Τα botnets «εξόρυξης bitcoin» επέστρεψαν: «Μολύνουν» χιλιάδες υπολογιστές, αποφέροντας απίστευτα κέρδη στους εγκληματίες

Η Ομάδα Anti-Malware Έρευνας της Kaspersky Lab αναγνώρισε δύο botnets υπολογιστών που έχουν «μολυνθεί» με κακόβουλο λογισμικό, τα οποία μυστικά εγκαθιστούν cryptocurrency miners – νόμιμο λογισμικό που χρησιμοποιείται για την εξόρυξη ("mine") εικονικών νομισμάτων βάσει της blockchain τεχνολογίας. Στη μία περίπτωση οι ερευνητές ήταν σε θέση να υπολογίσουν ότι ένα δίκτυο 4.000 υπολογιστών μπορεί να αποφέρει στους κατόχους του μέχρι και 30.000$ τον μήνα και σε άλλη περίσταση οι ερευνητές έγιναν μάρτυρες ενός ‘’τζακ ποτ’’ που ξεπερνούσε τα 200.000$ από ένα PC botnet 5.000 υπολογιστών.

Η αρχιτεκτονική του Bitcoin και άλλων cryptocurrencies υποδηλώνει ότι εκτός από την αγορά cryptocurrency, ο χρήστης μπορεί να δημιουργήσει μια νέα νομισματική μονάδα (ή κέρμα) χρησιμοποιώντας την υπολογιστική ισχύ υπολογιστών που διαθέτουν εξειδικευμένο λογισμικό για "mining". Την ίδια στιγμή, σύμφωνα με την ιδέα που κρύβεται πίσω από τα cryptocurrencies, όσα περισσότερα νομίσματα παράγονται, τόσος περισσότερος χρόνος και υπολογιστική δύναμη απαιτούνται για να δημιουργήσεις ένα νέο νόμισμα. Πριν από

μερικά χρόνια, το κακόβουλο λογισμικό εγκαθιστούσε μυστικά Bitcoin miners (που χρησιμοποιούν τους υπολογιστές των θυμάτων για την εξόρυξη νομισμάτων για ψηφιακούς εγκληματίες), συνηθισμένη πρακτική στο τοπίο των απειλών, αλλά όσα περισσότερα Bitcoins εξορύσσονταν, τόσο πιο δύσκολη γινόταν η εξόρυξη καινούριων και σε μερικές περιπτώσεις αυτή η μέθοδος δεν ήταν χρήσιμη: το πιθανό οικονομικό όφελος που μπορούσε να έχει ένας εγκληματίας από μια προσπάθεια εξόρυξης bitcoin δεν κάλυπτε τις επενδύσεις που απαιτούνταν για τη δημιουργία και τη διανομή κακόβουλου λογισμικού αλλά και το σύστημα υποστήριξης της υποδομής.

Ωστόσο, η τιμή του Bitcoin – του πρώτου και πιο δημοφιλούς cryptocurrency – το οποίο έχει εκτοξευθεί τα τελευταία χρόνια από εκατοντάδες σε χιλιάδες δολάρια για κάθε νόμισμα, πυροδότησε έναν πραγματικό “cryptocurrency πυρετό” σε ολόκληρο τον κόσμο. Εκατοντάδες ενθουσιώδεις ομάδες και startups έχουν αρχίσει να παρουσιάζουν τις δικές τους εναλλακτικές για Bitcoins, πολλές από τις οποίες κέρδισαν επίσης σημαντική αγοραία αξία σε σχετικά σύντομο χρονικό διάστημα.

Αυτές οι αλλαγές στην αγορά των cryptocurrency έχουν αναπόφευκτα ‘’τραβήξει’’ την προσοχή των ψηφιακών εγκληματιών, οι οποίοι τώρα στρέφονται σε συστήματα απάτης που καταφέρνουν αθόρυβα να εγκαθιστούν λογισμικό εξόρυξης cryptocurrency σε χιλιάδες υπολογιστές.

