14 Ιουνίου 2015

Locker: Εξελιγμένο Ransomware μολύνει υπολογιστές και δρα σε προκαθορισμένο χρόνο

/ Πεμπτουσία

Image not found or type unknown

ransomware

Ερευνητές ασφάλειας έχουν εντοπίσει ένα ransomware με δυνατότητες κρυπτογράφησης αρχείων, που ονομάζεται Locker, το οποίο εισέρχεται στους παραβιασμένους υπολογιστές σε κατάσταση αναμονής και ενεργοποιείται σε συγκεκριμένο χρονικό διάστημα που ορίζεται από τον εισβολέα.

Αυτή η προσέγγιση δεν έχει εντοπιστεί σε άλλα κακόβουλα προγράμματα του ιδίου

τύπου, και δεν είναι σαφές γιατί οι επιτιθέμενοι καθυστερούν τη διαδικασία κρυπτογράφησης των αρχείων των θυμάτων.

Μια πιθανή εξήγηση είναι ότι ίσως η διανομή του ransomware ξεκίνησε πριν από τη δημιουργία των απαραίτητων υποδομών για την αποθήκευση των κλειδιών αποκρυπτογράφησης των αρχείων και παράδοσή τους στα θύματα που καταβάλλουν τα ζητούμενα λύτρα.

Επιπλέον, με την υιοθέτηση αυτής της μεθόδου, οι απατεώνες καθιστούν δυσκολότερο τον εντοπισμό του χρόνου μόλυνσης και των μεθόδων διανομής του κακόβουλου λογισμικού, το οποίο διαδίδεται μέσω spam e-mails που παραπέμπουν σε κακόβουλη τοποθεσία που φιλοξενεί το Locker ή μέσω επιθέσεων drive-by που βασίζονται σε κακόβουλες διαφημίσεις και παραβιασμένες ιστοσελίδες.

Σύμφωνα με μια ανάλυση της εταιρείας Bleeping Computer, τα αρχεία στους υπολογιστές που έχουν μολυνθεί με το Locker ξεκίνησαν να κρυπτογραφούνται στις 25 Μαΐου τα μεσάνυχτα (τοπική ώρα). Σε αντίθεση με τις απειλές του ιδίου είδους, το Locker δεν αλλάζει την επέκταση των επηρεαζόμενων αρχείων τα οποία εμφανίζονται ανέγγιχτα μέχρι να τα ανοίξει ο χρήστης.

Επιπλέον, το κακόβουλο λογισμικό διαγράφει τα αντίγραφα που δημιουργούνται από την υπηρεσία Shadow Copy των Windows, αλλά μόνο στη μονάδα δίσκου συστήματος (system drive). Τα αρχεία που είναι αποθηκευμένα σε οποιοδήποτε άλλο partition μπορούν να ανακτηθούν. Επιπλέον, υπάρχουν αναφορές ότι η διαγραφή των “Shadow Copies” δεν είναι πάντα επιτυχής και τα δεδομένα μπορούν να αποκατασταθούν με ειδικό λογισμικό.

Μετά την κρυπτογράφηση όλων των δεδομένων (κυρίως εγγράφων και εικόνων), το Locker εμφανίζει το μήνυμα των λύτρων, απαιτώντας 0,1 bitcoins ($ 24 / € 22) σε αντάλλαγμα για το κλειδί αποκρυπτογράφησης, το οποίο είναι αποθηκευμένο σε έναν διακομιστή κρυμμένο στο δίκτυο ανωνυμίας Tor.

Πηγή: SecNews.gr