30 Ιουλίου 2015

Operation Kofer: Ransomware με συμπεριφορά χαμαιλέοντα!

/ Πεμπτουσία

Image not found or type unknown

ransomware

Image not found or type unknown

Την εμφάνισή της στο κυβερνοχώρο έκανε τεράστια επιχείρηση *ransomware*, που ονομάστηκε *“Operation Kofer”*— η οποία έχει την δυνατότητα να μεταλλάσσεται για να ξεγελάει τους μηχανισμούς εντοπισμού.

Οι ερευνητές της *Cybereaon Labs*, αφού εξέτασαν διάφορες εκδοχές του *Kofer ransomware* απ’ όλο τον κόσμο, ανακάλυψαν πως αυτές μοιράζονται τις ίδιες τεχνικές κατασκευής και παράδοσης αλλά ενσωματώνουν ως επίσης τυχαίες μεταβλητές ώστε να αποφεύγουν το static-signature και την hash-based ανίχνευση. Το γεγονός αυτό οδήγησε την ομάδα των ερευνητών να πιστεύουν πως όλες οι εκδοχές δημιουργήθηκαν από την ίδια ομάδα hacker η οποία χρησιμοποίησε συγκεκριμένο αλγόριθμο ώστε να αναμείξει και να ταιριάξει διαφορετικά τα συστατικά, δίνοντας έτσι στο ransomware δυνατότητες διαφυγής παρόμοιες με APT.

Τα δείγματα του ***Kofer*** που ανέλυσαν οι ειδικοί, είχαν διαφορετικά hashes και χαρακτηριστικά, αλλά τα ίδια γνωρίσματα και ιδιότητες, όπως τα *fake icons*, τα πλαστά ονόματα αρχείων, και ένα συγκεκριμένο packaging pattern, το οποίο συνδέει τα δείγματα, που θα φαίνονταν άσχετα μεταξύ τους υπό άλλες συνθήκες, κάτω από μια μοναδική επιχείρηση. Επιπλέον, στους μηχανισμούς που βοηθούν στην αποφυγή της ανίχνευσης από sandboxes και δυναμικά εργαλεία ανίχνευσης, οι παραλλαγές του Kofer, περιλαμβάνουν επίσης διακοσμητικά στοιχεία που έχουν ως στόχο την παραπλάνηση των ερευνητών.

«Το γεγονός πως οι παραλλαγές του Kofer προέρχονται από μόνο μια πηγή είναι δείγμα εμπορευματοποίησης του ransomware σε ένα εντελώς νέο επίπεδο», αναφέρει ο Uri Sternfeld, της Cybereason.

«Η Operation Kofer, εμφανίζεται να είναι η πρώτη “drive-by” επιχείρηση ransomware, που ενσωματώνει ένα επίπεδο πολυπλοκότητας APT/nation-state, καθιστώντας το προϊόν της όλο και μεγαλύτερη απειλή για τις εταιρείες. Όσον αφορά τον ανεξέλεγκτο πολλαπλασιασμό των παραλλαγών, βρέθηκαν όλες και συγκρίθηκαν τις προηγούμενες εβδομάδες, ενώ δημιουργούνται πιθανότατα και νέες κάθε λίγες μέρες ή και ώρες!

Η *Cybereason* πιστεύει πως η Operation Kofer, έχει ήδη πανευρωπαϊκή παρουσία, όπως επιβεβαιώνουν οι ερευνητές, που εντόπισαν εκδοχές στηην Ισπανία, την Πολωνία, την Ελβετία την Τουρκία αλλά και άλλες.

Πηγή: SecNews.gr