17 Φεβρουαρίου 2015

«Συμβόλαια» hacking: Πόσο κοστίζει το hack ενός λογαριασμού;

Επιστήμες / Πληροφορική & Internet

Υπάρχουν πολλοί, που ίσως να μην μπορούν να θυμηθούν τις ημέρες που η HTML γραφόταν εξολοκλήρου με το χέρι, όπως παρομοίως υπάρχουν πολλοί *hackers*, που δεν μπορούν να θυμηθούν πότε ένα exploit χρειάστηκε να κατασκευαστεί από το μηδέν. Η διαδικασία του hacking δεν έπαψε να είναι παράνομη, αλλά φαίνεται να έχει γίνει πιο user–friendly . Συνδυάζοντας το γεγονός αυτό με την αύξηση του αριθμού των συναλλαγών που πραγματοποιούνται online, δημιουργείται πρόσφορο έδαφος για την ανάπτυξη της παραοικονομίας.

Με τα εξελιγμένα exploit kits, τα δωρεάν εργαλεία, τα botnets και τους hackers προς ενοικίαση, έχει καταστεί σχετικά εύκολο κάτι που παλιότερα ήταν δυνατό να πραγματοποιηθεί μόνον από ειδικευμένους hackers. Έχει δημιουργηθεί μία παράνομη αγορά όπου ο καθένας μπορεί να αγοράσει και να πουλήσει malware, exploit kits, botnets, πληροφορίες για πιστωτικές κάρτες, zero-day ευπάθειες (για τις οποίες κανένα patch δεν είναι διαθέσιμο) για δημοφιλή λειτουργικά συστήματα ή για εφαρμογές καθώς και υπηρεσίες όπως η επίθεση και η καταστροφή ενός website ή η εκτέλεση επιθέσεων DDoS. Πώς, λοιπόν, λειτουργεί όλη αυτή η αγορά;

Όπως το Software ως υπηρεσία (SaaS) μετατρέπει τον τρόπο που έχουμε πρόσβαση στις εφαρμογές, έτσι και το Hacking as a Service (HaaS) διευκολύνει τους επιτιθέμενους.

Από οικονομικής άποψης, το κόστος που απαιτείται για να προσληφθεί ένας hacker είναι παρόμοιο με εκείνο που απαιτείται για την πρόσληψη οποιουδήποτε άλλου επαγγελματία. Ο χρόνος που θα αφιερώσουν οι hackers καθορίζει και την αμοιβή τους, όσο περισσότερος χρόνος χρειαστεί για να ολοκληρωθεί η διαδικασία της επίθεσης τόσο μεγαλύτερη θα είναι η αμοιβή τους. Μία απλή επίθεση DDoS ή μερικά κακόβουλα SEO links θα μπορούσαν να κοστίσουν μόλις $100, ενώ τα RATs όπως το Blackshades ή η ενοικίαση botnet θα μπορούσε να κοστίσουν από $250 μέχρι και $500. Ο πλήρης έλεγχος ενός botnet όπως το ZeuS με δυνατότητες διαχείρισης και ελέγχου μπορεί να κυμανθεί στα $20,000.

Δεδομένου ότι οι hackers προφανώς δεν θα περιμένουν μέχρι να ζητήσουν τις υπηρεσίες τους για να αναζητήσουν οικονομικά οφέλη, συνήθως αναζητούν έσοδα μέσω της πώλησης exploit toolkits. Αρχικά η πώληση των toolkits δεν ήταν και τόσο επικερδής, καθώς μόλις αγοραστούν, γίνουν download και μεταπωληθούν, τα κέρδη που μπορούν να αποφέρουν στους developers μειώνονται σταδιακά. Το Blackhole toolkit έλυσε αυτό το πρόβλημα, εισάγοντας ένα μοντέλο παροχής υπηρεσιών για updates, με το οποίο ο χρήστης μπορεί να λάβει υποστήριξη, νέα features και νέα Zero-Day exploits με την προϋπόθεση ότι έχει γίνει συνδρομητής

στον αρχικό developer. Οι προγραμματιστές με τη σειρά τους θα επενδύσουν κάποια χρήματα για την εύρεση και δημιουργία νέων exploits και features στο toolkit. Exploit kits ανοιχτού πηγαίου κώδικα όπως το Metasploit μπορεί να γίνει download δωρεάν.

Υπάρχουν διαφορετικές ειδικότητες μεταξύ των Hackers;

Όπως ακριβώς συμβαίνει με τους "νόμιμους" και ηθικούς hackers και τους IT/Network security επαγγελματίες, οι hackers έχουν ειδικότητες. Πιθανά να υπάρχουν κάποιοι, οι οποίοι είναι περισσότερο ειδήμονες στον προγραμματισμό και στην δημιουργία ιών ή Trojans, όπως ακριβώς υπάρχουν επαγγελματίες IT Security που ειδικεύονται στην δημιουργία signatures για να εντοπίζουν τέτοιου είδους malware και συμμετέχουν στην δημιουργία προϊόντων antivirus/antimalware. Πιθανά να υπάρχουν και άλλοι, που έχουν ειδίκευση στην ταυτοποίηση ευπαθειών στο λογισμικό ή στα λειτουργικά συστήματα. Μπορεί να υπάρχουν και άλλοι, οι οποίοι είναι έμπειροι στην παραβίαση websites ή δικτύων. Αυτός ο κλάδος είναι τόσο ποικιλόμορφος όσο και ο κατάλογος των πιστοποιήσεων ασφαλείας δικτύων, που οι υπεύθυνοι πληροφορικής προσπαθούν να αποκτήσουν για να γίνουν πιο καταρτισμένοι.

Ποια είναι η λύση;

Όπως έχει διαπιστωθεί το κόστος μπορεί να είναι σχετικά χαμηλό, για την πρόκληση μεγάλης ζημιάς, ενώ έχουν μειωθεί σημαντικά τα εμπόδια έτσι ώστε να δράσει κάποιος αυτοβούλως. Από την πλευρά ενός IT administrator, η κατάσταση αυτή δεν πρέπει να οδηγήσει σε παραίτηση, αλλά στην αναζήτηση νέων έξυπνων τρόπων προστασίας. Γενικά, η εξασφάλιση ότι όλα τα software patches έχουν γίνει update, και η πλήρης ενημέρωση για τις νέες τάσεις στον κλάδο αποτελούν μια σημαντική αρχή. Μιλώντας για τάσεις, βεβαιωθείτε ότι είστε σε επαφή με τις αρμόδιες αρχές σε περίπτωση που πέσετε θύματα μιας επίθεσης botnet. Το έργο της Symantec σε αυτόν τον τομέα έχει οδηγήσει σε αρκετά πλήγματα ενάντια σε botnets μέχρι στιγμής.

Είναι σημαντικό οι χρήστες να είναι εκπαιδευμένοι έτσι ώστε να γνωρίζουν πως να προστατεύσουν τα δεδομένα τους. Οι διαχειριστές του δικτύου θα πρέπει να τους ενημερώσουν ότι πρέπει να αποφεύγουν να κάνουν κλικ σε email links που δεν γνωρίζουν ή να αποφεύγουν να ανοίγουν συνημμένα αρχεία που δεν αναγνωρίζουν. Επίσης, οι διαχειριστές πρέπει να απαγορεύσουν το «πειρατικό» λογισμικό και να διεξάγουν μαθήματα ευαισθητοποίησης για να κρατήσουν ενήμερους τους χρήστες.

Πηγή: Secnews.gr

http://bitly.com/1CvSXPG