ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΣΧΟΛΗ ΘΕΤΙΚΩΝ ΕΠΙΣΤΗΜΩΝ
ΤΜΗΜΑ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΤΗΛΕΠΙΚΟΙΝΩΝΙΩΝ

ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
«ΝΕΕΣ ΤΕΧΝΟΛΟΓΙΕΣ ΠΛΗΡΟΦΟΡΙΚΗΣ ΚΑΙ ΕΠΙΚΟΙΝΩΝΙΩΝ»

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

BotNet
σε συσκευές κινητής τηλεφωνίας
3ης γενιάς

Άγγελος Ν. Κουλός

Επιβλέποντες: **Καθ. Παναγιώτης Γεωργιάδης**
Δρ. Κωνσταντίνος Παπαπαναγιώτου

ΑΘΗΝΑ

10 - 2011

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

BotNet
σε συσκευές κινητής τηλεφωνίας
3ης γενιάς

Άγγελος Ν. Κουλός

Α.Μ.: 1117

ΕΠΙΒΛΕΠΟΝΤΕΣ: **Καθ. Παναγιώτης Γεωργιάδης**
Δρ. Κωνσταντίνος Παπαπαναγιώτου

ΕΞΕΤΑΣΤΙΚΗ ΕΠΙΤΡΟΠΗ:

10 - 2011

ΠΕΡΙΛΗΨΗ

Η παρούσα διπλωματική εργασία εκπονήθηκε στα πλαίσιο ολοκλήρωσης του προγράμματος μεταπτυχιακών σπουδών του Τμήματος «Πληροφορικής και Τηλεπικοινωνιών». Αντικείμενο της εργασίας, αποτελεί η διερεύνηση των μεθόδων εντοπισμού και αντιμετώπισης των botnet, εστιάζοντας στη περίπτωση των κινητών τηλεφώνων τελευταίας γενιάς. Η υπολογιστική ισχύς των έξυπνων κινητών τηλεφώνων έχει αυξηθεί κατακόρυφα και χρησιμοποιούνται τώρα πλέον, όχι μόνο για τηλεφωνικές κλήσεις και αποστολή-λήψη sms, αλλά και σε εφαρμογές διαδικτύου όπως κοινωνική δικτύωση, e-baniking, e-mail, ηλεκτρονικές αγορές. Τα τελευταία δύο χρόνια μάλιστα, τα έξυπνα κινητά τηλέφωνα τείνουν να αντικαταστήσουν στην χρήση τους φορητούς ηλεκτρονικούς υπολογιστές .
Ο σκοπός της εργασίας είναι η κατανόηση του τρόπου λειτουργίας των botnet, των απειλών που επιφέρουν καθώς και των μεθόδων εντοπισμού και αντιμετώπισης τους. Μεθοδολογικά, η παρούσα εργασία, βασίζεται στην εκτενή βιβλιογραφική ανασκόπηση ξένων και αρκετά πρόσφατων πηγών, όπως οι τεχνικές αναφορές του Ευρωπαϊκού Οργανισμού για την Ασφάλεια Δικτύων και Πληροφοριών (ENISA).

ΘΕΜΑΤΙΚΗ ΠΕΡΙΟΧΗ: Ασφάλεια Δικτύων

ΛΕΞΕΙΣ ΚΛΕΙΔΙΑ: Ασφάλεια, Δίκτυα, Ασφάλεια Δικτύων, Botnet, έξυπνα τηλέφωνα.

ABSTRACT

This thesis was produced as a part of completion of the postgraduate program in the Department «Informatics and Telecommunication». The scope of this work is to investigate methods for identifying and addressing the botnet, focusing on the case of the latest mobile phones. The computing power of smart mobile phones has increased dramatically and now are used not only for telephone calls and send-receive SMS, but also in web applications like social networking, e-banking, e-mail, online shopping. The last two years, especially, smart mobile phones, tend to replace the use of laptop computers. The purpose of this work is to understand the workings of the botnet, the threats and bring about the methods to identify and respond to them. Methodologically, this thesis is based on extensive literature review and several recent foreign sources, such as technical reports of the European Agency for Safety and Information Network (ENISA)

SUBJECT AREA: network security

KEYWORDS: security, network, network security, Botnet, smart mobile phones.

Αφιερώμενο στην οικογενειά μου και τους γονείς μου.

ΕΥΧΑΡΙΣΤΙΕΣ

Στον προιστάμενο και φίλο Στρατή Μαραγκό για την καθοδήγηση
Στο φίλο και συνάδελφο Κώστα Ιωάννου για την κριτική ανάγνωση.

ΠΙΝΑΚΑΣ ΠΕΡΙΕΧΟΜΕΝΩΝ

ΚΑΤΑΛΟΓΟΣ ΣΧΗΜΑΤΩΝ

ΚΑΤΑΛΟΓΟΣ ΠΙΝΑΚΩΝ

ΕΙΣΑΓΩΓΗ

Τα botnet ορίζονται ως δίκτυα υπολογιστών που ελέγχονται με απομακρυσμένη πρόσβαση από τον botmaster έχοντας υπονομεύσει τα συστήματα χωρίς τη γνώση ή την έγκριση των κατόχων τους. Οι botmaster χρησιμοποιούν αυτούς του υπολογιστές-ζόμπι για διάφορους παράνομους σκοπούς, αφού έχει τη δυνατότητα πρόσβασης στα αρχεία του συστήματος όσο και τη χρήση της σύνδεσης δικτύου του υπολογιστή, χωρίς να το αντιληφθεί ο ιδιοκτήτης του. Το γεγονός αυτό παρέχει στον botmaster αμέτρητες δυνατότητες, όπως η μετάδοση του κακόβουλου κώδικα bot ή η μαζική αποστολή spam. Επιπλέον, εκτός της υποκλοπής δεδομένων ο botmaster καταφέρνει να αποκρύπτει τη ταυτότητα του αφού ως διακομιστής μεσολάβησης χρησιμοποιείται ο υπολογιστής του θύματος.

Κατά συνέπεια γίνεται εύκολα αντιληπτό ότι η σύγχρονη παγκόσμια οικονομία αντιμετωπίζει μια μεγάλη ποικιλία απειλών λόγω κακόβουλου λογισμικού, που μπορούν να προκαλέσουν μεγάλη ζημιά. Επιπλέον, τα botnet έχουν εξελιχθεί σε μια από τις μεγαλύτερες παράνομες πηγές εσόδων στο Internet, ενώ οι εκάστοτε κυβερνήσεις και φορείς ξοδεύουν πολλά εκατομμύρια για να τα εξαλείψουν.

Σε ότι αφορά τις κυριότερες επιθέσεις που αναμένεται να εκδηλωθούν στον κυβερνοχώρο στο άμεσο μέλλον, οι τάσεις που διαφαίνονται στην ανάπτυξη των botnet και του ηλεκτρονικού εγλήματος γενικότερα, καταδεικνύουν ότι τα έξυπνα κινητά τηλέφωνα και οι εφαρμογές κοινωνικές δικτύωσης αποτελούν τους άμεσους στόχους των botmaster.

Είναι αναμενόμενο ότι όσο η υπολογιστική ισχύς των κινητών τηλεφώνων θα αυξάνεται, η διάδοση των υπολογιστών Mac και των ‘έξυπνων’ κινητών τηλεφώνων θα συνεχίζεται και οι τεχνολογίες τους θα αναπτύσσονται, τόσο περισσότεροι εισβολείς θα ασχολούνται με τη δημιουργία κακόβουλου λογισμικού που θα εκμεταλλεύεται τα ευπαθή σημεία αυτών των συσκευών.

Για το λόγο αυτό σημαντικοί φορείς συνεργάζονται και πραγματοποιούν έρευνα τόσο σχετικά με τον εντοπισμό των botnet όσο και με την εφαρμογή κατάλληλων αντιμέτρων για την αντιμετώπιση τους.

Στο πρώτο κεφάλαιο περιγράφεται το κακόβουλο λογισμικό και η σχέση του με τα δίκτυα bot, η βασική υποδομή ενός δικτύου bot και τα είδη αρχιτεκτονικής του, τα κίνητρα (κυρίως οικονομικά) που κρύβονται πίσω από την χρήση τους, οι απειλές που απορρέουν από τις δράσεις τους, ενώ ενδεικτικά παρουσιάζονται συνοπτικά κάποια διάσημα botnet είτε λόγω του μεγέθους που έφτασαν, είτε λόγω της δράσης που έχουν αναπτύξει, είτε λόγω των επιπτώσεων που επέφεραν.

Στη συνέχεια αναπτύσσονται οι τεχνικές ανίχνευσης των botnet, αναλύονται διακριτά οι δύο μεγάλες ομάδες τους και γίνεται αξιολόγηση τους, ανάλογα με τον τρόπο εφαρμογής, την ποιότητα των αποτελεσμάτων αλλά και τους περιορισμούς (κυρίως νομικούς) που υπάρχουν. Οι παθητικές, που περιορίζονται κυρίως στην παρακολούθηση και συλλογή στοιχείων και ως εκ τούτου είναι αόρατες από τους κακόβουλους χρήστες, και οι ενεργητικές που αλληλεπιδρούν με τον περιβάλλον παρακολούθησης και άρα είναι δυνατόν να πυροδοτήσουν αντιδράσεις.

Στο τρίτο κεφάλαιο παρουσιάζονται τα αντίμετρα που μπορούν να ληφθούν για την αντιμετώπιση των botnet και διαχωρίζονται σε τρεις κατηγορίες, στις τεχνικές μεθόδους στις νομοθετικές ρυθμίσεις και στις κοινωνικού χαρακτήρα προσεγγίσεις. Επίσης δίνονται παραδείγματα από πρωτοβουλίες τόσο σε επίπεδο εθνικό, όσο και σε διεθνές, αλλά και από πετυχημένες δράσεις ομάδων εργασίας.

Ακολούθως σκιαγραφούνται οι τάσεις της εξέλιξης, στη δομή και τη διάδοση των botnet, στο τρόπο εμπορευματοποίησης και στη μελλοντική ανάπτυξη τους. Δίνονται συστάσεις που αφορούν την ορθή πρακτική κατά την καταπολέμηση της απειλής των botnet και ορίζονται σαν στόχοι: ο μετριασμός των υφιστάμενων botnet, η πρόληψη νέων μολύνσεων και η μείωση του κέρδους από την εκμετάλλευση τους. Τέλος γίνονται προβλέψεις που αφορούν τη διάδοση των ‘έξυπνων’ **κινητών τηλεφώνων** και τον κίνδυνο που σχετίζεται με τα ευπαθή σημεία αυτών των συσκευών.

1 ΤΑ BOTNET

1.1 Γενικές αρχές

Το κακόβουλο λογισμικό, για συντομία «Malware», έχει αποκτήσει μια σημαντική θέση στη σύγχρονη υψηλή τεχνολογία. Ξεκινώντας από την πρώτη χρήση προγραμματιζόμενων συστημάτων, υπήρχαν προσεγγίσεις να τα “προσβάλλουν” με λογισμικό που περιέχει κακόβουλη λειτουργικότητα, αλλά, στο παρελθόν, το κακόβουλο λογισμικό είχε μόνο περιορισμένη ή τοπική επίπτωση. Η επιτυχία του Διαδικτύου έγινε επίσης ένα σημείο εκκίνησης για τις αναφορές σχετικά με εκτεταμένες μολύνσεις από κακόβουλο λογισμικό που αφορά πολλά εκατομμύρια συστήματα σε όλο τον κόσμο. Σχεδόν ταυτόχρονα, τηλεχειριζόμενο δίκτυα υπολογιστών που είχαν υποστεί πειρατεία, τα λεγόμενα botnet, άρχισαν να γίνονται δημοφιλή. Μια σημαντική παρατήρηση είναι ότι το κίνητρο για τη δημιουργία κακόβουλου λογισμικού έχει αλλάξει δραματικά κατά την τελευταία δεκαετία. Δεν έχει πλέον πρωταρχικό στόχο να εδραιώσει τη φήμη του μέσα σε μια σχεδόν μυστικιστική κοινότητα ατόμων με υψηλή τεχνικά εξειδίκευση. Με το Διαδίκτυο εύκολα προσβάσιμο σε όλους και διαδεδομένη πλέον τη χρήση οικονομικά προσανατολισμένων υπηρεσιών, όπως οι ηλεκτρονικές αγορές και τραπεζικές συναλλαγές, περιστασιακοί χρήστες, με ελάχιστες τεχνικές γνώσεις έχουν γίνει πολλά υποσχόμενοι στόχοι για τους εγκληματίες. Τώρα πλέον το οικονομικό κέρδος είναι τώρα το κύριο κίνητρο για “on line” εγκληματικές πράξεις, και τη δημιουργία κακόβουλου λογισμικού.

Ως αποτέλεσμα, η παγκόσμια οικονομία σήμερα αντιμετωπίζει ένα ευρύ φάσμα malware που, στο σύνολό του, κάνει μεγάλη ζημιά. Αλλά οι εκτιμήσεις για το πόσο, διαφέρουν σε μεγάλο βαθμό. Μια έκθεση της ITU, δίνοντας μια γενική εικόνα των οικονομικών μελετών σχετικά με κακόβουλο λογισμικό, παρουσίασε ποσά που κυμαίνονται από 13.2$ US δισεκατομμυρίων για την παγκόσμια οικονομία το 2006 έως 67.2$ US δισεκατομμυρίων για τις αμερικανικές επιχειρήσεις μόνο το 2005. Εκθέσεις εκτιμούν, άμεσο κόστος για τους πολίτες των ΗΠΑ από malware και spam σε 7.1$ US δισ. δολάρια το 2007. Το κόστος της απάτης (click fraud) το 2007 στις ΗΠΑ εκτιμάται σε $ US1 δις . Ενώ το πλήθος των malware αυξάνεται με εκθετικούς ρυθμούς τα τελευταία χρόνια, έχει μετρηθεί μια φθίνουσα πορεία, στον αντίκτυπο των επιθέσεων malware, για τις επιχειρήσεις παγκοσμίως, με οικονομικό κόστος της 17.5 δισ. δολάρια το 2004, 14 0,2$ US δισ. το 2005 και 13.3$ US δισ. ευρώ το 2006. Οι λόγοι αυτής της μείωσης, είναι ότι, σε αυτά τα χρόνια, τα anti-virus προϊόντα έχουν διαδοθεί ευρύτερα σε εταιρείες και ότι ο στόχος των δημιουργών malware έχει μετατοπιστεί από τη πρόκληση καταστροφής σε άμεσο οικονομικό όφελος. Κατά συνέπεια, οι έμμεσες και δευτερογενείς δαπάνες που πραγματοποιήθηκαν από κακόβουλο λογισμικό αυξάνονται. Την ίδια στιγμή, έχει γίνει μετατόπιση του κέντρου βάρους στο να κλέψουν τα στοιχεία και διαπιστευτήρια για πρόκληση οικονομικών απωλειών, για παράδειγμα, η κατάχρηση πιστωτικών καρτών έχει αυξήσει σημαντικά την απειλή για ιδιώτες χρήστες του Διαδικτύου.

Όροι, όπως ιός, worm, δούρειος ίππος, rootkit, και άλλοι, έχουν συσταθεί για την ταξινόμηση και διάκριση διάφορων τύπων κακόβουλου λογισμικού, σύμφωνα με τη λειτουργικότητα και το σκοπό τους. Ακολούθως θα δοθεί μια σύντομη επισκόπηση αυτών των διαφορετικών τύπων και περιγραφή της σημασίας τους στο πλαίσιο των botnet.

1.1.1 Το "Malware"

Τα τελευταία χρόνια, η ποικιλομορφία του κακόβουλου λογισμικού έχει αυξηθεί σχεδόν εκθετικά. Νέες εκδόσεις εμφανίζονται κάθε μέρα, με συνεχή βελτίωση των τεχνικών που χρησιμοποιούνται και ένα αυξανόμενο βαθμό πολυπλοκότητας. Ένας δείκτης που αναφέρεται συχνά, της εξέλιξης malware, είναι ο αριθμός των δειγμάτων malware που έχουν ανακαλυφθεί, ή υπογραφές ανίχνευσης που παράγονταν από τους παρόχους anti-malware λογισμικού. Για παράδειγμα, η Symantec αναφέρει ότι, το 2009 δημιουργήθηκαν, συνολικά 2.895.802 νέες υπογραφές για την ανίχνευση του malware, το 51% του συνόλου των υπογραφών που δημιουργήθηκε ποτέ από αυτούς . Η Kaspersky εντόπισε περίπου 15 εκατομμύρια μοναδικά δείγματα malware το 2009, πράγμα που σημαίνει ότι ένα άγνωστο δείγμα ανακαλύφθηκε κάθε 2 περίπου δευτερόλεπτα.

Η αύξηση του αριθμού των δειγμάτων είναι αποτέλεσμα της ευρείας εφαρμογής της έννοιας του πολυμορφισμού σε δυαδικά αρχεία malware. Το πολυμορφικό κακόβουλο λογισμικό περιέχει μια σταθερή ακολουθία κώδικα που τροποποιεί το κακόβουλο δυαδικό κώδικα κατά τη διάρκεια της μετάδοσης, αλλά παραμένει αμετάβλητη η ίδια. Έτσι το κακόβουλο λογισμικό αλλάζει πλήρως σε κάθε προσπάθεια διάδοσης.

Πολυμορφισμός και μεταμόρφωση είναι δύο μόνο παραδείγματα από τεχνικές που χρησιμοποιούν οι προγραμματιστές και χρήστες malware για να επιτύχουν τους στόχους τους. Σε γενικές γραμμές, τα κίνητρα πίσω από τη δημιουργία του malware είναι, για παράδειγμα, το προσωπικό οικονομικό ή υλικό όφελος, πολιτικό συμφέρον ή απλά ενδιαφέρον για τις τεχνικές δυνατότητες του.

Virus (Ιός)

Ο όρος χρησιμοποιείται συχνά για να περιγράψει διάφορους τύπους malware, ακόμη και αν αυτά δεν ταιριάζουν με τα χαρακτηριστικά που σχετίζονται με τον πραγματικό ορισμό του ιού. Εκτός από τη γενική χρήση του όρου, ο ιός είναι ένας συγκεκριμένος τύπος κακόβουλου λογισμικού που χαρακτηρίζεται από αυτο-αναπαραγωγή. Κάθε ιός χρειάζεται έναν ξενιστή, π.χ. ένα εκτελέσιμο αρχείο, στον οποίο θα ενσωματώσει τον εαυτό του. Έτσι εξαπλώνεται, με την αντιγραφή του σε άλλα συστήματα υποδοχής. Η διάδοση του μεταξύ άλλλων συστημάτων συμβαίνει όταν τα μολυσμένα αρχεία μεταφέρονται στα άλλα συστήματα. Επομένως ένας ιός μπορεί να χαρακτηριστεί ως παθητικός. Ανάλογα με την ανάπτυξή του, ένας ιός μπορεί να χρησιμοποιήσει όλα τα είδη των μέσων για αυτά τις αναπαραγωγικές του δυνατότητες, όπως τα συστήματα αρχείων που βασίζονται σε δίκτυα ή αφαιρούμενα μέσα.

Worm (σκουλήκι)

Σε αντίθεση με έναν ιό, ο τύπος **worm**, όχι μόνο έχει τη δυνατότητα να αντιγράψει τον εαυτό του με διαφορετικά μέσα, αλλά είναι επίσης σε θέση να εξαπλωθεί ενεργά. Ένας τύπος worm είναι σε θέση να ψάξει μόνος του για άλλους υπολογιστές στο δίκτυο και να τους μολύνει, αν έχουν χαρακτηριστεί ως ευάλωτοι. Αυτό συνήθως επιτυγχάνεται με την αξιοποίηση γνωστών ή άγνωστων τα τρωτών σημείων του λειτουργικού συστήματος ή επιπλέον λογισμικό που είναι εγκατεστημένο σε αυτό. Ένας ιός τύπου worm δεν περιέχει απαραίτητα καταστροφικό ή διεισδυτικό κώδικα που βλάπτει τα συστήματα του θύματος άμεσα. Μερικά worm έχουν σχεδιαστεί αποκλειστικά για να εξαπλωθεί και να δημιουργήθει τελικά ένα κανάλι επικοινωνίας με κάποια ελέγχουσα οντότητα. Σε αυτό το πλαίσιο θα χρησιμεύσουν ως ενεργοί φορείς. Ωστόσο, πρέπει να αναφερθεί ότι τα σκουλήκια θα βλάψουν γενικά το σύστημα ή το δίκτυο έμμεσα. Με την κατανάλωση των πόρων, όπως η υπολογιστική ισχύ και το εύρος ζώνης του δικτύου, προκαλούν συχνά

αστάθεια στα συστήματα υποδοχής. Με δραστηριότητες ειδικά συνεχούς σάρωσης, καταναλώνουν πολλούς πόρους και μπορεί να επηρεαστεί σημαντικά το δίκτυο.

Trojan Horse (Δούρειος Ίππος)

Ενώ τα σκουλήκια λειτουργούν αθόρυβα και αυτόνομα, ο δούρειος ίππος είναι ένα κομμάτι του κακόβουλου λογισμικού που ακολουθεί μια διαφορετική προσέγγιση. Σε γενικές γραμμές, ένας δούρειος ίππος κρύβει κακόβουλες ρουτίνες προσποιούμενος ότι είναι νόμιμο λογισμικό που εκτελεί καλή τη πίστη εργασίες. Προσποιούμενα ότι έχουν έννομο σκοπό, παρασύρουν τον χρήστη σε εγκατάσταση ή εκτέλεση λογισμικού που περιέχει το δούρειο ίππο, ο οποίος φορτώνει τότε τις ενσωματωμένες κακόβουλες ρουτίνες.

Spyware, Keylogger, Sniffer

Ένα χαρακτηριστικό είδος κακόβουλου λογισμικού έχει τη δυνατότητα να εξάγει ζωντανά δεδομένα από ένα απομακρυσμένο σύστημα. Αυτό συνήθως επιτυγχάνεται με την υπονόμευση λειτουργιών σε επίπεδο λειτουργικού συστήματος. Δημιουργούνται έτσι υποομάδες malware που το όνομά τους σχετίζεται με τη δραστηριότητά τους. **Spyware** είναι ένας γενικός όρος για λογισμικό γραμμένο με την πρόθεση της εξόρυξης δεδομένων. Αυτό μπορεί να κυμαίνεται από την παρακολούθηση της συμπεριφοράς των χρηστών για τη βελτιστοποίηση των διαφημίσεων έως επιθετικές μορφές, όπως η κλοπή σειριακών αριθμών λογισμικού ή άλλα ευαίσθητα δεδομένα, όπως στοιχεία πιστωτικών καρτών. **Keylogger είναι** το κακόβουλο λογισμικό που καταγράφει τις πληκτρολογήσεις, προκειμένου να πάρει τα διαπιστευτήρια. S**niffers** λέγονται τα εργαλεία που για τις αναλύσεις του δικτύου, τα οποία είναι χρήσιμα σε ένα κακόβουλο πλαίσιο, και παρακολουθούν την κίνηση του δικτύου, προκειμένου να φιλτράρουν πληροφορίες.

Rootkit

Σε γενικές γραμμές, ένα malware κατοικεί στο σύστημα του υπολογιστή του θύματος, σιωπηλά εν αγνοία του συστήματος (του λογαριασμού root). Ακόμα και αν μετά τα πλήρη αποτελέσματα των δραστηριοτήτων του, ένα malware δεν μπορεί να κρυφτεί, συνήθως θα προσπαθήσει να μείνει όσο το δυνατόν περισσότερο δυσδιάκριτο. Γενικά, ένα **rootkit** είναι μια συλλογή από εργαλεία που βοηθούν τους προγραμματιστές, ώστε ορισμένες ρουτίνες και διαδικασίες να μην ανιχνεύονται ή απενεργοποιούνται. Η ιδέα πίσω από ένα rootkit είναι να διασφαλιστεί η συνεχής παρουσία των δικών του διαδικασιών ή για τη διατήρηση της πρόσβασης σε ένα απομακρυσμένο σύστημα. Συνήθως έχουν ενεργοποιηθεί, ειδικά προνόμια ή ειδικές λειτουργίες στο σύστημα που βρίσκεται σε κίνδυνο. Λόγω της εισβολής τους στο σύστημα-στόχο, τα rootkit είναι συχνά δύσκολο να αφαιρεθούν.

Ιστορικά γεγονότα σχετικά με botnet

Ο όρος bot είναι σύντμηση της λέξης robot, και αναφέρεται στους “client” ενός botnet. Προέρχεται από τη Τσεχική λέξη "robota", που σημαίνει κυριολεκτικά την εργασία. Εναλλακτικές ονομασίες για τα bot είναι ζόμπι ή drones.

Ιστορικά, η έννοια του ρομπότ δεν περιλαμβάνει επιβλαβείς συμπεριφορές από προεπιλογή. Ο όρος χρησιμοποιήθηκε αρχικά για τις περιπτώσεις ελέγχου στα chat room του Internet Relay Chat (IRC), η οποία εμφανίστηκε από το 1989 και μετά. Ήταν σε θέση να ερμηνεύουν απλές εντολές, να παρέχουν διαχειριστική υποστήριξη ή να προσφέρουν υπηρεσίες όπως απλά παιχνίδια για να τους χρήστες του chat. Το πρώτο γνωστό IRC bot είναι το Eggdrop, δημοσιεύτηκε για πρώτη φορά το 1993 και από τότε αναπτύχθηκε περαιτέρω. Στη συνέχεια, μετά την απελευθέρωση του Eggdrop, εμφανίστηκαν κακόβουλα IRC bot, υιοθετώντας τη βασική ιδέα, αλλά πρωτίστως με σκοπό να επιτεθούν σε άλλους χρήστες του IRC ή ακόμα και ολόκληρων διακομιστών. Λίγο μετά, με αυτά τα bot,

υλοποιήθηκαν Denial of Service (DoS) και στη συνέχεια Distributed Denial of Service (DDoS).

Στα τέλη της δεκαετίας του 1990 που οι υπολογιστές έγινα περισσότερο διαθέσιμοι στο ευρύ κοινό, η κατάσταση Distributed Denial of Service έγινε ακόμη πιο δημοφιλής. Εργαλεία όπως τα Trin00, Stacheldraht, shaft, και Tribal Flood Network 2000 ήταν προγραμματισμένα και βελτιστοποιημένα σε επικεντρωμένες επιθέσεις από πολλαπλές πηγές.

Η έννοια των σκουληκιών, πηγαίνει πίσω στο 1971, όταν γράφτηκε το πρώτο δείγμα, που είναι γνωστό ως Creeper. Αυτό το πρόγραμμα αυτο-αντιγράφεται μεταξύ των μηχανών του δίκτυου ARPANET. Εμφάνισε ένα μήνυμα στην οθόνη, αλλά πάντα προσπαθούσε να αφαιρέσει την παρουσία του από τον υπολογιστή προέλευσης. Αργότερα τα σκουλήκια, στις αρχές του 1980, έχουν σχεδιαστεί με καλές προθέσεις, για παράδειγμα, με σκοπό τη γνωστοποίηση των άλλων χρηστών στο δίκτυο (Town Crier Worm) ή την ικανότητα διαχείρισης υπολογιστικού φόρτου τη νύχτα, όταν κανείς δεν χρησιμοποιούσε τα μηχανήματα (Vampire Worm). Το 1988, το σκουλήκι Morris εμφανίστηκε στο Cornell University και είχε ένα τεράστιο αντίκτυπο, μολύνοντας πιθανών το ένα δέκατο όλων των υπολογιστών στο διαδίκτυο εκείνη τη στιγμή (περίπου 6.000 μηχανές). Κακόβουλες εφαρμογές με τη συμπεριφορά των worm εντοπίστηκαν αμέσως μετά, μερικά από τα πρώτα είναι, για παράδειγμα, το Father Christmas Worm ή Worms Against Nuclear Killers. Τα σκουλήκια ήταν ένα από τα κύρια μέσα διάδοση των πρώιμων botnet.

Με τον ερχομό των εργαλείων απομακρυσμένης πρόσβασης, όπως Back orifice 2k ή SubSeven στα τέλη του 1990, δημιουργήθηκε ένα πρότυπο για την έννοια botnet με τον έλεγχο μόνο μίας μηχανής. Τα εργαλεία αυτά περιείχαν ήδη λειτουργείες, όπως η καταγραφή πληκτρολογήσης και της προώθηση των συνδέσεων.

Ο συνδυασμός των παραπάνω λειτουργιών τελικά είχε ως αποτέλεσμα την έννοια των botnet, με τους πρώτους εκπροσώπους όπως το Pretty Park, GTbot, Sdbot, Agobot, Spybot, Rbot και πολλά περισσότερα.

Σήμερα, η επεξεργαστική ισχύς των κινητών τηλεφώνων αυξάνεται διαρκώς και περάσαμε χωρίς να το καταλάβουμε, από τα απλά κινητά, στα smartphone που είναι μικροί φορητοί υπολογιστές με διαρκή σύνδεση στο internet ή άλλα ασύρματα δίκτυα.

Εξάλλου υπήρξε διείσδυση αυτής της νέας τεχνολογίας σε ένα χώρο που μέχρι τώρα επικρατούσε ψηφιακός αναλφαβητισμός. Αυτά, μαζί με όλα τα παραπάνω, άλλα και την περιορισμένη χρήση προγραμμάτων προστασίας, ανέδειξε την δυνατότητα και την ευκολία εξάπλωσης ενός botnet σε αυτό το νέο χώρο.

1.1.2 Περιγραφή των BotNet

Ο σύγχρονος ορισμός του “bot” περιέχει την έννοια του προηγμένου κακόβουλου λογισμικού που ενσωματώνει συνήθως μία ή περισσότερες από τις προαναφερθήσες τεχνικές, των ιών, worm, δούρειων ίππων και rootkit, με στόχο αφού πολλαπλασιαστούν και ενσωματωθούν σε ένα ξένο σύστημα (πχ. κινητό τηλεφωνο), να θέσουν στη διάθεσή του εισβολέα, τη λειτουργικότητα του συστήματος.

Ένα καθοριστικό χαρακτηριστικό των bot είναι ότι, μετά την επιτυχή προσβολή του συστήματος υποδοχής, το συνδέουν σε έναν κεντρικό server ή σε άλλα μολυσμένα μηχανήματα σχηματίζοντας έτσι ένα δίκτυο. Το δίκτυο αυτό είναι το λεγόμενο botnet. Τα bot αντίστοιχα παρέχουν μια σειρά από δυνατότητες σε μία οντότητα που ασκεί τον έλεγχο. Αυτή η οντότητα είναι συνήθως ένας C&C server, υπό τον έλεγχο ενός ή

περισσοτέρων προσώπων, που ονομάζεται botmaster ή botherder, που μεταδίδουν εντολές μέσα από αυτό το server. Ανάλογα με την υποδομή του δικτύου, τα bot μπορούν να συνδεθούν μεταξύ τους για την ενεργοποίηση της δομής ελέγχου που είναι επιθυμητή. Εναλλακτικά, μπορούν να υπάρχουν και τελείως ανεξάρτητα, χωρίς να γνωρίζουν την ύπαρξη των άλλων bot. Μια τυπική λειτουργία που παρέχουν τα bot στους κυρίους τους περιλαμβάνει την αυτοματοποιημένη εξαγωγή των διαπιστευτηρίων του θύματος, την οργανωμένη διανομή spam, τη δυνατότητα να συμμετάσχουν σε επιθέσεις άρνησης εξυπηρέτησης (DoS), ή την επέκταση των botnet με την πρόσληψη νέων bot. Το κίνητρο για αυτές τις δραστηριότητες είναι κυρίως τα οικονομικά συμφέροντα του botmaster. Αυτό έχει οδηγήσει σε ένα είδος, επικεντρωμένης στο botnet, οικονομίας με διακριτό μοντέλο ρόλων και συμμετεχόντων.

1.1.3 Η υποδομή ενός botnet

Το πιο σημαντικό μέρος ενός botnet είναι η λεγόμενη υποδομή διοίκησης και ελέγχου (C&C). Η υποδομή αυτή αποτελείται από τα bot και μια οντότητα ελέγχου που μπορεί να είναι είτε κεντρική είτε κατανεμημένη. Ένα ή περισσότερα πρωτόκολλα επικοινωνίας χρησιμοποιούνται από τον botmaster για να δείνονται εντολές στα μηχανήματα των θυμάτων για να συντονιστούν οι δράσεις τους. Το σύνολο εντολών και λειτουργικότητας των botnet ποικίλλουν ευρέως, ανάλογα με το κίνητρο της χρήσης τους.

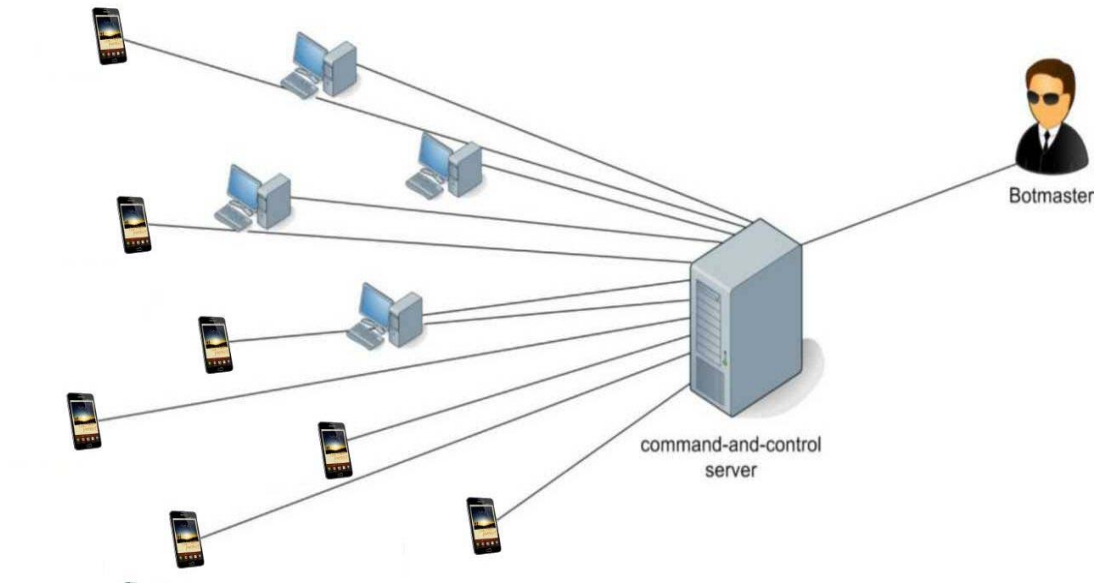
Η υποδομή C&C χρησιμεύει συνήθως ως ο μόνος τρόπος για τον έλεγχο των bot στο πλαίσιο του botnet. Τα bot είναι απαραίτητο να διατηρούν μια σταθερή σύνδεση σε αυτή την υποδομή ώστε να λειτουργούν αποτελεσματικά. Ως εκ τούτου, η αρχιτεκτονική του C&C υποδομής καθορίζει την ευρωστία, τη σταθερότητα και το χρόνο αντίδρασης. Σε γενικές γραμμές, μπορούμε να διακρίνουμε δύο προσεγγίσεις αρχιτεκτονικής, την συγκεντρωτική και την αποκεντρωμένη. Η συγκεντρωτική προσέγγιση μπορεί να συγκριθεί με το κλασικό μοντέλο δίκτυου client-server. Σε αυτά τα botnet, τα bot δρουν ως πελάτες και συνδέονται σε έναν ή περισσότερους κεντρικούς διακομιστές, από τους οποίους λαμβάνουν τις εντολές τους. Τα μοντέλα αποκεντρωμένης προσέγγισης C&C συχνά απαιτούν τα bot να ενεργήσουν, τουλάχιστον εν μέρει αυτόνομα. Τα bot διατηρούν την ικανότητα σύνδεσης με άλλα bot και ζητούν νέες εντολές για να το botnet. Επειδή δεν υπάρχει ένας μοναδικός C&C server που να μπορεί να έχει αποτυχία, και ο botmaster μπορεί να κρυφτεί στο εσωτερικό του δικτύου των bot, όταν δίνει εντολές, η προσέγγιση αυτή είναι πιο δύσκολο να περιοριστεί.

Τα σύγχρονα botnet απαιτούν μεγάλη ευελιξία και ευρωστία για να είναι σε θέση να χειριστούν μεγάλο αριθμό από bot και να μεγιστοποιηθεί το κέρδος που θα παραχθεί. Τα πρότυπα που χρησιμοποιούνταν από τα πρώτα botnet, ήταν κυρίως γνωστά πρωτόκολλα, σχεδόν χωρίς τροποποίηση. Η σημερινή τεχνολογία C&C έχει αναπτυχθεί ραγδαία, με την εισαγωγή πλήρως προσαρμοσμένων σετ οδηγιών και τη χρήση της κρυπτογραφίας. Η εφαρμογή των προσεγγίσεων μείωσης οδηγεί σε μια συνεχή εξέλιξη των πρωτοκόλλων διοίκησης και ελέγχου.

1.1.4 Αρχιτεκτονική Κεντρικής Διοίκησης και Ελέγχου (C&C)

Σε μια κεντρική C&C υποδομής, όλα τα bot δημιουργούν διαύλους επικοινωνίας με μία, ή περισσότερες απλές συνδέσεις όπως φαίνεται στο σχήμα 1. Αυτοί είναι συνήθως C&C διακομιστές, υπό τον έλεγχο του botmaster. Επειδή όλα τα bot συνδέονται με αυτούς τους διακομιστές, ο botmaster είναι σε θέση να επικοινωνεί με τα bot ταυτόχρονα και μπορεί να δώσει εντολές προς όλα τα bot που είναι σε απευθείας σύνδεση και συνδέονται με το

botnet. Αυτό προσφέρει χαμηλό χρόνο αντίδρασης και καλό συντονισμό. Η άμεση ανατροφοδότηση επιτρέπει την εύκολη παρακολούθηση της κατάσταση botnet για τον botmaster και δίνει πληροφορίες σχετικά με τα θεμελιώδη μεγέθη, όπως ο αριθμός των ενεργών bot ή την συνολική διανομή τους.



Σχήμα 1: Κεντρικοποιημένο botnet

Η ιδέα των botnet προήλθε από Internet Relay Chat (IRC), ένα σύστημα συνομιλίας που βασίζεται σε κείμενο και οργανώνει την επικοινωνία σε κανάλια. Το IRC πρωτόκολλο χρησιμεύει ακόμα ως μια σημαντική τεχνολογία για τον έλεγχο του botnet και σε ένα κεντρικοποιημένο μοντέλο επικοινωνίας. Σύμφωνα με την έκθεση Symantec Internet Security Threat 2010, το 31% των κεντρικών C&C server που παρατηρήθηκαν, χρησιμοποιούσαν IRC ως πρωτόκολλο επικοινωνίας το 2009. Μια σημαντική ιδιότητα του πρωτοκόλλου αυτού είναι ότι ο αριθμός των πιθανών συμμετεχόντων σε ένα κανάλι είναι τεχνικά απεριόριστος. Αυτό επιτρέπει τη συγκέντρωση πολλών bot σε ένα κανάλι και την δυνατότητα να εντέλλονται παράλληλα. Επιπλέον, είναι δυνατή ιδιωτική συνομιλία σε ένα προς ένα κόμβο. Αυτό δίνει τη δυνατότητα άμεσου χειρισμού ενός μεμονωμένου bot. Επειδή το πρωτόκολλο IRC βασίζεται σε κείμενο, είναι εύκολο να προσαρμοστεί. Αυτές οι ιδιότητες προσφέρουν μια ισχυρή, καλά οργανωμένη και εύκολη στην εφαρμογή της προσέγγιση, για διοίκηση ενός botnet. Τα κανάλια IRC για τον έλεγχο του botnet είτε φιλοξενούνται σε δημόσιους διακομιστές IRC ή σε διακομιστές που ανήκουν στον botmaster. Τα bot συνήθως χρησιμοποιούν μόνο ένα υποσύνολο από τις εντολές IRC. Αυτό είναι αρκετό για να επιτρέψει στον χειριστή να ελέγξει τα bot και να μειώσει τη λειτουργικότητα στο ελάχιστο απαιτούμενο. Εάν χρησιμοποιούν δικούς τους διακομιστές, μπορούν να γίνουν αυθαίρετες τροποποιήσεις του πρωτοκόλλου ώστε να χρησιμοποιούνται δικά τους set οδηγιών και κρυπτογράφηση. Το γεγονός αυτό ενισχύει το botnet έναντι των αντιμέτρων.

