Ναυτιλιακές, εμπορικές αλυσίδες και Δημόσιο οι νέοι στόχοι των χάκερ

ΑΝΑΒΑΘΜΙΣΜΕΝΕΣ ΚΑΙ ΣΥΧΝΑ *δύσκολα ανιχνεύσιμες ψηφιακές επιθέσεις τροφοδοτούν μια μαύρη αγορά πολλών δισεκατομμυρίων, μέσω υφαρπαγής πολύτιμων πληροφοριών, μεταπώληση δεδομένων και online εκβιασμών*

Οποιαδήποτε εταιρεία και οργανισμός μπορεί να δεχτεί ψηφιακή επίθεση, προειδοποιούν οι ειδικοί σε θέματα κυβερνοασφάλειας, καταρρίπτοντας το στερεότυπο που θέλει τους χάκερ να στοχεύουν κατά προτίμηση τις τράπεζες και τους οικονομικούς οργανισμούς, «γιατί εκεί είναι τα λεφτά».

Του **Παναγιώτη Μαρκίδη**
markidis@gmail.com

Αναγνωρίζοντας την πραγματικότητα της ψηφιακής εποχής, όπου τα πάσης φύσεως δεδομένα μπορεί να έχουν αξία, γίνεται αντιληπτό ότι οι σύγχρονοι εγκληματίες χτυπάνε προς κάθε κατεύθυνση, είτε δρώντας για λογαριασμό τρίτων, οπότε συνήθως αναζητούν συγκεκριμένες πληροφορίες, είτε αποσκοπώντας στην υφαρπαγή στοιχείων και προσδοκώντας όφελος από τη μεταπώλησή τους στη μαύρη αγορά, είτε ακόμα με σκοπό να παγιδεύσουν τα θύματά τους και να τους αποσπάσουν στη συνέχεια λύτρα. Εξάλλου, και βάσει του συνολικού αριθμού των διαπιστωμένων ψηφιακών επιθέσεων, ο ευρύτερος οικονομικός τομέας βρίσκεται στην τρίτη θέση (15,7%). Προηγούνται ο δημόσιος (27,1%) και ο βιομηχανικός τομέας (25,2%). Μάλιστα, η ετήσια έκθεση ασφαλείας της Cisco αποκαλύπτει μείωση της εμπιστοσύνης των επιχειρήσεων στη στρατηγική τους σε θέματα ψηφιακής ασφάλειας και αυξημένες επιπτώσεις από τις επιθέσεις. Ειδικότερα, οι μικρές και μεσαίες επιχειρήσεις αναφέρονται ως ο «δυνητικά αδύναμος κρίκος», καθώς συχνά χρησιμοποιούν λιγότερα εργαλεία και διαδικασίες άμυνας έναντι απειλών, δημιουργώντας κερκόπορτες καθώς τα συστήματά τους μπορεί να επικοινωνούν με αυτά μεγαλύτερων οργανισμών. Αντίθετα είναι δεδομένο ότι οι μεγάλοι οργανισμοί επενδύουν σημαντικούς πόρους στην ψηφιακή τους ασφάλεια και βρίσκονται στην κορυφή από πλευράς υιοθέτησης των πιο σύγχρονων λύσεων προστασίας.

Περιζήτητα στοιχεία

Συγκεκριμένα, για την ελληνική αγορά προκύπτει ότι στο στόχαστρο των χάκερ μπαίνουν είτε συγκεκριμένου τύπου επιχειρήσεις, όπως οι ναυτιλιακές λόγω μεγάλου αριθμού προμηθευτών που θεωρητικά προσφέρει περισσότερες ευκαιρίες στους ψηφιακούς εγκληματίες, είτε εμπορικές αλυσίδες, τα πελατολόγια των οποίων συγκεντρώνουν πολύτιμα στοιχεία, είτε συχνά

