά πάνω από 100.000 δολάρια για την ασφάλεια στον κυβερνοχώρο. Η εταιρεία χρησιμοποιεί προϊόντα κυβερνοασφάλειας όπως "Prolexic" (λύσεις ασφαλείας για την προστασία ιστοσελίδων, κέντρων δεδομένων και εταιρικών εφαρμογών IP από επιθέσεις Distributed Denial of Service (DDoS))", "Proofpoint" (λύση για την προστασία των ανθρώπων και των κρίσιμων δεδομένων σας από προηγμένες απειλές ηλεκτρονικού ταχυδρομείου), "F5 BIG-IP Application Security Manager" (ευέλικτο τείχος προστασίας εφαρμογών ιστού που διασφαλίζει εφαρμογές ιστού σε παραδοσιακά, εικονικά και ιδιωτικά περιβάλλοντα cloud) , "Check Point" (προστατεύει τους πελάτες της από κυβερνοεπιθέσεις 5ης γενιάς με κορυφαίο στον κλάδο ποσοστού αλίευσης κακόβουλου λογισμικού, ransomware και προηγμένων στοχευμένων απειλών), κ.λπ.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Η μέθοδος που εφαρμόστηκε για τη συλλογή των πληροφοριών για την παρούσα μελέτη περίπτωσης ήταν η έρευνα γραφείου, ενώ οι συγκεκριμένες πηγές πληροφοριών μπορούν να βρεθούν στην ενότητα "Αναφορές" του παρόντος εγγράφου.

ΠΡΟΛΗΨΗ

☑ **Πρακτικές που είχαν μηδενικό αποτέλεσμα:**

1. Διάχυση δικτύου Anycast - η William Hill διαθέτει τέτοιου είδους άμυνα - η οποία είναι χρήσιμη για να συγκρατήσει τεράστιες ποσότητες πελατών που επισκέπτονται τον ιστότοπό της ή μπορεί να διαλύσει τεράστιες ποσότητες ανεπιθύμητης δικτυακής κίνησης (όπως η επίθεση DDoS). Αυτή η στρατηγική συνήθως λειτουργεί για τις περισσότερες περιπτώσεις επιθέσεων DDoS.

2. Η απλή αύξηση του εύρους ζώνης του δικτύου (πόση κίνηση μπορεί να συγκρατήσει) δεν αποδείχθηκε αποτελεσματική σε αυτή την επίθεση.

☑ **Πρακτικές που είχαν αποδεδειγμένα αποτελέσματα σε πραγματικές κυβερνοεπιθέσεις αυτού του τύπου:**

1. Εφαρμογή προστασίας DDoS σε επίπεδο διακομιστή - πρόσθετοι κανόνες που βοηθούν στον εντοπισμό και τον αποκλεισμό κακόβουλης κυκλοφορίας δικτύου.

2. Προσθήκη 3rd διάχυσης δικτύου Anycast - αυτό μπορεί να βοηθήσει τις εταιρείες να αυξήσουν σημαντικά την ικανότητά τους να αναλαμβάνουν πολύ μεγαλύτερη κυκλοφορία δικτύου ή να χειρίζονται επιθέσεις DDoS cks.

3. **ΑΝΑΓΝΩΡΙΣΗ**

"Σύμφωνα με την Cloudflare, το τέταρτο τρίμηνο του 2021 ο κλάδος της μεταποίησης δέχθηκε τις περισσότερες επιθέσεις DDoS σε επίπεδο εφαρμογών, καταγράφοντας αύξηση 641% από τρίμηνο σε τρίμηνο στον αριθμό των επιθέσεων." (Cook, 2022)

ΑΝΑΓΝΩΡΙΣΗ

Η επίθεση κατά της William Hill ήταν **τύπου άρνησης παροχής υπηρεσιών**.

Την 1η Νοεμβρίου 2016 η William Hill έγινε στόχος μιας κατανεμημένης επίθεσης άρνησης παροχής υπηρεσιών υψηλής απόδοσης[1]. Πριν από την επίθεση, οι αντίπαλοι συγκέντρωσαν πληροφορίες σχετικά με τα στοιχεία του δικτύου του ιστότοπου της William Hill[2]. Στη συνέχεια, οι αντίπαλοι κατέκλυσαν τον ιστότοπο της William Hill με κίνηση, ώστε να μην μπορεί να λειτουργήσει σωστά. Η επίθεση δεν επέτρεψε στους πελάτες να τοποθετήσουν στοιχήματα στους αγώνες του UEFA Champions League το βράδυ της Τρίτης. Η επίθεση στην William Hill επιτεύχθηκε με τη βοήθεια ενός κακόβουλου λογισμικού που ονομάζεται "Mirai"[4], το οποίο δημιουργεί ένα δίκτυο πολυάριθμων συστημάτων υπολογιστών που είναι γνωστό ως "botnet"[3] για να ξεκινήσει η επίθεση DDoS μέσω αυτών.

Η επίθεση που περιγράφεται από το πλαίσιο MITRE ATT&CK:
[1] Άρνηση εξυπηρέτησης δικτύου: (T1498.001).
[2] Συγκέντρωση πληροφοριών για το δίκτυο του θύματος: (T1590.005).
[3] Απόκτηση υποδομών: (T1583.005).
[4] Αυτό-διαδούμενος ιός σκουλήκι που χρησιμοποιεί βάση δεδομένων με προεπιλεγμένα διαπιστευτήρια. Με αυτά τα διαπιστευτήρια σαρώνονται και μολύνονται συσκευές IoT (έξυπνες συσκευές όπως fitness trackers, φωνητικοί βοηθοί, αξεσουάρ smarthome κ.ά.).

Η επίθεση εντοπίστηκε αμέσως μετά την απενεργοποίηση του ιστότοπου της William Hill και τη διακοπή της πρόσβασης σε αυτόν.

ΑΠΑΝΤΗΣΗ

ΠΟΙΟΣ: Άγνωστος.
ΣΕ ΠΟΙΟΝ: William Hill.
ΓΙΑΤΙ: Επιχειρηματικές βεντέτες - είναι πολύ πιθανό ο αντίπαλος της εταιρείας να προβεί σε τέτοιες ενέργειες, ειδικά κατά τη διάρκεια δημοφιλών αθλητικών εκδηλώσεων όπως το UEFA Champions League / Εκβιασμός - αν η William Hill δεν καταφέρει να χειριστεί την κατάσταση, είναι πιθανό να ζητηθούν λύτρα.

ΤΙ: Η ιστοσελίδα της William Hill έπεσε για 24ωρη διακοπή λειτουργίας, η οποία προκάλεσε απώλειες ύψους 4,4 εκατομμυρίων λιρών. Χρειάστηκαν ημέρες για να αποκαταστήσει πλήρως την ιστοσελίδα και τα συστήματά της η William Hill.
ΠΩΣ: Στον ιστότοπο της William Hill διεξήχθη επίθεση κατανεμημένης άρνησης παροχής υπηρεσιών υψηλής απόδοσης με δίκτυο "botnet" (πολλαπλοί υπολογιστές που μολύνθηκαν από ιό κακόβουλου λογισμικού και χρησιμοποιήθηκαν για τη διεξαγωγή της επίθεσης αυτής χωρίς τη γνώση ή τη συγκατάθεσή τους) που δημιουργήθηκε από ένα κακόβουλο λογισμικό που ονομάζεται "Mirai".
ΣΤΡΑΤΗΓΙΚΗ: Αφού παρατήρησαν ότι ο ιστότοπός τους είναι εκτός λειτουργίας, οι ειδικοί πληροφορικής της William Hill άρχισαν να φιλτράρουν την εισερχόμενη κυκλοφορία. Η William Hill χρησιμοποίησε τη διάχυση δικτύου Anycast - αποστολή δικτυακής κίνησης διασκορπίζοντας την στο δίκτυο των διακομιστών της εταιρείας. Αυτός ο μετριασμός διανέμει την κίνηση δικτύου μέχρι το σημείο όπου η κίνηση απορροφάται από το δίκτυο της εταιρείας. Η χρησιμότητα αυτής της στρατηγικής εξαρτάται από το πόσο μεγάλο είναι το δίκτυο της εταιρείας και πόσο μεγάλη είναι η επίθεση DDoS. Στην περίπτωση της William Hill - ακόμη και με την κορυφαία υποδομή και την ασφάλειά της δεν ήταν αρκετά για να αντιμετωπίσει το μια τέτοια επίθεση.

ΑΝΑΚΑΜΨΗ

ΕΠΙΠΤΩΣΗ: Η επίθεση DDoS κατά της William Hill προκάλεσε την απενεργοποίηση του ιστότοπού της για περισσότερες από 24 ώρες, κατά τις οποίες οι πελάτες δεν μπορούσαν να στοιχηματίσουν στους αγώνες του Champions League της UEFA. Αυτό είχε ως αποτέλεσμα απώλειες άνω των 4,4 εκατομμυρίων λιρών σε μία μόνο ημέρα. Ευτυχώς για την William Hill στοχοποιήθηκε μόνο ο ιστότοπός της, γεγονός που διατήρησε άθικτα τα ευαίσθητα δεδομένα των χρηστών της (γεγονός που αποτελεί ένδειξη ότι οι αντίπαλοι ήθελαν να εμποδίσουν τους χρήστες να επισκεφθούν τον ιστότοπο και όχι να κλέψουν δεδομένα). Χρειάστηκαν πάνω από 4 ημέρες

εργασίας όλο το εικοσιτετράωρο για τους ειδικούς πληροφορικής της William Hill για να αναβιώσουν την ιστοσελίδα και τα επηρεαζόμενα συστήματα.

ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ: Για την αντιμετώπιση της επίθεσης, η William Hill φιλτράρισε την εισερχόμενη κυκλοφορία του δικτύου[1]. Φιλτράρισμα της κυκλοφορίας του δικτύου - μπλοκάρισμα της κυκλοφορίας που αφορά μόνο την επίθεση και αποδοχή της νόμιμης. Επίσης, άρχισε να χρησιμοποιεί 3rd party Anycast network diffusion vendors (εταιρείες που προσφέρουν τέτοιου είδους υπηρεσίες - οι οποίες διαλύουν την επίθεση DDoS όταν διασκορπίζουν όλη την εισερχόμενη κίνηση μέσω του δικτύου τους).

ΚΑΛΥΤΕΡΗ ΣΤΡΑΤΗΓΙΚΗ:

☑ Έλεγχος της υγείας του κεντρικού υπολογιστή, ο οποίος θα ειδοποιεί τους ειδικούς πληροφορικής της εταιρείας όταν εντοπίζεται μη φυσιολογική χρήση του δικτύου [2]. Εάν εντοπιστεί εγκαίρως, μπορούν να ληφθούν μέτρα που θα βοηθήσουν στη διατήρηση της διαθεσιμότητας της υπηρεσίας του ιστότοπου.

☑ Μπορεί να χρησιμοποιηθεί η "δρομολόγηση μαύρης τρύπας". Πρόκειται για μια τεχνική η οποία διοχετεύει τόσο τη νόμιμη όσο και την κακόβουλη κυκλοφορία σε μια μηδενική διαδρομή και εγκαταλείπεται από το δίκτυο. Δεν αποτελεί ιδανική λύση, καθώς καθιστά τον ιστότοπο μη προσβάσιμο.

☑ Περιορισμός ποσοστού. Περιορίζει τον αριθμό των αιτημάτων που μπορεί να λάβει ο διακομιστής - από μόνο του δεν μπορεί να σταματήσει την επίθεση DDoS, αλλά είναι ένα χρήσιμο εργαλείο στη συνολική στρατηγική άμυνας.

Η στρατηγική ανάκαμψης που περιγράφεται από το πλαίσιο ATT&CK της MITRE:

a. [1] Φίλτρο κίνησης δικτύου (M1037).
b. [2] Υγεία αισθητήρων: (DS0013).

ΔΙΔΑΓΜΑΤΑ

Η επίθεση εναντίον της William Hill μπορεί να μας δείξει ότι ακόμη και μια εταιρεία με εξαιρετική ασφάλεια στον κυβερνοχώρο και προετοιμασμένη να αντιμετωπίσει τέτοιες επιθέσεις μπορεί να υποφέρει από αυτές.

Παρόλο που ο ιστότοπός της κατέρρευσε από την επίθεση DDoS (συνήθως τέτοιες επιθέσεις είναι απλώς ένα προπέτασμα καπνού για την

πραγματική επίθεση), η κορυφαία ασφάλεια της εταιρείας ήταν άθικτη και λειτουργική, διατηρώντας τις ευαίσθητες πληροφορίες των πελατών της ασφαλείς. Αυτό έδειξε στους πελάτες τους ότι είναι ασφαλείς και διατήρησε την αξιοπιστία της εταιρείας. Με δεδομένο ότι οι αντίπαλοι δεν επιχείρησαν περαιτέρω να εκμεταλλευτούν την ευπάθεια της William Hill, επισημαίνει ότι πιθανότατα η επίθεση έγινε λόγω επιχειρηματικής αντιπαλότητας (ανταγωνιστική εταιρεία που θέλει να εκμεταλλευτεί την αγορά στοιχημάτων) ή προσπάθεια εκβιασμού (η εταιρεία βασίζεται στον ιστότοπό της και η μη λειτουργία του από τους αντιπάλους δημιουργεί απώλειες).

Με την είσοδο στην εποχή των έξυπνων συσκευών (IoT), όπου τα πάντα μπορούν να λειτουργούν εξ αποστάσεως (έξυπνα φώτα στο σπίτι, ηλεκτρικές σκούπες, ψυγεία, έξυπνα ρολόγια κ.λπ.), πρέπει επίσης να σκεφτούμε την ασφάλεια που πρέπει να εφαρμοστεί. Ολες αυτές οι έξυπνες συσκευές έχουν διεύθυνση IP και μπορούν να παραβιαστούν μέσω του δικτύου - για την απόκτηση πληροφοριών ή να "ζομπιστούν" (η συσκευή σας ελέγχεται χωρίς να το γνωρίζετε και αρχίζει να λειτουργεί με περίεργο τρόπο) και να χρησιμοποιηθούν σε επιθέσεις DDoS για να κατακλύσουν έναν ιστότοπο.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 7: COBALT STRIKE: Η ΧΡΗΣΗ ΕΡΓΑΛΕΙΩΝ RED TEAMING ΑΠΟ ΕΓΚΛΗΜΑΤΙΕΣ ΤΟΥ ΚΥΒΕΡΝΟΧΩΡΟΥ

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Το Cobalt Strike είναι ένα εργαλείο κόκκινης ομάδας που αναπτύχθηκε το 2012. Κύριος σκοπός του είναι να βοηθήσει τις κόκκινες ομάδες να δοκιμάσουν και να προσομοιώσουν επιθέσεις στον κυβερνοχώρο. Καθώς το εργαλείο έχει καλές δυνατότητες παράκαμψης των ορίων ασφαλείας μέσω παρακάμψεων, οι επιτιθέμενοι έχουν καταλάβει ορισμένες εκδόσεις του για να το καταχραστούν ως εργαλείο παράδοσης κακόβουλων ωφέλιμων φορτίων, όπως ransomware. Αυτή η μελέτη περίπτωσης δεν επικεντρώνεται σε έναν μεμονωμένο οργανισμό, καθώς το Cobalt Strike χρησιμοποιείται στην άγρια φύση για την εκτέλεση μαζικών επιθέσεων με στόχο διάφορους τύπους οργανισμών, όπως βιομηχανίες, χρηματοπιστωτικά ιδρύματα, εταιρείες τηλεπικοινωνιών κ.λπ.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Η μέθοδος που εφαρμόστηκε για τη συλλογή των πληροφοριών για την παρούσα μελέτη περίπτωσης ήταν η έρευνα γραφείου, ενώ οι συγκεκριμένες πηγές πληροφοριών μπορούν να βρεθούν στην ενότητα "Αναφορές" του παρόντος εγγράφου.

ΠΡΟΛΗΨΗ

Η ανίχνευση και η πρόληψη μιας επίθεσης που χρησιμοποιεί το εργαλείο κόκκινης ομάδας Cobalt Strike περιλαμβάνει μια αλυσίδα ασφαλείας σε ολόκληρη την υποδομή. Αυτή ξεκινάει ήδη με το λογισμικό προστασίας και παρακολούθησης στον πελάτη-τελικό σημείο και φτάνει μέχρι το επίπεδο

του δικτύου. Επιπλέον, η ενεργή πληροφόρηση σχετικά με τις απειλές είναι επίσης απαραίτητη για την ενημέρωση των εργαλείων ανίχνευσης που βασίζονται στην υπογραφή .

Αυτό συνήθως περιλαμβάνει:

- ☑ Ασφάλεια τελικών σημείων (όπως antivirus, παρακολούθηση με βάση τον κεντρικό υπολογιστή)
- ☑ Ασφάλεια δικτύου (όπως τείχος προστασίας, διακομιστής μεσολάβησης, ανίχνευση υπογραφών/προτύπων στην κυκλοφορία)
- ☑ Ασφάλεια ηλεκτρονικού ταχυδρομείου
- ☑ Σωστά ρυθμισμένες πολιτικές υποδοχής/ασφάλειας

ΑΝΑΓΝΩΡΙΣΗ

Το Cobalt Strike είναι ένα εμπορικό εργαλείο πολλαπλών λειτουργιών που ικανοποιεί διάφορες τεχνικές επιθέσεων. Λαμβάνοντας υπόψη το ίδιο το εργαλείο και τις δυνατότητές του, μπορεί να κατηγοριοποιηθεί ως αποκάλυψη πληροφοριών και αύξηση προνομίων. Ωστόσο, καθώς μπορεί επίσης να χρησιμοποιηθεί για την περαιτέρω ρίψη κακόβουλων ωφέλιμων φορτίων, ειδικά καθώς παρατηρήθηκαν επιθέσεις ransomware σε συνδυασμό με το Cobalt Strike, ο κατάλογος μπορεί να επεκταθεί με τις κατηγορίες Tampering και Denial of service.

Λαμβάνοντας υπόψη όλα τα χαρακτηριστικά του εργαλείου, πρόκειται για ένα εργαλείο απομακρυσμένης πρόσβασης με δυνατότητες πλευρικής μετακίνησης. Αυτό οδηγεί σε έναν τεράστιο κατάλογο τεχνικών επιθέσεων που χρησιμοποιεί το Cobalt Strike, και επομένως θα καλύψουμε μόνο μερικές από αυτές εδώ.

- ☑ Κατάχρηση Μηχανισμού Ελέγχου Ανύψωσης (T1548) Μόλις το Cobalt Strike εκτελεστεί σε ένα σύστημα, έχει τις δυνατότητες να εκτελέσει διάφορες τεχνικές που χρησιμοποιούνται για την απόκτηση υψηλότερων δικαιωμάτων.
- ☑ BITS Jobs (T1197) Το BITS είναι ένα εργαλείο των Windows που μπορεί να χρησιμοποιηθεί από το Cobalt Strike για τη λήψη ωφέλιμων φορτίων
- ☑ Διερμηνευτής εντολών και σεναρίων (T1059) Το Cobalt Strike μπορεί να χρησιμοποιήσει διάφορα εργαλεία για την εκτέλεση εντολών, κώδικα και σεναρίων. Αυτό περιλαμβάνει το

PowerShell, το Windows Command Shell, τη Visual Basic, την Python και τη JavaScript.

☑ Εκμετάλλευση για αύξηση προνομίων (T1068)
Για να αποκτήσει υψηλότερα προνόμια, το Cobalt Strike μπορεί να εκμεταλλευτεί ευπάθειες στο λειτουργικό σύστημα.

☑ Σύλληψη εισόδου (T1056)/Σύλληψη οθόνης (T1113)
Το Cobalt Strike μπορεί επίσης να λειτουργήσει ως keylogger και να συλλέξει στιγμιότυπα οθόνης από το μολυσμένο σύστημα.

ΑΠΑΝΤΗΣΗ

☑ **ΠΟΙΟΣ:** Άγνωστος

☑ **ΣΕ ΠΟΙΟΝ:** Πολλαπλές οργανώσεις σε όλο τον κόσμο

☑ **ΓΙΑΤΙ: Το** Cobalt Strike χρησιμοποιήθηκε σε πολλαπλές εκστρατείες που επικεντρώθηκαν σε διαφορετικούς στόχους. Ο λόγος της επίθεσης είναι η πρόσβαση στο εσωτερικό δίκτυο του οργανισμού για πλευρική μετακίνηση. Ενας άλλος λόγος μπορεί να είναι η πρόκληση ζημιάς σε εταιρείες με επίθεση στο παραβιασμένο δίκτυο με π.χ. ένα ransomware.

☑ **ΤΙ:** Κυρίως για απομακρυσμένη πρόσβαση, παραβίαση δικτύου και πλευρική μετακίνηση.

☑ **ΠΩΣ:** Το Cobalt Strike είναι ένα εμπορικό εργαλείο κόκκινης ομάδας που χρησιμοποιείται για την προσομοίωση επιθέσεων στον κυβερνοχώρο οι οποίες έχουν υποκλαπεί. Το εργαλείο χρησιμοποιείται για την απόκτηση της αρχικής πρόσβασης σε ένα εταιρικό δίκτυο, καθώς και για περαιτέρω ενέργειες με το παραβιασμένο δίκτυο.