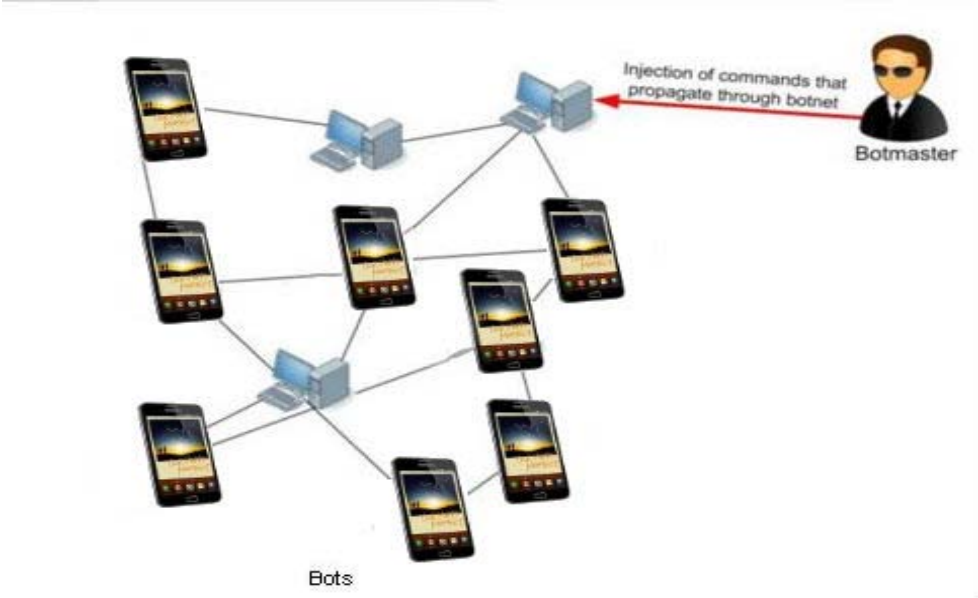
Ένα πολύ γνωστό πρότυπο που χρησιμοποιείται από όλες τις συσκευές που κάνουν χρήση του Διαδίκτυου (και στα smart phone) είναι το Hypertext Transfer Protocol (HTTP). Το http είναι το πρωτόκολλο που χρησιμοποιείται πιο συχνά για την παράδοση των δεδομένων μέσω του Διαδικτύου. Αυτό περιλαμβάνει αναγνώσιμο από τον άνθρωπο περιεχόμενο, όπως ιστοσελίδες και φωτογραφίες, καθώς επίσης και δυαδικά δεδομένα που μεταφέρονται κατά τις αποστολές και λήψεις. Λόγω αυτών των σημαντικών

χαρακτηριστικών, το HTTP είναι διαθέσιμο σχεδόν σε κάθε δίκτυο συνδεδεμένο στο Internet και σπάνια είναι φιλτραρισμένο. Αυτό είναι ιδιαίτερα ενδιαφέρον για τους διαχειριστές botnet, διότι το καθιστά σαν πρωτόκολλο διοίκησης και ελέγχου. Τα HTTP bot πρέπει να εκδίδουν περιοδικά αιτήματα προς το C&C εξυπηρετητή. Τα αιτήματα αυτά συνήθως αποτελούν μια αναφορά κατάστασης, με βάση την οποία ο διακομιστής αποφασίζει ποιες εντολές μεταφέρονται σε αυτό το συγκεκριμένο bot. Οι κεντρικοποιημένοι διακομιστές C&C που βασίζονται στο HTTP αποτελούν το 69% του συνόλου των server C&C και είναι ως εκ τούτου ο πιο συνηθισμένος τρόπος για τον έλεγχο ενός botnet. Ένα τυπικό παράδειγμα botnet που χρησιμοποιούν HTTP για την επικοινωνία είναι εκείνα που δημιουργούνται με το κακόβουλο εμπορικό toolkit ZeuS, το οποίο διαθέτει ένα γραφικό περιβάλλον για το χρήστη του διακομιστή C&C. Αυτό επιτρέπει να χειριστεί το botnet, κάποιος με ελάχιστες τεχνικές δεξιότητες.

Σε ορισμένες περιπτώσεις, ένα botnet οργανώνεται σε πολλαπλές βαθμίδες. Για παράδειγμα, αντί ενός μεμονωμένου κεντρικού διακομιστή C&C, μπορεί να υπάρξει μια υποδομή από server. Η υποδομή αυτή έχει συνήθως έναν ιεραρχικό σχεδιασμό και μπορεί να περιλαμβάνει, για παράδειγμα, εξειδικευμένους server για την ενορχήστρωση των bot σε υποομάδες, παρόμοια με ένα εξισορροπητή φορτίου, και περισσότερους server για την παράδοση του περιεχομένου στα bot, όπως τα spam template. Αυτή η δομή μπορεί επίσης να περιλαμβάνει διαφοροποίηση των bot, π.χ. τα άμεσα προσβάσιμα από το Internet, που ενεργούν ως πληρεξούσιοι κόμβοι (proxy) για το botnet, και εκείνα που κρύβονται σε εσωτερικά δίκτυα, σαν εργαζόμενοι.

1.1.5 Αρχιτεκτονική Αποκεντρωμένης Διοίκησης και Ελέγχου (Decentralized C&C Architecture)

Στην αποκεντρωμένη C&C αρχιτεκτονική, χαλαρά συνδεδεμένοι δεσμοί μεταξύ των bot εξασφαλίζουν την επικοινωνία στο εσωτερικό του botnet και παρέχουν τη βάση για την οργάνωσή της. Ένας κοινός όρος για αυτή την κατηγορία των botnet είναι το peer-to-peer (P2P) botnet, καθώς αυτό είναι το όνομα του αντίστοιχου μοντέλου του δικτύου. Η γνώση για τη συμμετοχή των ομότιμων κόμβων είναι κατανεμημένη σε όλο το botnet.



Σχήμα 2: Peer to Peer botnet

Ως εκ τούτου, πληροφορίες για όλο το botnet δεν μπορούν να ληφθούν άμεσα, και οι εντολές εισάγονται σε ένα από τους ομότιμους κόμβους του botnet. Συνήθως, αυτό είτε πραγματοποιείται μέσω του πρωτοκόλλου επικοινωνίας απευθείας ή μέσω της λειτουργίας ενημέρωσης. Στην τελευταία περίπτωση, τα bot, θα ανταλλάσσουν έναν αριθμό αναθεώρησης τους κατά την επικοινωνία και, αν αυτοί διαφέρουν, το παλαιότερο bot είναι ενημερωμένο για την έκδοση του νέου bot. Με τον τρόπο αυτό, η αναθεώρηση διαδίδεται μέσω του botnet με την πάροδο του χρόνου.

Η εισαγωγή των εν λόγω ενημερώσεων και εντολών μέσα στο botnet συνήθως συμβαίνει από ένα αυθαίρετο σημείο, καθιστώντας τον εντοπισμό του botmaster σχεδόν αδύνατο. Αυτό παρέχει υψηλό βαθμό ανωνυμίας. Η παρακολούθηση των δραστηριοτήτων του ή μετά από μια τέτοια νέα εντολή μέσω του δικτύου είναι πολύ δύσκολη. Στο σχήμα 2, εμφανίζεται ένα απλοποιημένο σχέδιο ενός botnet peer-to-peer, ως παράδειγμα προσέγγισης αποκεντρωμένου C&C botnet. Όσον αφορά την ευρωστία, τα peer-to-peer botnet έχουν το μεγάλο πλεονέκτημα ότι δεν έχουν ένα κεντρικό server που μπορεί να δεχθεί άμεση επίθεση. Από την άλλη πλευρά, η αυτο-διάδοση των εντολών μέσω του botnet σημαίνει χαμηλό χρόνο αντίδρασης. Υπάρχει τουλάχιστον μια γνωστή υπόθεση, η SpamThru botnet, όπου η peer-to-peer λειτουργία χρησιμοποιήθηκε ως εφεδρικό κανάλι. Στην περίπτωση αυτή, προαιρετικοί κεντρικοί εξυπηρετητές χρησιμοποιούνται επιπροσθέτως για επίβλεψη, φτιάχνοντας έτσι ένα υβριδικό botnet.

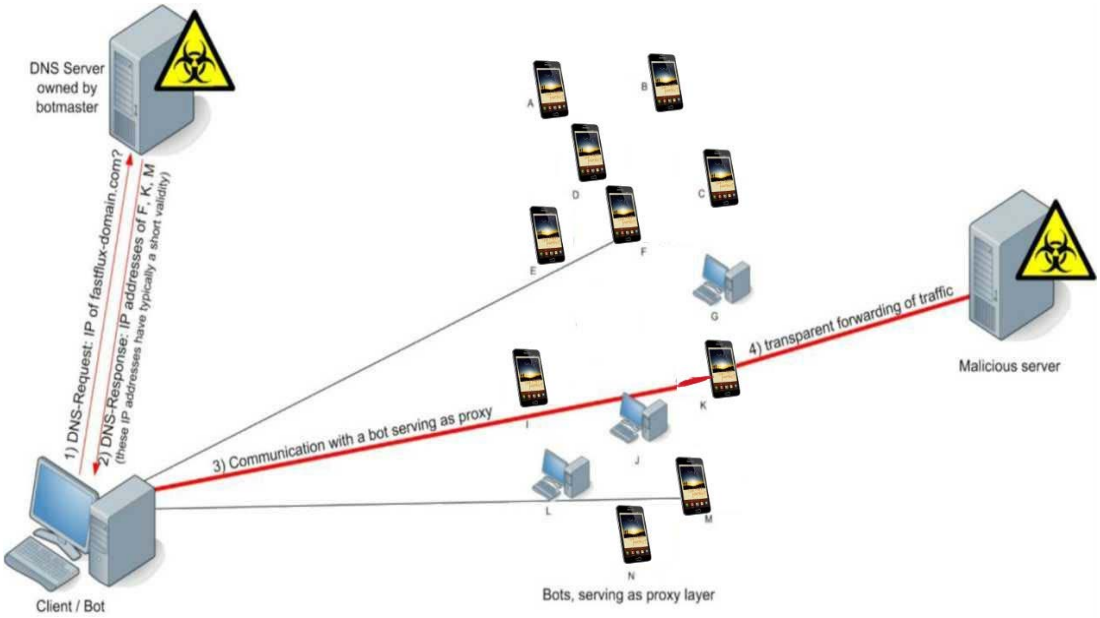
Ο ρόλος του Συστήματος Ονομάτων Τομέα (DNS) στα botnet

Για την κεντρικοποιημένη προσέγγιση, το Domain Name System (DNS) έχει σημαντικό ρόλο, καθώς επιτρέπει στην C&C υποδομή, αλλαγές που μπορούν να εκτελεστούν δυναμικά. Όταν χρησιμοποιείται DNS, ο C&C διακομιστής αναγνωρίζεται από ένα (C&C) όνομα τομέα που επιλύεται με DNS σε μια διεύθυνση IP. Πολλές, επιτυχημένες τεχνικές με στόχο το DNS, έχουν εφαρμοστεί στην πράξη για τον περιορισμό ενός botnet. Ένα παράδειγμα τέτοιο, είναι η διαγραφή από τα μητρώα DNS, των κακόβουλων ονομάτων τομέα. Ωστόσο, η παγκόσμια κατανεμημένη δομή του DNS περιπλέκει τη διαδικασία περιορισμού.

Η τεχνική που περιγράφεται παρακάτω δείχνει πώς η δημιουργία και διαχείριση botnet κάνει χρήση προσεγγίσεων, υψηλής τεχνικά πολυπλοκότητας. Η αρχή των λεγόμενων Fast-Flux δίκτυων εξυπηρέτησης (FFSN) είναι μια εφεύρεση των δημιουργών botnet, με σκοπό την αύξηση της ανθεκτικότητας και της ανωνυμίας, και έχει επιτύχει πολλά για αρκετά botnet. Η ιδέα της γρήγορης ροής (Fast-Flux) μπορεί να συγκριθεί με Δίκτυα Παράδοσης Περιεχομένου (CDN), όπως απεικονίζεται στο σχήμα 3**.** Όταν ένα κακόβουλο όνομα τομέα πρέπει να επιλυθεί, ένα ερώτημα συνήθως αποστέλλεται πρώτα στο πλησιέστερο διακομιστή DNS και στη συνέχεια παραδίδεται μέσω του συστήματος DNS σε ένα διακομιστή DNS που ελέγχεται από τον botmaster. Η Fast-Flux δικτύωση εκμεταλλεύεται τις ιδιότητες του DNS ως εξής: Η απάντηση στο ερώτημα θα περιλαμβάνει συνήθως ένα μεγάλο αριθμό διευθύνσεων IP που σχετίζονται με τα bot. Αυτά λειτουργούν ως proxy server, και διαβιβάζουν την επικοινωνία όλων των χρηστών σε ένα διακομιστή, που κρύβεται πίσω από το επίπεδο του proxy. Πίσω από αυτό, το επίπεδο του proxy μπορεί να κρυφτούν, κακόβουλες υπηρεσίες όπως το phishing ιστοσελίδων, ύποπτες διαφημίσεις, ή κακόβουλα αρχεία για λήψη.

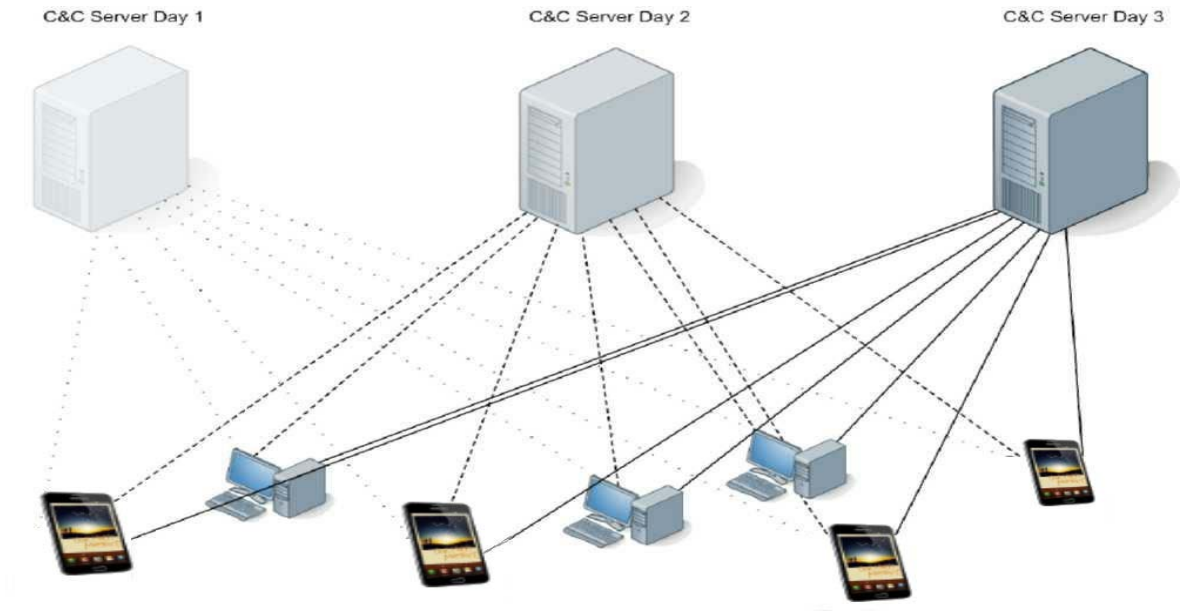
Όπως αναφέρθηκε προηγουμένως, μια κοινή προσέγγιση για τον περιορισμό των botnet είναι να μπλοκαριστούν τα κακόβουλα ονόματα τομέα. Ανάλογα με τον πάροχο υπηρεσιών DNS στο τέλος, η διαδικασία αυτή μπορεί να απαιτήσει σημαντικές προσπάθειες. Σε κάθε περίπτωση, μεμονωμένοι τομείς μπορούν να μπλοκαριστούν ή να τεθούν εκτός, σχετικά εύκολα. Αυτό έχει οδηγήσει σε μια άλλη έννοια που έχει εφευρεθεί για χρήση σε botnet,

τους αλγόριθμους δημιουργίας τομέων (DGA). Η ιδέα πίσω από τα DGA είναι να δημιουργήσει C&C domain name (ονόματα τομέων που συνδέονται με τις εγγραφές DNS σε C&C server), ανάλογα με μία ή περισσότερες εξωτερικές πηγές πληροφόρησης που παρέχουν προβλέψιμες τιμές που ονομάζονται δείκτες και που μπορούν να προσεγγιστούν τόσο από bot όσο και από botmaster.



Σχήμα 3: Fast-flux δικτύωση

Οι δείκτες που έχουν χρησιμοποιηθεί με αυτή την έννοια μπορεί να είναι χρονοσφραγίδες καθώς και στοιχεία από δημοφιλείς ιστοσελίδες όπως το Twitter Trends. Ενώ οι χρονοσφραγίδες παρέχουν τη δυνατότητα να παράγουν τα ονόματα τομέα εκ των προτέρων, η χρήση του δυναμικού web περιεχομένου, εξαλείφει αυτό το στοιχείο της προβλεψιμότητας. Εκατοντάδες, ή ακόμα και χιλιάδες, ονομάτων τομέα μπορεί να παραχθούν σε σύντομα χρονικά διαστήματα. Μια τυπική χρονική περίοδος για την ισχύ των εν λόγω τομέων είναι μία ημέρα. Οποιαδήποτε προσπάθεια να μετριαστεί αυτό το είδος της επίθεσης botnet αντιμετωπίζει σήμερα πολλούς ύποπτους τομείς. Η προσπάθεια που απαιτείται για την άμυνα έναντι αυτού του είδους της επίθεσης, αυξάνει μαζικά, καθώς ο botmaster μπορεί να επιλέξει να πάρει απλά έναν από τους πιθανούς τομείς, να τον δηλώσει και να του παρέχει νέες οδηγίες, ή μια ενημέρωση, καθ' όσο διαρκεί η ισχύς του εν λόγω τομέα.



Σχήμα 4: Botnet Locomotive.

Μια ειδική περίπτωση του κεντρικοποιημένου botnet είναι το λεγόμενο botnet locomotive. Η βασική ιδέα είναι ένα συγκεντρωτικό μοντέλο C&C όπου,ο κόμβος που ασκεί τον κεντρικό έλεγχο, μεταβαίνει τακτικά σε άλλη θέση.

Έμμεση διοίκηση και ελέγχος (indirection C&C)

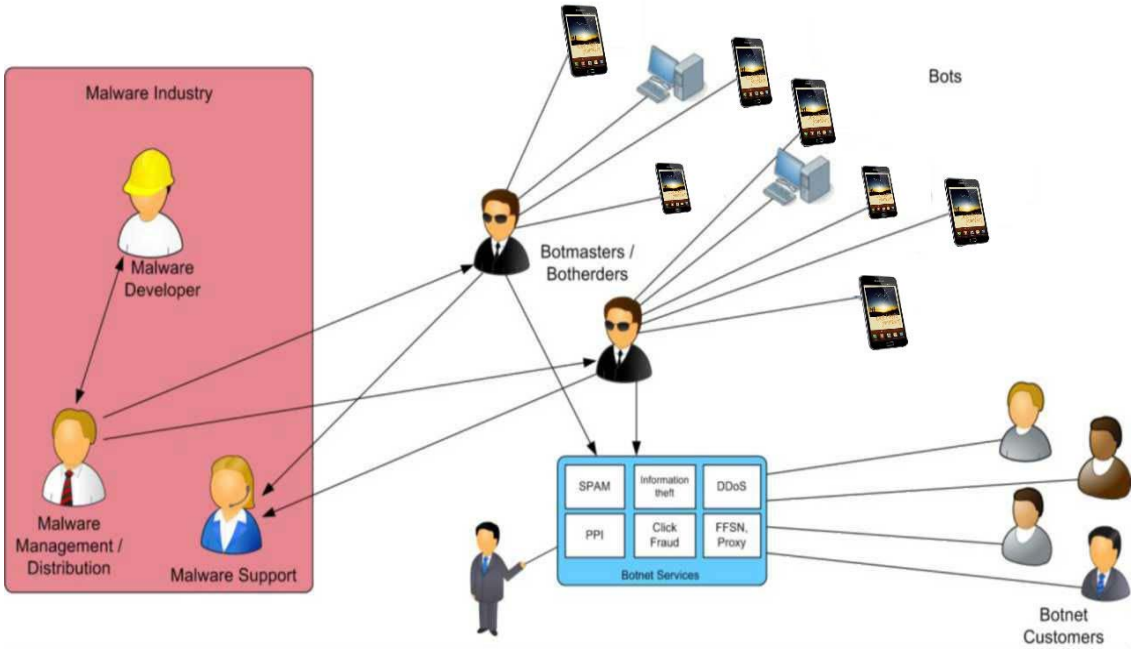
Εκτός από τις προσεγγίσεις που αναφέρονται, και άλλες τεχνολογίες έχουν αξιοποιηθεί για αρχιτεκτονικές botnet C&C, προκειμένου να επιτευχθεί ένα ορισμένο επίπεδο έμμεσης διοίκησης και ελέγχου. Η βασική ιδέα είναι να καθιερωθεί ένα συγκαλυμμένο κανάλι σε άλλες κοινές διαθέσιμες τεχνολογίες και υπηρεσίες του Διαδικτύου, όπως το Instant Messaging (IM), Really Simple Syndication (RSS) ή τα κοινωνικά δίκτυα. Το κίνητρο πίσω από τη χρήση αυτών των υφιστάμενων υποδομών είναι η εγγύηση για τη σταθερότητα του δικτύου, επειδή οι φορείς συντηρούν τις υπηρεσίες τους. Επιπλέον, αυτές οι υπηρεσίες απαιτούν χαμηλό επίπεδο εξακρίβωσης ταυτότητας κατά την αρχική εγγραφή κάτι που μπορεί να εκμεταλλευτεί κάποιος για έμμεσο ελέγχο της ροής. Θεωρείται πως, σχεδόν κάθε τεχνολογία που σχετίζεται με το **Internet**, ερευνάται από εγκληματίες που αναζητούν εργαλεία για εργασίες botnet.

1.1.6 Κίνητρα χρήσης των botnet

Η γρήγορη εξέλιξη του κακόβουλου λογισμικού και των botnet από τεχνική άποψη, παρουσιάζεται στις προηγούμενες σελίδες. Μαζί με την τεχνολογία, μια υπόγεια οικονομία του εγκλήματος στον κυβερνοχώρο έχει αναπτυχθεί γύρω από τον τομέα των botnet (Σχήμα 5). Αυτή η ενότητα επικεντρώνεται στο κίνητρο πίσω από τη λειτουργία των botnet. Αυτό περιλαμβάνει τις υπηρεσίες που προσφέρονται από botnet που μπορούν να χρησιμοποιηθούν για να αποφέρουν οφέλη, και πρότυπα προς μίμηση στον κλάδο του malware.

Κατ 'αρχάς, το κακόβουλο λογισμικό και το botnet λογισμικό πρέπει να δημιουργηθεί. Αυτό γίνεται συνήθως από την βιομηχανία του malware, από κακόβουλους προγραμματιστές

και δημιουργούς ιών. Οι προγραμματιστές δεν είναι απαραιτήτως οι ίδιοι άνθρωποι που χρησιμοποιούν τις δημιουργίες τους. Συχνά, προ-μεταγλωττισμένα malware, πακέτα λογισμικού για προσαρμοσμένη δημιουργία εκτελέσιμων αρχείων ή επέκταση μονάδων πωλούνται στους botmaster. Άλλα "προϊόντα" που ενδείκνυνται για τη διάδοση malware εκμεταλλεύονται ή ενσωματώνονται σε κακόβουλο λογισμικό για τη στήριξη της διαδικασίας μετάδοσης. Η πώληση κακόβουλου λογισμικού μπορεί επίσης να διαιρεθεί σε πολλαπλά στάδια στην αλυσίδα εφοδιασμού, συμπεριλαμβανομένων των υπηρεσιών διανομής malware ή botnet ή κιτ κατασκευής crimeware. Στην περίπτωση αυτή, ένα άλλο επίπεδο εισάγεται στην επιχείρησή τους, παρέχοντας επιπλέον ανωνυμία για τους προγραμματιστές. Για μερικά κιτ δημιουργίας botnet, υπάρχει ένα είδος "service level agreements", κυρίως με στόχο τις ενημερώσεις και αναβαθμίσεις. Ακόμα και υπηρεσίες τηλεφωνικής υποστήριξης έχουν εντοπιστεί.



Σχήμα 5: Απλοποιημένο μοντέλο της malware οικονομίας

1.1.7 Θέματα απειλών από ένα botnet

Οι δικτυακές επιθέσεις μπορούν να κατηγοριοποιηθούν, ανάλογα με την ζημιά που προκαλούν, στους παρακάτω τύπους:

- **Άρνηση Υπηρεσίας:** Οι επιθέσεις άρνησης υπηρεσίας ή DoS (Denial of Service) όπως είναι ευρέως γνωστές, έχουν στόχο τους όπως φανερώνει και το όνομα τους, την διακοπή παροχής υπηρεσιών από την πλευρά των συστημάτων που δέχονται την επίθεση. Αυτό επιτυγχάνεται συνήθως όταν ο επιτιθέμενος αποστέλλει μεγάλο αριθμό αιτήσεων εξυπηρέτησης στον διακομιστή-στόχο που αυτός αδυνατεί να τις διεκπεραιώσει στον προκαθορισμένο χρόνο. Το αποτέλεσμα είναι να γεμίζει η ουρά και να μην εξυπηρετούνται οι νόμιμες αιτήσεις. Τέτοιου τύπου επιθέσεις σε περίπτωση επιτυχής περάτωσης τους, αποφέρουν σημαντικά πλήγματα αξιοπιστίας αλλά και μείωση κερδοφορίας κυρίως σε επιχειρήσεις παροχής υπηρεσιών και πώλησης αγαθών (π.χ. αεροπορικές εταιρίες, ηλεκτρονικά καταστήματα, μηχανές αναζήτησης) οι οποίες και χρειάζεται να παρέχουν συνεχή και αδιάκοπη λειτουργία.

- **Επιθέσεις Πλαστοπροσωπίας (Spoofing):** Σε αυτές τις ηλεκτρονικές επιθέσεις ο επιτιθέμενος τροποποιεί κατάλληλα τις αιτήσεις έτσι ώστε να φαίνεται ότι προέρχονται από άλλη πηγή. Κατά αυτό τον τρόπο μπορεί να ξεγελάσει τα συστήματα-στόχους προσποιούμενος κάποιο έμπιστο μηχάνημα. Γνωστές επιθέσεις αυτού του είδους είναι συνήθως οι IP spoofing όπου κάποιος χρήστης τροποποιεί την διεύθυνση IP στα πακέτα που αποστέλλει.
- **Επιθέσεις Λαθρακρόασης (Eavesdropping):** Είναι μια παθητική επίθεση που πραγματοποιούνται από άτομα τα οποία παρεμβάλλονται στην επικοινωνία δύο υπολογιστών, αποκαλύπτουν το περιεχόμενο της και παραβιάζουν το απόρρητο της επικοινωνίας. Αυτό μπορεί να επιτευχθεί με διάφορους τρόπους. Ο πιο κοινός είναι με τη χρήση προγραμμάτων καταγραφής δικτυακής κίνησης (sniffers).
- **Επιθέσεις Επιπέδου Εφαρμογής:** Οι επιθέσεις αυτού του τύπου εκμεταλλεύονται αδυναμίες και κενά ασφαλείας που υπάρχουν σε εφαρμογές και προγράμματα τα οποία χρησιμοποιεί ο χρήστης ή οι υπηρεσίες που προσφέρει ένας διακομιστής. Παραδείγματα τέτοιου τύπου επιθέσεων αποτελούν τα trojans, οι ιοί, επιθέσεις στον διακομιστή διαδικτύου (Web server), SQL Injection, Buffer overflow. Ανάλογα με τον τύπο της αδυναμίας ο επιτιθέμενος μπορεί από το να τροποποιήσει η να υποκλέψει δεδομένα μέχρι και να αποκτήσει πρόσβαση στη μηχανή.
- **Επιθέσεις Παράνομης Παραβίασης:** Οι επιθέσεις αυτές στοχεύουν στην παράνομη, εκ μέρους κακόβουλων χρηστών, είσοδο σε κάποιο μηχάνημα δια μέσω του δικτύου. Σε αυτές περιλαμβάνονται επιθέσεις εναντίων των συστημάτων αυθεντικοποίησης, επιθέσεις κοινωνικής μηχανικής και βέβαια επιθέσεις εναντίον εφαρμογών.

Επιπλέον, σύμφωνα με μελέτη της Trendo Micro (2006) επιχειρείται η ταξινόμηση των botnet αναλόγως των απειλών που επιφέρουν. Η ταξινόμηση αυτή παρουσιάζεται συνοπτικά στον πίνακα 1. Σημειώνεται ότι η ταξινόμηση των δικτύων Botnet μπορεί να γίνει με βάση πολλά από τα χαρακτηριστικά τους όπως η αρχιτεκτονική του C&C καναλιού, το πρωτόκολλο επικοινωνίας, τον τύπο των επιθέσεων, τον τρόπο εντοπισμού του C&C server, τις ενέργειες που παρατηρούνται και τις τεχνικές απόκρυψης που χρησιμοποιούν.

Πίνακας 1: Ταξινόμηση απειλών Botnet

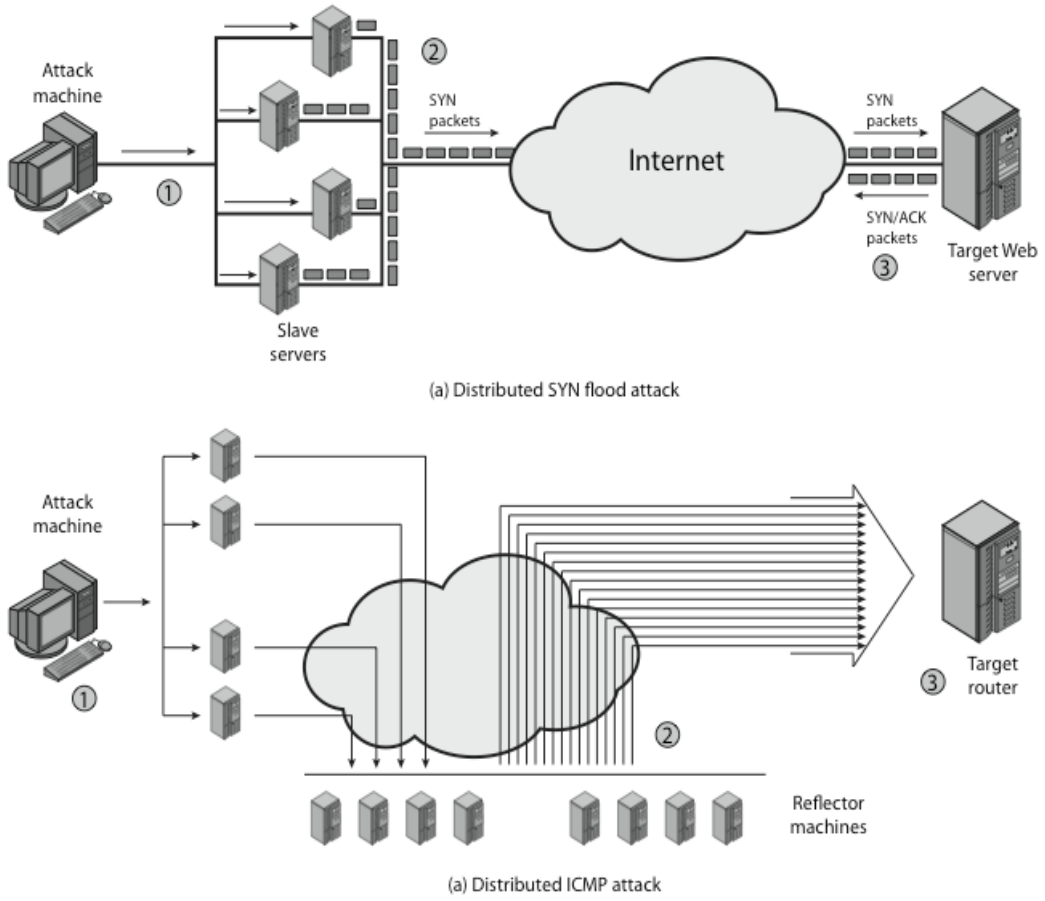
Category	Examples
Attacking behavior	DDoS; scan; remote exploits; junk emails (phishing and virus attachments); phishing websites; spyware; identity theft; etc
C&C models	centralized; distributed; P2P; etc
Rally mechanisms	Hard-coded IP; Dynamic DNS; Distributed DNS; etc
Communication protocols	IRC; HTTP; IM; P2P; etc
Observable botnet activities	DNS queries; burst short packets; abnormal system calls; etc
Evasion Techniques	HTTP/VOIP tunneling; IPv6 tunneling; P2P encrypted traffic; etc

[Trend Micro, 2006-TAXONOMY OF BOTNET THREATS]

Κατανεμημένες Επιθέσεις Άρνησης Υπηρεσιών – DDoS Attacks

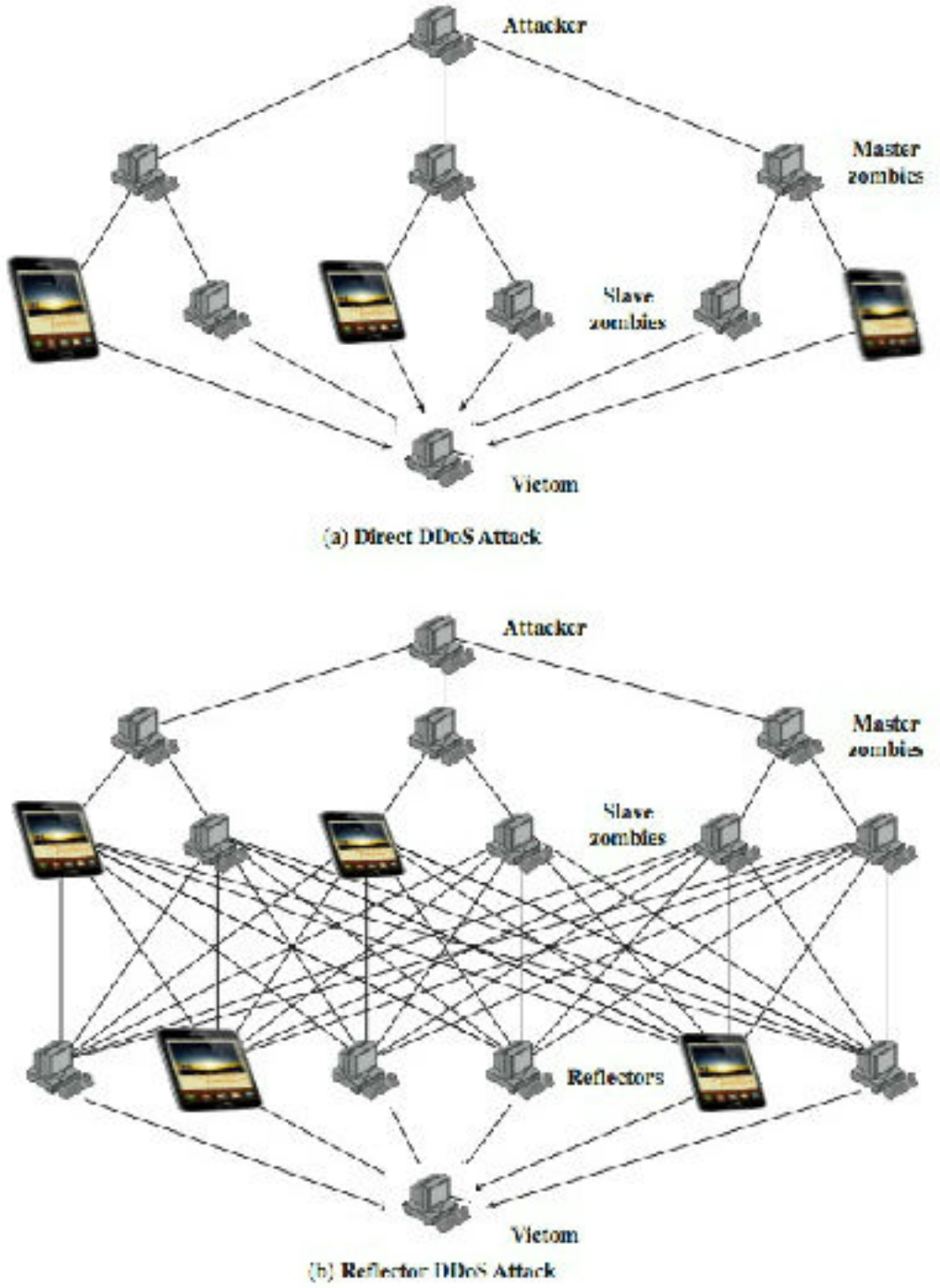
Η κατανεμημένη επίθεση άρνησης υπηρεσιών (Distributed Denial of Service Attack) αποτελεί ένα από τα κυριότερα είδη επιθέσεων που δύναται να πραγματοποιήσουν τα

δίκτυα botnet. Ουσιαστικά πρόκειται για ένα μεγάλο αριθμό συνδέσεων των κόμβων-bot (σχήμα 6) προς κάποιον εξυπηρετητή ή δίκτυο που προσφέρει υπηρεσίες μέσα από το διαδίκτυο. Αυτό έχει ως αποτέλεσμα την εξάντληση των πόρων του συστήματος και την αδυναμία εξυπηρέτησης αιτήσεων από νόμιμους χρήστες. Οι μέθοδοι πραγματοποίησης μίας τέτοιας επίθεσης είναι αρκετές, πιο συχνά εμφανιζόμενες όμως, στην υλοποίηση των bot, είναι οι TCP SYN flood και η UDP flood επιθέσεις, όπου πραγματοποιείται αποστολή ενός μεγάλου αριθμού TCP SYN και UDP πακέτων, αντίστοιχα.



Σχήμα 6: Σχηματική απόδοση ροής Κατανεμημένης Επίθεσης Άρνησης Υπηρεσιών (DDoS)

Στόχος τέτοιου είδους επιθέσεως (σχήμα 7) είναι κυρίως ιστοσελίδες με μεγάλη επισκεψιμότητα, επιφέροντας στις εταιρίες που τις φιλοξενούν απώλεια κερδών. Το γεγονός αυτό κάνει τα δίκτυα botnet ένα εργαλείο οικονομικής ωφέλειας, τοποθετώντας το στο παιχνίδι μεγάλων επιχειρηματικών δραστηριοτήτων. Εκτός βέβαια από επιθέσεις σε ιστοσελίδες, τα δίκτυα botnet είναι δυνατόν να πραγματοποιήσουν DDoS επιθέσεις σε οποιαδήποτε υπηρεσία διατίθεται μέσα από το διαδίκτυο. Σε αυτές συγκαταλέγονται μέχρι και κρατικές υπηρεσίες, δίνοντας ακόμα περισσότερη αξία στα δίκτυα botnet, προάγοντας τα σε εργαλείο διακρατικών μαχών.



Σχήμα 7: Σχηματική απόδοση επιθέσεων DDoS

[http://www.cs.ucy.ac.cy/courses/EPL674/lectures/Malicious-Software-ch21-GR.pdf]

Αποστολή Ανεπιθύμητης Ηλεκτρονικής Αλληλογραφίας – Spamming

Κάνοντας χρήση του πρωτοκόλλου SMTP τα bot εκτελούν εντολές μαζικής αποστολής ανεπιθύμητων ηλεκτρονικών μηνυμάτων, γνωστά και ως Spam. Έχοντας λίστες ηλεκτρονικών διευθύνσεων στη διάθεση τους, κάθε bot αποστέλλει ένα πλήθος από ηλεκτρονικά μηνύματα, τα οποία στο σύνολο τους αποτελούν ένα αρκετά μεγάλο όγκο

δεδομένων. Τα Spam περιλαμβάνουν διαφημιστικά μηνύματα από οποιονδήποτε θελήσει να εκμεταλλευτεί, έναντι πληρωμής, τη συγκεκριμένη λειτουργία-υπηρεσία των δικτύων botnet. Το γεγονός αυτό αποτελεί μία ακόμα αιτία που τα κάνει να αποτελούν σημείο ενδιαφέροντος στην οικονομία των επιχειρήσεων. Τα ανεπιθύμητα μηνύματα μπορεί επίσης να περιλαμβάνουν περιεχόμενο με τέτοιο τρόπο ώστε ο παραλήπτης να νομίζει ότι προέρχονται από κάποιο νόμιμο αποστολέα, ζητώντας του να επισκεφτεί κάποια ιστοσελίδα και να συμπληρώσει τα απαραίτητα στοιχεία. Η ιστοσελίδα αυτή είναι κατασκευασμένη με τέτοιο τρόπο, ώστε να φαίνεται αληθινή, πείθοντας τον επισκέπτη να συμπληρώσει τα στοιχεία που του ζητάει, στη συνέχεια όμως το μόνο που κάνει είναι να τα υποκλέπτει. Η επίθεση αυτή ονομάζεται ηλεκτρονικό ψάρεμα (phishing).

