University of the Aegean, Samos, **2016-2017**
Information & Communication Systems Engineering - **ICSD**

Ασφάλεια Δικτύων Υπολογιστών & Τεχνολογίες Προστασίας της Ιδιωτικότητας

Review of “Botnets: A Survey”

(Διδάσκων)
Γιώργος Καμπουράκης

(Εργαστηριακοί Συνεργάτες)
Δημήτρης Παπαμαρτζίβανος
Αλέξανδρος Φακής

Παρασκευή Παπαδοπούλου
(icsd11122)

Νίκος Τρίτσης
(icsd11162)

Χρήστος Αυλακιώτης
(icsd12015)

University of the Aegean, Samos, **2016-2017**
Information & Communication Systems Engineering - **ICSD**

Ασφάλεια Δικτύων Υπολογιστών & Τεχνολογίες Προστασίας της Ιδιωτικότητας

Review of “Botnets: A Survey”

(Διδάσκων)
Γιώργος Καμπουράκης

(Εργαστηριακοί Συνεργάτες)
Δημήτρης Παπαμαρτζίβανος
Αλέξανδρος Φακής

Παρασκευή Παπαδοπούλου
(icsd11122)

Νίκος Τρίτσης
(icsd11162)

Χρήστος Αυλακιώτης
(icsd12015)

Περιεχόμενα

Εισαγωγή

Στα πλαίσια του μαθήματος Ασφάλεια Δικτύων Υπολογιστών & Τεχνολογίες Προστασίας της Ιδιωτικότητας, κάναμε ένα review του άρθρου Botnets: A Survey. Ακολουθεί μια σύντομη περιγραφή/περίληψη του, και στην συνέχεια η κρίση μας σχετικά με το περιχόμενο του.

Ενότητες

Σημείωση:
Designed for Two-Page View & Show Cover Page (PDF reader settings)

1 Σύντομη Περιγραφή του Άρθρου

Το άρθο αυτό αναφέρεται στα botnets. Με τον όρο botnet αναφερόμαστε σε δίκτυα μηχανών που έχουν προσβληθεί από κακόβουλο λογισμικό και δύναται να καθοδηγηθούν από κάποιον (botmaster/botherder) σε αξιόποινες πράξεις. Αποτελούν ολοένα και περισσότερο αυξανόμενη απειλή στο διαδίκτυο, καθώς οι τύποι επιθέσεων που μπορούν να πραγματωθούν με χρήση ενός botnet αποφέρουν τεράστιες ζημίες (της τάξης των δισεκατομμυρίων δολλαρίων συμφωνα με στατιστικές μελέτες), ενώ η δημιουργία ενός botnet, δεν έχει κόστος, και η απόκτηση ενός είναι πολύ φθηνή (κόστος της τάξης μερικών δολλαρίων).

