Πανεπιστήμιο Πειραιώς

Τμήμα Ψηφιακών Συστημάτων

Δικτυοκεντρικά Συστήματα

Μελέτη Των Worms

Καθηγητής : Σωκράτης Κάτσικας

Μυλωνάς Εμμανουήλ ΜΕ/07096

Πειραιάς

Νοέμβριος, 2010

ΠΕΡΙΕΧΟΜΕΝΑ

ΠΕΡΙΕΧΟΜΕΝΑ 1
ΠΙΝΑΚΕΣ 3
1. ΕΙΣΑΓΩΓΗ 4
2. ΤΕΧΝΟΛΟΓΙΑ ΤΩΝ ΙΩΝ ΤΥΠΟΥ WORM 5
2.1. Ανάλυση των Ιών Τύπου Worm 5
2.2. Επιλεγμένα Worms 6
2.3. Ταξινόμηση Worms 9
2.4. Ζωτικές Λειτουργίες των Worms 10
2.4.1. Λοίμωξη 10
2.4.2. Επιβίωση 13
2.4.3. Διάδοση 15
2.4.4. Ωφέλιμο Φορτίο 19
3. ΓΝΩΡΙΣΜΑΤΑ ΤΗΣ ΕΠΙΘΕΣΗΣ ΤΩΝ ΙΩΝ ΤΥΠΟΥ WORM 22
4. ΤΕΧΝΙΚΕΣ ΚΑΙ ΜΗΧΑΝΙΣΜΟΙ ΆΜΥΝΑΣ 25
4.1. Τείχη Προστασίας – Φιλτράρισμα Πακέτων 25
4.2. Τείχη Προστασίας – Stateful 25
4.3. Τείχη Προστασίας – Εφαρμογή Proxy 25
4.4. Συστήματα Ανίχνευσης Εισβολέων 26
4.5. Τείχη Προστασίας – Host 26
4.6. Εικονικά Μηχανήματα 26
4.7. Διαμόρφωση 26
4.8. Anti-virus Heuristics 27
4.9. Host-Based Συστήματα Ανίχνευσης Εισβολέων 27
4.10. Έλεγχος Ακεραιότητας 27
4.11. Stackguarding 27
5. ΕΠΙΘΕΣΕΙΣ ΕΝΑΝΤΙΑ ΤΩΝ ΑΜΥΝΩΝ 28
5.1. Πίνακας Άμυνας 29
5.2. Παρατηρήσεις επί του Πίνακα Άμυνας 30
5.2.1. Τείχη Προστασίας – Φιλτράρισμα Πακέτων 30
5.2.2. Τείχη Προστασίας – Stateful 31
5.2.3. Τείχη Προστασίας – Εφαρμογή Proxy 31
5.2.4. Συστήματα Ανίχνευσης Εισβολέων 31
5.2.5. Τείχη Προστασίας-Host 32
5.2.6. Εικονικά Μηχανήματα 32
5.2.7. Διαμόρφωση 32
5.2.8. Anti-virus Heuristics 33
5.2.9. Host-Based Συστήματα Ανίχνευσης Εισβολέων 33
5.2.10. Έλεγχος Ακεραιότητας 34
5.2.11. Stackguarding 34
6. ΑΠΟΤΕΛΕΣΜΑΤΑ 35
6.1. Άμυνα σε Βάθος 35
6.2. Τι έκανα 36
6.3. Η Κατάσταση του Ιού Τύπου Worm 38
7. ΠΑΡΑΔΕΙΓΜΑΤΑ: ΕΦΑΡΜΟΓΗΣ ΑΜΥΝΤΙΚΗΣ ΜΕΘΟΔΟΛΟΓΙΑΣ 40
7.1. YAHA.G 40

7.1.1. Μόλυνση 40
7.1.2. Επιβίωση 40
7.1.3. Διάδοση 41
7.1.4. Ωφέλιμο Φορτίο 41
7.2. SLAMMER 42
7.2.1. Μόλυνση 42
7.2.2. Επιβίωση 42
7.2.3. Διάδοση 43
7.2.4. Ωφέλιμο Φορτίο 43
7.3. BUGBEAR 44
7.3.1. Μόλυνση 44
7.3.2. Επιβίωση 44
7.3.3. Διάδοση 45
7.3.4. Ωφέλιμο Φορτίο 45
7.4. LEAVE 46
7.4.1. Μόλυνση 46
7.4.2. Επιβίωση 46
7.4.3. Διάδοση 47
7.4.4. Ωφέλιμο Φορτίο 47
7.5. NIMDA 48
7.5.1. Μόλυνση 48
7.5.2. Επιβίωση 48
7.5.3. Διάδοση 49
7.5.4. Ωφέλιμο Φορτίο 49
ΒΙΒΛΙΟΓΡΑΦΙΑ – ΠΗΓΕΣ 51

ΠΙΝΑΚΕΣ

Πίνακα 1 – Ευπάθειες που Εκμεταλλεύονται τα Worms..... 12
Πίνακα 2 – Σημαντικά Χαρακτηριστικά του Πολλαπλασιασμού των Worms..... 18
Πίνακα 3 – Ιδιότητες των Ωφέλιμων Φορτίων των Worms 21
Πίνακας 4 – Λεπτομερής Πίνακας Άμυνας..... 29
Πίνακας 5 – Πίνακας Άμυνας..... 37
Πίνακας 6 – Σύνοψη των αποτελεσμάτων της υπόθεσης..... 50

1. ΕΙΣΑΓΩΓΗ

Τα worms του διαδικτύου γίνονται αντιληπτά ως μερικές από τις πρωταρχικές απειλές για την υποδομή του καθώς και για τις πληροφορίες που υπάρχουν στο διαδίκτυο. Πρόκειται για μια σημαντική αιτία ανησυχίας τόσο όσο αφορά την ασφάλεια του δικτύου όσο και την οικονομική προοπτική του. Σύμφωνα με το Κέντρο Πληροφόρησης Worms[1], τα worms Sobig και Blaster, τα οποία εμφανίστηκαν ταυτόχρονα, εκτιμάται ότι κόστισαν στις εταιρείες παραπάνω από δύο δισεκατομμύρια δολάρια.

Σε αυτή την εργασία, θα μελετήσω τρέχουσες στρατηγικές και εφαρμογές κατά των worms και θα προσπαθήσω να εξακριβώσω αν οι τάσεις δείχνουν μια σημαντική επιδείνωση του προβλήματος στο εγγύς μέλλον. Οι τεχνολογίες των worms βελτιώνονται; Γίνονται οι επιθέσεις όλο και πιο πολύπλοκες;

Επίσης, θα ασχοληθώ με τις αμυντικές τεχνολογίες που μπορούν να χρησιμοποιηθούν για την καταπολέμηση του προβλήματος. Που εφαρμόζονται καλύτερα οι αμυντικές τεχνολογίες; Πρέπει άλλες τεχνολογίες να αναπτυχθούν για να βοηθήσουν στην αντιμετώπιση αυτού του προβλήματος; Σε τελική ανάλυση, είναι ενδιαφέρον να ερευνηθεί αν μια εξελιγμένη επίθεση μπορεί να προληφθεί – θα μπορούσαν οι σημερινοί αμυντικοί μηχανισμοί να χρησιμοποιηθούν για την άμυνα έναντι μελλοντικών εξελιγμένων επιθέσεων;

[1] Worm Information Center

2. ΤΕΧΝΟΛΟΓΙΑ ΤΩΝ ΙΩΝ ΤΥΠΟΥ WORM

Πολλά διαφορετικά worms έχουν εμφανιστεί στο διαδίκτυο τα τελευταία χρόνια, επομένως είναι ανέφικτο να μελετήσω όλα αυτά, γι' αυτό επέλεξα ένα υποσύνολο των worms που ελπίζω ότι καλύπτει το σύνολο του τομέα αυτού του κινητού κακόβουλου κώδικα.

Χρησιμοποιώντας αυτό το υποσύνολο, θα αναπτυχθεί μια μέθοδος για να περιγράψω πλήρως αυτά τα κοινά χαρακτηριστικά, τα οποία καλούνται ζωτικές λειτουργίες τους. Η μέθοδος αυτή είναι χρήσιμη όχι μόνο για να περιγράφει τα τρέχοντα worms, αλλά και τα μελλοντικά worms.

Θα περιγραφούν αυτού του είδους τα δεδομένα που συλλέγονται για την εκτέλεση αυτής της μελέτης στην Ανάλυση των Ιών Τύπου Worm που υπάρχει παρακάτω. Το δείγμα των worms που θα επιλεχθεί παρουσιάζεται στην ενότητα Επιλεγμένα Worms και η μεθοδολογία μου για την περιγραφή worms εξηγείται στα τμήματα Ταξινόμηση Worms και Ζωτικές Λειτουργίες.

2.1. Ανάλυση των Ιών Τύπου Worm

Η ανάλυσή κρίνει μόνο τα worms, όπως περιγράφονται από τον Nazario[2], και όχι άλλα είδη ιών κώδικα. Η διάκριση μεταξύ των ιών και worms γίνεται όλο και πιο θολή, αλλά πιστεύω ότι ένα στοιχείο λογισμικού που έχει την ικανότητα να μολύνει άλλα συστήματα με αυτοματοποιημένο τρόπο περιγράφεται καλύτερα ως ένα worm. Αναγνωρίζω ότι τα worms μπορούν επίσης να ενεργοποιηθούν μέσω των μη αυτοματοποιημένων μέσων, σε κάθε περίπτωση, με τα αμυντικά μέτρα που προτείνω να αμυνθούμε κατά των ιών και worms, καθώς και άλλων μορφών κακόβουλου κώδικα.

Έχουν συλλεχτεί πληροφορίες σχετικά με τριάντα διαφορετικά worms που έχουν παρατηρηθεί στο Διαδίκτυο τα τελευταία χρόνια. Τα περισσότερα από τα δεδομένα προέρχονται από προμηθευτές λογισμικού αντιμετώπισης ιών που είναι αναρτημένα στις ιστοσελίδες τους[3]. Το υπόλοιπο μέρος των δεδομένων αποκτήθηκαν από την εργασία άλλων ερευνητών[4] σε επιμέρους worms και από ανεξάρτητη έρευνα μου.