☑ **ΣΤΡΑΤΗΓΙΚΗ:** Ανάλογα με την εταιρεία που δέχθηκε την επίθεση, οι πληροφορίες σχετικά με τον τρόπο με τον οποίο αναγνώρισε και αντέδρασε στην επίθεση είναι άγνωστες.

ΑΝΑΚΑΜΨΗ

☑ **ΕΠΙΠΤΩΣΗ:** Ο επιτιθέμενος μπορεί να αποκτήσει πλήρη πρόσβαση στο δίκτυο της εταιρείας. Αυτό μπορεί να οδηγήσει σε αποκάλυψη πληροφοριών, καθώς και σε περαιτέρω επιθέσεις που πραγματοποιούνται ανάλογα με τον φορέα της επίθεσης.

☑ **ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΥΚΛΩΣΗΣ:** Ανάλογα με την εταιρεία που δέχθηκε την επίθεση, οι πληροφορίες για το πώς μοιάζει η στρατηγική ανάκαμψης είναι άγνωστες.

☑ **ΚΑΛΥΤΕΡΗ ΣΤΡΑΤΗΓΙΚΗ:**

- Διατηρείτε τα συστήματα προστασίας από ιούς ενημερωμένα
- Χρήση συστημάτων ανίχνευσης και πρόληψης εισβολών
- Σωστή παρακολούθηση των συστημάτων για ύποπτες δραστηριότητες
- Σωστή διαμόρφωση των συστημάτων και απενεργοποίηση των μη απαιτούμενων υπηρεσιών
- Εκπαίδευση ευαισθητοποίησης των εργαζομένων

- Χρησιμοποιήστε τμηματοποίηση σε επίπεδο δικτύου και περιορίστε την επιτρεπόμενη επικοινωνία στο απαιτούμενο ελάχιστο.

ΔΙΔΑΓΜΑΤΑ

Παρόλο που είναι απαραίτητη η δημιουργία εργαλείων "κόκκινης ομάδας" που μπορούν να χρησιμοποιηθούν για προσομοίωση επιθέσεων σε ένα δίκτυο για την εύρεση πιθανών ευάλωτων σημείων, πρέπει να έχουμε κατά νου ότι ένα τέτοιο εργαλείο μπορεί επίσης να παραβιαστεί και να χρησιμοποιηθεί από έναν επιτιθέμενο.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 8: ΕΠΙΘΕΣΗ ZERO-DAY - HACKER GROUP HAFNIUM TARGETING EXCHANGE SERVERS

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Στις αρχές του 2021 ερευνητές βρήκαν πολλαπλές κρίσιμες ευπάθειες στον Microsoft Exchange Server, οι οποίες οδήγησαν σε μαζική εκμετάλλευση σε όλο τον κόσμο. Οι ευπάθειες χρησιμοποιήθηκαν στην άγρια φύση από πολλαπλές εγκληματικές οργανώσεις, κυρίως από την ομάδα HAFNIUM, προτού παρασχεθούν διορθωτικά στοιχεία από τη Microsoft. Αυτό έκανε τις επιθέσεις ιδιαίτερα δύσκολες στην αντιμετώπιση και την ανάκαμψη από αυτές.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Η μέθοδος που εφαρμόστηκε για τη συλλογή των πληροφοριών για την παρούσα μελέτη περίπτωσης ήταν η έρευνα γραφείου, ενώ οι συγκεκριμένες πηγές πληροφοριών μπορούν να βρεθούν στην ενότητα "Αναφορές" του παρόντος εγγράφου

ΠΡΟΛΗΨΗ

Δεκάδες χιλιάδες εταιρείες επηρεάστηκαν από αυτή την επίθεση. Λόγω της γενικής έκθεσης των Microsoft Exchange Servers στο διαδίκτυο και της δυνατότητας παράκαμψης της αυθεντικοποίησης της επίθεσης, ήταν πολύ δύσκολο να αποτραπεί εξαρχής. Αυτό οδηγεί περαιτέρω στην υπόθεση ότι οι διαφορετικές πρακτικές ασφαλείας που ισχύουν για αυτές τις εταιρείες είχαν μηδενικό αντίκτυπο.

ΑΝΑΓΝΩΡΙΣΗ

Υπάρχουν τέσσερις διαφορετικές ευπάθειες που οδήγησαν στις περιγραφόμενες επιθέσεις. Οι ευπάθειες είναι οι **CVE-2021-26855, γνωστή ως "ProxyLogon", CVE-2021-27065, CVE-2021-26857 και CVE-2021-26858**. Η τεχνική για την εκμετάλλευση αυτών των ευπαθειών περιγράφεται ως **"Exploitation for Client Execution" (T1203)** στο MITRE ATT&CK framework.

Το CVE-2021-26855 είναι μια παράκαμψη ελέγχου ταυτότητας με χρήση του εσωτερικού διακομιστή μεσολάβησης από τον Exchange Server. Με αυτό ένας εισβολέας μπορεί να αποκτήσει προνομιακή πρόσβαση στον ίδιο τον διακομιστή. Συνδυάζοντάς το με μια άλλη ευπάθεια όπως το CVE-2021-27065, που επιτρέπει την εγγραφή αυθαίρετων αρχείων στο σύστημα, ή το CVE-2021-26857, για την απόκτηση πρόσβασης στο SYSTEM (T1078) μέσω μιας μη ασφαλούς από-διαταγής, δημιουργείται μια αλυσίδα εκμετάλλευσης χωρίς περιορισμούς.

Οι επιθέσεις έλαβαν χώρα στην άγρια φύση πριν η Microsoft προλάβει να κυκλοφορήσει ένα patch για τις ευπάθειες. Σύμφωνα με πολυάριθμες πηγές, το χρονικό αυτό διάστημα ήταν περίπου 58 ημέρες εκμετάλλευσης μηδενικής ημέρας. Η πρώτη ομάδα που συνδέθηκε με αυτές τις ευπάθειες ήταν η HAFNIUM. Αργότερα πολλές άλλες ομάδες άρχισαν να κάνουν κατάχρηση αυτών των ευπαθειών. Οι δυνατότητες της επίθεσης επέτρεπαν πολλαπλά σενάρια, που έφταναν από την εκροή δεδομένων (T1567) έως την ανάπτυξη ransomware (T1486).

Ακολουθεί ένας κατάλογος ενεργειών που έγιναν από την ομάδα HAFNIUM με τη χρήση αυτού του φορέα επίθεσης:

- ☑ T1589 - Συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου για χρήστες στους οποίους σκόπευαν να απευθυνθούν
- ☑ T1071 - πλαίσιο ανοικτού κώδικα C2 (π.χ. covenant)
- ☑ T1560 - 7-Zip, WinRAR για τη συμπίεση κλεμμένων αρχείων για εξαγωγή
- ☑ T1059 - Εξαγωγή δεδομένων γραμματοκιβωτίου μέσω PowerShell
- ☑ T1567 - Απορρόφηση δεδομένων μέσω ιστότοπων κοινής χρήσης, συμπεριλαμβανομένου του MEGA
- ☑ T1105 - Λήψη κακόβουλου λογισμικού και εργαλείων σε παραβιασμένους κεντρικούς υπολογιστές (π.χ. Nishang, PowerCat)
- ☑ T1003 - Εκφόρτωση διαπιστευτηρίων των βάσεων δεδομένων LSASS και Active Directory (NTDS.DIT)
- ☑ T1505 - Ανάπτυξη WebShells σε εκτεθειμένους υπολογιστές (SIMPLESEESHARP, SPORTSBALL, κ.λπ.)
- ☑ T1589 – Collecting E-Mail addresses for users they intended to target
- ☑ Identification of the attacks may take place due to log inspection on possible compromised machines. Microsoft released guidance on

detecting every vulnerability according to their Indicator of Compromise.

ΑΠΑΝΤΗΣΗ

ΠΟΙΟΣ: HAFNIUM (πιθανώς κρατικά χρηματοδοτούμενη ομάδα με διασυνδέσεις με την Κίνα)
ΣΕ ΠΟΙΟΝ: Διαφορετικές εταιρείες σε όλο τον κόσμο, κυρίως βιομηχανία των ΗΠΑ
ΓΙΑΤΙ: Διείσδυση δεδομένων και πιθανώς κέρδος χρημάτων μέσω ransomware
ΤΙ: Γνώση της εταιρείας, όπως δεδομένα, διευθύνσεις ηλεκτρονικού ταχυδρομείου, γραμματοκιβώτια
ΠΩΣ: Αξιοποίηση πολλαπλών ευπαθειών στον Microsoft Exchange Server για να επιτραπεί μη εξουσιοδοτημένη απομακρυσμένη εκτέλεση κώδικα.
ΣΤΡΑΤΗΓΙΚΗ: Σάρωση της περιοχής IP του διαδικτύου για τη συλλογή λιστών IP των διακομιστών Microsoft Exchange. Εκμετάλλευση των αναφερόμενων ευπαθειών για την ανάπτυξη κελυφών ιστού ή C2 beacons. Χρήση αυτής της πρόσβασης που επέτρεπε τη συμπίεση και διακίνηση δεδομένων μέσω διαδικτυακών ιστότοπων διαμοιρασμού όπως το MEGA. Περιστασιακά ανάπτυξη του ransomware "DearCry". Αυτό ήταν δυνατό λόγω της καθυστερημένης διαθεσιμότητας του patch και της κακής διαχείρισης των patch από τις εταιρείες.

ΑΝΑΚΑΜΨΗ

ΕΠΙΠΤΩΣΕΙΣ: Οι συνέπειες αυτής της επίθεσης μπορούν να θεωρηθούν ως απώλεια πληροφοριών, καθώς τόσο η διαρροή όσο και το ransomware εντάσσονται σε αυτή την κατηγορία. Επιπλέον, εάν οι οργανισμοί προσπάθησαν να πληρώσουν τα λύτρα για να πάρουν πίσω τα δεδομένα τους, κατέληξαν επίσης σε οικονομική ζημιά.

ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ: Ανάλογα με τη συγκεκριμένη επίθεση, η αποκατάσταση μπορεί να διαφέρει. Η διαδικασία ανάκτησης από ένα ransomware μπορεί να διαρκέσει πολύ. Ολα τα μολυσμένα συστήματα πρέπει είτε να επανεγκατασταθούν είτε πρέπει να γίνει επαναφορά ενός αντιγράφου ασφαλείας. Εάν τα αντίγραφα ασφαλείας έχουν αποθηκευτεί σε ένα μολυσμένο σύστημα, προφανώς δεν μπορούν να χρησιμοποιηθούν για τη διαδικασία ανάκτησης. Η ανάκτηση από τη διείσδυση δεδομένων είναι διαφορετική. Αρχικά θα πρέπει να εφαρμοστούν τα διαθέσιμα διορθωτικά προγράμματα και να αφαιρεθούν τα ίχνη των web shells ή των C2 beacons. Είναι σημαντικό να αξιολογηθεί ποια και πόσα δεδομένα εκλάπησαν για να μετρηθεί ο αντίκτυπος.

ΚΑΛΥΤΕΡΗ ΣΤΡΑΤΗΓΙΚΗ

- ☑ Διατηρείτε τα συστήματα προστασίας από ιούς ενημερωμένα
- ☑ Χρήση συστημάτων ανίχνευσης και πρόληψης εισβολών
- ☑ Σωστή παρακολούθηση των συστημάτων για ύποπτες δραστηριότητες
- ☑ Σωστή διαμόρφωση των συστημάτων και απενεργοποίηση των μη απαιτούμενων υπηρεσιών
- ☑ Γρήγορη διαχείριση διορθώσεων για την επιδιόρθωση ευπαθειών το συντομότερο δυνατό
- ☑ Χρησιμοποιήστε τμηματοποίηση σε επίπεδο δικτύου και περιορίστε την επιτρεπόμενη επικοινωνία στο απαιτούμενο ελάχιστο.

ΔΙΔΑΓΜΑΤΑ

Η εκμετάλλευση μηδενικής ημέρας με αλυσίδες επιθέσεων φαίνεται πολύ τρομακτική. Το κλειδί για την αντιμετώπιση αυτών των προκλήσεων είναι η κατάλληλη τμηματοποίηση του δικτύου και η παρακολούθηση του συστήματος για τον έγκαιρο εντοπισμό πιθανών επιθέσεων. Τα συστήματα εισβολής και πρόληψης δικτύου μπορούν επίσης να βοηθήσουν στον εντοπισμό τέτοιων επιθέσεων. Αυτό που είναι επίσης σημαντικό είναι ότι πρέπει να εφαρμόζονται το συντομότερο δυνατόν διορθώσεις για κρίσιμα τρωτά σημεία για την περαιτέρω αποκατάσταση των φορέων επιθέσεων.

Ως άλλο μάθημα που πήραμε, θέλω να αναφέρω τους ερευνητές ασφαλείας της DevCore που εντόπισαν πρώτοι τις ευπάθειες και βοήθησαν τη Microsoft στη διαδικασία επιδιόρθωσης. Αυτό ενισχύει τη σημασία της ανεξάρτητης έρευνας ασφάλειας για καλό σκοπό.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 9: WannaCry: ΟΤΑΝ ΕΝΑ RANSOMWARE ΠΑΡΑΛΥΣΕΙ ΤΟ ΣΥΣΤΗΜΑ ΥΓΕΙΑΣ

Το 2017, ένα νέο ransomware με την ονομασία **WannaCry (WannaCrypt),** το οποίο στοχεύει στο λειτουργικό σύστημα Windows, μόλυνε χιλιάδες πελάτες σε όλο τον κόσμο. Αντί να στοχεύει έναν συγκεκριμένο οργανισμό, η επίθεση ήταν ευρέως διαδεδομένη και επηρέασε πολλές εταιρείες σε διάφορους τομείς.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Η μέθοδος που εφαρμόστηκε για τη συλλογή των πληροφοριών για την παρούσα μελέτη περίπτωσης ήταν η έρευνα γραφείου, ενώ οι συγκεκριμένες πηγές πληροφοριών μπορούν να βρεθούν στην ενότητα "Αναφορές" του παρόντος εγγράφου.

ΠΡΟΛΗΨΗ

Πολλές εταιρείες επηρεάστηκαν από την επίθεση αυτή, γεγονός που οδηγεί στην υπόθεση ότι οι διαφορετικές πρακτικές ασφαλείας που ισχύουν για τις εταιρείες αυτές είχαν μηδενικό αντίκτυπο.

ΑΝΑΓΝΩΡΙΣΗ

Το WannaCry είναι μια κακόβουλη εφαρμογή που χαρακτηρίζεται ως ransomware, καθώς κρυπτογραφεί συγκεκριμένα αρχεία του χρήστη σε ένα στοχευμένο σύστημα. Αυτό οδηγεί σε αλλοίωση των δεδομένων και καταστροφή τους, καθώς ο ιδιοκτήτης του μολυσμένου συστήματος δεν είναι σε θέση να αποκρυπτογραφήσει τα αρχεία. Αυτό καταλήγει στη συνέχεια σε μια επίθεση άρνησης παροχής υπηρεσιών λόγω των αρχείων και των δεδομένων που λείπουν.

Ενα από τα κύρια χαρακτηριστικά του WannaCry είναι η τεχνική που χρησιμοποιεί για την αυτόματη αναζήτηση πιθανών συστημάτων-στόχων, τα οποία το ransomware προσπαθεί στη συνέχεια να μολύνει. Καθώς αυτό το κακόβουλο λογισμικό μπορεί να μολύνει άλλα συστήματα από ένα ήδη

μολυσμένο, αναφέρεται επίσης ως σκουλήκι. Για την επίτευξη αυτού του στόχου, χρησιμοποιείται ένα exploit για ευπάθεια λογισμικού στο πρωτόκολλο SMB των Microsoft Windows που ονομάζεται Eternal Blue και αντιστοιχεί στο MITRE ATT&CK ID T1210.

Πριν το κακόβουλο λογισμικό εξαπλωθεί και μολύνει άλλα συστήματα, πρέπει πρώτα να τα αναζητήσει και να τα βρει. Αυτό γίνεται με διάφορες τεχνικές, όπως σάρωση για απομακρυσμένα συστήματα (T1018), απαρίθμηση ενεργών συνόδων απομακρυσμένης επιφάνειας εργασίας (T1563), σάρωση για νέες συνδεδεμένες μονάδες δίσκου στο μολυσμένο σύστημα (T1120). Μόλις βρεθεί μια πιθανή απομακρυσμένη συσκευή ή μονάδα δίσκου, το WannaCry προσπαθεί να αντιγραφεί στο σύστημα-στόχο και να εκτελέσει την κακόβουλη συμπεριφορά του.

Για τον εντοπισμό αυτής της επίθεσης με βάση τη συμπεριφορά, μπορούν να χρησιμοποιηθούν οι ακόλουθες τεχνικές MITRE ATT&CK:

- ☑ T1210: Εκμετάλλευση απομακρυσμένων υπηρεσιών
- ☑ T1018: Απομακρυσμένη ανακάλυψη συστήματος
- ☑ T1563: 002 RDP Hijacking)
- ☑ T1120: Ανακάλυψη περιφερειακών συσκευών
- ☑ T1490: Αναστολή ανάκτησης συστήματος
- ☑ T1083: Ανακάλυψη αρχείων και καταλόγων
- ☑ T1486: Δεδομένα κρυπτογραφημένα για τον αντίκτυπο
- ☑ T1573: 002 Ασύμμετρη κρυπτογραφία)
- ☑ T1090: μεσολάβησης (.003 Multi-hop Proxy)

"Η επιδημία WannaCry, έπληξε πάνω από 200.000 υπολογιστές σε περισσότερες από 150 χώρες. Κόστισε στο Ηνωμένο Βασίλειο 92 εκατομμύρια λίρες Αγγλίας και ανέβασε το παγκόσμιο κόστος στο ιλιγγιώδες ποσό των 6 δισεκατομμυρίων λιρών Αγγλίας". (Acronis, 2020)

ΑΠΑΝΤΗΣΗ

Το 2017 ένα νέο ransomware με την ονομασία WannaCry (WannaCrypt), το οποίο στοχεύει στο λειτουργικό σύστημα Windows, μόλυνε χιλιάδες πελάτες σε όλο τον κόσμο. Αντί να στοχεύει έναν συγκεκριμένο οργανισμό, η επίθεση ήταν ευρέως διαδεδομένη. Από το ransomware επλήγησαν μεγάλες εταιρείες, όπου ορισμένες από αυτές λειτουργούν τις επιχειρήσεις τους σε όλο τον κόσμο, όπως η αυτοκινητοβιομηχανία. Ωστόσο, επηρεάστηκαν και άλλες ομάδες οργανισμών όπως οι δημόσιες μεταφορές, οι υπηρεσίες υγείας ή οι υπηρεσίες τηλεπικοινωνιών.

- ☑ **ΠΟΙΟΣ:** Άγνωστος
- ☑ **ΣΕ ΠΟΙΟΝ:** Διαφορετικές εταιρείες σε όλο τον κόσμο
- ☑ **ΓΙΑΤΙ:** Φτάστε σε υψηλές ζημιές λόγω απώλειας δεδομένων και πιθανότατα κερδίστε χρήματα
- ☑ **ΤΙ:** Γνώση της εταιρείας, όπως δεδομένα
- ☑ **ΠΩΣ:** που διανεμήθηκε μέσω μιας ευπάθειας που βρέθηκε στα Microsoft Windows.
- ☑ **ΣΤΡΑΤΗΓΙΚΗ:** Το σημείωμα λύτρων που χρησιμοποιήθηκε από το WannaCry εμφανίστηκε στην οθόνη των συστημάτων που είχαν μολυνθεί. Τα συστήματα προστασίας από ιούς και τα τείχη προστασίας εντόπισαν τη μόλυνση και την εξάπλωση του ransomware και ως εκ τούτου δεν απέτρεψαν τα συστήματα από περαιτέρω μολύνσεις και ζημιές.

ΑΝΑΚΑΜΨΗ

ΕΠΙΠΤΩΣΕΙΣ: Οι συνέπειες αυτής της επίθεσης μπορούν να θεωρηθούν ως απώλεια πληροφοριών, καθώς όλα τα αρχεία που έχουν κρυπτογραφηθεί από το ransomware δεν είναι πλέον αναγνώσιμα. Επιπλέον, εάν οι οργανισμοί προσπάθησαν να πληρώσουν τα λύτρα για να πάρουν πίσω τα δεδομένα τους, κατέληξαν επίσης σε οικονομική ζημία.

ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ: Η διαδικασία αποκατάστασης από ένα ransomware μπορεί να διαρκέσει πολύ. Ολα τα μολυσμένα συστήματα πρέπει είτε να επανεγκατασταθούν είτε να γίνει επαναφορά ενός αντιγράφου ασφαλείας. Εάν τα αντίγραφα ασφαλείας έχουν αποθηκευτεί σε ένα μολυσμένο σύστημα, προφανώς δεν μπορούν να χρησιμοποιηθούν για τη διαδικασία ανάκτησης.

