Οι κανόνες του «παιχνιδιού» στα θέματα ασφάλειας άλλαξαν

Οι επιτιθέμενοι χρησιμοποιούν πλέον εργαλεία που προσαρμόζονται ανάλογα την επίθεση, με στόχο να αποδιοργανώσουν την υποδομή ασφάλειας.

Νίκος Μουρτζίνος,
Product Sales Specialist, Cisco

Για να κατανοήσουμε πραγματικά κάθε κακόβουλη δικτυακή επίθεση, πρέπει να λάβουμε υπόψη τα βήματα που ακολουθούνται σε κάθε στάδιο και ανάλογα να προσαρμόσουμε την αρχιτεκτονική και τη στρατηγική ασφάλειας.

Σας παρουσιάζουμε τα 5 συνήθη βήματα μιας επαγγελματικά σχεδιασμένης επίθεσης:

1. Έρευνα

Στο στάδιο αυτό, οι επιτιθέμενοι χρησιμοποιούν ειδικά κακόβουλα λογισμικά επιτήρησης, με στόχο να αποκτήσουν την πλήρη εικόνα του περιβάλλοντος και της αρχιτεκτονικής ασφάλειας που έχει αναπτυχθεί. Ταυτόχρονα, ανιχνεύουν τα ευάλωτα σημεία, καθώς και ποιους λογαριασμούς θα μπορούσαν να υποκλέψουν με στόχο να αποκτήσουν αυξημένα δικαιώματα. Το κακόβουλο λογισμικό επιτήρησης χρησιμοποιεί κοινά κανάλια για να επικοινωνήσει και έχει σχεδιαστεί ώστε να παραμένει απαρατήρητο στη φάση αυτή.

2. Καταγραφή

Γνωρίζοντας πλέον τι έχουν να αντιμετωπίσουν, τα άτομα που κάνουν την επίθεση δημιουργούν στοχευμένο κακόβουλο λογισμικό. Μπορούν δηλαδή να σχεδιάσουν λογισμικά που δρουν διαφορετικά ανάλογα με το στόχο τους και τι ακριβώς επιδιώκουν. Στη συνέχεια, έχουν τη δυνατότητα να επεκτείνουν τις δραστηριότητες επιτήρησης και να συλλέξουν σημαντικές πληροφορίες σχετικά με τους «πολύτιμους πόρους», πού αυτοί βρίσκονται και πώς θα αποκτήσουν πρόσβαση σε αυτούς. Στοχεύουν συγκεκριμένους οργανισμούς, εφαρμογές, χρήστες, συνεργάτες και διαδικασίες.

3. Έλεγχος

Στη συνέχεια ελέγχουν τη σωστή λειτουργία του λογισμικού. Οι δημιουργοί τους διαθέτουν σημαντικούς οικονομικούς πόρους και αναπτυγμένα δίκτυα ανταλλαγής πληροφοριών. Δημιουργούν ένα περιβάλλον παρόμοιο με αυτό που στοχεύουν να επιτεθούν και ελέγχουν το κακόβουλο λογισμικό έναντι σε εργαλεία προστασίας, για να είναι σίγουροι πως περνά απαρατήρητο από τους μηχανισμούς άμυνας. Μπορούν ακόμα και να εγγυηθούν ότι το λογισμικό τους θα περάσει απαρατήρητο για έξι ή και εννιά μήνες. Επομένως, μιλάμε για πραγματική εκβιομηχάνιση του hacking.

4. Εκτέλεση

Το οικονομικό κίνητρο για μυστικότητα είναι πολύ υψηλότερο από τη δόξα. Τα άτομα που κάνουν την επίθεση, «πλοηγούνται» στο ευρύτερο δίκτυο, ήδη γνωρίζοντας το περιβάλλον αυτό, αποφεύγοντας την ανίχνευση και κινούμενοι περιμετρικά μέχρι να φτάσουν στο τελικό τους στόχο. Υπάρχουν διαρκώς αυξανόμενες περιπτώσεις, όπου δημιουργούνται προσαρμοσμένοι Command & Control servers (CnC) και από εκεί γίνεται ο έλεγχος του κακόβουλου λογισμικού με σχετική ασφάλεια πως δεν παρακολουθούνται από περιμετρικά εργαλεία ασφάλειας.

5. Εκπλήρωση αποστολής

Ορισμένες φορές το τελικό στάδιο είναι η συλλογή πληροφοριών. Σε άλλες περιπτώσεις είναι απλά η καταστροφή τους. Σε κάθε περίπτωση, διαθέτουν πληροφορίες και ένα στοχευμένο πλάνο επίθεσης, για να μεγιστοποιήσουν την επιτυχία της αποστολής τους. Όταν αυτή ολοκληρωθεί, θα αφαιρέσουν τα στοιχεία, αλλά θα διατηρήσουν τη θέση τους για μελλοντικές επιθέσεις.

Η Cisco έχει εστιάσει και αναπτύξει συγκεκριμένη λύση ασφάλειας για να αντιμετωπιστεί η παραπάνω διαδικασία επίθεσης και για να προστατευθούν οι πολύτιμοι πόροι. Πιστεύει στην εφαρμογή ενός μοντέλου ασφάλειας επικεντρωμένου απόλυτα στις απειλές (Threat Centric), που επεκτείνεται πέρα από τις δυνατότητες των επιθέσεων και ανταποκρίνεται στο ευρύτερο δίκτυο και το εξελισσόμενο σύγχρονο επιχειρηματικό περιβάλλον.
Η αρχιτεκτονική ασφάλειας της Cisco που είναι προσαρμοσμένη στις απειλές (Cisco Threat Centric Security Architecture), μειώνει την πολυπλοκότητα και παρέχει ασύγκριτη ορατότητα, συνεχή έλεγχο και προηγμένη προστασία σε όλα τα στάδια μιας επίθεσης, τόσο πριν από την επίθεση όσο κατά τη διάρκεια αλλά και μετά από αυτή.

Επισκεφθείτε το Cisco security blog για τα τελευταία νέα στην αρχιτεκτονική ασφάλειας και δείτε τις λύσεις της Cisco στην επίσημη ιστοσελίδα μας.

DIRECTION BUSINESS NETWORK: Μ. ΑΣΙΑΣ 43, 152 33 ΧΑΛΑΝΔΡΙ | **Τ.** 210 77.12.400 | **F.** 210 77.13.343 (INFO@DIRECTION.GR)
| **ΕΚΔΟΤΗΣ** ΒΑΓΓΕΛΗΣ ΠΑΠΑΛΙΟΣ | **ΣΥΜΒΟΥΛΟΣ ΕΚΔΟΣΗΣ** ΓΙΩΡΓΟΣ ΣΤΟΥΡΑΪΤΗΣ
| **PROJECT MANAGER** ΓΙΑΝΝΗΣ ΧΑΡΑΜΙΔΗΣ (HARAMIDIS@DIRECTION.GR) | **ΥΠΕΥΘΥΝΗ ΥΛΗΣ** ΑΝΝΑ ΑΝΔΡΕΟΛΑ (ANDREOLA@DIRECTION.GR)
| **ΥΠΟΔΟΧΗ ΔΙΑΦΗΜΙΣΗΣ** ΑΝΝΑ ΜΗΛΙΑΔΗ (MILIADI@DIRECTION.GR) | **ΣΥΝΔΡΟΜΕΣ** ΑΦΡΟΔΙΤΗ ΧΑΤΖΗ (HATZI@DIRECTION.GR)
ΕΤΗΣΙΑ ΣΥΝΔΡΟΜΗ 245€