Κλοπή Ταυτότητας – Identity Theft

Με τις λειτουργίες καταγραφής των πληκτρολογήσεων (keylogging) και ανίχνευσης κίνησης πακέτων δικτύου (packet sniffing) υπάρχει δυνατότητα, σε κάθε bot, υποκλοπής προσωπικών ιδιωτικών δεδομένων. Τα δεδομένα αυτά περιλαμβάνουν συνθηματικά (passwords) λογαριασμών, όπως ηλεκτρονικού ταχυδρομείου, αποστολής άμεσων μηνυμάτων (ICQ,MSN,Yahoo,Skype), τραπέζης, αριθμούς πιστωτικών καρτών και, ανάλογα με το σύστημα που είναι εγκατεστημένο το bot, δεδομένα μεγάλης αξίας και εμπιστευτικότητας, όπως δεδομένα κρίσιμων υποδομών κρατών. Η δυνατότητα αυτή που έχουν τα δίκτυα botnet αποτελεί και τη μεγαλύτερη απειλή, αφού μεγάλοι οργανισμοί, επιχειρήσεις, ακόμα και κρατικοί φορείς απειλούνται με αποκάλυψη κρίσιμων ιδιωτικών δεδομένων.

Απάτη Κλικ – Click Fraud

Εκμεταλλευόμενα τον μεγάλο αριθμό υπολογιστών με διαφορετική IP διεύθυνση, τα δίκτυα botnet συμμετέχουν στην απάτη κλικ (click fraud), όπου επισκέπτονται ιστοσελίδες και κάνουν κλικ πάνω σε διαφημιστικές ετικέτες (banners), προς όφελος των διαφημιστών που τα φιλοξενούν και οι οποίοι πληρώνονται ανάλογα με τον αριθμό των επισκέψεων, που πραγματοποιούνται μέσα από το banner. Η κίνηση της επισκεψιμότητας παρουσιάζεται να είναι νόμιμη, αφού προέρχεται από υπολογιστές με IP διευθύνσεις παγκόσμιας εμβέλειας.

Καταγραφή πληκτρολογήσεων (Keystroke logging)

Η καταγραφή πληκτρολογήσεων των χρηστών, γνωστή και ως keystroke logging ή πιο σύντομα ως keylogging, είναι ίσως το πιο απειλητικό χαρακτηριστικό γνώρισμα ενός botnet για την ιδιωτικότητα ενός ατόμου. Πολλά bot “αφουγκράζονται” τη δραστηριότητα των πληκτρολογίων και αναφέρουν τις πληκτρολογήσεις στο bot-herder. Μερικά bot ενεργοποιούν την καταγραφή των πληκτρολογήσεων όταν οι χρήστες πραγματοποιούν επισκέψεις σε ιδιαίτερους ιστοχώρους οι οποίοι απαιτούν την πληκτρολόγηση προσωπικών κωδικών ή πληροφοριών τραπεζικών λογαριασμών. Αυτό δίνει στο herder τη δυνατότητα να αποκτήσει πρόσβαση σε ευαίσθητες προσωπικές πληροφορίες, να αποκτήσει στοιχεία των πιστωτικών καρτών που οι χρήστες κατέχουν κτλ.

Επίσης πολλά bot δίνουν στον επιτιθέμενο τη δυνατότητα πλήρους πρόσβασης στο σύστημα αρχείων. Οι πληροφορίες που αντλούνται μπορεί να είναι τόσο κρίσιμες ώστε να οδηγήσουν ακόμη και σε κλοπή ταυτότητας (identity theft) των ανυποψίαστων χρηστών.

Τέλος, οι λειτουργίες keylogging συχνά συνδυάζονται με την απόκτηση στιγμιοτύπων από τις οθόνες των θυμάτων (screenshots), την καταγραφή της δραστηριότητας του προγράμματος ιστο-περιήγησης και την καταγραφή της τοπικής δικτυακής κίνησης.

Παράνομο Λογισμικό – Warez

Τα δίκτυα bot μπορούν επίσης να χρησιμοποιηθούν για τη διακίνηση παράνομου λογισμικού, είτε υποκλέπτοντας το από τον εκάστοτε υπολογιστή όπου είναι εγκατεστημένο το bot, είτε αποθηκεύοντας το σε αυτόν και δίνοντας τη δυνατότητα, στη συνέχεια, σε άλλους να το κατεβάσουν. Το ίδιο μπορεί να συμβεί και για τη διακίνηση οποιουδήποτε παράνομου περιεχομένου, χωρίς να ενοχοποιείται ο κάτοχος του, αλλά ο χρήστης του μηχανήματος που έχει μολυνθεί.

Εξάπλωση κακόβουλου λογισμικού μέσω Exploit scanning/autorooting

Τα bot περιλαμβάνουν συνήθως βασικούς ανιχνευτές πορτών (port scanners) που προσπαθούν να εντοπίσουν ανοιχτές πόρτες των πρωτοκόλλων TCP ή UDP στα συστήματα. Καθώς το κακόβουλο λογισμικό που τα bot χρησιμοποιούν εξελίσσεται, αυτοί οι βασικοί ανιχνευτές ενισχύονται με προηγμένες δυνατότητες ανίχνευσης και αυτόματης εκμετάλλευσης ευπαθειών των συστημάτων, έτσι ώστε οι botmasters να αποκτούν πλήρη πρόσβαση στα απομακρυσμένα συστήματα (autorooting). Με αυτό τον τρόπο τα bot μολύνουν άλλους υπολογιστές και εξαπλώνονται ταχύτατα.

Σχεδόν όλα τα bot περιέχουν τη λειτουργία που επιτρέπει τη μεταφόρτωση (download) και εκτέλεση των κακόβουλων binaries με χρήση πρωτοκόλλων όπως το FTP, TFTP, ή HTTP. Αυτή είναι η βασική μέθοδος που χρησιμοποιείται για την ενημέρωση του κακόβουλου κώδικα στο botnet, αλλά δεν περιορίζεται μόνο στις ενημερώσεις. Μπορεί να χρησιμοποιηθεί για να μεταφορτώσει στα bot οποιοδήποτε αρχείο επιθυμεί ο επιτιθέμενος. Αυτά τα αρχεία μπορούν να εκτελεστούν αμέσως ή σε κάποιο μεταγενέστερο χρόνο. Αυτή η δυνατότητα να μεταφορτωθούν και να εκτελεστούν αυθαίρετα προγράμματα χρησιμοποιείται συχνά για να εγκατασταθεί πρόσθετο malware, όπως spyware, adware, ή άλλα εργαλεία που μπορούν να αυξήσουν τη δραστικότητα του επιτιθέμενου.

Φιλοξενία Παράνομων Ιστοσελίδων

Η φιλοξενία ιστοσελίδων από τα bot επιτρέπει την ευκολότερη διακίνηση αρχείων παράνομου περιεχομένου, όπως πειρατικό λογισμικό και παράνομο φωτογραφικό υλικό. Επίσης μπορεί να φιλοξενήσει ιστοσελίδες ηλεκτρονικού ψαρέματος, όπως προαναφέρθηκε, ιστοσελίδες για την αναφορά των bot προς τους bot-master και ιστοσελίδες για τον έλεγχο των bot από τους bot master.

Διάδοση Δικτύου Botnet

Για τη διάδοση τους τα botnet πραγματοποιούν επιθέσεις, σαρώνοντας ένα σύνολο από IP διευθύνσεις για γνωστές TCP και UDP υπηρεσίες , και κάνοντας χρήση κώδικα εκμετάλλευσης ευπαθειών (exploit code) αποκτούν τον έλεγχο του μηχανήματος. Στη συνέχεια μεταφορτώνουν το λογισμικό που συνιστά το bot και το μηχάνημα πλέον αποτελεί και αυτό μέλος του botnet. Οι επιθέσεις που σχετίζονται με τη διάδοση του δικτύου μπορούν συνεχώς να εξελίσσονται, ενημερώνοντας τα bot με νέα exploit και νέες τεχνικές.

1.1.8 Διάσημα BotNet -Torping botnet

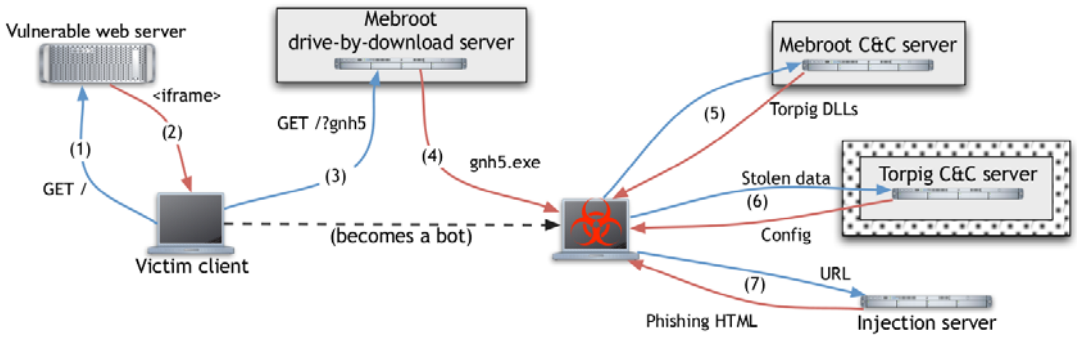
Στην ενότητα αυτή περιγράφονται ενδεικτικά κάποια διάσημα botnet εστιάζοντας στον τρόπο διάδοση τους και στο μέγεθος των δραστηριοτήτων και των χρηστών που προσβάλλουν. Ωστόσο αρχικά δίνεται ένας πίνακας όπου συνοψίζονται τα χαρακτηριστικά των κυριότερων botnet, από την εμφάνισή τους στις αρχές της δεκαετίας του 1990 και μέχρι και το 2007.

Πίνακας 2: Η εξέλιξη των Botnet (1990-2007)

Bot	Έτος	Γλώσσα προγραμματισμού	Πρωτόκολλο	Μηχανισμός διάδοσης
eggdrop	1993	C	IRC	Active download
Pretty Park	1999	Delphi	IRC	Send Email
Subseven 2.1	1999	Delphi	IRC	Send Email
GTBot	2000	MIRC Script	IRC	Binding to MIRC
SDBot	2002	C	IRC	Free Download
Slapper	2002	C	P2P	Remote Vulnerability Scan
AgoBot	2002	C++	IRC	Remote Vulnerability Scan
rxBot	2004	C	IRC	Remote Vulnerability Scan
phatBot	2004	C++	WASTE	Remote Vulnerability Scan
Bobax	2004	VC++	http	Send Email/ Remote Vulnerability Scan
ClickBot.A	2006	PHP	http	Binding to other malware
Nuwar or Storm worm	2007	VC++	P2P	Remote Vulnerability Scan
Zunker	2007	PHP/CGI	http	P2P file sharing

[Πηγή: Guide on Policy and Technical Approaches against Botnet,2008]

Torpig: Είναι ένα πρόγραμμα malware που στοχεύει στη συλλογή προσωπικών και οικονομικών στοιχείων από χρήστες λειτουργικού συστήματος Windows (σχήμα 8). Ερευνητές από το Πανεπιστήμιο της Καλιφόρνιας Santa Barbara κατάφεραν να “εισέλθουν” για 10 μέρες σε αυτό το botnet εκμεταλλευόμενοι της αδυναμίας που έχουν τα bot στο να πάρουν εντολές από τον ιδιοκτήτη τους. Μέσα σε αυτό το διάστημα οι ερευνητές ήταν σε θέση να συλλέξουν πληροφορίες συνολικού μεγέθους 70GB που είχαν κλέψει τα bot. Στις πληροφορίες αυτές συμπεριλαμβανόντουσαν 56.000 κωδικοί πρόσβασης οι οποίοι συλλέχθηκαν σε λιγότερο από μία ώρα. Οι πληροφορίες αυτές δεν τους έδειξαν μόνο πως πραγματικά λειτουργούσε το botnet, αλλά συνειδητοποίησαν πόσο “επισφαλείς” είναι οι χρήστες που βρίσκονται online.



Σχήμα 8: Η υποδομή του Torpig network. Με διάστικτο υπόβαθρο εμφανίζονται τα στοιχεία που έχουν υποστεί "πειρατεία"

[http://www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf]

Μέσα σε αυτές τις 10 μέρες οι ερευνητές κατάφεραν να συλλέξουν 300.000 διαφορετικά login για 368.501 διαφορετικά site, μάλιστα ένα 28% των χρηστών επαναχρησιμοποιούσε τα ίδια password. Με όλα αυτά τα στοιχεία οι ερευνητές κατάφεραν να διαβάσουν εκατοντάδες mais και μηνύματα σε forum, τα οποία πολλές φορές περιείχαν πολύ προσωπικές λεπτομέρειες για τα θύματα. Φυσικά ο κύριος σκοπός του Torpig είναι η συλλογή τραπεζικών πληροφοριών από τους χρήστες, όπως είναι οι αριθμοί πιστωτικών καρτών, οι online τραπεζικοί λογαριασμοί, τα paypal accounts κτλπ. Με τις πληροφορίες που είχε μαζέψει το συγκεκριμένο botnet στο διάστημα των 10 ημερών, οι ιδιοκτήτες του θα μπορούσαν να αποκομίσουν από 83.000 δολάρια έως 8,3 εκατομμύρια δολάρια.

Εν ολίγοις οι ερευνητές μετά τη μελέτη του συγκεκριμένου botnet, κατέληξαν στα εξής συμπεράσματα:

- η αξιολόγηση του μεγέθους ενός botnet με βάση το πλήθος των διακριτών IP δεν αποδίδει ακριβή αποτελέσματα,
- τα θύματα των botnet είναι άτομα τα οποία δε έχουν ενημερωμένους browsers, antivirus και χρησιμοποιούν εύκολους κωδικούς πρόσβασης,
- η αλληλεπίδραση μεταξύ καταχωρητών, εγκαταστάσεων hosting, ιδρυμάτων των θυμάτων και επιβολή του νόμου είναι μια αρκετά περίπλοκη διαδικασία.

Botnet Mariposa: Το botnet Mariposa ήταν ένα από πλέον διαδεδομένα botnet μέχρι και τις αρχές του 2010. Σε αυτό φαίνεται να ευθύνονται εκατομμύρια επιθέσεις παγκοσμίως, στην προσπάθειά του να υποκλέψει τραπεζικές και προσωπικές πληροφορίες μέσω των μολυσμένων Η/Υ.

Το Mariposa ανακαλύφθηκε το 2009 από το Mariposa Working Group, ένα ανεπίσημο γκρουπ εθελοντών από το τομέα της ασφάλειας Η/Υ και υπηρεσιών ασφαλείας, με σκοπό να ερευνήσει και να εξοντώσει το συγκεκριμένο botnet. Το Mariposa κατόρθωσε να δημιουργήσει αρκετές παραλλαγές του που εκμεταλλεύτηκαν συνολικά 12.7 εκατομμύρια Η/Υ παγκοσμίως.

http://www.virus.gr/portal/content/trend-micro-οι-δημιουργοί-του-botnet-mariposa-συλλαμβάνονται

Zeus και SpyEye: Οι πλατφόρμες Zeus και SpyEye διαδίδονται με trojan και εισχωρούν μέσω phishing ή πλαστών σελίδων στα υπολογιστικά συστήματα των χρηστών του

διαδικτύου, ενώ μπορούν να εισάγουν κώδικα σε σελίδες HTML. Είναι περίτεχνα κατασκευασμένα ώστε να βοηθούν τους κατόχους τους να δημιουργούν εύκολα botnet και να υποκλέπτουν στοιχεία, καταγράφοντας ό,τι πληκτρολογεί ο χρήστης, ανακατευθύνοντας παράλληλα τις αιτήσεις DNS (αλλαγές στο host των windows) και παρουσιάζοντας πλαστές σελίδες αντί για τις αυθεντικές.

http://malapetsasc.blogspot.com/2010/04/blog-post.html

Kelihos botnet: Botnet που εκτιμάται ότι αποστέλλει καθημερινά 4 εκατομμύρια spam email. Η Microsoft ανακοίνωσε πρόσφατα την εξάρθρωση του. Οι κατηγορούμενοι είχαν δημιουργήσει περίπου 3.700 subdomains μέσω της υπηρεσίας cz.cc, πολλά από τα οποία χρησιμοποιούνταν για παράνομες δραστηριότητες. Εκτιμάται ότι περίπου 41.000 υπολογιστές σε όλο τον κόσμο είχαν μολυνθεί και συμμετείχαν στις δραστηριότητες του botnet.

Σύμφωνα με τη Microsoft, το Kelihos botnet έχει χρησιμοποιηθεί για την υποκλοπή προσωπικών δεδομένων και άλλες παράνομες δραστηριότητες, πέρα από την αποστολή spam email. Το Kelihos είναι επίσης γνωστό με το όνομα Waledac 2.0.

http://www.real.gr/DefaultArthro.aspx?page=arthro&id=95611&catID=22&curPage=5

Koobface: Ο ιός “Koobface” χρησιμοποιεί το σύστημα μηνυμάτων του Facebook για να εξαπλωθεί και να μολύνει υπολογιστές.

http://www.virus.gr/portal/content/trend-micro-το-σκουλήκι-koobface-προσπαθεί-να-μεταδοθεί-ξανά-μέσω-του-facebook

Win32/Delf.QCZ: Το Win32/Delf.QCZ είναι ιδιαίτερα παραπλανητικό εφόσον χρησιμοποιεί το chat του Facebook για να εξαπλωθεί. Το κακόβουλο λογισμικό έχει τη δυνατότητα να απενεργοποιήσει την antivirus προστασία, εφόσον δεν είναι ανανεωμένη

[http://www.technopress.gr/2011/09/facebook.html]

Pushbot:Το Pushbot προσβάλει τα συστήματα μέσω της χρήσης Yahoo Messenger, MSN messenger or AIM, διαδίδεται μέσω zip files και δίνει την δυνατότητα απομακρυσμένης πρόσβασης. Έχει καταγραφή στη λίστα των botnet της Microsoft.

[http://www.pcthreat.com/parasitebyid-14821en.html]

Stormworm: Το ‘Storm worm’ είναι ένα πρόγραμμα ρομπότ (bot) με χαρακτηριστικά «δούρειου ίππου» που προσβάλει μηχανήματα με λειτουργικό σύστημα Windows. Ξεκίνησε μολύνοντας χιλιάδες από αυτά, στην Ευρώπη και την Αμερική στις 19 Ιανουαρίου 2007 χρησιμοποιώντας ένα μήνυμα ηλεκτρονικού ταχυδρομείου με θέμα σχετικό με μια πρόσφατη καιρική καταστροφή: «230 νεκροί καθώς η καταιγίδα χτυπά την Ευρώπη». Εκτιμήθηκε ότι δημιούργησε 1,5 εκατομμύριο μολύνσεις (PC World, 21/10/2007) με ταυτόχρονα ενεργά bot από 5.000 έως 40.000. Το Storm botnet χρησιμοποιούσε το πρωτόκολλο Overnet που βασίζεται στον αλγόριθμο Kademlia για την επικοινωνία των κόμβων.

2 ΑΝΙΧΝΕΥΣΗ

Σε αυτό το κεφάλαιο, παρουσιάζονται διάφορες μετρήσεις botnet και προσεγγίσεις ανίχνευσης. Οι τεχνικές διαπιστώθηκαν από έρευνα ειδικών μεταξύ των διαφόρων συμετεχόντων που δραστηριοποιούνται στον τομέα του περιορισμού των botnet.

2.1 Γενικοί τρόποι

2.1.1 Παθητικές τεχνικές

Αυτή η ομάδα των «τεχνικών παθητικής μέτρησης» αποτελείται από εκείνες όπου τα στοιχεία συλλέγονται αποκλειστικά και μόνο μέσω της παρατήρησης. Μέσα από την παρακολούθηση, οι δραστηριότητες μπορούν να παρακολουθούνται χωρίς να παρεμβαίνουν στο περιβάλλον ή να προκαλούν αλλοίωση των στοιχείων. Το γεγονός αυτό καθιστά αυτές τις προσεγγίσεις διαφανής και, σε πολλές περιπτώσεις, η εφαρμογή τους μπορεί να κρυφτεί από τους botmaster. Αξίζει να σημειωθεί, ωστόσο, ότι οι παθητικές μέθοδοι μπορούν επίσης να περιορίσουν τον όγκο των δεδομένων που μπορούν να συγκεντρωθούν για ανάλυση.

Παρουσιάζονται διάφορες προσεγγίσεις όσον αφορά την παθητική μέτρηση και την ανίχνευση των botnet, που χρησιμοποιούνται στις καθημερινές δραστηριότητες. Περιγράφονται μέθοδοι για την ανάλυση της κίνησης του δικτύου, και εξειδικευμένα πρωτόκολλα που χρησιμοποιούνται συχνά στον τομέα των botnet. Αυτό ακολουθείται από προσεγγίσεις που επικεντρώνονται στην αναγνώριση των επιθέσεων και την ερμηνεία των malware δυαδικών ακολουθιών .

Επιθεώρηση πακέτων

Μια δημοφιλής ιδέα για την αύξηση της ασφάλειας ενός δικτύου είναι να επιθεωρεί τα πακέτα δεδομένων του δικτύου. Η βασική ιδέα είναι να γίνεται ταίριασμα των διάφορων πεδίων του πρωτοκόλλου, ή του φορτίου του πακέτου, σε σύγκριση με ήδη αναγνωρισμένα μοτίβα αφύσικου ή ύποπτου περιεχόμενου. Αυτό μπορεί, για παράδειγμα να είναι, ένα πακέτο που περιέχει αλληλουχίες κώδικα κέλυφους (shell) που χρησιμοποιούνται για τη διάδοση malware, ή επικοινωνία με μια διεύθυνση Internet που αποδεδειγμένα φιλοξενεί κακόβουλο περιεχόμενο, ή ένας διακομιστής αρχείων που ξαφνικά αρχίζει να επικοινωνεί μέσω του πρωτοκόλλου chat, IRC. Αυτά τα “μοτίβα” ονομάζονται επίσης «υπογραφές ανίχνευσης».

Μια σημαντική εφαρμογή της έννοιας αυτής είναι «τα συστήματα ανίχνευσης εισβολής (IDS). Ο σκοπός των IDS είναι να προφυλαχθεί ένα περιβάλλον και να εκδοθεί μια προειδοποίηση σε περίπτωση που αναγνωρισθεί επίθεση. Οι υποομάδες των IDS κατηγοριοποιούνται σε δύο τύπους, ανάλογα με το πού είναι τοποθετημένα: network-based (NIDS) ή host-based συστήματα ανίχνευσης εισβολής (HIDS).

Εάν ένα IDS δεν εκδίδει μόνο μια προειδοποίηση κατά τον προσδιορισμό μιας επίθεσης αλλά αναλαμβάνει περαιτέρω δράση, ονομάζεται «σύστημα πρόληψης εισβολής» (IPS). Κατά κανόνα, οι δράσεις περιλαμβάνουν την απόρριψη του πακέτου ή το κλείσιμο της σύνδεσης. Μια άλλη επιλογή είναι να διαβιβάσει το περιεχόμενο πακέτων σε ένα σύστημα ανάλυσης. Οι πληροφορίες που εξάγονται για την επίθεση μπορεί επίσης να χρησιμοποιηθούν για να συμβάλουν στη δημιουργία μιας μαύρης λίστας ή για να ενημερωθούν οι κανόνες του firewall.

Ωστόσο, τα συστήματα ανίχνευσης εισβολής έχουν ορισμένα μειονεκτήματα:

1. Ο πλήρης έλεγχος όλων των περιεχομένων του πακέτου, είναι δύσκολος σε δίκτυα με υψηλό φορτίο κυκλοφορίας, τουλάχιστον όταν εφαρμόζονται από μια κεντρική θέση. Η χρήση τεχνικών, όπως η δειγματοληψία πακέτων ή το φιλτράρισμα πριν από την ανάλυση αυξάνει τον κίνδυνο να λείπουν κακόβουλα πακέτα. Η κλιμάκωση του εις βάθος ελέγχου πακέτου για την παρακολούθηση της κυκλοφορίας, για παράδειγμα, εξετάζεται στην μεγάλης κλίμακας παρακολούθηση των υποδομών του ευρυζωνικού διαδικτύου (LOBSTER). Σε αυτό το έργο, αναπτύχθηκε μια αποκεντρωμένη υποδομή για παρακολούθηση με παθητικούς αισθητήρες. Κατά τη διάρκεια του έργου, αναπτύχθηκαν πολλαπλά εργαλεία με επίκεντρο την επιθεώρηση της κυκλοφορίας και ανωνυμίας σε σχέση με την απαιτούμενη ανταλλαγή δεδομένων.
2. Εντοπίζονται μόνο γραμμές επικοινωνίας που περιέχουν γνωστά μοτίβα. Εξ ου και υπάρχουν διαφορετικοί τρόποι αποφυγής της ανίχνευσης. Μια τεχνική είναι να χωριστεί το κακόβουλο περιεχόμενο μεταξύ πολλών πακέτων, αποκρύπτοντας το ωφέλιμο φορτίο. Αυτό έχει ως αποτέλεσμα ότι μόνο τμήματα της υπογραφής θα πρέπει να περιλαμβάνονται στα απλά πακέτα. Ωστόσο, άλλες τεχνικές που χρησιμοποιούν ειδική κωδικοποίηση ή κρυπτογράφηση, προκειμένου να αποκρύψουν το ωφέλιμο φορτίο είναι ακόμη σε θέση να παρακάμψουν την ανίχνευση.
3. Τα IDS είναι πιθανό να έχουν ένα αξιοπρόσεχτο ποσοστό λανθασμένων ειδοποιήσεων (false positive). Από τη μία πλευρά αισθητήρες πρέπει να βαθμονομούνται έτσι ώστε να μην χάσουν καμία επίθεση και από την άλλη αυτό μπορεί να οδηγήσει σε προβλήματα χαρακτηρισμού κανονικών πακέτων ως κακόβουλα.

Παράδειγμα 1: Μια πρώτη προσέγγιση έδειξαν οι Blinkley και Singh. Παρουσίασαν μια προσέγγιση βασισμένη σε αφύσικη ανίχνευση, που χρησιμοποιεί έλεγχο των πακέτων δεδομένων για τη συλλογή δεδομένων. Ανέπτυξαν έναν αλγόριθμο για την ανίχνευση botnet που χρησιμοποιεί IRC, με βάση τη συμπεριφορά σάρωσης τους. Η προσέγγιση τους αποτελείται από δύο συνιστώσες, μία για TCP και ένα για το IRC. Η πρώτη συνιστώσα μέτρα το βάρος εργασίας TCP για μια διεύθυνση IP. Αυτό ορίζεται ως ο αριθμός των TCP πακέτων ελέγχου σύνδεσης (δηλαδή SYN, RST και FIN) σε σχέση με όλα τα πακέτα TCP, με δειγματοληψία κάθε τριάντα δευτερόλεπτα. Μια τιμή κοντά στο ένα (1) θεωρείται αφυσική και αποτελεί μια ισχυρή ένδειξη της δραστηριότητας σάρωσης. Η δεύτερη συνιστώσα αποτελείται από δύο στοιχεία παρακολούθησης IRC, που συλλέγουν στατιστικά στοιχεία σχετικά με κανάλια IRC, αφενός, και τη δραστηριότητα των διακριτών διευθύνσεων IP από την άλλη. Συσχέτισαν τα δεδομένα και από τις δύο συνιστώσες για τον εντοπισμό των καναλιών IRC που ήταν πιθανόν να φιλοξενούνται μολυσμένα μηχανήματα αφού δημιουργήθηκαν υποψίες λόγω του υψηλού φόρτου εργασίας. Το σύστημα αυτό δοκιμάστηκε στο τοπικό δίκτυο του πανεπιστημιού για τον εντοπισμό bot. Ως μειονέκτημα, και πιθανά αντιμέτρο, σημείωσαν ότι η κρυπτογράφηση των μηνυμάτων IRC ή η μη τυπική κωδικοποίηση του πρωτοκόλλου επικοινωνίας θα εμπόδιζε τη δυνατότητα συσχετισμού του IRC με το φόρτο εργασίας του TCP και ως εκ τούτου τη σωστή διάγνωση.

Παράδειγμα 2: Μια άλλη μέθοδος υποβληθείσα από τους Gu et al. συνδυάζει πολλές υπάρχουσες τεχνικές παρακολούθησης. Το εργαλείο τους "BotHunter», παρατηρεί τις εισερχόμενες και εξερχόμενες ροές πακέτων και εκτελεί ένα συσχετισμό με βάση το διάλογο για την ανίχνευση μολύνσεων. Το κέντρο του μηχανισμού συσχέτισης αποτελεί το σύστημα ανίχνευσης εισβολής στο δίκτυο Snord, ενισχυμένος με προσαρμοσμένους κανόνες και δύο plug-in εστιασμένα στα malware. Αυτά τα στοιχεία περιλαμβάνουν μηχανισμούς ανίχνευσης που καλύπτουν διάφορα στάδια της διαδικασίας μόλυνση, για παράδειγμα, τον εντοπισμό και την συνεχή επίθεση ενός στόχου. Επίσης, οι επόμενες ενέργειες θεωρούνται προσπάθειες να επικοινωνήσει με ένα C&C διακομιστή σε

περιπτώσεις επιτυχημένης μόλυνσης και δραστηριότητες για τη λήψη πρόσθετων κακόβουλων στοιχείων. Το σύστημα είναι σε θέση να παράγει αναφορές συνοψίζοντας τα βήματα μόλυνσης.

Ανάλυση των αρχείων ροής

«Η ανάλυση των αρχείων ροής» μπορεί να θεωρηθεί ως μια τεχνική για την ανίχνευση κίνησης του δικτύου σε ένα αφηρημένο επίπεδο. Αντί για τον έλεγχο μεμονωμένων πακέτων, όπως περιγράφηκε στην προηγούμενη ενότητα, οι ροές επικοινωνίας θεωρούνται σε συνολική μορφή. Σε αυτό το πλαίσιο, ένα record ροής αποτελείται από διάφορες ιδιότητες που περιγράφουν μια ροή δεδομένω δικτύου. Τυπικά χαρακτηριστικά είναι τα εξής: διεύθυνση προέλευσης και προορισμού, οι σχετικοί αριθμοί θύρας καθώς επίσης και το πρωτόκολλο που χρησιμοποιείται στο εσωτερικό των πακέτων, η διάρκεια της συνόδου, και το σωρευτικό μέγεθος και αριθμός των μεταδιδόμενων πακέτων.

Δεδομένου ότι το πραγματικό ωφέλιμο φορτίο των πακέτων αγνοείται από την προσέγγιση αυτή, μπορεί να αντιμετωπιστούν υψηλότερα ποσοστά κυκλοφορίας παρά με έλεγχο των πακέτων δεδομένων. Ωστόσο, για να βγάλουμε συμπέρασμα για τις ροές από τα πακέτα, πρέπει να παρακολουθείται η σύνοδος που σχετίζεται με τις επικεφαλίδες (headers). Συνήθως, κάθε σύνοδος παρακολουθείται, η δραστηριότητα παρακολουθείται με ένα μετρητή «ωρίμανσης». Όταν η δραστηριότητα εμφανιστεί, ο μετρητής έχει ρυθμιστεί σε ένα καθορισμένο χρονικό διάστημα και μειώνεται συνεχώς από τότε. Εάν ο μετρητής έχει εξαντληθεί, η παρούσα σύνοδος είναι πιθανόν να έχει τελειώσει. Αυτή η παρακολούθηση συνήθως παράγει ένα αξιοσημείωτο φορτίο για τα συστήματα καταγραφής των ροών. Μια τεχνική για να αντιμετωπιστεί αυτό είναι να δοκιμαστεί η κυκλοφορία του δικτύου, δηλαδή να ενσωματωθεί μόνο ένα από n πακέτα. Συνήθως χρησιμοποιούνται ενδεικτικές τιμές δειγματοληψίας 0,1-1%. Σε περίπτωση που η δειγματοληψία διενεργείται, τα δεδομένα σύνοδου επηρεάζονται έντονα και τα στατιστικά στοιχεία σχετικά με τον αριθμό των πακέτων και το συνολικό αριθμό των byte που μεταφέρθηκαν μπορεί να καταστούν αναξιόπιστα.

Το πρωτόκολλο δικτύου "NetFlow" από τη Cisco Systems μπορεί να θεωρηθεί ως “de facto” πρότυπο για την ανάλυση ροής. Οι δρομολογητές μπορεί να ρυθμιστούν ωστε το σύνολο της κυκλοφορίας σε αρχεία ροής να διέρχονται από αυτούς τα οποία στη συνέχεια αποστέλλονται σε μια εξωτερική μονάδα που συγκεντρώνει τα δεδομένα.

Ο στόχος της ανάλυσης των καταγραφών ροής είναι να προσδιοριστούν τα πρότυπα κυκλοφορίας που μπορεί να χρησιμοποιηθούν για το διαχωρισμό καλής από την κακόβουλη κίνηση και να δημιουργηθεί ένα σύστημα για την ανίχνευση πιθανής κακόβουλης επικοινωνίας.

Η ανάλυση των καταγραφών ροής για την ανίχνευση botnet επιτρέπει, τον προσδιορισμό των κόμβων που αλληλεπιδρούν με γνωστούς C&C διακομιστές. Ο προσδιορισμός επομένως συγκεκριμένων μολύνσεων μέσα σε ένα δίκτυο είναι δυνατός. Η εφαρμογή αυτής της τεχνικής μπορεί να θεωρηθεί ως μέσο για την υποστήριξη της ενεργού αντιμετώπισης περιστατικών και των διαδικασιών καθαρισμού.

Ένας πλήρης κατάλογος των εργαλείων για τη συγκέντρωση και την ανάλυση των ροών παρέχεται από τον SWITCH.ch.

Παράδειγμα 1: Οι Strayer et al. ανέλυσαν διάφορες μηχανές-μάθησης αλγορίθμων για την ανίχνευση της κυκλοφορίας IRC chat και IRC με βάση την κίνηση στο C&C botnet. Εξήγαγαν ροές που προέρχονται από πειραματικά αρχεία καταγραφής κυκλοφορίας και διαχώρισαν την εξέταση σε δύο στάδια. Το πρώτο στάδιο περιλαμβάνει τον εντοπισμό

γενικής IRC κυκλοφορίας μέσω ροών. Το δεύτερο στάδιο εκτελεί διαχωρισμό της καλής και κακόβουλης κίνησης στο IRC. Δήλωσαν ότι η επιλογή των παραμέτρων εισόδου στη διαμόρφωση των χαρακτηριστικών της ροής για τη μηχανή-μάθησης αλγορίθμων είχε σημαντικό αντίκτυπο στα αποτελέσματα. Το ισχυρότερο διακριτικό γνώρισμα του χαρακτηριστικού της ροής που εντοπίστηκε ήταν τα byte ανά πακέτο και η διακύμανση τους με την πάροδο του χρόνου.

Παράδειγμα 2: Οι Zeidanloo et al. πρότειναν ένα πλαίσιο για τον εντοπισμό των P2P botnet. Είναι βασισμένο στην υπόθεση ότι τα bot που ανήκουν στο ίδιο botnet είναι πιθανό να συμπεριφερθούν με τον ίδιο τρόπο όσον αφορά την αποστολή και λήψη μηνυμάτων ελέγχου, καθώς εκτελούν κακόβουλες δραστηριότητες, όπως η σάρωση και η διάδοση, όπως επίσης και το spamming. Το σύστημά τους είναι χωρισμένο σε διαφορετικές μονάδες. Η πρώτη μονάδα συγκεντρώνει την κίνηση από πηγές του δικτύου, όπως δρομολογητές και switch. Η δεύτερη μονάδα φιλτράρει γνωστές φιλικές διευθύνσεις IP και τα ονόματα domain από τα συλλεχθέντα πακέτα, με σκοπό τη μείωση του φορτίου του συστήματος ή ημιτελείς προσπάθειες σύνδεσης (οι οποίες δείχνουν επίσης σάρωση). Στο επόμενο βήμα, η κυκλοφορία συγκεντρώνεται σε εγγραφές ροής χρησιμοποιώντας το εργαλείο ελέγχου δίκτυου ARGUS. Αυτά τα αρχεία ροής συγκεντρωμένα σε ομάδες παρόμοιας δομής, με διαφορετικά χαρακτηριστικά κίνησης. Το “Packet Inspection”, εκτελείται παράλληλα. Το output των δύο τεχνικών, στη συνέχεια, συσχετίζεται για βελτίωση των αποτελεσμάτων.

Παράδειγμα 3: Οι Yen και Reiter παρουσίασαν μια προσέγγιση που ονομάζεται “Συνυπολογισμός κυκλοφορίας για ανίχνευση κακόβουλου λογισμικού”, ή TAMD για συντομία, από το όνομα του εργαλείου. Αυτό το εργαλείο εκτελεί ένα μοτίβο που ταιριάζει στη ροή του δικτύου. Τρία είναι τα επιλεγμένα χαρακτηριστικά:

- πρώτον, οι ροές που επικοινωνούν με έναν κοινό προορισμό, που είναι πιο απασχολημένος από το μέσο όρο όλων των προορισμών
- δεύτερον, εκείνοι που έχουν ένα παρόμοιο φορτίο ανάλογο με την απόσταση επεξεργασίας, ως μέτρο για την ομοιότητα, και
- τρίτον, οι ροές που ανήκουν σε κόμβο με ένα κοινό λειτουργικό σύστημα (OS), καθώς τα περισσότερα malware είναι για ένα συγκεκριμένο λειτουργικό σύστημα.

Εφάρμοσαν το TAMD σε ροές που προέρχονται από ένα πανεπιστημιακό δίκτυο, με περισσότερες από 33.000 διακριτές και ενεργές διευθύνσεις IP. Το σύστημά τους ήταν σε θέση να ανιχνεύσει όλες τις δευτερεύουσες δραστηριότητες κακόβουλου λογισμικού και το 87,5% των bot από την καταγραφή της κίνησης στο botnet.

Παράδειγμα 4: Οι Jelasity και Bilicki ανέλυσαν την ανίχνευση σε peer-to-peer botnet σε ένα (Αυτόνομο Σύστημα) AS μέσω προσομοιώσεων. Σε απάντηση στο γεγονός ότι πολλές από τις σημερινές peer-to-peer προσεγγίσεις ανίχνευσης botnet χρειάζονται υψηλά ποσοστά χειροκίνητης προσπάθειας από την άποψη της αντίστροφης μηχανικής και του πρωτόκολλου ανασυγκρότησης, εξέτασαν ένα αυτοματοποιημένο αλγόριθμο για την ανίχνευση αυτών των δικτύων P2P χρησιμοποιώντας διαγράμματα διασποράς κυκλοφορίας. Ακόμα και με τη χρήση ενός μάλλον απλού μοντέλουυ δικτύου, διαπίστωσαν ότι η εφαρμογή των τοπικών προσεγγίσεων για την ανίχνευση δίκτυο P2P δεν είναι πολύ ελπιδοφόρα, καθώς η προβολή αυτών των δικτύων μπορεί να είναι πολύ περιορισμένη στο εσωτερικό ενός AS συστήματος, ειδικά όταν τα bot έχουν σκοπό να διατηρηθεί χαμηλά ο αριθμός των συνδέσεων με άλλα bot.

Προσεγγίσεις που βασίζονται σε DNS

Όταν ένας κόμβος έχει παραβιαστεί από ένα botnet, η επικοινωνία καθορίζεται είτε πρός ένα διακομιστή ή πρός άλλους μολυσμένους κόμβους, ανάλογα με την υποδομή botnet. Αυτό απαιτεί την ένταξη του πρωτοκόλλου επικοινωνίας στο malware. Δύο τρόποι προσδιορισμού ενός σημείου επαφής είναι διαθέσιμοι για το σκοπό αυτό:

1. Σταθερές διευθύνσεις IP μπορούν να ενσωματωθούν στο bot, εκτελέσιμες κατά τη διανομή.
2. Ένα όνομα χώρου (domain name ή το σύνολο των domain) μπορεί να οριστεί ότι θα ειδοποιηθεί όταν το σύστημα είναι σε κίνδυνο.

Η χρήση ενός domain name προσφέρει ευελιξία με διάφορους τρόπους. Πρώτα απ 'όλα, ένα όνομα τομέα μπορεί να συνδέεται με πολλαπλές διευθύνσεις IP, βοηθώντας να δημιουργηθεί μια “redundant” αρχιτεκτονική που είναι πιο ανθεκτική. Αυτές οι διευθύνσεις IP δεν χρειάζεται να είναι στατικές, αλλά μπορεί να αλλάζουν δυναμικά κατά παραγγελία.

Αν το κακόβουλο όνομα τομέα έχει αναγνωριστεί μια φορά, μπορεί να χρησιμοποιηθεί για περαιτέρω ενέργειες. Για παράδειγμα, η παθητική αναπαραγωγή DNS μπορεί να χρησιμοποιηθεί για τη συλλογή πληροφοριών από DNS server και το αρχείο αυτό για επεξεργασία αργότερα. Αυτό επιτρέπει, για παράδειγμα, τον προσδιορισμό των κόμβων που έχουν ζητήσει ένα κακόβουλο όνομα τομέα πριν αυτό το όνομα σημειωθεί ως κακόβουλο ή τον αυτόματο εντοπισμό των «typo squatting». Typo squatting είναι η προσέγγιση που χρησιμοποιείται για την επίτευξη υψηλού αριθμού των “κατά λάθος” επισκεπτών σε μια ιστοσελίδα, χρησιμοποιώντας ονόματα τομέα που προέρχονται από την τροποποίηση της ορθογραφίας των νόμιμων πολύ γνωστών τομέων. Διάσημα παραδείγματα είναι

- " goggle.com "αντί για" google.com ", το οποίο είχε μολύνει στο παρελθόν, επισκέπτες με λογισμικό υποκλοπής spyware.
- " facebooik.com "αντί για" facebook.com ", η οποία υιοθετεί ακόμη και το σχεδιασμό της γνήσιας πλατφόρμας κοινωνικής δικτύωσης.

