Η Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος, ενημερώνει τους πολίτες, για την εμφάνιση ενός **νέου κακόβουλου λογισμικού**, που ονομάστηκε ως CTB-Locker (Curve-Tor-Bitcoin Locker) και ανιχνεύεται ως «Critroni», ενώ αποτελεί την εξέλιξη του γνωστού κακόβουλου λογισμικού Crypto locker Ransomware.

Ειδικότερα, το νέο κακόβουλο λογισμικό, με την εγκατάστασή του στο λειτουργικό σύστημα, κρυπτογραφεί διαφόρους τύπους αρχείων (φωτογραφίες, βίντεο, έγγραφα κ.α.).

Στη συνέχεια, εμφανίζει ένα μήνυμα "μπλοκαρίσματος" του υπολογιστή, ενημερώνοντας το χρήστη ότι, για να ξεκλειδωθούν τα αρχεία του, πρέπει να καταβληθεί χρηματικό ποσό (ransom).

Η καταβολή του χρηματικού ποσού γίνεται με τη χρήση του ψηφιακού νομίσματος bitcoin (BTC). Εάν το θύμα δεν διαθέτει bitcoins, οι δημιουργοί του λογισμικού παρέχουν οδηγίες για την απόκτησή τους.

Όπως στο Cryptolocker, το κακόβουλο λογισμικό «Critroni» δημιουργεί ένα ζεύγος δημόσιου

και ιδιωτικού «κλειδιού», που ουσιαστικά είναι κωδικοί αριθμοί, οι οποίοι «ξεκλειδώνουν» τον «μολυσμένο» υπολογιστή.

Το ένα «κλειδί» (δημόσιο) αποθηκεύεται στο μολυσμένο σύστημα και δίνεται στο χρήστη ελεύθερα, χωρίς πληρωμή.

Το άλλο «κλειδί» (ιδιωτικό) αποθηκεύεται στο διακομιστή διοίκησης και ελέγχου (C&C servers) και δίδεται από τους δράστες στο θύμα για να αποκρυπτογραφηθούν τα αρχεία, μόνο μετά την καταβολή του χρηματικού ποσού που έχει ζητηθεί και συμφωνηθεί, το οποίο είναι πάντα σε ψηφιακό νόμισμα «bitcoin».

Οι διαδικασίες και οι τρόποι εξάπλωσης του ανωτέρω κακόβουλου λογισμικού είναι παρόμοιες με αυτή του κακόβουλου λογισμικού Cryptolocker.

Καλούνται οι χρήστες του διαδικτύου να είναι ιδιαίτερα προσεκτικοί και να λαμβάνουν τα ακόλουθα μέτρα προστασίας για την αποφυγή προσβολής από το προαναφερόμενο κακόβουλο λογισμικό.

Συγκεκριμένα:

- να ελέγχουν και να έχουν πάντοτε ενημερωμένη την έκδοση του λειτουργικού τους συστήματος,

- να δημιουργούν αντίγραφα ασφαλείας των αρχείων της συσκευής τους (backup) σε τακτά χρονικά διαστήματα, σε εξωτερικό μέσο αποθήκευσης,

- να χρησιμοποιούν εφαρμογές ασφαλείας, όπως antivirus, το οποίο πρέπει να είναι πάντοτε ενημερωμένο και

- να μην ανοίγουν τους συνδέσμους (links) και να μην κατεβάζουν τα συνημμένα αρχεία, που περιέχονται σε μηνύματα ηλεκτρονικού ταχυδρομείου, για τα οποία δεν γνωρίζουν με βεβαιότητα τον αποστολέα και το περιεχόμενο του συνημμένου αρχείου.

Υπενθυμίζεται ότι για ανάλογα περιστατικά, οι πολίτες μπορούν να επικοινωνούν με την Διεύθυνση Δίωξης Ηλεκτρονικού Εγκλήματος στα ακόλουθα στοιχεία επικοινωνίας:

- Τηλεφωνικά στο: 210-6476464

- Στέλνοντας e-mail στο: ccu@cybercrimeunit.gov.gr