Η συλλογή πληροφοριών θα βοηθήσει στο να απαντηθούν τα ακόλουθα ερωτήματα:

- Ποιες κατηγορίες τρωτών σημείων το worm εκμεταλλεύεται;

[2] J. Nazario, J. Anderson, R. Wash, C. Connelly, “The Future of Internet Worms”,

[3] CERT Coordination Center, F-Secure Virus Info Center, Kaspersky Labs Virus Encylopedia, Network Associates AVERT Virus Information Library, Sophos Virus Information, Symantec Security Response, Trend Micro Virus Encylopedia, Virus Bulletin

[4] CAIDA Analysis of Code Red,
Eeye Blaste Analysis,
D. Moore, C. Shannon, K. Claffy, “Code Red: a case study on the spread and victims of an Internet worm”,
J. Van Hoogstraten, “Blasting Windows: An Analysis of the W32/Blaster Worm”,
E. Manrique, “An Analysis of W32.Bugbear and the Technical Procedural Controls Needed for Protection”,
A. Marinescu, “An Analysis of Simile”,
P. Ferrie, “WHO? WHAT? WHERE? SWEN?”,
P. Ferrie, “Klez”,
Max Vision, “Lion Internet Worm Analysis”,
Max Vision, “Ramen Internet Worms Analysis”

- Πόσο γρήγορα εξαπλώνεται;
- Πώς αποφεύγει την ανίχνευση;
- Μήπως ο ιός τύπου worm έχει μια απομακρυσμένη διοίκηση και ικανότητα ελέγχου;
- Ποιες απαιτήσεις ή προϋποθέσεις είναι απαραίτητες για την επιτυχία του;
- Πόσο δύσκολο ήταν για να αναλυθεί;
- Πόσο πολύπλοκος ήταν ο κώδικας;
- Ποια υπολείμματα μένουν πίσω, όταν ο ιός τύπου worm μολύνει το σύστημα;
- Ο ιός τύπου worm προκαλεί αισθητές παρενέργειες;

2.2. Επιλεγμένα Worms

Για το υποσύνολο μας με τα worms, επιλέγω παραδείγματα που θα μπορούσαν να είναι τα πιο αντιπροσωπευτικά από αυτό το χώρο του κινητού κακόβουλου κώδικα. Τα επιλεγμένα worms σημείωσαν τη μεγαλύτερη επιτυχία στην αναπαραγωγή, πολυπλοκότητα, ή ήταν τα πιο βλαβερά για την υποδομή του δικτύου. Επιλέγοντας αυτό το σύνολο των σημερινών worms, ελπίζω να βοηθήσουν ώστε να προληφθούν τα χαρακτηριστικά που μπορεί να έχουν μελλοντικά worms.

Παρακάτω είναι η λίστα με τα επιλεγμένα worms καθώς και μια σύντομη περιγραφή για τους λόγους που επελέγησαν:

BADTRANS : win32 worm που εξαπλώνεται μέσω Application Program Interface (MAPI) εντολών. Στέλνει πληροφορίες για το χρήστη, κωδικούς πρόσβασης και καταγραφής των πλήκτρων.

BLASTER/LOVSAN/MSBLAST[5] : win32 worm που εκμεταλλεύεται την MS RPC DCOM Buffer υπερχείλιση. Επιχείρησε μια κατανεμημένη επίθεση άρνηση εξυπηρέτησης (DDoS) ενάντια στην τοποθεσία της Microsoft η οποία διανέμει ενημερώσεις κώδικα λογισμικού (windowsupdate.com).

BUGBEAR/TANATOS[6] : παρόμοιος με τον BADTRANS, αλλά έχει κάποιες επιπλέον δυνατότητες. Απενεργοποιεί το λογισμικό κατά των ιών και εξαπλώνεται μέσω κοινόχρηστων δικτύων και στέλνει την κυκλοφορία σε εκτυπωτές δικτύου. Έχει, επίσης, μηχανισμούς προστασίας, όπως UPX συμπίεση και πολυμορφικό infector αρχείο.

CODERED[7] : Win32 worm που επιτίθεται στο Microsoft Windows WWW server IIS (Internet Information Services). Ήταν ένα από τα πρώτα worms που έτυχε προσοχής

[5] J. Van Hoogstraten, “Blasting Windows: An Analysis of the W32/Blaster Worm”
[6] E. Manrique, “An Analysis of W32.Bugbear and the Technical Procedural Controls Needed for Protection”.
[7] CAIDA analysis of Code Red και D. Moore, C. Shannon, K. Claffy, “Code Red: a case study on the spread and victims of an Internet worm”

ενώ είναι εκτός της κοινότητας της ασφάλειας του δικτύου λόγω της ταχύτητας του και αποτελεσματικής διάδοσης του.

DUMARU : win32 worm που μολύνει όλα τα EXE αρχεία στους roots drives μολυσμένου συστήματος χρησιμοποιώντας εναλλακτικές ροές δεδομένων για να κλέψουν τον ιό. Περιέχει τη δική του μηχανή SMTP και εμφανίζεται στο χρήστη ως Microsoft Patch.

ETAP/SIMILE [8]: Cross-platform worm που μολύνει και το Windows Portable Executable (PE) καθώς και τα Executable and Linkable Format (ELF). Χρησιμοποιεί μια entry-point τεχνική και ένα εκλεπτυσμένο πολυμορφικό infector αρχείο για να αποφύγει τον εντοπισμό από anti-virus προγράμματα.

FRETHEM : win32 worm που κατεβάζει εντολές από μια ιστοσελίδα για να αλλάξει η συμπεριφορά του. Χρησιμοποιεί τη δική του μηχανή SMTP και κοινωνικές τεχνικές εφαρμοσμένης μηχανικής για να «μάθει» τα ονόματα και τους κωδικούς πρόσβασης των χρηστών.

GIBE/SWEN[9] : win32 worm που μέσω ενός ηλεκτρονικού ταχυδρομείου εμφανίζεται στο χρήστη ως ένα patch ασφαλείας της Microsoft.

HLLW.CAKE : win32 worm που εξαπλώνεται μέσω πολλαπλών δικτύων peer-to-peer, συμπεριλαμβανομένων των KaZaA, Grokster και iMesh. Προστατεύεται από tElock ant-tamper συμπίεση.

JONBARR/PEPEX : Μαζική αποστολή αλληλογραφίας τύπου worm που χρησιμοποιεί τη δική του μηχανή SMTP για αποστολή email που προσποιείται ότι είναι ένα patch της Microsoft. Απλώνεται επίσης-μέσω των διαφόρων δικτύων peer-to-peer, συμπεριλαμβανομένων των KaZaA, eDonkey2000, Μορφέα, και mIRC.

KLEZ[10] : Ένα ευρέως εξαπλωμένο Win32 worm που μολύνει πραγματικές διευθύνσεις ηλεκτρονικού ταχυδρομείου, απενεργοποιεί το λογισμικό anti-virus, και μολύνει συμπιεσμένα αρχεία. Προσποιείται ότι είναι ένα patch από ιούς έναντι του εαυτού
του.

LION[11] : Linux worm που εξαπλώνεται με τη χρήση ενός γνωστού ελαττώματος BIND.

[8] A. Marinescu, “An Analysis of Simile”,
[9] P. Ferrie, “WHO? WHAT? WHERE? SWEN?”
[10] P. Ferrie, “Klez”
[11] Max Vision, “Lion Internet Worm Analysis”

LEAVE : Win32 worm που χρησιμοποιεί μια ήδη υπάρχουσα «πίσω πόρτα» για να μολύνει τα συστήματα. Χρησιμοποιεί πολλαπλά κωδικοποιημένα κανάλια Διοίκησης και Ελέγχου.

LOVELETTER/ILOVEYOU : visual basic email worm που χρησιμοποιεί πολύ αποτελεσματική κοινωνική μηχανική.

MAGISTR : win32 worm με ένα κακόβουλο ωφέλιμο φορτίο που σβήνει τα BIOS σε ένα μολυσμένο σύστημα καθώς και το σκληρό του δίσκο. Χρησιμοποιεί εξελιγμένη προστασία και anti-debugging μηχανισμούς και απενεργοποιεί το Zone Alarm στο προσωπικό firewall.

MIMAIL : Πολύ αποτελεσματικό win32 mass-mailing worm που σαρώνει τα αρχεία του χρήστη για πιθανούς στόχους και χρησιμοποιεί έναν αριθμό διαφορετικών φορτίων καθώς εξαπλώνεται.

MEXER.D : Win32 worm που εξαπλώνεται μέσω πολλαπλών δικτύων peer-to-peer, συμπεριλαμβανομένων των Kazaa και iMesh. Επιχειρεί επίσης να κατεβάσει το ωφέλιμο φορτίο του, από μια σκληρά κωδικοποιημένη ιστοσελίδα.

MYPARTY : Win32 mass-mailing worm που αφήνει ένα trojan στη «πίσω πόρτα» ενός μολυσμένου συστήματος.

NIMDA : εξελιγμένος, γρήγορα εξαπλώσιμος Win32 worm που χρησιμοποιεί τόσο τον πελάτη όσο και τον διακομιστή.

NACHI : Win32 worm που χρησιμοποιεί την ίδια εκμετάλλευση με τον Blaster για να αφαιρέσει τις μολύνσεις του Blaster και μολύνει ευπαθή συστήματα.

NEROMA : Visual Basic worm που χρησιμοποιεί το Outlook για να στείλει ένα μήνυμα 9/11-related (χρησιμοποιεί την εν λόγω ημερομηνία στη επικεφαλίδα του μολυσμένου μηνύματος).

RECORY : Win32 worm που εγκαθίσταται στο τοπικό filesystem και διαδίδεται προσποιώντας ότι είναι ένα anti-virus εργαλείο.

RAMEN[12] : Linux worm που συσσωρεύει από κοινού έναν αριθμό γνωστών explots εναντίον Linux υπηρεσιών, μεταξύ των οποίων είναι οι: Wuftp. LPRng, και rpc.statd.

REPAD : Win32 worm που διαδίδεται μέσω του δικτύου Kazaa.