Βασισμένοι σε αποτελέσματα πρόσφατων ερευνών που πραγματοποίησαν οι ειδικοί της Kaspersky Lab, οι εγκληματίες που κρύβονται πίσω από τα προσφάτως ανακαλυφθέντα botnets διανέμουν το λογισμικό εξόρυξης με τη βοήθεια προγραμμάτων adware και με τον τρόπο αυτό τα θύματά τους το εγκαθιστούν οικειοθελώς. Αφού εγκατασταθεί το πρόγραμμα adware στον υπολογιστή του θύματος, ‘’κατεβάζει’’ ένα κακόβουλο εργαλείο: Το miner installer. Αυτό το εργαλείο εγκαθιστά το πρόγραμμα εξόρυξης και στη συνέχεια εκτελεί κάποιες δραστηριότητες για να επιβεβαιώσει ότι το miner θα λειτουργεί σωστά για όσο το δυνατόν περισσότερο. Αυτές οι

διαδικασίες περιλαμβάνουν:

- Προσπάθεια απενεργοποίησης του λογισμικού ασφάλειας.
- Παρακολούθηση όλων των εφαρμογών εκκίνησης και αναστολή των δικών τους δραστηριοτήτων αν ξεκινήσει ένα πρόγραμμα που παρακολουθεί τις δραστηριότητες του συστήματος ή τις τρέχουσες διαδικασίες.
- Διασφάλιση της παρουσίας ενός τουλάχιστον λογισμικού εξόρυξης στον σκληρό δίσκο και επαναφορά του σε περίπτωση που διαγραφεί.

Όταν πραγματοποιηθεί η εξόρυξη των πρώτων νομισμάτων, μεταφέρονται σε ηλεκτρονικά πορτοφόλια που ανήκουν στους εγκληματίες, αφήνοντας τα θύματα με έναν αναπάντεχα υπολειτουργικό υπολογιστή και με ελαφρώς υψηλότερους λογαριασμούς ηλεκτρικού ρεύματος από ό,τι συνήθως. Σύμφωνα με τις παρατηρήσεις της Kaspersky Lab, οι εγκληματίες προσπαθούν να εξορύξουν δύο cryptocurrencies: το Zcash και το Monero. Αυτά τα συγκεκριμένα νομίσματα πιθανών να επιλέχτηκαν διότι παρέχουν έναν αξιόπιστο τρόπο για να παραμείνουν ανώνυμες οι μεταφορές από και προς τα ηλεκτρονικά πορτοφόλια των κατόχων.

Τα πρώτα σημάδια επιστροφής των κακόβουλων miners εντοπίστηκαν από την Kaspersky Lab ήδη από τον Δεκέμβριο του 2016, όταν ένας ερευνητής της εταιρείαςανέφερε τουλάχιστον 1.000 υπολογιστές που είχαν «μολυνθεί» από κακόβουλο λογισμικό, το οποίο έκανε εξόρυξη του Zcash – ένα cryptocurrency που παρουσιάστηκε στα τέλη Οκτωβρίου 2016. Την περίοδο αυτή – χάρη στην τιμή του Zcash που αναπτύσσεται ταχέως – το botnet αυτό θα μπορούσε να φέρει στους ιδιοκτήτες του μέχρι και $6.000 την εβδομάδα. Τότε, έγινε πρόβλεψη για εμφάνιση νέων mining botnets, με τα αποτελέσματα πρόσφατων ερευνών να αποδεικνύουν ότι η πρόβλεψη αυτή ήταν σωστή.

