Οι καλοκαιρινές επιθέσεις τύπου «watering-hole» του StrongPity παγίδευσαν χιλιάδες χρήστες που αναζητούσαν κρυπτογράφηση

Ένας αόρατος απειλητικός φορέας, γνωστός και ως StrongPity, πέρασε το καλοκαίρι προσελκύοντας χρήστες λογισμικού κρυπτογράφησης σε «watering holes» και «μολυσμένα» προγράμματα εγκατάστασης, σύμφωνα με εργασία που παρουσιάστηκε στο Virus Bulletin, από τον ερευνητή ασφάλειας της Kaspersky Lab Kurt Baumgartner. Οι χρήστες στην Ιταλία και το Βέλγιο ήταν αυτοί που επλήγησαν περισσότερο, αλλά επηρεάστηκαν επίσης και χρήστες στην Τουρκία, τη Βόρεια Αφρική και τη Μέση Ανατολή.

Το StrongPity είναι ένας τεχνικά ικανός φορέας επιθέσεων τύπου APT, που ενδιαφέρεται για κρυπτογραφημένα δεδομένα και επικοινωνίες. Κατά τη διάρκεια των τελευταίων μηνών, η Kaspersky Lab παρατήρησε μια σημαντική κλιμάκωση των επιθέσεων του σε χρήστες που αναζητούν δύο πολύ σημαντικά εργαλεία κρυπτογράφησης: το αρχείο WinRAR και το σύστημα κρυπτογράφησης TrueCrypt.

Το κακόβουλο λογισμικό StrongPity περιλαμβάνει στοιχεία που δίνουν στους επιτιθέμενους τον πλήρη έλεγχο του συστήματος του θύματος. Ουσιαστικά τους δίνει τη δυνατότητα να κλέψουν το περιεχόμενο του δίσκου αλλά και να «κατεβάσουν» πρόσθετες μονάδες για να συγκεντρώσουν επικοινωνίες και επαφές. Η

Kaspersky Lab έχει μέχρι στιγμής εντοπίσει επισκέψεις σε ιστότοπους του StrongPity και την παρουσία εργαλείων του σε περισσότερα από χίλια συστήματα-στόχους.

«Watering holes» και «μολυσμένα» προγράμματα εγκατάστασης

Για να παγιδεύσουν τα θύματα τους, οι επιτιθέμενοι έφτιαξαν ψεύτικες ιστοσελίδες. Στη μία περίπτωση, μετέφεραν δύο γράμματα σε ένα domain name για να ξεγελάσουν τους πελάτες νομίζοντας ότι ήταν ένας επίσημος ιστότοπος εγκατάστασης του λογισμικού WinRAR. Στη συνέχεια, τοποθέτησαν έναν περίοπτο σύνδεσμο σε μία τοποθεσία διανομής WinRAR στο Βέλγιο, προφανώς αντικαθιστώντας τον «προτεινόμενο» σύνδεσμο της ιστοσελίδας με εκείνη του κακόβουλου domain. Καθώς οι επισκέπτες πλοηγούνταν σε αυτή την ιστοσελίδα, αυτό οδηγούσε τους ανυποψίαστους χρήστες στο «μολυσμένο» πρόγραμμα εγκατάστασης του StrongPity. Η πρώτη ανίχνευση επιτυχημένης ανακατεύθυνσης από την Kaspersky Lab έγινε στις 28 Μαΐου 2016.

Σχεδόν παράλληλα, στις 24 Μαΐου, η Kaspersky Lab άρχισε να εντοπίζει μία κακόβουλη δραστηριότητα σε μια ιταλική ιστοσελίδα διανομής WinRAR. Στην περίπτωση αυτή, ωστόσο, οι χρήστες δεν ανακατευθύνονταν σε μια απατηλή ιστοσελίδα, αλλά δέχονταν το κακόβουλο πρόγραμμα εγκατάστασης του StrongPity απευθείας από την ιστοσελίδα του διανομέα.