[12] Max Vision, “Ramen Internet Worms Analysis”

SOBIG.F : Win32 worm που υποκλέβει διευθύνσεις ηλεκτρονικού ταχυδρομείου από μολυσμένα μηχανήματα και πιστεύεται ότι χρησιμοποιεί τεχνικές spamming, για να εξαπλωθεί χρησιμοποιώντας τη δική του μηχανή SMTP. Επιχειρεί να κατεβάσει κώδικα από ένα σύνολο μηχανών κάποια προκαθορισμένη ώρα.

SLAMMER[13] : Win32 worm που εκμεταλλεύεται ένα ελάττωμα στον SQL Server της Microsoft. Εξαπλώνεται πολύ γρήγορα, μολύνοντας το 90% των ευάλωτων μηχανών μέσα σε 10 λεπτά.

SPIDA : Ένα JavaScript worm που χρησιμοποιεί αδύναμα ονόματα χρηστών και κωδικούς πρόσβασης για συμβιβασμό συστημάτων που εκτελούν Microsoft SQL server.

STRANO : Κακόβουλος κώδικας που εξαπλώνεται από κανάλια IRC και μολύνει έγγραφα του Word.

VOTE.K : Καταστρεπτικό mass-mailing worm γραμμένο σε Visual Basic. Χρησιμοποιεί το Outlook Express addressbook και KaZaA για να εξαπλωθεί.

YAHA : Πολυγραφότατος mass-mailing Win32 worm που απενεργοποιεί τα προγράμματα anti-virus και τα προσωπικά firewalls.

2.3. Ταξινόμηση Worms

Θα περιγράψω με έναν απλό τρόπο τους ιούς τύπου worm σύμφωνα με τα κοινά χαρακτηριστικά τους. Τα χαρακτηριστικά τους που ενδιαφέρουν περισσότερο είναι αυτά που θα επιτρέψουν σε έναν αμυντικό μηχανισμό να τους ανιχνεύσει και / ή να αποτρέψει αυτά τα worms. Μέχρι τώρα δεν έχουν υπάρξει πολλές περιπτώσεις όπου η συμπεριφορά των worm δεν έχει περιγραφεί με επίκεντρο τις αμυντικές υποστηρίξιμες συνθήκες.

Ο Nazario[14] ανέλυσε τις λειτουργίες των worms χρησιμοποιώντας έξι γενικά χαρακτηριστικά. Πιστεύουμε ότι τα worms έχουν μια άλλη σημαντική δυνατότητα για την άμυνα που δεν αναφέρεται. Αυτή είναι η ικανότητα ενός ιού τύπου worm να επιβιώσει σε ένα σύστημα και να περάσει απαρατήρητος. Είναι σημαντικό για έναν αμυντικό μηχανισμό να είναι σε θέση να καθορίσει εάν ο κώδικας ενός worm έχει μια σταθερή θέση σχετικά με ένα σύστημα και να το αποτρέψει από να κάνει οποιαδήποτε ζημιά.

Ο Singh[15] επίσης, κατηγοριοποιεί τη συμπεριφορά των worms σε έξι κατηγορίες, τις οποίες αποκαλεί «όργανα» για να συμπίπτουν με τις βιολογικές αναλογίες του worm. Η προσέγγισή του χρησιμοποιεί παραδείγματα visual basic για να περιγράψει τις συμπεριφορές και του ιού και του worm. Ενώ η κατηγοριοποίηση του είναι πλήρης, είναι πολύ πολύπλοκη να τη χρησιμοποιεί για τους σκοπούς μας αυτής μελέτης

[13] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, V. Weaver, “The Spread of the Sapphire/Slammer Worm”
[14] J. Nazario, J. Anderson, R. Wash, C. Connelly, “The Future of Internet Worms”
[15] P. K. Singh “A Physiological Decomposition of Virus and Worms Programs”

Η μέθοδος που θα εφαρμόσω για να περιγράψω τους ιούς τύπου worm χρησιμοποιεί μόνο τα πιο βασικά χαρακτηριστικά που εμφανίζουν. Καταγράφω τις απαιτήσεις που είναι αναγκαίες για τα worms για να αποκτήσουν τον έλεγχο ενός κεντρικού υπολογιστή, διατηρούν τον έλεγχο, διαδίδονται σε άλλους κεντρικούς υπολογιστές, και εκτελούν ένα ωφέλιμο φορτίο. Όλα τα worms πληρούν τις τρεις πρώτες προϋποθέσεις, και τα περισσότερα εκπληρώνουν την τελευταία. Θα περιγράψω λεπτομερώς με παραδείγματα κάθε μία από αυτές τις απαιτήσεις αυτές στην ενότητα Ζωτικές Λειτουργίες παρακάτω.

2.4. Ζωτικές Λειτουργίες των Worms

Σε αυτή την ενότητα θα αναλύσω τα worms με βάση τις ζωτικές λειτουργίες που εκτελούν. Για κάθε λειτουργία, καλύπτω τις τεχνικές που χρησιμοποιούνται σήμερα, αναφέροντας τα πλεονεκτήματα που έχει η κάθε μια. Αυτό θα οδηγήσει στην προοπτική για την κατάσταση των worms και πώς θα μπορέσουμε να αμυνθούμε τελικά από τις επιθέσεις τους. Πιστεύω ότι μπορούμε να ταξινομήσουμε κάθε worm, σύμφωνα με τις ακόλουθες λειτουργίες:

- ✓ Λοίμωξη
- ✓ Επιβίωση
- ✓ Διάδοση
- ✓ Ωφέλιμο φορτίο

2.4.1. Λοίμωξη

Η λοίμωξη αναφέρεται στον τρόπο που ένα worm κερδίζει τον αρχικό έλεγχο του συστήματος.

2.4.1.1. Είδη φορέων λοίμωξης

Τα worms στηρίζονται σε δύο γενικές μεθόδους για να μολύνουν έναν κεντρικό υπολογιστή. Είτε εκμεταλλεύονται ένα ελάττωμα στο λογισμικό που εκτελείται σε ένα σύστημα ή είναι το αποτέλεσμα κάποιων μέτρων που λαμβάνονται από ένα χρήστη. Κοιτάζοντας τις λεπτομέρειες από το σύνολο των worms που μελετήσαμε εντοπίσαμε τέσσερις διαφορετικές κατηγορίες των φορέων της λοίμωξης.

I. Μια αξιοποιήσιμη μερίδα του δικτύου που γνωρίζει τον κωδικό

Οι υπερχειλίσεις μνήμης βρίσκονται πιο συχνά ευάλωτες σε ένα δίκτυο που γνωρίζει τον κώδικα. Δημιουργούνται όταν ένα πρόγραμμα δέχεται περισσότερα δεδομένα εισόδου από ότι είναι διατεθειμένο να αποθηκεύσει. Σε μια τέτοια περίπτωση, τα εισαγόμενα δεδομένα υπερχειλίζουν άλλα μέρη της μνήμης αντικαθιστώντας άλλα βασικά στοιχεία του προγράμματος. Αν η αντικατάσταση των δεδομένων ελέγχει τη ροή του προγράμματος, όπως return addresses ή function pointers, ένας εισβολέας μπορεί να είναι σε θέση να διαμορφώσει ειδικά την είσοδο του προκειμένου να εκτελέσει εξ' αποστάσεως οδηγίες για το σύστημα τροποποιώντας αυτή τη πληροφορία ελέγχου.

Είναι σημαντικό να θυμόμαστε ότι, προκειμένου να εκμεταλλευτεί μια τέτοια κατάσταση υπερχείλισης, ο εισβολέας θα πρέπει να είναι σε θέση να ελέγχει τις εισαγωγές στο ευάλωτο πρόγραμμα. Μετά την απόκτηση του ελέγχου με τον τρόπο

αυτό, ο αξιοποιήσιμος κώδικας τρέχει με τα ίδια προνόμια με τον εκμεταλλεύσιμο κώδικα.

Έτσι, η υπερχείλιση μνήμης από έναν εισβολέα είναι αυτή που βρέθηκε σε ένα πρόγραμμα που δέχεται είσοδο από το δίκτυο και τρέχει σε ένα προνομιακό πλαίσιο όπως Administrator, SYSTEM, ή root. Δυστυχώς, πολλές από τις υπηρεσίες δικτύου σε σύγχρονα λειτουργικά συστήματα τρέχουν σε υψηλά προνομιακά επίπεδα.

Εκτός από την υπερχείλιση μνήμης, υπάρχει μια σειρά από άλλες ατέλειες του προγραμματισμού που θα μπορούσαν ενδεχομένως να οδηγήσουν σε εκμεταλλεύσιμα τρωτά σημεία. Αυτά περιλαμβάνουν τα σφάλματα λογικής στο file directory traversal functions, uninitialized variables, λάθη σε ASCII σε Unicode (και Unicode σε ASCII) conversion routines, race conditions, signed/unsigned comparison λάθη και off-by-one λάθη. Αλλά είναι πιο δύσκολο να βρεθούν, να αναλυθούν, και να αξιοποιηθούν, οι άλλες αδυναμίες που δεν έχουν αξιοποιηθεί από τους συγγραφείς worms από ότι είναι οι υπερχειλίσεις μνήμης.

Αν οι υπερχειλίσεις μνήμης έγιναν πιο δύσκολα εκμεταλλεύσιμες, χρησιμοποιώντας μέτρα προφύλαξης όπως stackguarding τότε είναι πιθανό οι δημιουργοί των worms να αρχίσουν να εκμεταλλεύονται άλλα, πιο τρωτά σημεία. Ένα πιθανό αποτέλεσμα αυτής της εξέλιξης είναι να δούμε λιγότερα worms, αλλά την ίδια στιγμή, να είναι πολύ πιο πολύπλοκα και ενδεχομένως πιο επικίνδυνα.