Η τελευταία αυτή περίπτωση καταδεικνύει τη δυναμικότητα αυτής της τεχνικής για χρήση σε phishing.

Από τεχνική άποψη, τα κακόβουλα ονόματα τομέα μπορεί να αποκλειστούν εύκολα από καταχωρητές σε παγκόσμιο επίπεδο ή από τους διαχειριστές των διακομιστών DNS σε τοπικό επίπεδο. Εναλλακτικά, το όνομα τομέα μπορεί να αναλάβει, σε συνεργασία με τους διαχειριστές των διακομιστών DNS, να παρακολουθεί τις εισερχόμενες αιτήσεις για το botnet διακομιστή C&C.

Εάν ένα όνομα τομέα έχει ήδη αναγνωριστεί ως κακόβουλο, είναι πολύ πιο πιθανό ότι όλα τα εισερχόμενα ερωτήματα για αυτή την καταχώρηση να προέρχονται από μολυσμένους κόμβους. Δίνει τη δυνατότητα ως εκ τούτου το μολυσμένο μηχάνημα να παρακολουθείται κάθε φορά που χρησιμοποιεί ένα διακομιστή DNS. Επιπλέον, εξελιγμένες μέθοδοι μπορούν να αναπτυχθούν με χρήση των χαρακτηριστικών των ερωτημάτων προς κακόβουλα domain, συμπεριλαμβανομένων συνήθως χαρακτηριστικών όπως χωρικών ή χρονικών σχέσεων. Αυτό επιτρέπει προσεγγίσεις που πρέπει να εφαρμόζονται με βάση την ανίχνευση ανωμαλιών στο DNS.

Παράδειγμα 1: Choi et al. παρουσίασαν μια προσέγγιση ανίχνευσης C&C διακομιστών και bot (βασισμένη σε κάποια ανωμαλία) που έχει ως στόχο ειδικές ιδιότητες στη συμπεριφορά των ερωτημάτων που κάνουν τα bot. Παρατήρησαν ότι τα botnet έχουν την τάση να εμφανίζουν συντονισμένη συμπεριφορά που ονομάζεται “ομαδική

δραστηριότητα". Για παράδειγμα, κάθε φορά που ένας C&C server έχει μια αποτυχία σύνδεσης ή μετεγκαθίσταται σε ένα νέο domain name, αυτό οδηγεί σε ένα γεγονός που επηρεάζει όλα τα συμμετέχοντα bot. Τα συνδεδεμένα μέλη του botnet θα ξεκινήσουν σχεδόν ταυτόχρονα με το ερώτημα για τον χαμένο C&C διακομιστή τους. Επιπλέον, συντονισμένες κακόβουλες δραστηριότητες, όπως DDoS και η αποστολή spam, είναι επίσης πιθανό να οδηγήσουν ώστε η ομαδική δραστηριότητα στο DNS να δίνει πληροφορίες για κάθε bot που συμμετέχει σε αυτή. Επιπλέον, η χρήση των δυναμικών υπηρεσιών DNS (DDNS) είναι συχνά μια ένδειξη του C&C server, η οποία επίσης ενσωματώθηκε στο μοντέλο τους.

Παράδειγμα 2: Οι Villamarin-Salomon και Brustoloni παρουσίασαν μια προσέγγιση για την ανίχνευση C&C διακομιστών (που βασίζεται επίσης σε κάποια ανωμαλία). Στο έργο τους, γίνεται σύγκριση διαφορετικών αλγορίθμων και αξιολογείται η αποτελεσματικότητά τους. Κατέληξαν στο συμπέρασμα ότι ασυνήθιστα ποσά επαναλαμβανόμενων NX DOMAIN απαντήσεων είναι κατάλληλοι δείκτες της παρουσίας ενός botnet. Μια NX domain απάντηση παράγεται από ένα διακομιστή DNS, αν ένα όνομα τομέα δεν μπορεί να επιλυθεί. Στο πλαίσιο των botnet, αυτό είναι συχνά το αποτέλεσμα της κατάργησης ή της μετεγκατάστασης ενός διακομιστή C&C. Επιπλέον, δήλωσε ότι η προσέγγιση που βασίζεται σε NX DOMAIN απαντήσεις είναι λιγότερο επιρρεπείς σε ψευδώ-θετικά αποτελέσματα από άλλους αλγορίθμους που έχουν αξιολογηθεί, καθώς είναι πιθανό να μην αναφέρουν υψηλού προφίλ τοποθεσίες που χρησιμοποιούν χαμηλή TTLS για την εξισορρόπηση φορτίου.

Παράδειγμα 3: Μια άλλη προσέγγιση, η οποία κάνει σύγκριση με την προαναφερθείσα (host-based) μέθοδο, παρουσιάστηκε από τους Morales et al. Θα διερευνηθεί πώς οι διαδικασίες αντιδρούν σε μια απάντηση που έλαβαν από ένα διακομιστή DNS μετά από ένα ερώτημα. Εκτός από τις άμεσες απόπειρες σύνδεσης που γίνονται προκειμένου να ενταχθούν στο botnet μετά την επίλυση ενός domain name, κάποια δείγματα malware που αναλύονται έκαναν επίσης αντίστροφα ερωτήματα DNS και μερικές φορές ακόμη και στις διευθύνσεις IP που είχαν ελήφθη αρχικά. Η πρόθεση αυτής της συμπεριφοράς είναι η απόκτηση επιπλέον ονόματων τομέων που συνδέονται με το botnet για τη δημιουργία πλεονασμού. Με βάση αυτά τα ευρήματα, οι Morales et al. δημιούργησαν μια ευρετική που μπορεί να βοηθήσει να βελτιωθεί το ποσοστό ανίχνευσης των host-based εργαλείων ανίχνευσης κακόβουλου λογισμικού.

Παράδειγμα 4: Οι Musahi et al. μελέτησαν τις αλλαγές στο μοτίβο της κίνησης DNS των κόμβων που μολύνθηκαν μαζικά με worm μέσω αλληλογραφίας. Παρατήρησαν ότι η λήψη email μέσω του Post Office Protocol (POP) και Simple Mail Transfer Protocol (SMTP) παράγει πολύ λιγότερη κίνηση DNS από την αποστολή e-mail μέσω SMTP. Για να εξηγήσουν αυτή τη συμπεριφορά έγινε η παραδοχή, ότι τα email έχουν συνήθως πολλαπλούς προορισμούς domain names που πρέπει να επιλυθούν. Στην περίπτωση που υπήρχε μια μόλυνση από έναν τύπο worm μαζικής αλληλογραφίας, αυτό το SMTP που σχετίζοταν με την κυκλοφορία αυξήθηκε σημαντικά, επιτρέποντας στους ερευνητές να εντοπίσουν μολύνσεις αποκλειστικά μέσω της κυκλοφορίας DNS.

Ανάλυση των Spam Records

Ένας κοινός σκοπός των botnet είναι η διανομή των "αυτόκλητων"ή ανεπιθύμητων e-mail, που είναι γνωστά ως spam. Μια αρκετά έμμεση προσέγγιση για τη μέτρηση των botnet και των αντίστοιχων δραστηριοτήτων τους είναι η ανάλυση των spam Records. Στο πλαίσιο αυτό, έμμεση σημαίνει ότι, αντί για την παρατήρηση της επικοινωνίας, όπως τα μηνύματα εντολών και τα μηνύματα ελέγχου, οι πληροφορίες προέρχονται από την έρευνα των spam μηνυμάτων που αποστέλλονται από ένα botnet. Προφανώς αυτή η μέθοδος θα

παρατηρήσει μόνο botnet που εκτελούν δραστηριότητα spamming. Για να λειτουργήσει αποδοτικά, πρέπει να δημιουργηθεί αντιστοίχιση μεταξύ μηνύματων spam και botnet. Αυτό είναι συχνά δυνατό, επειδή τα spam είναι πιθανό να οργανωθούν στις λεγόμενες “καμπάνιες” spam. Στο πλαίσιο αυτό, ο όρος “καμπάνια”, περιγράφει την πραγματική ιδιότητα των μηνύματων, να είναι πανομοιότυπα ή τουλάχιστον να έχουν ένα κοινό παρατηρήσιμο μοτίβο. Καθώς τα μηνύματα spam πρέπει να παράγονται από το bot, θα ακολουθήσουν ένα παρόμοιο μοτιβο, που αποτελεί τη βάση της διαδικασίας παραγωγής. Ακόμα κι αν το περιεχόμενο του μηνύματος αποτελεί ένα καλό σημείο εκκίνησης για μια τέτοια αντιστοιχία, ο μηχανισμός χαρακτηρισμού λαμβάνει επίσης υπόψη, περισσότερες ιδιότητες, όπως τα χαρακτηριστικά των υποκείμενων συνομιλιών SMTP και τα αντίστοιχα πεδία του πρωτοκόλλου στην κεφαλίδα ηλεκτρονικού ταχυδρομείου.

Όλες αυτές οι ιδιότητες επιτρέπουν σε μηνύματα spam να συγκριθούν, συγκεντρώνοντας τα σε “καμπάνιες” ανεπιθύμητων μηνύματων και τελικά συνδέοντάς τα με αντίστοιχο botnet. Για να γίνει αυτό αποτελεσματικά, το μοτίβο του spam μπορεί να εξαχθεί από bot που δρά ως “drone”, όταν εκτελείται σε ένα ελεγχόμενο περιβάλλον. Με βάση τις κεφαλίδες των μηνυμάτων ανεπιθύμητης αλληλογραφίας, είναι δυνατό να εξαχθούν συμπεράσματα σχετικά με τη θέση του ρομπότ και ως εκ τούτου για την παγκόσμια διανομή του botnet. Σαφώς, αναγνωρίζονται μόνο τα bot που συμμετέχουν σε spam “καμπάνιες”. Για διάφορους λόγους, ένα bot μπορεί να συμμετάσχει στο botnet, αλλά δεν είναι σε θέση, να στείλει μηνύματα spam. Ένας πιθανός λόγος για αυτό είναι ότι λείπει από την εφαρμογή του bot, ένα module για την αποστολή spam μηνυμάτων, ή δεν έχει εγκατασταθεί στο κινητό τηλέφωνο του θύματος. Εναλλακτικά, το bot μπορεί να αποφασίσει να μην στείλει spam, αν υπάρχει η υποψία ότι λειτουργεί μέσα σε ένα περιβάλλον ανάλυσης.

Όσον αφορά την ανίχνευση, η ανάπτυξη παγίδων του spam μπορεί να είναι ευεργετική προσθήκη σε αυτή την προσέγγιση. Παγίδες spam είναι διευθύνσεις ηλεκτρονικού ταχυδρομείου χωρίς παραγωγική λειτουργία εκτός από το να λάμβάνουν ανεπιθύμητα email, και έτσι μπορεί να θεωρηθούν ως ένας ειδικός τύπος honeypot, συνηθέστερα αναφερόμενα ως honeytoken. Η διαφορά μεταξύ αυτών των δύο μέσων είναι ότι οι παγίδες μηνυμάτων spam πρέπει να διαφημιστούν, π.χ. με την εγγραφή σε πολλά δελτία ενημέρωσης, φόρουμ συζητήσεων, κλπ. Σε περίπτωση που το spam χρησιμοποιείται ως μέσο διάδοσης, η αξιολόγηση των spam μηνυμάτων σε σχέση με τα συνημμένα και των συμπεριλαμβανομένων συνδέσεων μπορεί να οδηγήσει στην ανίχνευση άγνωστων ακόμη οικογενειών malware.

Παράδειγμα 1: Οι Kreibich et al. έχουν εκτελέσει μια βαθιά ανάλυση της συμπεριφοράς του botnet “Storm”. Ήταν σε θέση να εξάγουν διαφορετικά σύνολα δεδομένων από το botnet. Ελήφθησαν τρεις προσεγγίσεις:

1. Spam e-mail πρότυπα έχουν περισυλλεγεί από μία C&C υποδομή. Χρησιμοποιήθηκε ένα crawler (ρομπότ ανίχνευσης), συχνά αναζητώντας νέα πρότυπα.
2. Είχαν τοποθετήσει το δικό τους επίπεδο από proxy κόμβους, στο εσωτερικό του botnet. Αυτό τους επέτρεψε να τροποποιήσουν τα spam email πρότυπα και να συμπεριλάβουν δικές τους πληροφορίες, οι οποίες στη συνέχεια χρησιμοποιήθηκαν για να συναχθούν πληροφορίες σχετικά με τη μετατροπή spam email και τα ποσοστά επιτυχίας.
3. Δημιουργήθηκαν διευθύνσεις ηλεκτρονικού ταχυδρομείου "δείκτες" που τους επέτρεψε να διερευνήσουν τη χρήση των διευθύνσεων ηλεκτρονικού ταχυδρομείου που προέρχονται από τους προσβεβλημένους κόμβους για περαιτέρω spamming.

Τα κύρια αποτελέσματα των ερευνών τους είναι τα εξής:

- Οι διευθύνσεις ηλεκτρονικού ταχυδρομείου που συλλέγονται από τους κόμβους- θυμάτα σπάνια βρέθηκαν στο Διαδίκτυο. Δεδομένου ότι είναι επομένως πιθανό να μην είναι δυνατή η πρόσβαση μέσω της ανίχνευσης των σελίδων του διαδικτύου, αυτό δείχνει την αξία για τον botmaster της συγκέντρωσης διευθύνσεων ηλεκτρονικού ταχυδρομείου.
- Η αξιολόγηση πάνω από 460 εκατομμύρια μηνύματα spam είχε ως αποτέλεσμα τα ακόλουθα στατιστικά στοιχεία. Μόνο 1 στα 12.500.000 spam μηνύματα για φάρμακα, οδήγησε σε αγορά. Εναλλακτικά, εποχιακά μηνύματα ηλεκτρονικού ταχυδρομείου φαίνεται να είναι πιο αποτελεσματικά: 1 σε 265.000 spam ευχετήρια μηνύματα και 1 σε 178.000 spam "πρωταπριλιάς" οδήγησαν σε μόλυνση. Επίσης, 1 στα 10 άτομα που επισκέπτονταν μια προετοιμασμένη ιστοσελίδα κατέβασε και έτρεξε ένα εκτελέσιμο που τους προσφέρθηκε.
- Κατά μέσο όρο, τα ονόματα τομέα που χρησιμοποιούνται σε μηνύματα spam μπορούν να χρησιμοποιηθούν για λίγες μέρες μόνο, πριν από την εγγραφή τους σε μαύρες λίστες

Παράδειγμα 2: Λαμβάνοντας υπόψη ότι τα κανάλια ελέγχου των σύγχρονων botnet γίνονται πιο αόρατα, οι Hao και Feamster ανέπτυξαν μια νέα μέθοδο για την εκτίμηση του πληθυσμού των botnet και τη δυναμική συμμετοχή του, με την οποία αναλύεται η κυκλοφορία της επίθεσης, όπως τα αρχεία του spam ηλεκτρονικού ταχυδρομείου. Έδειξαν ότι ακόμη και η εξέταση των μικρών επιμέρους δείγματων από μια τοπική εξάπλωση μπορεί να είναι επαρκής για μια αξιόπιστη εκτίμηση μιας παγκόσμιας προοπτικής. Η διασταύρωση των αποτελεσμάτων τους, με δεδομένα από μια άλλη ερευνητική ομάδα, η οποία παρακολουθούσε το botnet "Storm" με καταμέτρηση των peer-to-peer συνδέσεων, έδειξε ότι η μέθοδος με βάση τα μηνύματα spam, παρήγαγε μόνο 4% -10% απόκλιση.

Παράδειγμα 3: Οι Dunagan et al. έδειξαν ότι η ανάλυση των μεγάλων ποσοτήτων spam μπορεί να χρησιμοποιηθεί επιτυχώς για τη αντιστοίχιση εντοπισμένων spam bot σε διαφορετικά botnet. Γι 'αυτό, έκαναν εκτεταμένη χρήση της έννοιας "καμπάνια" στα spam. Τα κύρια αναγνωριστικά για τις "καμπάνιες" αυτές ήταν ο περιορισμένος κύκλος διαφημιζόμενων προϊόντων, ή οι όμοιες φράσεις που χρησιμοποιούνται σε όλα τα e-mail.

Παρατήρηση των TPC και UDP συνδέσεων

Η τελευταία γενιά των botnet χρησιμοποιεί για την επικοινωνία μεταξύ bot και C&C server το πρωτόκολλο (P2P) peer to peer. Αυτό έχει ως αποτέλεσμα τον αυξημένο αριθμό TCP και UDP συνδέσεων, συνήθως αποτυχημένων. Επίσης υπάρχει ένα εύρος από ανοιχτά udp και tcp ports. Εφόσον λοιπόν σε ένα δίκτυο δεν χρησιμοποιούνται peer to peer προγράμματα και παρατηρείται εκρηκτική αύξηση των συνδέσεων και των ανοιχτών port, τότε είναι ένδειξη για την ύπαρξη δικτύου botnet

http://grhoneypots.wordpress.com/2010/01/13/τεχνικές-ανίχνευσης-botnet/

Ανάλυση των log files

Οι σύγχρονες εφαρμογές και τα υπολογιστικά συστήματα είναι σχεδιασμένα έτσι ώστε όχι μόνο να πραγματοποιούν μια ενέργεια αλλά και να την καταγράφουν αρχειακά. Αυτές οι καταγραφές ονομάζονται log files. Στα αρχεία αυτά αποθηκεύεται κάθε δραστηριότητα του υπολογιστή, όπως συνδέσεις και αποσυνδέσεις χρηστών, συνδέσεις δικτύου, αλλαγές στο file system, κ.α. Οι εγγραφές μέσα στα log file, που συσχετίζονται με botnet μπορεί να είναι αρκετά εμφανείς, αφού το πλήθος τους, λόγω της αυξημένης χρήσης υπηρεσιών, είναι αρκετά μεγάλο, χωρίς προφανή αιτία.

Επιπλέον, υπάρχει και η μέθοδος, όπου log file από διαφορετικά μηχανήματα συγκρίνονται μεταξύ τους. Η σύγκριση γίνεται στο μέγεθος των αρχείων και στο πλήθος

κάποιων κλήσεων συστήματος, ώστε να εντοπιστούν διαφοροποιήσεις από την ομαλή λειτουργία των συστημάτων. Λαμβάνοντας, επίσης, υπόψη ότι τα botnet δρουν κατά συνεκτικό τρόπο, υλοποιώντας αποστολές κατά ομάδες, συμπεραίνεται ότι η αύξηση του μεγέθους των αρχείων και του πλήθους των κλήσεων συστήματος που προαναφέρθηκαν θα είναι ταυτόχρονη. Η σύγκριση και συσχέτιση λοιπόν των αρχείων μεταξύ τους μπορεί να κάνει εμφανείς τις ενέργειες των botnet

Κατά συνέπεια, η ανάλυση των Log file είναι μια έμμεση μέθοδος ανίχνευσης και μέτρησης η οποία σχετίζεται με την καταγραφή δεδομένων ως απόρροια της δράσης Bot. Για το λόγο αυτό παρουσιάζει ομοιότητες με την μέθοδο της ανάλυσης των spam record.

Στην περίπτωση που κάποια συσκευή τρέχει πολλά service, και καθένα από αυτά καταγράφει τα δικά του γεγονότα, είναι απαραίτητη η μελέτη κάθε αρχείου καταγραφής ξεχωριστά. Επίσης αν στο σύστημα είναι εγκατεστημένο κάποιο firewall ή IDS σύστημα τότε τα αρχεία καταγραφής τους μπορούν να προσφέρουν χρήσιμες πληροφορίες. Η ανάλυση μπορεί να πραγματοποιείται παράλληλα στις πολλαπλές πηγές εισόδου.

Ωστόσο, παρόλο που η αυτόματη διάκριση μεταξύ spam και ασφαλών email έχει φθάσει σε ένα εξελιγμένο και αρκετά αποδοτικό επίπεδο, η διάκριση μεταξύ τακτικής, ήπιας επεξεργασίας. και καταχρηστικής συμπεριφοράς που προκαλείται από την δράση bot είναι αρκετά δύσκολη μέσω μόνο της θεώρησης των log file.

Ένα χαρακτηριστικό παράδειγμα μιας τέτοιας περίπτωσης θα ήταν μια κατανεμημένη άρνηση εξυπηρέτησης με στόχο έναν web server, όπου η ανάλυση των αρχείων καταγραφής θα σήμαινε μια λίστα συμμετεχουσών διευθύνσεων IP. Σε κάποιες περιπτώσεις, μπορεί να είναι εντελώς αδύνατη μια τέτοια διάκριση, είτε τοπικά είτε από απομακρυσμένο σημείο. Συνεπώς, μια τέτοια μέθοδος είναι εφαρμόσιμη μόνο στις περιπτώσεις όπου τα χαρακτηριστικά της κακόβουλης συμπεριφοράς μπορούν να ταυτοποιηθούν υπό την έννοια της ανάπτυξης μηχανισμών αυτόματης ταξινόμησης

Έχουν γίνει προσπάθειες για την ανακάλυψη μη κανονικών γεγονότων και ανωμαλιών, όπως η άτυπη χρήση μιας υπηρεσίας ή εμφανών και μη κανονικών ακολουθιών αιτημάτων και ερωτημάτων. Σε αυτό το πλαίσιο η χρήση έχει έννοια ποιοτική και ποσοτική. Για παράδειγμα, μια αξιοσημείωτη αύξηση στα αιτήματα μια διαδικτυακής υπηρεσίας μπορεί να υποδεικνύει τη δράση ενός botnet.

Γενικά παρατηρείται ότι, τα bot μέσω της πρόσβασης στα URL προκαλούν αναγνωρίσιμες εισόδους log για διάφορους λόγους. Για παράδειγμα, το Conficher botnet χρησιμοποιεί απλά αιτήματα HTTP σε μεγάλης επισκεψιμότητας ιστοτόπους (όπως yahoo.com κ.λπ.) προκειμένου να συγχρονίσει τα bot και να πιστοποιήσει τη συνδεσιμότητα με το διαδίκτυο. Αρχικά οι καταχωρήσεις του αρχείο καταγραφής που δημιουργούνται κατά αυτό τον τρόπο φαίνονται ως κανονικά αιτήσεις HTTP, γεγονός που δυσκολεύει τον εντοπισμό τους και τη διάκριση μεταξύ κανονικών και κακόβουλων δράσεων. Τα χαρακτηριστικά μπορεί να είναι διφορούμενα. Το Conficker ζητά μόνο την αρχική σελίδα, και όχι το περιεχόμενο που συνδέεται με αυτή (όπως οι εικόνες) το οποίο συνήθως είναι φορτωμένο μέσω web server. Επίσης, στην περίπτωση που ένας συγκεκριμένος μηχανισμός, χρησιμοποιείται από δύο ή περισσότερα διακριτά botnet, μπορεί να ανιχνευθεί μόνο η παρουσία του bot, και όχι το botnet με το οποίο συνδέεται.

Παράδειγμα: Εστιάζοντας, στις ανωμαλίες των εφαρμογών των log file, οι Linary et al. απέδειξαν ότι τα Botnet μπορούν να ανιχνευθούν και να μετρηθούν χωρίς να είναι απαραίτητη η υπόθεση της υποκείμενης αρχιτεκτονικής τους. Επέδειξαν την προσέγγισης τους σε μια μελέτη περίπτωσης στην οποία οι ανωμαλίες στα πρότυπα των ερωτημάτων

της διανεμημένης υπηρεσίας WHOIS χρησιμοποιήθηκαν για την ανίχνευση και εντοπισμό των δραστηριοτήτων των botnet.

Honeypots

Η τεχνολογία των honeypot χρησιμοποιεί συσκευές που «προσελκύουν» και καταγράφουν επιθέσεις για τον εντοπισμό botnet. Τα honeypot αποτελούν παθητικά συστήματα ασφαλείας. Δεν συμμετέχουν δηλαδή ενεργά στην ασφάλεια κινητών-υπολογιστών, αποτρέποντας δικτυακές επιθέσεις όπως άλλα συστήματα ασφαλείας (firewalls, IPS), αλλά παθητικά συλλέγοντας πληροφορίες. Τα honeypot αποτελούν παγίδες κατάλληλα παραμετροποιημένες, ώστε να προσομοιάζουν πραγματικά συστήματα με σκοπό την καταγραφή δεδομένων δικτυακών επιθέσεων.

Η ανάλυση αυτών των δεδομένων, οδηγεί στην απόκτηση περισσότερης γνώσης. Η γνώση αυτή βοηθάει στην καλύτερη κατανόηση του προβλήματος και επομένως στην εφαρμογή ιδανικότερων μέτρων προστασίας από τα ήδη υπάρχοντα. Αυτό συνεπάγεται μείωση του κινδύνου πρόκλησης ζημίας στα ευαίσθητα δεδομένα. Η αξία των honeypot χαρακτηρίζεται από την ικανότητα τους να προκαλέσουν το ενδιαφέρον των κακόβουλων χρηστών ώστε να καταγράψουν τις περισσότερες δυνατές επιθέσεις.

Η τεχνολογία των honeypot είναι ένα σημαντικό εργαλείο για τη καταγραφή και μελέτη των botnet και της κίνησης που δημιουργούν, η οποία σε καμία περίπτωση δεν μπορεί να αποκρυφτεί, παρά μόνο να κρυπτογραφηθεί και να «καμουφλαριστεί» μέσα σε άλλα πρωτόκολλα επικοινωνίας.

Τα honeypot διακρίνονται σε δύο κατηγορίες:

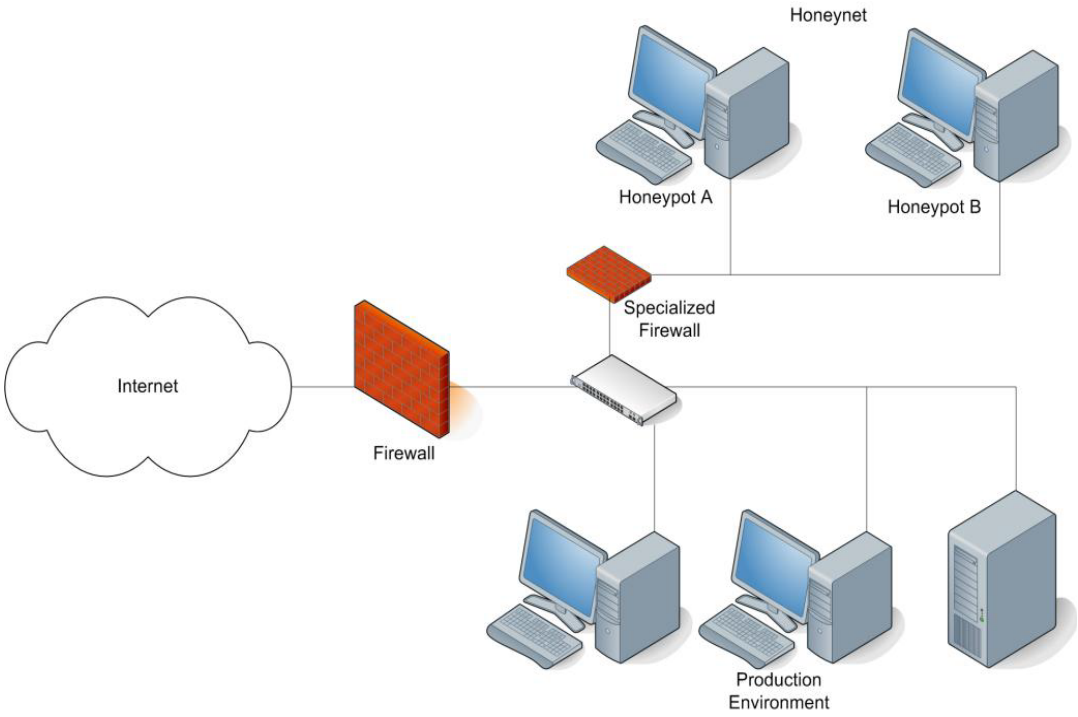
- client and server honeypots: τα οποία εγκαθίστανται συνήθως σε εταιρίες ή οργανισμούς, παράλληλα με τα μηχανήματα παραγωγής και έχουν ως σκοπό να διερευνήσουν το είδος των δεδομένων που διακινούνται στο δίκτυο.
- interaction honeypots: τα οποία διακρίνονται σύμφωνα με είδος αλληλεπίδρασης το οποίο προσφέρουν, σε χαμηλής και υψηλής αλληλεπίδρασης.

Όπως αναφέρθηκε, ο κύριος λόγος για την ανάπτυξη και εφαρμογή των Honeypot είναι η απόκτηση περισσότερης γνώσης σχετικά με τις πρακτικές και στρατηγικές που χρησιμοποιούν οι δημιουργοί του κακόβουλου υλικού και των hackers.

Γενικά, δύο τύποι πληροφορίας μπορούν να συγκεντρωθούν με τη χρήση των honeypot:

- τύποι φορέων επίθεση σε λειτουργικά συστήματα και λογισμικό επίθεσης, καθώς και τον αντίστοιχο κώδικα.
- δράσεις που εκτελούνται σε μια εκμεταλλευόμενη μηχανή. Αυτές μπορούν να καταγραφούν ενώ το κακόβουλο λογισμικό που φορτώνεται στο σύστημα μπορεί να διατηρηθεί για περεταίρω διερεύνηση.

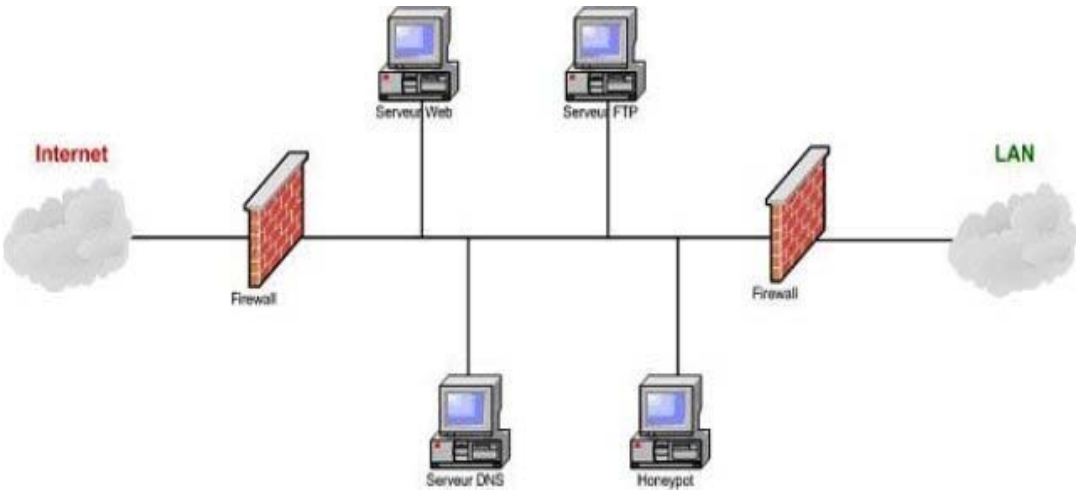
Τα client honeypot έχουν ως στόχο να μιμηθούν την τακτική συμπεριφορά ενός λογισμικού ή χρήστη. Ουσιαστικά, χαρακτηρίζονται από την προσπάθεια να δεχθούν επίθεση. Σε αντίθεση τα server honeypot, μένουν παθητικά.



Σχήμα 9: Honeypot υψηλής αλληλεπίδρασης

Τα honeypot υψηλής αλληλεπίδρασης (σχήμα 9), προσφέρουν ένα περιβάλλον υψηλής αλληλεπίδρασης στον κακόβουλο χρήστη. Δεν αποτελούν εξομοιωτές, αλλά πρόκειται για πραγματικά συστήματα με πραγματικές υπηρεσίες που έχουν ως σκοπό να ξεγελάσουν πλήρως τον επιτιθέμενο χρήστη. Πολλές φορές αυτά τα συστήματα αποτελούν αντίγραφα πραγματικών παραγωγικών μηχανών, τα οποία έχουν ως σκοπό να εξετάσουν τα κενά ασφαλείας που υπάρχουν σε αυτά. Το ότι τα honeypot υψηλής αλληλεπίδρασης αποτελούν αντίγραφα πραγματικών συστημάτων συνεπάγεται ότι ο εντοπισμός τους από τον έμπειρο επιτιθέμενο απαιτεί περισσότερο χρόνο. Κατά αυτό τον τρόπο καταγραφούν ένα μεγάλο αριθμό επιθέσεων, παράγοντας ένα μεγάλο όγκο δεδομένων και συνεπώς ένα αυξημένο επίπεδο γνώσης για τους διαχειριστές τους.

Τα honeypot υψηλής αλληλεπίδρασης είναι πιο δύσκολα στη χρήση και ανάπτυξη τους, καθώς απαιτούν τη ρύθμιση πολλών παραμέτρων, ενώ χρειάζονται και περισσότερους πόρους συστήματος προκειμένου να λειτουργήσουν. Η ανάλυση του μεγάλου όγκου δεδομένων τον οποίο παράγουν είναι δύσκολη και απαιτεί πολύωρη εργασία. Επίσης επειδή δύναται να παραβιαστούν, ο επιτιθέμενος μπορεί να τα χρησιμοποιήσει ως πλατφόρμες επίθεσης σε άλλα συστήματα. Λόγω του ότι η χρήση honeypot έστω και για εκπαιδευτικούς σκοπούς, δεν μπορεί να αποτελέσει άλλοθι για κακουργηματικές πράξεις, θα πρέπει πάντα να υπάρχουν οι κατάλληλες δικλείδες ασφαλείας. Σε περίπτωση που αυτά τα συστήματα παραβιαστούν και χρησιμοποιηθούν για παράνομες δραστηριότητες, οι συνέπειες θα επιβαρύνουν τους διαχειριστές και όχι μόνο τους παραβάτες.



Σχήμα 10: Networking using Honeypot χαμηλής αλληλεπίσρασης

[http://forums.techarena.in/guides-tutorials/1347805.htm]

Τα honeypot χαμηλής αλληλεπίδρασης, όπως δηλώνει και το όνομα τους, είναι συστήματα τα οποία δεν προσφέρουν υψηλό επίπεδο αλληλεπίδρασης στον κακόβουλο χρήστη. Αυτού του είδους τα honeypot έχουν περιορισμένες δυνατότητες και εξομοιώνουν μονάχα βασικές λειτουργίες ενός πραγματικού μηχανήματος παραγωγής. Για παράδειγμα εξομοιώνουν την στοίβα του TCP/IP δικτύου ενός συστήματος και κάποιες άλλες απλές υπηρεσίες. Συνεπώς όντας εξομοιωτές μικρής κλίμακας και όχι πραγματικά συστήματα, ο επιτιθέμενος δεν έχει τη δυνατότητα να αναπτύξει μια ολοκληρωμένη επίθεση π.χ. παραβίαση μηχανής. Τα χαμηλής αλληλεπίδρασης honeypot έχουν τα πλεονεκτήματα ότι είναι εύκολα στην εγκατάσταση και τη συντήρηση και δεν απαιτούν πολλούς πόρους συστήματος προκειμένου να λειτουργήσουν. Επιπλέον η χρήση τους είναι ιδιαίτερα απλή, δεν διατρέχουν τον κίνδυνο να παραβιαστούν και παράγουν ένα μικρό σχετικά όγκο δεδομένων για ανάλυση. Αποτελούν συνήθως ιδανική λύση για κάποιο αρχάριο χρήστη ο οποίος θέλει να εισέλθει σε αυτό το χώρο.

Από την άλλη πλευρά τα honeypot χαμηλής αλληλεπίδρασης προσφέρουν ένα περιβάλλον με βασικές μονάχα λειτουργίες. Ένας έμπειρος επιτιθέμενος θα είναι σε θέση αρκετά σύντομα να καταλάβει ότι δεν έχει να αντιμετωπίσει ένα πραγματικό σύστημα. Άμεση συνέπεια αυτού του γεγονότος, θα είναι ο επιτιθέμενος να εγκαταλείψει την προσπάθεια αμέσως. Επίσης ο μικρός όγκος δεδομένων τον οποίο παράγουν τα χαμηλής αλληλεπίδρασης honeypot σημαίνει την καταγραφή λιγότερων πληροφοριών σχετικά με τις διενεργημένες επιθέσεις και συνεπώς έχουν μικρότερη εκπαιδευτική αξία.

Παραδείγματα honeypot χαμηλής αλληλεπίδρασης είναι τα εξής: La Brera Dionaea, Nepenthes, mwcollectd, Honeytrap, και honeyd.

Τα οφέλη από την εφαρμογή των honeypot εξαρτάται από την ικανότητα τους να ταξινομούν την κίνηση στο διαδίκτυο και τις εσωτερικές δραστηριότητες π.χ. αλλαγές στα αρχεία του συστήματος. Αυτό δημιουργεί την ανάγκη για στενή και πλήρη παρακολούθηση των διαδικασιών. Είναι κρίσιμης σημασίας η υιοθέτηση εξελιγμένων προσεγγίσεων για την ανάλυση και ερμηνεία της κακόβουλης συμπεριφοράς προκειμένου να αναγνωριστούν οι μέχρι τώρα άγνωστες επιθέσεις.

Τα honeypot παίζουν έναν σημαντικό ρόλο στην ανάλυση των botnet. Χρησιμοποιούνται ως εργαλεία για την ανίχνευση γεγονότων σάρωσης και κρουσμάτων κακόβουλου λογισμικού. Επιτρέπουν την ταυτοποίηση και καταμέτρηση των κεντρικών υπολογιστών που εμπλέκονται και μπορούν να συλλέξουν αυτόματα δείγματα κακόβουλου λογισμικού

για ανάλυση. Βέβαια, ένα hoenypot μπορεί να δει την εισερχόμενη κίνηση από τις διευθύνσεις IP. Σε αυτό το πλαίσιο, ένα διαδικτυακό τηλεσκόπιο (network telescope) το οποίο παρακολουθεί τη δικτυακή κίνηση από ή προς ένα κομμάτι των διευθύνσεων του δικτύου που δεν έχουν αποδοθεί προς χρήση, μπορεί να χρησιμοποιηθεί για να παρέχει Input σε honeypot που αποτελούν ένα σύστημα honeyfarm. Παραδείγματα ενεργών darknet που λειτουργούν σε παγκόσμια κλίμακα είναι τα ATLAS system και CAIDA darknet .

Παράδειγμα 1: Οι Li et al χρησιμοποίησαν ένα συνδυασμένο daknet και honeynet αποτελούμενο από 2.540 διευθύνσεις από 10 συνεχούς τάξη C δίκτυα και ανέλυσαν την εισερχόμενη κίνηση το έτος 2006. Μισοί από τους αισθητήρες ήταν μη-αποκρινόμενοι και οι άλλοι μισοί χρησιμοποιούσαν το honeyd. Μετά το φιλτράρισμα της εισερχόμενης κίνησης παρατήρησαν 43 παγκόσμιας σάρωσης γεγονότα botnet διενεργούμενα από 63.851 μοναδικές διευθύνσεις αποστολέα. Ανακάλυψαν ότι το 75% των γεγονότων σάρωσης με επιτυχία οδήγησαν σε μια επίθεση κακόβουλου φορτίου.

Παράδειγμα 2: Οι Goebel et al ανέπτυξαν το λογισμικό nepenthes σε ακαδημαϊκά πλαίσια για την παρατήρηση 16.000 διαευθύνσεων για 8 εβδομάδες (10/06-01/07). Την περίοδο αυτή συγκέντρωσαν 13.400.000 malware binaries, εκ των οποίων 2.558 είχαν ένα μοναδικό MD5 hash. Επιπλέον προχώρησαν στα εξής περαιτέρω βήματα ανάλυσης μετά την αρχική συγκέντρωση των αρχικών δειγμάτων:

- το GFI Sandbox χρησιμοποιήθηκε για τον χαρακτηρισμό της συμπεριφορά του malware.
- 4 διαφορετικά antivirus scanner χρησιμοποιήθηκαν για τη διάγνωση της οικογένειας του malware.
- Η ανάλυση ολοκληρώθηκε με τη χρήση του λογισμικού botspy, ένα εργαλείο το οποίο αυτόματα εξάγει πληροφορία για τη λειτουργικότητα του απομακρυσμένου έλεγχου ενός δοσμένου δυαδικού στοιχείου.