ΚΑΛΥΤΕΡΗ ΣΤΡΑΤΗΓΙΚΗ

- ☑ Διατηρείτε τα συστήματα προστασίας από ιούς ενημερωμένα
- ☑ Χρήση συστημάτων ανίχνευσης και πρόληψης εισβολών
- ☑ Σωστή παρακολούθηση των συστημάτων για ύποπτες δραστηριότητες
- ☑ Σωστή διαμόρφωση των συστημάτων και απενεργοποίηση των μη απαιτούμενων υπηρεσιών
- ☑ Γρήγορη διαχείριση διορθώσεων για την επιδιόρθωση ευπαθειών το συντομότερο δυνατό
- ☑ Εκπαίδευση ευαισθητοποίησης των εργαζομένων
- ☑ Χρησιμοποιήστε τμηματοποίηση σε επίπεδο δικτύου και περιορίστε την επιτρεπόμενη επικοινωνία στο απαιτούμενο ελάχιστο.

ΔΙΔΑΓΜΑΤΑ

Οι επιθέσεις Ransomware είναι σήμερα συνηθισμένες και μπορούν να πλήξουν όλες τις εταιρείες. Συνιστάται ιδιαίτερα να ακολουθείτε τις γνωστές πρακτικές ασφαλείας για να καταστήσετε την υποδομή πληροφορικής όσο το δυνατόν πιο ασφαλή, ώστε να περιορίσετε τη ζημία μιας επίθεσης στο ελάχιστο.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 10: ΚΑΤΑΣΚΟΠΕΙΑ ΕΥΑΙΣΘΗΤΩΝ ΙΔΙΩΤΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Το φθινόπωρο του 2020, σε εθνικό επίπεδο ανακοινώθηκε νέος συναγερμός ασφαλείας. Διευκρινιζόταν ότι πολλοί δημόσιοι και ιδιωτικοί φορείς έχουν πληγεί σοβαρά, όπως και σε άλλα προηγούμενα διαδοχικά κύματα, από **επιθέσεις κακόβουλου λογισμικού τύπου EMOTET,** οι οποίες οδήγησαν σε πολυάριθμα προβλήματα. Το EMOTET είναι ένα **κακόβουλο λογισμικό** που μολύνει υπολογιστές με λειτουργικό σύστημα Microsoft Windows μέσω μολυσμένων κακόβουλων συνδέσμων ή συνημμένων αρχείων (π.χ. PDF, DOC, ZIP κ.λπ.).

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Οι πληροφορίες που απαιτούνται για την περιγραφή αυτής της κυβερνοεπίθεσης συλλέχθηκαν μέσω συνέντευξης με τον τεχνικό πληροφορικής της εταιρείας. Η αλληλεπίδραση πραγματοποιήθηκε με την προϋπόθεση της ανωνυμίας των ευαίσθητων πληροφοριών. Ακόμη και αν ο ερωτηθείς ήταν πρόθυμος να περιγράψει το περιστατικό, ορισμένες πληροφορίες δεν ήταν δυνατόν να ληφθούν επειδή το πρόβλημα είχε ανατεθεί σε εξειδικευμένη εταιρεία και έπρεπε να διερευνηθεί χωριστά.

ΠΡΟΛΗΨΗ

Αν και έχουν διεξαχθεί εκστρατείες ευαισθητοποίησης από εξειδικευμένους φορείς και οργανώσεις σχετικά με τα μέτρα που πρέπει να ληφθούν, πολλοί δημόσιοι και ιδιωτικοί οργανισμοί έχουν επηρεαστεί, σύμφωνα με τις υπάρχουσες εκθέσεις.

Στην περίπτωση της εταιρείας που αναλύθηκε, από την άποψη της ασφάλειας στον κυβερνοχώρο, λειτούργησαν συγκεκριμένες διαδικασίες και μηχανισμοί, οι οποίοι όμως δεν ήταν αρκετοί λόγω της χαμηλής εμπειρίας ορισμένων εργαζομένων στον ψηφιακό τομέα.

ΑΝΑΓΝΩΡΙΣΗ

Το Emotet είναι ένα Trojan που αρχικά σχετιζόταν με τραπεζικές απάτες, το οποίο, από το 2017, περιορίζεται σε spam και δευτερεύουσα διανομή ωφέλιμου φορτίου. Επί του παρόντος μπορούν να εντοπιστούν πολυάριθμες παραλλαγές του Emotet και δυστυχώς αυτό το κακόβουλο λογισμικό συνεχίζει να εξελίσσεται σε νέες παραλλαγές με πιο σύνθετες δυνατότητες και τεχνικές αποφυγής.

Με βάση τις περιγραφές που δόθηκαν και συμπληρωματικά από τις αναφορές των μέσων ενημέρωσης, στο περιστατικό εμπλέκονται τα ακόλουθα στοιχεία:

- ☑ Λάβατε ένα κοινωνικά σχεδιασμένο ηλεκτρονικό μήνυμα ηλεκτρονικού "ψαρέματος" με συνημμένο ένα αρχείο Zipped και με τον κωδικό πρόσβασης να περιλαμβάνεται στο μήνυμα.
- ☑ Το κακόβουλο λογισμικό ήταν κρυπτογραφημένο και προστατευμένο με κωδικό πρόσβασης σε ένα αρχείο αρχειοθέτησης
- ☑ Παρέκαμψε λύσεις anti-malware χρησιμοποιώντας αρχεία προστατευμένα με κωδικό πρόσβασης ως συνημμένα αρχεία
- ☑ Ο φορτωτής Trojan περιείχε καλοήθη κώδικα από ένα DLL της Microsoft για να αποφύγει τις λύσεις προστασίας από ιούς.
- ☑ Κατάχρηση νήματος για τη διανομή κακόβουλου κώδικα με χρήση αρχείων που προστατεύονται με κωδικό πρόσβασης ως συνημμένα αρχεία
- ☑ Τα παραβιασμένα συστήματα χρησιμοποιήθηκαν για την αποστολή κακόβουλων μηνυμάτων ηλεκτρονικού ταχυδρομείου σε άλλες επαφές
- ☑ Προσωρινή διακοπή λειτουργίας των συστημάτων ηλεκτρονικού ταχυδρομείου για να σταματήσει η περαιτέρω εξάπλωση του Trojan
- ☑ Επηρεασμένα εσωτερικά δίκτυα

Σύμφωνα με το MITRE ATT&CK framework, το περιστατικό αυτό μπορεί να περιγραφεί ως εξής:

1. T1566.001 - Επισύναψη Spearphishing
2. T1204.002 - Εκτέλεση από τον χρήστη: Αρχείο: Κακόβουλο αρχείο
3. T1027 - Συγκαλυμμένα αρχεία ή πληροφορίες
4. T1036 - Μεταμφιέσεις
5. T1586.002 - Λογαριασμοί συμβιβασμού: Λογαριασμοί ηλεκτρονικού ταχυδρομείου
6. T1586.002 - Λογαριασμοί συμβιβασμού: Λογαριασμοί ηλεκτρονικού ταχυδρομείου
7. T1499 - Άρνηση παροχής υπηρεσιών σε τελικό σημείο
8. T1498 - Άρνηση υπηρεσίας δικτύου

ΑΠΑΝΤΗΣΗ

ΠΟΙΟΣ: Ο επιτιθέμενος δεν μπόρεσε να αναγνωριστεί με ακρίβεια. Μόνο ο τόπος καταγωγής, το Βιετνάμ, ήταν γνωστός.
ΣΕ ΠΟΙΟΝ: μη συγκεκριμένος στόχος
ΓΙΑΤΙ: Συλλογή ευαίσθητων δεδομένων και πληρωμές ransomware
ΤΙ: Δεδομένα εταιρείας/χρηστών
ΠΩΣ: Spearphishing Attachment, εκτέλεση σεναρίου, έγχυση διαδικασίας.
ΣΤΡΑΤΗΓΙΚΗ: Η απειλή ξεκίνησε από έναν υπολογιστή χωρίς antivirus και εξαπλώθηκε πλευρικά. Πραγματοποιήθηκε διαδικασία καθαρισμού από εξειδικευμένη εταιρεία IT&C.

"Το EMOTET ήταν κάτι πολύ περισσότερο από ένα κακόβουλο λογισμικό. Αυτό που έκανε το EMOTET τόσο επικίνδυνο είναι ότι το κακόβουλο λογισμικό προσφερόταν προς ενοικίαση σε άλλους εγκληματίες του κυβερνοχώρου για να εγκαταστήσουν άλλους τύπους κακόβουλου λογισμικού, όπως τραπεζικά Trojans ή ransomwares, στον υπολογιστή του θύματος". (EUROPOL, 2022)

ΑΝΑΚΑΜΨΗ

IMPACT: The main consequences of the attack were as following:

- ☑ Data loss
- ☑ Regular activity disruption
- ☑ System compromise
- ☑ Financial costs

ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ: The recovery strategy was focused on cleaning and reinstalling the compromised computers, cleaning and/or reinitialising the compromise e-mail-boxes.

BETTER STRATEGY

- ☑ Install and keep an updated Antivirus/Antimalware
- ☑ Adopt a Network Intrusion Prevention
- ☑ Restrict Web-Based Content
- ☑ Assure the user awareness
- ☑ Better Password Policies
- ☑ Privileged Account Management
- ☑ Disable or Remove Feature or Program
- ☑ Execution Prevention
- ☑ Audit
- ☑ User Account Management
- ☑ Behavior Prevention on Endpoint
- ☑ Account Use Policies.

ΔΙΔΑΓΜΑΤΑ

Ακόμη και αν η Emotet καταργήθηκε μέσω μιας διεθνούς συντονισμένης δραστηριότητας, μένει να δούμε αν αυτό θα έχει μακροχρόνιο αντίκτυπο.

Πρέπει να σημειωθεί ότι τα κακόβουλα προγράμματα χρησιμοποιούν σχεδόν τις ίδιες τεχνικές για να διεισδύσουν και να εξαπλωθούν στη φύση, οπότε είναι υποχρεωτικό να είστε ενήμεροι και προσεκτικοί, καθώς οι κυβερνοεπιθέσεις θα συνεχίσουν να υπάρχουν και στο μέλλον. Μέτρα όπως το ενδεχόμενο να επικοινωνείτε με τον κόσμο χρησιμοποιώντας υπολογιστή απομονωμένο από το δίκτυο που φιλοξενεί κρίσιμες υποδομές, η χρήση ικανών και ενημερωμένων λύσεων ασφαλείας, το ενδεχόμενο να έχετε τις τελευταίες ενημερώσεις είναι μερικά από αυτά που πρέπει να προβλεφθούν.

Ακόμη και αν η Emotet καταργήθηκε μέσω μιας διεθνούς συντονισμένης δραστηριότητας, μένει να δούμε αν αυτό θα έχει μακροχρόνιο αντίκτυπο.

Πρέπει να σημειωθεί ότι τα κακόβουλα προγράμματα χρησιμοποιούν σχεδόν τις ίδιες τεχνικές για να διεισδύσουν και να εξαπλωθούν στη φύση, οπότε είναι υποχρεωτικό να είστε ενήμεροι και προσεκτικοί, καθώς οι κυβερνοεπιθέσεις θα συνεχίσουν να υπάρχουν και στο μέλλον. Μέτρα όπως το ενδεχόμενο να επικοινωνείτε με τον κόσμο χρησιμοποιώντας υπολογιστή απομονωμένο από το δίκτυο που φιλοξενεί κρίσιμες υποδομές, η χρήση ικανών και ενημερωμένων λύσεων ασφαλείας, το ενδεχόμενο να έχετε τις τελευταίες ενημερώσεις είναι μερικά από αυτά που πρέπει να προβλεφθούν.

Το Phishing είναι ένας γενικός όρος για τις επιθέσεις τύπου κοινωνικής μηχανικής που πραγματοποιούνται σήμερα μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου ή εφαρμογών κοινωνικής δικτύωσης.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 11: ΠΑΡΑΝΟΜΗ ΠΡΟΣΒΑΣΗ ΣΕ ΔΙΑΠΙΣΤΕΥΤΗΡΙΑ

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Όπως κάθε σύγχρονη εταιρεία, στην περίπτωση της περιγραφείσας κατάστασης, η ηλεκτρονική επικοινωνία μέσω του Διαδικτύου με τους πελάτες και τους προμηθευτές της είναι ο πλέον προτιμώμενος τρόπος. Στο πλαίσιο αυτού του τύπου επικοινωνίας, ένας από τους πλέον χρησιμοποιούμενους είναι το ηλεκτρονικό ταχυδρομείο. Επιτρέπει την ασύγχρονη διατήρηση επαφής με τους ενδιαφερόμενους που διαχειρίζονται με αποτελεσματικό τρόπο περισσότερα από ένα άτομα. Η εταιρεία που βρίσκεται πάνω από μισό αιώνα στην αγορά έχει αναπτυχθεί έντονα στην ψηφιοποίηση σε κάθε τμήμα, και σε αυτό το πλαίσιο περιλαμβάνεται και το τμήμα σχέσεων με τους πελάτες. Για τους σχετικούς υπαλλήλους έχει δημιουργηθεί μια ομάδα ηλεκτρονικού ταχυδρομείου για τη διαχείριση των ηλεκτρονικών αιτημάτων από ειδικούς υπολογιστές που προστατεύονται από λειτουργίες προστασίας από ιούς και φιλτραρίσματος ανεπιθύμητης αλληλογραφίας στον διακομιστή ηλεκτρονικού ταχυδρομείου.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Οι πληροφορίες που απαιτούνται για την περιγραφή αυτής της κυβερνοεπίθεσης συλλέχθηκαν μέσω συνέντευξης με έναν από τους τεχνικούς πληροφορικής της εταιρείας. Η αλληλεπίδραση πραγματοποιήθηκε με την προϋπόθεση της ανωνυμίας των ευαίσθητων πληροφοριών. Ακόμη και αν ο συνεντευξιαζόμενος ήταν πρόθυμος να

περιγράψει το περιστατικό, ορισμένες πληροφορίες δεν ήταν δυνατόν να ληφθούν επειδή το πρόβλημα το διαχειριζόταν διαφορετική ομάδα.

ΠΡΟΛΗΨΗ

Παρά το γεγονός ότι η Εθνική Διεύθυνση Ασφάλειας στον Κυβερνοχώρο έχει πραγματοποιήσει εκστρατείες ευαισθητοποίησης σχετικά με τα μέτρα που πρέπει να ληφθούν, πολλοί δημόσιοι, ιδιωτικοί οργανισμοί και ιδιώτες έχουν επηρεαστεί, σύμφωνα με τις υπάρχουσες εκθέσεις.

Η εταιρεία επέβαλε τη χρήση εργαλείων ασφαλείας και προσαρμοσμένων κανονισμών για την εργασία στο διαδίκτυο, αλλά αυτά δεν ήταν αρκετά λόγω της βασικής εμπειρίας ορισμένων εργαζομένων στον ψηφιακό τομέα.

ΑΝΑΓΝΩΡΙΣΗ

Το **Phishing** είναι ένας γενικός όρος για τις **επιθέσεις τύπου κοινωνικής μηχανικής που πραγματοποιούνται** σήμερα μέσω μηνυμάτων ηλεκτρονικού ταχυδρομείου ή εφαρμογών κοινωνικής δικτύωσης. Συνήθως, οι εγκληματίες του κυβερνοχώρου στέλνουν μαζικά ανεπιθύμητα μηνύματα. Θέλουν να στοχεύσουν όσο το δυνατόν περισσότερους ανθρώπους, προκειμένου να πιάσουν κάποιους από αυτούς με το κόλπο τους.

Οι εγκληματίες του κυβερνοχώρου προσπαθούν να εκμεταλλευτούν την τάση κάποιου είδους "μεγάλων προσφορών" ή με κάποιες διοικητικές οδηγίες. Πολλά από αυτά τα είδη μηνυμάτων φαίνονται να είναι νόμιμα, καθώς χρησιμοποιούν την ίδια οπτική ταυτότητα με γνωστές εταιρείες, διαδικτυακές υπηρεσίες ή εφαρμογές. Ορισμένα παραδείγματα περιλαμβάνουν εταιρείες όπως οι Google, Amazon, Microsoft, Yahoo, LinkedIn κ.λπ. ή δημοφιλείς τραπεζικές υπηρεσίες και εφαρμογές όπως αυτή της διαχείρισης ηλεκτρονικού ταχυδρομείου μέσω διαδικτύου.

Η αξιοπιστία επιδιώκεται να επιτευχθεί με την αντιγραφή του χρωματικού σχεδιασμού, του στυλ, του λογότυπου και των συνθημάτων της αντιγραμμένης ταυτότητας. Χρησιμοποιούνται τυπικές ελκυστικές γραμμές θέματος.

Με βάση την παρεχόμενη περιγραφή και τις συμπληρωματικές αναφορές των μέσων ενημέρωσης, τα ακόλουθα στοιχεία εμπλέκονται στο περιστατικό:

- ☑ Εγινε λήψη ενός κοινωνικά σχεδιασμένου ηλεκτρονικού μηνύματος ηλεκτρονικού "ψαρέματος" που ισχυριζόταν ότι πρέπει να αλλάξει επειγόντως ο κωδικός πρόσβασης για να αποφευχθεί το τέλος της υπηρεσίας,
- ☑ Η παροχή διαπιστευτηρίων στην παράνομη οντότητα οδήγησε στην πρόσβαση στο λογαριασμό ηλεκτρονικού ταχυδρομείου και στη διακοπή της νόμιμης πρόσβασης με την αλλαγή του κωδικού πρόσβασης,
- ☑ Ο παραβιασμένος λογαριασμός χρησιμοποιήθηκε για ανεπιθύμητα μηνύματα ηλεκτρονικού "ψαρέματος" που στάλθηκαν στις υπάρχουσες επαφές και σε άλλες διευθύνσεις που ανήκαν στον επιτιθέμενο,

- ☑ Λόγω της μαζικής αποστολής μηνυμάτων ανεπιθύμητης αλληλογραφίας μέσω του Διαδικτύου, η υπηρεσία ηλεκτρονικού ταχυδρομείου μπήκε σε μαύρη λίστα, με αποτέλεσμα να διακοπεί η κανονική λειτουργία,
- ☑ Το σύστημα ηλεκτρονικού ταχυδρομείου ανεστάλη προσωρινά για να σταματήσει η περαιτέρω αποστολή ανεπιθύμητων μηνυμάτων,
- ☑ Οι διαδικτυακές λειτουργίες επηρεάστηκαν.

Σύμφωνα με το MITRE ATT&CK framework, το περιστατικό αυτό μπορεί να περιγραφεί ως εξής:

1. T1598.001- Υπηρεσία Spearphishing
2. T1598.002- Συνημμένο Spearphishing
3. T1598.003- Σύνδεσμος Spearphishing

ΑΠΑΝΤΗΣΗ

- ☑ **ΠΟΙΟΣ:** Ο επιτιθέμενος δεν μπόρεσε να ταυτοποιηθεί επακριβώς, καθώς έχουν καταγραφεί καταβολές από διάφορες χώρες. Πιθανή χρήση VPN εμπλέκεται.
- ☑ **ΣΕ ΠΟΙΟΝ:** μη συγκεκριμένος στόχος
- ☑ **ΓΙΑΤΙ:** Συλλογή ευαίσθητων δεδομένων και εκβιασμός χρημάτων
- ☑ **ΤΙ:** Δεδομένα εταιρείας/χρηστών
- ☑ **ΠΩΣ:** Phishing, κλοπή διαπιστευτηρίων.
- ☑ **ΣΤΡΑΤΗΓΙΚΗ:** Η απειλή ξεκίνησε με το άνοιγμα ενός υποδυόμενου ηλεκτρονικού ταχυδρομείου, την πρόσβαση σε παραποιημένους συνδέσμους και την υποβολή ευαίσθητων δεδομένων. Η ομάδα πληροφορικής πραγματοποίησε επαναφορά των διαπιστευτηρίων και διαγραφή από τις υπηρεσίες μαύρης λίστας.

ΑΝΑΚΑΜΨΗ

ΕΠΙΠΤΩΣΕΙΣ: Οι κύριες συνέπειες της επίθεσης ήταν οι εξής:

- ☑ Απώλεια διαπιστευτηρίων
- ☑ Διακοπή της τακτικής δραστηριότητας
- ☑ Συμβιβασμός του συστήματος.

ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ: Η στρατηγική αποκατάστασης επικεντρώθηκε στην επαναφορά των διαπιστευτηρίων και στον καθαρισμό των παραβιασμένων προγραμμάτων ηλεκτρονικού ταχυδρομείου.

ΚΑΛΥΤΕΡΗ ΣΤΡΑΤΗΓΙΚΗ

- ☑ Εγκαταστήστε και διατηρήστε ένα ενημερωμένο σύστημα φιλτραρίσματος Antivirus/Antimalware/Email.
- ☑ Υιοθετήστε ένα σύστημα πρόληψης εισβολών στο δίκτυο
- ☑ Περιορισμός του περιεχομένου που βασίζεται στο Web
- ☑ Διασφάλιση της ευαισθητοποίησης του χρήστη
- ☑ Καλύτερες πολιτικές κωδικού πρόσβασης

- ☑ Διαχείριση προνομιακών λογαριασμών
- ☑ Έλεγχος
- ☑ Διαχείριση λογαριασμού χρήστη
- ☑ Πρόληψη συμπεριφοράς στο Endpoint
- ☑ Πολιτικές χρήσης λογαριασμού.