1.1 Ζημίες και τρόποι αντιμετώπισης τους

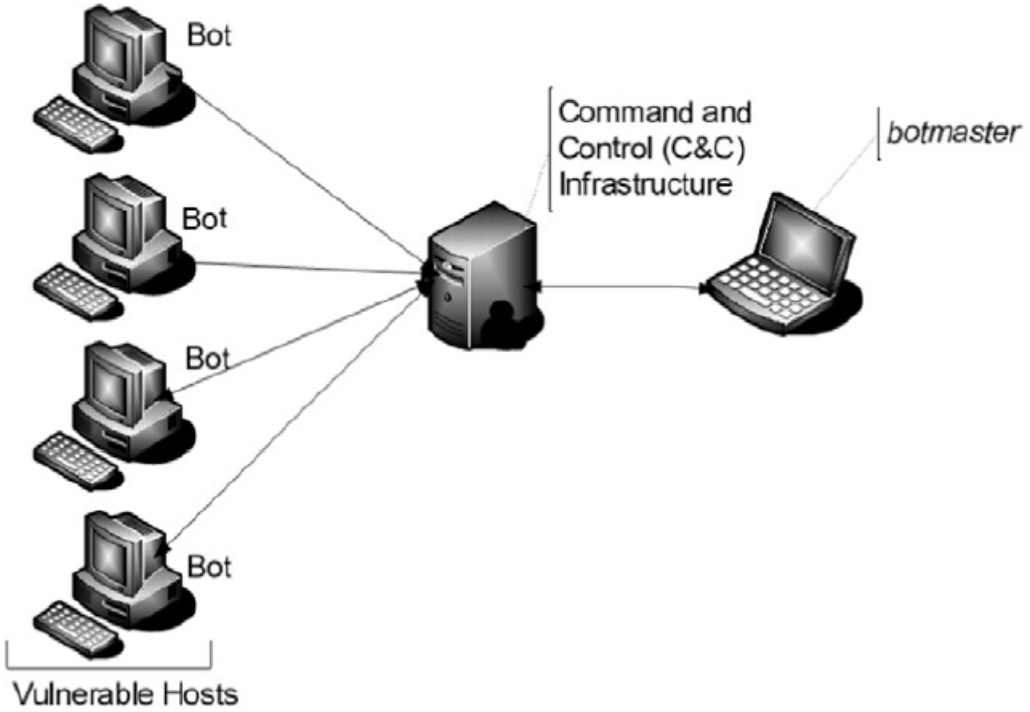
Η δημιουργία ενός botnet βασίζεται στην διασπορά κακόβουλου λογισμικού που δίνει την δυνατότητα σε έναν botmaster να εκτελέσει κακόβουλες διεργασίες απομακρυσμένα. Αυτό φαίνεται να έχει μία αυξητική τάση, λόγω του ότι οι μηχανές που έχουν συνεχή και σταθερή σύνδεση στο Internet, αλλά ταυτόχρονα παρουσιάζουν και ορισμένες ευπάθειες, συνεχώς αυξάνονται καθώς η χρήση του Internet γίνεται όλο και πιο διαδεδομένη. Οι κακόβουλες επιθέσεις που μπορούν να εκτελεστούν με χρήση ενός botnet περιλαμβάνουν τη διανομή κακόβουλου λογισμικού, την πειρατεία λογισμικού, επιθέσεις DDoS (οι οποίες αποτελούν και την συνηθέστερη χρήση ενός botnet), κλοπή προσωπικών δεδομενων, εκβιασμό, spamming και άλλες. Οι δράσεις που μπορούν να παρθούν για την αντιμετώπιση του φαινομένου αυτού, χωρίζονται σε δύο κατηγορίες. Τις αποτρεπτικές/προληπτικές (preventive) και τις αντιδρασης/ανακαμψης (reactive).

Στις δράσεις ανάκαμψης που είναι και οι πιο διαδεδομένες, ανήκουν οι μεθοδολογίες εκείνες που εντοπίζουν και καταστέλλουν μία επίθεση. Βασικά μειονεκτήματα των δράσεων αυτών είναι οι υψηλές απαιτήσεις σε πόρους, καθώς και το γεγονός οτι η επίθεση θα είναι ήδη σε εξέλιξη ώστε να εντοπιστεί, οπότε πιθανόν να υπάρχουν επιπτώσεις ήδη μέχρι την στιγμή της ανακάλυψης της.

Στις δράσεις πρόληψης, ανήκουν οι τεχνικές εκείνες που σκοπό έχουν την αποτροπή των επιθέσεων ή και την παροχή βοήθειας προς το θύμα της επίθεσης ως προς την ενδυνάμωση των αμυνών που παρουσιάζει. Αυτό βέβαια ως στρατηγική, ενέχει πάντοτε τον κίνδυνο και ο επιτιθέμενος να ενδυναμώσει τους πόρους και τα εργαλεία που θα χρησιμοποιήσει.

