Νέα ενημέρωση της Kaspersky Lab για τις επιθέσεις ransomware «ExPetr»

Η ανάλυση μας δείχνει πως λίγες ελπίδες υπάρχουν για να ανακτήσουν τα θύματα των επιθέσεων ransomware «ExPetr» τα δεδομένα τους.

Έχοντας αναλύσει τον υψηλού επιπέδου κώδικα της ρουτίνας κρυπτογράφησης, έχουμε καταλάβει πως μετά από την κρυπτογράφηση δίσκου, ο φορέας απειλής δεν μπορούσε να αποκρυπτογραφήσει τους δίσκους των θυμάτων. Για να αποκρυπτογραφήσουν το δίσκο ενός θύματος, οι φορείς απειλής χρειάζονται το αναγνωριστικό εγκατάστασης. Σε προηγούμενες εκδόσεις από παρόμοια ransomware όπως το Petya/Mischa/GoldenEye αυτό το αναγνωριστικό εγκατάστασης περιέχει πληροφορίες απαραίτητες για την επαναφορά.

Το ExPetr δεν το έχει αυτό, το οποίο σημαίνει πως ο φορέας απειλής δεν μπορούσε να εξάγει τις απαραίτητές πληροφορίες για την αποκρυπτογράφηση. Με λίγα λόγια, τα θύματα δεν μπορούσαν να επαναφέρουν τα δεδομένα τους.

Περαιτέρω τεχνολογικές λεπτομέρειες θα παρέχονται στο blog μας, το οποίο θα ενημερώνεται διαρκώς.