ΔΙΔΑΓΜΑΤΑ

Παρόλο που το phishing δεν είναι μια νέα τεχνική, παραμένει ένας από τους κύριους τρόπους σε πολλές επιθέσεις κυβερνοασφάλειας.

Πρέπει να σημειωθεί ότι τα κακόβουλα προγράμματα χρησιμοποιούν σχεδόν αυτή την τεχνική για να διεισδύσουν και να εξαπλωθούν στην άγρια φύση, οπότε είναι υποχρεωτικό να είστε ενήμεροι και προσεκτικοί, καθώς οι κυβερνοεπιθέσεις με αυτόν τον τρόπο θα συνεχίσουν να υπάρχουν. Μέτρα όπως η εξέταση της χρήσης καλύτερα ενημερωμένων προστατευμένων υπηρεσιών ηλεκτρονικού ταχυδρομείου, η μεγαλύτερη ευαισθητοποίηση σχετικά με την πρόσβαση σε μηνύματα ηλεκτρονικού ταχυδρομείου και η σωστή ανάλυση της νομιμότητας του αποστολέα.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 12: ΞΕΠΕΡΑΣΜΕΝΕΣ ΕΦΑΡΜΟΓΕΣ ΠΟΥ ΕΚΤΙΘΕΝΤΑΙ ΣΤΟ ΔΙΑΔΙΚΤΥΟ

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

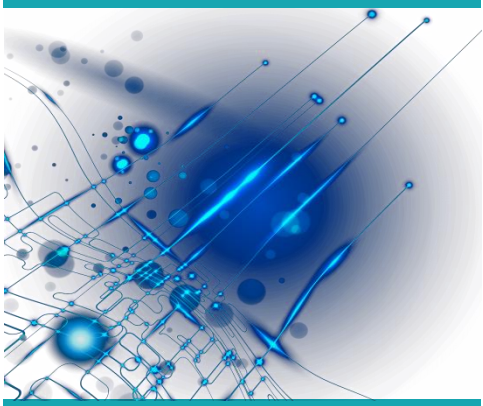
Στις μέρες μας πολλές επιχειρήσεις έχουν αλλάξει τον τρόπο παροχής των υπηρεσιών τους μετακινούμενες στο διαδίκτυο. Αυτή είναι η περίπτωση του αχρησιμοποίητου παραδείγματος, όπου στο γραφείο παρέχονται υπηρεσίες χρηματοπιστωτικού τύπου που ξεκίνησαν το 1998 έχουν μεταφερθεί στο διαδίκτυο για περισσότερο από μια δεκαετία. Η νέα προσέγγιση βελτίωσε τη συνολική δραστηριότητα της εταιρείας και την ικανοποίηση των πελατών. Ωστόσο, τα επιτεύγματα αυτά ήταν δυνατά μόνο μετά από σημαντική προσπάθεια για την ανάπτυξη του απαιτούμενου προσαρμοσμένου λογισμικού που αναπτύχθηκε εσωτερικά. Αυτή η διαδικτυακή εφαρμογή επέτρεψε στους πελάτες και τους υπαλλήλους να εκτελούν τις απαραίτητες εργασίες. Η παρεχόμενη πλατφόρμα που αναπτύχθηκε σε εκείνο το δημοφιλές πλαίσιο της εποχής διατηρήθηκε μέχρι την υποστήριξη που ήταν διαθέσιμη πριν από την κυκλοφορία της νέας μεγάλης αναβάθμισης. Με την πάροδο του χρόνου ο αριθμός των εργαζομένων μειώθηκε λόγω της αυτοματοποίησης των υφιστάμενων διαδικασιών και των αλλαγών στην αγορά. Η αναβάθμιση

στη νέα διανομή καθυστέρησε καθώς απαιτούνταν σημαντικό υλικό και λογισμικό.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Οι πληροφορίες που απαιτούνται για την περιγραφή αυτής της κυβερνοεπίθεσης συλλέχθηκαν μέσω συνέντευξης με τον διευθύνοντα σύμβουλο της εταιρείας. Η αλληλεπίδραση πραγματοποιήθηκε με την προϋπόθεση της ανωνυμίας των ευαίσθητων πληροφοριών.

ΠΡΟΛΗΨΗ



Παρά το γεγονός ότι η Εθνική Διεύθυνση Ασφάλειας στον Κυβερνοχώρο έχει πραγματοποιήσει εκστρατείες ευαισθητοποίησης σχετικά με τα μέτρα που πρέπει να ληφθούν, πολλοί δημόσιοι ή ιδιωτικοί οργανισμοί αγνοούν ή καθυστερούν την απόφαση και τις ενέργειες που απαιτούνται για την ενημέρωση των πληροφοριακών τους συστημάτων.

Η εταιρεία επέβαλε τη χρήση γνωστών λύσεων ασφαλείας, τείχη προστασίας, τμηματοποίηση δικτύου κ.λπ., αλλά αυτά δεν ήταν αρκετά, καθώς παρέμεινε εκτεθειμένη ευπάθεια σε μία από τις λειτουργούσες μονάδες λογισμικού.

ΑΝΑΓΝΩΡΙΣΗ

Οι επιθέσεις έγχυσης ροής κάνουν κατάχρηση της ικανότητας μιας διαδικτυακής εφαρμογής να δέχεται περιεχόμενο που έχει μεταφορτωθεί, όπως διαφορετικού τύπου έγγραφα ή αρχεία εικόνων. Χρησιμοποιώντας την προσέγγιση απομακρυσμένης ένταξης αρχείων, ένας εισβολέας μπορεί να εκμεταλλευτεί την ευπάθεια στον κώδικα από την πλευρά του διακομιστή ώστε να δεχτεί μια διεύθυνση URL σε έναν άλλο ιστότοπο ως έγκυρη είσοδο. Αυτή η ενέργεια χρησιμοποιείται στη συνέχεια για την εκτέλεση κακόβουλου κώδικα του επιτιθέμενου. Επιπλέον, η τοπική ενσωμάτωση αρχείων μπορεί να χρησιμοποιηθεί για να κάνει μια εφαρμογή ιστού να επιστρέψει το επιθυμητό περιεχόμενο από το τοπικό σύστημα αρχείων.

Ενα δημοφιλές παράδειγμα συναντάται στην περίπτωση του πλαισίου PHP που χρησιμοποιείται από το WordPress και επιτρέπει στον χάκερ να έχει πρόσβαση στο αρχείο ρυθμίσεων. Αυτή η επίθεση μπορεί επίσης να επιτρέψει την πρόσβαση στη λήψη οποιουδήποτε αρχείου πηγαίου κώδικα PHP που εκτελεί τον ιστότοπο, προσφέροντας νέες δυνατότητες για άλλα τρωτά σημεία ασφαλείας. Οι πρόσφατες εκδόσεις PHP προστατεύονται από προεπιλογή από την απομακρυσμένη συμπερίληψη

αρχείων, αλλά αν κατά λάθος εκτεθεί η τοπική συμπερίληψη αρχείων αυτός ο τύπος επίθεσης εξακολουθεί να είναι δυνατός.

Με βάση την παρεχόμενη περιγραφή, τις συμπληρωματικές τεχνικές εκθέσεις, τα δελτία ασφαλείας και τα δελτία ευπαθειών, το περιστατικό αφορούσε τις ακόλουθες λεπτομέρειες:

- ☑ Με μια επίθεση τύπου brute force, ένας λογαριασμός που προστατεύεται με έναν αδύναμο κωδικό πρόσβασης αποκτά παράνομη πρόσβαση,
- ☑ Τα διαπιστευτήρια που ανακαλύφθηκαν επιτρέπουν την αλλαγή των δεδομένων που σχετίζονται με το λογαριασμό,
- ☑ Ο παραβιασμένος λογαριασμός επέτρεψε την αποκάλυψη της ευπάθειας stream injection και η ανεπιθύμητη εκτέλεση κώδικα στον διακομιστή χρησιμοποιήθηκε για την αφαίρεση των αρχείων καταγραφής ιστορικού πρόσβασης,
- ☑ Λόγω της ανεξέλεγκτης εκτέλεσης κώδικα από την πλευρά του διακομιστή, ορισμένες ενότητες της εφαρμογής κατέστησαν άχρηστες και οδήγησαν στον τερματισμό της υπηρεσίας, οπότε η κανονική λειτουργία διακόπηκε,
- ☑ Το σύστημα αποσυνδέθηκε προσωρινά από το Διαδίκτυο για περαιτέρω έρευνα σχετικά με τη δυσλειτουργία της διαδικτυακής εφαρμογής,
- ☑ Οι διαδικτυακές λειτουργίες επηρεάστηκαν.

Σύμφωνα με το MITRE ATT&CK framework, το περιστατικό αυτό μπορεί να περιγραφεί ως εξής:

1. T1110.001 - Μάντεμα κωδικού πρόσβασης
2. T1078 - Πρόσβαση σε έγκυρους λογαριασμούς
3. T1518 - Ανακάλυψη λογισμικού
4. T1082 - Ανακάλυψη πληροφοριών συστήματος
5. T1007 - Ανακάλυψη υπηρεσιών συστήματος
6. T0826 - Απώλεια διαθεσιμότητας.

ΑΠΑΝΤΗΣΗ

- ☑ **ΠΟΙΟΣ:** Ο επιτιθέμενος δεν μπόρεσε να αναγνωριστεί με ακρίβεια.
- ☑ **ΣΕ ΠΟΙΟΝ:** μη συγκεκριμένος στόχος
- ☑ **ΓΙΑΤΙ:** Συλλογή ευαίσθητων δεδομένων και άρνηση παροχής υπηρεσιών
- ☑ **ΤΙ:** Δεδομένα εταιρείας/χρηστών
- ☑ **ΠΩΣ:** Κλοπή διαπιστευτηρίων και εκτέλεση κώδικα με έγχυση ροής.
- ☑ **ΣΤΡΑΤΗΓΙΚΗ:** Η απειλή ξεκίνησε με επίθεση ωμής βίας που οδήγησε σε ανακάλυψη αδύναμων διαπιστευτηρίων, εκμετάλλευση ευπάθειας σε μη δημόσια προσβάσιμη ενότητα λογισμικού και στη συνέχεια μη εξουσιοδοτημένη εκτέλεση κώδικα. Η αδύναμη στρατηγική προστασίας της διαδικτυακής πρόσβασης, η ξεπερασμένη ενότητα λογισμικού και ο μη συντηρημένος κώδικας είναι η κύρια αιτία του περιστατικού.

ΑΝΑΚΑΜΨΗ

ΕΠΙΠΤΩΣΕΙΣ: Οι κύριες συνέπειες της επίθεσης ήταν οι εξής:

- ☑ Απώλεια διαπιστευτηρίων
- ☑ Συμβιβασμός του συστήματος
- ☑ Διακοπή της τακτικής δραστηριότητας.

ΣΤΡΑΤΗΓΙΚΗ ΑΝΑΚΑΜΨΗΣ: Η στρατηγική ανάκαμψης επικεντρώθηκε στη μεγάλη αναβάθμιση της πλατφόρμας με την επανεγγραφή ενός σημαντικού μέρους του κώδικα.

ΚΑΛΥΤΕΡΗ ΣΤΡΑΤΗΓΙΚΗ

- ☑ Εγκαταστήστε και διατηρήστε ενημερωμένο λογισμικό
- ☑ Επιβολή πολιτικής ισχυρών κωδικών πρόσβασης
- ☑ Πολιτικές χρήσης λογαριασμού
- ☑ Υιοθέτηση μηχανισμού ελέγχου ταυτότητας δύο παραγόντων
- ☑ Υιοθετήστε ένα σύστημα πρόληψης εισβολών στο δίκτυο
- ☑ Περιορισμός της απομακρυσμένης πρόσβασης
- ☑ Διασφάλιση της ευαισθητοποίησης του χρήστη
- ☑ Εφαρμογή περιοδικού ελέγχου ασφαλείας
- ☑ Διαχείριση λογαριασμού χρήστη
- ☑ Πρόληψη συμπεριφοράς στο Endpoint.

ΔΙΔΑΓΜΑΤΑ

Ακόμη και αν το ξεπερασμένο λογισμικό που εκτελείται είναι γνωστό ότι είναι επιρρεπές σε ευπάθειες ασφαλείας, παραμένει ένας από τους κύριους τρόπους σε πολλές επιθέσεις κυβερνοασφάλειας.

Οι διαδικτυακές εφαρμογές που είναι προσβάσιμες παγκοσμίως είναι εκτεθειμένες σε πολλά τρωτά σημεία και, κατά συνέπεια, απαιτούν ιδιαίτερη προσοχή από πολλές απόψεις.

Μέτρα όπως η συνεχής ενημέρωση του λογισμικού, οι βελτιώσεις και η υιοθέτηση νέων τεχνικών και λύσεων για τους μηχανισμούς ελέγχου ταυτότητας, η υιοθέτηση μιας τακτικής διαδικασίας ελέγχου είναι μερικά από τα συνήθη μέτρα που μπορούν να εξεταστούν.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 13: ΟΙ ΚΙΝΔΥΝΟΙ ΜΙΑΣ ΕΠΙΘΕΣΗΣ ΑΠΟ ΕΝΑΝ ΠΡΩΗΝ ΥΠΑΛΛΗΛΟ

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Ο οργανισμός στον οποίο σημειώθηκε η κυβερνοεπίθεση, δραστηριοποιείται στην εμπορική παρακολούθηση, σε έναν κλάδο της αυτοκινητοβιομηχανίας, με περίπου 2000 υπαλλήλους. Βρίσκεται στην πολιτεία Παρανά και Σάντα Καταρίνα της Βραζιλίας.

Η κυβερνοεπίθεση στόχευε τον τομέα της τεχνολογίας πληροφοριών, λόγω της γνώσης που είχε ο χάκερ από το γεγονός ότι ήταν πρώην υπάλληλος του οργανισμού, δίνοντάς του το πλεονέκτημα να πείσει το σύστημα.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ;

Οι πληροφορίες που περιέχονται σε αυτή τη μελέτη περίπτωσης βασίζονται σε μια μελέτη περίπτωσης σχετικά με τους κινδύνους μιας επίθεσης στον κυβερνοχώρο υπό την καθοδήγηση ενός πρώην εργαζομένου. Η μελέτη περίπτωσης γίνεται από τη σκοπιά του οργανισμού που υπέστη την κυβερνοεπίθεση.

Ο γενικός στόχος αυτής της μελέτης περίπτωσης είναι να καταδείξει τη σημασία που πρέπει να δώσουν οι εταιρείες σε σχέση με την κοινωνική μηχανική στο περιβάλλον τους, προκειμένου να αποφύγουν τις εισβολές ή/και τις απάτες που προκαλούνται από την απερισκεψία ή την ακούσια συνδρομή των εργαζομένων ως παραβιάσεις για τη δουλειά του χάκερ.

ΠΡΟΛΗΨΗ

Για την αποτροπή πιθανών ζημιών, η εταιρεία διέθετε ήδη ένα τμήμα πληροφορικής που διαχειριζόταν τείχη προστασίας, εργαλεία διαρροής πληροφοριών και κρυπτογράφηση δεδομένων.

ΑΝΑΓΝΩΡΙΣΗ

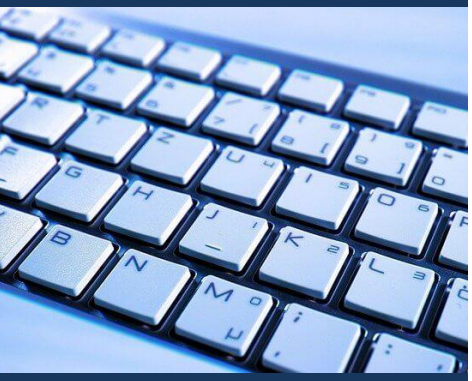
Σε αυτή τη μελέτη περίπτωσης, το αποτύπωμα ξεκίνησε με διάφορες επισκέψεις στην ιστοσελίδα της ένωσης, με σκοπό να κατανοήσει τη δυναμική τους, τις επιχειρήσεις τους και κυρίως τα εμπορικά τους σήματα (λαμβάνοντας υπόψη ότι ο επιτιθέμενος κατεύθυνε την αναζήτηση για δεδομένα που ο χάκερ δεν γνώριζε ακόμη). Οταν ξεκίνησε το αποτύπωμα και οι εσωτερικές και συγκεκριμένες πληροφορίες του οργανισμού ήταν στην πλευρά του επιτιθέμενου, προχώρησε με συνδέσεις σε ένα από τα καταστήματα της αλυσίδας για να ανακαλύψει τα ονόματα των διευθυντών και των ατόμων που θα μπορούσαν να έχουν προνομιακή πρόσβαση στον οργανισμό.

Για τον σκοπό αυτό, ο επιτιθέμενος εμφανίστηκε, μέσω τηλεφώνου, ως πελάτης που είχε νομικά προβλήματα με την εταιρεία. Για την επίλυση του προβλήματος αυτού, η εταιρεία θα καλούσε τον πελάτη και θα του ζητούσε να μιλήσει με τον διευθυντή του εν λόγω καταστήματος, δεδομένου ότι αυτός/αυτή θα ήταν το πρόσωπο με τη μεγαλύτερη αυτονομία να απαντήσει για μια τέτοια

κατάσταση. Λόγω αυτής της αλληλεπίδρασης, επιτεύχθηκε εύκολα, το όνομα του διευθυντή, η τοποθεσία όπου εργαζόταν και ο αριθμός τηλεφώνου.

Μετά από αυτό το τηλεφώνημα, έγιναν προσπάθειες να επικοινωνήσουμε με τον διευθυντή στα ενημερωμένα κανάλια για να ελέγξουμε τις πληροφορίες που συλλέχθηκαν. Η επαναφορά του κωδικού πρόσβασης έγινε κατά την επικοινωνία με τον τομέα της πληροφορικής, υποδυόμενος τον ίδιο τον υπάλληλο, προκειμένου ο εν λόγω τομέας να τον ενημερώσει για τα δεδομένα πρόσβασης του χρήστη.

Με λίγη πειθώ και το επιχείρημα ότι τα δεδομένα για τον πίνακα εξαρτώνται από αυτή την πρόσβαση, τελικά ο τεχνικός επανέφερε τον κωδικό πρόσβασης και ενημέρωσε τηλεφωνικά για τον νέο κωδικό πρόσβασης. Επιπλέον, ήταν δυνατό να τον πείσει να εγκαταστήσει πρόσβαση VPN (τεχνολογία για απομακρυσμένη πρόσβαση στο περιβάλλον της εταιρείας), ώστε ο υποθετικός χρήστης να μπορεί να εργαστεί εκτός γραφείου.



ΑΠΑΝΤΗΣΗ

ΠΟΙΟΣ: Ο επιτιθέμενος ήταν πρώην υπάλληλος,
ΣΕ ΠΟΙΟΝ: Ενας οργανισμός που ασχολείται με την εμπορική παρακολούθηση, στον κλάδο της αυτοκινητοβιομηχανίας,
ΓΙΑΤΙ: Η επίθεση είχε στόχο τον οργανισμό με άγνωστα κίνητρα,
ΤΙ: Η ιδιοκτησία που αποτέλεσε στόχο ήταν ο τομέας της πληροφορικής με σκοπό τη συλλογή εσωτερικών πληροφοριών του οργανισμού και προσωπικών δεδομένων των σημερινών εργαζομένων,

ΠΩΣ: Η επίθεση ξεκίνησε με την απόκτηση του ονόματος του διευθυντή ενός καταστήματος, προχώρησε σε επικοινωνία με τον τομέα πληροφορικής της εταιρείας και τους έπεισε να επαναφέρουν τον κωδικό πρόσβασης. Με αυτόν τον τρόπο ο πρώην εργαζόμενος προσποιήθηκε τον διευθυντή και είχε πρόσβαση σε όλα όσα αφορούν εσωτερικές πληροφορίες, προσωπικά δεδομένα εργαζομένων και πελατών και ό,τι άλλο θέλει ο χάκερ.

ΑΝΑΚΑΜΨΗ

Η εταιρεία άρχισε να εκπαιδεύει τους συνεργάτες να δίνουν προσοχή στους τύπους των πληροφοριών που συνήθως δίνουν σε τρίτους, ειδικά αν πρόκειται για κρίσιμες πληροφορίες. Ποτέ, σε καμία περίπτωση, ένας εργαζόμενος δεν θα πρέπει να δίνει κρίσιμες πληροφορίες, όπως κωδικούς πρόσβασης, μέσω τηλεφώνου. Αυτά πρέπει να δίνονται στους ενδιαφερόμενους με ασφαλείς μεθόδους, όπως συστημένες επιστολές ή μέσω του αρμόδιου διευθυντή.

Παρέχετε επίσης εκπαίδευση για να ευαισθητοποιήσετε τους υπαλλήλους ώστε να είναι προσεκτικοί με τις πληροφορίες που μοιράζονται στο

διαδίκτυο. Η εκπαίδευση επικεντρώθηκε στους κινδύνους που μπορούν να επιφέρουν οι πληροφορίες που μοιράζονται στο επάγγελμά τους αλλά και στην προσωπική τους ζωή, όπως απαγωγές, λεπτομέρειες ζωής και προσωπική ασφάλεια.