Ο κ. Νίκος Μουρτζίνος της Cisco

και το Δημόσιο, αφού τα φορολογικά και περιουσιακά στοιχεία είναι πάντα περιζήτητα. Και είναι διαπιστωμένο ότι οι επιτιθέμενοι γίνονται ολοένα και πιο τολμηροί, συντονίζονται μεταξύ τους και εξαπολύουν πιο σύνθετες και στοχευμένες επιθέσεις. Ουσιαστικά πρόκειται για ομάδες εργασίας οι οποίες τις περισσότερες φορές οργανώνονται επί τούτου, για να πραγματοποιήσουν δηλαδή μια συγκεκριμένη κακόβουλη ενέργεια. Αφιερώνουν μήνες στη σχεδίασή της και συνήθως διαθέτουν αρκετά χρήματα και άλλους πόρους ώστε να έχουν το αποτέλεσμα που θέλουν. Παγκοσμίως η αγορά του ψηφιακού εγκλήματος υπολογίζεται σε δεκάδες δισ. δολάρια, προσελκύοντας ομάδες χάκερ που λειτουργούν πλέον με τη μορφή εταιρειών. Αντίστοιχα διογκώνεται και η αγορά γύρω από την ψηφιακή ασφάλεια, με τζίρο που φτάνει ετησίως τα 100 δισ. δολάρια και υψηλές χρηματιστηριακές αποδόσεις των εταιρειών που δραστηριοποιούνται στην παροχή τέτοιων λύσεων.

«Ολόκληρη η βιομηχανία που ασχολείται με την αντιμετώπιση των ψηφιακών επιθέσεων κάνει βήματα προόδου, κυρίως στο κομμάτι που αφορά τους χρόνους αντίδρασης. Το ζητούμενο πλέον είναι η αντιμετώπιση αυτών των επιθέσεων σε πραγματικό χρόνο, μειώνοντας σημαντικά τη διάρκεια εντοπισμού του κακόβουλου λογισμικού. Προφανώς τα αποτελέσματα διαφέρουν όταν κάποια επιχείρηση πέφτει θύμα μιας ψηφιακής επίθεσης και χρειάζεται ημέρες, εβδομάδες ή και μήνες για να εντοπίσει το πρόβλημα, ενώ περιορίζονται σημαντικά αν ο εντοπισμός και η αντίδραση είναι ζήτημα ωρών», παρατηρεί ο κ. **Νίκος Μουρτζίνος,** ειδικός στα προϊόντα ψηφιακής ασφάλειας της Cisco.

«Από τις επιθέσεις που μελετήσαμε, είδαμε ότι ο μέσος χρόνος αντίδρασης κινείται μεταξύ 100 και 200 ημερών. Η Cisco κατάφερε να τον μειώσει από τις δύο ημέρες στη μία, χρόνος ο οποίος για τις δικές μας απαιτήσεις και πάλι δεν είναι επαρκής, γι' αυτό και συνεχίζουμε να προσπαθούμε», συμπληρώνει ο ίδιος.

Πλήθος online συσκευών

Οπως εξηγεί, ουσιαστική πρόκληση για την προάσπιση της ψηφιακής ασφάλειας κάθε επιχείρησης και οργανισμού είναι πλέον το πλήθος των διασυνδεδεμένων συσκευών. Και ενώ παλαιότερα είχαμε να κάνουμε μόνο με servers και υπολογιστές, τώρα μπορεί να είναι οτιδήποτε συνδέεται στο Ιντερνετ, όπως smartphones, tablets, κάμερες, ή ακόμα συστήματα φωτισμού, κλιματισμού και PLCs (μονάδες αυτοματισμού) αν πρόκειται για εργοστάσια. Και καθώς οι online συσκευές αυξάνονται, διαπιστώνεται ότι το 92% αυτών έχει τρωτά σημεία, τα οποία προκύπτουν από τη φύση των μηχανών ή του λογισμικού. Αυτά συνήθως είναι που αναζητά κάποιος χάκερ για να διεισδύσει σε ένα σύστημα και να αποκτήσει απομακρυσμένη πρόσβαση. Μάλιστα, στο 36% αυτών των συσκευών είναι εγκατεστημένο όχι μόνο παλιό, αλλά λογισμικό για το οποίο έχει πάψει να παρέχεται υποστήριξη από τον κατασκευαστή ή τον προμηθευτή, με αποτέλεσμα τα όποια κενά ασφαλείας να μην μπορούν στο εξής να διορθωθούν. *«Και όσο κι αν ακούγεται περίεργο, συναντάμε περιπτώσεις όπου ο πελάτης αγνοεί την ύπαρξη εντός του δικτύου του αυτών των μηχανημάτων»*, λέει χαρακτηριστικά ο κ. Μουρτζίνος.

Ως αποτέλεσμα, λιγότερες από τις μισές (45%) επιχειρήσεις φαίνεται να έχουν εμπιστοσύνη στην ικανότητά τους να καθορίζουν το αντικείμενο μιας διαδικτυακής απειλής και να αποκαθιστούν τη ζημιά. Αλλά η συντριπτική πλειονότητα των οικονομικών και διοικητικών στελεχών συμφωνεί ότι οι ρυθμιστικές αρχές και οι επενδυτές αναμένουν από τις εταιρείες να παρέχουν μεγαλύτερη διαφάνεια σχετικά με μελλοντικούς κινδύνους για την ψηφιακή ασφάλεια. Παρ' όλα αυτά, πολλές εταιρείες αποφεύγουν όχι μόνο να δημοσιοποιούν, αλλά και να μοιράζονται με άλλες την εμπειρία που αποκομίζουν από την αντιμετώπιση ψηφιακών επιθέσεων, υπολογίζοντας πρωτίστως τον κίνδυνο φήμης έναντι του λειτουργικού κινδύνου.