1.2 Συστατικά στοιχεία ενός botnet

Αναλόγως με την δομή της υλοποίησης μπορεί να υπάρξουν κάποιες μικροδιαφορές, η γενική όμως δομή ενός botnet φαίνεται στο Σχήμα 1. Αποτελούνται από ένα πλήθος μηχανών που έχουν προσβληθεί από malware (Hosts/bots) που ανήκουν σε ένα Command &Control Channel Infrastructure, το οποίο χρησιμοποιεί ο botmaster ώστε να επικοινωνεί με τα bots, και προφανώς την μηχανή του botmaster. Με τον όρο Command & Control Channel Infrastructure, αναφερόμαστε στα bots και μια κεντρικοποιημένη ή αποκεντρικοποιημένη δομή με ρόλο τον έλεγχο των bots.



Σχήμα 1: Συστατικά Στοιχεία ενός Botnet

Οι μηχανές που θα αποτελέσουν μέρος ενός botnet, είναι επιθυμητό να έχουν τα εξής χαρακτηριστικά:

- Υψηλής ταχύτητας σταθερή σύνδεση στο Internet, έτσι ώστε να είναι χρήσιμες στον botmaster, και ταυτόχρονα να μην γίνονται εύκολα αντιληπτό στο θύμα οτι υπάρχουν καθυστερήσεις λόγω του προστιθέμενου φόρτου στο δίκτυο του.

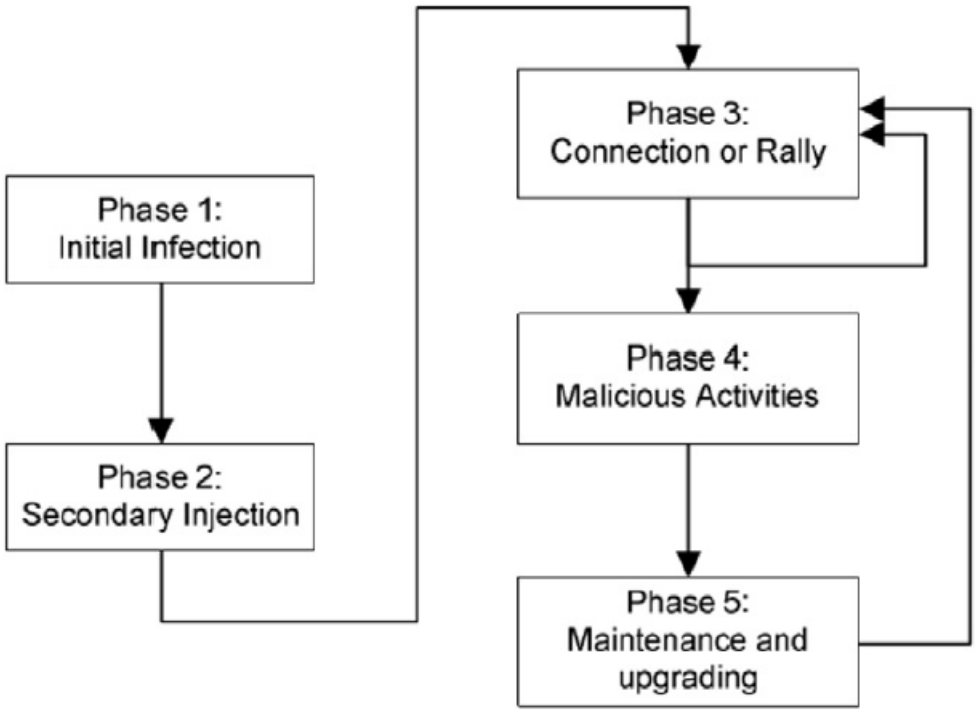
- Διάσπαρτες τοποθεσίες ώστε να εκμεταλλεύεται η διαφορετική ζώνη ώρας στις διάφορες περιοχές, ώστε οι επιθέσεις να είναι ανεξάρτητες του χρόνου.

- Μεγάλη γεωγραφική απόσταση από τον botmaster είναι επιθυμητή, ώστε να μην είναι εύκολο επιθέσεις να συνδεθούν με εκείνον.

