Σπάζοντας τη φούσκα του bitcoin: Οι spammers εξαργυρώνουν την ευφορία της τεχνολογίας blockchain

Ενώ οι κάτοχοι cryptocurrency αναζητούν νέες επενδυτικές ευκαιρίες και τρόπους για να αυξήσουν τις αποταμιεύσεις τους και οι λάτρεις ψάχνουν να μάθουν περισσότερα για τα οφέλη της μετάβασης σε συναλλαγές χωρίς μετρητά, οι κακόβουλοι χρήστες αναζητούν επίσης τρόπους αξιοποίησης της δημοτικότητας του φαινομένου blockchain. Πολλαπλοί μηχανισμοί απάτης με θέμα την τεχνολογία blockchain που εκμεταλλεύονται τη δημοσιότητα γύρω από την τεχνολογία αυτή έχουν εντοπιστεί πρόσφατα ελεύθεροι στο Διαδίκτυο, σύμφωνα με την έκθεση της Kaspersky Lab "Spam and phishing in Q3 2017".

Για αρκετούς μήνες, οι αποστολείς spam αλληλογραφίας παρουσιάζουν αυξημένη ευρηματικότητα, με τις δραστηριότητές τους να αποδεικνύουν ότι παρακολουθούν τις τελευταίες τάσεις και τις παγκόσμιες εξελίξεις στα cryptocurrencies. Με βάση την τεχνολογία blockchain, τα cryptocurrencie έχουν γίνει ένας ελκυστικός στόχος για τους ψηφιακούς εγκληματίες, οι οποίοι έχουν στοχεύσει με επιτυχία και επιθετικά τα θύματά τους μέσω της «διαδικτυακής εξόρυξης» (web-mining). Παράλληλα, κατά τη διάρκεια των τελευταίων τριών μηνών, οι ερευνητές της Kaspersky Lab έχουν επίσης εντοπίσει αύξηση των δραστηριοτήτων spam που σχετίζονται με την κρυπτογράφηση. Σύμφωνα με την αναφορά "Spam and phishing in Q3 2017", οι εγκληματίες έχουν χρησιμοποιήσει αρκετά επιτυχημένα κόλπα για να ξεγελάσουν τους χρήστες και να κλέψουν τα χρήματά τους.

Οι μηχανισμοί απάτης, που βασίζονται στις συναλλαγές με

cryptocurrency, έχουν επικρατήσει κατά το τελευταίο τρίμηνο. Σε ένα τέτοιο σενάριο, οι χρήστες λαμβάνουν μια πρόσκληση μέσω email για την εγκατάσταση ειδικού λογισμικού συναλλαγών με cryptocurrency, αλλά όταν πατούν το link, ανακατευθύνονται σε διαφορετικές ιστοσελίδες που προωθούν επενδυτικές επιλογές, συμπεριλαμβανομένων binary options συναλλαγών. Ωστόσο, για το θύμα δεν υπάρχει εγγύηση ότι αυτό θα οδηγήσει σε κάτι θετικό ή ότι θα πάρει τα χρήματά του πίσω. Αυτός ο τύπος μηχανισμού απάτης είναι παρόμοιος με το set-up των καζίνο και αποσκοπεί στο να προκαλέσει τους χρήστες να κάνουν προσφορές έως ότου δεν τους έχει μείνει τίποτα, αφήνοντας στους ψηφιακούς εγκληματίες τα πάντα.

Πιο απαρχαιωμένες, αλλά όχι λιγότερο αποτελεσματικές, τακτικές που χρησιμοποιούνται για την εκμετάλλευση θυμάτων περιλαμβάνουν τη διανομή email που προσφέρουν τη μεταφορά χρημάτων σε ένα συγκεκριμένο κρυπτογραφημένο πορτοφόλι, όπου ο χρήστης θα λαμβάνει τα χρήματά του πίσω. Αλλά, φυσικά, αυτό δεν συμβαίνει ποτέ. Οι χρήστες αρχικά μεταφέρουν τα χρήματα σε ένα άγνωστο πορτοφόλι και οι ψηφιακοί εγκληματίες τα εξαργυρώνουν.