Η εταιρεία αυτή γνωρίζει ότι πρέπει να παρέχει τις τεχνικές και φυσικές συνθήκες για την εφαρμογή ορθών πρακτικών ασφαλείας, αλλά, κυρίως, να εκτιμά και να ενθαρρύνει την υιοθέτηση βέλτιστων πρακτικών και αυστηρότερων πρωτοκόλλων ασφαλείας από τους υπαλλήλους της, είτε σε εταιρικό είτε σε προσωπικό περιβάλλον, προκειμένου να ελέγχει, με τον καλύτερο δυνατό τρόπο, τον πιο αδύναμο παράγοντα της ασφάλειας των πληροφοριών: τον ανθρώπινο παράγοντα.

ΔΙΔΑΓΜΑΤΑ

Ο οργανισμός θα πρέπει να καθιερώσει τις πληροφορίες σε μια απλή διαδικασία μοτίβου που μπορεί να απογοητεύσει τον χάκερ. Αυτή η διαδικασία έχει 3 στάδια:

☑ **Δημόσιο:** Για παράδειγμα, σε εμπορικές επαφές και συγκεκριμένες εταιρείες, πληροφορίες μεταξύ πελατών και επιχειρήσεων της εταιρείας,

☑ **Ιδιωτικός:** Πληροφορίες που δεν μπορούν να δοθούν σε κανέναν και αφορούν μόνο το εταιρικό περιβάλλον. Στην κατηγορία αυτή υπάγονται πληροφορίες που αναφέρονται σε εσωτερικές διαδικασίες, εταιρικά δεδομένα διοικητικές και στρατηγικές πτυχές της εταιρείας,

☑ **Εμπιστευτικό:** Πληροφορίες και δεδομένα που δεν πρέπει να κοινοποιούνται εντός και εκτός της εταιρείας, όπως τα στοιχεία εγγραφής των εργαζομένων, οι αμοιβές, τα αποτελέσματα των τομέων και οι στρατηγικές ενέργειες που αφορούν μόνο τη διεύθυνση ή την προεδρία.

Επίσης, οι οργανισμοί θα πρέπει να διαθέτουν εσωτερικές διαδικασίες για την προστασία τους από επιθέσεις κοινωνικής μηχανικής. Οι χειριστές πρέπει να είναι καλά εκπαιδευμένοι σχετικά με τις διαδικασίες που πρέπει να ακολουθούν και τις ενέργειες στις οποίες πρέπει να προβαίνουν σε περιπτώσεις όπου η εταιρεία αισθάνεται ότι δέχεται επίθεση, όπως η μεταφορά της κλήσης σε ένα άτομο που έχει εκπαιδευτεί να χειρίζεται τέτοιου είδους καταστάσεις. Απλές ενέργειες μπορούν να προκαλέσουν την αποτυχία της επίθεσης. Αμέσως μπορεί να ειπωθεί ότι ένας αρχικός κατάλογος ελέγχου για την επιβεβαίωση των δεδομένων του αιτούντος θα καθιστούσε ήδη δύσκολη την πρόσβαση του χάκερ. Λαμβάνοντας υπόψη ότι τα προσωπικά δεδομένα δεν είναι κάτι πολύ δύσκολο να αποκτηθούν, οι τεχνικοί θα μπορούσαν να υιοθετήσουν μια διαδικασία επιστροφής της επικοινωνίας στον καταχωρημένο αριθμό τηλεφώνου του υπαλλήλου, προκειμένου να επιβεβαιώσουν ότι πρόκειται πράγματι για τον εν λόγω υπάλληλο.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 14: ΟΙ ΚΥΒΕΡΝΟΕΠΙΘΕΣΕΙΣ ΩΣ ΝΕΑ ΠΡΟΚΛΗΣΗ ΓΙΑ ΤΗΝ ΕΣΩΤΕΡΙΚΗ ΑΣΦΑΛΕΙΑ

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Πορτογαλικοί κυβερνητικοί φορείς (ιδίως το Υπουργείο Εσωτερικής Διοίκησης), οι Δυνάμεις Ασφαλείας και μεγάλες εταιρείες.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ;

Οι πληροφορίες για την παρούσα μελέτη περίπτωσης συλλέχθηκαν μέσω μιας έρευνας γραφείου που αναφέρεται σε μια μεταπτυχιακή διατριβή, όπου ο συγγραφέας εφαρμόζει μια μελέτη και αρκετές διερευνητικές συνεντεύξεις με ειδικούς και υπεύθυνους των εθνικών δυνάμεων ασφαλείας, προκειμένου να συμπεράνει αν το φαινόμενο των χακτιβιστών αποτελεί απειλή για τις πορτογαλικές δυνάμεις ασφαλείας.

ΠΡΟΛΗΨΗ

Για την πρόληψη επιθέσεων, ένα από τα μέτρα που λαμβάνει η ομάδα πληροφορικής που είναι υπεύθυνη για την ασφάλεια στον κυβερνοχώρο σε αυτούς τους οργανισμούς είναι η παρακολούθηση των κοινωνικών καναλιών, για παράδειγμα: (Internet Relay Chat), όλα τα είδη των συνομιλιών, το Facebook, τα πάντα από τα οποία είναι δυνατόν να ληφθούν πληροφορίες στο διαδίκτυο, κάνουν επίσης μια παρακολούθηση και προσπαθούν να δουν αν υπάρχουν ύποπτες ενέργειες.

Σύμφωνα με το "modus operandi", που ορίζεται από τους όρους της ομάδας Anonymous (Πορτογαλία), αρχικά διαφημίζουν στα κοινωνικά δίκτυα (IRC και Facebook) τις ενέργειες που θα κάνουν και τότε είναι που αρχίζουν να επικοινωνούν μεταξύ τους. Στη συνέχεια χρησιμοποιούν ιδιωτικά κανάλια συνομιλίας για να επικοινωνούν μεταξύ τους, γεγονός που οδήγησε στην υλοποίηση του SOC (Κέντρο Επιχειρήσεων Ασφαλείας) του MIA (Υπουργείο Εσωτερικής Διοίκησης), για την προετοιμασία αυτού του είδους των επιθέσεων.

ΑΝΑΓΝΩΡΙΣΗ

Οι συνέπειες αυτών των επιθέσεων ποικίλλουν, ανάλογα με τον τύπο της επίθεσης. Πολλές αφορούσαν μια επίθεση άρνησης παροχής υπηρεσιών, (DOS, DDOS), η οποία προκαλεί εξάντληση των πόρων όσον αφορά

τα συστήματα ή τις επικοινωνίες. Επίσης, ασχολήθηκαν με ορισμένους τύπους απόπειρας επιθέσεων εισβολής, όπως SQL Injection και defacements. Η αλιεία μέσω ηλεκτρονικού ταχυδρομείου, είναι επίσης μια από τις πιο συχνές επιθέσεις, που οδηγεί μερικές φορές σε πρόσβαση σε ιδιωτικές πληροφορίες.

Τον Νοέμβριο του 2011, πραγματοποιήθηκε επίθεση στον δικτυακό τόπο της εθνικής ένωσης για τη σταδιοδρομία των αρχηγών της PSP, με την αποκάλυψη προσωπικών και εμπιστευτικών δεδομένων (πατέντες, αριθμοί τηλεφώνου και διευθύνσεις ηλεκτρονικού ταχυδρομείου) 107 στελεχών της PSP.

"Οι επιθέσεις DDoS αυξάνονται σταθερά σε συχνότητα τα τελευταία χρόνια. Σύμφωνα με έκθεση της Cloudflare, οι επιθέσεις DDoS με λύτρα αυξήθηκαν κατά σχεδόν ένα τρίτο μεταξύ 2020 και 2021 και αυξήθηκαν κατά 75% το τέταρτο τρίμηνο του 2021 σε σύγκριση με τους τρεις προηγούμενους μήνες.". (Cook, 2022)

ΑΠΑΝΤΗΣΗ

Μια επίθεση κατά της Αστυνομίας Δημόσιας Ασφάλειας ανέλαβε η ομάδα LulzSec Portugal. Η πορτογαλική ομάδα των Anonymous έχει αναλάβει αρκετές επιθέσεις σε κυβερνητικούς ιστότοπους και σχετικούς φορείς. Σε γενικές γραμμές, το προφίλ του χάκερ είναι κάποιου νέου, σχολικής ηλικίας, στη δευτεροβάθμια εκπαίδευση (10th έως 12th τάξη). Μπορεί να υπάρχει η μία ή η άλλη περίπτωση κατά την οποία είναι ήδη πιο ενήλικα άτομα ίσως με λιγότερες γνώσεις στον τεχνολογικό τομέα αλλά δυσαρεστημένα με την κοινωνία.

Αυτό το είδος επίθεσης είναι διαθέσιμο σε κάθε πολίτη. Αρκεί να ψάξει κάποιος στο διαδίκτυο για εργαλεία, μεθόδους και ομάδες και να αρχίσει να συμμετέχει. Αυτές οι ομάδες των Anonymous, την εποχή των επιθέσεων, πραγματοποιούσαν εργαστήρια για το πώς να κάνουν μια επίθεση, μαθήματα "abc" για το πώς να κατανοήσουν την επίθεση. Παρέχουν εργαλεία που έχουν ήδη αναπτυχθεί και ότι ο καθένας μπορεί να έχει πρόσβαση στον ιστότοπο, είναι απαραίτητο μόνο να εισαχθεί η διεύθυνση προορισμού και μια εφαρμογή αναπτύσσει την επίθεση.

Οι περισσότεροι από τους επιτιθέμενους, δηλαδή οι νέοι που φοιτούν ακόμη στο σχολείο, χρησιμοποιούν εργαλεία που χρησιμοποιούνται από πολλούς ειδικούς, οι οποίοι είναι άτομα με πιο προχωρημένο ακαδημαϊκό πτυχίο, αλλά και μεγαλύτεροι σε ηλικία, που χρησιμοποιούν εργαλεία που έχουν ήδη αναπτυχθεί για τους σκοπούς των κυβερνοεπιθέσεων. Δηλαδή, στο διαδίκτυο, είναι δυνατόν να αναζητήσει και να αποκτήσει πληροφορίες για την πραγματοποίηση της επίθεσης, πώς να το κάνει και τι είδους εργαλεία χρησιμοποιούνται για να βοηθήσουν στην πραγματοποίηση της επίθεσης.

Η επίθεση που πραγματοποίησε η LulzSec Portugal δικαιολογήθηκε στο Twitter υποστηρίζοντας ότι ως απάντηση στη δράση των προβοκατόρων διείσδυσαν σε μια διαδήλωση που διοργάνωσαν οι ίδιοι.

Αλλά τις περισσότερες φορές αυτές οι επιθέσεις συμβαίνουν επειδή αυτοί οι άνθρωποι αναζητούν την προβολή ή θέτουν σε κίνδυνο τις οργανώσεις, καθώς αυτό έχει συχνά να κάνει με τη δυσαρέσκεια των ανθρώπων όσον αφορά το σημερινό πλαίσιο στο οποίο ζουν οι Πορτογάλοι πολίτες, και οι άνθρωποι συχνά εκδηλώνουν τη δυσαρέσκειά τους με αυτόν τον τρόπο. Αλλες φορές είναι απλώς ένα αστείο για τους επιτιθέμενους, ηλικίας 16 ή 17 ετών, οι οποίοι δεν έχουν πολλές ανησυχίες από κοινωνική άποψη, είναι συχνά επειδή το κάνουν οι φίλοι και για να προωθήσουν τον εαυτό τους μέσα στην ομάδα των φίλων, άλλες φορές αυτές είναι εμπειρίες που κάνουν επειδή είναι η ηλικία που πειραματίζονται με νέα πράγματα. Τις περισσότερες φορές δεν συνειδητοποιούν τον αντίκτυπο που μπορεί να έχουν αυτές οι επιθέσεις.

Ολα ξεκινούν από μια ομάδα χάκερς που έχουν τις τεχνικές γνώσεις και αναπτύσσουν εργαλεία που μπορούν να χρησιμοποιηθούν από ομάδες ανθρώπων που δεν έχουν τις ίδιες γνώσεις, γεγονός που καθιστά τη διαδικασία της πειρατείας εύκολη για τον καθένα.

Χαρακτηριστικό των πορτογαλικών ομάδων είναι να επιτίθενται σε απροστάτευτους ιστότοπους και να εκμεταλλεύονται ευπάθειες. Σχεδιάζουν επιθέσεις σε IRC's (Internet Relay Chat) και chatrooms, δεν αναλαμβάνουν την ταυτότητά σας και χρησιμοποιούν ψευδώνυμα. Οι Πορτογάλοι χακτιβιστές χρησιμοποιούν τα εργαλεία που είναι διαθέσιμα στο διαδίκτυο για να πραγματοποιήσουν τις επιθέσεις, δηλαδή "δεν κατασκευάζουν προσαρμοσμένα προγράμματα, αλλά χρησιμοποιούν αυτά που είναι διαθέσιμα στο δίκτυο". Οσον αφορά τα άτομα που αναλαμβάνουν την οργάνωση και την ηγεσία αυτού του είδους των πρωτοβουλιών, είναι συχνά άτομα με μικρή τεχνική εξειδίκευση, που αφιερώνουν τον εαυτό τους στην πραγματοποίηση ανακοινώσεων και τη διάδοση των δράσεων που θα αναπτυχθούν, και συχνά "εκείνοι που έχουν ακόμη και πολύ εξειδικευμένες τεχνικές δεξιότητες, δεν έχουν ιδέα ότι είναι οι πιο ικανοί και εξειδικευμένοι στην ομάδα, νομίζουν ότι είναι άνθρωποι που γνωρίζουν λίγα και ότι απλώς βοηθούν άλλους που γνωρίζουν περισσότερα".

Η ομάδα Anonymous χρησιμοποιεί συμβατικές μεθόδους hacking, όπως το Havij114 και το SQL Injection, ενώ η κύρια καινοτομία της είναι η δημιουργία ιστοσελίδων που πραγματοποιούν επιθέσεις DoS.

ΑΝΑΚΑΜΨΗ

Οι πιθανές συνέπειες είναι η κλοπή πληροφοριών, η μη διαθεσιμότητα των υπηρεσιών και οι αλλοιώσεις του ιστότοπου όπου γίνονται αλλαγές στις πληροφορίες, καθώς οι χάκερς μερικές φορές αφαιρούν πληροφορίες, αλλά μπορούν επίσης να τις προσθέσουν.

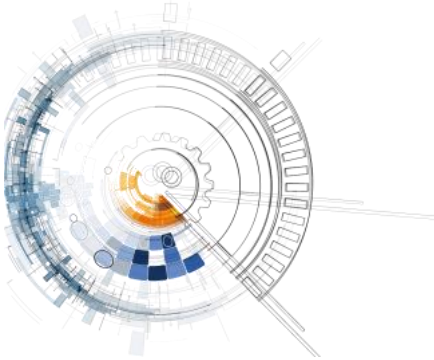
Οι επιθέσεις αυτές μπορεί να θέσουν σε κίνδυνο την εμπιστοσύνη των πολιτών στους θεσμούς που είναι θύματα αυτών των ομάδων, αλλά και ο εντοπισμός των τρωτών σημείων και η επιρροή άλλων ανθρώπων με συγκεκριμένα ιδανικά είναι καταστάσεις που μπορεί να συμβούν.

Αυτοί οι τύποι επιθέσεων εξελίσσονται και οι τεχνικές βελτιώνονται με την πάροδο του χρόνου και οι οργανισμοί πρέπει να προσαρμόζονται και να εξελίσσονται για την προστασία του δικτύου τους. Αναγκάστηκαν να σταματήσουν την πρόσβαση στο δίκτυο μέχρι να εκπληρωθούν οι προϋποθέσεις

για να διασφαλιστεί η διατήρηση της ασφάλειας των εσωτερικών πληροφοριών. Και αυτό το έκαναν ήδη, συνολικά, για μία ώρα το πολύ. Περιστασιακά, ορισμένες υπηρεσίες ήταν επίσης μη προσβάσιμες κατά τη διάρκεια της νύχτας.

Αναπτύσσεται το CNCseg (Εθνικό Κέντρο Κυβερνοασφάλειας), το οποίο θα έχει περισσότερη σχέση με το θέμα της εθνικής άμυνας, από ό,τι υπάρχει το Κέντρο Κυβερνοάμυνας, το οποίο είναι στην αρμοδιότητα του Υπουργείου Εθνικής Αμυνας, του οποίου η κύρια δράση είναι η επίθεση σε χάκερς που μπορεί να αναπτύσσουν επιθέσεις, κάνοντας τον εντοπισμό και την αντεπίθεση αυτών των στοιχείων.

Το MIA θα συμμετέχει, τουλάχιστον στο CNCseg, συνεργάζεται με το GNS, το οποίο είναι ο φορέας που έχει αυτή την αρμοδιότητα και θα είναι μία από τις εισροές πληροφοριών για αυτό το είδος της κυβερνοασφάλειας. Η ιδέα είναι αυτό το κέντρο να έχει τις πληροφορίες για το τι συμβαίνει σε εθνικό επίπεδο, ο στόχος είναι να συλλέξει πληροφορίες τόσο από τα τεχνολογικά κέντρα της δημόσιας διοίκησης, τις τράπεζες, τη βιομηχανία, τους διάφορους τομείς της πορτογαλικής κοινωνίας και, με αυτό, να έχει μια ιδέα για τον αντίκτυπο και την έκταση που μπορεί να έχει ένας συγκεκριμένος τύπος επίθεσης.



ΔΙΔΑΓΜΑΤΑ

Ο χακτιβισμός θεωρείται ως μια νέα πρόκληση για τους θεσμούς και, ειδικά στην περίπτωση των Σωμάτων Ασφαλείας, μια επίθεση χακτιβισμού μπορεί να προκαλέσει επιζήμιες συνέπειες, οι οποίες μπορούν ακόμη και να επηρεάσουν την εκτέλεση των αποστολών τους, θεωρώντας την ως πραγματική απειλή, υπό την έννοια ότι αυτή χαρακτηρίζεται από αντίθεση με τους στόχους του οργανισμού, προκαλώντας, κατά κανόνα, υλικές ή/και ηθικές ζημίες.

Η ικανότητα των ομάδων χακτιβιστών να πραγματοποιήσουν μια επίθεση είναι συνήθως χαμηλή, καθώς χρησιμοποιούν εργαλεία που είναι διαθέσιμα στο δίκτυο και δεν είναι ιδιαίτερα καινοτόμες όσον αφορά την πειρατεία, εκμεταλλευόμενες την εκμετάλλευση των υφιστάμενων τρωτών σημείων. Οσον αφορά την ευκαιρία, οποιοσδήποτε από έναν υπολογιστή με πρόσβαση στο δίκτυο και με κάποια γνώση ή διάθεση να μάθει από τις πληροφορίες που είναι διαθέσιμες στο δίκτυο είναι σε θέση να αναπτύξει μια κυβερνοεπίθεση, και το γεγονός αυτό γίνεται ανησυχητικό για τις δυνάμεις ασφαλείας.

Οσον αφορά την ασφάλεια των υπολογιστών, συχνά λέγεται ότι δεν υπάρχει απόλυτη ασφάλεια και δεν υπάρχουν 100% ασφαλή συστήματα , οπότε η κυβέρνηση και η Πορτογαλία δεν αποτελούν εξαίρεση. Αυτό που έχει παρατηρηθεί είναι η δημιουργία ενός συνόλου υποδομών που επιτρέπουν μια δομή ασφάλειας που μπορεί να ανταποκριθεί σε αυτού του είδους τα φαινόμενα: το πρόσφατα δημιουργηθέν CNCseg, που δημιουργήθηκε από την

"Το Ransomware θα κοστίσει στα θύματα πάνω από 265 δισεκατομμύρια δολάρια ετησίως μέχρι το 2031". (Cybersecurity Ventures)

PJ για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Η εκπαίδευση των ανθρώπων είναι σίγουρα κάτι που θα προκαλέσει όλους να συνειδητοποιήσουμε ότι χρησιμοποιούμε επίσης νέες τεχνολογίες, διαδικτυακές πλατφόρμες και άλλα δίκτυα που έχουν τη δύναμη να αλλάξουν την ασφάλεια των πολιτών.

Συνέπειες μιας χακτιβιστικής επίθεσης στις εθνικές δυνάμεις ασφαλείας: Ο χακτιβισμός θεωρείται ως μια νέα πρόκληση για τους θεσμούς και, ειδικά στην περίπτωση των Σωμάτων Ασφαλείας, μια επίθεση χακτιβισμού μπορεί να προκαλέσει επιζήμιες συνέπειες, οι οποίες μπορούν ακόμη και να επηρεάσουν την εκτέλεση των αποστολών τους, θεωρώντας την ως πραγματική απειλή, υπό την έννοια ότι αυτή χαρακτηρίζεται από αντίθεση με τους στόχους του οργανισμού, προκαλώντας, κατά κανόνα, υλικές ή/και ηθικές ζημίες.