- Τέλος, στατιστικά έχει δειχθεί οτι οι περισσότερες μηχανές που αποτελούν στόχο για προσβολή με malware ώστε να αποτελέσουν μέρος ενός botnet τρέχουν λειτουργικό MS Windows.

1.3 Κύκλος ζωής ενός Botnet

Για να ενταχθεί μία μηχανή σε ένα botnet, πρέπει να περάσει από ορισμένα στάδια, τα οποία φαίνονται στο σχήμα 2.



Σχήμα 2: Κύκλος ζωής ενός botnet

Αρχικά, μία μηχανή θεωρείται εν δυνάμει botnet απο την στιγμή της μολυνσης της με κακόβουλο κώδικα (Phase 1). Η τελική φάση (Phase 2) αυτού του σταδίου είναι η λήψη και εκτέλεση του κακόβουλου κώδικα στην μηχανή αυτή, ώστε να μπορέσει να λειτουργήσει ως zombie. Στην συνέχεια η μηχανή πρέπει να συνδεθεί με το C&C ώστε να λάβει updates και οδηγίες(Phase 3), διαδικασία που επαναλαμβάνεται με κάθε boot, και πλεόν είναι μέλος του botnet (Phase 4), και έτοιμη να συμμετέχει σε κακόβουλες ενέργειες.Στο στάδιο αυτό ανταλλάσονται μηνύματα για το σκοπό αυτό, τα οποία όμως οφείλουν να είναι μικρά σε μέγεθος ώστε να μην εγείρουν υποψίες. Τέλος πρέπει να γίνεται συντήρηση και update του κακόβουλου λογισμικού που τρέχει η μηχανή zombie ώστε ο botmaster να συνεχίσει να την έχει υπό τον έλεγχό του.

1.4 Αρχιτεκτονικές C&C

Υπάρχουν 4 βασικές αρχιτοκτονικές για το Command & Control Infrastructure.

1.4.1 Centralized C&C

Στην Συγκεκριμένη αρχιτεκτονική ακολουθείται το client-server μοντέλο, όπου clients θεωρούνται τα bots καi υπάρχουν ένας ή περισσότεροι servers που ρόλο έχουν την απόδοση εντολών στα bots.

Βασικά πλεονεκτήματα αυτής της αρχιτεκτονικής είναι οι γρήγοροι χρόνοι απόκρισης και ο καλό συντονισμός, που κοστίζουν όμως, αφού είναι πιο εύκολο να εντοπιστεί έτσι ένα botnet, ή να διακοπεί η λειτουργία του λόγω αστοχίας του C&C server.

1.4.2 Decentralized C&C

Στην αποκεντρικοποιημένη αρχιτεκτονική το πρόβλημα αυτό μετριάζεται, αφού δεν υπάρχει πλέον κεντρικός C&C server για να εντοπιστεί και να απενεργοποιηθεί. Αντ'αυτού, υπάρχουν P2P overlays. Ετσι, ακόμα και αν εντοπιστούν ορισμένα bots και απενεργοποιηθούν, το botnet μπορεί να συνεχίσει να υπάρχει αφού δεν θα εκτεθούν όλα και θα ανακτήσει το μέγεθος του σε βάθος χρόνου.

1.4.3 Hybrid C&C

Στην υβριδική αρχιτεκτονική συνδυάζονται οι κεντρικοποιημένη και αποκεντρικοποιημένη αρχιτεκτονική. Τα bots θα μπορούσαν να χωριστούν σε δύο ομάδες, τα servant και τα client bots. Τα servant λειτουργούν και ως clients και ως servers, ενώ τα client όχι. Η επικοινωνία των servant bots είναι κρυπτογραφημένη και καθιστά πολύ δύσκολο τον εντοπισμό τους.