Ένας άλλος μηχανισμός εξαπάτησης, που ανακαλύφθηκε από τους ερευνητές της Kaspersky Lab το τρίτο τρίμηνο, ήταν με τη μορφή προσφοράς για να βοηθήσει τους χρήστες να μάθουν περισσότερα για τα cryptocurrencies και πώς θα μπορούσαν να επωφεληθούν από αυτά. Αυτή η ύπουλη τακτική είχε ως στόχο να εκμεταλλευτεί την έλλειψη κατανόησης σχετικά με την τεχνολογία blockchain και του τρόπου που λειτουργούν τα cryptocurrencies. Οι εγκληματίες διαφημίζουν εκπαιδευτικά εργαστήρια μέσω email που θα βοηθούσαν τους χρήστες να βελτιώσουν τις γνώσεις και τις δεξιότητές τους γύρω από τα cryptocurrencies και να ενημερωθούν για επενδυτικές ευκαιρίες. Με μια υψηλή τιμή, οι χρήστες εξαπατήθηκαν και πλήρωσαν πιστεύοντας ότι αυτή ήταν μια νόμιμη αγγελία. Ωστόσο, τα χρήματα που κατέβαλαν για να λάβουν τέτοιου είδους συμβουλές κατέληξαν να εμπλουτίζουν το πορτοφόλι κάποιου άλλου, και όχι τη γνώση του χρήστη. Κι αυτό

γιατί συνήθως τέτοια εργαστήρια που προωθούνται μέσω spam email είναι αρκετά δαπανηρά και συνεπάγονται περισσότερη διαφήμιση παρά πραγματική γνώση.

«Ενώ κατά το δεύτερο τρίμηνο του έτους παρατηρήσαμε τις επιθέσεις spam και phishing του WannaCry, τους τελευταίους τρεις μήνες διαπιστώσαμε εγκληματίες που εκμεταλλεύονται ενεργά τη δημοτικότητα και το ενδιαφέρον γύρω από το cryptocurrency. Αυτό δείχνει για άλλη μια φορά ότι ο πιο αξιόπιστος τρόπος για να στοχεύουν τα θύματα είναι να αξιοποιούν τις τρέχουσες τάσεις και να εξαργυρώνουν μια αναδυόμενη αγορά την οποία οι χρήστες δεν έχουν κατανοήσει πλήρως και επιθυμούν να διερευνήσουν. Δεν υπάρχει αμφιβολία ότι οι επιθέσεις σε αυτή τη μορφή θα συνεχιστούν, οπότε είναι εξαιρετικά σημαντικό για τους χρήστες να δίνουν ιδιαίτερη προσοχή και να ενημερώνονται όταν πρόκειται για παγκόσμιο φαινόμενο», δήλωσε η Darya Gudkova, Spam Analyst Expert της Kaspersky Lab.

Μαζί με την αύξηση των blockchain απατών, ο μέσος όρος των spam email έχει αυξηθεί στο 58,02%, μέγεθος 1,05 ποσοστιαίες μονάδες υψηλότερο σε σύγκριση με το δεύτερο τρίμηνο. Σύμφωνα με την έκθεση, η μέγιστη δραστηριότητα spam email πραγματοποιήθηκε τον Σεπτέμβριο και άγγιξε το 59,56%.

Επιπλέον, κατά το τρίτο τρίμηνο του έτους οι ερευνητές ανίχνευσαν αύξηση των επιθέσεων phishing κατά 13 εκατομμύρια – το σύστημα Kaspersky Lab Anti-Phishing ενεργοποιήθηκε 59.569.508 φορές στους υπολογιστές των χρηστών της Kaspersky Lab. Ταυτόχρονα, οι εγκληματίες έχουν επικεντρωθεί περισσότερο στη χρήση εφαρμογών messenger σε φορητές συσκευές για την πραγματοποίηση δημοφιλών διαδικτυακών απατών.

