Στην Ελλάδα διασπείρουν εκβιαστές χάκερ τον παγ-κοσμίως γνωστό ιό «Ransomware». Πρόκειται για έναν ισχυρό ιό που «παραλύει» τους υπολογιστές, καθώ ς κρυπτογραφεί αρχεία (βίντεο, φωτογραφίες,...

αρχεία word), τα οποία οι χρήστες δεν μπορούν να επανακτήσουν ούτε με τη βοήθεια ειδικώ ν. Ο μόνος τρόπος «ξεκλειδώ ματος» είναι να υποκύψουν στον εκβιασμό και να πληρώ σουν «λύτρα» σε ηλεκτρονικό νόμισμα (bitcoin).

Οι «black» (με κακόβουλα κίνητρα) χάκερ στέλνουν χιλιάδες e-mail με τον ιό και όποιος χρήστης κάνει το λάθος να τα ανοίξει τότε τα αρχεία του υπολογιστή του αχρηστεύονται. Η επιφάνεια εργασίας χακάρεται αυτομάτως και εμφανίζεται ένα μήνυμα με πράσινα γράμματα που γράφει: «Τα αρχεία σας, οι φωτογραφίες σας, τα δεδομένα σας και άλλοι σημαντικοί φάκελοι έχουν κρυπτογραφηθεί από το 'Cerber Ransomware'! Αν καταλαβαίνεις το πόσο σημαντικό είναι το πλήγμα αυτό σου προτείνουμε να κλικάρεις τα λινκ που σου προτείνουμε για να βρεις τις οδηγίες μέσω των οποίων μπορεί να ανακτήσεις τα αρχεία σου».

Το επόμενο βήμα είναι η απαίτηση «λύτρων» που κυμαίνονται από 10 bitcoins (5.731 ευρώ) έως 500 bitcoins (286.571 ευρώ).

«Έχω πάρα πολλούς πελάτες που έπεσαν θύματα διαδικτυακού εκβιασμού λόγω του συγκεκριμένου ιού. Δυστυχώ ς δεν μπορείς να επανακτήσεις τα αρχεία σου, τα οποία έχουν κρυπτογραφηθεί. Ο μόνος τρόπος να τα πάρεις πίσω είναι να πληρώ σεις, χωρίς σε καμία περίπτωση να είσαι σίγουρος ότι θα σου τα αποκρυπτογραφήσουν. Οι έρευνες της εταιρίας Cisco δείχνουν ότι η πιθανότητα επανάκτησης σε περίπτωση πληρωμής είναι 55%. Για το λόγο αυτό οι χρήστες πρέπει πάντα να κρατούν backup (αντίγραφα των αρχείων τους)», λέει πληροφορικός που ασχολείται με την επιδιόρθωση υπολογιστώ ν που «χτυπήθηκαν» από τον ιό.

Ο ιός «Ransomware» έχει απασχολήσει τις διωκτικές Αρχές σχεδόν σε όλο τον κόσμο. Ως «αντίδοτο» έχει δημιουργηθεί με τη συνδρομή της Europol και εταιριώ ν-κολοσσώ ν στον κλάδο της πληροφορικής η ιστοσελίδα «www.nomoreransom.org».

Στον συγκεκριμένο ιστότοπο μπορούν οι χρήστες να λάβουν οδηγίες για το πώ ς

μπορούν να αντιμετωπίσουν μία επίθεση χωρίς να ενδώ σουν στον εκβιασμό των χάκερ.
Δίνεται, επίσης, η δυνατότητα στα θύματα να επισυνάψουν ένα ανενεργό –λόγω του χάκινγκ- αρχείο τους για να «ταυτοποιηθεί» ο ιός σε περίπτωση που αυτό είναι δυνατό. Η απάντηση της ιστοσελίδας μπορεί να είναι «λυπούμαστε δεν μπορούμε να βοηθήσουμε» ή η διάθεση οδηγιώ ν αντιμετώ πισης.

HuffPost Greece