Το StrongPity ανακατεύθυνε επίσης επισκέπτες δημοφιλών ιστοσελίδων με δωρεάν λογισμικό στα προγράμματα εγκατάστασης του TrueCrypt που είχαν «μολυνθεί» από Trojan. Η δραστηριότητα αυτή βρισκόταν ακόμα σε εξέλιξη στα τέλη Σεπτεμβρίου.

Οι κακόβουλες συνδέσεις από τις ιστοσελίδες διανομής WinRAR έχουν πλέον αρθεί, αλλά μέχρι και το τέλος του Σεπτεμβρίου η κακόβουλη ιστοσελίδα TrueCrypt λειτουργούσε ακόμα.

Γεωγραφία των επιθέσεων

Τα δεδομένα της Kaspersky Lab αποκαλύπτουν ότι μέσα σε μία

εβδομάδα το κακόβουλο λογισμικό που παρέχεται από την ιστοσελίδα του διανομέα στην Ιταλία εμφανίστηκε σε εκατοντάδες συστήματα σε όλη την Ευρώπη και τη Βόρεια Αφρική/Μέση Ανατολή, με πολλές περισσότερες πιθανές «μολύνσεις». Κατά τη διάρκεια του καλοκαιριού, η Ιταλία (87%), το Βέλγιο (5%) και η Αλγερία (4%) επλήγησαν περισσότερο. Η γεωγραφία των θυμάτων από το «μολυσμένο» ιστότοπο στο Βέλγιο ήταν παρόμοια, με τους χρήστες στο Βέλγιο να αντιπροσωπεύουν το ήμισυ (54%), με πάνω από 60 επιτυχημένες επιθέσεις.

Οι επιθέσεις σε χρήστες μέσω της δόλιας ιστοσελίδας TrueCrypt φτάνουν μέχρι και το Μάιο του 2016, με το 95% των θυμάτων να βρίσκεται στην Τουρκία.

«Οι τεχνικές που χρησιμοποιήθηκαν από αυτόν τον απειλητικό φορέα είναι αρκετά έξυπνες. Μοιάζουν με την προσέγγιση που υιοθετήθηκε στις αρχές του 2014 από τις APT επιθέσεις Crouching Yeti / Energetic Bear, στην οποία συμμετείχαν νόμιμα προγράμματα εγκατάστασης λογισμικού για συστήματα βιομηχανικού ελέγχου που είχαν «μολυνθεί» από Trojan και έθεταν σε κίνδυνο γνήσιες ιστοσελίδες διανομής λογισμικού. Αυτές οι τακτικές είναι μια ανεπιθύμητη και επικίνδυνη τάση που η βιομηχανία της ασφάλειας πρέπει να αντιμετωπίσει. Η αναζήτηση για προστασία της ιδιωτικής ζωής και της ακεραιότητας των δεδομένων δεν θα πρέπει να εκθέτουν το άτομο σε επιζήμιες «waterholes». Οι επιθέσεις τύπου «waterhole» είναι εγγενώς ασαφείς και ελπίζουμε να τονώσουμε τη συζήτηση γύρω από την ανάγκη για ευκολότερη και βελτιωμένη επαλήθευση της παράδοσης εργαλείων κρυπτογράφησης», δήλωσε ο Kurt Baumgartner, , Principal Security Researcher της Kaspersky Lab.

Η Kaspersky Lab εντοπίζει όλα τα συστατικά του StrongPity με τις ονομασίες: HEUR:. Trojan.Win32.Strong Pity.gen και Trojan.Win32.StrongPity * και ως άλλες γενικές ανιχνεύσεις.

Για περισσότερες πληροφορίες σχετικά με τις επιθέσεις τύπου «watering hole» του StrongPity, μπορείτε να επισκεφτείτε τον ειδικό ιστότοπο Securelist.com.

Για πληροφορίες σχετικά με τον μετριασμό απειλών με «μολυσμένο» λογισμικό κρυπτογράφησης, μπορείτε να επισκεφτείτε το blog Kaspersky Business.