Η αναλογία του spam στην κίνηση των email το 2^{ο} τρίμηνο του 2017 σε σύγκριση με το τρίτο τρίμηνο

Άλλες σημαντικές τάσεις και στατιστικά στοιχεία για το τρίτο τρίμηνο που επισημάνθηκαν από τους ερευνητές της Kaspersky

Lab, περιλαμβάνουν τα εξής:

- Η Κίνα έγινε η πιο δημοφιλής πηγή spam, ξεπερνώντας το Βιετνάμ και τις Η.Π.Α. Στις υπόλοιπες 10 χώρες περιλαμβάνονται η Ινδία, η Γερμανία, η Βραζιλία, η Γαλλία, η Πολωνία και η Ισλαμική Δημοκρατία του Ιράν.
- Η χώρα που αποτέλεσε στόχο κακόβουλων αποστολών email τις περισσότερες φορές ήταν η Γερμανία. Ο κορυφαίος στόχος της προηγούμενης περιόδου, η Κίνα ήρθε δεύτερη, ακολουθούμενη από τη Ρωσία, την Ιαπωνία και την Ιταλία.
- Το μεγαλύτερο ποσοστό χρηστών που επηρεάστηκαν από phishing email ήταν στη Βραζιλία (19,95%), όπως και το προηγούμενο τρίμηνο. Συνολικά, το 9,49% μοναδικών χρηστών προϊόντων της Kaspersky Lab παγκοσμίως δέχτηκαν επίθεση phishing.
- Οι κύριοι στόχοι επιθέσεων phishing παρέμειναν οι ίδιοι από την αρχή του έτους. Πρόκειται κυρίως για τον χρηματοπιστωτικό τομέα και περιλαμβάνονται οι τράπεζες, οι υπηρεσίες πληρωμών και τα ηλεκτρονικά καταστήματα.

Περισσότερες πληροφορίες σχετικά με το spam και το phishing το τρίτο τρίμηνο του 2017 μπορείτε να βρείτε στον ειδικό ιστότοπο Securelist.com.

Η Kaspersky Lab συνιστά στους οικιακούς χρήστες να εγκαταστήσουν μια αξιόπιστη λύση ασφάλειας για την ανίχνευση και την παρεμπόδιση spam μηνυμάτων και επιθέσεων phishing, όπως η λύση Kaspersky Total Security.

Στις επιχειρήσεις συνιστάται να χρησιμοποιούν λύσεις ασφάλειας με αποκλειστική λειτουργικότητα που στοχεύει στην ανίχνευση και την παρεμπόδιση phishing επιθέσεων, κακόβουλων συνημμένων και spam μηνυμάτων. Οι μικρές επιχειρήσεις μπορούν να προστατευθούν με τις λύσεις Kaspersky Small Office Security και Kaspersky Endpoint Security Cloud, ενώ οι μεγαλύτερες εταιρείες μπορούν να επωφεληθούν από την cloud-assisted anti-spam σάρωση όλων των μηνυμάτων σε πραγματικό χρόνο, με την εφαρμογή Kaspersky Security for Mail Server που περιλαμβάνεται

στη λύση Kaspersky Total Security for Business.

Για να διασφαλίσουμε ότι θα συνεχίσουμε να παρέχουμε τα υψηλότερα επίπεδα προστασίας στους πελάτες μας, η Kaspersky Lab θα παρουσιάσει το 2018 το Kaspersky Security for Office 365, μια νέα υπηρεσία Security-as-a-Service που παρέχει βραβευμένη προστασία από spam αλληλογραφία, phishing και κακόβουλο λογισμικό, για το Exchange online στο Microsoft Office 365. Το προϊόν διατίθεται προς το παρόν δημόσια σε beta έκδοση και θα συνεχίσει να διατίθεται δωρεάν μέχρι τον Φεβρουάριο του 2018.