1.4.4 Random C&C

Τέλος, ένα θεωρητικό μοντέλο για την αρχιτεκτονική του C&C, προτίνει μη ενεργή επικοινωνία μεταξύ botmaster και bot, ή μεταξύ bots. Αντιθέτως, κάθε bot αναμένει συνδέση απο τον botmaster ώστε να λάβει εντολές. Ο botmaster οφείλει να ψάξει στο δικτυό του για να βρει zombie μηχανές. Η πρακτική αυτή καθιστά τον εντοπισμό του botnet δύσκολη, αλλά εισάγει προβλήματα συντονισμού.

1.4.5 Τεχνικές Ανίχνευσης

Η ανίχνευση ενός botnet είναι το πρώτο και σημαντικοτερο βήμα που πρέπει να γίνει για την αντιμετώπιση τέτοιων απειλών. Οι επιλογές είναι δύο σε αυτό το κομμάτι, η χρήση honeynet ή η χρήση IDS (Intrusion Detection System).

1.4.6 HoneyNets

Με τον όρο HoneyNet αναφερόμαστε σε δίκτυα που έχουν ηθελημένες ευπάθειες ώστε να προσελκύσουν τον εν δυνάμει επιτιθέμενο. Όμως παρουσιάζουν περιορισμούς και πλέον αποτελέι γνωστή τακτικη, και οι επιτιθέμενοι μαθαίνουν να τις αναγνωρίζουν ως παγίδες και να τις αποφεύγουν.

1.4.7 IDS

Τα συστήματα ανίχνευσης εισβολών λειτουργούν με δύο διαφορετικές τεχνικές. Signature-based ή anomaly-based. Με τον όρο signature-based αναφερόμαστε σε σε τεχνικές ανίχνευσης με βάση την υπογραφή του κακόβουλου λογισμικού. Αυτό συνεπάγεται μία καθυστέρηση στην ανίχνευση του, αφού πρώτα θα πρέπει να έχει εντοπιστεί και να αποτελεί γνωστή απειλή. Ετσι βασικό μειονέκτημα είναι η μη ανίχνευση άγνωστων υπογραφών καθώς και η αδυναμία εντοπισμού zero-day bot attacks. Επιπρόσθετα, αποτελεί μη αυτοματοποιημένη διαδικασία, αφού η γνώση σχετικά με τις υπογραφές των malware θα πρέπει συνεχώς να ανανεώνεται.
Με τον όρο anomaly-based αναφερόμαστε σε τεχνικές που θα ανιχμεύσουν τυχόν ανωμαλίες στην γενικότερη επίδοση του συστήματος μας. Αποκλίσεις απο την “αποδεκτή/συνήθη” συμπεριφορά κινούν υποψίες. Αυτός ο έλεγχος μπορεί να είναι είτε host-based είτε network-based. Η διαφορά έγκειται στο ότι στην περίπτωση των host-based τεχνικών η σκοπιά παρατήρησης είναι η ίδια η μηχανή και ενδιαφέρουν μετρικές όπως η αύξηση του χρόνου επεξεργασίας ή η πρόσβαση σε συγκεκριμένα αρχεία συστήματος. Αντιθέτως, στην περίπτωση network-based τεχνικών μας ενδιαφέρουν μετρικές της απόδοσης του δικτύου και της απόκρισης του. Αυτό γίνεται είτε με active τεχνικές όπως η εισροή πακέτων και η παρακολούθηση της απόκρισης του δικτύου σε αυτά ώστε να καθοριστεί εάν ένα bot ελέγχει την επικοινωνία, ή με passive τεχνικές όπως η παρακολούθηση της κίνησης του δικτύου και η προσπάθεια ανιχνευσης ύποπτων επικοινωνιών.
Στον τομέα του network-based ελέγχου, έχει προταθεί η ανίχνευση χρήσης IRC πρωτοκόλλου, αφού ο botmaster θα μπορούσε να επικοινωνεί με τα bots με χρήση IRC και άρα θα αποτελούσε ένδειξη για την ύπαρξη botnet. Επίσης θα μπορούσαν να αναλυθούν DNS ερωτήματα ώστε να οδηγήσουν στον εντοπισμό ενός botnet. Επίσης η χρήση διαφόρων εργαλείων για την αποφυγή περετάιρω εξάπλωσης ενος botnet μέσω spam emails έχει προταθεί και ερευνηθεί, καθώς και ο εντοπισμός μέσω P2P πρωτοκόλλου και αναλύσης των δεδομένων που ανταλάσσονται. Και για αυτό το κομμάτι αναπτύχθηκαν εργαλεία με σκοπό τον εντοπισμό ενεργών botnet.