Από τα δείγματα αυτά, ταυτοποίησαν 40 C&C server από τη μοναδική IP διεύθυνση τους

Παράδειγμα 3: Οι Palm και Dacier πραγματοποίησαν μια μεγάλης διάρκειας μελέτη πάνω στα honeypot χαμηλής αλληλεπίδρασης. Αξιολόγησαν τα αποτελέσματα από 40 αναπτύγματα πολλαπλών hoenyd, καθένα από τα οποία «έτρεχε» για 800 ημέρες. Διαχωρίζοντας τα δεδομένα των χωρών από τις οποίες προέρχονταν οι μηχανές επίθεσης, ταυτοποίησαν τις μέσω IP πηγών διευθύνσεις και διαχωρίζοντας τις επιθέσεις μέσω των honeypot, παρατηρήθηκαν διαφορετικές συσχετίσεις επιθέσεων. Εφαρμόζοντας παρόμοια μέτρηση, μπορούν να ταυτοποιηθούν μεμονωμένα ή group από botnet με κοινά χαρακτηριστικά, δείχνοντας διάρκεια ζωής περισσότερο από 750 μέρες.

Αξιολόγηση ανάδρασης των λογισμικών προστασίας (ANTI-VIRUS SOFTWARE FEEDBACK)

Τα τελευταία χρόνια, οι πάροχοι λογισμικού anti-virus ανέπτυξαν λύσεις βασισμένες στη διάδοση κατανεμημένης πληροφορίας, οι οποίες ενσωματώνουν την ανάδραση από το λογισμικό που είναι εγκατεστημένο στις μηχανές των χρηστών τους.

Αναλόγως του βαθμού των λεπτομερειών της πληροφορίας που προσφέρει αυτή η λειτουργία ανάδρασης, η προσέγγιση αυτή βοηθά τις εταιρίες λογισμικού προστασίας να αντιδρούν γρηγορότερα σε αναδυόμενες απειλές και να αποκτούν πληροφόρηση σχετικά με τη ποιότητα και τη γεωγραφική κατανομή των πιθανών προσβολών.

Η βασική διαφορά τους από τα κλασικά προϊόντα προστασίας είναι η διπλής κατεύθυνσης επικοινωνία μεταξύ χρήστη και παρόχου.

Παράδειγμα: Ένα υποσχόμενο λογισμικό αυτής της κατηγορίας είναι το Malicious Software Removal Tool της Microsoft. Οι μηχανές που έχουν εγκατεστημένο αυτό το εργαλείο δίνουν feedback στη Microsoft το οποίο στη συνέχεια ενσωματώνεται στη “Security Intelligence Report”. Αξίζει να αναφερθεί ότι η τελευταία έκθεση (Ιανουάριος – Ιούνιος 2010) περιλάμβανε δεδομένα από περισσότερα των 600 εκατομμυρίων συστημάτων παγκοσμίως.

2.1.2 Ενεργητικές τεχνικές

Η ομάδα των ενεργητικών τεχνικών μέτρηση περιλαμβάνει προσεγγίσεις οι οποίες αφορούν την αλληλεπίδραση με τις πηγές πληροφόρησης που παρακολουθούνται. Αν και αυτό επιτρέπει την άσκηση μετρήσεων εις βάθος, η εφαρμογή τους μπορεί να αφήσει τα ίχνη που θα επηρεάσουν τα αποτελέσματα, ή να περιλαμβάνει δραστηριότητες που μπορούν να παρατηρηθούν.

Αυτό μπορεί να προκαλέσει αντιδράσεις, όπως μια DDoS επίθεση εναντίον του αναλυτή ή την εισαγωγή αλλαγών στη δομή του botnet που θα περιπλέξει τις μετρήσεις, ακόμη και τη μετανάστευση της υπηρεσίας, προκειμένου να αποφύγει τον έλεγχο.

Κατ 'αρχάς, παρουσιάζονται δύο γενικές τεχνικές για την ενεργό μέτρηση. Και οι δύο μπορεί να εφαρμοστούν σε μια πολύ παρεμβατική μορφή η οποία είναι ήδη συνδεδεμένη με τα πιθανά αντίμετρα botnet, αλλά μπορούν επίσης να εφαρμόζονται «σιωπηλά». Οι ακόλουθες προσεγγίσεις επικεντρώνονται σε ορισμένα πρωτόκολλα που χρησιμοποιούνται σε botnet ή ειδικούς τύπους αρχιτεκτονικής botnet.

Sinkholing

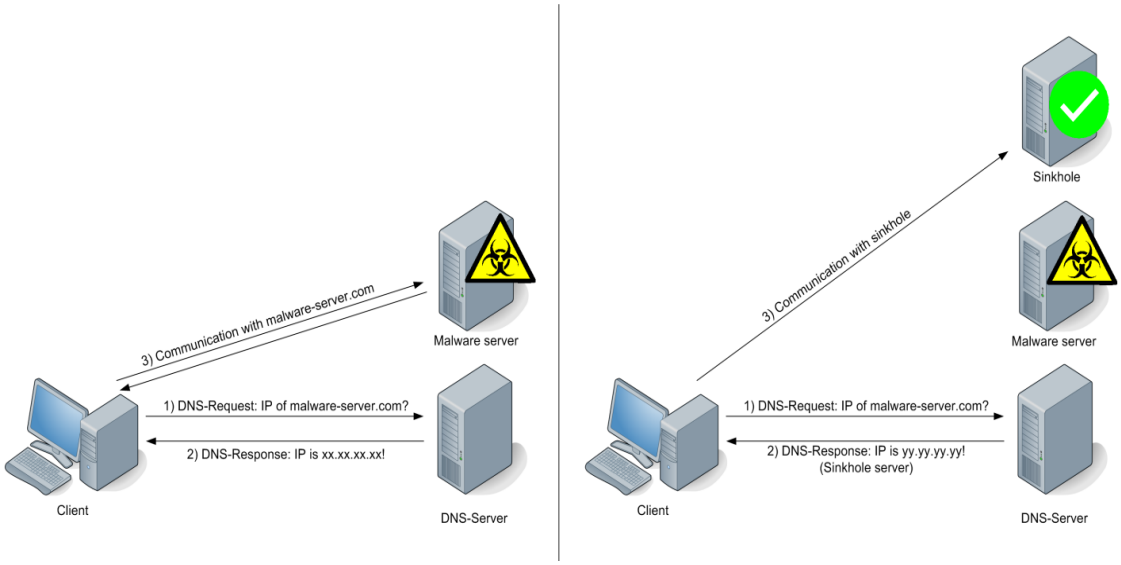
Ο όρος Sinkholing περιγράφει μια τεχνική αντιμέτρησης για την αποκοπή μιας κακόβουλης πηγής από το υπόλοιπο botnet. Μπορεί να εφαρμοστεί ενάντια διαφόρων στόχων, κυρίως κατά των C&C server των botnet ή των tojan dropzones.

Μια από τις πιο διαδεδομένες παραλλαγές αυτής της τεχνικής είναι η αλλαγή του κακόβουλου domain name, έτσι ώστε να δείχνει σε μια μηχανή έμπιστα ελεγχόμενη από ερευνητές. Παρόμοια δράση μπορεί να επέλθει με την αλλαγή της δρομολόγησης μιας στατικής διεύθυνσης IP με όμοιο τρόπο. Και οι δύο προσεγγίσεις, με μικρή πρόσθετη προσπάθεια, επιτρέπουν τη ρύθμιση του πλαισίου ανάλυσης προκειμένου να μετρηθεί το botnet.

Επιπλέον είναι δυνατή η προώθηση σε δευτερεύον προορισμό, αλλά συνήθως δεν είναι επιθυμητή γιατί κρατάει «ζωντανό» το botnet. Αυτό μπορεί να αποδειχθεί χρήσιμο στην περίπτωση που ο botherder αποτυγχάνει να ανιχνεύσει εν εξελίξει διερευνήσεις και ως τμήμα προετοιμασίας μιας ευρύτερης και συντονισμένης εξάρθρωσης πολλών C&C server που χρησιμοποιούνται σε ένα botnet.

Ένα μειονέκτημα αυτής της τεχνικής είναι ότι η ακρίβεια της μέτρησης εξαρτάται σημαντικά από την διαθέσιμη πληροφορία που φιλοξενεί ο στόχος. Αν τα bot που έρχονται σε επαφή με τη sinkhole παρέχουν πληροφορία που μπορεί να οδηγήσει σε μοναδική ταυτοποίηση, η ακρίβεια της μέτρησης θα είναι σχετικά υψηλή. Από την άλλη πλευρά, αν η ποσότητα της αποσπάσιμης πληροφορίας είναι χαμηλή, τότε τα αποτελέσματα των μετρήσεων θα επηρεαστούν από σημαντικές μεταβλητές. Για παράδειγμα, αν τα εισερχόμενα πακέτα είναι πλήρως κρυπτογραφημένα, μόνο η διεύθυνση της IP μπορεί να χρησιμοποιηθεί σαν χαρακτηριστικό ταυτοποίησης.

Η μέτρηση μέσω μοναδικής διεύθυνσης IP συνεπάγεται ποικίλους παράγοντες που μπορεί να επηρεάσουν σημαντικά τα αποτελέσματα, όπως διαφαίνεται και από τα επόμενα παραδείγματα. Αν πολλαπλές προσβεβλημένες μηχανές συνδεθούν με ένα μοναδικό διακομιστή που εμφανίζεται με μία στατική διεύθυνση IP εκτός του τοπικού δικτύου, τότε οι πολλαπλές προσβολές θα μετρηθούν ως μία. Επιπλέον, αν πολλές διευθύνσεις IP είναι δυναμικά κατανεμημένες, αυτό μπορεί να προκαλέσει πολλαπλές μετρήσεις των στατιστικών στοιχείων. Αυτό ισχύει ιδιαίτερα στη περίπτωση της πρόσβασης στο Internet μέσω κινητών τηλεφώνων, όπου διάφορες διευθύνσεις μεταφράζονται μέσω κεντρικών πυλών ή όταν ο πελάτης συνδέεται και αποσυνδέεται συχνά αποκτώντας νέα διεύθυνση IP κάθε φορά.



Σχήμα 11: Sinkholing [Enisa 2011]

Οι χρήστες μιας sinkhole πρέπει να λαμβάνουν υπόψη τους ότι τα εισερχόμενα δεδομένα μπορεί συχνά να περιέχουν σημαντικές ποσότητες ευαίσθητου περιεχομένου. Για παράδειγμα, αν ο server της sinhole λαμβάνει δεδομένα από κακόβουλο λογισμικό με χαρακτηριστικά κλοπής δεδομένων, τότε τα εισερχόμενα πακέτα θα περιέχουν στοιχεία πιστωτικών καρών, τραπεζικών λογαριασμών ή άλλων οικονομικών συναλλαγών.

Παράδειγμα 1: Αυτή η τεχνική μπορεί να εφαρμοστεί εναντίον αποκεντρωμένων botnet που χρησιμοποιούν δυναμικά σημεία επαφής για περιστασιακές αναβαθμίσεις. Ένας τρόπος σχεδιασμού δυναμικών επαφών είναι η παραγωγή ονομάτων χώρου περιορισμένης ισχύος π.χ. για μια μέρα μόνο. Πιθανότατα, η πιο γνωστή περίπτωση όπου η τεχνική αυτή χρησιμοποιείται εντατικά από τον Φεβρουάριο του 2009 είναι αυτή κατά του botnet Conficker. Η αντίστοιχη ομάδα εργασίας συντονίζει τον αποκλεισμό 500 ονομάτων χώρου κάθε μέρα και παγιδεύει κάθε σύνδεση που παραπέμπει σε αυτά μέσω του sinkholing.

Παράδειγμα 2: Μια από τις πιο πρόσφατες χρήσεις του sinkholing για μέτρηση είναι αυτή από την Symantec για την περίπτωση του W32.Stuxnet. Με την παρακολούθηση της κίνησης στους C&C εξυπηρετητές του Stuxnet, μπορούν να συγκεντρωθούν στατιστικά στοιχεία σχετικά με τα ποσοστά προσβολής και τη παγκόσμια διασπορά. Κατά το διάστημα 20 Ιουλίου-29 Σεπτεμβρίου του έτους 2010, περίπου 100.000 υπολογιστές-ξενιστές ταυτοποιήθηκαν μέσω της παρακολούθησης της κίνησης.

Η ταυτοποίηση πραγματοποιήθηκε συνδυάζοντας τα χαρακτηριστικά τους όπως, όνομα υπολογιστή, έκδοση του λειτουργικού συστήματος, των εσωτερικών και εξωτερικών διευθύνσεων IP, τα οποία εξάχθηκαν από τα εισερχόμενα πακέτα κατάστασης. Στο σύνολο πάνω από 40.000 μοναδικές εξωτερικές διευθύνσεις IP παρατηρήθηκαν. Αυτό καταδεικνύει ότι η μέτρηση των bot μόνο μέσω της διεύθυνσης IP μπορεί να οδηγήσει σε σημαντικό βαθμό αβεβαιότητας, τόσο υπο- όσο και υπερεκτιμώντας των αριθμό των bot.

Διήθηση (Infiltration)

Η τεχνική αυτή μπορεί να διακριθεί σε software- και harware-based . Η πρώτη κατηγορία καλύπτει την έρευνα στην εξερχόμενη και παρακολουθούμενη κίνηση του bot προκείμενου να επιτευχθούν μετρήσεις. Η δεύτερη μπορεί να εφαρμοστεί εφόσον είναι δυνατή η πρόσβαση στον C&C εξυπηρετητή και μπορεί να χρησιμοποιηθεί για να υποκλέψει την επικοινωνία. Αυτό περιλαμβάνει φυσικές και εικονικές μηχανές που πιθανόν να τρέχουν σε ένα κέντρο δεδομένων.

Η διήθηση που βασίζεται στο λογισμικό στοχεύει στην κατάκτηση του ελέγχουν του botnet και αποτελεί προέκταση προσεγγίσεων όπως η IRC-based ανίχνευση η απαρίθμηση Peer-to-Peer δικτύων.

Αυτό συνήθως απαιτεί ως σημείο εκκίνηση την αντιστροφή των μηχανισμών επικοινωνίας που χρησιμοποιούνται από το botnet. Μια τέτοια ακριβής ανάλυση μπορεί να οδηγήσει στην ταυτοποίηση πιθανόν αδυναμιών. Επίσης, αυτή η διαδικασία μπορεί να συγκριθεί με ένα κοινό ασφαλείας ή με μια δοκιμή διείσδυσης στο botnet και την υποδομή του. Η γνώση που κερδίζεται με αυτή τη διαδικασία μπορεί να αξιοποιηθεί σε περαιτέρω στάδια προκειμένου να κατακτηθεί μια θέση εντολών μέσα στο botnet. Με αυτό τον τρόπο μπορεί να καθίσταται δυνατή η εκτέλεση μετρήσεων ή αποκάλυψη πληροφοριών σχετικά με τους μολυσμένους ξενιστές ή τον κύριο του bot.

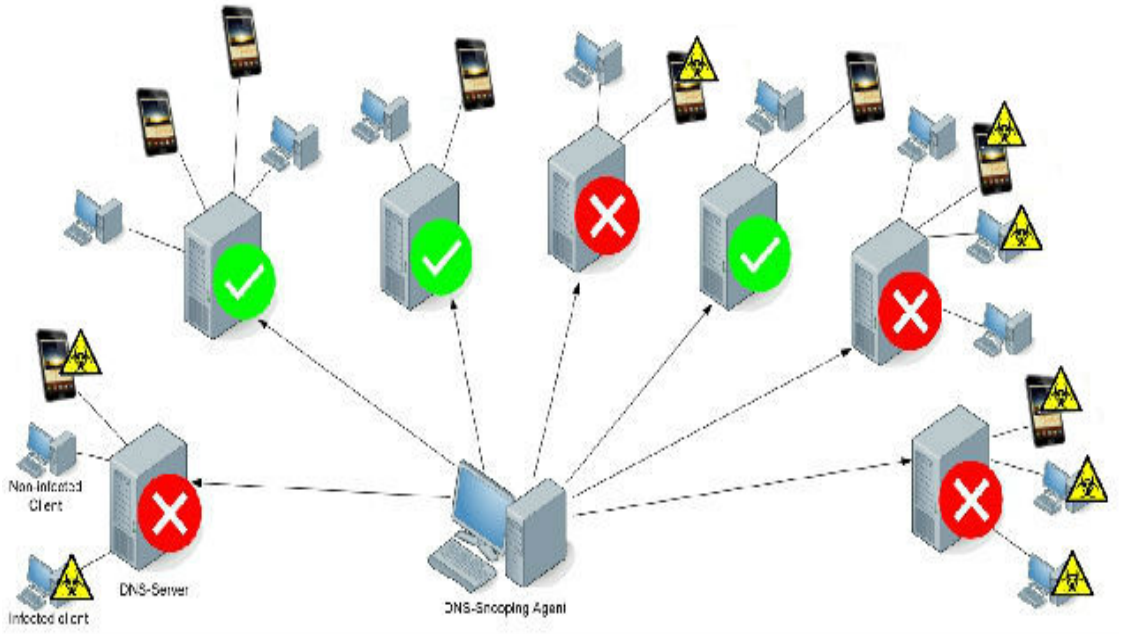
Η άλλη προσέγγιση που βασίζεται στο hardware στην περίπτωση όπου έχει ταυτοποιηθεί μια διεύθυνση IP που ανήκει σε έναν C&C εξυπηρετητή και έχει καθιερωθεί μια σχέση με ένα κέντρο διακίνηση δεδομένων ή μια εταιρεία φιλοξενίας. Αποκτώντας σύνδεση σε μια mirror-port στους ύποπτους εξυπηρετητές, μπορεί να γίνει υποκλοπή της επικοινωνίας και να αναλυθεί. Αυτό επιτρέπει την παρακολούθηση όλης της κίνησης από και προς τον server, το οποίο επίσης επιτρέπει την συγκέντρωση πληροφόρησης σχετικά με τον αριθμό, τη θέση και άλλα χαρακτηριστικά των μολυσμένων ξενιστών.

Οι περιορισμοί αυτής της προσέγγισης είναι συγκρίσιμοι με αυτούς του sinkholing. Για παράδειγμα, η κρυπτογράφηση της κίνησης μπορεί να μειώσει τον αριθμό των χρησιμων χαρακτηριστικών και κατά συνέπεια να επηρεάσει την ακρίβεια των μετρήσεων.

DNS Cache Snooping

Αυτή η τεχνική μέτρησης βασίζεται στην ιδιότητα πολλών DNS server, να χρησιμοποιούν κρυφές μνήμες. Αν ένας εξυπηρετητής ονομάτων χώρου (DNS) ζητά το domain για το οποίο δεν έχει οριστεί είσοδος, θα προκύψει ένα ερώτημα προς τον authoritative name server από μέρους του πελάτη και θα αποθηκευτεί το δεδομένο καταγραφής σε μια τοπική κρυφή μνήμη. Η διαδικασία της κρυφής μνήμης χρησιμοποιείται για να αυξήσει την απόδοση του server και να μειώσει το φορτίο κίνησης.

Επιπλέον η λειτουργικότητα μπορεί να χρησιμοποιηθεί με ένα ακούσιο τρόπο, για λόγους μέτρησης. Η κεντρική ιδέα είναι να ελεγχθεί έμμεσα αν ένας στόχος domain έχει ζητηθεί μέσω ενός συγκεκριμένου domain server δοκιμάζοντας αν μια απάντηση κρυφής μνήμης έχει αποθηκευτεί όπως φαίνεται στο σχήμα (12) που ακολουθεί.



Σχήμα 12: DNS cache snooping.

Για το σκοπό αυτό μπορούν να χρησιμοποιηθούν δύο εκδοχές, η επιλογή των οποίων εξαρτάται από την σύνθεση του DNS server.

Στην πρώτη εκδοχή, ένα αίτημα στέλνεται στον DNS server με ειδική μεταβλητή (ρύθμιση: no-recursion-flag) η οποία δεν θα επιτρέπει την προώθηση του αιτήματος στον authoritative name server. Η συμπεριφορά του server θα διαφοροποιηθεί αναλόγως αν ο αιτούμενος διακομιστής έχει αποθηκεύσει μια κρυφής μνήμης απάντηση για το στόχο όνομα ή όχι. Είτε θα στείλει μια άμεση απάντηση στο αίτημα, που θα περιλαμβάνει σχετικές διευθύνσεις IP, είτε αν ο DNS server δεν μπορεί να απαντήσει, θα στείλει μια απάντηση που θα περιέχει authoritative server για περαιτέρω επικοινωνία. Αυτή η μέθοδος δεν μπορεί να λειτουργήσει σε όλους του DNS server, αφού πολλοί απορρίπτουν αιτήματα όπως αυτά προκειμένου να προστατευθούν απέναντι στις επιθέσεις άρνησης υπηρεσιών.

Η δεύτερη εκδοχή μπορεί να λειτουργήσει με κάθε είδους DNS server, αλλά μολύνει την κρυφή μνήμη του στοχευόμενου server. Σε αυτή την περίπτωση η μεταβλητή που προαναφέρθηκε δεν ρυθμίζεται και επιτρέπεται στον server να στείλει το αίτημα σε άλλους name server. Κατ' αυτόν τον τρόπο καθίσταται δυνατό να προσδιοριστεί αν ένα αίτημα έχει ήδη αποθηκευθεί προσωρινά ή όχι αναλύοντας το πότε το συγκεκριμένο domain name ζητήθηκε για τελευταία φορά. Αυτό επιτυγχάνεται αξιολογώντας τη τιμή Time-to-Live (TTL) που περιλαμβάνεται στην απόκριση. Σαν αυτή η τιμή είναι η προεπιλεγμένη του server τότε καμιά πληροφορία δεν έχει κρυφά αποθηκευθεί πριν το ερώτημα. Αν είναι μικρότερη από την προκαθορισμένη τιμή, θα σημαίνει ότι το domain έχει ήδη ζητηθεί πριν. Αυτή η τεχνική είναι εφαρμόσιμη διότι ο server δεν ανανεώνει την τιμή TTL για ένα cached domain name όταν ζητείται. Ένα μειονέκτημα αυτής της εκδοχής είναι ότι το ερώτημα του αναλυτή θα αφήσει μια είσοδο κρυφής μνήμης, η οποία θα αποκλείσει το ενδεχόμενο να χρησιμοποιηθεί η τεχνική αυτή ξανά στον server για τη διάρκεια caching του server.

Η τεχνική αυτή χαρακτηρίζεται από καλή κλιμάκωση, αφού DNS-server-στόχοι συνήθως δεν είναι αλληλοσχετιζόμενοι, γεγονός που επιτρέπει πλήρως την παράλληλη εκτέλεση της διαδικασίας. Περιορισμοί προκύπτουν μόνο αναφορικά με τον αριθμό των domain που

υπόκεινται στη διαδικασία εντοπισμού. Πολλοί DNS-server δέχονται περιορισμένο αριθμό αιτημάτων που εκτελούν για μία συγκεκριμένη διεύθυνση IP πελάτη. Αυτό σημαίνει ότι η διαδικασία θα πρέπει να είναι τμηματική και πιθανόν να υπάρχει καθυστέρηση στα αποτελέσματα.

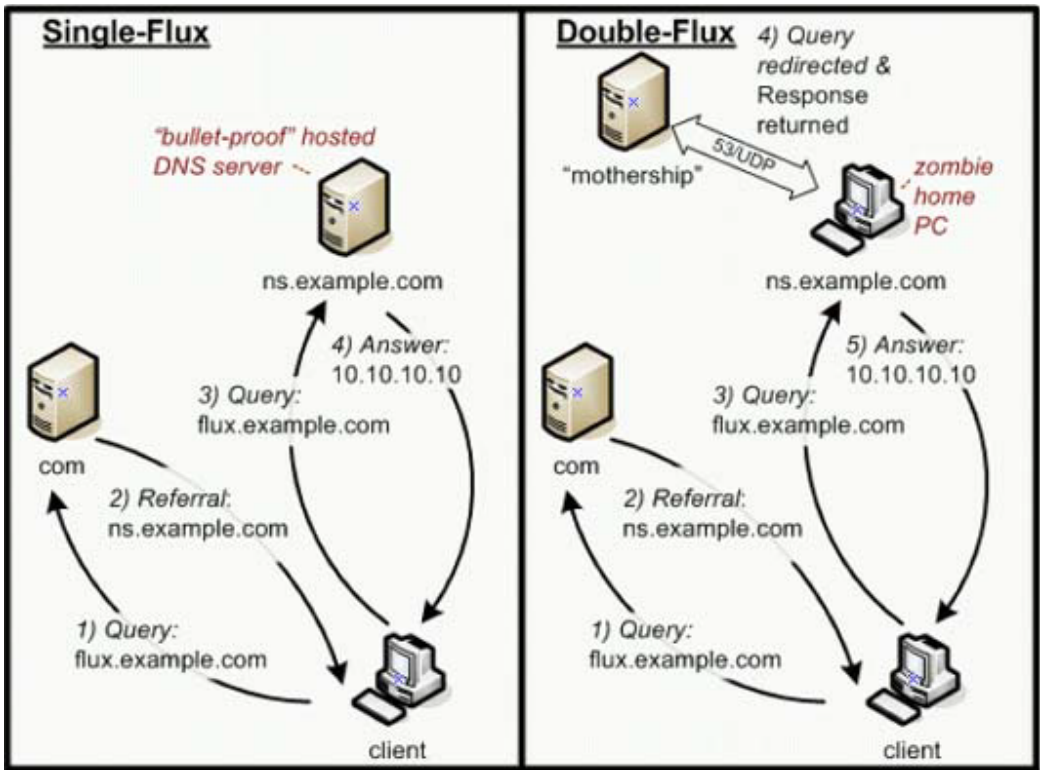
Η αξία της πληροφόρησης εφαρμόζοντας αυτή την τεχνική βασίζεται στο πλήθος των serve που εμπλέκονται, και συνεπώς είναι επιθυμητή μια μεγάλη λίστα αυτών.

Σε ότι αφορά την ακρίβεια αυτής της προσέγγισης, είναι εμφανές ότι δεν είναι κατάλληλη για τον υπολογισμό του πραγματικού μεγέθους ενός Botnet. Όμως, είναι χρήσιμο για την αξιοποίηση τη φυσική συμμετοχή του internet μέσω της σχέσης των host από τις διευθύνσεις IP και τους DNS server που συνήθως είναι υπεύθυνοι.

Παράδειγμα: Οι Rajeb et al υλοποίησαν μια εκτενή ανάλυση πάνω στην τεχνική του cache snooping. Δημιούργησαν αρχικά ένα μοντέλο κανονικής συμπεριφοράς διακομιστών domain names στην απάντηση αιτημάτων από αυθαίρετους host προκειμένου να υπολογίζουν cache hits. Με αυτόν τον τρόπο μπορούσαν να εκτιμήσουν την παρουσία εισερχόμενων ονομάτων κρυφά αποθηκευμένων από επαναλαμβανόμενα αιτήματα προς τους DNS server και να μετρήσουν τους χρόνους άφιξης των αιτημάτων. Αξιολόγησαν το συγκεκριμένο μοντέλο σε περιβάλλον γραφείου, όπου τα δεδομένα ήταν διαθέσιμα τόσο από τους DNS server όσο και από το cache snooping. Για τα πειράματα που ακολούθησαν χρησιμοποίησαν μια λίστα από 758.000 συνεργαζόμενους αναλυτές DNS προκειμένου να παρακολουθήσουν τα cached domain names που σχετίζονταν με τα botnet και πραγματοποίησαν διασταυρούμενη επαλήθευση με IRC-logs προκειμένου να υπολογίσουν το πραγματικό μέγεθος του botnet.

Εντοπισμός fast-flux δικτύων (TRACKING OF FAST-FLUX NETWORKS)

Η πιο δημοφιλής τεχνική για ένα botmaster να ‘συλλέξει’ υπονομευμένους υπολογιστές (bot) σε ένα botnet περιλαμβάνει το ‘Σύστημα Ονομάτων Τομέα’ γνωστό ως Domain Name System (DNS).



Σχήμα 13: Σύγκριση τεχνικών Fast-flux (**http://www.honeynet.org)**

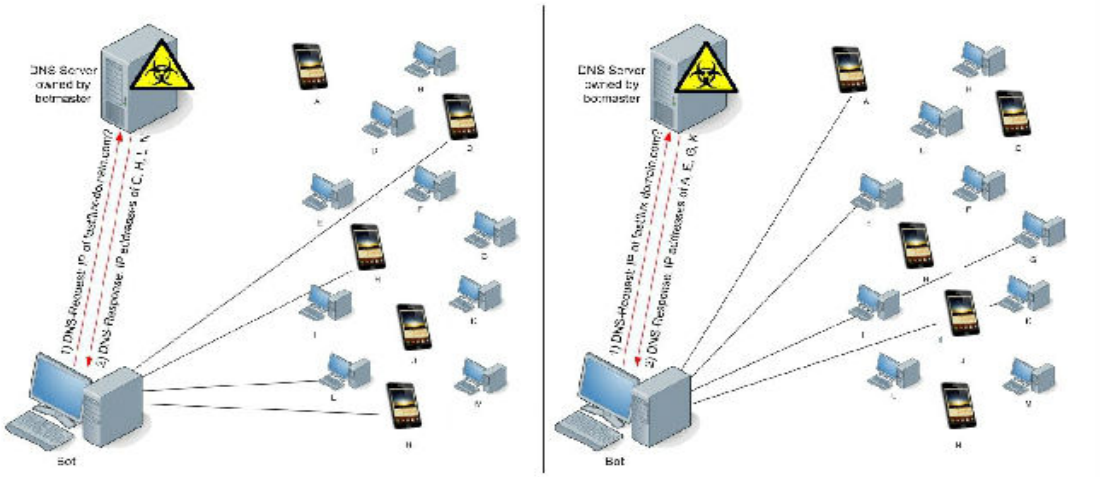
Οι νέες γενιές botnet όμως πηγαίνουν ένα βήμα ακόμη πιο πέρα χρησιμοποιώντας μια νέα τεχνική που ονομάζεται Fast-flux DNS. Πρόκειται για μια τεχνική που σκοπό έχει την απόκρυψη των ιστοχώρων που παραδίδουν περιεχόμενο ηλεκτρονικού ψαρέματος (phishing) και γενικότερα κακόβουλο περιεχόμενο, χρησιμοποιώντας διαρκώς μεταβαλλόμενα δίκτυα υπονομευμένων υπολογιστών που λειτουργούν ως πληρεξούσιοι (proxies). Αυτή η τεχνική κάνει τα κακόβουλα δίκτυα περισσότερο ανθεκτικά στη ανακάλυψή τους και στα αντίμετρα εναντίον τους.

Στα botnet επιπλέον αυτή η τεχνική χρησιμοποιείται για να συνδέσει και να αποκρύψει τους C&C εξυπηρετητές όπως στο κανονικό DNS. Η μεγάλη διαφορά όμως είναι ότι τα ονόματα τομέων (DNS domains) που χρησιμοποιούν τα bot είναι κλεμμένα, υπονομευμένα ή καταχωρημένα (registered) με συνήθως κλεμμένες πιστωτικές κάρτες.

Ο πιο απλός τύπος fast-flux DNS που αναφέρεται ως Single-flux χαρακτηρίζεται από πολλαπλούς μεμονωμένους κόμβους, στην περίπτωση μας τα bot, οι οποίοι εγγράφουν και διαγράφουν τις διευθύνσεις τους σαν μέρος μιας λίστας εγγραφών A (DNS A records) για ένα μοναδικό όνομα τομέα (DNS name). Αυτό συνδυάζει το DNS εκ περιτροπής ανάμεσα στους κόμβους με πολύ μικρές τιμές (συνήθως λιγότερο από 5 λεπτά ή 300 δεύτερα) για χρόνο ζωής (Time To Live) κάθε κόμβου, έχοντας ως αποτέλεσμα τη συνεχή αλλαγή της λίστας των διευθύνσεων προορισμού για ένα μοναδικό όνομα τομέα. Η λίστα μπορεί να έχει μήκος εκατοντάδων χιλιάδων καταχωρήσεων και κάθε πελάτης (bot) θα δοκιμάσει τις διευθύνσεις IP της λίστας μέχρις ότου συνδεθεί σε κάποια.

Ένας πιο προχωρημένος τύπος fast-flux που ονομάζεται Double-flux χαρακτηρίζεται από πολλαπλούς μεμονωμένους κόμβους, στην περίπτωση μας τα bot, οι οποίοι εγγράφουν και διαγράφουν τις διευθύνσεις τους σαν μέρος μιας λίστας εγγραφών NS (DNS NS records) για τη ζώνη DNS. Δημιουργούνται δηλαδή πολλαπλοί εξυπηρετητές ονομάτων (name servers) για μια ζώνη DNS, παρέχοντας ένα επιπρόσθετο επίπεδο πλεονασμού και βιωσιμότητας των bot μέσα στο κακόβουλο δίκτυο.

Ωστόσο, ακριβώς αυτές οι ιδιαίτερες ιδιότητες των DNS εγγραφών που εξυπηρετούν τέτοιου είδους δίκτυα επιτρέπουν τη διάκριση τους. Οι εγγραφές αυτές που συνδέονται με fast-flux networks έχουν τυπικά περιορισμένη περίοδο ισχύος μερικών λεπτών. Αυτό φαίνεται από την τιμή TTL περιλαμβανομένης της απόκρισης που παράγεται από τον αρχικό DNS server στο τέλος της αλυσίδας των DNS ερωτημάτων, που είναι υπό τον έλεγχο του botmaster. Ένας κακόβουλος DNS server λειτουργείται συνήθως απευθείας από τον botmaster ή είναι εγκατεστημένος ως υπηρεσία σε έναν υπονομευμένο server.



Σχήμα 14: Εντοπισμός fast-flux δικτύων

Μετά από μικρό χρονικό διάστημα μια νέα ερώτηση θα έχει συνήθως ως αποτέλεσμα μια διαφορετική ρύθμιση σχετικών διευθύνσεων IP με μικρή έως καθόλου ομοιότητα ή τοπολογική σχέση. Επιπροσθέτως, ένα ιδιαίτερο γνώρισμα που μπορεί να παρατηρηθεί είναι ποικιλία των διευθύνσεων IP που επιστρέφουν για ένα fast-flux domain. Αυτές συνήθως ξεκινάνε από διάφορα δίκτυα και ISP. Νόμιμες υπηρεσίες με χαμηλό TTL, όπως για παράδειγμα δικτυακοί τόποι σαν το google.com ή σαν το facebook.com συνήθως επιστρέφουν διευθύνσεις IP που έχουν πολύ μεγάλη ομοιότητα, γεγονός που υποδεικνύει ότι έχουν ως αφετηρία το ίδιο δίκτυο και ότι σχετίζονται μεταξύ τους.

Η παρακολούθηση τομέων των οποίων οι αποκρίσεις DNS χαρακτηρίζονται από χαμηλή τιμή TTL δεν επιτρέπει μόνο την ταυτοποίηση αυτών των fast-flux τομέων, αλλά μπορούν να συγκεντρωθούν οι host που συμμετέχουν στο δίκτυο από τις εγγραφές επαναλαμβανόμενων DNS queries.

Παράδειγμα: Οι Nazario και Holz παρουσίασαν τα αποτελέσματα της παρακολούθησης fast-flux botnet. Χρησιμοποίησαν το ATLAS, μόνιτορ άρνησης υπηρεσιών και άλλου είδους συλλέκτες δεδομένων. Το σύστημα χρησιμοποιεί διάφορες πηγές δυνατών fast-flux domains όπως URL εξαγόμενα από spam mail και μαύρες λίστες τομέων καθώς και ονόματα τομέων από δείγματα κακόβουλου υλικού που έχουν αυτόματα ή χειροκίνητα αναλυθεί. Αυτοί οι υποψήφιοι τομείς στη συνέχεια ταξινομούνται (με βάση χαρακτηριστικά όπως ο χρόνος ζωής, ο αριθμός και η απόσταση των διευθύνσεων IP που απαντούν κ.λπ.). Τα δεδομένα που συγκεντρώθηκαν κατά την μελέτη αυτή στο διάστημα Ιανουάριος-Μάιος 2008, αφορούσαν 928 διαφορετικούς τομείς τεχνολογίας fast-flux με ένα σύνολο περισσοτέρων των 15 εκατομμυρίων σχετικών διευθύνσεων IP οι οποίες ταυτοποιήθηκαν. Με βάση τον χρόνο ζωής, οι Nazrio και Holz βρήκαν ότι περισσότερο από το 33% των τομέων ήταν ενεργοί για λιγότερο από μια εβδομάδα, με αιχμή μιας ημέρας ή και λιγότερου χρόνου. Ωστόσο, ο μέσος χρόνος χρήση των fats-flux τομέων που παρατηρήθηκαν ήταν 18,5 ημέρες. Ένα άλλο εύρημα ήταν το γεγονός ότι οι τομείς που εντοπίστηκαν στο 80% των περιπτώσεων ήταν ενεργοποιημένοι για περισσότεροι από ένα μήνα μετά την εγγραφή. Σε ότι αφορά τη μετρήσεις του botnet, το ATLAS χρησιμοποιήθηκε για να εντοπίσει μεταξύ άλλων το Storm botnet, το οποίο χρησιμοποιεί τη fast-flux τεχνολογία.

Ανίχνευση και μέτρηση βασισμένη στο IRC (IRC based measurement and detection)

Το IRC εξυπηρετεί ως μια κοινή υποδομή C&C για την δημιουργία botnet. Το IRC αποτελεί (μαζί με το HTTP) ένα από το πιο πιθανό κανάλι επικοινωνίας του botmaster με τα bot Αξίζει να σημειωθεί ότι εκτιμάται πως τα IRC botnet[1] θα επιβιώσουν για αρκετό χρόνο ακόμη, σε αντίθεση με την τάση για μεταφορά της αρχιτεκτονικής του C&C σε άλλα πρωτόκολλα όπως το HTTP και το P2P. Επιπλέον είναι χαρακτηριστικό ότι σύμφωνα με την ετήσια έκθεση της Symantec του 2010, το 31% των εντοπισμένων C&C server χρησιμοποιούν το IRC ως πρωτόκολλο επικοινωνίας.

Το πρωτόκολλο IRC αποτελεί το κυρίαρχο πρωτόκολλο για την επικοινωνία στα botnet λόγω της απλότητας και ωριμότητάς του και προσφέρεται ως προς την λειτουργική καταλληλότητα του για τον έλεγχο μεγάλων botnet. Μια αρχιτεκτονική εντολής και ελέγχου βασισμένη στο IRC συνεπάγεται την χρήση ενός ή περισσοτέρων καναλιών, διακομιστών δημόσιων IRC δικτύων ή πελατών, όπου τα bot αναφέρουν την παρουσία τους και δέχονται εντολές.

[1] Το 'Agobot' συχνά γνωστό και ως 'Gaobot' είναι μια οικογένεια botnet με χαρακτηριστικά «σκουληκιών» (worms) στους υπολογιστές. Ο πηγαίος κώδικάς του το περιγράφει σαν ένα αρθρωτό IRC bot για συστήματα Win32 και Linux. Είναι πολυνηματικό (multi-threaded) και το object-oriented πρόγραμμά του είναι γραμμένο κυρίως σε C++ και λιγότερο σε Assembly [Σιδηρόπουλος Α. 2009].

Προκειμένου να μετρηθούν τα bot που χρησιμοποιούν ένα μοντέλο επικοινωνίας βασισμένο στο IRC χρειάζεται αρχικά να αποκτηθεί η κατάλληλη πληροφορία έτσι ώστε να είναι δυνατή η συμμετοχή στο κανάλι του botnet. Βασική πληροφορία σύνδεσης η οποία περιλαμβάνει την διεύθυνση IP και τον αριθμό θύρας του IRC server καθώς και το κανάλι που χρησιμοποιείται για τον έλεγχο του botnet, μπορεί να εξαχθεί από δείγματα κακόβουλου υλικού του εν λόγω botnet.

Δεύτερο βήμα είναι η σύνδεση στο κανάλι και η συλλογή δεδομένων. Η ποιότητα και η ποσότητα της πληροφορίας που μπορεί να αποκτηθεί εξαρτάται σημαντικά από τα μέτρα που έχει λάβει ο botherder. Αν το κανάλι ελέγχου φιλοξενείται σε κάποιο δημόσιο IRC server, μπορεί να είναι πιθανή μια απλή εγγραφή και εντοπισμός Usernames στο κανάλι χωρίς ιδιαίτερη προσπάθεια. Τα μηνύματα κατάστασης δίνουν πρόσθετη πληροφορία σχετικά με τη διακύμανση εντός του botnet.

Στην περίπτωση που ο IRC server φιλοξενείται στον ίδιο τον botherder, τροποποιημένες εφαρμογές έχουν παρατηρηθεί αναλόγως των αναγκών του botnet. Για παράδειγμα μπορεί να αρκεί ένα μειωμένο σύνολο εντολών που να δίνουν εντολές στα bot. Συχνά, οι κλασικές εντολές που περιλαμβάνονται σε ένα κανονικό πρωτόκολλο IRC chat αφαιρούνται, και το δημόσιο chat απενεργοποιείται. Η επικοινωνία μεταξύ botherder και bot πραγματοποιείται με ιδιωτικά μηνύματα ώστε η παρουσία μεταξύ bot να μην είναι εμφανής. Επίσης το πρωτόκολλο μπορεί να χρησιμοποιεί κρυπτογράφηση. Αυτό περιορίζει σημαντικά τη ποσότητα της πληροφορίας που μπορεί να συγκεντρωθεί μέσω του καναλιού C&C.

