Έκθεση της Symantec δείχνει ότι οι επιχειρήσεις αποτελούν πλέον σημαντικό στόχο ransomware επιθέσεων

Σύμφωνα με την πρόσφατη έκθεση **ISTR2016 Ransomware and Businesses** της **Symantec Corp**. (NASDAQ: SYMC), της μεγαλύτερης παγκοσμίως εταιρείας ασφάλειας στον κυβερνοχώρο, το **ransomware αναδείχθηκε ως μία από τις πιο επικίνδυνες απειλές** στον κυβερνοχώρο, τόσο για τις επιχειρήσεις και τους μεγάλους οργανισμούς, όσο και για τους καταναλωτές εν γένει, με τις παγκόσμιες απώλειες να φθάνουν πλέον τα εκατοντάδες εκατομμύρια δολάρια.

Τους τελευταίους 12 μήνες το ransomware έχει φτάσει σε ένα νέο επίπεδο ωριμότητας και απειλής. Σημαντικές «συμμορίες» ransomware είναι σε θέση να διοχετεύσουν το κακόβουλο λογισμικό τους σε εκατομμύρια υπολογιστές. Οι χρήστες που έχουν χτυπηθεί από ransomware βρίσκουν τα πολύτιμα δεδομένα τους κλειδωμένα με ισχυρή και συχνά αδιαπέραστη κρυπτογράφηση.

Η τελειότητα του επιχειρηματικού μοντέλου που χρησιμοποιεί το ransomware έχει δημιουργήσει μια νοοτροπία χιονοστιβάδας μεταξύ των επιτιθέμενων, καθώς καθημερινά αυξάνεται το χρηματικό ποσό που προσπαθούν να εκμαιεύσουν από τα θύματά τους. Οι αριθμοί παρουσιάζουν συνεχώς αυξητική τάση, με τον αριθμό των νέων οικογενειών ransomware που ανακαλύφθηκε το

2015 μόνο, να φτάνει τις 100 και ο μέσος όρος λύτρων που ζητούν οι επιτιθέμενοι είναι τα 679 δολάρια ΗΠΑ!
Οι επιθέσεις ενάντια σε επιχειρήσεις παρουσιάζει αύξηση με τις ευρείας κλίμακας επιθέσεις ransomware να παραμένουν η πιο διαδεδομένη μορφή της απειλής. Όπως αποδεικνύεται από δύο μελέτες περιπτώσεων που έγιναν στα πλαίσια της έκθεσης της Symantec, οι επιθέσεις αυτές χαρακτηρίζονται από υψηλό επίπεδο τεχνογνωσίας, ενώ χρησιμοποιούνται τεχνικές που βλέπουμε συχνότερα σε εκστρατείες κυβερνοκατασκοπίας.

Μία επιτυχημένη επίθεση σε έναν οργανισμό, μπορεί ενδεχομένως να μολύνει χιλιάδες υπολογιστές, προκαλώντας μαζική λειτουργική ζημιά και σοβαρή βλάβη στα έσοδα αλλά και στη φήμη. Μόλις οι συμμορίες του κυβερνοεγκλήματος δουν ορισμένες επιχειρήσεις να υποκύπτουν σε αυτές τις επιθέσεις και να πληρώνουν τα λύτρα, όλο και περισσότεροι εισβολείς ακολουθούν στην προσπάθεια να αρπάξουν το μερίδιό τους από τα πιθανά κέρδη.
Οι οργανισμοί θα πρέπει να είναι πλήρως ενημερωμένοι για τις απειλές στις οποίες τους θέτει το ransomware και να χτίζουν κατά προτεραιότητα πάνω στην ασφάλειά τους. Μία πολυεπίπεδη προσέγγιση σ την ασφάλεια ελαχιστοποιεί την πιθανότητα μόλυνσης, ενώ είναι επίσης ζωτικής σημασίας και η εκπαίδευση των τελικών χρηστών σχετικά με το ransomware, αφού και οι επικίνδυνοι κυβερνοεγκληματίες βελτιώνουν συνεχώς τις τακτικές επίθεσης που χρησιμοποιούν.

Συνοπτικά τα σημαντικότερα ευρήματα της έκθεσης είναι τα ακόλουθα:

- Ενώ οι ransomware επιθέσεις δρούσαν μέχρι σήμερα σε μεγάλο βαθμό αδιακρίτως, πλέον δείχνουν ένα αυξανόμενο ενδιαφέρον για στοχευμένες επιθέσεις σε επιχειρήσεις.
- Ένας μεγάλος αριθμός από ομάδες ransomware έχουν αρχίσει να χρησιμοποιούν προηγμένες τεχνικές επίθεσης, εμφανίζοντας ένα επίπεδο παρόμοιο με επιθέσεις κυβερνοκατασκοπίας.

