Ο Μήνας της Ασφάλειας στο tech.in.gr

Τι εστί botnet; Είναι το PC μου Ζόμπι;

Δημοσίευση: 18 Απρ 2011, 11:06

Ο υπολογιστής σας μπορεί να είναι ήδη μαριονέτα στα χέρια επίδοξων ληστών χωρίς να το έχετε αντιληφθεί. Πώς όμως μπορεί να συμβεί κάτι τέτοιο;

Ως botnet ορίζεται ένα δίκτυο υπολογιστών, το οποίο ελέγχεται εξ αποστάσεως από τον λεγόμενο botmaster χωρίς τη γνώση ή την έγκριση των κατόχων των μεμονωμένων υπολογιστών. Οι υπολογιστές που είναι μέλη του δικτύου αυτού ονομάζονται *ζόμπι*.

Ο botmaster μπορεί να χρησιμοποιεί αυτούς τους υπολογιστές-ζόμπι για διάφορους παράνομους σκοπούς. Καθώς μπορεί να έχει πρόσβαση στον κάθε υπολογιστή-ζόμπι σαν να βρισκόταν ο ίδιος μπροστά σε αυτόν, είναι δυνατή τόσο η πρόσβαση στα αρχεία του συστήματος όσο και η χρήση της σύνδεσης δικτύου του υπολογιστή, χωρίς να το αντιληφθεί ο ιδιοκτήτης του.

Αυτό του δίνει αμέτρητες δυνατότητες. Πέρα από την υποκλοπή δεδομένων, η πρόσβαση στους υπολογιστές-ζόμπι επιτρέπει και την απόκρυψη της ταυτότητας του δράστη, καθώς ως διακομιστής μεσολάβησης χρησιμοποιείται ο υπολογιστής του θύματος. Ανάλογα με το μέγεθος του botnet, ο δράστης μπορεί να αλλάζει σε ορισμένες εξαιρετικές περιπτώσεις τη διεύθυνση IP του ακόμη και ανά δευτερόλεπτο, ώστε να μπορεί να προβαίνει σε παράνομες ενέργειες μέσω των συνδέσεων των θυμάτων του. Επιπλέον, ο εξ αποστάσεως έλεγχος των υπολογιστών εξυπηρετεί ιδανικά τη μετάδοση του κακόβουλου κώδικα bot ή τη μαζική αποστολή spam.

Κατανεμημένες επιθέσεις: Denial of Service Attack

Αναλογιζόμενοι το μέγεθος ενός τυπικού botnet, που αποτελείται από μερικές εκατοντάδες έως περισσότερες χιλιάδες υπολογιστές-ζόμπι, δεν μπορεί κανείς παρά να σκεφτεί μια περαιτέρω εφαρμογή των στρατιών των botnet: τη χρήση τους ως όπλο για την εκτέλεση των λεγόμενων επιθέσεων DDoS (Distributed Denial of Service). Στην περίπτωση αυτοί, οι διακομιστές web ή αλληλογραφίας που βρίσκονται στο στόχαστρο "γονατίζουν" υπό το βάρος μαζικών αιτημάτων σύνδεσης. Με τον κατάλληλο αριθμό ζόμπι, ο διακομιστής θα τεθεί εκτός λειτουργίας. Η μέθοδος αυτή ανοίγει την πόρτα για εγκληματικές ενέργειες όπως εκβιασμούς.

Είναι ο υπολογιστής μου άνδρο ληστών;

Επίσης δημοφιλής είναι η χρήση των υπολογιστών-ζόμπι ως διακομιστές web ή FTP. Αυτό μπορεί να εξυπηρετεί διάφορους σκοπούς: αφενός στη διάθεση μολυσμένων τοποθεσιών web με σκοπό την παροχή περαιτέρω πληροφοριών, αφετέρου στη χρήση των συστημάτων ανυποψίαστων θυμάτων για την αποθήκευση πορνογραφίας, πειρατικών αντιγράφων, κ.λπ.

Στρατιά σε ετοιμότητα

Η διαχείριση και ο συντονισμός των υπολογιστών-ζόμπι, που πιθανόν είναι διασκορπισμένοι ανά την υφήλιο, μπορεί να γίνει με διάφορους τρόπους. Ενώ στα πρώτα botnets χρησιμοποιούνται κεντρικοί διακομιστές εντολών και ελέγχου, σήμερα προτιμώνται όλο και περισσότερο αποκεντρωμένες δομές επικοινωνίας, οι οποίες μοιάζουν με τα γνωστά δίκτυα P2P (Peer-to-Peer). Αυτό κάνει ακόμη δυσκολότερο το κλείσιμο ενός botnet, διότι δεν υπάρχει κεντρικός διακομιστής, του οποίου η απενεργοποίηση θα διέκοπτε τη λειτουργία ολόκληρου του δικτύου. Αντί αυτού όλα τα ζόμπι επικοινωνούν απευθείας μεταξύ τους, γεγονός που προσδίδει στο botnet πολύ μεγαλύτερη σταθερότητα.

Πώς γίνεται η στρατολόγηση

Τα botnets μπορούν να στρατολογούν νέα ζόμπι με διάφορους τρόπους. Εκτός από την εξάπλωση μέσω μολυσμένων e-mail, για την ανάπτυξη ενός botnet μπορούν να χρησιμοποιηθούν και τοποθεσίες web των οποίων τον έλεγχο έχουν αναλάβει χάκερς, εκμεταλλευόμενοι κενά ασφαλείας σε λειτουργικά συστήματα ή λογισμικό εφαρμογών, με αποτέλεσμα τη λεγόμενη "drive-by-infection" δηλαδή, μόλυνση με απλή επίσκεψη. Μια απλή επίσκεψη στη μολυσμένη τοποθεσία web αρκεί για τη μετάδοσή της.

Τα botnets έχουν εξελιχθεί σε μια από τις μεγαλύτερες παράνομες πηγές εσόδων στο Internet. Αφενός με τις ποσότητες των δεδομένων που γίνονται λεία στα χέρια επιτηδείων, αφετέρου με την ενοικίαση botnets σε τρίτους με ωριαία ή μηνιαία ή εφάπαξ χρέωση, π.χ. βάσει του αριθμού της αλληλογραφίας spam που αποστέλλεται μέσω του botnet.

In.gr Τεχνολογία, **G Data**