Καταμέτρηση δικτύων ομότιμων κόμβων (Enumeration of Peer-to-Peer networks)

Το κανάλι ‘Command and Control’ μπορεί να είναι ένα σύνολο κόμβων σε ένα δίκτυο δομής ομότιμων υπολογιστών peer-to-peer (P2P). Η τοπολογία P2P ανήκει στην κατηγορία των κατανεμημένων (distributed) τοπολογιών. Η P2P επικοινωνία είναι δυσκολότερο να ανιχνευτεί γιατί οι κόμβοι δεν συνδέονται σε κάποιο κεντρικό και μπορούν να δρουν και ως πελάτες (bot) και ως εξυπηρετητές (C&C server). Ο εντοπισμός και η αποσύνδεση κάποιων bot δεν έχει ιδιαίτερη επίδραση στα εναπομείναντα bot και έτσι η απενεργοποίηση του botnet γίνεται πιο δύσκολη, αφού οι C&C server μπορεί να λειτουργούν σε οποιοδήποτε bot.

Αυτό που χρειάζεται στο κατανεμημένο C&C είναι το κάθε bot κατά την αρχική διαδικασία της σύνδεσή του (bootstrapping) στο κακόβουλο δίκτυο, να γνωρίζει κάποια άλλα συνδεδεμένα bot. Τα ήδη συνδεδεμένα bot θα δώσουν τις πληροφορίες που χρειάζονται στο νέο bot κάνοντας το έτσι μέλος του botnet [Schoof R. & Koning R]. Οι πληροφορίες αυτές μπορεί να βρίσκονται σε κάποιο κρυπτογραφημένο αρχείο και να είναι δεδομένα (π.χ. λίστες spam) και εντολές που το νέο bot θα πρέπει να εκτελέσει.

Χαρακτηριστικά παραδείγματα Botnet που χρησιμοποιούν μηχανισμού ομότιμων κόμβων είναι τα Storm, Waledac και Conficker.

2.2 Ανάλυση και αξιολόγηση

Έχοντας παρουσιάσει τις διάφορες προσεγγίσεις ανίχνευσης και μέτρησης, σε αυτή την ενότητα επιχειρείται η σύγκριση των βασικών χαρακτηριστικών τους και πλεονεκτημάτων αυτών. Στόχος είναι η ανάδειξη των δυνατών αλλά και αδύναμων σημείων τους.

Αρχικά θα πρέπει να αναφερθεί ότι το μέγεθος δεν είναι ο μόνος δείκτης που καθορίζει τη πιθανή βλάβη που μπορεί να προκαλέσει ένα botnet. Οι δυνατότητες, η ευρωστία και η

ευελιξία είναι εξίσου κρίσιμης σημασίας. Ακόμη και ένα μικρό botnet μπορεί να προκαλέσει σοβαρές ζημιές, αναλόγως των μεμονωμένων μηχανών που παραβιάζει.

Περαιτέρω μετρήσεις για την εκτίμηση της απειλής ενός botnet περιλαμβάνουν, για παράδειγμα, την ποσότητα και την ποιότητα των spam e-mail, τη χρήση του εύρους ζώνης κατά τη διάρκεια των επιθέσεων DDoS, ή την επιθετικότητα με την οποία υποκλέπτει ευαίσθητα δεδομένα που προέρχονται από τον υπολογιστή του θύματος. Όσον αφορά το ίδιο το botnet, η ευρωστία της υποδομής εντολής και ελέγχου, η ανθεκτικότητα που επιδεικνύει έναντι στα αντίμετρα και οι ικανότητες υποκλοπής του κακόβουλου λογισμικού, αποτελούν επίσης σημαντικούς παράγοντες που συμβάλλουν στον καθορισμό του επιπέδου απειλής ενός botnet. Επιθετικά χαρακτηριστικά, όπως για παράδειγμα οι μηχανισμοί διάδοσης και ο τρόπος χρήσης των στοιχείων που υποκλέπτονται, παίζουν επίσης σημαντικό ρόλο σε αυτές τις εκτιμήσεις.

Επιπλέον, ανεξαρτήτως από το ποια μέθοδος θα εφαρμοστεί για τη μέτρηση, είναι σημαντικό να περιγραφεί κάθε λεπτομέρεια της μετρητικής διαδικασίας έτσι ώστε να μπορεί να υποστηριχθεί και αιτιολογηθεί η σημασία των αποτελεσμάτων που θα προκύψουν.

Όσον αφορά τα γενικά χαρακτηριστικά της μεθοδολογικής προσέγγισης που θα εφαρμοστεί για την ανίχνευση και τη μέτρηση, μεγάλης σημασίας είναι η ευελιξία της να προσαρμόζεται στις αλλαγές, και η γενικότητα ως προς τα είδη των botnet που μπορεί να καλύψει.

Οι παθητικές τεχνικές όπως τα honeypot, ο έλεγχος πακέτων δεδομένων και η ανάλυση ροών διακρίνονται από καλή ευελιξία. Εξειδικευμένες προσεγγίσεις που στοχεύουν στα DNS, IRC ή P2P συχνά παρέχουν καλύτερα αποτελέσματα από ό,τι γενικευμένες προσεγγίσεις, αλλά εμφανίζουν έλλειψη ευελιξίας.

Οι μέθοδοι που βασίζονται στα spam καθώς και η αξιολόγηση εφαρμογής των log files χαρακτηρίζονται από περιορισμένη γενικότητα εφαρμογής δεδομένου ότι βασίζονται σε δράσεις που προκαλούνται από τα botnet.

Η ανατροφοδότηση των Anti-virus, και τα δίκτυα αισθητήρων εξαρτώνται από το ίδιο το προϊόν, καθώς και από τη πελατειακή βάση ή πιο συγκεκριμένα, από το πώς θα διανεμηθεί και σε ποιους τομείς (κυβέρνηση, επιχειρήσεις, τελικούς χρήστες, κλπ), το λογισμικό που έχει αναπτυχθεί.

Επίσης αξίζει να αναφερθεί ότι οι περισσότερες παθητικές τεχνικές ανίχνευσης και μέτρησης είναι αόρατες στους botmaster. Αντιθέτως οι ενεργητικές τεχνικές εμφανίζουν διαφορετικό βαθμό ορατότητας καθώς αλληλεπιδρούν με το botnet.

Σε ότι αφορά την ποιότητα των αποτελεσμάτων σημειώνονται τα εξής:

- Οι μεθοδολογίες μετρήσεις πρέπει να τεκμηριώνονται με διαφάνεια και τα αποτελέσματα πρέπει να αξιολογούνται σε σταθερή επιστημονική βάση.
- Η Reverse Engineering είναι μια πλεονεκτική προσέγγιση για την εκτίμηση της δυναμικής που έχει ένα κακόβουλο λογισμικό στην πρόκληση βλαβών.
- Η διαδικασία του sinkholing της κίνησης ενός botnet παρέχει πλήρη άποψη ως προς τον ζωντανό πληθυσμό του.
- Η παρατήρηση μόνο των μοναδικών διευθύνσεων IP αποτελεί δείκτη με μεγάλη έλλειψη ακριβείας για την εκτίμηση του μεγέθους του botnet.
- Οι ενεργητικές προσεγγίσεις απαρίθμησης μπορούν να αποτελούν προσεγγίσεις αποδεκτής ακρίβειας για την εκτίμηση του ζωντανού πληθυσμού ενός botnet.

- Οι παθητικές προσεγγίσεις ανίχνευσης μπορούν να λειτουργούν και ως συνδυασμένοι αισθητήρες σε ένα σύστημα έγκαιρης προειδοποίησης.

Σχετικά με την δυσκολία εφαρμογής και τους απαραίτητους πόρους μπορεί να αναφερθεί συνοπτικά ότι:

- Οι κεντρικοποιημένες τεχνικές ανίχνευσης στοχεύοντας στη γενικότητα συχνά αντιμετωπίζουν προκλήσεις σε ότι αφορά την επεκτασιμότητα.
- Ο εντοπισμός της κίνησης ενός botnet ανάμεσα σε άλλες κανονικές κινήσεις είναι σαν να προσπαθεί κανείς να εντοπίσεις ένα στοιχείο μικροσκοπικού χαρακτήρα με μακροσκοπική μέθοδο.

Τέλος σε ότι αφορά τους περιορισμούς κατά την προσπάθεια εντοπισμού και μέτρησης ενός botnet, οι περισσότεροι από αυτούς αφορούν νομικής φύσης θέματα. Σε γενικές γραμμές όλες οι τεχνικές πρέπει να αντιμετωπίζουν ζητήματα διαχείρισης προσωπικών δεδομένων και ιδιωτικότητας καθώς και την αντίστοιχη νομοθεσία. Χαρακτηριστικά αναφέρεται ότι σε κάποιες ευρωπαϊκές χώρες όπως η Ελβετία, οι διευθύνσεις IP θεωρούνται προσωπικά δεδομένα. Η ευρωπαϊκή οδηγία 2002/58/EC καλύπτει θέματα που αφορούν διαδικασίες προσωπικών δεδομένων, ενώ η οδηγία 2006/24/ΕΚ, στοχεύει στη φύλαξη δεδομένων σύνδεσης, προκειμένου να καταπολεμηθεί το οργανωμένο έγκλημα. Μια άλλη πτυχή που αφορά τα νομικά θέματα και σχετίζεται με την αντίστροφη μηχανική είναι ότι κάποιες εκδόσεις κακόβουλου λογισμικού περιέχουν συμφωνίες άδειας εκμετάλλευσης, οπότε τυπικά απαγορεύουν την αποσυναρμολόγηση ή ανάλυση ενός bot.

Εν κατακλείδι, θα πρέπει να σημειωθεί ότι η μέτρηση των botnet είναι μια διαδικασία πολύ περίπλοκη και επηρεάζεται από πολλούς διαφορετικούς παράγοντες. Λίγες μόνο από τις τρέχουσες μεθόδους, ή εκείνες που βασίζονται στις ειδικές ιδιότητες ορισμένων botnet, προσφέρουν αποδεκτά επίπεδα ακρίβειας σχετικά με το πραγματικό μέγεθος των botnet. Λόγω αυτών των ευρημάτων, προτείνεται ότι η απειλή των botnet θα πρέπει να εκτιμάται σε ένα ευρύτερο πλαίσιο, για παράδειγμα, συμπεριλαμβανομένης της σοβαρότητας της βλάβης, τη δυνητική και την πραγματική, και όχι μόνο λαμβάνοντας υπόψη το μέγεθός τους σχετικά με τον αριθμό των host που έχουν παραβιαστεί.

3 ΑΝΤΙΜΕΤΩΠΙΣΗ

Σε αυτό το κεφάλαιο παρουσιάζονται τα αντίμετρα που μπορούν να λαμβάνονται έναντι των απειλών των botnet. Τα μέτρα αυτά διαχωρίζονται σε τρεις κατηγορίες, στις τεχνικές μεθόδους στις νομοθετικές ρυθμίσεις και στις κοινωνικού χαρακτήρα προσεγγίσεις.

3.1 Τεχνικά αντίμετρα

Τα αντίμετρα που περιγράφονται στην ενότητα αυτή εφαρμόζονται σε τεχνικό επίπεδο. Τα περισσότερα από αυτά εστιάζουν στη δομή C&C του botnet, και αφορούν για παράδειγμα το φιλτράρισμα της κίνησης που σχετίζεται με το botnet, το sinkholing των τομέων με τη βοήθεια των καταχωρητών DNS ή επιτυγχάνοντας τον τερματισμό των κακόβουλων server στα data center.

Ωστόσο, τέτοιου είδους τεχνικές δεν πετυχαίνουν τη από-μόλυνση των μηχανών που έχουν υπονομευτεί και συμμετέχουν στο botnet.

Blacklisting

Η διαδικασία της καταχώρηση σε «μαύρη λίστα» δεν αποτελεί ένα άμεσο και αυτοτελές αντίμετρο για την αντιμετώπιση των botnet, αλλά μια υποστηρικτική διαδικασίας από την οποία προκύπτουν τα κατάλληλα δεδομένα που θα εισέλθουν σε άλλα τεχνικά μέσα. Τα περιεχόμενα μιας τέτοιας λίστας έχουν πολυδιάστατη αξία και μπορούν να χρησιμοποιηθούν σε διαφορετικούς τομείς. Για παράδειγμα μια «μαύρη λίστα» μπορεί να παρέχει μοναδικές διευθύνσεις IP κακόβουλων host ή ολόκληρα υποδίκτυα που εμφανίζουν ύποπτη δραστηριότητα.

Ομάδες που χρησιμοποιούν blacklist είναι οι παροχείς email, ISP, CERT και εταιρείς λογισμικού προστασίας(anti-virus).

Παράδειγμα: Το abuse.ch (The Swiss Security Blog) διατηρεί μια υπηρεσία παρακολούθησης που στοχεύει στους διακομιστές C&C αμφότερων των Zeus (Zbot) και SpyEye Trojan. Το σύστημά τους είναι βασισμένο στην αυτοματοποιημένη ανάλυση των δυαδικών ακολουθιών του Zeus, τα οποία παρέχονται από anti-virus εταιρείες, συμβάλλοντας στην επίτευξη χαμηλού ποσοστού ψευδο-θετικών αποτελεσμάτων. Οι λίστες Zeus Tracker ταυτοποιούν όλες τους κακόβουλους host σε μια κεντρική μαύρη λίστα που επίσης διανέμεται σε πραγματικό χρόνο.

Διανομή ψευδών/ανιχνεύσιμων διαπιστευτηρίων (Distribution of fake/traceable credentials)

Η διανομή των παραποιημένων διαπιστευτηρίων δεν είναι μόνο ένα καθαρά τεχνικό αντιμέτρο, αλλά στοχεύει και στη κερδοφορία του επιτιθέμενου botnet στο υποκείμενο επιχειρηματικό μοντέλο.

Μια συνήθισμενη λειτουργεία botnet είναι η κλοπή ταυτότητας. Κέρδη αποσπώνται από τη κλοπή διαπιστευτηρίων ή στοιχείων πιστωτικών καρτών. Με την παρακολούθηση ενός botnet, την ανάλυση της λειτουργικότητας των bot και προσδιορίζοντας τις ιστοσελίδες στόχους όπου κλεμμένα στοιχεία υποβάλλονται, οι λεγόμενες ζώνες ρίψης, μια προσέγγιση της μέτρησης της συμπεριφοράς είναι η υποβολή ψευδών, στοχοθετημένων πληροφοριών στις ζώνες ρίψης.

Επιπλέον, αυτά τα καθορισμένα με βάση τον πελάτη διαπιστευτήρια μπορούν να χρησιμοποιηθούν για την παρακολούθηση εμπλεκόμενων μερών, καθώς και πού και πότε χρησιμοποιούνται. Αν και αυτή η διαδικασία απαιτεί πολλή προσπάθεια από το σύνολο

των ομάδων των ενδιαφερομένων μερών, μπορεί να συμβάλει στην ενίσχυση της συνεργασίας.

Παράδειγμα: ∉⌈ Ormerod et al. παρουσίασαν μια bottom-up προσέγγιση για τον μετριασμό των botnet, η οποία στην προοπτική της κερδοφορίας τόσο αυτών που ανέπτυξαν τα πακέτα εργαλειών, όπως των Zeys και SpyEye, όσο και των αντιστοίχων πελατών τους, των botherder. Υπέθεσαν ότι μια επίδραση τύπου cascading μπορεί να καθιερωθεί μεταξύ των εμπλεκομένων μερών, αν εισαχθεί “chaff” σε ένα botnet. Αυτό θα μπορούσε να είναι τεράστια ποσά τυχαίων δεδομένων, με σκοπό να διαταράξουν τις βάσεις δεδομένων, ή δημιουργημένα ψεύτικα (αλλά ανιχνεύσιμα) διαπιστευτήρια που να αποσκοπούν στον εντοπισμό εγκληματιών που κάνουν κατάχρηση τους για χρηματοοικονομικές συναλλαγές. Ως προϋπόθεση, η εσωτερική δομή της επικοινωνίας και ο μηχανισμός υποβολής του botnet πρέπει να μελετηθεί είτε με τεχνική αντίστροφης-μηχανικής των δείγματων, είτε με επικεντρωμένη ανάλυση συμπεριφοράς στο σύστημα αρχείων και στις δραστηριότητες του δικτύου.

Αντίμετρα βασισμένα στο DNS (DNS-Based Countermeasures)

Η προσέγγιση αυτή συνδέεται με το DNS με τις τεχνικές μέτρησης που βασίζονται στο DNS και περιγράφτηκαν προηγουμένως (DNS-based προσεγγίσεις, Sinkholing και DNS cache Snooping). Ανάλογα με τον τύπο του botnet, πολλά δείγματα κακόβουλου λογισμικού χρησιμοποιούν σταθερά ονόματα τομέων ως αναγνωριστικά για την υποκείμενη C&C υποδομή τους, που είναι σε επαφή με τους παραβιασμένους host.

Εάν ένα όνομα τομέα όπως αυτό μπορεί να βρεθεί ότι σχετίζεται με κακόβουλο λογισμικό, και έχει διαπιστωθεί ότι χρησιμοποιείται μόνο για δόλιους σκοπούς, ο τομέας θα πρέπει να κλείσει από τον αρμόδιο καταχωρητή. Βέβαια μια τέτοια ενέργεια πορεί να εξαρτάται κατά πόσο θα υλοποιηθεί από νομοθετικά πλαίσια ή από την προθυμία του παρόχου να συνεργαστεί και να επέμβει.

Σε γενικές γραμμές, αυτή η μέθοδος δεν μπορεί να εφαρμοστεί εάν ένα botnet χρησιμοποιεί νόμιμο τομέα ή υπηρεσία για να εκτελέσει την επικοινωνία του. Δημοφιλή παραδείγματα οι λογαριασμοί κοινωνικών δικτύων. Αυτές οι εντολές εφαρμόζονται ως μηνύματα κατάστασης σε ένα δημιουργημένο προφίλ, όπως συνέβη πρόσφατα με έναν αυξανόμενο αριθμό botnet, όπως το Twitter Mehika botnet, το οποίο προέρχονται από το Μεξικό.

Παράδειγμα: Οι Αντωνακάκης et al. Παρουσιάσαν το Notos, ένα σύστημα ανάλυσης για τη δυναμική γένεση βαθμολογιών φήμης ονομάτων τομέα. Το σύστημά τους βασίζεται κυρίως σε δύο πηγές πληροφοριών:

1. Ιστορικά στοιχεία DNS που συλλέγονται παθητικά από recursive DNS resolvers που λειτουργούν από ISP για τη μοντελοποίηση καλοήθους χρήσης DNS.
2. Spam-παγίδες, honeynets, υπηρεσίες ανάλυσης malware και άλλα παρόμοια μέσα για τη μοντελοποίηση της χρήση του DNS από εγκληματίες.

Το Notos είναι σε θέση να αναθέτει σκορ φήμης σε προηγουμένως αόρατα ονόματα τομέα και έχει επιτύχει υψηλό ποσοστό, πραγματικό-θετικών (96,8%) και χαμηλό ψευδό- θετικών (0,38%) βαθμολογιών.

Απεθείας απενεργοποίηση του C&C διακομιστή (Direct takedowng of C&C server)

Η τεχνική μετριασμού γνωστή ως «άμεση απενεργοποίηση» ή «αποκεφαλισμός» του C&C server αποβλέπει στην εξάλειψη των περιπτώσεων των C&C server με τους οποίους ελέγχονται απμακρυσμένα τα bot. Η εφαρμογή αυτής της τεχνικής προυποθετεί την

υπαρξη ενός botnet κεντρικοποιημένης αρχιτεκτονικής, όπως συνήθως χρησιμοποιείται στα botnet που βασίζονται στο IRC και HTTP.

Το πρώτο βήμα για την εφαρμογή αυτής της μεθόδου είναι ο εντοπισμός της διεύθυνσης IP του στόχου.Το επόμενο βήμα είναι να προσδιοριστεί ο υπεύθυνος πάροχος υπηρεσιών ή το κέντρο δεδομένων που φιλοξενεί το αντίστοιχο διακομιστή και να επικοινωνήσει με αυτόν. Δεδομένου ότι αυτό το βήμα περιλαμβάνει συνεργασίες οντοτήτων που μπορεί να τοποθετούνται σε οποιοδήποτε σημείο παγκοσμίως, διάφορες προκλήσεις μπορεί να προκύψουν:

- Τα πιο σοβαρά προβλήματα είναι πιθανό να προκύψουν εξαιτίας της μη συνεργασίας του παρόχου φιλοξενίας που είναι υπεύθυνος για το διακομιστή.
- Σε ορισμένες χώρες, ο πάροχος φιλοξενείας δεν μπορεί καν να υποχρεωθεί να σταματήσει τη λειτουργία του διακομιστή, λόγω έλλειψης πολιτικής ελέγχου και σχετικής νομοθεσίας.
- Διαφορετικές χρονικές ζώνες μπορεί να επηρεάσουν τη διαθεσιμότητα των σημείων επαφής.
- Πιθανά θέματα γλώσσας θα μπορούσαν να περιπλέξουν την επικοινωνία γενικότερα.

Μια αίτηση απενεργοποίησης εξαρτάται κυρίως από τους όρους και τις προϋποθέσεις του παρόχου καθώς και τους νόμους της υπεύθυνης χώρας. Οι botmaster γενικά προσπαθούν να αναπτύξουν τους διακομιστές τους που προορίζουν για κακόβουλες πράξεις σε παρόχους που εγγυώναται στους πελάτες τους την ανωνυμία και την ευρωστία, στην περίπτωση που ο διακομιστής τους είναι ο στόχος μιας έρευνας. Περιπτώσεις όπου C&C server φιλοξενούνται στην υπηρεσία της EC2 Amazon και στην AppEngine της Google έχουν ήδη εντοπιστεί από το 2009

Καθώς η απενεργοποίση γίνεται είτε με την αφαίρεση της σύνδεσης από το δίκτυο ή με το κλείσιμο του διακομιστή, αυτό μπορεί να οδηγήσει σε απώλεια δεδομένων, παράλληλα με την καταστροφή αποδεικτικών στοιχείων. Επίσης, πρέπει να σημειωθεί ότι επειδή δεν καθαρίζονται οι προσβεβλημένοι host, τα συστήματα συχνά παραμένουν ευάλωτα σε περαιτέρω απειλές, αφού πολλοί τύποι κακόκοβουλου λογισμικού χρησιμοποιούν Anti-AV μηχανισμούς και αποτρέπουν το σύστημα από την εφαρμογής patches.

Παράδειγμα: Οι Song et al. παρουσίασαν μια λεπτομερή ανάλυση του MegaD spamming botnet. Αποκάλυψαν, την αρχιτεκτονική διαχείρισης του MegaD, η οποία χωρίζεται σε Master Server που εκτελούν εντολές, Template servre που παρέχουν ηλεκτρονικά μηνύματα-στόχους και πρότυπα για καμπάνιες spam, Drop Server που χρησιμοποιούνται για τη διανομή update binaries και SMTP server που προορίζονται κυρίως για τις δοκιμές της ικανότητάς των bot να αποστέλουν με επιτυχία τα spam και να λαμβάνουν ενημερώσεις κατάστασης. Επιπλέον, οι Song et al. παρακολούθησαν τα αποτελέσματα της προσπάθειας της FireEye να εφαρμόσει την τεχνική takedown. Αν και η απενεργοποίηση φάνηκε επιτυχής σε πρώτη φάση, οι MegaD botherder ήταν σε θέση να ανακτήσουν τον έλεγχο μέσα σε τρεις εβδομάδες, ακόμη και να διευρύνουν την ικανότητα του δικτύου. Οι Song et al. δήλωσαν ότι πιστεύουν πως οι botherder χρησιμοποιούν μια υπηρεσία pay-per-Install (PPI) για την ενημέρωση του λογισμικού του bot για νέους C&C διακομιστές.

Φιλτράρισμα πακέτων σε επίπεδο δικτύου και εφαρμογής (Packet filtering on network and application level)

Η μέθοδος αυτή είναι στενά συνδεδεμένη με την τεχνική μέτρησης που περιγράφεται ως Packet Inspection. Επεκτείνει την ιδέα της διαφανούς παρακολούθησης και ανίχνευσης για

την πραγματική εφαρμογή περαιτέρω ενεργειών, όταν αναγνωρίζονται ύποπτες δραστηριότητες.

Το φιλτράρισμα μπορεί γενικά να εφαρμόζεται σε επίπεδο κεντρικού υπολογιστή, δικτύου και ISP. Ένα τυπικό στοιχείο που πραγματοποιεί φιλτράρισμα πακέτων σε επίπεδο host είναι ένα desktop firewall. Σκοπός του είναι να παρακολουθεί τις δραστηριότητες του δικτύου όλων των ενεργών διεργασιών. Δεδομένου ότι το ποσό της κίνησης σε επίπεδο host είναι συνήθως διαχειρίσμο, μπορεί να εφαρμοστεί ο έλεχος πακέτων εις βάθος.

Εάν η τεχνική εφαρμόζεται σε επίπεδο δικτύου, το φιλτράρισμα πακέτων συνήθως εκτελείται από ένα τείχος προστασίας. Επιπλέον, ένα σύστημα ανίχνευσης εισβολής μπορεί να ενισχυθεί όχι μόνο για να παρακολουθεί και να αναφέρει γεγονότα, αλλά και να λαμβάνει αυτόματα δράσεις, όπως η πτώση πακέτων ή το κλείσιμο συνδέσεων, ανάλογα με τη σοβαρότητα των αναγνωρισμένων γεγονότων, προωθώντας έτσι την IDS σε ένα σύστημα πρόληψης εισβολής. Η μέθοδος λειτουργεί επίσης σε επίπεδο ροής, εάν τελικά σημεία επικοινωνίας έχουν σαφώς χαρακτηριστεί ως κακοήθους προέλευσης, για παράδειγμα, χρησιμοποιώντας μαύρες λίστες ή αποκτώντας πληροφορίες για γνωστούς C&C διακομιστές.

Το φιλτράρισμα πακέτων μπορεί επίσης να εφαρμοστεί σε επίπεδο ISP. Αρκεί η επιθεώρηση πακέτων που προέρχονται από το δίκτυο, ώστε να είναι δυνατό το φιλτράρισμα όλων των πακέτων που έχουν διεύθυνση πηγής που δεν ανήκει στο χώρο διευθύνσεων που ανήκει στην υπηρεσία παροχής Internet. Τέτοιες πλαστογραφημένες διευθύνσεις πηγής είναι συνήθως ένα σημάδι κακόβουλων δραστηριοτήτων.

Κλείδωμα της θύρας 25 (Port 25 blocking)

Το κλείδωμα της θύρας είναι ένα προληπτικό μέτρο που μπορεί να εφαρμοστεί από τους ISP για να περιρίσουν τις ποσότητες των spam μηνυμάτων που διέρχονται από το δίκτυό τους. Καθώς περισσότερο από το 87% του συνόλου των e-mail αναφέρεται ως spam, ο μετριασμός αυτής της απειλής είναι επιθυμητός. Η ακόλουθη προσέγγιση βασίζεται στην υπόθεση ότι η χρήση μη εξουσιοδοτημέων υπηρεσιών μέσω της θύρας 25, όπως το διαφημιστικό ταχυδρομείο είναι σχεδόν αποκλειστικά για σκοπούς διανομής spam.

Συνεπώς, το κλείδωμα της θύρας 25 σε επίπεδο σε ISP συστήνεται ως βέλτιστη πρακτική από την Messaging Anti-Abuse Working Group (MAAWG) από το 2005. Κάθε υπηρεσία ηλεκτρονικού ταχυδρομείου θα πρέπει να παρέχεται μέσω της θύρας 587, όπως ορίζεται στο RFC 2476 και να χρησιμοποιεί εξουσιοδότηση. Επιπλέον, το κλείδωμα της θύρας 25 προτείνεται ως βασική βέλτιστη πρακτική, με μεγάλη αποτελεσματικότητα, από την ETIS (Παγκόσμια IT Ένωση για τις Τηλεπικοινωνίες). Σύμφωνα με την ETIS, το spam outputs της Turk Telecom και της Telecom Italia μειώθηκαν σε σημαντικό βαθμό μέσω της εισαγωγής του κλειδώματος της θύρας 25.

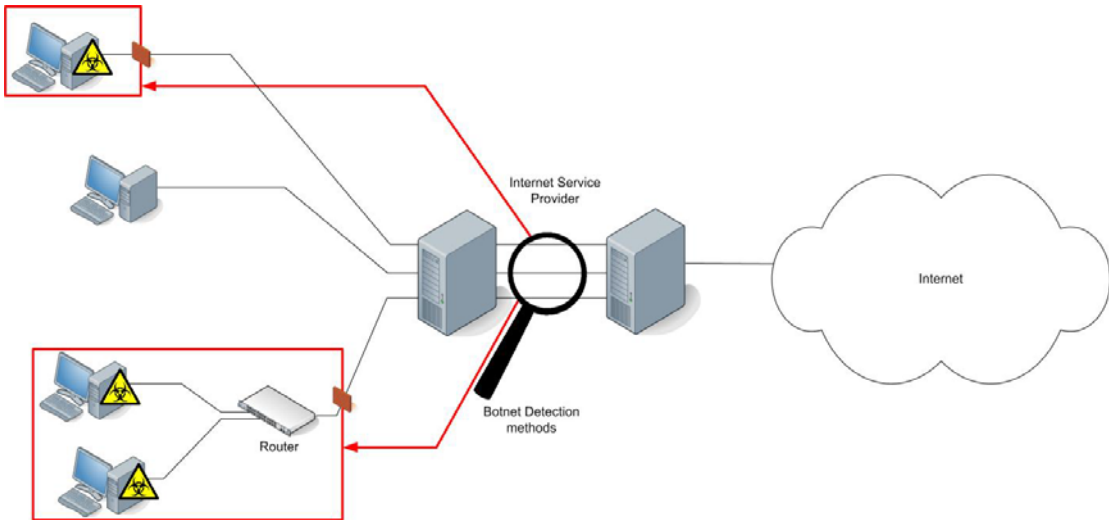
Παράδειγμα: Ο Schmidt παρουσίασε μια περιπτωσιολογική μελέτη σχετικά με το κλείδωμα της θύρας 25. Ένα δευτερεύον δίκτυο των 20.000 συνδρομητών σε ένα Multiple Systems Operator (MSO), με συνολικά 240.000 συνδρομητές Internet αντιμετωπίστηκε με προσαρμοστικό κλείδωμα της θύρας 25, που εφαρμόστηκε σύμφωνα με τη συμπεριφορά του υπολογιστή του συνδρομητή. Οι κανόνες που περιελάμβαναν, για παράδειγμα, το άμεσο κλείδωμα host που είχαν περισσότερες από 40 συνδέσεις στη θύρα 25 σε κάθε ένα λεπτό και συχνή κοινοποίηση των συνδρομητών κοντά ή πάνω από το όριο των 5 e-mails ανά λεπτό στη θύρα 25. Κατά τη διάρκεια μιας δοκιμής δύο εβδομάδων το Μάιο του 2005, οι καταγγελίες παραβίασης για το υποδίκτυο μειώθηκαν σχεδόν στο μηδέν από 100 την ημέρα, και μόνο 5 νόμιμοι μεγάλου όγκου χρήστες παραπονέθηκαν για τους κανονισμούς. Μετά από την ενεργοποίηση του κλειδώματος για το σύνολο των 240.000 συνδρομητών, η

παραγωγή email μειώθηκε κατά 95% και οι καταγγελίες μειώθηκαν σε μονοψήφια κατά μέσο όρο δεδομένα από 600 ανά ημέρα που ήταν πριν.

«Περιφραγμένες τοποθεσίες» (“Walled Gardens”)

Η έννοια των “walled gardens” έχει ως στόχο την προστασία των πελατών των IPS’s και χρηστών του Internet από περαιτέρω ζημία, κατά την παρακολούθηση και απομόνωση των εξερχόμενων συνδέσεων από ένα υπονομευμένο host που ανιχνεύεται. Σε ότι αφορά τη διαδικασία αυτή μπορεί να χωριστεί σε τρία στάδια: τον **εντοπισμό**, την **κοινοποίηση** και την **αποκατάσταση**.

Για την αρχική ανίχνευση του malware, σε ένα απομακρυσμένο σύστημα και την αύξηση τη αποτελεσματικότητάς της, η υπηρεσία παροχής Internet μπορεί να χρησιμοποιήσει μία από τις τεχνικές ανίχνευσης που περιγράφονται στο προηγούμενο κεφάλαιο όπως π.χ. τα honeypot, ή η NetFlow ανάλυση, η αξιολόγηση των μαύρων λιστών, ή ένα συνδυασμό των προσεγγίσεων αυτών. Εφόσον από μια μόλυνση έχει επιβεβαιωθεί για τη σύνδεση, ο χρήστης βρίσκεται σε μια “περιφραγμένη τοποθεσία”, όπως φαίνεται στο σχήμα 15 Αυτό σημαίνει ότι η σύνδεση του είναι περισσότερο ή λιγότερο αυστηρά περιορισμένη, ανάλογα με τις πολιτικές του ISP, και ότι θα σταλεί σε αυτόν μια ειδοποίηση. Η γενική ιδέα των walled gardens, είναι να απαγορεύει σχεδόν όλες τις προσπάθειες σύνδεσης από τον απομονωμένο χρήστη, εκτός από εκείνες προς μια προσδιορισμένη «λευκή λίστα» υπηρεσιών μετριασμού του malware. Όλα τα άλλα ερωτήματα DNS αντιμετωπίζονται με μια δημιουργημένη απάντηση που θα οδηγήσει τον πελάτη σε μια έτοιμη ιστοσελίδα που ανήκει στην υπηρεσία παροχής Internet, η οποία θα πληροφορεί τον πελάτη σχετικά με την μόλυνση που έχει εντοπιστεί και θα προσφέρει χρήσιμες συμβουλές, π.χ. παρέχοντας οδηγίες αφαίρεσης, μια λίστα με συνδέσμους σε εργαλεία αφαίρεσης κακόβουλου λογισμικού, μέτρα για τη μείωση του κινδύνου μελλοντικών μολύνσεων και έναν οδηγό για τη δημιουργία αντιγράφων ασφαλείας των χρηστών. Η αυτο-αποκατάσταση είναι ως εκ τούτου η συνήθης επιδίωξη αυτής της προσέγγισης, καθώς υπάρχει η άποψη ότι η ευθύνη για τα συστήματα που επηρεάζονται βρίσκεται στα χέρια των πελατών.



Σχήμα 15: Λειτουργία των Walled Gardens [Enisa 2011]

Μερικά ζητήματα σχετικά με την υλοποίηση ενός walled garden θα πρέπει να εξετάζονται. Επειδή η περιορισμένη συνδεσιμότητα θεωρείται από τους πελάτες ως ένας σοβαρός περιορισμός, θα πρέπει να υπάρχει μια πολιτική επιλογής παραμονής στο wall garden. Εάν δεν πραγματοποιηθεί καθαρισμός του συστήματος, τότε η πλήρης συνδεσιμότητα θα

πρέπει να ενεργοποιηθεί εκ νέου μόνο για ορισμένο χρονικό διάστημα. Οι περιορισμοί της σύνδεσης στη συνέχεια ανανεώνονται όταν ανιχνευτεί μια εκ νέου μόλυνση και / ή όταν μεσολαβήσει η περίοδος χάριτος. Είναι σημαντικό να σημειωθεί ότι ο περιορισμός της πρόσβασης στο Διαδίκτυο μπορεί να οδηγήσει σε δραστικές παρενέργειες, αν η τηλεφωνία λειτουργεί πάνω στην ίδια σύνδεση. Στην περίπτωση αυτή, το κλείδωμα της σύνδεσης σε γενικές γραμμές μπορεί να απενεργοποιήσει και την ικανότητα του πελάτη να πραγματοποιήσει κλήσεις έκτακτης ανάγκης, το οποίο δεν είναι επιθυμητό.

Μια παραλλαγή της ιδέας του walled garden είναι οι υπηρεσίες που απαγορεύουν την πρόσβαση σε ενδεχομένως επικίνδυνες ιστοσελίδες, χρησιμοποιώντας τις μαύρες λίστες που περιέχουν ονόματα τομέα και διευθύνσεις IP οι οποίες συγκεντρώνονται από πρωτοβουλίες όπως το StopBadware ή το Spamhaus.

Αντίμετρα ομότιμων κόμβων (Peer-to-peer Countermeasures)

Κάθε δίκτυο βασισμένο σε δομή peer-to-peer έχει να διαχειριστεί πληροφορίες που αφορούν τη σύνδεση και τη δρομολόγηση. Νέοι κόμβοι πρέπει να κοινοποιούνται στο δίκτυο και οι πληροφορίες σχετικά με τους διάφορους κόμβους πρέπει να δημοσιοποιούνται στο δίκτυο. Συνήθως, αυτό επιτυγχάνεται με τη διατήρηση και την ανταλλαγή λιστών κόμβων. Πρόκειται για συλλογές από εγγραφές που περιέχουν τα στοιχεία επαφής των άλλων κόμβων. Μια πλήρης επισκόπηση ολόκληρου του χώρου διευθύνσεων είναι δυναμικά κοινή σε όλο το δίκτυο ομότιμων κόμβων, αλλά δεν είναι διαθέσιμη σε ένα μόνο σημείο.

Αντίμετρα με στόχο τα peer-to-peer botnet εκμεταλλεύονται αυτή την έννοια των καταλόγων κόμβων και τους μηχανισμούς δημοσίευσή τους. Μία προσέγγιση είναι να επιχειρηθεί να μολυνθούν οι κατάλογοι αυτοί με την προσθήκη άκυρων καταχωρήσεων σύνδεσης μη υφιστάμενων κόμβων. Η κοινοποίηση ενός μεγάλου αριθμού μη έγκυρων κόμβων σε γνωστούς μπορεί να οδηγήσει σε απώλεια της συνολικής διασύνδεσης και μπορεί ακόμη και να είναι επαρκής για να μολύνει και να διαταράξει ολόκληρο το botnet, αφού η διαθέσιμη μνήμη για τις peer-list είναι περιορισμένη. Σε εύθετο χρόνο, οι bot κόμβοι δεν θα είναι σε θέση να αποθηκεύουν πληροφορίες σχετικά με τους νέους κόμβους και θα απορρίπτουν την παλία αλλά ισχύουσα πληροφορία για τους υφιστάμενους.

Παράδειγμα: Οι Holz et al δεν παρουσιάζουν μόνο μια μέθοδο για τον περιορισμό των peer-to-peer botnet, αλλά, μετά από την ανάλυση του πρωτοκόλλου επικοινωνίας και εφόσον είναι σε θέση να απαριθμήσουν όλους τους κεντρικούς υπολογιστές, καθιέρωσαν μια βάση για την αξιολόγηση των αντιμέτρων. Υποθέτοντας ότι μια αποτελεσματική μέθοδος μετρίασης απαιτεί μια επίθεση στη δομή ελέγχου του botnet, αναπτύχθηκαν πολλές θεωρητικές στρατηγικές κατά των κλασικών peer-to-peer δικτύων.

Διείσδυση και απομακρυσμένη αντιμετώπιση (Infiltration and Remote Disinfection)

Η διείσδυση σχετικά με τα botnet, περιγράφει τη διαδικασία του να βρεθεί ένας τρόπος μίμησης του botherder και απόκτησης ελέγχου των μολυσμένων host. Όπως σχεδόν όλες οι οικογένειες botnet παρουσιάζουν διαφορές ως προς την εφαρμογή τους και τον τρόπο λειτουργίας, μια διείσδυση μπορεί να θεωρηθεί ως μία ειδική προσέγγιση για κάθε botnet στόχο. Η προσέγγιση αυτή μπορεί να χωριστεί σε δύο στάδια. Το πρώτο στάδιο αποτελείται από την ανάλυση του μηχανισμού επικοινωνίας του botnet. Το δεύτερο στάδιο περιλαμβάνει το σχεδιασμό και την υλοποίηση ενός εργαλείου για την πραγματική διείσδυση, με βάση το προηγούμενο βήμα της ανάλυσης.

Η προσπάθεια που απαιτείται για την εκτέλεση αυτής της τεχνικής είναι σε μεγάλο βαθμό σταθμισμένη προς το πρώτο στάδιο, καθώς αυτό περιλαμβάνει μεγάλες ποσότητες αντίστροφης μηχανικής του κακόβουλου κώδικα.

