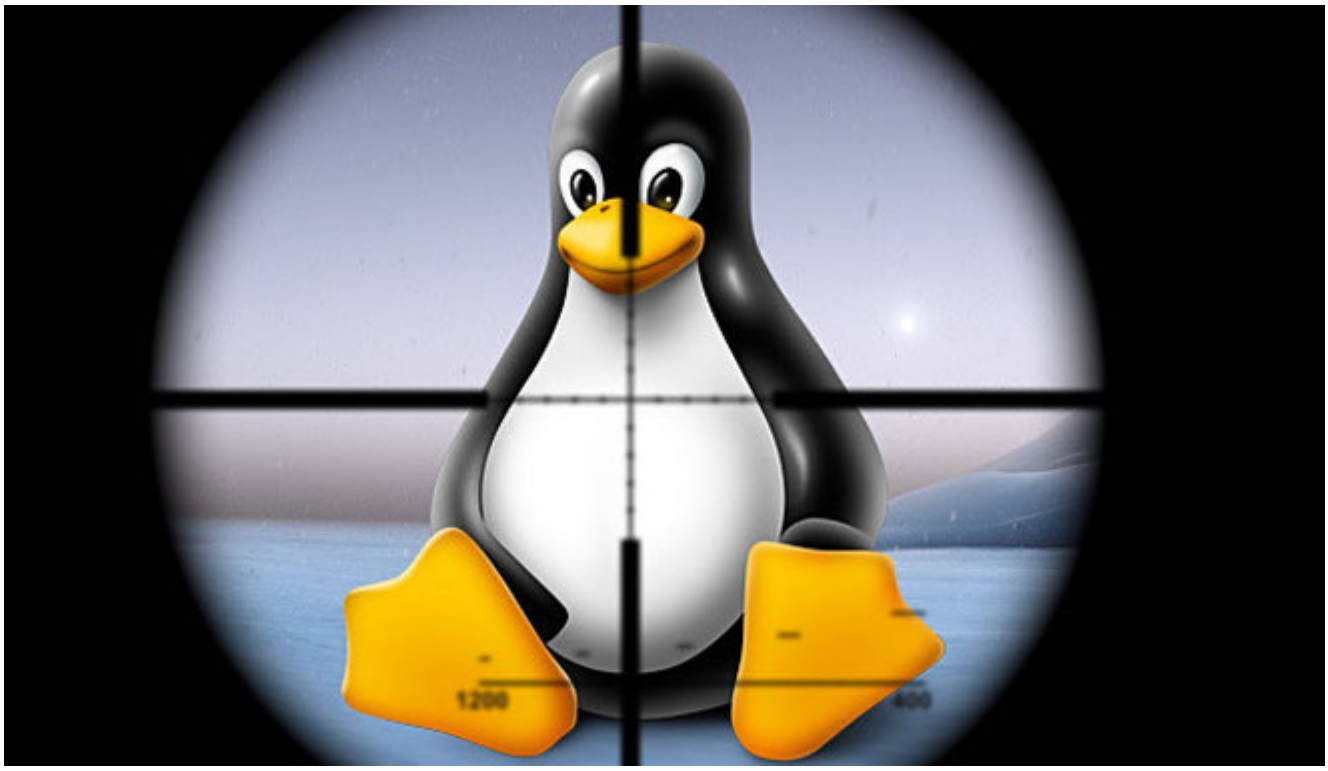
3 Ιανουαρίου 2016

Rekoobe: νέο malware – κίνδυνος για χρήστες Linux

/ Πεμπτουσία

Image not found or type unknown



Ειδικοί στην Ρώσικη εταιρεία anti-virus, Dr.Web, ανακάλυψαν το Rekoobe, ένα νέο malware που στοχεύει τα συστήματα Linux. Οι ειδικοί της Dr.Web ανακάλυψαν το Rekoobe Trojan τον Οκτώβρη, και στη συνέχεια οι ειδικοί αναλυτές ερευνούσαν την νέα απειλή για τους επόμενους δύο μήνες.

Το Rekoobe Trojan αρχικά αναπτύχθηκε για να επηρεάσει μόνο τα Linux SPARC architectures, ενώ αργότερα αναβαθμίστηκε για να στοχεύσει τα Linux PCs που τρέχουν σε intel chips, και σε 32 bit αλλά και σε 64-bit architectures. Οι ειδικοί εξηγούν πως το Rekoobe Trojan είναι πολύ απλό, αλλά πολύ δύσκολο να εντοπισθεί. Η κρυπτογράφηση του malware του επιτρέπει να προστατεύει το configuration file και τα data που ανταλλάσσει με τον C&C server.

“Το Linux.Rekoobe.1 χρησιμοποιεί ένα κρυπτογραφημένο configuration file. Όταν

αυτό το αρχείο διαβασθεί, το Trojan περιοδικά επικοινωνεί με τον C&C server για να πάρει οδηγίες. Κάτω από ειδικές περιπτώσεις, η σύνδεση με τον server γίνεται μέσω ενός proxy server.” Αναφέρεται στο blog post που δημοσιεύθηκε από την Dr.Web. “Το malware εξάγει τα authorization data από το configuration file του. Όλες οι πληροφορίες που αποστέλλονται και λαμβάνονται χωρίζονται σε ξεχωριστά blocks. Κάθε block κρυπτογραφείται και περιλαμβάνει την δική του υπογραφή.”

Η ανάλυση του Rebooke αποκάλυψε πως θα μπορούσε να μοιράζει κακόβουλα payloads στα μολυσμένα συστήματα, προκειμένου να επιτευχθεί η πλήρης έκθεση του στόχου.

Δυστυχώς οι δημιουργοί του Rekoobe έχουν ήδη μεταφέρει το Trojan και σε άλλα λειτουργικά συστήματα, συμπεριλαμβανομένων των Android, Mac OS X και Windows.

Παρόλο που πάρα πολλοί χρήστες θεωρούν τα συστήματα Linux απρόσβλητα από κακόβουλα λογισμικά, άλλες απειλές έχουν ανακαλυφθεί πρόσφατα, όπως το ransomware Linux.Encoder.1.

Πηγή: secnews.gr