Ο server μου έχει πέσει θύμα hacker. Τι να κάνω;

- 2019-03-07 - Διαχείριση

Σε περίπτωση παραβίασης του server από τρίτους, ο διαχειριστής δέχεται ενημέρωση από το data center ή από άλλους διαχειριστές οι οποίοι ενοχλήθηκαν από την παραβατική δράση του server του.

Πως το καταλαβαίνω ότι έχω πέσει θύμα επίθεσης;

Πολλοί διαχειριστές παρατηρούν πως προσπαθούν να τρέξουν εντολές συστήματος όπως ls ή Netstat και εμφανίζεται segmentation fault ή χρειάζεται για παράδειγμα να πατήσουν δύο φορές το enter για να πραγματοποιήσουν τα αιτήματα των εφαρμογών τους.

Τα παραπάνω είναι τα πρώτα σημάδια που κάποιος μπορεί να καταλάβει πως ο server του δεν είναι υπό τον πλήρη έλεγχο του και το πιο πιθανό είναι πως έχει πέσει θύμα παραβίασης.

Στις περισσότερες περιπτώσεις η παραβίαση γίνεται με σκοπό την αποστολή spam emails μέσω του server σας, επίθεση σε άλλους server χρησιμοποιώντας μνήμη, CPU και bandwidth ή ακόμα και εγκατάσταση phishing website με σκοπό την απόκτηση πρόσβασης σε προσωπικά δεδομένα.

Τι μπορώ να κάνω τώρα;

1. Σταματήστε άμεσα τις εργασίες που εκτελεί ο server.

2. Απενεργοποιείστε τα site σας (καλό θα ήταν να ανεβάσετε μία σελίδα «υπό συντήρηση»).

3. Αποθηκεύστε ένα backup των site σας.

4. Ερευνήστε για non-root λογαριασμούς χρηστών στο /etc/passwd με UID 0.

5. Ελέγξτε αν υπάρχουν και άλλοι λογαριασμοί που δεν γνωρίζετε όπως r00t ή hax0r ή το όνομα κάποιας υπηρεσίας με αλλαγμένο κάποιο από τους χαρακτήρες του.

6. Ανοίξτε το .bash_history χρηστών για να ελέγξετε για ύποπτες εντολές που έχουν εκτελέσει.

7. Ελέγξτε τις διεργασίες που ήδη εκτελούνται στο σύστημά σας, χρησιμοποιώντας την top την ps ή για πόρτες που είναι ανοιχτές (συνήθως πάνω από τη 1024), με τη βοήθεια του Netstat.

8. Ελέγξτε αν υπάρχουν και άλλοι SSHD σε διαφορετικές πόρτες.

9. Ελέγξτε τα log files για το ποιος και πότε απέκτησε πρόσβαση στην SSH υπηρεσία, στην mail υπηρεσία, ακόμα και για το ποιος συνδέθηκε τελευταία φορά στο server.

10. Ελέγξτε για rootkits.

Πως απέκτησαν πρόσβαση στο server μου;

Το πιο πιθανό είναι ο παραβάτης να έχει υποκλέψει κωδικούς μέσω κάποιας εφαρμογής όπως για παράδειγμα του FTP client ή να έχει εκμεταλλευτεί αδυναμία του συστήματος.

Πως μπορώ να προστατευτώ;

1. Χρησιμοποιείτε ισχυρούς κωδικούς για κάθε υπηρεσία (αλφαριθμητικούς και με σύμβολα). Αν είναι εφικτό, μην τους αποθηκεύετε και να τους αλλάζετε όσο πιο συχνά μπορείτε. Δημιουργήστε ισχυρούς κωδικούς με το Top.Pass, το δωρεάν εργαλείο της Top.Host.

2. Χρησιμοποιείτε μηχανισμούς ασφαλείας όπως antivirus και firewalls.

3. Κρατάτε αντίγραφα ασφαλείας.

4. Διατηρείτε ενημερωμένο το λειτουργικό του συστήματος σας.

5. Μη χρησιμοποιείτε πειρατικό λογισμικό.

6. Διατηρείτε ενημερωμένες τις εφαρμογές, τα themes και τα plugin σας.

Τέλος, αφού κάνετε τα παραπάνω θα πρέπει να παρακολουθείτε στενά τον server σας καθώς ο εισβολέας θα προσπαθήσει να ανακτήσει την πρόσβαση.