II. Μια ευάλωτη διαμόρφωση ενός δικτύου Aware Component

Ακόμη και αν μια υπηρεσία δικτύου έχει προγραμματιστεί προσεκτικά, μπορεί να είναι εκμεταλλεύσιμη αν δεν έχει ρυθμιστεί σωστά. Ο ιός τύπου worm Spida εκμεταλλεύτηκε μια αδύναμη προεπιλεγμένη ρύθμιση παραμέτρων εφαρμογής βάσης δεδομένων SQL Server. Η αρχική ρύθμιση περιείχε ένα προνομιακό λογαριασμό που δεν χρειαζόταν κωδικό πρόσβασης. Ο Spida συνδεόταν με μηχανήματα τα οποία εκτελούσαν τον SQL Server και επιχειρούσε να κάνει login χρησιμοποιώντας αυτόν τον λογαριασμό. Εάν ο διαχειριστής δεν είχε απενεργοποιήσει ειδικά αυτό το λογαριασμό, τότε το worm θα μπορούσε να αποκτήσει υψηλού επιπέδου έλεγχο του συστήματος.

III. Δράση του χρήστη

Ένας μεγάλος αριθμός από τα worms που μελέτησα δεν διαδίδονται μέσω των τρωτών σημείων, αλλά στηρίζονται σε μια ξεχωριστή ενέργεια του χρήστη για την αρχική μόλυνση. Στην περίπτωση αυτή, ο χρήστης λαμβάνει συνήθως ένα πρόγραμμα μέσω ηλεκτρονικού ταχυδρομείου που τον ξεγελάει και τον κάνει να πιστέψει ότι είναι κάτι άλλο, όπως ένα παιχνίδι, μια προφύλαξη οθόνης, ή ψηφιακές φωτογραφίες από ένα πάρτυ. Δεδομένου ότι η τεχνική αυτή βασίζεται σε λοιμώδεις δράσεις εκτός του ελέγχου του εισβολέα, είναι λιγότερο αξιόπιστη και διαδίδεται πιο αργά από τεχνικές που είναι πιο αυτόματες και δεν απαιτούν καμία ενέργεια του χρήστη.

IV. Μια υπάρχουσα πίσω πόρτα

Μερικά worms εκμεταλλεύονται «πίσω πόρτες» που άφησαν κάποιες προηγούμενες παραβιάσεις ασφάλειας.

Η πίσω πόρτα είναι ένας μηχανισμός που έχει δημιουργηθεί από ένα πρόγραμμα ενός υπολογιστή και επιτρέπει σε οποιονδήποτε γνωρίζει την ύπαρξή της να αποκτήσει κάποιον έλεγχο επί του συστήματος. Ο Leave μόλυνε συστήματα που είχαν ήδη εγκαταστημένη μια πίσω πόρτα τύπου SubSeven. Σωστά ενημερωμένα

antivirus θα είχαν την ικανότητα να ανιχνεύσουν την SubSeven και να την αναιρέσουν, κλείνοντας έτσι την πίσω πόρτα. Αυτό θα ήταν το σωστό ανοσοποιητικό για τους ανθρώπους που χρησιμοποιούσαν δίκτυα που παραβιάζονται από τον Leave.

2.4.1.2. Χαρακτηριστικά γνωρίσματα συνδεδεμένα με τη λοίμωξη

Στον παρακάτω Πίνακα 1, περιγράφω τα τρωτά σημεία που τα worms χρησιμοποιούν για να είναι επιτυχής η μόλυνση. Πολλά worms εκμεταλλεύονται γνωστές ευπάθειες, ενώ άλλα απαιτούν ενέργειες του χρήστη, ώστε να πάρουν τον έλεγχο του συστήματος.

Ευπάθειες ή Ενέργειες που απαιτούνται	**Worms**
MS00-0 2-Registry-Invoke Programs Use Standard Path	CODERED
MS00-078-Patch for 'Web Server Folder Traversal' Vulnerabilty	NIMDA
MS01-020-Incorrect MIME Header Can Cause IE to execute Email Attachment	BADTRANS, RETHEM, YAHA, NIMBA, BUGBEAR
MS01-033-Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise	CODERED
MS01-044-15 August 2001 Cumulative Patch for IIS	NIMDA
MS03-014-April 2003 Cumulative Patch for Outlook Express	MIMAIL
MS02-01528 March Cumulative Patch for Internet Explorer	MIMAIL
MS02-039-Buffer Overruns in SQL Server 2000 Resolution Service Might Enable Code Execution	SLAMMER
MS03-007-Unchecked Buffer in Windows Component May Cause Web Server Compromise	NACHI
MS03-026-Buffer Overrun in RPC May Allow Code Execution	BLASTER, NACHI
Microsoft advisory Q313418-Unsecured SQL Server password	SPIDA
Preexisting SubSeven infection	LEAVE
VU-196945-ISC Bind 8 Buffer Overflow in Transaction Signature (TSIG) Handling Code	LION
VU#29823, VU#34043, VU#382365: Multiple Format Strings Errors	RAMEN
VU#102795-Buffer Overflows in OpenSSL Servers	SLAPPER
User Runs Infected File	DUMARU, ETAP, FRETHEM, GIBE, HLLW, CAKE, JONBARR, KLEZ, LEAVE, LOVELETTER, MAGISTR, MEXER, MYPARTY, NEROMA, REPAD, SOBIG, STRANO, VOTE.K

Πίνακα 1 – Ευπάθειες που Εκμεταλλεύονται τα Worms

2.4.1.3. Κατάσταση των φορέων λοίμωξης

Ένα από τα λίγα worms που χρησιμοποίησε μια zero-day εκμετάλλευση ήταν το κλασσικό worm του Morris το 1988[16]. Σχεδόν όλα τα worms τα τελευταία δεκαπέντε χρόνια έχουν αξιοποιήσει δημόσια γνωστές ευπάθειες ή έχουν εξαπατήσει τον χρήστη ώστε να τα εκτελέσει. Στη μελέτη δεν ανακάλυψα κανένα στοιχείο αλλαγής στην πολυπλοκότητα των φορέων μόλυνσης. Ενώ ορισμένα τρωτά σημεία απαιτούν σαφώς μεγαλύτερη ικανότητα από άλλα για να εκμεταλλευτούν (ένα μαζικών μηνυμάτων ηλεκτρονικού ταχυδρομείου worm είναι πολύ πιο εύκολο να αναπτυχθεί από ένα άλλο που χρησιμοποιεί την υπερχείλιση μνήμης), τα είδη των φορέων μόλυνσης που φαίνεται να είναι αρκετά σταθερά. Ορισμένα προηγμένα worms χρησιμοποιούν συνδυασμούς αυτών των τυπικών φορέων για να αυξήσουν την αποτελεσματικότητά τους. Πιστεύω ότι στο μέλλον θα εμφανιστούν περισσότερα από αυτά τα worms, όπως το Nimda, που είναι ικανά να μολύνουν hosts με μια σειρά από διάφορους τρόπους.

Σε γενικές γραμμές, οι διαχειριστές συστήματος δεν μπορούν να στηριχτούν στο να εγκαθιστούν ενημερωμένες εκδόσεις κώδικα και οι χρήστες δεν μπορούν να υπολογίζουν την εκτέλεση προγραμμάτων που λαμβάνουν μέσω ηλεκτρονικού ταχυδρομείου. Η έλλειψη της εξέλιξης σε σχέση με φορείς μόλυνσης μπορεί να αποδοθεί σε έναν κυρίαρχο λόγο, στην τεράστια αποτελεσματικότητα που έχουν τα worms (και εξακολουθούν να έχουν) στην αξιοποίηση γνωστών δημόσιων τρωτών σημείων και στην εξαπάτηση χρηστών ώστε να εκτελούν τον κώδικα τους.

2.4.2. Επιβίωση

Αυτή η λειτουργία ζωής περιγράφει πώς ένας ιός τύπου worm διατηρεί τον έλεγχο ενός ξενιστή , αφού έχει εισχωρήσει στις άμυνες του. Αυτή η κατηγορία περιλαμβάνει τις ακόλουθες συμπεριφορές:

- Επανάληψη εκτέλεσης σε μεταγενέστερο χρόνο
- Αποφυγή ανίχνευσης
- Απενεργοποίηση του λογισμικού ανίχνευσης
- Πρόληψη μεταγλώττισης ή αντίστροφης μηχανικής

2.4.2.1. Επανάληψη εκτέλεσης σε μεταγενέστερο χρόνο

Μία από τις πρώτες ενέργειες που λαμβάνονται από τα περισσότερα worms είναι να εγκαταστήσουν κάποιο μηχανισμό για να εξασφαλιστεί ότι θα εκτελεστούν και πάλι αργότερα. Ο μηχανισμός αυτός χρησιμοποιείται κατά κύριο λόγο για να εξασφαλίσει τη δυνατότητα επιβίωσης του worm μεταξύ επανεκκινήσεων, αλλά έχει και άλλες χρήσεις, καθώς μπορεί και να χρησιμοποιηθεί για να εκτελέσει κάποιον από τον κώδικα του worm ως απάντηση μιας ενέργειας που συνέβη από το μολυσμένο σύστημα. Για παράδειγμα, μερικά worms μπορούν να ξεκινήσουν τη διάδοση του κώδικά τους μια καθορισμένη ημερομηνία ή όταν ένας χρήστης στείλει ένα μήνυμα ηλεκτρονικού ταχυδρομείου.

Υπάρχουν πολλές διαφορετικές στρατηγικές που χρησιμοποιούνται από τα worms για να διασφαλίσουν ότι μπορούν να επανακτήσουν τον έλεγχο σε μεταγενέστερο χρόνο. Πολλά worms χρησιμοποιούν ένα συνδυασμό αυτών των τεχνικών για να διασφαλίσουν μεγαλύτερη πιθανότητα επιβίωσης.

[16] Το πρώτο γνωστό worm

I. Τροποποιώντας τα αρχεία εκκίνησης

Αυτά τα αρχεία ελέγχουν την εκκίνηση του λειτουργικού συστήματος (ή κάποια συνιστώσα του). Τα worms μπορούν να εισάγουν οδηγίες σε αυτά τα αρχεία ώστε να ξεκινήσουν στις επόμενες επανεκκινήσεις. Αρχεία που συχνά αποτελούν στόχο worms περιλαμβάνουν:

- system.ini, win.ini, etc. for Windows
- /etc/rc.d/rc.sysinit, etc. for Linux

II. Χρησιμοποιώντας ένα βοηθητικό πρόγραμμα δρομολόγησης εργασιών

Μερικά worms προγραμματίζουν τον εαυτό τους ώστε να τρέχουν σε μια χρονομετρημένη βάση, συνήθως γνωστή ως δουλειά «cron». Τυπικές εγκαταστάσεις που στοχοποιούνται περιλαμβάνουν:

- AT utility in Windows
- anacron in Linux

III. Λοίμωξη ή αντικατάσταση φακέλων

Μερικά worms εισέρχονται σε δυαδικά αρχεία ή προγράμματα κελύφους, ή εξ ολοκλήρου αντικαθιστούν το αρχείο με κώδικα του worm. Κάθε φορά που το τροποποιημένο πρόγραμμα εκτελείται, το worm αποκτά τον έλεγχο του συστήματος.

