



Non-Stop: 0 αριθμός των χρηστών που δέχτηκαν επίθεση με ransomware προγράμματα κρυπτογράφησης μεγάλωσε κατά 2,6 φορές

Ο αριθμός των χρηστών του Διαδικτύου που αντιμετώπισε ransomware προγράμματα κρυπτογράφησης υπερδιπλασιάστηκε κατά το τρίτο τρίμηνο 2016, αγγίζοντας τα 821.865 άτομα, σύμφωνα με την τριμηνιαία έκθεση της Kaspersky Lab για την εξέλιξη των απειλών στον τομέα της Πληροφορικής. Ο αριθμός των ατόμων που έχουν δεχτεί επίθεση εξακολουθεί να αυξάνεται για το τρίτο τρίμηνο στη σειρά.

Το ransomware κρυπτογράφησης, κακόβουλο λογισμικό που κρυπτογραφεί τα αρχεία του θύματος και απαιτεί λύτρα σε αντάλλαγμα για την αποκρυπτογράφηση του αρχείου, εξακολουθεί να είναι ένα από τα πιο διαδεδομένα είδη δραστηριοτήτων με το οποίο ασχολούνται οι σύγχρονοι ψηφιακοί εγκληματίες. Έχει ένα σχετικά χαμηλό κόστος ανάπτυξης και μπορεί να αποδώσει ένα δυνητικά υψηλό εισόδημα αν οδηγήσει σε μια επιτυχημένη «μόλυνση».

Εκτός από την αύξηση του αριθμού των θυμάτων τους, οι εγκληματίες διερευνούν επίσης νέες γεωγραφικές περιοχές. Στο τρίτο τρίμηνο, οι πέντε χώρες με το υψηλότερο ποσοστό χρηστών που δέχτηκαν επίθεση με ransomware κρυπτογράφησης ήταν η Ιαπωνία (4,83%), η Κροατία (3,71%), η Νότια Κορέα (3,36%), η Τυνησία (3,22%) και η Βουλγαρία (3,2%). Το προηγούμενο τρίμηνο, την πρώτη θέση κατείχε η Ιαπωνία, ενώ στη δεύτερη, την τρίτη και την τέταρτη θέση βρισκόνταν η Ιταλία, το

Τζιμπουτί και το Λουξεμβούργο αντίστοιχα. Αυτές οι τρεις χώρες εγκατέλειψαν την πρώτη πεντάδα στο τρίτο τρίμηνο για να δώσουν τη θέση τους σε άλλες.

Ο βασικός υπαίτιος της αύξησης του αριθμού των χρηστών που δέχτηκαν επίθεση ήταν το Trojan-Downloader.JS.Cryptoload, μια οικογένεια downloaders γραμμένη σε γλώσσα JavaScript και ικανή να «κατεβάζει» διαφορετικές οικογένειες crypto ransomware. Στις πιο διαδεδομένες από αυτές το τρίτο τρίμηνο περιλαμβάνονται το CTB-Locker (28,34% χρηστών που δέχτηκαν επίθεση), το Locky (9,6%) και το CryptXXX (8,95%).

«Τα προγράμματα crypto ransomware συνεχίζουν να είναι μια από τις πιο επικίνδυνες απειλές, τόσο για ιδιώτες χρήστες όσο και για επιχειρήσεις. Η πρόσφατη άνοδος στον αριθμό των χρηστών που δέχτηκαν επίθεση μπορεί να έχει προκληθεί από το γεγονός ότι ο αριθμός των τροποποιήσεων των ransomware προγραμμάτων που ανιχνεύσαμε στο τρίτο τρίμηνο (περισσότερες από 32.000 τροποποιήσεις) ήταν 3,5 φορές μεγαλύτερος από ό, τι στο δεύτερο τρίμηνο. Αυτό μπορεί να οφείλεται στο γεγονός ότι οι εταιρείες ασφάλειας επενδύουν στις μέρες μας πολλούς πόρους για να είναι σε θέση να ανιχνεύσουν νέα δείγματα ransomware όσο το δυνατόν γρηγορότερα. Οι εγκληματίες θα πρέπει, συνεπώς, να αποφύγουν τον εντοπισμό, δημιουργώντας περισσότερες νέες τροποποιήσεις του κακόβουλου λογισμικού τους», σχολίασε ο Fedor Sinitsyn, ransomware expert της Kaspersky Lab.

Τα άλλα βασικά πορίσματα της Έκθεσης «IT Threat Evolution in Q3» περιλαμβάνουν:

- Σύμφωνα με τα στοιχεία του Kaspersky Security Network, στο τρίτο τρίμηνο οι λύσεις της Kaspersky Lab ανίχνευσαν και απώθησαν συνολικά 171.802.109 κακόβουλες επιθέσεις από διαδικτυακές πηγές παγκοσμίως. Είναι ελαφρώς λιγότερες σε σχέση με το προηγούμενο τρίμηνο, κατά τη διάρκεια του οποίου εμποδίστηκαν 171.895.830 επιθέσεις.
- Από αυτές, 45.169.524 ήταν κακόβουλα URLs που φιλοξενούσαν 12.657.673 κακόβουλα αντικείμενα όπως

σενάρια, exploits, εκτελέσιμα αρχεία κ.λπ.

- Ο αριθμός των χρηστών που δέχτηκαν επίθεση με τραπεζικά κακόβουλα προγράμματα αυξήθηκε κατά 5,8% και ανήλθε στα 1.198.264 θύματα.
- Τα προγράμματα περιήγησης και τα λειτουργικά συστήματα Android παραμένουν τα λογισμικά που δέχονται πιο συχνά επιθέσεις όταν πρόκειται για exploits. Το 45% των exploits που ανιχνεύτηκαν από την Kaspersky Lab είχαν ως στόχο browsers, και το 19% αυτών των κακόβουλων προγραμμάτων δημιουργήθηκαν για να εκμεταλλευτούν τις αδυναμίες του δημοφιλοφύς Android λειτουργικού συστήματος.

Για περισσότερες πληροφορίες σχετικά με τις πιο σημαντικές αλλαγές στο τοπίο των ψηφιακών απειλών για το διάστημα Ιούλιος-Σεπτέμβριος 2016, μπορείτε να διαβάσετε την πλήρη έκθεση στον ειδικό ιστότοπο Securelist.com (Επισκόπηση & Στατιστικά στοιχεία)