Ο κύριος στόχος είναι να εντοπιστούν οι αδυναμίες στο πρωτόκολλο επικοινωνίας του botnet, που μπορούν να χρησιμεύσουν ως φορείς της επίθεσης με την οποία μπορεί να υλοποιηθεί η πραγματική διείσδυση. Αυτό συνήθως περιλαμβάνει τον προσδιορισμό της δομής των μηνυμάτων εντολής των botnet, κρυπτογραφικά μέτρα που χρησιμοποιούνται από το botnet και μηχανισμούς εξουσιοδότησης για τη πιστοποίηση της προέλευσης των εντολών.

Αν το πρώτο στάδιο είναι επιτυχές και τα μέσα της διείσδησης στο botnet έχουν βρεθεί, είναι δυνατή να μίμηση του μηχανισμού ελέγχου του botherder μέσα από ένα προσαρμοσμένο εργαλείο το οποίο προσομοιώνει το πρωτόκολλο. Ο κύριος στόχος αυτής της διαδικασίας είναι να βρεθεί ένας τρόπος απομακρυσμένης «θεραπείας» των host που έχουν μολυνθεί.

Στο σημείο αυτό πρέπει να ανεφερθεί ότι η ενεργοποίηση μιας τέτοιας επέμβασης δεν επιτρέπεται νομικά σε όλες τις χώρες ενώ ενέχει τον κίνδυνο απρόβλεπτων παρενεργειών αφού δεν είναι δυνατή η δοκιμή όλων των επηρεαζόμενων συστημάτων και ρυθμίσεων.

Παράδειγμα: Διαφορετικές προσεγγίσεις και πρότυπα για την εξάλειψη των διαφόρων botnet έχουν παρουσιαστεί από τους Leder και Werner. Επίσης, η έρευνά τους περιελάμβανε στρατηγικές απολύμανσης για διάφορα μεγάλα botnet και αρχιτεκτονικές botnet, συμπεριλαμβανομένων των Storm και Conficker botnet.

3.2 Νομοθετικές ρυθμίσεις

Γίνεται εύκολα αντιληπτή η ανάγκη θεσμοθέτησης των κατάλληλων νόμων για την αντιμετώπιση του ηλεκτρονικού εγκλήματος και κατά συνέπεια τον περιορισμό των botnet.

Σε ότι αφορά την Ευρωπαϊκή Ένωση, η οδηγία του Ευρωπαϊκού Κοινοβολίου και του Συμβουλίου για τις επιθέσεις κατά των συστημάτων πληροφοριών και την κατάργηση της απόφασης-πλαισίου 2005/222/ΔΕΥ του Συμβουλίου**,** προβλέπει κυρώσεις για την παραγωγή, πώληση, προμήθεια για χρήση, εισαγωγή, διανομή ή άλλη διάθεση συσκευών/εργαλείων που χρησιμοποιούνται για τη διάπραξη των αδικημάτων.

Η παρούσα οδηγία λαμβάνει υπόψη τις νέες μεθόδους διάπραξης εγκλημάτων στον κυβερνοχώρο, ιδίως με τη χρήση δικτύων προγραμμάτων ρομπότ (botnet) και αναγνωρίζει το γεγονός ότι οι επιθέσεις από δίκτυα προγραμμάτων ρομπότ συχνά εξαπολύονται σε μεγάλη κλίμακα. Κατά την οδηγία οι μεγάλης κλίμακας επιθέσεις είναι οι επιθέσεις εκείνες που είτε πραγματοποιούνται με τη χρήση εργαλείων που πλήττουν σημαντικό αριθμό συστημάτων πληροφοριών, είτε είναι επιθέσεις που προκαλούν σημαντικές ζημίες, π.χ. διαταραχή των υπηρεσιών συστημάτων, οικονομικό κόστος ή απώλεια δεδομένων προσωπικού χαρακτήρα κ.λπ..

Οι στόχοι της οδηγίας συνάδουν με τις πολιτικές της ΕΕ για την καταπολέμηση του οργανωμένου εγκλήματος, την αύξηση της ανθεκτικότητας των δικτύων υπολογιστών, την προστασία των υποδομών πληροφοριών ζωτικής σημασίας και την προστασία των δεδομένων. Οι στόχοι συνάδουν επίσης με το πρόγραμμα «Ασφαλέστερο Διαδίκτυο» που αποβλέπει στην προαγωγή της ασφαλέστερης χρήσης του Διαδικτύου και των νέων επιγραμμικών τεχνολογιών, καθώς και στην καταπολέμηση του παράνομου περιεχομένου.

Τέλος, η οδηγία:

- Προβλέπει κυρώσεις για την παραγωγή, πώληση, προμήθεια για χρήση, εισαγωγή, διανομή ή άλλη διάθεση συσκευών/εργαλείων που χρησιμοποιούνται για τη διάπραξη των αδικημάτων.

- Περιλαμβάνει επιβαρυντικές περιστάσεις όπως τη μεγάλης κλίμακας διάσταση των επιθέσεων – αντιμετώπιση των botnet ή παρόμοιων εργαλείων με τη θέσπιση νέων επιβαρυντικών περιστάσεων, με την έννοια ότι η εγκατάσταση botnet ή παρόμοιων μέσων θα συνιστά επιβαρυντικό παράγοντα όταν διαπράττονται τα εγκλήματα που απαριθμούνται στην υφιστάμενη απόφαση-πλαίσιο, καθώς και όταν πραγματοποιούνται τέτοιες επιθέσεις με την απόκρυψη της πραγματικής ταυτότητας του αυτουργού και προκαλείται ζημία στον νόμιμο δικαιούχο της ταυτότητας. Τέτοιοι κανόνες θα πρέπει να είναι σύμφωνοι με τις αρχές της νομιμότητας και της αναλογικότητας των ποινικών αδικημάτων και κυρώσεων και συνεπείς με την υπάρχουσα νομοθεσία για την προστασία των δεδομένων προσωπικού χαρακτήρα.
- Χαρακτηρίζει την «παράνομη υποκλοπή» ως ποινικό αδίκημα.
- Θεσπίζει μέτρα για τη βελτίωση της ευρωπαϊκής δικαστικής συνεργασίας σε ποινικές υποθέσεις συνεργασίας με την ενίσχυση της υφιστάμενης υποδομής σημείων επαφής που είναι διαθέσιμη σε 24ωρη βάση και τις επτά ημέρες της εβδομάδας. Στο πλαίσιο αυτό προτείνεται υποχρέωση ικανοποίησης αιτήματος συνδρομής από τα λειτουργικά σημεία επαφής εντός ορισμένου χρονικού ορίου. Στόχος του μέτρου αυτού είναι να εξασφαλιστεί ότι τα σημεία επαφής θα δηλώνουν εντός ενός ορισμένου χρονικού ορίου εάν είναι σε θέση να ανταποκριθούν στην αίτημα συνδρομής, και μέχρι πότε το σημείο επαφής που υποβάλλει το αίτημα μπορεί να αναμένει την εξεύρεση λύσης.
- Ανταποκρίνεται στην ανάγκη παροχής στατιστικών στοιχείων για το έγκλημα στον κυβερνοχώρο καθιστώντας υποχρεωτική για τα κράτη μέλη τη θέσπιση κατάλληλου συστήματος για την καταγραφή, την παραγωγή και την παροχή στατιστικών στοιχείων για τα αδικήματα που αναφέρονται στην υφιστάμενη απόφαση-πλαίσιο και την «παράνομη υποκλοπή» που προστίθεται τώρα *[http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0517:FIN:EL:HTML].*

Άλλα παραδείγματα εθνικής νομοθεσίας σχετικά με την αντιμετώπιση του ηλεκτρονικου εγκλήματος που μπορούν να αναφερθούν ενδεικτικά είναι τα παρακάτω:

- Μια αλλαγή στην ελβετική νομοθεσία, η οποία επιβεβαιώθηκε το 2007, απαγορεύει την μαζική αποστολή διαφήμισης (spam) σε περιπτώσεις όπου ο αποστολέας δεν έχει αποκτήσει ρητή έγκριση από τον αποδέκτη. Επιπλέον, οι πάροχοι υπηρεσιών που απαιτείται να καταπολεμούν ενεργά την μαζική διαφήμιση. για την ενεργό καταπολέμηση της εν λόγω διαφήμισης μάζα.Το παράδειγμα της Ελβετίας αποδεικνύει ότι οι πάροχοι υπηρεσιών θα μπορούσαν να αναγκαστούν να αλλάξουν τις πρακτικές τους.
- Το 2010, το Γερμανικό Ομοσπονδιακό Ανώτατο Δικαστήριο εξέδωσε απόφαση που υποχρέωνε όλους τους πολίτες να λειτουργούν τα ασύρματα δίκτυά τους με ενεργοποιημένη την κρυπτογράφηση συνεχώς. Αυτό προέκυψε από μια περίπτωση όπου κάποιος κατηγορούνταν για παραβίαση πνευματικών δικαιωμάτων μέσω της κοινής χρήσης αρχείων. Το άτομο, που λειτουργεί ένα απροστάτευτο ασύρματο δίκτυο, υποστήριξε ότι το αδίκημα πνευματικής ιδιοκτησίας συνέβη κατά τη διάρκεια διακοπών του, ώστοσο όμως κρίθηκε υπεύθυνη, αφού επέτρεψε να λειτουργεί η συσκευή χωρίς δυνατότητα κρυπτογράφησης, πράξη που θεωρήθηκε ως αμέλεια. Το παράδειγμα αυτό δείχνει πως οι νόμοι για το έγκλημα στον κυβερνοχώρο θα μπορούσαν επίσης να επεκτείνονται ως προς την ευθύνη των πελατών.

3.3 Κοινωνικού χαρακτήρα προσεγγίσεις

Οι δράσεις που περιγράφονται ως αντίμετρα στην ενότητα αυτή στοχεύουν στη βελτίωση του περιβάλλοντος που απαιτείται για την αντιμετώπιση και περιορισμό ενός botnet. Αυτό συνεπάγεται τη στάση και συμπεριφορά των τελικών χρηστών που επηρεάζονται από τις επιπτώσεις των botnet, το πώς μπορεί να βελτιωθεί ο συντονισμός καθώς και τους τρόπους δράσης στην αντιμετώπιση της πρόκλησης των botnet από διεθνή σκοπιά.

Ευαισθητοποίηση των χρηστών και εκπαίδεση

Η ευαισθητοποίηση των χρηστών είναι μια προσέγγιση για το περιορισμό των botnet που εστιάζει στις γενεσιουργές αιτίες τους, δηλαδή την μόλυνση των υπολογιστών των τελικών χρηστών των δικτύων μια εταιρείας. Η εμφάνιση των μολύνσεων είναι συχνά αποτέλεσμα της χρήσης κινητών τηλεφώνων και ηλεκτρονικών υπολογιστών η οποία καθοδηγείται από την άγνοια των πιθανών πηγών μόλυνσης και την έλλειψη προσοχής.

Κατά συνέπεια είναι λογικό κάποιες δράσεις να στοχεύουν στην τεχνική κατάρτιση των τελικών χρηστών και στην αίσθηση της κοινωνικής υπευθυνότητας τους υπό τον όρο της ασφαλούς λειτουργίας. Αυτό περιλαμβάνει θέματα όπως:

- Εκπαίδευση στους μηχανισμούς διασποράς του κακόβουλου λογισμικού. Αυτό μπορεί να βοηθήσει στην πρόληψη των drive-by μολύνσεων, όπου περιλαμβάνονται τα ανεπιθύμητα e-mail, που προκαλούνται από συνδεόμενες ιστοσελίδες. Αυτό περιλαμβάνει επίσης τον χειρισμό των αφαιρούμενων μέσων, όπως εξωτερικούς δίσκους αποθήκευσης δεδομένων, των οποίων η προέλευση δεν είναι πλήρως αξιόπιστη.
- Υπογράμμιση τη σημασίας της διατήρησης των συστημάτων ενημερωμένων μέχρι και την ημερομηνία με patches για το εγκατεστημένο λογισμικό. Αυτό που προστατεύει από τις ήδη γνωστές τρωτότητες τις οποίες εκμεταλεύονται οι διανομείς malware.
- Πληροφόρηση για την ερμηνεία των πιθανών συμπτωμάτων μόλυνσης και καθοδήγηση σχετικά με τη θεραπεία, συμπεριλαμβανομένης και της χρήσης anti-malware εργαλείων. Η δράση αυτή μπορεί να βοηθήσει στην ελαχιστοποίηση των πιθανών βλαβών από ενέργειες κλοπής ταυτότητας και οικονομικής απάτης.
- Καλά μελετημένη διαχείριση κωδικών πρόσβασης. Μια τέτοιου είδους διαχείριση μπορεί επίσης να συμβάλει στην μείωση των βλαβών.

Κεντρικό Γραφείο Βοήθειας Περιστατικών (Central Incident help desk)

Η ιδέα ενός κεντρικού γραφείου βοήθειας περιστατικών που θα προσφέρει συμβουλευτική σχετικά με την αντιμετώπιση των μολύνσεων από bot προϋποθέτει την υπόθεση ότι ένας καθορισμένος οργανισμός θα επιδοτεί αυτές τις υπηρείες. Μια τέτοια οργάνωση μπορεί να υποστηριχτεί και διαφημιστεί από κάποια ιδρύματα.

Ένα πρωτοπόρο έργο ανάπτυξης ενός τέτοιου γραφείου αποτελεί αυτό του Γερμανικού Anti Botnet HelpDesk. Στόχος της πρωτοβουλίας είναι αποχωρήσει η Γερμανία από τη λίστα με τις δέκα κορυφαίες χώρες από τις οποίες προέρχονται δραστηριότητες. που σχετίζονται με botnet.

Αποκεντρωμένες προσεγγίσεις για την ενημέρωση των πελατών που εμπλέκονται σε μολύνσεις, αποτελούν για παράδειγμα αυτές της Αυστραλίας και της Ιαπωνίας. Η Αυστραλιανή Πρωτοβουλία για την ασφάλεια στο Διαδίκτυο (AISI) ξεκίνησε τον Νοέμβριο του 2005. Η AISI συλλέγει δεδομένα από διάφορες πηγές για τον εντοπισμό λοιμώξεων στο αυστραλιανό Internet. Η επεξεργασία των δεδομένων γίνεται σε καθημερινή βάση και εκθέσεις αποστέλλονται στους συμμετέχοντες ISP μέσω e-mail.

Στην Ιαπωνία, το Cyber Clean Center (CCC) έχει ενεργό ρόλο στην καταπολέμηση των λοιμώξεων από bot. Ο οργανισμός χωρίζεται σε τρεις ομάδες εργασίας. Η ομάδα εργασίας που διαχειρίζεται το σύστημα αντιμέτρων BOT συλλέγει δείγματα bot και συνεργάζεται με πολλές ιαπωνικές ISP για την πληροφόρηση πελατών που σχετίζονται με μολύνσεις. Αποτελεσματικές και αποδοτικές τεχνικές ανάλυσης μελετώνται από την ομάδα ανάλυσης BOT. Η ομάδα αναπτύσσει επίσης τα αντίμετρα και τις στρατηγικές απολύμανσης με βάση την ανάλυση των δειγμάτων botnet. Τέλος, η ομάδα πρόληψης από τη μόλυνση BOT προωθεί έργα για τη δημοσίευση και την προώθηση των πληροφοριών σχετικά με τις απειλές που συνδέονται με τα botnet και παρέχει συλλογές δειγμάτων bot στους πωλητές anti-malware και security tools.

Ενίσχυση της συνεργασίας μεταξύ εμπλεκόμενων φορέων

Ένας βασικός παράγοντας για την καταπολέμηση των botnet με επιτυχία είναι η έκταση και αποτελεσματικότητα της συνεργασίας μεταξύ των εμπλεκόμενων φορέων, καθώς οι απαιτούμενες γνώσεις, οι πόροι, και οι αρχές είναι γενικά κατανημένοι. Για παράδειγμα, οι ερευνητές ασφαλείας από τον ακαδημαϊκό χώρο και τη βιομηχανία μπορεί να έχουν πληροφορίες σχετικά με τους βασικούς παράγοντες ενός συγκεκριμένου botnet, π.χ. έναν κατάλογο των προσδιορισμένων C&C διακομιστών και των μηχανισμών επικοινωνίας. Οι CERT's μπορεί να έχουν πληροφορίες και στοιχεία για τα περιστατικά που σχετίζονται με τα botnet που μπορούν να υποστηρίξουν την τις έρευνες. Η νομοθετική εξουσία έχει τη δύναμη της επιβολής στην τάξη ή της εντολής εκτέλεσης αντιμέτρων κατά του botnet. Αυτό καταδεικνύει ότι διαφορετικοί φορείς με διαφορετικό ρόλο και δυνατότητες εμπλέκονται στην καταπολέμηση των botnet.

Ζητήματα που μπορεί να προκύψουν κατά τη συνεργασία αυτών των φορέων μπορεί να αφορούν:

- αρχικό σχεδιασμό και αντιμέτωπιση που δεν λαμβάνουν υπόψη την ύπαρξη άλλων μερών,
- ιδιαίτερους μηχανισμούς επικοινωνίας,
- έλλειψη χρόνου,
- έλλειψη εμπιστοσύνης προς άγνωστες ομάδες
- απουσία γνώσης σχετικά με τη μορφοποίηση και οργάνωση των δεδομένων ώστε να μπορούν να τα επεξεργαστούν αποδοτικά και άλλα μέρη.

Η συνεργασία μεταξύ φορέων και η παγκόσμια ενοποίηση των εγγραφών δεδομένων βοηθάει στην απόκτηση μιας πιο λεπτομερούς εικόνας της διεθνούς κατάστασης των botnet και της ανάπτυξης. Καθώς τα botnet εξαπλώνονται σε όλες τις χώρες, αυτή η συνεργασία αποτελεί αναγκαίο βήμα για την επιτυχή καταπολέμηση τους.

Παράδειγμα: Το Ιταλικό «Chapter of The Honeynet Project έχει δημιουργήσει το πλαίσιο "Dorothy" ως ένα ανοικτό πλαίσιο ανάλυσης botnet που μπορεί να χρησιμοποιηθοεί για την αυτόματη ανίχνευση των δραστηριοτήτων και την απεικόνιση τους. Το έργο στοχεύει στην παροχή σχετικής πληροφορίας αυτόματα στους ISP και την επιβολή του νόμου προκειμένου να τονωθεί η στρατηγική μετριασμού των επιπτώσεων. Το Dorothy συλλέγει δείγματα malware με ένα honeypot, τα εκτελεί σε ένα sandbox και αποσπά πληροφορία που μπορεί να χρησιμοποιηθεί για τη δημιουργία ενός drone το οποίο στη συνέχεια εισάγεται στο botnet. Τα δεδομένα από την παρακολούθηση των botnet συγκεντρώνονται σε πραγματικό χρόνο και παρουσιάζονται σε μια διεπαφή ιστού. Το Dorothy στη στην τρέχουσα έκδοσή του περιορίζεται σε IRC-based botnet.

3.4 Παραδείγματα πρωτοβουλιών και ιδρυμάτων για την καταπολέμηση των απειλών των botnet

Με την αυξανόμενη σημασία της παγκόσμιας απειλής των botnet, πολλές πρωτοβουλίες συνεργασίας ξεκίνησαν σε εθνικό και διεθνές επίπεδο, προκειμένου να ενισχυθούν οι δραστηριότητές αντιμετώπισης. Οι πρωταρχικοί στόχοι των ομάδων αυτών περιλαμβάνουν την κατασκευή και τη συντήρηση σχέσεων εμπιστοσύνης μεταξύ των διαφόρων οργανισμών για την επιτάχυνση των εργασιών, πράγμα που καθιστά ευκολότερη τη διαδικασία ανταλλαγής κρίσιμων πληροφοριών για την υποστήριξη των ερευνών και τη μεταφορά γνώσεων, και για να βελτιώσει τις αρμοδιότητες όλων των εμπλεκομένων μερών.

Δεδομένου ότι η εν λόγω αρμοδιότητες μεταξύ των διαφόρων μερών ποικίλλουν τόσο από επαγγελματική όσο και από νομοθετική άποψη, η συνεργασία και ο συντονισμός είναι σαφώς επιθυμητά. Μερικά παραδείγματα από τέτοιες πρωτοβουλίες παρουσιάζονται συνοπτικά στη συνέχεια.

3.4.1 Πρωτοβουλίες σε εθνικό επίπεδο

Στην ενότητα αυτή παρουσιάζονται συνοπτικα πρωτοβουλίες συνεργασίας σε εθνικό επίπεδο δύο ευρωπαϊκών χωρών αλλά και άλλων.

Γερμανία

Το γερνανικό Anti Botnet HelpDesk είναι ένα έργο που «τρέχει» η ένωση της γερμανικής βιομηχανίας του διαδικτύου (σε συνεργασία με τη γερμανική Ομοσπονδιακή Υπηρεσία για την Ασφάλεια Πληροφοριών (BSI)).

Η οικονομική υποστήριξη παρέχεται από το Γερμανικό Ομοσπονδιακό Υπουργείο Εσωτερικών. Στόχος της πρωτοβουλίας είναι αποχωρήσει η Γερμανία από τη λίστα με τις δέκα κορυφαίες χώρες από τις οποίες προέρχονται δραστηριότητες. που σχετίζονται με botnet.

Το έργο του Anti Botnet HelpDesk καθοδηγείται από τις προσεγγίσεις της Αυστραλίας, της Ιαπωνίας και της Κορέας. Οι επιχειρησιακές δραστηριότητες του εστιάζονται στους πελάτες ISP και χωρίζονται σε τρία βήματα:

1. Εντοπισμός των θυμάτων έμμεσα μέσω παγίδων spam και honeypot.
2. Αποστολή ειδοποίησης μέσω του ISP στους χρήστες που εντοπίζονται.
3. Προσφορά διαδραστικής βοήθειας στους χρήστους όπου ήταν μη επιτυχής η προσπάθεια αφαίρεσης του κακόβουλου λογισμικού από τους ίδιους. Για το σκοπό αυτό έχει συσταθεί ένα κεντρικό κέντρο υποστήριξης.

Κάτω Χώρες

Τον Ιούλιο του 2009, 14 Ολλανδικοί ISP συμφώνησαν να ενωθούν στον αγώνα κατά των botnet. Αυτοί οι φορείς πρόσβασης αντιπροσωπεύουν το σύνολο σχεδόν των συνδέσεων των καταναλωτών στο Διαδίκτυο στις Κάτω Χώρες, και ανέρχονται στο 98% της αγοράς. Ένας από τους πρωτεργάτες αυτής της «συμμαχίας» ήταν η Ολλανδική Ρυθμιστική Αρχή Τηλεπικοινωνιών.

Παρόλο που η συμφωνία δεν προβλέπει διατάξεις διατάξεις σχετικά με τον τρόπο μετριασμού, οι προσεγγίσεις που ορίζονται περιλαμβάνουν την ανταλλαγή πληροφοριών σχετικά με τα μολυσμένα συστήματα και καλές πρακτικές μεταξύ των συμμετεχόντων ISP,

μια υπηρεσία ειδοποίησης των πελατών, και, ως μέτρο, προστασίας περιορισμούς στην πρόσβαση στο Διαδίκτυο των host που εντοπίζονται.

Η Εθνική Υποδομή κατά της εγκληματικότητας στον κυβερνοχώρο (NICC) είναι ένα ολλανδικό πρόγραμμα, που ιδρύθηκε το 2006, με επίκεντρο τη βελτίωση της ανθεκτικότητας των υποδομών ζωτικής σημασίας απέναντι στις απειλές που προέρχονται από το έγκλημα στον κυβερνοχώρο. Αν και η NICC δεν καταπολεμά την εγκληματικότητα άμεσα, στηρίζει όμως τα μέρη που συμμετέχουν στις προσπάθειές τους να βελτιώσουν την ασφάλεια όλων των διαδικασιών που σχετίονατι με τις τεχνολογίες της πληροφορικής. Η πρωτοβουλία αυτή λειτουργεί ως σύνδεσμος μεταξύ των φορέων, καθιστόντας τις πηγές και τους πόρους διαθέσιμα και ενθαρρύνονας την αναταλληγή πληροφοριών.

Αυστραλία

Το 2005, η Αυστραλιανή Αρχή Επικοινωνιών και Μέσων (Australian Communications and Media Authority-ACMA) ξεκίνησε την Αυστραλιανή Internet Security Initiative (AISI) με σκοπό τη μείωση του αριθμού των μολυσμένων υπολογιστών στην Αυστραλία που είναι συνδεδεμένοι στο Internet. Η πρωτοβουλία αυτή συνδέεται με τον Κώδικα Ορθής Πρακτικής Βιομηχανίας Internet (Internet Industry Code of Good Practice), ο οποίος περιγράφει μια κατευθυντήρια γραμμή των δράσεων συμμετοχής για την εφαρμογή τους από τους παρόχους υπηρεσιών Διαδικτύου σε συνεργασία με την CERT Αυστραλίας. Το πρόγραμμα είναι εθελοντικό, αλλά έτυχε καλή υποδοχής.

Η κύρια ιδέα της AISI είναι η ευαισθητοποίηση σχετικά με τη συνολικής κατάσταση που αφορά το κακόβουλου λογισμικό και τις συνοδές δράσεις, εκτελώντας κεντρικά οργανωμένη και εξ αποστάσεως ανίχνευση των μολυσμένων συσκευών και ενημερωνόντας τους αρμόδιους παρόχους δικτύων, π.χ. Παροχείς Υπηρεσιών Διαδικτύου ή διαχειριστές επιχειρήσεων IT . Η AISI στέλνει καθημερινές εκθέσεις για τα συμμετέχοντα μέρη και αποτελεί τον ακρογωνιαίο λίθο του έργου. Ανάλογα με τις λεπτομέρειες εφαρμογής των παρόχων δικτύου, περαιτέρω μέτρα λαμβάνονται, από τη προώθηση των πληροφοριών μόλυνσης και τη παροχή συμβουλών για την αφαίρεση του κακόβουλου λογισμικού, μέχρι το περιορισμός της συνδεσιμότητας στο Internet του μολυσμένου συστήματος, προκειμένου να προστατεύσει τον ιδιοκτήτη και τους άλλους από περαιτέρω βλάβη.

Επιπλέον, οποιαδήποτε περιστατικά που δημιουργούν υποψίες για εγκληματική δραστηριότητα, θα πρέπει να αναφέρονται στους αρμόδιους κυβερνητικούς οργανισμούς.

Ιαπωνία

Οι Ιαπωνικές προσπάθειες για την καταπολέμηση των botnet συγκεντρώνονται στο εθνικό Cyber Clean Center (CCC), και ξεκίνησαν το 2006. Μια συντονιστική επιτροπή, που αποτελείται από το Ιαπωνικό Υπουργείο Εσωτερικών Υποθέσεων και Επικοινωνιών και το Υπουργείο Οικονομίας, Εμπορίου και Βιομηχανίας, οργανώνει τις δραστηριότητές του. Πολλά ιδρύματα και εταιρείες από διάφορες ομάδες συμφερόντων εργάζονται από κοινού, συμπεριλαμβανομένων περισσότερων από 70 Ιαπωνικών ISP, μεταξύ των οποίων αυτοι που συγκεντρώνουν το 90% όλων των χρηστών του Διαδικτύου. Οι συμμετέχοντες χωρίζονται σε τρεις εσωτερικές ομάδες:

- Το Κέντρο Διαμοιρασμού και Ανάλυσης Πληροφορίας Τηλεπικοινωνιών της Ιαπωνίας (Telecom Information Sharing and Analysis Centre -ISAC), το οποίο είναι υπεύθυνο για την ομάδα λειτουργίας του συστήματος αντιμέτρων κατά των Bot .
- Την JP-CERT, υπεύθυνη για την ομάδα ανάλυσης προγράμματος botnet.

- Τον Οργανισμό Προώθης της Πληροφορικής (Information Technology Promotion Agency-IPA), ο οποίος εργάζεται για την ευαισθητοποίηση των χρηστών και είναι υπεύθυνος για προώθησης της ομάδας πρόληψης από τη μόλυνση botnet .

Η όλη διαδικασία είναι συγκρίσιμη με την προσέγγιση της Αυστραλίας, καθώς το CCC στέλνει επίσης κεντρικά πληροφορίες σχετικά με τις μολύνσεις που εντοπίζονται στα συμμετέχοντα ISP. Επίσης, είναι περισσότερο προσανατολισμένη προς την εξειδίκευση αναλόγως του είδους του κακόβουλου λογισμικού και την προσαρμογή των εργαλειών για την αντιμετώπιση τους.

Νότια Κορέα

Ως αντίδραση στις σημαντικές επιθέσεις DDoS σε βάρος της χώρας τους και στις εκθέσεις που έδειχναν υψηλά ποσοστά μόλυνσης μεταξύ των υπολογιστών της Νότιας Κορέας, ο κορεατικός Οργανισμός για την Ασφάλεια στο Διαδίκτυο (Korean Internet Security Agency KISA) και η CERT Κορέας (KRCERT) ξεκίνησαν μια εκτεταμένη αντι-botnet εκστρατεία. Η προσέγγιση αυτή αποτελείται από τρία μέρη:

- Οι μολυσμένοι υπολογιστές ανιχνεύοναται από απόσταση με διάφορους τρόπους
- Η KRCERT πραγματοποιεί εκτενή παρακολούθηση των botnet και δράσεις μετριασμού, χρησιμοποιώντας μια κεντρική υπηρεσία διαχείρισης DNS.
- Για να συμπληρώσει τις προσπάθειες μετριασμού, η συνεργασία μεταξύ KRCERT, ISP και προμηθευτών πηρεσιών ασφάλειας πληροφορικής επιδιώκεται μέσω της γνωστοποίησης των τελικών χρηστών των μολύνσεων και παρέχοντάς τους τα εργαλεία αφαίρεσης για τον καθαρισμό των συστημάτων τους.

Εκτός από αυτές τις προσπάθειες, η Κορέα έχει δημιουργήσει το E-Call Center 118, μια δωρεάν τηλεφωνική γραμμή έκτακτης ανάγκης για το χειρισμό των περιστατικών Internet. Οι χειριστές του τηλεφωνικού κέντρου είναι εκπαιδευμένοι να παρέχουν συμβουλές σχετικά με την απομάκρυνση του κακόβουλου λογισμικού, για την αντιμετώπιση, ή τον εντοπισμό, spam email, και να δίνει απαντήσεις σε ερωτήσεις σχετικά με την τεχνολογία και την προστασία της ιδιωτικής ζωής στο Διαδίκτυο γενικότερα.

3.4.2 Πρωτοβουλίες σε διεθνές επίπεδο

Σε αυτή την παράγραφο παρουσιάζονται, επιλεγμένες πρωτοβουλίες και έργα κατά των botnet με παγκόσμιο προσανατολισμό.

ITU Botnet Mitigation Toolikit

Το 2007, η ITU ξεκίνησε την ανάπτυξη ενός Toolkit για τον μετριασμό των Botnet. Αυτή η ομάδα εργαλείων χαρακτηρίζει την απειλή των botnet γενικά, και παρέχει συστάσεις για την αντιμετώπιση του προβλήματος σε διάφορα επίπεδα. Χωρίζει σε τρεις πτυχές το προβλήμα: **πολιτικές, τεχνικές** και **κοινωνικές**.

- Η ενότητα σχετικά με την **πολιτική** άπτεται της νομικής κατάστασης, προωθεί την πιο διαδεδομένη αρμοδιότητα στο χειρισμό του εγκλήματος στον κυβερνοχώρο, προωθεί τη συνεργασία μεταξύ των ομάδων των ενδιαφερομένων και παρέχει γνώσεις σχετικά με την ισορροπία μεταξύ της προστασίας της ιδιωτικής ζωής των χρηστών και την ασφάλεια γενικότερα.
- Στο **τεχνικό** τμήμα, δίδεται μια γενική επισκόπηση σχετικά με την ανίχνευση botnet και την έρευνα, ο ρόλος των ISP, μητρώων ονομάτων τομέα και των καταχωρητών

περιγράφεται και ο ρόλος των χρηματοπιστωτικών ιδρυμάτων στην ανάπτυξη ικανοτήτων για το μετριασμό των botnet παρουσιάζεται.

- Τέλος, τα **κοινωνικά** μέτρα περιλαμβάνουν την έναρξη ευρείας κλίμακας εκστρατειών που στοχεύουν στην ευαισθητοποίηση των χρηστών και τη χρήση οπτικών μέσων ώστε να καταστούν πιο προσβάσιμες. Αυτά επίσης υποδεικνύουν το πως θα γίνει πιο εύκολη η απόκτηση κα εγκατάσταση λογισμικού προστασίας καθώς και τη δημιουργία μιας νοοτροπίας για την εκτέλεση τακτικών ενημερώσεων λογισμικού.

ITU-T CYBEX

Η τυποποίηση μιας συνολικής προσέγγισης για ένα πλαίσιο, αποτελεί το αντικείμενο με το οποίο ασχολείται το ITU-T, Το πλαίσιο αυτό είναι το Cybersecurity Information Exchange Framework (CYBEX). Το πλαίσιο επικεντρώνεται στην ανάπτυξη δεσμών επικοινωνίας μεταξύ διαφορετικών οργανισμών ασφάλειας στον κυβερνοχώρο μέχρι το ίδιο επίπεδο, στην εξάλειψη σφαλμάτων που προκαλούνται από την έλλειψη κατανόησης και στην ανάπυτξη των αυτοματοποιημένων διαδικασιών. Οι πληροφορίες είναι δομημένες και συγκεντρωμένες ανάλογα με τους τομείς ενδιαφέροντος. Οι οργανισμοί θα πρέπει να αναγνωρίζεται από ένα μοναδικό αναγνωριστικό αντικειμένου, καθιστώντας τις υπηρεσίες και τις πηγές πληροφόρησης πιο εύκολες στην εύρεση.

3.4.3 Στοχευμένες ομάδες εργασίας

Προκειμένου να αντιμετωπιστούν τα botnet και οι απειλές που επιφέρουν οι δράσεις τους, έχουν αναπτυχθεί ομάδες εργασίες που ασχολούνται αποκλειστικά με την καταπολέμηση μεγάλων και σημαντικών botnet. Αυτές οι ομάδες αποτελούν έξοχα παραδείγματα όπου η συνεργασία οδήγησε τελικά στο κλείσμο μεγάλων Botnet όπως τα Conficker, Mariposa, και Waledac. Αυτές οι ομάδες εργασίας είναι οι

- Conficker Working GRoup
- Mariposa Working Group
- Operation B49.

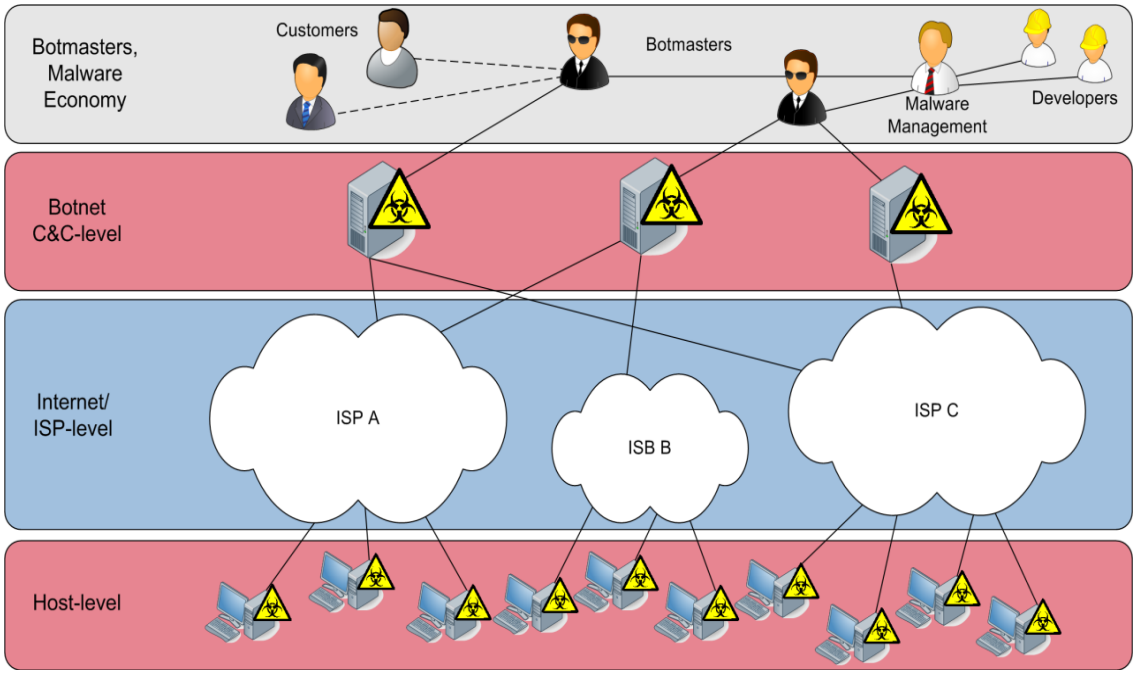
3.5 Ανάλυση και αξιολόγηση των προσεγγίσεων αντιμετώπισης και μετριασμού των botnet

Στην ενότητα αυτή, οι προσεγγίσεις που παρουσιάζονται για την αντιμετώπιση της απειλής των botnet αναλύονται και συγκρίνονται.

Όλα τα αντίμετρα λειτουργούν σε διαφορετικά επίπεδα της επικοινωνιακής υποδομής. Ενώ ορισμένες προσεγγίσεις μπορεί να στοχεύουν στους C&C server, (π.χ. takedown ή DNS-sinkholing), και κατά συνέπεια δουλεύνκατά της ανώτερης βαθμίδας της τεχνικής υποδομής, άλλες αρχές, όπως οι walled garden, μπορεί να περιλαμβάνουν τους μολυσμένους host και ως εκ τούτου να στοχεύουν στα γενεσιουργά αιτία (σχήμα 16). Άλλα στοχεύουν τους εγκληματίες που βρίσκονται πίσω από τα botnet άμεσα, για παράδειγμα μέσω της νομοθεσίας και των κανονισμών για το ηλεκτρονικό έγκλημα.

Μια γενική παρατήρηση είναι ότι, αν και πολλές προσεγγίσεις είναι καλά δομημένες, η εφαρμογή τους σε μεγάλο βαθμό περιορίζεται από διάφορους νόμους και τις διαφορές στη νομοθεσία και την ερμηνεία της σε διασυνοριακό επίπεδο, μειώνοντας την αποτελεσματικότητά τους με την εισαγωγή καθυστερήσεων που επηρεάζουν τον χρόνο αντίδρασης ή απαγορεύουν την εφαρμογή τους.

Επίσης, είναι σημαντικό να σημειωθεί ότι πολλές από αυτές τις προσεγγίσεις είναι συνδεδεμένες με τις τεχνικές ανίχνευσης, διότι, σε πολλές περιπτώσεις, οι σχετικοί στόχοι πρέπει να πρώτα να προσδιορίζονται πριν από ενεργοποίηση και εφαρμογή των κατάλληλων αντιμέτρων.



Σχήμα 16: Επίπεδα λειτουργίας Botnet [Enisa 2001]

Σε ότι αφορά τα γενικά χαρακτηριστικά των αντιμέτρων αξίζει να σημειωθούν τα εξής:

- Η ομάδα των αντισταθμιστικών μέτρων που βασίζονται σε αλλαγές στη συνδεσιμότητα, όπως τα blackholing, sinkholing, και το φιλτράρισμα πακέτων, προσφέρουν καλή γενικότητα, δεδομένου ότι δεν εξαρτώνται από τα ιδιαίτερα χαρακτηριστικά ορισμένων botnet ή τους τύπους botnet.
- Η ομάδα των αντισταθμιστικών μέτρων που στοχεύουν ειδικούς τύπους, ή τις υποδομές των botnet είναι φυσικά λιγότερο γενικά, αλλά πλεονεκτούν δεδομένου ότι η αποτελεσματικότητα τους αυξανεί ακριβώς λόγω της εξειδίκευσης τους.
- Το αντίμετρο των takedown μπορεί να εφαρμοστεί μόνο σε κεντρικοποιημένα στοιχεία των botnet
- Τα takedown των C&C server είναι μια βιώσιμη προσέγγιση, η οποία συχνά μπορεί να εφαρμοστεί, διότι η πλειοψηφία των botnet διαθέτουν μια κεντρική αρχιτεκτονική που θα μπορούσε να αποτελείται από έναν ή περισσότερους C&C server.
- Προσεγγίσεις που στοχεύουν σε peer-to-peer υποδομές επικοινωνίας μπορεί να είναι χρήσιμες σε έρευνες botnet , αν και μόνον αν, χρησιμοποιείται αυτό το είδος του πρωτοκόλλου
- Οι νόμοι για το έγκλημα στον κυβερνοχώρο πρέπει να έχουν παγκόσμιο προσανατολισμό και πρέπει να παρέχουν ευελιξία, ώστε να αντιμετωπίζουν τη με γρήγορο ρυθμό εξέλιξη της εγκληματικότητας στον κυβερνοχώρο.