IV. Αλλαγές Μητρώου (Σε συστήματα Microsoft Windows)

Ίσως ο πιο συνηθισμένος τρόπος για να διασφαλιστεί ότι ένα worm είναι δυνατό να τρέχει σε ένα σύστημα windows είναι να αλλάξει ένα από τα "κλειδιά Run" του μητρώου. Αυτά τα κλειδιά περιέχουν καταλόγους των προγραμμάτων που το λειτουργικό σύστημα ξεκινά αυτόματα. Εκτός από τα κλειδιά Run, υπάρχουν πολλές άλλες καταχωρήσεις μητρώου που ελέγχουν την έναρξη των προγραμμάτων ή των υπηρεσιών.

V. Αλλάζοντας αρχεία τύπου Handler

Στα Windows (και πολλά συστήματα παραθύρων για συστήματα Unix / Linux), μια εφαρμογή μπορεί να σχετίζεται με έναν τύπο αρχείου που καθορίζεται από την επέκταση του (στα Windows). Ένα worm θα μπορούσε να αντικαταστήσει τον χειριστή σε μια συγκεκριμένη επέκταση (ή τύπο αρχείου για τα λειτουργικά συστήματα τα οποία δεν καθορίζουν τον τύπο αρχείου που βασίζεται σε επέκταση), έτσι ώστε ένα διπλό κλικ ή απλά ένα «άνοιξε» του αρχείου να προκαλεί την εκτέλεση του κώδικα του worm.

2.4.2.2. Αποφυγή ανίχνευσης

Αποφεύγοντας την ανίχνευσή τους από προγράμματα προστασίας από ιούς και άλλα λογισμικά της άμυνας είναι ζωτικής σημασίας για τη δυνατότητα επιβίωσης των worms. Μερικές τεχνικές που χρησιμοποιούνται από τα worms για να αποφύγουν τον εντοπισμό τους είναι τα εξής:

- Χρησιμοποιώντας συσκότιση ή κρυπτογράφηση για να αποφύγουν να επισημανθούν από signature-based.

- Χρησιμοποιώντας πολυμορφικές και μεταμορφωμένες τεχνικές για να αλλάξουν, προκειμένου να αποφύγουν αμυντικά συστήματα που βασίζονται σε εντοπισμό υπογραφής.
- Συγκαλύπτοντας την εξερχόμενη κίνηση, έτσι ώστε να μοιάζει με κανονική κυκλοφορία του δικτύου, προκειμένου να αποφευχθεί η ανίχνευσης από συστήματα που αναλύουν την κυκλοφορία του δικτύου.

2.4.2.3. Απενεργοποίηση του λογισμικού ανίχνευσης

Είναι κοινό για ένα κακόβουλο κώδικα να απενεργοποίει το λογισμικό προστασίας, τα προσωπικά τείχη προστασίας, ή τα συστήματα ανίχνευσης εισβολής. Τα worms μπορούν να απενεργοποιήσουν το μηχανισμό ανίχνευσης ή να το τροποποιήσουν έτσι ώστε να μην λειτουργεί σωστά.

2.4.2.4. Πρόληψη μεταγλώττισης ή αντίστροφης μηχανικής

Ο πραγματικός σκοπός και οι δυνατότητες των νέων worms δεν μπορούν να γίνουν πλήρως κατανοητά μέχρι να αντιστραφούν μηχανικά. Οι δημιουργοί αυτών των κακόβουλων κωδικών λαμβάνουν μέτρα για να διασφαλίσουν ότι αυτό δεν μπορεί να γίνει γρήγορα. Αυτό εμποδίζει επίσης τον γρήγορο υπολογισμό του από μια υπογραφή η οποία μπορεί να χρησιμοποιηθεί από το λογισμικό εντοπισμού. Αντίστροφης μηχανικής μέτρα πρόληψης μπορούν να εφαρμοστούν στο ίδιο το worm ή σε φορτίο του. Ορισμένες από τις τεχνικές αυτές που έχω δει περιλαμβάνουν:

- Βασισμένο στη ζήτηση deobfuscation, όπου ο ιός τύπου worm αποκρυπτογραφεί μόνο μερίδες του κώδικα ανάλογα με τις ανάγκες, και κρυπτογραφεί εκ νέου τις ποσότητες αυτές όταν δεν χρειάζονται πλέον.
- Antidebugging τεχνικές που χρησιμοποιούνται για τον εντοπισμό προγραμμάτων εντοπισμού σφαλμάτων.
- Ισχυρή κρυπτογράφηση όταν το κλειδί κρυπτογράφησης δεν μπορεί να προσδιοριστεί μετά την εξέταση ενός αντιγράφου του worm.

2.4.3. Διάδοση

Φορείς διάδοσης μπαίνουν στο παιχνίδι όταν ένας ιός τύπου worm έχει ήδη καθιερώσει τον έλεγχο μιας υποδοχής. Ασχολούνται με τι το worm πρέπει να κάνει προκειμένου να μεταδοθεί σε άλλους υπολογιστές.

2.4.3.1. Είδη Διάδοσης

Οι τέσσερις κυρίες μεθόδους πολλαπλασιασμού ενός worm που εντόπισα είναι:

I. Αποστολή μολυσμένων μηνυμάτων ηλεκτρονικού ταχυδρομείου

Πολλά worms τους στέλνουν τον εαυτό τους συνημμένο σε μηνύματα ηλεκτρονικού ταχυδρομείου. Πριν από την αποστολή τέτοιων μηνυμάτων, τα worms συγκεντρώνουν συνήθως τις διευθύνσεις του στόχου από τα εισερχόμενα του χρήστη, το τοπικό σύστημα αρχείων του και από τα Registry κλειδιά. Αυτά τα worms χρησιμοποιούν το πρόγραμμα ηλεκτρονικού ταχυδρομείου από το μολυσμένο μηχάνημα ή χρησιμοποιούν τη δικιά τους μηχανή SMTP για να στείλουν μηνύματα ηλεκτρονικού ταχυδρομείου στα πιθανά θύματα. Η χρήση μιας ανεξάρτητης SMTP επιτρέπει στα worms να διαδοθούν ανεξάρτητα από τα μηνύματα ηλεκτρονικού

ταχυδρομείου του ξενιστή. Τα Frethem, Dumaru, και Yaha worms περιείχαν όλα τις δικές τους SMTP μηχανές.

II. Εισάγοντας αντίγραφα σε Peer-to-Peer (P2P) δίκτυα

Μια πιο πρόσφατη τεχνική και για τον πολλαπλασιασμό του ιού τύπου worm είναι η χρησιμοποίηση των peer-to-peer (P2P) δικτύων. Σε P2P λογισμικά, που επιτρέπουν σε αρχεία να μοιραστούν και να κατεβούν από υπολογιστές που άμεσα ή έμμεσα συνδέονται μεταξύ τους, έχει βρεθεί μια δραματική αύξηση. Worms όπως τα HLLW. Cake και Repad, επωφελούνται από αυτά τα προγράμματα, προκειμένου να μολύνουν και άλλους υπολογιστές. Αυτά τα worms είναι διαθέσιμα για P2P δίκτυα μέσω ονομάτων αρχείων που οι περισσότεροι χρήστες θα βρουν δελεαστικά. Μπορούν να μεταμφιέζονται σε κωδικοποιημένα ψηφιακά τραγούδια, εφαρμογές, ή οποιοδήποτε άλλο τύπο αρχείου που το δίκτυο P2P επιτρέπει.

III. Διάθεση αντίγραφων στο κοινόχρηστο αρχείο

Τα worms μπορούν επίσης να διαδίδονται μέσω των κοινόχρηστων αρχείων. Ένας ιός τύπου worm τοποθετεί ένα αντίγραφο του εαυτού του σε έναν κατάλογο που μοιράζεται με άλλους υπολογιστές. Αυτά τα worms βασίζονται σε χρήστες άλλων μηχανημάτων που βλέποντας το αρχείο το αντιγράφουν στους υπολογιστές τους, μπερδεύοντας το ότι είναι κάποιο νόμιμο αρχείο. Η μέθοδος αυτή δεν είναι πολύ επιτυχής για διασπορά μεταξύ των δικτύων, αλλά μπορεί να λειτουργήσει καλά, όταν συνδυάζεται με άλλες μεθόδους πολλαπλασιασμού. Για παράδειγμα, όταν ένα worms έχει μολύνει μια μηχανή του δικτύου μέσω ενός μηχανισμού που δεν έχει καμία σχέση με τα κοινόχρηστα στοιχεία αρχείων, τότε μπορεί να αξιοποιήσει τα κοινόχρηστα αρχεία ως φορέα μετάδοσης για να εξαπλωθεί σε άλλους υπολογιστές μέσω το τοπικό LAN. Δεδομένου ότι τα τείχη προστασίας περιορίζουν τυπικά την χρήση των κοινόχρηστων αρχείων μεταξύ των bcal LAN και το Internet, πολύ σπάνια κάποιο τείχος προστασίας μπλοκάρει κάποιο κοινόχρηστο αρχείο του LAN. Τα Bugbear, Nimda, και Gibe χρησιμοποίησαν αυτή τη μέθοδο για να αυξήσουν τον πολλαπλασιασμό τους.