1.4.8 Αποφυγή Ανίχνευσης

Για να αποφευχθεί η ανίχνευση ενός botnet με τις παραπάνω τεχνικές, οι botmasters προσπαθούν να αναπτύξουν δίκτυα από bots με βάση δύο παράγοντες. Το πόσο εύκολα μπορούν να αλλάξουν τον κακόβουλο κώδικά τους τόσο, όσο να αποφύγουν την ανίχνευση και το πόσο λειτουργικό απομένει το botnet αφού εφαρμοστούν τα αντίμετρα. Προφανώς επιδιώκεται μεγάλη ευκολεία στις μεταβολές του κώδικα σε συνδυασμό με τη μέγιστη λειτουργικότητα. Τετοιες τεχνικές είναι η κρυπτογραφηση των δεδομένων κίνησης, η απόδοση διαφορετικών εργασιών σε διαφορετικά bots του ίδιου botnet, τυχαιοποίηση των patterns σύμφωνα με τα οποία επικοινωνούν τα bots κτλ.

1.4.9 Τεχνικές Άμυνας

Από την στιγμή που θα ανιχνευθεί ένα botnet είτε θα σταματίσει να λειτουργεί ως bot η συγκεκριμενη μηχανή που αποκαλύφθηκε, είτε θα απενεργοποιηθεί όλο το botnet. Προφανώς στην πρώτη περίπτωση δεν λύνεται το πρόβλημα καθώς αποτελεί αμελητέα απώλεια για το σύνολο. Οι αμυντικές τεχνικές συμπεριλαμβάνουν την αποφυγή διάδοσης κακόβουλου λογισμικού άρα την αποφυγή της εξάπλωσης ενός botnet και άρα τελικά την μείωση της ισχύς του από πλευράς λειτουργικότητας. Για το λόγο αυτό θα πρέπει να υπάρχουν μέτρα πρόληψης, αντιμετώπισης και περιορισμού. Σημαντικό ρόλο σε αυτό το κομμάτι παίζει και ο σχεδιασμός των συστημάτων, καθώς η ασφάλεια που παρέχεται θα πρέπει να είναι built-in και όχι add-on, όσον αφορά το σχεδιασμό λογισμικού.

1.4.10 Νέες Τάσεις

Με την εξέλιξη της τεχνολογίας και αναπόφευκτα την εξέλιξη των συστημάτων επικοινωνίας, δόθηκαν πολλές νέες ευκαιρίες προς κακόβουλη εκμετάλλευση. Πέρα από τους υπολογιστές, μια μεγάλη ποικιλία νεών συσκευών (κινητά τηλέφωνα, φορητοί υπολογιστές) αποτελούν στόχο κακόβουλων ενεργειών. Οι πλατφόρμες κοινωνικών δικτύων επίσης έχουν τραβήξει το ενδιαφέρον, καθώς φαίνεται πως μπορούν να λειτουργήσουν ως μέρος ενός botnet, ή να παραπλανήσουν χρήστες. Εμφάνιση έκαναν και τα mini-bots που αποτελούν μικρής κλίμακας εξειδικευμένα botnets που χρησιμοποιούνται κυρίως για άλλες μορφές επιθέσεων πέρα από DDoS, κυρίως για κλοπή ταυτότητας και προσωπικών στοιχείων.