Η ικανότητα των ομάδων χακτιβιστών να πραγματοποιήσουν μια επίθεση είναι συνήθως χαμηλή, καθώς χρησιμοποιούν εργαλεία που είναι διαθέσιμα στο δίκτυο και δεν είναι ιδιαίτερα καινοτόμες όσον αφορά την πειρατεία, εκμεταλλευόμενες την εκμετάλλευση των υφιστάμενων τρωτών σημείων. Οσον αφορά την ευκαιρία, οποιοσδήποτε από έναν υπολογιστή με πρόσβαση στο δίκτυο και με κάποια γνώση ή διάθεση να μάθει από τις πληροφορίες που είναι διαθέσιμες στο δίκτυο είναι σε θέση να αναπτύξει μια κυβερνοεπίθεση, και το γεγονός αυτό γίνεται ανησυχητικό για τις δυνάμεις ασφαλείας.

Οσον αφορά την ασφάλεια των υπολογιστών, συχνά λέγεται ότι δεν υπάρχει απόλυτη ασφάλεια και δεν υπάρχουν 100% ασφαλή συστήματα , οπότε η κυβέρνηση και η Πορτογαλία δεν αποτελούν εξαίρεση. Αυτό που έχει παρατηρηθεί είναι η δημιουργία ενός συνόλου υποδομών που επιτρέπουν μια δομή ασφάλειας που μπορεί να ανταποκριθεί σε αυτού του είδους τα φαινόμενα: το πρόσφατα δημιουργηθέν CNCseg, που δημιουργήθηκε από την PJ για την καταπολέμηση του εγκλήματος στον κυβερνοχώρο. Η εκπαίδευση των ανθρώπων είναι σίγουρα κάτι που θα προκαλέσει όλους να συνειδητοποιήσουμε ότι χρησιμοποιούμε επίσης νέες τεχνολογίες, διαδικτυακές πλατφόρμες και άλλα δίκτυα που έχουν τη δύναμη να αλλάξουν την ασφάλεια των πολιτών.

Συνέπειες μιας χακτιβιστικής επίθεσης στις εθνικές δυνάμεις ασφαλείας: Direct: economic, social, political, and security consequences.

- ☑ Αμεσες: οικονομικές, κοινωνικές, πολιτικές συνέπειες και συνέπειες στον τομέα της ασφάλειας.
- ☑ Εμμεσα: το αίσθημα ασφάλειας, η κοινωνική απορρύθμιση και, τελικά, η κυριαρχία της χώρας, των θεσμών και των οικογενειών.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 15: Η "ΧΡΥΣΗ ΕΠΟΧΗ" ΤΟΥ "RANSOMWARE". ΠΩΣ ΝΑ ΑΠΟΤΡΕΨΕΤΕ ΚΑΙ ΝΑ ΑΝΤΙΜΕΤΩΠΙΣΕΤΕ ΜΙΑ ΠΕΙΡΑΤΕΙΑ ΔΕΔΟΜΕΝΩΝ

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Οι περισσότερες πορτογαλικές εταιρείες βρίσκονται στη "γενιά 3" της κυβερνοασφάλειας και οι επιθέσεις στη "γενιά 6". Σε αυτή τη μελέτη περίπτωσης μαθαίνουμε πώς να προχωρήσουμε για να αποτρέψουμε επιθέσεις ransomware όπως αυτή που αντιμετώπισε ο όμιλος IMPRESA, όλο και πιο συχνά.

Η IMPRESA είναι ο μεγαλύτερος πορτογαλικός όμιλος μέσων ενημέρωσης, ο οποίος δραστηριοποιείται σε τρεις επιχειρηματικούς τομείς - τον έντυπο, τον ψηφιακό και τον τηλεοπτικό.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Οι πληροφορίες για την παρούσα μελέτη περίπτωσης αποκτήθηκαν μέσω ενός ειδησεογραφικού άρθρου σχετικά με την πρόληψη των ransomwares, το οποίο περιλαμβάνει τη συνέντευξη του Rui Duro, ειδικού σε θέματα κυβερνοασφάλειας.

ΠΡΟΛΗΨΗ

Η εποχή της πανδημίας διευκόλυνε την ανάπτυξη αυτού του τύπου επιθέσεων ransomware. Από τη μία πλευρά, η εργασία στο σπίτι, η οποία οδηγεί στη διασπορά των συστημάτων και αυξάνει τον κίνδυνο. Από την άλλη πλευρά, όλο και περισσότερες εφαρμογές μεταφέρουν τα συστήματα στο "cloud".

"Αυτό έχει αρκετούς συναφείς κινδύνους", λέει ο Rui Duro. Τα συστήματα βρίσκονται τώρα "σε άλλον πάροχο υπηρεσιών" και είναι απαραίτητο "να αγοράσουμε τεχνολογία και για το cloud, επειδή δεν είναι ασφαλές από μόνο του". Για τον ειδικό, "αυτή η εξέλιξη προς το "cloud" ήταν συχνά ταχύτερη από την εξέλιξη των γνώσεων των υπαλλήλων της πληροφορικής".

Από την άλλη πλευρά, πολλές εταιρείες έχουν ξεπεραστεί από την πολυπλοκότητα των επιθέσεων. "Εμείς (ο όμιλος IMPRESA) βρισκόμαστε στη γενιά 6 των επιθέσεων και οι περισσότερες εταιρείες βρίσκονται ακόμη στη γενιά 3, σε πολύ πρώιμο στάδιο προστασίας, δεδομένης της εξέλιξης των επιθέσεων. Η νοοτροπία πρέπει να αλλάξει, πρέπει να υπάρχει προϋπολογισμός και πόροι για την προσαρμογή σε αυτή τη νέα πραγματικότητα", εξηγεί ο Rui Duro.

ΑΝΑΓΝΩΡΙΣΗ

Στις σελίδες των ιστότοπων του ομίλου εμφανίζεται ένα μήνυμα παρόμοιο με αυτό που έλαβε το SIC (πορτογαλικό τηλεοπτικό κανάλι): "Τα εσωτερικά δεδομένα των συστημάτων αντιγράφηκαν και διαγράφηκαν. 50 TB δεδομένων βρίσκονται στα χέρια μας. Επικοινωνήστε μαζί μας αν θέλετε τα δεδομένα πίσω".

Ο Rui Duro εξηγεί ότι "συνήθως το ransomware εμφανίζεται σε εταιρείες μέσω αυτού που ονομάζουμε τοποθέτηση ενός αρχικού "payload" εντός της εταιρείας".

Αυτό συμβαίνει με διάφορους τρόπους, όπως μέσω μιας επίθεσης phishing σε ένα στοιχείο της εταιρείας. Αλλες φορές, κάποιος στην εταιρεία "κατεβάζει" κατά λάθος το κακόβουλο λογισμικό. Υπάρχει ακόμη ένας τρίτος τρόπος, όταν οι δράστες έχουν σκοπό να επιτεθούν σε μια συγκεκριμένη εταιρεία και αναζητούν ευπάθειες - πρόκειται για "επίθεση-στόχο".

Αφού το αρχικό κακόβουλο λογισμικό εισέλθει στην εταιρεία, κατεβάζει ένα δεύτερο κακόβουλο λογισμικό, το οποίο εκτελεί το ransomware. Στη συνέχεια αρχίζει να κάνει "σάρωση", αναζητώντας διακομιστές και άλλα συστήματα. Στόχος είναι να αποκομίσει όσο το δυνατόν μεγαλύτερο κέρδος - σύμφωνα με τον εμπειρογνώμονα, για τους εγκληματίες "δεν έχει νόημα να κρυπτογραφήσουν έναν ή δύο υπολογιστές, η ιδέα είναι να κρυπτογραφήσουν όσο το δυνατόν περισσότερους υπολογιστές και κατά προτίμηση τους ζωτικούς".

Στη συνέχεια, οι χάκερ εγκαθιστούν το κακόβουλο λογισμικό σε όσο το δυνατόν περισσότερα συστήματα, αλλά δεν κρυπτογραφεί τα δεδομένα αμέσως. Συνήθως, "αφήνεται για αρκετές εβδομάδες, μερικές φορές και περισσότερο".

Αυτοί που επιτίθενται γνωρίζουν ότι ένας από τους τρόπους με τους οποίους οι εταιρείες ανακάμπτουν είναι μέσω αντιγράφων ασφαλείας - έτσι περιμένουν να υπάρχει ένα αντίγραφο ασφαλείας και μόλις αυτό αποκατασταθεί, υπάρχει και πάλι μόλυνση.

Οταν πραγματοποιείται κρυπτογράφηση, οι εγκληματίες ασκούν πίεση στις εταιρείες, συνήθως για να ζητήσουν λύτρα σε μετρητά - συνήθως σε κρυπτονομίσματα.

ΑΠΑΝΤΗΣΗ

Δύο ημέρες μετά την επίθεση της ομάδας χάκερ "Lapsus$ Group" στους ιστότοπους του ομίλου Impresa, οι ιστότοποι εξακολουθούσαν να μην είναι διαθέσιμοι.

Η Πορτογαλική Δικαστική Αστυνομία επιβεβαίωσε ότι διερευνά την υπόθεση, μαζί με το Εθνικό Κέντρο Κυβερνοασφάλειας (CNCS), όπως είχε ήδη προχωρήσει ο όμιλος μέσων ενημέρωσης.

Αυτή η καθυστέρηση στην επαναφορά των συστημάτων είναι συνηθισμένο φαινόμενο σε επιθέσεις όπως αυτή. Σύμφωνα με τον Rui Duro, υπεύθυνο της Check Point Software στην Πορτογαλία, "ο χρόνος που απαιτείται για την αντιμετώπιση αυτών των επιθέσεων ποικίλλει σε μεγάλο βαθμό. Εξαρτάται σε μεγάλο βαθμό από το μέγεθος της εταιρείας, την επίθεση, την ικανότητα της εταιρείας όσον αφορά τις τεχνολογίες πληροφοριών (ΤΠ) και το πόσο προετοιμασμένη ήταν η εταιρεία για την αντικατάσταση των συστημάτων. Σε μια μικρή εταιρεία, μερικές φορές χρειάζεται μια ή δύο ημέρες, αν πρόκειται για μια μεγάλη εταιρεία, μπορεί να χρειαστούν ακόμη και αρκετές εβδομάδες και μερικές φορές μπορεί να χρειαστεί να ξανακάνει μια ολόκληρη υποδομή".

Η επίθεση ransomware έχει ήδη γίνει μια πραγματική και άμεση απειλή για τις εταιρείες σε όλο τον κόσμο - και η Πορτογαλία δεν αποτελεί εξαίρεση. Για τον Ευρωπαϊκό Οργανισμό Κυβερνοασφάλειας (ENISA), η πανδημία έφερε μαζί της μια "χρυσή εποχή" για τους εγκληματίες του κυβερνοχώρου.

Σύμφωνα με τον οργανισμό, μεταξύ Απριλίου 2020 και Ιουλίου 2021, οι καταγεγραμμένες επιθέσεις αυξήθηκαν κατά 150%.

Στην Πορτογαλία, δεν υπάρχουν ακόμη επίσημα στοιχεία για το περασμένο έτος, αλλά στην ετήσια έκθεση εσωτερικής ασφάλειας, για το 2020, το ransomware έχει ήδη αναγνωριστεί ως "η πιο κοινή μορφή δολιοφθοράς σε υπολογιστές, που διατηρεί υψηλά ποσοστά κρουσμάτων και επηρεάζει ιδιαίτερα τα κυβερνητικά ιδρύματα και τις μικρές και μεσαίες επιχειρήσεις".

Σύμφωνα με την εν λόγω έκθεση, οι επιθέσεις στον κυβερνοχώρο διπλασιάστηκαν στην Πορτογαλία από το 2019 (754 περιστατικά) έως το 2020 (1418 περιστατικά). Στον τομέα της ασφάλειας πληροφοριών, όπου κυριαρχούν οι επιθέσεις ransomware, το 2020 σημειώθηκαν περίπου 10 φορές περισσότερα περιστατικά από ό,τι το 2019. Ο Rui Duro, επικεφαλής της Check Point Software στην Πορτογαλία, εξηγεί ότι "το 90 έως 95% των περιπτώσεων δεν αναφέρονται ούτε είναι γνωστές. Οι εταιρείες καταλήγουν να ανακάμπτουν μέσω αντιγράφων ασφαλείας και δεν αναφέρουν τις επιθέσεις".

Σύμφωνα με στοιχεία μελέτης που δημοσίευσε η εταιρεία της οποίας ηγείται, η οποία δημιουργεί τεχνολογικές λύσεις ασφαλείας για τις μεγαλύτερες εταιρείες του κόσμου, οι πορτογαλικοί οργανισμοί δέχονται κατά μέσο όρο 947 επιθέσεις κακόβουλου λογισμικού την εβδομάδα, αριθμός υψηλότερος από τον παγκόσμιο μέσο όρο των 870 επιθέσεων. Περίπου το 90% των κακόβουλων αρχείων φθάνουν μέσω ηλεκτρονικού ταχυδρομείου.

Τα στοιχεία της Check Point Software δείχνουν επίσης ότι τον Δεκέμβριο του 2021, οι επιθέσεις ransomware έφτασαν σε πάνω από το 2,5% των πορτογαλικών εταιρειών.

ΑΝΑΚΑΜΨΗ

Το ransomware είναι μια μορφή κακόβουλου λογισμικού (συνδυασμός των αγγλικών λέξεων "malicious" (κακόβουλο) και "software" (λογισμικό)) που έχει σχεδιαστεί για την κρυπτογράφηση διακομιστών και χώρων αποθήκευσης υπολογιστών.

Συνήθως, οι "χάκερς" πίσω από την επίθεση εμφανίζουν μηνύματα που απαιτούν την καταβολή ενός ποσού για να αποκρυπτογραφήσουν το σύστημα και να το επιστρέψουν στον ιδιοκτήτη. Σύμφωνα με τον εμπειρογνώμονα κυβερνοασφάλειας, οι επιθέσεις ransomware είναι όλο και πιο εξελιγμένες και όλο και συχνότερα παρατηρείται ότι οι πειρατές προσπαθούν να "διπλασιάσουν ή να τριπλασιάσουν τον εκβιασμό".

Στον διπλό εκβιασμό, "κατά τη διάρκεια της περιόδου που το κακόβουλο λογισμικό περιμένει για δημιουργία αντιγράφων ασφαλείας, αντιγράφει σημαντικά δεδομένα από βάσεις δεδομένων, διακομιστές ηλεκτρονικού ταχυδρομείου, οικονομικούς διακομιστές, προσπαθεί να αναζητήσει ευαίσθητα δεδομένα και εξάγει τεράστιες ποσότητες δεδομένων. Και λένε ότι δεν αξίζει τον κόπο να προσπαθήσουν να ανακτήσουν την υπηρεσία με αντίγραφα ασφαλείας, επειδή έχουν τα δεδομένα σε ομηρία".

Στην περίπτωση του τριπλού εκβιασμού, με τα ευαίσθητα δεδομένα στην κατοχή τους, οι πειρατές απειλούν να βάλουν στο στόχαστρο τους πελάτες και τους προμηθευτές της εταιρείας, εάν η εταιρεία δεν καταβάλει τα λύτρα.

ΔΙΔΑΓΜΑΤΑ

Για να αποτρέψετε μια επίθεση είναι απαραίτητο να αλλάξετε νοοτροπία και να υποθέσετε ότι θα συμβεί. Για τον εμπειρογνώμονα κυβερνοασφάλειας, αυτό είναι το πιο σημαντικό πράγμα. "Εχω περισσότερα από 30 χρόνια στην αγορά που εργάζομαι σε αυτόν τον τομέα, ξεκίνησα όταν οι επιθέσεις ήταν αστείο, σε σύγκριση με αυτό που είναι σήμερα, αλλά ακόμη και σήμερα βλέπω τους υπε ύθυνους λήψης αποφάσεων να σκέφτονται ότι δεν είναι ακόμη ανησυχητικό, δεν είναι σχετικό και ότι πιστεύουν ότι δεν θα τους συμβεί. Το πρώτο βήμα είναι να αλλάξουμε αυτή τη νοοτροπία. Μπορεί να συμβεί σε όλους, μόλις πριν από λίγο καιρό συνέβη στην EDP. Οταν συμβεί, πρέπει να είμαι προετοιμασμένος γι' αυτό".

Πάρτε στα σοβαρά τους τρεις πυλώνες της ασφάλειας στον κυβερνοχώρο: άνθρωποι, διαδικασίες και τεχνολογία.

Για να αποτρέψετε μια επίθεση είναι απαραίτητο να αλλάξετε νοοτροπία και να υποθέσετε ότι θα συμβεί. Για τον εμπειρογνώμονα κυβερνοασφάλειας, αυτό είναι το πιο σημαντικό πράγμα. "Εχω περισσότερα από 30 χρόνια στην αγορά που εργάζομαι σε αυτόν τον τομέα, ξεκίνησα όταν οι επιθέσεις ήταν αστείο, σε σύγκριση με αυτό που είναι σήμερα, αλλά ακόμη και σήμερα βλέπω τους υπεύθυνους λήψης αποφάσεων να σκέφτονται ότι δεν είναι ακόμη ανησυχητικό, δεν είναι σχετικό και ότι πιστεύουν ότι δεν θα τους συμβεί. Το πρώτο βήμα είναι να αλλάξουμε αυτή τη νοοτροπία. Μπορεί να συμβεί σε όλους, μόλις πριν από λίγο καιρό συνέβη στην EDP. Οταν συμβεί, πρέπει να είμαι προετοιμασμένος γι' αυτό".

Πάρτε στα σοβαρά τους τρεις πυλώνες της ασφάλειας στον κυβερνοχώρο: άνθρωποι, διαδικασίες και τεχνολογία.

α) Ανθρωποι

"Συχνά, ακόμη και οι εταιρείες που λαμβάνουν σοβαρά υπόψη τους την ασφάλεια στον κυβερνοχώρο εστιάζουν υπερβολικά στην τεχνολογία ως τρόπο προστασίας και ξεχνούν ότι είναι απαραίτητο να εκπαιδεύσουν τους ανθρώπους να συμπεριφέρονται με ασφάλεια", λέει ο ειδικός.

β) Διαδικασίες

"Είναι σημαντικό να υπάρχει μια διαδικασία για την ανάκαμψη από την καταστροφή, για τη διαχείριση και την εξειδίκευση των πληροφοριών, για μια αποτελεσματική διαδικασία δημιουργίας αντιγράφων ασφαλείας, για την ύπαρξη αποθετηρίων πληροφοριών. Πολλές εταιρείες δεν είναι προετοιμασμένες και τις πρώτες ώρες επικρατεί το απόλυτο χάος, επειδή δεν είχαν φροντίσει να προετοιμάσουν τη διαδικασία ανάκαμψης", αποκαλύπτει.

γ) Τεχνολογία

"Χρησιμοποιώντας τεχνολογία κατάλληλη για την πραγματικότητα που έχουμε σήμερα. Πολλές εταιρείες αγοράζουν τεχνολογία και είναι αυτό που ονομάζω αγορά μιας "ψευδούς αίσθησης ασφάλειας" - αγοράζουν τεχνολογία, αλλά δεν είναι πλέον κατάλληλη για την πραγματικότητα που έχουμε σήμερα. το παραδοσιακό τείχος προστασίας, αντί να αγοράσουν ένα προηγμένο τελικό

σημείο που αποφεύγει την κρυπτογράφηση των συστημάτων, χρησιμοποιείται ένα απλό τελικό σημείο, το οποίο ανιχνεύει κάποιο κακόβουλο λογισμικό, αλλά δεν εμποδίζει αυτές τις κρυπτογραφήσεις".

Ο ειδικός υπενθυμίζει ότι, σε αυτές τις περιπτώσεις, "ο πανικός δεν βοηθάει καθόλου". Σε αυτές τις περιπτώσεις, είναι απαραίτητο να ενημερώνετε τις αρχές και να μην πληρώνετε ποτέ τα λύτρα, καθώς αυτό ισοδυναμεί με διαιώνιση του εγκλήματος, λέγοντας στους εγκληματίες ότι αξίζει τον κόπο. Μία από τις διαδικασίες που πρέπει να έχουν εκ των προτέρων οι εταιρείες, για τον ειδικό, είναι ο τρόπος ανάκαμψης από μια τέτοια επίθεση, ώστε να υπάρχει αυτή η ηρεμία και να γνωρίζουν όλοι το ρόλο τους σε αυτή τη διαδικασία.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 16: ΚΑΚΟΒΟΥΛΟ ΛΟΓΙΣΜΙΚΟ/ KEYLOGGER

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Μια μικρή οικογενειακή κατασκευαστική εταιρεία έκανε εκτεταμένη χρήση της ηλεκτρονικής τραπεζικής. Ο υπάλληλος του λογιστηρίου συνδεόταν στο online τραπεζικό σύστημα με ένα εταιρικό και ένα ειδικό για κάθε χρήστη αναγνωριστικό και κωδικό πρόσβασης. Για συναλλαγές άνω των 1.000 ευρώ έπρεπε να απαντηθούν δύο ερωτήσεις πρόκλησης.