IV. Σαρώνοντας και αξιοποιώντας μακρινές αδυναμίες

Αυτή η μέθοδος του πολλαπλασιασμού εκμεταλλεύεται ένα προγραμματισμό ή ένα σφάλμα στο λογισμικό που εκτελείται σε ένα απομακρυσμένο σύστημα. Το worm σαρώνει για τις ευάλωτες μηχανές και προσπαθεί να τους στείλει κακόβουλα ή ακατάλληλα δεδομένα σε μια προσπάθεια να τους εκμεταλλευτεί. Μερικά worms δεν ερευνούν για ευπαθείς μηχανές, απλά υποθέτουν ότι κάθε υπολογιστής στο διαδίκτυο είναι ευάλωτος και προσπαθούν να εκμεταλλευτούν τυχαίες διευθύνσεις IP. Είτε έτσι είτε αλλιώς, η τεχνική αυτή πολλαπλασιασμού βασίζετε στο ότι το worm χρησιμοποιεί έναν κεντρικό υπολογιστή που έχει τεθεί σε κίνδυνο για την έρευνα και την εκμετάλλευση άλλων υπολογιστών.

Μέθοδοι σάρωσης που χρησιμοποιούνται από τα worms μπορούν να ποικίλλουν. Πολλά worms χρησιμοποιούν τυχαία σάρωση, απλά δημιουργούν μια διεύθυνση στην τύχη και προσπαθούν να μολύνουν αυτό τον υπολογιστή. Μερικά worms χρησιμοποιούν μια διακύμανση των τυχαίων σαρώσεων, ευνοώντας τις διευθύνσεις που είναι πιο κοντά στη μηχανή υποδοχής, όπως αυτές στο ίδιο υποδίκτυο. Ένας worm μπορεί να έχει μια λίστα από πιθανούς στόχους που παρέχεται από το συντάκτη του worm ή αναπτύσσετε μέσω σαρώσεων από απομακρυσμένα συστήματα. Μελλοντικές καινοτομίες σάρωσης μπορούν επίσης να περιλαμβάνουν συντονισμό μεταξύ των αντιγράφων των worms, εξασφαλίζοντας ότι οι μηχανές

σαρώνονται μόνο μία φορά. Μια εις βάθος συζήτηση των διαφόρων μεθόδων ανίχνευσης worms καλύπτεται από τον Staniford[17].

Προκειμένου να διαδοθούν μέσω απομακρυσμένων ευπαθειών, τα worms πρέπει να αντιγραφούν από τον μολυσμένο υπολογιστή καθώς και από το δίκτυο. Ένα κοινό σενάριο για ένα worm είναι να τρυπώσει σε μια υπάρχουσα υπηρεσία. Εάν ένα worm χρησιμοποιήσει μια θύρα δικτύου που έχει ήδη ανοίξει, έχει το πλεονέκτημα ότι είναι ακόμα πιο δύσκολο να φιλτραριστεί. Για παράδειγμα, τα worm που χρησιμοποιούν τη θύρα TCP 80 για επικοινωνία δεν μπορούν να μπλοκαριστούν από το τείχος προστασίας. Worms όπως ο Slammer που χρησιμοποιεί μια κανονική θύρα η οποία χρησιμοποιείται από μια συγκεκριμένη τοπική υπηρεσία μπορούν εύκολα να εντοπιστούν και να ηττηθούν από δίκτυα καθώς και τείχη προστασίας τα οποία είναι κατάλληλα σχεδιασμένα και διαρρυθμισμένα.

2.4.3.2. Χαρακτηριστικά διάδοσης συνδεδεμένα με το πολλαπλασιασμό

Υπάρχουν πολλά χαρακτηριστικά που συνδέονται με την διάδοση του worm, όπως η χρήση των Registry keys και τα αρχεία πρόσβασης για αναγνώριση στόχου. Άλλα χαρακτηριστικά περιλαμβάνουν την τροποποίηση των διαδικασιών ή τη χρήση των θυρών για τη διευκόλυνση της διάδοσης. Στον παρακάτω Πίνακα 2 παρουσιάζω μερικά από τα πιο σημαντικά ή συχνότερα χαρακτηριστικά που έχουν καταγραφεί.

[17] S. Stanford, V. Paxson, N. Weaver, “How to own the Internet in Your Spare Time”

Ιδιότητα Πολλαπλασιασμού	Worm
Reconnaissance – Registry Related	
Active Internet Settings Key	GIBE, MAGISTR
HKCU\Software\Microsoft\Inernet Acct Manager\Accounts\00000001\SMTP Server	FRETHEM, MYPARTY
Reconnaissance – File System	
.dbx (Outlook Express email folder)	DUMARU, FRETHEM, MAGISTR, MYPARTY, SOBIG
.wab files (Outlook Address Book)	DUMARU, FRETHEM, KLEZ, MAGISTR, MYPARTY, SOBIG, YAHA
.mbx (Outlook email folder)	FRETHEM, MAGISTR
.eml (Outlook email message)	FRETHEM, SOBIG
.txt (ASCII text file)	KLEZ, SOBIG
.html/.html (HTML file)	JONBARR, KLEZ, SOBIG
ICQ list	KLEZ, YAHA
Network Ports Used	
Port 25/TCP	BADTRANS, DUMARU, FRETHEM, GIBE, JONBARR, KLEZ, MAGISTR, RECORY, YAHA
Port 27374/TCP	LEAVE, LION
Port 80/TCP	LEAVE, SLAPPER
IRC Ports	LEAVE, LOVELETTER, STRANO
Windows File Shares	BUGBEAR, ETAP
Spreading – Mass Mail Engine	
Uses Outlook	RECOVERY, LOVELETTER, NEROMA, VOTE.K
Uses its own SMTP engine	BUGBEAR, DUMARU, FRETHEM, JONBARR, KLEZ, YAHA
Spreading	
Tries to infect all files on drives C-Z	DUMARU, KLEZ, NIMDA
HKCU\Software\Kazaa\LocalContent	MEXER, RECOVERY, VOTE.K
\Documents and Settings\%infected user name%\Start Menu\Programs\Startup	GIBE, MYPARTY
Uses network shares	BUGBEAR, KLEZ
Infects Microsoft Word documents with macro virus	STRANO
Spreading – Peer-to-Peer Networks	
Peer-to-Peer Music Networks	GIBE, HLLW.CAKE, JONBARR, RECOVERY, REPAD
KaZaa	HLLW.CAKE, JONBARR, MEXER, REPAD, VOTE.K
iMesh	HLLW.CAKE, MEXER
mIRC folder – script.ini	GIBE, VOTE.K, STRANO, JONBARR
Spreading – Server Modifications	
Modifies web content to infect visiting Clients/hosts	NIMDA
Creates IIS Virtual Directories for C & D drives (wide open)	CODERED

Πίνακα 2 – Σημαντικά Χαρακτηριστικά του Πολλαπλασιασμού των Worms

2.4.3.3. Η Κατάσταση της Διάδοσης

Ένας καλά σχεδιασμένος ιός τύπου worm μπορεί να εξαπλώνεται με απίστευτη ταχύτητα. Ο Slammer είναι ένα εξαιρετικό παράδειγμα του τύπου worm που εκμεταλλεύεται μια ευπάθεια ώστε να επιβραδυνθεί ο γρήγορος ρυθμός πολλαπλασιασμού του. Δεδομένου ότι, απαιτείται μόνο ένα ενιαίο πακέτο UDP να αποσταλεί στον στόχο, ο Slammer θα μπορούσε συνεχώς να σαρώνει και να μολύνει μηχανήματα χωρίς να χρειάζεται να περιμένει για απάντηση. Εντός δέκα λεπτών είχε μολύνει περίπου το 90 τοις εκατό των ευάλωτων μηχανημάτων (τουλάχιστον 75.000) του διαδικτύου[18].

Εάν η διαθέσιμη ενημερωμένη έκδοση κώδικα για την ευπάθεια που αξιοποιεί ο Slammer είχε εφαρμοστεί, τότε ο αριθμός των μολυσμένων μηχανημάτων θα μπορούσε να έχει μειωθεί εντυπωσιακά. Λόγω της ταχύτητας της μόλυνσης, οι διαχειριστές δικτύου δεν ήταν σε θέση να ανταποκριθούν γρήγορα ώστε να το σταματήσουν.

Συνήθως, η επιτυχία πολλαπλασιασμού του worm στηρίζεται στην ποσότητα των μηχανημάτων που μολύνουν καθώς και πόσο γρήγορα τα μολύνουν. Στο μέλλον, θα υπάρχουν και άλλοι τρόποι για να δούμε την επιτυχία στην αναπαραγωγή. Ένα worm επιδιώκει να μεταδίδεται χωρίς να ανιχνεύετε. Για παράδειγμα, ο Badtrans χρησιμοποίησε ένα 30-δεύτερο χρονόμετρο για προγραμματισμένες αποστολές, προκειμένου να αποφευχθούν οι πλημμύρες του δικτύου που θα ειδοποιούσε τους διαχειριστές. Worms, όπως ο Badtrans μπορούν να οδηγήσουν σε μια νέα κατηγορία των τεχνικών πολλαπλασιασμού που προσπαθούν να κινηθούν κάτω από το ραντάρ των διαχειριστών δικτύου, κινούμενα χαμηλά και αργά.

Στοχοθετημένη διάδοση, είναι όταν ένας ιός τύπου worm προσπαθεί να μολύνει συγκεκριμένες μηχανές, που είναι μια χρονιά αναδυόμενη τεχνική. Ενώ κανένα από τα worms που παρατήρησα δεν χρησιμοποιούν αποκλειστικά στοχοθετημένο πολλαπλασιασμό, μερικά worms έδειξαν σημάδια αρχικού σταδίου στοχευμένων επιθέσεων. Ο Spida αποκλείει συγκεκριμένες IP διευθύνσεις από τους πιθανούς στόχους του. Ο Bugbear εμφανίζει κάποιες πρώιμες μορφές των στοχοθετημένων πολλαπλασιασμού. Ο Bugbear καταλαμβάνει κωδικούς πρόσβασης του δικτύου και πληκτρολογήσεις του χρήστη και στη συνέχεια τους αποστέλλει στον δημιουργό του εάν ο τομέας της διεύθυνσης ηλεκτρονικού ταχυδρομείου προεπιλογής του συστήματος φαίνεται να είναι ένα χρηματοπιστωτικό ίδρυμα. Η στοχοθετημένη διάδοση είναι πιθανό να αναπτυχθεί περαιτέρω με τη ροή του χρόνου.