1.4.11 Προκλήσεις

Μεγάλη πρόκληση στο πεδίο αυτό αποτελεί η άνιση κατανομή των πόρων απέναντι σε κακόβουλους χρήστες και ευρευνητές που ασχολούνται με το φαινόμενο αυτό. Οι πρώτοι έχουν στη διάθεση του μια πληθώρα από πόρους και πιθανούς στόχους, ενώ οι δεύτεροι έχουν περιορισμένους πόρους και δεδομένα προς ανάλυση. Ετσι είναι πιθανό κάποιες φορές η έρυνα να μην ανταποκρίνεται απολύτως σε πραγματικά στοιχεία. Επίσης, είναι πολύ δύσκολο να συγκριθούν τεχνικές που προτίνονται σε ερευνητικό επίπεδο καθώς δεν υπάρχουν κοινά

αποδεκτές μετρικές ώστε να είναι αντικειμενική η σύγκριση. Ανοιχτά πεδία είναι αυτά των κινητών συσκευών μιας και η έρευνα σε αυτό το κομμάτι είναι σε αρχικό στάδιο, ενώ παρουσιάζουν διαφορές στον τρόπο λειτουργίας τους, όπως πχ ο τρόπος σύνδεσης στο διαδίκτυο είναι δυναμικός λόγω της φύσης της συσκευής. Η άμεση λύση που φαίνεται σε αυτό το πεδίο είναι η ενημέρωση του χρήστη και η εκπαίδευση του.

1.4.12 Συμπεράσματα

Τα botnets αποτελούν μεγάλη απειλή ασφάλειας στο διαδίκτυο. Για την καταπολέμιση τους χρειάζονται αποτελεσματικές τεχνικές ανίχνευσης και στην συνέχεια εύρεση ενός τρόπου για τον “διαμελισμό” του botnet. Από την πλευρά του botmaster, νέες ευκαιρίες εμφανίζονται καθώς εξελίσεται η τεχνολογία, ενώ παράλληλα έχει την δυνατότητα να κάνει ακόμα πιο “αόρατη” την ύπαρξη του. Από την πλευρά των ερευνητών, σημαντική τροχοπέδη αποτελεί η έλλειψη συγκριτικής βάσης των προτάσεων τους, ένω προτείνεται η δημιουργία παγκόσμιων συστημάτων και η λήψη παγκοσμιων αντίμετρων για την καταπολέμηση τέτοιων φαινομένων.

2 Κρίση του Άρθρου

Κίνητρο των συγγραφέων αποτελεί το αυξανόμενο ερευνητικό ενδιαφέρον που παρουσιάζουν τα botnets. Οι ίδιοι θεωρούν πως μέχρι εκείνη τη στιγμή υπήρχε ένα κενό στην βιβλιογραφία αφού τα μέχρι τότε άρθρα δεν έχουν συγκεντροτικό χαρακτήρα και στόχος τους είναι να δώσουν περιεκτικά και με σαφήνεια το περιεχόμενο των ερευνών στο αντικείμενο έως τότε, καθώς και να συζητηθούν προτάσεις, λύσεις και ανοιχτές προκλήσεις στο πεδίο έρευνας αυτό. Θεωρούμε πως οι συγγραφείς πετυχαίνουν το στόχο τους αυτό, γράφοντας ένα περιεκτικό και σαφές survey, που συνεισφέρει στην επιστημονική κοινότητα, καθώς συνοψίζει εργασίες ετών πάνω στο αντικείμενο, κατατοπίζει έτσι πιθανόν και νέους ερευνητές. Θεωρούμε επίσης πως το αρθρο αυτό καλύπτει το θέμα που συζητάει αφού κάνει εκτενείς αναφορές σε προηγούμενες δημοσιεύσεις χωρις παραλήψεις, και μάλιστα το κάνει με τρόπο κατανοητό από τον αναγνώστη, αφού το ύφος που χρησιμοποιείται και ο τρόπος συγγραφής του κρίνεται ως ιδιαίτερα άμεσος.

3 Βιβλιογραφία

[1] Sergio S.C. Silva, Rodrigo M.P. Silva, Raquel C.G. Pinto, Ronaldo M. Salles, “Botnets: A Survey”, Computer Networks vol.57, pp.378-403, 2013