- Ο τομέας των υπηρεσιών πλήττεται περισσότερο με ποσοστό 38%. Ακολουθούν οι κατασκευές και ο οικονομικός τομέας με 17%, ενώ οι ασφάλειες, η κτηματαγορά και η δημόσια διοίκηση βρίσκονται επίσης σε υψηλές θέσεις με ποσοστό 10%.
- Η μέση ζήτηση σε λύτρα υπερδιπλασιάστηκε και βρίσκεται στα 679$, από 294$ στα τέλη του 2015
- Ο αριθμός των νέων οικογενειών ransomware παρουσιάζει σταθερή αύξηση από το 2011 με το 2015 να καταγράφει υψηλό ρεκόρ αφού ανακαλύφθηκαν 100 νέες οικογένειες.
- Η έλευση του ransomware-as-a-service (RaaS) σημαίνει ότι ένας μεγαλύτερος αριθμός εγκληματιών του κυβερνοχώρου μπορεί να αποκτήσει το δικό του ransomware, ακόμη και με χαμηλά επίπεδα τεχνογνωσίας.
- Η στροφή προς το crypto-ransomware συνεχίζεται. Οι νέες παραλλαγές που έχουν ανακαλυφθεί μέχρι τώρα μέσα στο 2016 φτάνει στο 80%.
- Μεταξύ Ιανουαρίου 2015-Απριλίου 2016, οι ΗΠΑ έχουν πληγεί περισσότερο από το ransomware, κατέχοντας το 28% στην παγκόσμια κατάταξη. Ακολουθούν: Καναδάς, Αυστραλία, Ινδία, Ιαπωνία, Ιταλία, Ηνωμένο Βασίλειο, Γερμανία, Ολλανδία και Μαλαισία.

Συμβουλές για επιχειρήσεις και τελικούς χρήστες

- Νέες παραλλαγές ransomware εμφανίζονται σε τακτική βάση γι’ αυτό θα πρέπει να έχετε πάντα ενημερωμένο το λογισμικό ασφαλείας.
- Διατηρήστε το λειτουργικό σύστημα και τις υπόλοιπες εφαρμογές ενημερωμένα, αφού οι ενημερώσεις περιλαμβάνουν patches για ευπάθειες ασφάλειας ransomware που ανακαλύπτονται.
- Το ηλεκτρονικό ταχυδρομείο είναι μία από τις κύριες

μεθόδους διόδους για επιθέσεις. Διαγράψτε τυχόν ύποπτα e-mail που λαμβάνετε, ειδικά εάν περιέχουν συνδέσμους ή/και άγνωστα συνημμένα.

- Να είστε εξαιρετικά επιφυλακτικοί για κάθε συνημμένο αρχείο που φτάνει μέσω ηλεκτρονικού ταχυδρομείου του Microsoft Office και σας συμβουλεύει να ενεργοποιήσετε μακροεντολές για να δείτε το περιεχόμενό του.
- Δημιουργήστε αντίγραφα ασφαλείας σημαντικών δεδομένων για να καταπολεμήσετε αποτελεσματικά τις επιθέσεις από ransomware. Οι επιτιθέμενοι έχουν επιρροή πάνω στα θύματά τους κρυπτογραφώντας τα πολύτιμα αρχεία τους. Αν το θύμα έχει αντίγραφα ασφαλείας, μπορεί να αποκαταστήσει τα αρχεία του μόλις αντιληφθεί και «καθαρίσει» την επίθεση.

Υιοθετώντας μια πολυεπίπεδη προσέγγιση για την ασφάλεια, ελαχιστοποιείται η πιθανότητα μόλυνσης. Η Symantec διαθέτει μια ολοκληρωμένη στρατηγική που προστατεύει από το ransomware σε τρία στάδια: Την πρόληψη, τον περιορισμό και την ανταπόκριση.

1. **Πρόληψη**: Εργαλεία όπως τα Symantec Email security, Intrusion Prevention, Download Insight, Browser Protection, και Proactive Exploit Protection (PEP) μπορούν να προστατέψουν ολοκληρωμένα αλλά και να προλάβουν κακόβουλες επιθέσεις ransomware και όχι μόνο.
2. **Περιορισμός**: Σε περίπτωση μόλυνσης, ένα κρίσιμο βήμα είναι να περιοριστεί η εξάπλωση της προσβολής. Οι τεχνολογίες της Symantec που βασίζονται σε αρχεία διασφαλίζουν ότι κάθε αρχείο που έχει κατεβάσει ένας χρήστης στον υπολογιστή του δεν θα είναι σε θέση να εκτελεστεί άμεσα. Η Symantec διαθέτει μία ομάδα ασφάλειας 24/7 που είναι υπεύθυνη για τη συνεχή ανάπτυξη και βελτίωση θεμάτων που αφορούν το ransomware. Η ομάδα πραγματοποιεί συνεχή παρακολούθηση των ransomware οικογενειών και της αλυσίδας διανομής τους, προκειμένου να συλλέγονται όλα τα νέα δείγματα και να εξασφαλίζεται

ισχυρή πρόληψη και αναγνώριση.

3. **Ανταπόκριση**: Η ομάδα Symantec Incident Response (IR) είναι πάντα εκεί για να βοηθήσει τις επιχειρήσεις να ανταποκριθούν και να ανακτήσουν τα δεδομένα τους μετά από μια επίθεση ransomware.

Η πλήρης έκθεση της Symantec για την προστασία των επιχειρήσεων από το ransomware με τίτλο **Ransomware and Businesses 2016: An ISTR special report** διατίθεται προς download **εδώ!**