2.4.4. Ωφέλιμο Φορτίο

Το ωφέλιμο φορτίο ενός worm είναι ο κώδικας ή το πακέτο που μεταφέρει την εκτέλεση μιας εργασίας πέρα από τυπικές λειτουργίες του κύκλου ζωής του.

2.4.4.1. Τύποι Ωφέλιμου Φορτίου

Παρατηρήθηκαν τέσσερις σημαντικές κατηγορίες ωφέλιμου φορτίου:

I. Αποκτώντας τον έλεγχο μιας «πίσω πόρτας»

«Πίσω πόρτες» είναι τμήματα κώδικα που επιτρέπουν τον τηλεχειρισμό σε συστήματα που είναι σε κίνδυνο. Υπάρχουν διάφοροι τρόποι που χρησιμοποιούνται για την επικοινωνία με αυτές τις πίσω πόρτες. Μερικά worms χρησιμοποιούν

[18] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, V. Weaver, "The Spread of the Sapphire/Slammer Worm"

κοινόχρηστες τεχνολογίες που έχουν αναπροσαρμοστεί για να παρέχουν τη διοίκηση και τον μηχανισμό ελέγχου, όπως: κοινόχρηστα αρχεία (Bugbear και Nimda), P2P δίκτυα (slapper), και IRC (Dumaru). Ένα από τα πιο εξελιγμένα worms μέχρι σήμερα, ο Leave, ανακτά κωδικοποιημένες εντολές από καταλόγους που κατεβάζει από δικτυακούς τόπους και από τα ιδιωτικά κανάλια IRC.

II. Καθιέρωση πράκτορα άρνησης υπηρεσίας

Αρκετά worms σχεδιάστηκαν με σκοπό τη δημιουργία ενός δικτύου με παράγοντες κατανεμημένης άρνησης εξυπηρέτησης[19]. Είδαμε δύο τύπους ωφέλιμου φορτίου με παράγοντες κατανεμημένης άρνησης εξυπηρέτηση. Ορισμένοι με σκληρή κωδικοποίηση των στόχων (π.χ. Blaster σε windowsupdate.com), και μερικοί που ήταν προσαρμόσιμοι (π.χ. ο Leave, ο οποίος αποδέχθηκε στόχευση πληροφοριών από μακριά).

III. Συλλογή Πληροφοριών

Μερικά ωφέλιμα φορτία worms είναι σχεδιασμένα να συλλέγουν πληροφορίες από μολυσμένα μηχανήματα. Οι Lion και Ramen αντιγράφουν και φιλτράρουν αρχεία κωδικών πρόσβασης. Οι Badtrans και Bugbear εγκαταθισούν keystroke loggers, προκειμένου να συλλέξουν κωδικούς πρόσβασης χρηστών από το ηλεκτρονικό εμπόριο και από άλλες εφαρμογές.

IV. Προκαλώντας Καταστροφή

Το worm Magistr είναι ένα καλό παράδειγμα ενός worm με ένα καταστροφικό ωφέλιμο φορτίο. Ο ιός αυτός προσπάθησε να αντικαταστήσει τους τοπικούς σκληρούς δίσκους και να καταστρέψει τα BIOS, καθιστώντας το σύστημα δυσλειτουργικό και μόνο διορθώσιμο από έναν ειδικευμένο τεχνικό. Ο Spida είχε απλώς ως στόχο να καταστρέψει συγκεκριμένα αρχεία. Αυτό το είδος του ωφέλιμου φορτίου, όπου ο στόχος είναι να καταστρέψει τα συστήματα που βρίσκονται σε κίνδυνο, φαίνεται να είναι σπάνιο και δεν υπάρχει πολύ συχνά στην ομάδα των worms που μελέτησα.

2.4.4.2. Χαρακτηριστικά γνωρίσματα συνδεδεμένα με το ωφέλιμο φορτίο

Στον Πίνακα 3 παρακάτω συνοψίζω τις πιο σημαντικές ενέργειες που εκτελούνται ή παρουσιάζονται:

Ιδιότητα Ωφέλιμου Φορτίου	Worms
Network Ports Used	
Port 80 /TCP (To download backdoor)	FRETHEM, LION
Port 80 /TCP (To download commands)	LEAVE
IRC ports	LEAVE, LOVELETTER
Port 27374/TCP/SubSeven (διανομή)	LEAVE
Port 1434/UDP (διανομή)	SLAMMER
Port 1434/UDP (διανομή)	SPIDA
Port 1080/TCP (διανομή και πίσω πόρτα)	BUGBEAR

[19] Denial-of-Service

Ιδιότητα Ωφέλιμου Φορτίου	Worms
Network Ports Used	
Port 36794/TCP (Βρίσκει το firewall, κτλπ, και σταματάει)	BUGBEAR
Port 433/TCP	SLAMMER
Port 2002/UDP (Εγκαθιστά p2p Δίκτυο)	SLAMMER
Port 1978/UDP (Εγκαθιστά p2p Δίκτυο)	SLAMMER
Port 4156/UDP (Εγκαθιστά p2p Δίκτυο)	SLAMMER
Port 1052/UDP (Εγκαθιστά p2p Δίκτυο)	SLAMMER
Συλλογή	
Installs keystroke logger	BADTRANS, BUGBEAR, LOVELETTER
IRC	LEAVE
Στέλνει μέσω email αρχεία σε διευθύνσεις στην Κίνα	LION, RAMEN
Στέλνει μέσω email αρχεία που περιέχουν τη διεύθυνση IP	SPIDA
Στέλνει μέσω email τυχαία αρχεία από κάποιον υπολογιστή με επεκτάσεις όπως : .mp8, .txt, .html, .wab, .asp, .doc, .rtf, .xls, .jpg, .cpp, .pas, .mpg, .mpeg, .bak, .mp3, .pdf	KLEZ
Αναγνώριση	
Ελέγχει τον τίτλο που παραθύρου που είναι εκείνη την ώρα ανοικτό	BADTRANS
Ανιχνεύει για πιθανά θύματα μέσω FTP	RAMEN
Καταστροφή	
Overwrites CMOS	MAGISTR
Flashes BIOS	MAGISTR
Καταστρέφει τον BLASTER	NACHI
DDoS Payload	BLASTER
Installs rootkit(tOrn)	LION
Trojan system binaries	LION
Παρέχει τη δυνατότητα σε έναν εισβολέα να εκτελέσει αυθαίρετες εντολές	LEAVE
Σε συγκεκριμένο χρόνο, συνδέεται με μια hardcored IP (20 από αυτές) και κατεβάζει και τρέχει ένα αρχείο	SOBIG
Διαγράφει και ξαναγράφει αρχεία	LOVELETTER, NEROMA, SPIDA, VOTE.K
Απενεργοποιεί τον υπολογιστή	REPAD
Ενώνει p2p δυναμικό δίκτυο DDoS	SLAPPER
Ασφάλεια	
Τερματίζει το AV ή το firewall	BUGBEAR, JONBARR, KLEZ, YAHA
Αφαιρεί ή τροποποιεί το πρωτόκολλο TCP wrappers	LION
Σκοτώνει το syslogd	LION
Κρυπτογραφεί τα αρχεία, τις εντολές και τα κλειδιά μητρώου	LEAVE
Απενεργοποιεί το FTP και το rpc.statd για να αποτρέπει νέα προσβολή	RAMEN
Αλλάζει τους κωδικούς	SPIDA

Πίνακα 3 – Ιδιότητες των Ωφέλιμων Φορτίων των Worms

3. ΓΝΩΡΙΣΜΑΤΑ ΤΗΣ ΕΠΙΘΕΣΗΣ ΤΩΝ ΊΩΝ ΤΥΠΟΥ WORM

Το δείγμα από τα worms που μελέτησα παρουσιάζει κοινά χαρακτηριστικά κατά τις επιλογές της ζωής του, όπως περιγράφεται στην Τεχνολογία των Ιών Τύπου Worm. Τα χαρακτηριστικά αυτά αποτελούν συγκεκριμένες ενέργειες που παρατηρούνται με τα worms για να εξασφαλιστεί η επιτυχής μόλυνση, η επιβίωση και αναπαραγωγή τους.

Αυτά τα χαρακτηριστικά γνωρίσματα της επίθεσης του ιού τύπου worm τα κατηγοριοποιούμε σε τρεις βασικές κατηγορίες: Η πρώτη είναι μια οποιαδήποτε κατάσταση που υπάρχει για να καταστεί δυνατή μια επιτυχημένη επίθεση worm, όπως μια ευάλωτη υπηρεσία δικτύου ή εσφαλμένη ρύθμιση παραμέτρων του συστήματος. Η δεύτερη κατηγορία είναι υπολείμματα που μένουν πίσω, όταν ένα worm μολύνει ένα σύστημα, όπως μια αλλοίωση αρχείου, αλλαγές που έγιναν στο μητρώο των Windows, ή μιας τροποποιημένης διαδικασίας που έχει απομείνει από τον ιό τύπου worm. Η τελευταία κατηγορία των ιδιοτήτων επίθεσης είναι οποιαδήποτε συμπεριφορά που προκαλείται ως παρενέργεια της λοίμωξης τύπου worm, όπως παρατηρήσιμη αύξηση της κίνησης του δικτύου όταν το worm προσπαθεί να βρει νέους στόχους.

Εντόπισα περίπου διακόσια λεπτομερή χαρακτηριστικά επίθεσης. Χώρισα αυτά τα χαρακτηριστικά σε δεκατέσσερις γενικές κατηγορίες. Πιστεύω ότι αυτές τις δεκατέσσερις κατηγορίες που καλύπτουν ολόκληρο το φάσμα των χαρακτηριστικών που εμφανίζεται από τα worms στο παρελθόν είναι και πολύ πιθανό να δούμε από worms του μέλλοντος. Παρακάτω, παρουσιάζετε κάθε ένα από τα χαρακτηριστικά.

1. Εκμετάλλευση Ευάλωτου Κώδικα Δικτύου

Το χαρακτηριστικό αυτό είναι μερικές φορές απαραίτητη προϋπόθεση για τη μόλυνση από το worm. Τα ταχύτερα worms σε εξάπλωση αξιοποιούν γενικά την επίγνωση – δικτύου των υπηρεσιών με αυτοματοποιημένο τρόπο. Στο σύνολο των worms που μελέτησα, η πιο κοινή ευπάθεια σε αυτή την κατηγορία είναι μια υπερχείλιση.

