25 Μαΐου 2015

Κινέζοι χάκερς χρησιμοποιούν το TechNet για τις επιθέσεις τους

/ Πεμπτουσία

Image not found or type unknown

Η Microsoft έχει λάβει μέτρα για να εμποδίσει μια κινέζικη ομάδα χάκερς να χρησιμοποιεί το TechNet website της, ως τμήμα της υποδομής της επίθεσής της, σύμφωνα με τον προμηθευτή ασφάλειας FireEye. Η ομάδα, που η FireEye αποκαλεί APT (advanced persistent threat) 17, είναι γνωστή για τις επιθέσεις της ενάντια στους προμηθευτές όπλων, στις νομικές εταιρίες, στις υπηρεσίες της αμερικανικής κυβέρνησης και σε εταιρείες τεχνολογίας και εξωρύξεων.

Το TechNet είναι ιδιαίτερα εμπορικό website που έχει την τεχνική έκθεση για τα προϊόντα της Microsoft. Έχει επίσης ένα μεγάλο φόρουμ, όπου οι χρήστες μπορούν να αφήσουν σχόλια και να υποβάλουν τις ερωτήσεις τους.

Η ομάδα APT17 –με το ψευδώνυμο DeputyDog- δημιούργησαν accounts στο TechNet και έπειτα άφηναν σχόλια σε ορισμένες σελίδες. Εκείνα τα σχόλια περιείχαν το όνομα ενός κωδικοποιημένου domain, στον οποίο οδηγήθηκαν οι υπολογιστές που είχαν μολυνθεί από το malware που είχε δημιουργήσει η ομάδα.

Το κωδικοποιημένο domain ανάφερε έπειτα τον υπολογιστή του θύματος σε έναν command-and-control server που ήταν μέρος της υποδομής της APT17, αναφέρει στην δήλωσή του ο Bryce Boland, ο chief technology για το κομμάτι της Ασίας και του Ειρηνικού της εταιρείας FireEye.

Η τεχνική της επικοινωνίας ενός μολυσμένου υπολογιστή με έναν ενδιάμεσο domain χρησιμοποιείται συχνά. Συχνά, οι χάκερ θέλουν οι μολυσμένες μηχανές να φτάσουν σε ένα domain που είναι απίθανο να φανεί ύποπτο πρίν προχωρήσουν σε έναν άλλο λιγότερο αξιόπιστο.

Μερικές φορές, οι command-and-control domains ενσωματώνονται στο ίδιο το malware, αλλά αυτό διευκολύνει τους ερευνητές ασφάλειας να διαπιστώσουν με ποιον επικοινωνεί. Άλλες φορές , το malware κωδικοποιείται με έναν αλγόριθμο που παράγει πιθανά domains names με τα οποία πρέπει να επικοινωνήσει, αλλά αυτό μπορεί επίσης να γίνει reverse engineered (αποσυμπίληση) από τους αναλυτές, αναφέρει ο Boland.

Οι ειδικοί ασφάλειας έχουν δει τους επιτιθεμένους να κάνουν κακή χρήση άλλων νόμιμων domains και υπηρεσιών, όπως τα Google Docs και το Twitter, για να πετύχουν τον ίδιο στόχο με APT17, όπως αναφέρει ο Boland.

Η FireEye και η Microsoft αντικατέστησαν τους κωδικοποιημένους domains στο TechNet με εκείνους που ελέγχονται από τις επιχειρήσεις, οι οποίες τους έδωσαν μια εικόνα του προβλήματος όταν οι μολυσμένες μηχανές επικοινώνησαν με τα εν λόγω domains.

Η APT17 «έχει ως στόχο τους πελάτες μας για πολλά χρόνια,» λέει ο Boland. Οι οργανισμοί χαρακτηριστικά στοχεύονται μέσω spear-phishing -, το οποίο περιλαμβάνει την αποστολή emails με κακόβουλα links ή συνημμένα.

Πηγή: SecNews.gr