«Το μεγαλύτερο πρόβλημα με τα κακόβουλα miners είναι ότι είναι πραγματικά δύσκολο να ανιχνεύσουμε αξιόπιστα μια τέτοια δραστηριότητα, επειδή το κακόβουλο λογισμικό χρησιμοποιεί πλήρως νόμιμο λογισμικό εξόρυξης, το οποίο σε κανονική

κατάσταση θα μπορούσε επίσης να εγκατασταθεί από έναν νόμιμο χρήστη. Ένα άλλο ανησυχητικό γεγονός που εντοπίσαμε κατά την παρατήρηση αυτών των δύο νέων botnet, είναι ότι τα κακόβουλα miners καθίστανται τα ίδια πολύτιμα στην υπόγεια αγορά. Έχουμε δει τους εγκληματίες να προσφέρουν τους λεγόμενους «δημιουργούς miner»: λογισμικό το οποίο επιτρέπει σε οποιονδήποτε είναι πρόθυμος να πληρώσει για την πλήρη έκδοση, να δημιουργήσει το δικό του botnet εξόρυξης. Αυτό σημαίνει ότι τα botnets που έχουμε εντοπίσει προσφάτως δεν θα είναι και τα τελευταία», δήλωσε ο Evgeny Lopatin, αναλυτής κακόβουλου λογισμικού της Kaspersky Lab.

Σε γενικές γραμμές, ο αριθμός των χρηστών που αντιμετώπισαν cryptocurrency miners έχει αυξηθεί δραματικά τα τελευταία χρόνια. Για παράδειγμα, το 2013, τα προϊόντα της Kaspersky Lab προστάτευσαν περίπου 205.000 χρήστες σε παγκόσμιο επίπεδο, όταν δέχτηκαν επίθεση από τέτοιου είδους απειλή. Το 2014, ο αριθμός αυξήθηκε σε 701.000 και ο αριθμός των προσβεβλημένων χρηστών κατά τους πρώτους οκτώ μήνες του 2017 έφθασε τα 1,65 εκατομμύρια.

Αριθμός των χρηστών που προστάτευσε η Kaspersky Lab από κακόβουλα cryptocurrency miners από το 2011 μέχρι το 2017

Προκειμένου να αποφευχθεί να μετατραπεί ο υπολογιστής τους σε ζόμπι συλλογής ηλεκτρικού ρεύματος, ο οποίος εργάζεται σκληρά για να κερδίσει χρήματα για εγκληματίες, οι ερευνητές της Kaspersky Lab συμβουλεύουν τους χρήστες να ακολουθήσουν τα παρακάτω μέτρα:

- Μην εγκαταστήσετε ύποπτο λογισμικό από μη αξιόπιστες πηγές στον υπολογιστή σας
- Η λειτουργία ανίχνευσης adware ενδέχεται να απενεργοποιηθεί από προεπιλογή στη λύση ασφάλειας. Βεβαιωθείτε ότι την έχετε ενεργοποιημένη
- Χρησιμοποιήστε μια αποδεδειγμένη λύση διαδικτυακής ασφαλείας για να προστατεύσετε το ψηφιακό σας περιβάλλον από όλες τις πιθανές απειλές, συμπεριλαμβανομένων των

κακόβουλων miners.

- Αν χρησιμοποιείτε server, βεβαιωθείτε ότι προστατεύεται με μια λύση ασφάλειας, καθώς οι servers είναι επικερδείς στόχοι για εγκληματίες χάρη στην υψηλή υπολογιστική τους απόδοση (σε σύγκριση με τον μέσο υπολογιστή)

Τα προϊόντα της Kaspersky Lab ανιχνεύουν και εμποδίζουν με επιτυχία το κακόβουλο λογισμικό που διαδίδει κακόβουλο λογισμικό εξόρυξης με τα ακόλουθα ονόματα ανίχνευσης:

- RiskTool.Win32.BitCoinMiner.hxao
- PDM:Trojan.Win32.Generic

Περισσότερες πληροφορίες για τα κακόβουλα botnets εξόρυξης μπορείτε να βρείτε στον ειδικό ιστότοπο Securelist.com.