Χρησιμοποιούν τα social media για να χτίσουν το προφίλ των θυμάτων τους

ΣΥΝΘΕΤΕΣ ΤΕΧΝΙΚΕΣ

ΠΟΛΛΕΣ ΦΟΡΕΣ ΟΙ κυβερνοεγκληματίες ξεκινάνε από επιθέσεις τύπου phishing, προσπαθώντας να ψαρέψουν τα θύματά τους, να τους αποσπάσουν στοιχεία που συνδέονται με την οικονομική διαχείριση και προχωράνε σε παραβιάσεις και υποκλοπές, την εγκατάσταση ransomware λογισμικού που κλειδώνει υπολογιστές και servers, οπότε απαιτούν λύτρα για την απελευθέρωσή τους ή την υφαρπαγή δεδομένων μεγάλου όγκου, τα οποία μπορεί να έχουν σημαντική αξία στη μαύρη αγορά - όπως αριθμοί πιστωτικών καρτών, πελατολόγια και φορολογικά δεδομένα. Αντλώντας στοιχεία από τα social media, οι χάκερ στοχεύουν εκείνους μέσα σε μια εταιρεία που πιθανότατα δεν έχουν την καλύτερη σχέση με την τεχνολογία.

ΟΙ ΣΥΓΧΡΟΝΟΙ ΨΗΦΙΑΚΟΙ εγκληματίες λειτουργούν και σαν ψυχολόγοι, χτίζοντας το προφίλ των υποψήφιων θυμάτων τους και αναζητώντας τους αδύναμους κρίκους ή τις πληροφορίες εκείνες που θα κάνουν ακόμα και κάποιον υποψιασμένο να πέσει στην παγίδα. Παράλληλα, κάποιες μορφές κακόβουλου λογισμικού είναι τόσο εξελιγμένες που μια εταιρεία θα πρέπει να έχει επενδύσει σε τελευταίας τεχνολογίας συστήματα προστασίας για να επιτύχει τον άμεσο εντοπισμό και την εξουδετέρωσή του. *«Τα προβλήματα γύρω από την ψηφιακή ασφάλεια έχουν να κάνουν με την αλλαγή του επιχειρηματικού μοντέλου. Πλέον ο καθένας μπορεί να συνδεθεί από οπουδήποτε στο εταιρικό δίκτυο, όπως και τα δεδομένα μέσω του cloud και του virtualization συνήθως βρίσκονται κάπου εκεί έξω. Αρα το να χτίσουμε ένα τείχος προστασίας και να προσπαθούμε να διαχωρίσουμε τους καλούς από τους κακούς δεν αρκεί. Επίσης, πλέον δεν αναφερόμαστε στην αντιμετώπιση γνωστών τύπων κακόβουλου λογισμικού, η οποία θα πρέπει να θεωρείται δεδομένη, αλλά σε στοχευμένες, αναβαθμισμένες απειλές μέσω λογισμικού που έχει σχεδιαστεί κατά περίπτωση και πολλές φορές έχει δοκιμαστεί προτού χρησιμοποιηθεί, ώστε να μην είναι ανιχνεύσιμο. Μιλάμε ουσιαστικά για μια βιομηχανοποίηση του χάκινγκ»*, υποστηρίζει ο κ. Μουρτζίνος της Cisco, αντιπροτείνοντας μέσω μιας νέας αρχιτεκτονικής δικτύου τη χαρτογράφηση υποδομών και τρωτών σημείων και την ανάλυση σε πραγματικό χρόνο της κίνησης δεδομένων, με στόχο τον ταχύτερο συσχετισμό γεγονότων που μπορεί να προκύπτουν από μια παραβίαση. Υπό το πρίσμα της παραδοχής ότι δεν είναι δυνατή η αποτροπή όλων των επιθέσεων.

ΕΤΣΙ ΩΣΤΕ ΑΠΟ τη στιγμή που εντοπιστεί τελικά κάποια απειλή να είναι δυνατή η αυτοματοποιημένη εξουδετέρωσή της και η ακολούθηση αντίστροφης πορείας για τον εντοπισμό των μολυσμένων σημείων.