Ο ιδιοκτήτης ειδοποιήθηκε ότι ξεκίνησε μεταφορά πληρωμής ύψους 5.000 ευρώ από άγνωστη πηγή. Επικοινώνησε με την τράπεζα και διαπίστωσε ότι μέσα σε μόλις μία εβδομάδα οι κυβερνοεγκληματίες είχαν πραγματοποιήσει δέκα μεταφορές από τους τραπεζικούς λογαριασμούς της εταιρείας, συνολικού ύψους 10.000 ευρώ. Πώς; Ενας από τους υπαλλήλους τους είχε ανοίξει ένα μήνυμα ηλεκτρονικού ταχυδρομείου από κάτι που νόμιζε ότι ήταν προμηθευτής υλικών, αλλά αντ' αυτού ήταν ένα κακόβουλο μήνυμα ηλεκτρονικού ταχυδρομείου με κακόβουλο λογισμικό από έναν απατεώνα λογαριασμό.

Οι επιτιθέμενοι μπόρεσαν να εγκαταστήσουν κακόβουλο λογισμικό στους υπολογιστές της εταιρείας, χρησιμοποιώντας ένα keylogger για να καταγράψουν τα τραπεζικά στοιχεία . Το keylogger είναι ένα λογισμικό που παρακολουθεί σιωπηλά τις πληκτρολογήσεις του υπολογιστή και στέλνει τις πληροφορίες σε έναν εγκληματία του κυβερνοχώρου. Στη συνέχεια μπορούν να έχουν πρόσβαση σε τραπεζικές και άλλες οικονομικές υπηρεσίες στο διαδίκτυο, χρησιμοποιώντας έγκυρους αριθμούς λογαριασμών και κωδικούς πρόσβασης.Ο ιδιοκτήτης ειδοποιήθηκε ότι ξεκίνησε μεταφορά πληρωμής ύψους 5.000 ευρώ από άγνωστη πηγή. Επικοινώνησε με την τράπεζα και διαπίστωσε ότι μέσα σε μόλις μία εβδομάδα οι κυβερνοεγκληματίες είχαν πραγματοποιήσει δέκα μεταφορές από τους τραπεζικούς λογαριασμούς της

εταιρείας, συνολικού ύψους 10.000 ευρώ. Πώς; Ενας από τους υπαλλήλους τους είχε ανοίξει ένα μήνυμα ηλεκτρονικού ταχυδρομείου από κάτι που νόμιζε ότι ήταν προμηθευτής υλικών, αλλά αντ' αυτού ήταν ένα κακόβουλο μήνυμα ηλεκτρονικού ταχυδρομείου με κακόβουλο λογισμικό από έναν απατεώνα λογαριασμό.

Οι επιτιθέμενοι μπόρεσαν να εγκαταστήσουν κακόβουλο λογισμικό στους υπολογιστές της εταιρείας, χρησιμοποιώντας ένα keylogger για να καταγράψουν τα τραπεζικά στοιχεία . Το keylogger είναι ένα λογισμικό που παρακολουθεί σιωπηλά τις πληκτρολογήσεις του υπολογιστή και στέλνει τις πληροφορίες σε έναν εγκληματία του κυβερνοχώρου. Στη συνέχεια μπορούν να έχουν πρόσβαση σε τραπεζικές και άλλες οικονομικές υπηρεσίες στο διαδίκτυο, χρησιμοποιώντας έγκυρους αριθμούς λογαριασμών και κωδικούς πρόσβασης.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Οι πληροφορίες για την εν λόγω κυβερνοεπίθεση συλλέχθηκαν μέσω δύο συνεντεύξεων, μία με τον ιδιοκτήτη της εταιρείας και μία με έναν τεχνικό της εταιρείας υποστήριξης της πληροφορικής. Και οι δύο ήταν πρόθυμοι να περιγράψουν και να δώσουν λεπτομέρειες για το περιστατικό, αλλά ζήτησαν να διατηρήσουν την ανωνυμία και των δύο εταιρειών επειδή οι πληροφορίες ήταν πολύ ευαίσθητες γι' αυτούς.

ΠΡΟΛΗΨΗ

Στην εταιρεία που αναλύθηκε, οι διαδικασίες και οι μηχανισμοί ασφάλειας στον κυβερνοχώρο δεν κρίθηκαν ικανοποιητικοί. Αν και οι υπολογιστές της εταιρείας διέθεταν λογισμικό προστασίας από ιούς, κανένας δεν ήταν ενημερωμένος. Επιπλέον, δεν πραγματοποιήθηκαν εκστρατείες ευαισθητοποίησης και ορισμένοι εργαζόμενοι φάνηκε να έχουν περιορισμένη κατανόηση των κινδύνων στον κυβερνοχώρο.

ΑΝΑΓΝΩΡΙΣΗ

Με βάση τις παρεχόμενες πληροφορίες, συλλέχθηκαν οι ακόλουθες λεπτομέρειες σχετικά με το περιστατικό:

- ☑ Εχει ληφθεί ένα κοινωνικά σχεδιασμένο ηλεκτρονικό μήνυμα ηλεκτρονικού ψαρέματος με ένα συμπιεσμένο αρχείο zip που επισυνάπτεται ως επαλήθευση σε μια παραγγελία προμηθευτή.
- ☑ Ανοίγοντας το αρχείο, το κακόβουλο λογισμικό εγκαταστάθηκε στον υπολογιστή
- ☑ Ενα λογισμικό keylogger εγκαταστάθηκε και παρακολουθεί σιωπηλά τις πληκτρολογήσεις του υπολογιστή και στέλνει τις πληροφορίες σε έναν εγκληματία του κυβερνοχώρου.
- ☑ Στη συνέχεια, ο εγκληματίας στον κυβερνοχώρο χρησιμοποιεί τα διαπιστευτήρια που κατέγραψε για να αποκτήσει πρόσβαση στον τραπεζικό λογαριασμό και πραγματοποιεί τη μεταφορά χρησιμοποιώντας έγκυρους αριθμούς λογαριασμού και κωδικούς πρόσβασης.
- ☑ Το περιστατικό εντοπίστηκε μόνο όταν ο εγκληματίας του κυβερνοχώρου προσπάθησε να πραγματοποιήσει μεταφορά ποσού άνω των 1000 ευρώ.

ΑΠΑΝΤΗΣΗ

Καθώς η εταιρεία δεν διέθετε σχέδιο ασφάλειας στον κυβερνοχώρο, η αντίδραση στην επίθεση καθυστέρησε.

ΠΟΙΟΣ: Ο επιτιθέμενος δεν μπόρεσε να αναγνωριστεί με ακρίβεια. Ήταν γνωστή μόνο μια διεύθυνση ηλεκτρονικού ταχυδρομείου και η πιθανή προέλευση.
ΣΕ ΠΟΙΟΝ: μη συγκεκριμένος στόχος
ΓΙΑΤΙ: Συλλογή ευαίσθητων δεδομένων και χρήση αυτών για κλοπή χρημάτων
ΤΙ: Πιστοποιητικά τραπεζικού λογαριασμού της εταιρείας
ΠΩΣ: Keylogger, παρακολουθεί σιωπηλά τις πληκτρολογήσεις του υπολογιστή

ΣΤΡΑΤΗΓΙΚΗ: Η απειλή ξεκίνησε από έναν υπολογιστή χωρίς antivirus. Πραγματοποιήθηκε μια διαδικασία καθαρισμού από τον εμπειρογνώμονα ΤΠΕ μιας εταιρείας. Ο τραπεζικός λογαριασμός έκλεισε και τα διαπιστευτήρια άλλαξαν. Η εταιρεία ΤΠΕ τους βοήθησε να ολοκληρώσουν μια πλήρη ανασκόπηση της κυβερνοασφάλειας των συστημάτων τους και να εντοπίσουν ποια ήταν η πηγή του περιστατικού. Συνέστησαν επίσης αναβαθμίσεις στο λογισμικό ασφαλείας τους.

ΑΝΑΚΑΜΨΗ

ΕΠΙΠΤΩΣΗ: Η εταιρεία έκλεισε τον τραπεζικό της λογαριασμό και κινήθηκε νομικά για να ανακτήσει τις απώλειές της. Η επιχείρηση ανέκτησε ένα μικρό μέρος των απωλειών. Δεν ανακτήθηκαν χρήματα για το χρόνο και τα νομικά έξοδα.

ΑΝΑΚΤΗΣΗ: Η στρατηγική ανάκαμψης επικεντρώθηκε στο κλείσιμο του τραπεζικού λογαριασμού για την αποφυγή περαιτέρω ζημιών. Αλλες ενέργειες ήταν, ο καθαρισμός του παραβιασμένου υπολογιστή και του παραβιασμένου ηλεκτρονικού γραμματοκιβωτίου. Έλεγχος όλων των υπολογιστών της εταιρείας για τυχόν άλλες επιθέσεις.

ΣΤΡΑΤΗΓΙΚΗ: Η εταιρεία θα πρέπει να εφαρμόσει διάφορες δράσεις για την πρόληψη τέτοιων περιστατικών. Η στρατηγική της πρέπει να επικεντρώνεται στις ακόλουθες ενέργειες/βήματα:

- ☑ Εφαρμόστε πολιτικές ασφαλείας, όπως η πολιτική αλλαγής κωδικού πρόσβασης και η πολιτική διαχείρισης λογαριασμών χρηστών.
- ☑ Εγκατάσταση και συντήρηση ενημερωμένου λογισμικού Antivirus/Antimalware.
- ☑ Εκτέλεση προγραμμάτων κατάρτισης για τη διασφάλιση της ευαισθητοποίησης των εργαζομένων.
- ☑ Περιορισμός του περιεχομένου που βασίζεται στον Ιστό.
- ☑ Εκτελείτε τακτικούς ελέγχους και επιθεωρήσεις.
- ☑ Εκτέλεση της πρόληψης και της εφαρμογής ενός συστήματος διαχείρισης κινδύνων.

ΔΙΔΑΓΜΑΤΑ

- ☑ Ειδοποιήσεις - ρυθμίστε ειδοποιήσεις συναλλαγών για όλες τις πιστωτικές, χρεωστικές κάρτες και τραπεζικούς λογαριασμούς.
- ☑ Έλεγχος πρόσβασης. Περιορίστε την πρόσβαση σε ευαίσθητους λογαριασμούς μόνο στους υπαλλήλους που χρειάζονται πρόσβαση- αλλάξτε συχνά τους κωδικούς πρόσβασης.
- ☑ Η εταιρεία θα πρέπει να αξιολογήσει τον κίνδυνο που διατρέχει και να εκτιμήσει τις επιλογές ασφάλισης αστικής ευθύνης στον κυβερνοχώρο.

- ☑ Επιλέξτε τράπεζες που προσφέρουν πολλαπλά επίπεδα ελέγχου ταυτότητας για την πρόσβαση σε λογαριασμούς και συναλλαγές.
- ☑ Δημιουργήστε, διατηρήστε και εξασκηθείτε σε ένα σχέδιο αντιμετώπισης περιστατικών στον κυβερνοχώρο, το οποίο να είναι γρήγορα εφαρμόσιμο.
- ☑ Οι εγκληματίες του κυβερνοχώρου παραδίδουν και εγκαθιστούν κακόβουλο λογισμικό μέσω ηλεκτρονικού ταχυδρομείου. Εκπαιδεύστε τους υπαλλήλους στην ασφάλεια ηλεκτρονικού ταχυδρομείου.

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 17: ΕΝΑΣ ΚΛΕΜΜΕΝΟΣ ΥΠΟΛΟΓΙΣΤΗΣ ΠΡΟΚΑΛΕΙ ΣΟΒΑΡΗ ΠΑΡΑΒΙΑΣΗ ΔΕΔΟΜΕΝΩΝ

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Μια εταιρεία συμβούλων 10 ατόμων έστειλε μια μικρή ομάδα στην Ουγγαρία για να ολοκληρώσει ένα έργο πελάτη. Κατά τη διάρκεια της παραμονής τους, ο ανώτερος σύμβουλος άφησε τον φορητό υπολογιστή που του είχε χορηγηθεί στην εργασία του, ο οποίος είχε πρόσβαση σε ευαίσθητες πληροφορίες πελατών και τραπεζικά στοιχεία της εταιρείας, σε ένα κλειδωμένο αυτοκίνητο, ενώ εκτελούσε μια εργασία. Το αυτοκίνητο παραβιάστηκε και ο φορητός υπολογιστής εκλάπη. Δυστυχώς, τα δεδομένα στον υπολογιστή δεν ήταν κρυπτογραφημένα, επειδή ο υπάλληλος δεν εφάρμοσε την πολιτική της εταιρείας για την κρυπτογράφηση όλων των ευαίσθητων δεδομένων στον υπολογιστή του. Η εταιρεία φοβόταν πλέον μια κυβερνοεπίθεση στα συστήματά της, τραπεζικούς λογαριασμούς και διαρροή δεδομένων πελατών.

Τύπος επίθεσης: Φυσική κλοπή ενός μη κρυπτογραφημένου υπολογιστή. Η κρυπτογράφηση είναι η διαδικασία της αποκρυπτογράφησης αναγνώσιμου κειμένου ώστε να μπορεί να διαβαστεί μόνο από το άτομο που έχει το κλειδί αποκρυπτογράφησης. Δημιουργεί ένα πρόσθετο επίπεδο ασφάλειας για ευαίσθητες πληροφορίες.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Οι πληροφορίες που απαιτούνται για την περιγραφή του περιστατικού συλλέχθηκαν μέσω συνέντευξης με τον ανώτερο σύμβουλο της εταιρείας και τον τεχνικό πληροφορικής της εταιρείας ΤΠΕ που υποστηρίζει την εταιρεία συμβούλων. Η αλληλεπίδραση πραγματοποιήθηκε με την προϋπόθεση της ανωνυμίας των ευαίσθητων πληροφοριών. Ακόμη και αν ο ερωτηθείς ήταν πρόθυμος να περιγράψει το περιστατικό, δεν ήταν δυνατόν να ληφθούν ορισμένες πληροφορίες κρυπτογράφησης και αυτός είναι ο λόγος που ζητήθηκε από την εταιρεία ΤΠΕ που υποστηρίζει την υπόθεση να διαφωτίσει.

ΠΡΟΛΗΨΗ

Παρόλο που το περιστατικό δεν αποτελεί ξεκάθαρο περιστατικό κυβερνοεπίθεσης, πρόκειται για ένα σοβαρό και πολύ συνηθισμένο περιστατικό που προκαλεί μια σειρά σημαντικών κυβερνοεπιθέσεων.

Στην περίπτωση της εταιρείας που αναλύθηκε, από την άποψη της ασφάλειας στον κυβερνοχώρο, λειτουργούσαν συγκεκριμένες πολιτικές και μηχανισμοί, οι οποίοι όμως δεν εφαρμόζονταν από ορισμένους υπαλλήλους λόγω της χαμηλής εμπειρίας τους στον τομέα των κινδύνων στον τομέα των πληροφοριών και της ασφάλειας στον κυβερνοχώρο.

ΑΝΑΓΝΩΡΙΣΗ

Ο εργαζόμενος κατήγγειλε αμέσως την κλοπή στην αστυνομία και στην εταιρεία του. Ενημερώθηκε επίσης η τράπεζα για την παρακολούθηση των συναλλαγών του λογαριασμού. Η εταιρεία ενημέρωσε αντίστοιχα την εταιρεία υποστήριξης ΤΠΕ για να απενεργοποιήσει την απομακρυσμένη πρόσβαση του φορητού υπολογιστή και άρχισε να παρακολουθεί τη δραστηριότητα. Ο φορητός υπολογιστής ήταν εξοπλισμένος με εργαλεία ασφαλείας και προστασία με κωδικό πρόσβασης. Τα δεδομένα που ήταν αποθηκευμένα στον σκληρό δίσκο δεν ήταν κρυπτογραφημένα - σε αυτά περιλαμβάνονταν ευαίσθητα, δεδομένα πελατών και τραπεζικά στοιχεία της εταιρείας.

Για τον εντοπισμό αυτής της επίθεσης με βάση τη συμπεριφορά, μπορούν να χρησιμοποιηθούν οι ακόλουθες τεχνικές MITRE ATT&CK:

- ☑ T1027 - Συγκαλυμμένα αρχεία ή πληροφορίες
- ☑ T1036 - Μεταμφιέσεις
- ☑ T1586.002 - Λογαριασμοί συμβιβασμού: Λογαριασμοί ηλεκτρονικού ταχυδρομείου

ΑΠΑΝΤΗΣΗ

Απάντηση: Η εταιρεία πρέπει να ακολουθήσει τους νόμους της πολιτείας όσον αφορά την παραβίαση δεδομένων. Οι πολιτειακοί νόμοι και οι κανονισμοί της ΕΕ σχετικά με την GPDR είναι πολύ αυστηροί με πρόστιμα υψηλού κόστους.

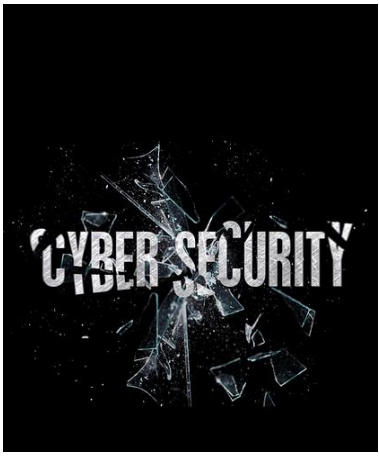
- ☑ **ΠΟΙΟΣ:** Ο επιτιθέμενος δεν μπόρεσε να ταυτοποιηθεί. Μόνο ο τόπος του περιστατικού ήταν γνωστός.
- ☑ **ΣΕ ΠΟΙΟΝ:** μη συγκεκριμένος στόχος
- ☑ **ΓΙΑΤΙ:** Συγκέντρωση ευαίσθητων δεδομένων και απόκτηση χρημάτων από την πώληση του κλεμμένου εξοπλισμού
- ☑ **ΤΙ:** ευαίσθητα δεδομένα πελατών και τραπεζικά στοιχεία της εταιρείας

- ☑ **ΠΩΣ:** απώλεια εξοπλισμού, διαρροή ευαίσθητων δεδομένων και επίθεση σε τραπεζικούς λογαριασμούς
- ☑ **ΣΤΡΑΤΗΓΙΚΗ:** Η απειλή ξεκίνησε από έναν υπολογιστή χωρίς antivirus και εξαπλώθηκε πλευρικά. Πραγματοποιήθηκε διαδικασία καθαρισμού από εξειδικευμένη εταιρεία IT&C.

ΑΝΑΚΑΜΨΗ

ΕΠΙΠΤΩΣΗ: Η εταιρεία συμβούλων δαπάνησε περισσότερα από 20.000 ευρώ για την εφαρμογή, την παρακολούθηση και τις λειτουργικές βελτιώσεις. Μια παραβίαση δεδομένων επηρεάζει αρνητικά ένα εμπορικό σήμα και η εμπιστοσύνη πρέπει να αποκατασταθεί.

Οι κύριες συνέπειες της επίθεσης ήταν οι εξής:



- ☑ Απώλεια δεδομένων
- ☑ Απώλεια PC
- ☑ Συμβιβασμός του συστήματος
- ☑ Χρηματοοικονομικό κόστος

ΑΠΟΚΑΤΑΣΤΑΣΗ: Η στρατηγική ανάκαμψης επικεντρώθηκε στην ελαχιστοποίηση της φήμης του εμπορικού σήματος και στην παρακολούθηση και τον έλεγχο των εσωτερικών συστημάτων και των τραπεζικών λογαριασμών της εταιρείας. Προληπτικά, άλλαξαν όλα τα διαπιστευτήρια των τραπεζικών λογαριασμών και αναστάλθηκαν και άλλαξαν τα προνόμια των συστημάτων των εργαζομένων.

ΣΤΡΑΤΗΓΙΚΗ: Η εταιρεία θα πρέπει να εφαρμόσει διάφορες δράσεις για την πρόληψη τέτοιων περιστατικών. Η στρατηγική της πρέπει να επικεντρώνεται

- ☑ Εκτέλεση εκπαιδευτικών προγραμμάτων για τη διασφάλιση της ευαισθητοποίησης των εργαζομένων
- ☑ Εκτέλεση τακτικών ελέγχων και επιθεωρήσεων
- ☑ Εκτέλεση Πρόληψη και εφαρμογή συστήματος διαχείρισης κινδύνων

ΔΙΔΑΓΜΑΤΑ

- ☑ Οι εταιρείες πρέπει να καθιερώσουν και να εκπαιδεύσουν τους εργαζομένους στον ασφαλή χειρισμό των συσκευών που χορηγούνται από την εργασία.
- ☑ Οι συσκευές πρέπει να αποθηκεύονται με ασφάλεια όταν δεν βρίσκονται στην άμεση παρουσία του εργαζομένου.
- ☑ Οι εταιρείες πρέπει να λαμβάνουν μέτρα για την κρυπτογράφηση των δεδομένων οπουδήποτε αποθηκεύονται ή διαβιβάζονται.
- ☑ Οι εργαζόμενοι θα πρέπει να κατανοούν σαφώς τη σημασία της κρυπτογράφησης και τον τρόπο χρήσης της.

