Οι χρήστες του Facebook, του Chrome και των κρυπονομισμάτων πρέπει να έχουν υπόψη τους ένα νέο malware που ονομάζεται FacexWorm το οποίο μολύνει τα θύματα με σκοπό την κλοπή κωδικών πρόσβασης, την κλοπή κρυπτονομισμάτων, την εκτέλεση cryptomining scripts και άλλα.

Η νέα αυτή παραλλαγή εντοπίστηκε στα τέλη Απριλίου από τους ερευνητές της Trend Micro και φαίνεται να σχετίζεται με δύο άλλες εκστρατείες spam του Facebook Messenger, μια που πραγματοποιήθηκε τον περασμένο Αύγουστο και μια άλλη το Δεκέμβριο του 2017, εξαπλώνοντας το κακόβουλο λογισμικό Digmine.

Η αρχή στην νέα παραλλαγή παραμένει η ίδια αφού συνήθως ξεκινάει με τους χρήστες να λαμβάνουν έναν ανεπιθύμητο σύνδεσμο μέσω του Facebook Messenger. Κάνοντας κλικ στο σύνδεσμο μεταφέρονται σε μια ιστοσελίδα που μιμείται το YouTube, το οποίο προσπαθεί να εξαπατήσει τον χρήστη για να εγκαταστήσει μια επέκταση Chrome με θέμα το YouTube.

Η Trend Micro αναφέρει ότι ανέλυσε την επέκταση αυτή και διαπίστωσε πολλές κακόβουλες λειτουργίες ωστόσο η συγκεκριμένη αφορά χρήστες που έχουν πρόσβαση σε λογαριασμούς Google, Coinhive ή MyMonero. Τα διαπιστευτήρια στην συνέχεια αποστέλλονται στους διακομιστές του FacexWorm.

Επιπλέον η παράνομη επέκταση ανακατευθύνει αυτόματα τους χρήστες σε μια ιστοσελίδα προτρέποντας τους να στείλουν ένα μικρό ποσό απο το κρυπτονόμισμα Ether για να επαληθεύσουν τον λογαριασμό τους Η επέκταση περιλαμβάνει συνολικά μια λίστα με 52 ιστότοπους.

Τρίτον, η επέκταση εισάγει ένα cryptomining script, φορτώνοντας το Coinhive miner, το οποίο χρησιμοποείται για την παραγωγή Monero.

Τελευταίο αλλά εξίσου σημαντικό, όταν οι χρήστες προσπαθούν να αποκτήσουν πρόσβαση σε συγκεκριμένους ιστότοπους, το FacexWorm τους ανακατευθύνει σε άλλες διευθύνσεις (Binance, το DigitalOcean, το FreeBitco.in, το FreeDoge.co.in και το HashFlare) χρησιμοποιώντας έναν άλλο τρόπο με τον οποίο οι hackers κερδίζουν χρήματα.

Η Trend Micro δήλωσε ότι έχει ήδη προβεί στις απαραίτητες ενέργειες αναφέροντα τα αποτελέσματα της έρευνας της τόσο στην Google όσο και στo Facebook. Το προσωπικό του Chrome Web Store παρενέβη αφαιρώντας τις μολυσμένες επεκτάσεις, ενώ το Facebook απαγόρευσε τα domains που συσχετίζονται με τα spam μηνύματα που διανέμονται λόγο του FacexWorm.