- Λαμβάνοντας άποψη ότι τα botnet είναι οργανωμένα σε παγκόσμιο επίπεδο, μόνο οι προσπάθειες παγκόσμιου χαρακτήρα μπορούν να προσφέρουν μια ικανοποιητική απάντηση και να έχουν σημαντική επιτυχία σε μακροπρόθεσμη βάση.

Για την αξιολόγηση των αποτελεσμάτων της εφαρμογής αντιμέτρων πρέπει να δοθεί πρώτα ένας ορισμός της επιτυχίας. Για την ανάλυση αυτή, εξετάζονται **τρία μέτρα**:

1. Η χρηστικότητα του botnet όσον αφορά την ικανότητα του botmaster να έχει πρόσβαση στη υποδομή C&C και για το χειρίζεται τα bot.
2. Ο αριθμός των σε λειτουργία bot. Αυτό στοχεύει συγκεκριμένα στις τεχνικές που οδηγούν στην απολύμανση των συστημάτων.
3. Η διαθεσιμότητα των ροών εσόδων των botmaster. Δεδομένου ότι το οικονομικό όφελος είναι το κύριο κίνητρο για τους εγκληματίες του κυβερνοχώρου, η πρόκληση εμποδίων και δυσκολίιών για αυτούς στο να εξαγάγουν χρήματα από τα botnet τους είναι επίσης ένα μέτρο της επιτυχίας.

Με ποιοτικούς όρους λοιπόν, θα πρέπει να λαμβάνονται υπό τα παρακάτω:

- Μια προσέγγιση τύπου takedown της υποδομής C&C δεν λύνει το πρόβλημα των μολυσμένων host.
- Η αξιολόγηση της επιτυχίας των προσεγγίσεων μετρίασης θα πρέπει να περιλαμβάνει τον καθαρισμό των υπολογιστών-θυμάτων.
- Ακόμη και ένας ακάλυπτος ή κάποιος C&C εξυπηρετητής που δεν έχει ανιχνευθεί μπορεί να δώσει στον botmaster την ευκαιρία να επανακτήσει τον έλεγχο του botnet.
- Οι walled garden και τα συστήματα κοινοποίησης είναι αποτελεσματικά, διότι φτάνουν στον τελικό χρήστη. Η καθοδήγηση του χρήστη μπορεί να βελτιώσει τον ρυθμό καθαρισμού.
- Μόνο οι μακροπρόθεσμες δράσεις που συντονίζονται σε διεθνές επίπεδο μπορούν να παράγουν αποτελεσματικά αντίμετρα.
- Η χειραγώγηση των απομακρυσμένων συστημάτων ηλεκτρονικών υπολογιστών απαγορεύεται από το νόμο σε όλες σχεδόν τις χώρες, καθιστώντας την προσέγγιση αυτή εφαρμόσιμη μόνο στη θεωρία υπό τις παρούσες συνθήκες.
- Η συνεργασία μεταξύ των διαφόρων φορέων είναι ουσιώδης για την επιτυχία της μετρίασης των botnet.

Η εφαρμογή των αντισταθμιστικών μέτρων σχετίζεται με διάφορες πτυχές της προσπάθειας και της ανάγκης σε πόρους για να εξασφαλιστεί η αποτελεσματική και αποδοτική λειτουργία τους. Ως προς τις πτυχές αυτές, πέντε μεγάλες κατηγορίες μπορούν να διακριθούν: τεχνική, αναπτυξιακή και διοικητική προσπάθεια και πόροι υπό τη μορφή τεχνογνωσίας και χρηματοδότησης. Ως προς την απαραίτητη προσπάθεια και ανάγκη πόρων σημειώνονται συνοπτικά τα εξής:

- Στην περίπτωση των τεχνικών απαιτήσεων υλικού και λογισμικού, μπορεί να παρατηρηθεί ότι οι περισσότερες προσεγγίσεις προϋποθέτουν ελάχιστα από αυτά.
- Οι περισσότερες προσεγγίσεις απαιτούν σημαντικές προσπάθειες ανάπτυξης και προσαρμογής.
- Η συνδιασμένη εξειδικευμένη γνώση στον τεχνικό, νομικό και κοινωνικό τομέα είναι η βασική προϋπόθεση για την αποτελεσματική εφαρμογή των αντιμέτρων κατά των botnet.

- Πρέπει να εξασφαλίζεται συμβατότητα με τα υπάρχοντα πλαίσια, όπως η εσωτερική πολιτική για την ασφάλεια και την προστασία προσωπικών δεδομένων, και η νομοθεσία.
- Θα πρέπει να βελτιωθεί η διεθνής συνεργασία και ανταλλαγή πληροφοριών.
- Τα αντίμετρα κοινωνικής βάσης έχουν το υψηλότερο οικονομικό κόστος από όλες τις προσεγγίσεις που παρουσιάστηκαν.

4 ΤΟ ΜΕΛΛΟΝ

4.1 Τάσεις

Ως επί το πλείστον, οι προβλέψεις για πιθανές μελλοντικές τάσεις στα botnet, προκύπτουν από τις παρατηρήσεις των πρόσφατων εξελίξεων και από τη συμβολή εμπειρογνωμόνων.

Περαιτέρω εμπορευματοποίηση της Βιομηχανίας Malware

Είναι πολύ πιθανό ότι οι υφιστάμενες μορφές οικονομίας στην επιχείρηση του κακόβουλου λογισμικού θα γίνουν ακόμα πιο ξεκάθαρες. Το πιο πρόσφατο παράδειγμα αυτού είναι η υπόθεση εξαγοράς του “ZeuS” ενός κιτ κατασκευής τραπεζικού malware από το ανταγωνιστικό προϊόν SpyEye. Σύμφωνα με το άρθρο, ένας λόγος για τη συγχώνευση αυτή θα μπορούσε να είναι οι πρόσφατες συλλήψεις των botmaster οι ποίοι χρησιμοποίησαν το “ZeuS” για οικονομικό όφελος, της τάξης των περίπου μερικών εκατομμυρίων ευρώ. Την πώληση θα μπορούσε, επομένως, να επιχειρήσει ο συγγραφέας του “ZeuS” για να καλύψει τα ίχνη του, ως μέτρο προφύλαξης κατά της σύλληψης. Η αντιπαλότητα μεταξύ των δύο αυτών σετ κατασκευής έχει τεκμηριωθεί καλά. Πριν από τη συνένωση, οι πρόσφατες εκδόσεις του SpyEye ολοκληρώθηκαν με ένα χαρακτηριστικό που θα διενεργεί έλεγχο για την παρουσία του ZeuS σε ένα σύστημα, που αφού το αφαιρέσει, στη συνέχεια το αντικαταθιστά με τον εαυτό του. Εικάζεται από αυτές τις παρατηρήσεις πως η οικονομία malware θα υιοθετήσει όλο και περισσότερο τις αρχές της οικονομίας της αγοράς.

Αύξηση χρήσης Botnet

Τα οικονομικά μοντέλα της ενοικίασης και μεταπώλησης botnet μέσω pay-per-install υπηρεσιών μπορεί επίσης να γίνει ακόμη πιο διαδεδομένη. Αυτά επιτρέπουν την ταχεία δημιουργία νέων botnet που με τη σειρά τους γιγαντώνονται. Τα νέα botnet γίνονται έτσι ανεξάρτητα από το botnet που ήταν υπεύθυνο για την αρχική μόλυνση τους. Ένα πλεονέκτημα αυτής της προσέγγισης για τους botmaster είναι ότι ο κίνδυνος της ανίχνευσης μπορεί να μειωθεί περαιτέρω. Μπορεί να αποφευχθεί η σάρωση και η συμπεριφορά διάδοσης, η οποία ωφελεί τη λειτουργία των μικρότερων και εξειδικευμένων botnet.

Η διαθεσιμότητα των bot προς πώληση σε μια ανοικτή αγορά, ανοίγει την αγορά botnet σε botmaster υποδεέστερους τεχνικά. Μπορεί επίσης να χρησιμεύσει ως σημείο εισόδου για τα κόμματα με πολιτικά συμφέροντα, χρησιμοποιώντας botnet ως μέσο πολιτικής επιρροής ή τρομοκρατία.

Τα τελευταία χρόνια υπάρχει μια τάση για botnet που θα χρησιμοποιηθούν σε ένα πολιτικό πλαίσιο. Πολλαπλές επιθέσεις παρατηρήθηκαν κατά κυβερνητικών ιστοσελίδων και εθνικά οικονομικών συμφερόντων. Χαρακτηριστικά παραδείγματα είναι οι επιθέσεις στο 2007 εναντίον της Εσθονίας, το 2008 κατά της Γεωργίας, ή το 2009 κατά της Νότιας Κορέας. Στην περίπτωση της Νότιας Κορέας, τα θύματα-κόμβοι που χρησιμοποιήθηκαν για την εκτέλεση της επίθεσης, είχαν εντολή να κατεβάσουν ένα άλλο δυαδικό malware. Αυτή το πρόσθετο malware ήταν προγραμματισμένο να γράψει στο σκληρό δίσκο του μολυσμένου ξενιστή με το μήνυμα «memory of independence day», ακολουθούμενο από ένα ατελείωτο βρόχο του χαρακτήρα "U", που έχει ένα δυαδικό ισοδύναμο του "01010101", προκειμένου να καταστεί ο προσβεβλημένος υπολογιστή άχρηστος.

Σε αυτές τις πολιτικά υποκινούμενες επιθέσεις, η χρήση των botnet πρέπει να διαχωρίζονται σαφώς από το φαινόμενο του “hacktivism”. Γενικά στην περίπτωση του hacktivism, συμπαθούντες συνεισφέρουν εθελοντικά τους ιδίους πόρους τους σε δράσεις. Πρόσφατα παραδείγματα αυτού του φαινομένου είναι οι επιθέσεις που οργανώνονται από

τους “Anonymous”, στο πλαίσιο της υπόθεσης WikiLeaks. Για παράδειγμα, τα χρηματοπιστωτικά ιδρύματα τα οποία σταμάτησαν να δέχονται μεταφορές χρημάτων σε WikiLeaks ήταν στόχος σε συντονισμένες επιθέσεις DDoS με εργαλεία όπως το “Low Orbit Ion Cannon”. Θα πρέπει να σημειωθεί, ωστόσο, ότι αν και έχουν κοινά χαρακτηριστικά, δεν ταιριάζουν με τον ορισμό ενός botnet, εφόσον η συμμετοχή είναι εντελώς εθελοντική .

Κακόβουλο λογισμικό και botnet σε κινητά τηλέφωνα

Μια πρόβλεψη που σχετίζεται με την διαρκώς αυξανόμενη διαθεσιμότητα κινητής πρόσβασης στο Διαδίκτυο αφορά την αυξανόμενη πιθανότητα ότι τα smartphone θα τεθούν σε κίνδυνο σε μεγάλη κλίμακα. Τα Smartphone είναι ελκυστικά στους εγκληματίες, λόγω της αύξησης της υπολογιστικής ισχύος των συσκευών και της ικανότητας να συνδέονται στο Internet. Μερικές εκθέσεις σχετικά με τη στόχευση των τηλεφώνων από κακόβουλο λογισμικό εμφανίστηκε ήδη από το 2001. Παραδείγματα από την αυτόματη εξάπλωση του κακόβουλου λογισμικού μεταξύ κινητών τηλεφώνων εμφανίστηκε στο 2009. Η εξάπλωση του worm υποστηρίχθηκε από την πρόσβαση στα προσωπικά στοιχεία επικοινωνίας που ήταν αποθηκευμένα σε μολυσμένα τηλέφωνα. Ωστόσο, χρειαζόταν και η αλληλεπίδραση του χρήστη για να μπορέσει να εξαπλωθεί.

Μεταξύ άλλων παραγόντων, τα ακόλουθα, προκαλούν το ενδιαφέρον των προγραμματιστών malware και botmaster για τις κινητές συσκευές:

- Οι χρήστες έχουν περισσότερη εμπιστοσύνη στα μηνύματα που προέρχονται από ανθρώπους που έχουν προσωπικές σχέσεις με τους. Αυτό είναι ένα γεγονός που είχε ήδη παρατηρηθεί νωρίτερα με την εξάπλωση, μέσω των κοινωνικών δικτύων του e-mail worm και κακόβουλου λογισμικού και μπορεί να καταστεί ευκολότερη η διάδοση του malware.
- Αν και οι φορητές συσκευές παρέχουν λιγότερο εύρος ζώνης και λιγότερο αξιόπιστη συνδεσιμότητα από τα άλλα συστήματα ηλεκτρονικών υπολογιστών, έχουν αναλάβει πλέον το ρόλο ενός συστήματος προσωπικών πληροφοριών. Αυτό τους καθιστά ελκυστικούς για την κλοπή ταυτότητας και η απάτη.
- Εκτός από την τηλεφωνία, τα Smartphone συνήθως έχουν πολλαπλές διεπαφές δικτύου, όπως WiFi ή Bluetooth. Αυτά είναι επιπλέον φορείς διάδοσης.
- Η ανάπτυξη ενημερώσεων και αναβαθμίσεων σε κινητές συσκευές δεν είναι τόσο απλές, όπως οι χρήστες έχουν εμπειρία με τους υπολογιστές τους. Αυτό μπορεί να οδηγήσει σε λιγότερο καλά “πατσαρισμένες” κινητές συσκευές και να αυξήσουν την εκμετάλευση των τρωτών σημείων και ευπαθειών.
- Η ανίχνευση malware και οι μηχανισμοί άμυνας για κινητές συσκευές δεν έχουν τόσο ευρέως αναπτυχθεί όπως ισοδύναμα υπάρχουν λύσεις για τους υπολογιστές. Αυτό είναι ένα πρόβλημα που αργά ή γρήγορα θα αντιμετωπίσουν όλες οι συσκευές με δυνατότητα σύνδεσης στο Internet.

Πρωτόκολλο Ipv6

Με τη προβλεπόμενη μεγάλης κλίμακας υιοθέτηση του Ipv6, αναμένεται ότι η τεχνολογία αυτή θα γίνει ολοένα και πιο σημαντική για τους εγκληματίες του κυβερνοχώρου. Σενάρια όπως η συγκάληψη καναλιών για την επικοινωνία C&C είναι πιθανά. Κάτι τέτοιο θα εκμεταλλεύεται τη μετράφραση των διευθύνσεων IP μεταξύ της έκδοσης 4 και της 6 παρακάμπτοντας τα μέτρα ασφαλείας.

Η στοίβα πρωτοκόλλων του IPv6 παρέχει επίσης νέους φορείς για τις επιθέσεις πρωτοκόλλου που θα μπορούσαν να χρησιμοποιηθεί σε DoS και DDoS.

Σημειώνεται ότι το IPv6 προσφέρει διευρυμένο χώρο διευθύνσεων από 32 σε128 bit, δυνατότητα μαρκαρίσματος των ροών κίνησης (Flow Label) και νέες δυνατότητες για την ασφάλεια (Authentication και Privacy)

Εξελίζεις στη δομή και τη διάδοση των botnet

Μια άλλη πρόβλεψη βασίζεται στις παρατηρήσεις της ποικιλίας και της ταχύτητας με την οποία μεφανίζονται νέα δείγματα κακόβουλου λογιμσικού. Αυτά τα υψηλά ποσοστά εμφάνισης νέων εκδόσεων είναι ευφικτά μέσω των ενοιών του πολυμορφισμού και μεταμορφισμού. Μια τάση που παρατηρείται τα τελευταία χρόνια είναι οι αλλαγές στον κώδικα που εκτελούνται μόνο για κακόβουλους διακομιστές, που αποκρύπτουν κατά συνέπεια τους ακριβείς μηχανισμούς τροποποίησης από τους ερευνητές κατά του κακόβολου λογισμικού. Το δείγμα το κακόβουλο λογσιμικού προσαρμόζεται στον host-στόχο. Αυτό επιδρά σημαντικά στις μεθοδολογικές προσεγγίσεις αυτόματης ανίχνευσης διότι το κακόβουλο λογισμικό μπορεί να εξεταστεί μόνο παρουσία των παραμέτρων του συστήματος για τις οποίες παράχθηκε.

Επίσης, θα πρέπει να αναμένεται η άφιξη νέων τεχνικών στη δομή C&C. Υπηρεσίες και το cloud hosting μπορούν να παραβιαστούν και να λειτουργούν ως νέα εργαλεία για τη δημιουργία προσωρινών καναλιών και τομέων C&C. Ομοίως και το περιεχόμενο Web 2.0 και οι υπηρεσίες παρόχων, όπως τα πρώτα πειραματικά δείγματα για τα Twitter ή Facebook.

Οι αναδυόμενες τεχνολογίες web όπως το HTML5 εισάγουν νέες ετικέτες περιεχομένου που είναι πιθανό να παρακάμψουν τις υπάρχουσες blacklist που δεν έχουν ενημερωθεί. Επίσης, η ιδέα των WebSocket παρέχει τη δυνατότητα να παραβιαστεί για κακόβουλες χρήσεις. Αυτό περιλαμβάνει ζητήματα που πιθανόν να προκύψουν από συσκευές που δεν είναι συμβατές με τις επιθέσεις διακομιστών διαμεσολάβησης (proxy attacks), εκθέτωντας τα συστήματα πίσω από τη NAT στο Internet.

Σε περιορισμένο βαθμό, τα botnet μπορεί να δημιουργηθούν εξ ολοκλήρου σε JavaScript, και έτσι να είναι ανεξάρτητα από το υποκείμενο λειτουργικό σύστημα.

4.2 Συστάσεις-Στόχοι

Στην ενότητα αυτή συμπυκνώνονται οι συστάσεις για την ορθή πρακτική κατά την καταπολέμηση της απειλής των botnet. Οι συστάσεις βασίζονται σε τεχνικές που έχουν ήδη αναλυθεί για την ανίχνευση, τη μέτρηση, και τα αντίμετρα κατά των botnet.

Μια περιληπτική εικόνα της απειλης των botnet έχει ως εξής, το κακόβουλο λογισμικό και τα botnet αναγνωρίζονται ως ένα παγκόσμιο πρόβλημα και ως εκ τούτου τοποθετούνται σε ένα πολύπλοκο σύστημα με πολλές εξαρτήσεις. Εκατομμύρια συστήματα ηλεκτρονικών υπολογιστών είναι μολυσμένα με συχνά πολλούς τύπους malware. Αυτά τα συστήματα οργανώνονται σε αρκετές εκατοντάδες διαφορετικά botnet. Για τον μέσο χρήστη, ο προσδιορισμός της μολυνσης υποτίθεται ότι γίνεται αναδρομικά. Αυτό σημαίνει ότι το κακόβουλο λογισμικό δεν έρχεται στην αντίληψη του χρήστη, μέχρι να το βιώσει προσωπικά. Ο χρόνος αντίδρασης για την ανίχνευση του malware, ακόμη και όταν κάποιο anti-malware λογισμικό έχει εγκατασταθεί, είναι μερικές φορές τόσο πολύ μεγάλος που οι μολύνσεις είναι πιθανό να συμβούν λόγω της αποτυχίας εγκατάστασης κρίσιμων ή πρόσφατων ενημερώσεων προϊόντος. Το κακόβουλο λογισμικό ξεκινά την επικοινωνία με τους διακομιστών C&C σχεδόν αμέσως, πράγμα που σημαίνει ότι οι παραβιάσεις των σημαντικών πληροφοριών, όπως τα διαπιστευτήρια και οι ταυτότητες μπορεί να συμβεί αμέσως. Αυτές οι πληροφορίες παραβιάζονται από τους botmaster με διάφορους

τρόπους, κυρίως για οικονομικό όφελος. Οι botmaster χρησιμοποιούν διάφορους μηχανισμούς για την ανωνυμία και είναι γενικά δύσκολο να προσδιοριστούν.

Συνεπώς, τα botnet είναι μια σοβαρή απειλή που μπορεί μόνο να αντιμετωπιστεί μέσω της συνεργασίας και της κοινής προσπάθειας όλων των ενδιαφερόμενων μερών. Στην ενότητα αυτή προτείνεται, μια ολοκληρωμένη προσέγγιση για την ελαχιστοποίηση της απειλής των botnet. Αυτή η προσέγγιση αποτελείται από τρεις άξονες:

1. Μετριασμός των υφιστάμενων botnet και των μολύνσεων.
2. Προληπτικά μέτρα που θα επιδεινώνουν την απόκτηση νέων bot και την ανάπτυξη των botnet.
3. Προσεγγίσεις που στοχεύουν στη χρηστικότητα των botnet, όπως αυτή εκλαμβάνεται από μέρους των botherder.

Σημειώνεται ότι η ενισχυμένη συνεργασία είναι θεμελιώδους σημασίας για όλους τους τομείς του μετριασμού, ενώ όλες οι συστάσεις που αφορού τα botnet έχουν ως στόχο το status quo.

Από τεχνικής άποψης για τον μετριασμό των υφιστάμενων botnet, στόχο αποτελούν τα υπονομευμένα συστήματα και οι δομές C&C μαζί με τα άτομα που ευθύνονται για αυτά.

Απαιτούμενες δράσεις που προτείνονται είναι:

- Σύλληψη των εγκληματιών που κρύβονται πίσω από τα botnet.
- Βελτίωση των εργαλειών ανάλυσης κακόβουλου λογισμικού.
- Συνεχής διασπορά και διαμοιρασμός πληροφορίας και τεχνογνωσίας.
- Εναρμόνιση νομοθεσίας κατά του ηλεκτρονικού εγκλήματος σε διεθνές επίπεδο.
- Μείωση των υφιστάμενων μολύνσεων.
- Ανίχνευση βασισμένη στους ISP και ειδοποίηση.

Για την πρόληψη νέων μολύνσεων οι δράσεις που προτείνονται είναι οι εξής:

- Επιβράδυνση της διάδοσης των botnet.
- Διαχείριση των ευάλωτων σημείων και προστασία του συστήματος.

Για τη μείωση του κέρδους των botnet και του ηλεκτρονικού εγκλήματος κρίνονται απαραίτητα:

- Δέσμευση των σχημάτων που δημιουργούν προστιθέμενη αξία και οικονομικά οφέλη στους χρήστες του κακόβουλου λογισμικού
- Ευαισθητοποίηση σε θέματα ασφαλείας
- Υπεύθυνος χειρισμός των μολύνσεων
- Βελτίωση της καταπολέμησης της απάτης
- Δίωξη και την αποτροπή

4.3 Προβλέψεις

Σύμφωνα με το Κέντρο Ασφαλείας GTISC (Georgia Tech Information Security Centre), ένα από τα πλέον αξιόπιστα ερευνητικά ιδρύματα στην Ατλάντα των ΗΠΑ, οι κυριότερες επιθέσεις που αναμένεται να εκδηλωθούν στον κυβερνοχώρο το 2011 αφορούν σε υψηλής αποτελεσματικότητας κακόβουλο λογισμικό τύπου botnet, επιθέσεις σε **κινητές συσκευές**, κοινωνικά δίκτυα (social network, web 2.0) και επιθέσεις σε συστήματα που συνδέονται με την κρίσιμη υποδομή μιας χώρας (π.χ. δίκτυα παροχής ηλεκτρικού ρεύματος, πυρηνικούς σταθμούς κ.ά.).

Είναι αναμενόμενο ότι όσο η διάδοση των υπολογιστών Mac και των 'έξυπνων' **κινητών τηλεφώνων** θα συνεχίζεται και οι τεχνολογίες τους θα αναπτύσσονται, τόσο περισσότεροι εισβολείς θα ασχολούνται με τη δημιουργία κακόβουλου λογισμικού που θα εκμεταλλεύεται τα ευπαθή σημεία αυτών των συσκευών.

Αναλυτικότερα, το Fast Flux είναι μια τεχνική που χρησιμοποιείται από μερικά δίκτυα bot, όπως το Storm botnet, για την απόκρυψη, κακόβουλων και phishing, ιστοσελίδων πίσω από ένα διαρκώς μεταβαλλόμενο δίκτυο κεντρικών υπολογιστών, οι οποίοι λειτουργούν ως proxy. Η χρήση ενός συνδυασμού δικτύων peer-to-peer, κατανεμημένων εντολών και ελέγχου, τεχνικών μέσω διαδικτύου εξισορρόπησης φορτίου και ανακατεύθυνσης των proxy, καθιστά δύσκολο τον εντοπισμό της αρχικής γεωγραφικής θέσης των botnet.

Επίσης, το Social engineering αποτελεί ένα από τα κύρια μέσα επιθέσεων που χρησιμοποιούνται σήμερα, ενώ με τη διάδοση των δικτυακών τόπων κοινωνικής δικτύωσης, οι οποίοι συνεχίζουν να παρουσιάζουν άνευ προηγουμένου ανάπτυξη, θα πρέπει να αναμένεται ότι οι απόπειρες εξαπάτησης των χρηστών των δικτυακών τόπων θα αυξάνονται ανάλογα.

Τέλος, οι αποστολείς spam θα συνεχίζουν να παραβιάζουν τους κανόνες**.** Καθώς η οικονομία συνεχίζει να βρίσκεται σε ύφεση, όλο και περισσότεροι άνθρωποι επιδιώκουν να εκμεταλλευτούν τις χαλαρές διατάξεις του νόμου για την καταπολέμηση του spam.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Τα botnet ορίζονται ως δίκτυα υπολογιστών που ελέγχονται με απομακρυσμένη πρόσβαση από τον botmaster έχοντας υπονομεύσει τα συστήματα χωρίς τη γνώση ή την έγκριση των κατόχων τους. Οι botmaster χρησιμοποιούν αυτούς του υπολογιστές-ζόμπι για διάφορους παράνομους σκοπούς, αφού έχει τη δυνατότητα πρόσβασης στα αρχεία του συστήματος όσο και τη χρήση της σύνδεσης δικτύου του υπολογιστή, χωρίς να το αντιληφθεί ο ιδιοκτήτης του. Το γεγονός αυτό παρέχει στον botmaster αμέτρητες δυνατότητες, όπως η μετάδοση του κακόβουλου κώδικα bot ή η μαζική αποστολή spam. Επιπλέον, εκτός της υποκλοπής δεδομένων ο botmaster καταφέρνει να αποκρύπτει τη ταυτότητα του αφού ως διακομιστής μεσολάβησης χρησιμοποιείται ο υπολογιστής του θύματος.

Τα botnet 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". Μια απλή επίσκεψη στη μολυσμένη τοποθεσία web αρκεί για τη μετάδοσή της.

Λαμβάνοντας υπόψη το μέγεθος ενός τυπικού botnet, που αποτελείται από μερικές εκατοντάδες έως κάποιες χιλιάδες υπολογιστές-ζόμπι, γίνεται κατανοητή και η η χρήση τους ως όπλο για την εκτέλεση επιθέσεων DDoS. 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.

Επίσης μια ακόμα χρήση των bot είναι αυτή ως διακομιστών web ή FTP για την εξυπηρέτηση διαφόρων σκοπών, όπως η διάθεση μολυσμένων τοποθεσιών web με σκοπό την παροχή περαιτέρω πληροφοριών, ή η χρήση των συστημάτων ανυποψίαστων θυμάτων για δημιουργία πειρατικών αντιγράφων και άλλου κακόβουλου ή παράνομου υλικού.

Ωστόσο, ως προς το μέγεθος της απειλής που μπορεί να προκαλέσει ένα botnet πρέπει να σημειωθεί ότι δεν αρκούν ποσοτικά δεδομένα, αλλά και ποιοτικά. Το μέγεθος δεν είναι το παν, ο αριθμός των μολυσμένων υπολογιστών και μόνο δεν αποτελεί κατάλληλο κριτήριο για την εκτίμηση του βαθμού της απειλής, αφού μικρά δίκτυα μπορούν να προκαλέσουν ζημιές εκατομύριων.

Σχετικά με τη διαχείριση και τον συντονισμό των bot, που πιθανόν είναι διασκορπισμένοι σε παγκόσμια κλίμακα, αυτά μπορούν να γίνει με διάφορους τρόπους.

Οι τρόποι αυτοί σχετίζονται με την εξέλιξη της τεχνολογίας και της αρχιτεκτονικής που χρησιμοποιούν τα botnet. Στα πρώτα botnet χρησιμοποιούνταν οι κεντρικοί διακομιστές εντολών και ελέγχου, σήμερα όμως προτιμώνται όλο και περισσότερο αποκεντρωμένες δομές επικοινωνίας, οι οποίες μοιάζουν με τα γνωστά δίκτυα P2P. Η εξέλιξη αυτή δυσχεραίνει την μετρίαση τους, τόσο σε επίπεδο ανίχνευσης όσο και σε επίπεδο λήψης αντιμέτρων (δεν υπάρχει ένας κεντρικός διακομιστής, του οποίου η απενεργοποίηση θα διέκοπτε τη λειτουργία ολόκληρου του δικτύου, αλλά ένα δίκτυο bot τα οποία επικοινωνούν μεταξύ τους, ενώ το δίκτυο χαρακτηρίζεται από μεγαλύτερη σταθερότητα).

Για τον εντοπισμό και την καταμέτρηση των botnet έχουν αναπτυχθεί παθητικές και ενεργητικές τεχνικές. Η επιλογή της προσέγγισης με την οποία επιχειρείται ο εντοπισμός ενός botnet εξαρτάται από τη δομή και τον τρόπο λειτουργίας του.

Σε ότι αφορά τα αντιμέτρα αυτά διακρίνονται σε τεχνικά, σε κοινωνικού και νομοθετικού χαρακτήρα. Τα τεχνικά αντιμέτρα σχετίζονται άμεσα με τον τύπο του Botnet και τις τεχνικές ανίχνευσης του. Επίσης, μπορούν να φτάνουν μέχρι τον τελικό χρήστη και να τον «από-μολύνουν» ή όχι. Σε ότι αφορά τα κοινωνικά μέτρα η ευαισθητοποίηση και ενημέρωση των χρηστών για την ορθή χρήση του Internet και τη συντήρηση και ενημέρωση των συστημάτων τους, αποτελούν κρίσιμο παράγοντα. Επιπλέον, επισημαίνεται η σημασία που έχει η συνεργασία των κυβερνήσεων με αντίστοιχους οργανισμούς ασφάλειας για την καταπολέμηση των botnet, ενώ η παγκόσμια συνεργασία είναι απολύτως απαραίτητη για την οργάνωση επιτυχούς άμυνας κατά των botnet. Άλλωστε, η σύγχρονη παγκόσμια οικονομία αντιμετωπίζει μια μεγάλη ποικιλία απειλών λόγω κακόβουλου λογισμικού, που μπορούν να προκαλέσουν μεγάλη ζημιά. Επιπλέον, τα botnet έχουν εξελιχθεί σε μια από τις μεγαλύτερες παράνομες πηγές εσόδων στο Internet, ενώ οι εκάστοτε κυβερνήσεις και φορείς ξοδεύουν πολλά εκατομύρια για να τα εξαλείψουν.

Τέλος, οι τάσεις που διαφαίνονται στην ανάπτυξη των botnet και του ηλεκτρονικού εγλήματος γενικότερα, καταδεικνύουν ότι τα έξυπνα κινητά τηλέφωνα και οι εφαρμογές κοινωνικής δικτύωσης αποτελούν τους άμεσους στόχους των botmaster.

ΟΡΟΛΟΓΙΑ

Denial of Service	Άρνηση Υπηρεσίας
Drive-by infection	Μόλυνση με απλή επίσκεψη
Fast-Flux	Πλημηρισμός
Proxy	Πληρεξούσιος
Reverse Engineering	Αντίστροφη Μηχανική
Server	Διακομηστής / Εξυπηρετητής
Smartphone	Έξυπνο τηλέφωνο
Social engineering	Κοινωνική Μηχανική (εκμετάλευση ανθρώπων)
SQL Injection	SQL ένεση
Takedown	Απενεργοποίηση

ΣΥΝΤΜΗΣΕΙΣ – ΑΡΚΤΙΚΟΛΕΞΑ – ΑΚΡΩΝΥΜΙΑ

ACMA	Australian Communications and Media Authority-
AS	Autonomous System
AISI	Australian Internet Security Initiative
ATLAS	Active Threat Level Analysis System
AV	Anti-Virus
BGP	Border Gateway Protocol
BSI	Bundesamt fur Sicherheit in der Informationstechnik (German Federal Office for Information Security)
CCC	Cyber Clean Center
C&C	Control & command
CDN	Content Delivery Network
CERT	Computer Emergency Response Team
CIIP	Critical Information Infrastructure Protection
CPNI	Centre for the Protection of National Infrastructure
DGA	Domain Generation Algorithm
DHCP	Dynamic Host Configuration Protocol
DNS / DDNS	Domain Name System
DoS / DDoS	(Distributed) Denial-of-Service
DPI	Deep Packet Inspection
ENISA	European Network and Information Security Agency
ENISA	European Network and Information Security Agency
FFSN	Fast-Flux Service Networks
HTTP	Hyper-Text Transfer Protocol
IDS / HIDS / NIDS / IPS	Intrusion Detection System (Host-based, Network-based), Intrusion Prevention System
IM	Instant Messaging
IP/IPv6	Internet Protocol, often also used as an abbreviation for an Internet Protocol address (version 6)
IPA	Information Technology Promotion Agency

IRC	Internet Relay Chat
ISAC	Telecom Information Sharing and Analysis Centre Japan
ISC	Internet Systems Consortium
ISP	Internet Service Provider
MD5	Message Digest version 5
NICC	National Infrastructure against Cybercrime
P2P	peer-to-peer
RFC	Request For Comments (IETF standard proposal documents)
RSS	Really Simple Syndication
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
TCP	Transmission Control Protocol
TTL	Time-To-Live
WAN	Wide Area Network

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

[Τελευταία ημερομηνία επιβεβαίωσης online αναφορών 26.09.2011]

1. ITU Study on the Financial Aspects of Network Security: Malware and Spam. ICT Applications and Cybersecurity Division, Policies and Strategies Department, ITU Telecommunication Development Sector, 2008
2. Legal Issues in Botnet Mitigation. ENISA Report, to appear, 2011
3. 2007 Malware Report: The Economic Impact of Viruses, Spyware, Adware, Botnets, and other Malicious Code. Computer Economics, 2007
4. Symantec Global Internet Security Threat Report: Trends for 2009 (Volume XV). Symantec Corp., 2010.
5. Kaspersky Security Bulletin 2009: Malware Evolution 2009
6. Malware: Fighting Malicious Code. Skoudis E., Zeltser L.,2003
7. Eggheads.org - eggdrop development. http://www.eggheads.org/
8. Enisa, Botnets: Detection, Measurement, Disinfection & Defence, 2011
9. Guide on Policy and Technical Approaches against Botnet, Asia-Pacific Economic Cooperation (APEC), Telecommunications and Information Working Group, project, December 2008
10. Schoof R. & Koning R., Detecting peer-to-peer botnets, University of Amsterdam project, 2007
11. Trend Micro, 2006 - TAXONOMY OF BOTNET THREATS
12. Καλαϊτζιδάκης Β. Ανίχνευση δικτύων υπό κακόβουλο έλεγχο κάνοντας χρήση της τεχνολογίας των Honeypot, Οικονομικό Πανεπιστήμιο Αθηνών, 2009.
13. Σιδηρόπουλος Α. Δίκτυα Υπολογιστών υπό Κακόβουλο Έλεγχο (Botnets): Τεχνικές ανίχνευσης και απόκρυψης, Οικονομικό Πανεπιστήμιο Αθηνών, 2009.
14. Τρούλης Ι. Μελέτη Χαμηλής και Υψηλής Αλληλεπίδρασης Honeypot, Ινστιτούτου Πληροφορικής-ΕΚΕΦΕ Δημόκριτος, 2010.
15. CAIDA Internet Data – Real time Monitors http://www.caida.org/data/realtime/
16. Honeypots: Tracking Hackers. Spitzer, L. Addison-Wesley Professional, 2002
17. Conficker Working Group http://www.confickerworkinggroup.org
18. 'Mariposa' Botnet Authors May Avoid Jail Time. Krebs, B. Krebs on Security, 2010. http://krebsonsecurity.com/2010/03/mariposa-botnet-authors-may-avoid-jail-time
19. The Botnet Chronicles - The Botnet Chronicles. Ferguson, R. Trend Micro Whitepaper, 2010.
20. On the Analysis of the Zeus Botnet Crimeware Toolkit. Binsalleeh, H., Ormerod, T., Boukhtouta, A., Sinha, P., Youssef, A., Debbabi, M., Wang, L. In: Proceedings of the 8th Annual Conference on Privacy, Security and Trust, PST'2010, 2010

21. Peer-to-Peer Botnets: Overview and Case Study. Grizzard, J. B., Sharma, V., Nunnery, C., Kang, B., Dagon, D. In: Proceedings of the First Workshop on Hot Topics in Understanding Botnets (HotBots'07), 2007.

22. An Analysis of Conficker's Logic and Rendezvous Points. Porras P., Saidi, H., Yegneswaran, v. Technical Report, SRI International, 2009

23. Taking over the Torpig botnet - Your Botnet is My Botnet: Analysis of a Botnet Takeover," in Proceedings of the ACM CCS, Chicago, IL, November 2009 (Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard Kemmerer, Chris Kruegel, and Giovanni Vigna)

24. Botnet Kit And Service Offered To Non-Techies. CyberInsecure, 2008. http://cyberinsecure.com/botnet-kit-and-service-offered-to-non-techies

25. Learning more about the underground economy: a case-study of keyloggers and dropzones. Holz, T., Engelberth, M., Freiling, F. In: Proceedings of the 14th European conference on Research in computer security (ESORICS'09), 2009

26. Insights from the Inside: A View of Botnet Management from Infiltration. Cho, C.Y., Caballero, J., Grier, C., Paxson, V., Song, D. In: Proceedings of the 3rd Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET'10), 2010

27. Spamalytics: An Empirical Analysis of Spam Marketing Conversion. Kanich, C., Kreibich, C., Levchenko, K., Enright, B., Voelker, G., Paxson, V., Savage, S. In: Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS), 2008

28. The biggest cloud on the planet is owned by ... the crooks. Mullins, R. Network World, 2010 http://www.networkworld.com/community/node/58829

29. Politically Motivated Denial of Service Attacks. Nazario, J. In: The Virtual Battlefield: Perspectives on Cyber Warfare (pp. 163-181), IOS Press, 2009

30. Is Stuxnet the 'best' malware ever? Keizer, G. Computerworld, 2010. http://www.computerworld.com/s/article/9185919/Is Stuxnet the best malware ever ?

31. Snort. An open source network intrusion prevention and detection system (IDS/IPS). SourceFire. http://www.snort.org/

32. Microsoft Security Intelligence Report, Volume 9 (January 1st - June 30th 2010). Microsoft, 2010. http://www.rn icrosoft.com/security/sir

33. SRI Honeynet and BotHunter Malware Analysis - Automatic Summary Analysis Table. SRI http://wasp.csl.sri.com/Honeynet/

34. Botnet Detection by Monitoring Group Activities in DNS Traffic. Choi, H., Lee H., Lee H., Kim H. In: Proceedings of the 7th IEEE International Conference on Computer and Information Technology (CIT '07), 2007

35. Measuring the Perpetrators and Funders of Typosquatting. Moore, T., Edelman, B. In: 14th International Conference on Financial Cryptography, (TC'10), 2010

36. Measurements and mitigation of peer-to-peer-based botnets: a case study on storm worm. Holz, T., Steiner, M., Dahl, F., Biersack, E., Freiling, F. In: Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats (LEET'08), 2008

37. Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC

38. Abuse.ch ZeuS Tracker https://zeustracker.abuse.ch

39. Staysafeonline (National Cyber Security Alliance)

http://www.staysafeonline.org

40. Zeus botnet's Real Host cut off from the internet. Ashford, W. ComputerWeekly, 2009. http://www.com puterweekly.com/Articles/2009/08/04/237165/Zeus-botnets-Real-Host-cut-off-from-the-internet.htm

41. Lessons in Botnets: The After-Effects of ISP Takedowns. Shipp, A. RSA 2010 Conference

42. Common Best Practices for Mitigating Large Scale Bot Infections in Residential Networks. Mody, N., O'Reirdan, M., Masiello, S, Zebek, J. MAAWG, 2009

43. Dynamic port 25 blocking to control spam zombies. Schmidt, J. In: Proceedings of the 3rd Conference on Email and Anti-Spam (CEAS'06), 2006.

44. 10th IEEE/IPSJ International Symposium on Applications and the Internet, 2010

45. Botnet C&C Handling with DNS Sinkhole. Jeong, H. C., Korea Information Security Agency, 2010

46. Best Practices in Anti-SPAM, Advisory document for the ETIS community. ETIS, 2010

47. The Role of Internet Service Providers in Botnet Mitigation - An Empirical Analysis Based on Spam Data. Van Eeten, M., Bauer, J.M., Asghari, H., Tabatabaie, S. OECD, STI Working Paper, 2010

48. Taking Down a Botnet. Amorosi, D. Infosecurity, 2010. http://www.infosecurity-us.com/view/10063/taking-down-a-botnet/

49. Smartphones: Information security risks, opportunities and recommendations for users. Report by ENISA, 2010

50. http://en.wikipedia.org/wiki/Fast_flux