- ☑ Οι εταιρείες πρέπει να κατανοούν και να γνωρίζουν τις ευθύνες τους σύμφωνα με τους νόμους περί κοινοποίησης παραβίασης δεδομένων της χώρας στην οποία δραστηριοποιούνται.
- ☑ Η τακτική επανεξέταση των πρακτικών ασφαλείας της εταιρείας είναι επιτακτική ανάγκη στους σύγχρονους οργανισμούς για την πρόληψη περιστατικών, την ανακάλυψη τρωτών σημείων και τη μείωση των επιπτώσεων των περιστατικών.

"Υπήρξε αύξηση 57% στις παραλλαγές του Mirai botnet που εντοπίστηκαν το 2019. Οι παραλλαγές Mirai χρησιμοποιούνται συνήθως για επιθέσεις ωμής βίας σε συσκευές IoT. Οι επιθέσεις αυτές αυξήθηκαν κατά 51%, ενώ τα web exploits αυξήθηκαν κατά 87% το 2019..." (MCCART, 2022).

ΜΕΛΕΤΗ ΠΕΡΙΠΤΩΣΗΣ 18: ΕΠΙΘΕΣΗ DDOS ΣΤΑΜΑΤΑ ΣΗΜΑΝΤΙΚΕΣ ΥΠΗΡΕΣΙΕΣ

ΣΤΟΧΕΥΟΜΕΝΟΣ ΟΡΓΑΝΙΣΜΟΣ

Ο στοχευόμενος οργανισμός ήταν μια εταιρεία παροχής φιλοξενίας. Οι επιτιθέμενοι εξαπέλυσαν μαζική κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών εναντίον συγκεκριμένου ιστότοπου στα μέσα Δεκεμβρίου 2021, ξεπερνώντας το εύρος ζώνης του 1,5 gigabits ανά δευτερόλεπτο και σχεδόν 100 εκατομμύρια πακέτα ανά δευτερόλεπτο, η μεγαλύτερη επίθεση που αντιμετώπισε εταιρεία φιλοξενίας

Η εταιρεία πιστεύει ότι ο επιτιθέμενος επικεντρώθηκε στους ιστότοπους με online παιχνίδια καζίνο και ότι ο πάροχος φιλοξενίας δεν ήταν ο πραγματικός στόχος. Η επίθεση DDOS προκαλεί τον τερματισμό της διαθεσιμότητας των υπηρεσιών του πελάτη για περισσότερες από 12 ώρες.

Μια κατανεμημένη επίθεση άρνησης παροχής υπηρεσιών (DDoS) είναι μια κακόβουλη προσπάθεια να διακοπεί η κανονική κυκλοφορία ενός στοχευμένου διακομιστή, υπηρεσίας ή δικτύου, κατακλύζοντας τον στόχο ή την περιβάλλουσα υποδομή του με πλημμύρα κυκλοφορίας στο Διαδίκτυο. Οι επιθέσεις DDoS επιτυγχάνουν αποτελεσματικότητα χρησιμοποιώντας πολλαπλά παραβιασμένα συστήματα υπολογιστών ως πηγές κίνησης επίθεσης. Οι εκμεταλλευόμενοι υπολογιστές μπορεί να περιλαμβάνουν υπολογιστές και άλλους δικτυακούς πόρους, όπως συσκευές IoT.

ΠΩΣ ΑΠΟΚΤΗΘΗΚΑΝ ΟΙ ΠΛΗΡΟΦΟΡΙΕΣ.

Οι πληροφορίες που απαιτούνται για την περιγραφή αυτής της κυβερνοεπίθεσης συλλέχθηκαν μέσω δύο συνεντεύξεων (προσωπικές συναντήσεις), μία με τον διευθύνοντα σύμβουλο της εταιρείας και μία με έναν μηχανικό πληροφορικής της εταιρείας. Και οι δύο ήταν πρόθυμοι να περιγράψουν και να δώσουν λεπτομέρειες για το περιστατικό, αλλά ζήτησαν να διατηρήσουν την ανωνυμία τόσο των

εταιρειών όσο και των ονομάτων τους, επειδή οι πληροφορίες ήταν πολύ ευαίσθητες γι' αυτούς.

ΠΡΟΛΗΨΗ

Παρόλο που ο πάροχος φιλοξενίας διαθέτει αρκετές διαδικασίες και μηχανισμούς κυβερνοασφάλειας, φαίνεται ότι οι επιτιθέμενοι βρήκαν ένα ευάλωτο σημείο για να το εξερευνήσουν.

Ο τεχνικός της εταιρείας παρατήρησε ότι ο ιστότοπος έγινε ξαφνικά αργός, αλλά υποθέτουν ότι επρόκειτο για μια νόμιμη αύξηση της επισκεψιμότητας λόγω της περιόδου των διακοπών. Η επίθεση εντοπίστηκε μόλις ο ιστότοπος έγινε μη διαθέσιμος και ο πελάτης παραπονέθηκε.

ΑΝΑΓΝΩΡΙΣΗ

Οι επιτιθέμενοι χρησιμοποίησαν κίνηση από πηγές σε όλο τον κόσμο. Φαίνεται ότι η επίθεση άρνησης παροχής υπηρεσιών δημιουργήθηκε από ένα botnet Mirai. Και επειδή το Mirai botnet έχει τη δυνατότητα να στέλνει περίπου 600 megabits ανά δευτερόλεπτο χρησιμοποίησαν επίθεση δεύτερου επιπέδου με ένα διαφορετικό Mirai botnet.

Το Mirai είναι κακόβουλο λογισμικό που μολύνει έξυπνες συσκευές που λειτουργούν με επεξεργαστές ARC, μετατρέποντάς τες σε ένα δίκτυο τηλεχειριζόμενων bots ή "ζόμπι". Αυτό το δίκτυο bots, που ονομάζεται botnet, χρησιμοποιείται συχνά για την εξαπόλυση επιθέσεων DDoS.

Ο πάροχος φιλοξενίας χρησιμοποίησε εργαλεία ανάλυσης της κίνησης για να εντοπίσει την επίθεση. Το βασικό χαρακτηριστικό της επίθεσης είναι ο μεγάλος όγκος που προέρχεται από την ίδια σειρά διευθύνσεων IP. Οι μηχανικοί κατάφεραν να απομονώσουν αυτές τις IP και ο ιστότοπος επανήλθε.

Στη συνέχεια, προσπαθούν να εντοπίσουν γιατί το εργαλείο ανάλυσης κυκλοφορίας δεν εντόπισε την επίθεση από τα πρώτα στάδια.

Σύμφωνα με το MITRE ATT&CK framework, το περιστατικό αυτό μπορεί να περιγραφεί ως εξής:

- ☑ T1499 - Άρνηση παροχής υπηρεσιών σε τελικό σημείο
- ☑ T1498 - Άρνηση υπηρεσίας δικτύου

ΑΠΑΝΤΗΣΗ

- ☑ **ΠΟΙΟΣ:** Ο επιτιθέμενος δεν μπορεί να αναγνωριστεί. Η επίθεση προήλθε από όλο τον κόσμο
- ☑ **ΣΕ ΠΟΙΟΝ:** Ο στόχος ήταν ένας συγκεκριμένος ιστότοπος που φιλοξενούσε online παιχνίδια καζίνο.
- ☑ **ΓΙΑΤΙ:** Για να διακόψετε τη λειτουργία του.
- ☑ **ΤΙ:** Ιστοσελίδα της εταιρείας.
- ☑ **ΠΩΣ:** Mirai botnets.
- ☑ **ΣΤΡΑΤΗΓΙΚΗ:** Η επίθεση ξεκίνησε σε ένα sever ενός παρόχου φιλοξενίας για να διακόψει τη λειτουργία ενός συγκεκριμένου ιστότοπου. Το εργαλείο ανάλυσης της κυκλοφορίας δεν κατάφερε να προειδοποιήσει για την πιθανότητα κυβερνοεπίθεσης. Η εταιρεία αύξησε την

ευαισθησία των συναγερμών στο εργαλείο ανάλυσης της κίνησης, ώστε να αποφύγει παρόμοια περιστατικά στο μέλλον.

ΑΝΑΚΑΜΨΗ

ΕΠΙΠΤΩΣΗ: Ο πάροχος φιλοξενίας είχε κάποια επιπλέον σημαντικά έξοδα για να καλύψει την επίθεση και επίσης, είχε σοβαρή ζημιά στη φήμη του. Είχαν το επιπλέον κόστος εργασίας για την ανάκτηση του ιστότοπου και τις κυρώσεις στη συμφωνία SLA με τον πελάτη. Το συνολικό κόστος εκτιμήθηκε σε περίπου 40.000 ευρώ.

ΑΠΟΚΑΤΑΣΤΑΣΗ: Η στρατηγική αποκατάστασης επικεντρώθηκε στην απομόνωση των επιτιθέμενων IP για να σταματήσει η επίθεση και να ανακτηθεί η λειτουργία του ιστότοπου. Αλλες ενέργειες ήταν, η αύξηση της ευαισθησίας των συναγερμών του εργαλείου ανάλυσης της κυκλοφορίας. Έλεγχος όλων των διακομιστών και υπηρεσιών φιλοξενίας για τυχόν άλλες επιθέσεις ή ύποπτες δραστηριότητες.

ΣΤΡΑΤΗΓΙΚΗ: Η εταιρεία θα πρέπει να εφαρμόσει διάφορες δράσεις για την πρόληψη τέτοιων περιστατικών. Η στρατηγική της πρέπει να επικεντρώνεται σε

- ☑ Αύξηση της ευαισθησίας του εργαλείου ανάλυσης της κυκλοφορίας
- ☑ Εγκαταστήστε ένα δεύτερο εργαλείο για επιπλέον ασφάλεια
- ☑ Εκτέλεση εκπαιδευτικών προγραμμάτων για τη διασφάλιση της ευαισθητοποίησης των εργαζομένων
- ☑ Περιορισμός ορισμένων περιοχών IP
- ☑ Εκτέλεση τακτικών ελέγχων και επιθεωρήσεων
- ☑ Εκτέλεση Πρόληψη και εφαρμογή συστήματος διαχείρισης κινδύνων
- ☑ Πιστοποίηση της υποδομής και των υπηρεσιών τους σύμφωνα με τα πρότυπα ISO27001 και ISO22301.

ΔΙΔΑΓΜΑΤΑ

- ☑ Η αποδιοργάνωση έχει πολλές μορφές. Οι διακοπές ή οι καθυστερήσεις μπορεί να έχουν πολλές μορφές, ειδικά για τους παρόχους φιλοξενίας. Οταν εντοπίζεται μια επίθεση, οι κατάλληλες ομάδες αντιμετώπισης πρέπει να αφιερώσουν πόρους για την αντιμετώπισή της.
- ☑ Πολλές επιθέσεις στον κυβερνοχώρο μπορούν εύκολα να αποτραπούν. Οι εξελιγμένες κυβερνοεπιθέσεις μπορούν να προκαλέσουν μεγάλη ζημιά, αλλά πολλές από αυτές μπορούν εύκολα να αποτραπούν με την κατάλληλη ασφάλεια. Είναι σημαντικό να δημιουργηθεί ένα ισχυρό και προληπτικό σύστημα διαχείρισης της ασφάλειας για να σταματήσουν οι επιθέσεις. Ενα τέτοιο σύστημα διαχείρισης απαιτεί συνεχή συντήρηση, παρακολούθηση όλων των συστημάτων και των συσκευών στο δίκτυο, συμπεριλαμβανομένης της ενημέρωσης της τεχνολογίας και της εφαρμογής διορθωτικών επιδιορθώσεων ασφαλείας για γνωστά exploits.
- ☑ Οι επιθέσεις DDoS πρέπει να λαμβάνονται σοβαρά υπόψη. Οι σημερινές επιθέσεις DoS και DDoS είναι διαφορετικές, καθώς είναι πιο μοχθηρές, στοχευμένες και ικανές.

- ☑ Χωρίς χρονικό περιορισμό. Οι επιθέσεις σε επίπεδο δικτύου μπορεί να διαρκέσουν περισσότερο από 48 ώρες, ενώ οι επιθέσεις σε επίπεδο εφαρμογής μπορεί να διαρκέσουν για ημέρες. Διείσδυση σε συστήματα και δίκτυα για κατασκοπεία - εβδομάδες και μήνες.
- ☑ Η ασφάλεια στον κυβερνοχώρο πρέπει να αποτελεί προτεραιότητα. Η ασφάλεια στον κυβερνοχώρο θα πρέπει να αποτελεί μία από τις υψηλότερες προτεραιότητες για όλες τις οντότητες που δραστηριοποιούνται στο σημερινό τοπίο. Οι επιθέσεις αυτές έχουν γίνει εξελιγμένες, στοχευμένες, ικανές και ανεξέλεγκτες. Ολες οι απειλές πρέπει να λαμβάνονται σοβαρά υπόψη, συμπεριλαμβανομένων των επιθέσεων DDoS, οι οποίες γίνονται όλο και πιο συχνές.

ΣΥΜΠΕΡΑΣΜΑ

Βάσει του διαφοροποιημένου χαρτοφυλακίου που παρουσιάζεται στο πλαίσιο του ENCRYPT 4.0 Documental battery σχετικά με τις επιθέσεις στον κυβερνοχώρο, μπορούν να εξαχθούν τα ακόλουθα συμπεράσματα:

- ☑ Με την ανάπτυξη των ΤΠΕ και στο πλαίσιο της Βιομηχανίας 4.0, η ασφάλεια στον κυβερνοχώρο αποκτά ολοένα και μεγαλύτερη σημασία και **οι εταιρείες που δεν διαθέτουν επαρκή άμυνα στον κυβερνοχώρο θέτουν τις δραστηριότητές τους σε σοβαρό κίνδυνο.**

- ☑ **Οι εργαζόμενοι διαδραματίζουν βασικό ρόλο στην κυβερνοάμυνα**, επομένως οι εργαζόμενοι τόσο στις ΜΜΕ όσο και στις μεγάλες επιχειρήσεις θα πρέπει να λαμβάνουν τουλάχιστον βασική εκπαίδευση σχετικά με τον τρόπο προστασίας των δεδομένων της εταιρείας και την εργασία με ευαίσθητες πληροφορίες, καθώς περισσότερες από πολλές κυβερνοεπιθέσεις συμβαίνουν λόγω έλλειψης γνώσεων σχετικά με αυτές τις πτυχές, ιδίως στο πλαίσιο της απομακρυσμένης εργασίας κατά τη διάρκεια της πανδημίας COVID-19.

- ☑ **Οι ΜΜΕ, ανεξαρτήτως του τομέα στον οποίο δραστηριοποιούνται, γίνονται πρωταρχικοί στόχοι για τους χάκερ και τους οργανωμένους εγκληματίες του κυβερνοχώρου**, αλλά ταυτόχρονα μόνο το 1/3 των ΜΜΕ έχει σχέδιο για τον περιορισμό μιας πιθανής κυβερνοεπίθεσης, επομένως οι ΜΜΕ πρέπει να θεωρήσουν την ασφάλεια στον κυβερνοχώρο

ως ύψιστη προτεραιότητα προκειμένου να διασφαλίσουν μακροπρόθεσμα την ανταγωνιστικότητά τους.

ΑΝΑΦΟΡΕΣ

1. Acronis, 2020. The NHS cyber-attack. [Online] Acronis. Available at:https://www.acronis.com/en-us/blog/posts/nhs-cyber-attack/

2. Barber, B., 2016. William Hill apologise after website attack. [Online] Racing Post. Available at: https://www.racingpost.com/news/william-hill-apologise-after-website-attack/266196 (Case study 6)

3. Blue goose, n.d. Information Security at William Hill. [Online] blue goose. Available at: https://bluegooseis.co.uk/work/william-hill (Case study 6)

4. Braue, D., 2022. Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031. [Online] 2022 Cybersecurity Ventures. Available at: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/

5. Cook, S., 2022. 20+ DDoS attack statistics and facts for 2018-2022. [Online]. Comparitech. Available at:https://www.comparitech.com/blog/information-security/ddos-statistics-facts/

6. Craver, R., 2015. Hanesbrands database hacked 900K phone, online customers affected. [e-journal] *Winston-Salem Journal.* Available at: https://journalnow.com/business/hanesbrands-database-hacked/article_543b338e-3664-11e5-b77e-c77df1e08b5c.html (Case study 4)

7. Cyber Startup Observatory. Available at: https://cyberstartupobservatory.com/ (Case study 4)

8. CyberNews, 2021. Thousands of Humana customers have their medical data leaked online by threat actors. [Online] 2022 Cybernews. Available at: https://cybernews.com/news/humana-insurance-customers-medical-data-leaked/ (Case study 5)

9. CyberTalks, 2022. Top 15 phishing attack statistics (and they might scare you) [Online]. CyberTalks. Available at: https://www.cybertalk.org/2022/03/30/top-15-phishing-attack-statistics-and-they-might-scare-you/

10. Cyware , 2018. Humana websites hit by sophisticated spoofing attack from 'foreign countries'. [Online] Cyware. Available at: https://cyware.com/news/humana-websites-hit-by-sophisticated-spoofing-attack-from-foreign-countries-5ac77624 (Case study 5)

11. Dissent, 2018. Humana notifies members after credential stuffing attack on Humana.com and Go365.com. [online] 2009 – 2022, DataBreaches.net and DataBreaches LLC. Available at:

https://www.databreaches.net/humana-notifies-members-after-credential-stuffing-attack-on-humana-com-and-go365-com/ (Case study 5)

12. EUROPOL, n.d. World's most dangerous malware EMOTET disrupted through global action. [Online] EUROPOL 2022. Available at: https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

13. Kolbasuk McGee, M., 2018. Humana Notifying Victims of 'Identity Spoofing' Attack. [online] *Data Breach Today*. Available at: https://www.databreachtoday.asia/humana-notifying-victims-identity-spoofing-attack-a-11153 (Case study 5)

14. McCart, C., 2022. 15+ Shocking botnet statistics. [Online] Comparitech. Available at:https://www.comparitech.com/blog/information-security/botnet-statistics/

15. Mimecast, 2022. Confronting the NEW WAVE OF CYBER ATTACKS: The State of Email security Report 2022. Mimecast. Available at: https://www.mimecast.com/globalassets/documents/ebook/state-of-email-security-2022.pdf

16. Moore, J., 2022. Top 10 List of Cybersecurity Facts for 2022. [Online] Elevity. Available at: https://www.gflesch.com/elevity-it-blog/cybersecurity-facts

17. Morran, Ch., 2015. Hanes Website Is The Latest, Oddest Victim Of Data Breach. Consumerist. Available at: https://consumerist.com/2015/07/30/hanes-website-is-the-latest-oddest-victim-of-data-breach/ (Case study 4)

18. StackHawk, 2022. What is Command Injection? [Online]. StackHawk, Available at: https://www.stackhawk.com/blog/what-is-command-injection/

19. The Cyber Wire, n.d. Definition of Spoofing. [Online]. The Cyber Wire. Available at: https://thecyberwire.com/glossary/spoofing

20. VentureBeat, 2022. Report: Average time to detect and contain a breach is 287 days. [Online] VentureBeat. Available at: https://venturebeat.com/2022/05/25/report-average-time-to-detect-and-contain-a-breach-is-287-days/

21. Verizon, 2021. DBIR: 2021 Data Breach Investigation Report. Verizon, 2021. Available at: https://www.verizon.com/business/resources/reports/2021-data-breach-investigations-report.pdf

22. Wallarm, 2021. The Biggest Hacker Attacks on Gambling. 10. [Online] Wallarm. Available at: https://lab.wallarm.com/the-biggest-hacker-attacks-on-gambling/ (Case study 6)

ΕΤΑΙΡΟΙ ΤΟΥ ΕΡΓΟΥ

ENCRYPT 4.0

Joint Cyber Workforce Development Initiative to Enable The European Industry to Overcome the Shortage of Cybersecurity Professionals

Το έργο ENCRYPT4.0 (2020-1-RO01-KA202-079983) έχει ως στόχο να δώσει τη δυνατότητα στη διοίκηση των μεταποιητικών ΜΜΕ να υιοθετήσουν μια προληπτική προσέγγιση για την ασφάλεια στον κυβερνοχώρο, υποστηρίζοντάς τες στη διαδικασία ανάλυσης, εντοπισμού και αντιμετώπισης των κινδύνων και απειλών στον κυβερνοχώρο που αφορούν τον οργανισμό τους. Προωθώντας τη διαδραστική μάθηση βάσει σχεδίου όσον αφορά την ενίσχυση των δεξιοτήτων και ικανοτήτων κυβερνοασφάλειας των εργαζομένων των ΜΜΕ ή/και των επαγγελματιών κυβερνοασφάλειας.

"George Emil Palade" University of Medicine, Pharmacy, Sciences and Technology of Târgu Mureș - Romania

Project coordinator

European Center for Quality Ltd., Consulting company - Bulgaria

Instituto de Soldadura e Qualidade, Technological institution - Portugal

Avantalia, technology-based SME - Spain

FH Joanneum, University of Applied Sciencies - Austria

PCX Management, Computers &