2. Παραπλάνηση του Χρήστη

Ένας άλλος κοινός μηχανισμός λοίμωξης είναι να παραπλανήσει έναν χρήστη ώστε να τον κάνει να εκτελέσει ο ίδιος το worm. Το περισσότερα worms μαζικού ηλεκτρονικού ταχυδρομείου βασίζονται στους χρήστες να τρέξουν ένα μολυσμένο πρόγραμμα, κάνοντας το να φαίνεται ένα καλό που απλά είναι επικολλημένο.

3. Εκμετάλλευση Ευάλωτων Ρυθμίσεων

Οι ευάλωτες συνθέσεις καλύπτουν μια ποικιλία προβλημάτων πέρα από αυτή του εσφαλμένου κώδικα, όπως οι ασθενείς ρυθμίσεις κωδικού πρόσβασης, τα ελεύθερα δικαιώματα, και κακή ρύθμιση παραμέτρων σχέσεις εμπιστοσύνης.

4. Εκμετάλλευση μιας υπάρχουσας Πίσω Πόρτας

Ένας ιός τύπου worm χρησιμοποιεί μια υπάρχουσα πίσω πόρτα του συστήματος για να εγκατασταθεί.

5. Αλλαγές σε Αρχείο του Συστήματος

Σχεδόν όλα τα worms αφήνουν κάποια στοιχεία στο σύστημα αρχείων. Αντιγράφουν γενικά τον εαυτό τους σε βασικά αρχεία του συστήματος και αλλάζουν τις ρυθμίσεις των αρχείων ώστε να εξασφαλίζεται ότι μπορούν να επιτεθούν ξανά σε μεταγενέστερο χρονικό σημείο.

6. Αλλαγές στις Ρυθμίσεις του Συστήματος

Των υπό μελέτη τριάντα worms, δεκαεπτά από αυτά προέβησαν σε τροποποιήσεις του μητρώου των Windows. Συχνά αυτό το χαρακτηριστικό συνδέεται με την επιβίωση του worm, καθώς οι εν λόγω τροποποιήσεις γίνονται συνήθως για να προκαλέσουν αυτόματα το τρέξιμο του worm.

7. Τροποποίηση μιας Διεργασίας

Μερικά από τα πιο εξελιγμένα worms εισάγουν τον εαυτό τους σε μια διαδικασία που ήδη τρέχει. Μαζί με τη δράση να τροποποιήσουν τη λειτουργία της διαδικασίας, το χαρακτηριστικό αυτό περιλαμβάνει την έναρξη ή τη διακοπή άλλων διαδικασιών.

8. Πρόσβαση στο Δίκτυο

Αυτό το χαρακτηριστικό είναι εμφανές σε worms που διαδίδονται μέσω δικτύου ή λαμβάνουν εντολές μέσω ενός δικτύου.

9. Απαίτηση Ανεπτυγμένων Προνομίων

Τα worms που χρειάζονται πρόσβαση σε περιορισμένους πόρους είναι επιτυχή μόνο όταν τρέχουν με αρκετά προνόμια για την πρόσβαση στους πόρους αυτούς. Τα worms που κερδίζουν τον αρχικό έλεγχο από την αξιοποίηση των υπηρεσιών του συστήματος έχουν ήδη τέτοια προνομία, όπως και τα worms που εκμεταλλεύονται τις εφαρμογές που εκτελούνται σε ένα υψηλό επίπεδο δικαιωμάτων. Άλλα worms προσπαθούν να ελέγξουν το σημερινό επίπεδο προνομίων τους ή επιδιώκουν να το αυξήσουν.

10. Διενεργούν Ανώμαλες Αναζητήσεις

Μερικά worms χρησιμοποιούν πληροφορίες από το σύστημα που έχουν μολύνει. Για παράδειγμα, οι mass-mailers κάνουν χρήση του τοπικού συστήματος για τη συλλογή διευθύνσεων ηλεκτρονικού ταχυδρομείου. Οι πληροφορίες αυτές συχνά βρίσκονται αναζητώντας τα κλειδιά μητρώου και τα αρχεία που είναι πιθανό να περιέχουν αυτά τα δεδομένα.

11. Επικαλώντας Κρίσιμα APIs

Τα worms πρέπει γενικά να εκτελούν κάποια δράση καθοριστικής σημασίας. Τα worms μαζικού ηλεκτρονικού ταχυδρομείου είναι πιθανό να επικαλεστούν το SMTP APIs του λειτουργικού συστήματος ώστε να διαδοθούν περαιτέρω.

12. Προκαλώντας Πλημμύρες Δικτύου

Επιθετικά πολλαπλασιαστικά worms μπορούν να επηρεάσουν το διαθέσιμο εύρος ζώνης του δικτύου. Οι διαχειριστές παρατηρούν την εξάντληση του διαθέσιμου εύρος ζώνης του δικτύου και χρησιμοποιούν sniffers ώστε να ανακαλύψουν την επίθεση ενώ μια νέα επίθεση βρίσκετε σε εξέλιξη.

13. Επιβραδύνει το Τοπικό Σύστημα

Τα worms μπορεί να έχουν αντίκτυπο στο χρόνο απόκρισης του συστήματος ή να του προκαλέσουν μια υπερδραστηριότητα. Αυτό είναι σε γενικές γραμμές, είτε εκ προθέσεως είτε ως αποτέλεσμα κακής σύνταξης του worm.

14. Να Περιέχει Υπογραφές Worms

Υπάρχει ένας περιορισμένος αριθμός τρόπων για τη λειτουργικότητα του κώδικα του worm. Ως εκ τούτου, τα προγράμματα μπορούν να εξεταστούν για την κωδικοποίηση μοτίβων παλαιότερων worms, ώστε να παρατηρήσουν κάποιο νέο. Σήμερα, τα περισσότερα λογισμικά προστασίας είναι σε θέση να εκτελέσουν έρευνα με την σάρωση σε αρχεία που μπορεί να υποδηλώνουν την ύπαρξη του κακόβουλου κώδικα.

4. ΤΕΧΝΙΚΕΣ ΚΑΙ ΜΗΧΑΝΙΣΜΟΙ ΆΜΥΝΑΣ

Οι πιο κοινές μέθοδοι που χρησιμοποιούνται για την άμυνα έναντι στα worms σήμερα είναι αντιδραστικές, π.χ. ανίχνευση ιών ή λογισμικά επιδιόρθωσης. Οι μηχανισμοί αυτοί δεν έχουν καμία ελπίδα για την πρόληψη γρήγορα εξαπλωμένων worms, ή worms που χρησιμοποιούν zero-day exploits για να πραγματοποιήσουν τις επιθέσεις τους. Αυτό δεν σημαίνει ότι αυτές οι τεχνολογίες δεν είναι χρήσιμες. Στην πραγματικότητα, είναι ουσιώδες μέρος της άμυνας στρατηγικής σε βάθος.

Σε αυτή την ενότητα θα προσδιορίσω ενεργητικές αμυντικές τεχνολογίες και μηχανισμούς που μπορούν να χρησιμοποιηθούν για την πρόληψη worms στο διαδίκτυο σήμερα. Για τη μελέτη αυτή, έχουν χρησιμοποιηθεί μόνο τρέχουσες τεχνολογίες και αγνοήθηκαν αναδυόμενες τεχνολογίες, όπως είναι οι τεχνικές που αποσκοπούν στη διάδοση των worms. Επίσης, δεν θεώρησα τα καθαρά layer 2 και layer 3 (στο μοντέλο OSI) των αμυντικών μηχανισμών, όπως Ιδιωτικά Εικονικά Τοπικά Δίκτυα (PVLANs). Ενώ και οι δύο τάξεις της τεχνολογίας είναι υποσχόμενες απέναντι στα worms, η ανάλυσή μας επικεντρώθηκε στις τρέχουσες, γνωστές και κοινές τεχνικές και πόσο αποτελεσματικές μπορεί να είναι ενάντια στα worms που χρησιμοποιούν αυτές τις τεχνολογίες.

4.1. Τείχη Προστασίας – Φιλτράρισμα Πακέτων

Το φιλτράρισμα πακέτων λειτουργεί στο δίκτυο μεταφέροντας layers του πρωτοκόλλου TCP / IP δικτύου μοντέλου. Επιτρέπει σε κάθε πεδίο στο δίκτυο ή μεταφερόμενες κεφαλίδες ενός πακέτου να συμπληρώνονται από ένα σύνολο κανόνων. Για παράδειγμα, πακέτα που περιέχουν συγκεκριμένες διευθύνσεις IP και ports μπορούν να αποκλειστούν. Δεν υπάρχει περιεχόμενο ελέγχου ή πρωτόκολλο επικύρωσης σε αυτό το επίπεδο. Το φιλτράρισμα πακέτων συνήθως εφαρμόζεται με ειδικό τείχος προστασίας ή δρομολογητή φιλτραρίσματος.

4.2. Τείχη Προστασίας – Stateful

Τα Τοίχοι Προστασίας – Stateful παρακολουθούν τις συνδέσεις δικτύου καθώς και την κατάστασή τους. Ένα τέτοιο τείχος προστασίας εντοπίζει τις αιτήσεις που έχουν αποσταλεί από το εσωτερικό του προστατευόμενου δικτύου και επιτρέπει τις απαντήσεις στις αιτήσεις αυτές του δικτύου ανάλογα με την περίπτωση. Μπορεί να φιλτράρει με βάση τις διευθύνσεις και τις θύρες που χρησιμοποιούνται από τον τοπικό ή απομακρυσμένο υπολογιστή. Εάν ένα πακέτο είναι μέρος μια υπάρχουσα σύνδεσης, μπορεί να επιτρέπεται, ενώ ένα παρόμοιο πακέτο που φαίνεται εκτός από μια υπάρχουσα σύνδεση να εγκαταλείπετε.

4.3. Τείχη Προστασίας – Εφαρμογή Proxy

Οι πελάτες και οι διακομιστές ποτέ δεν επικοινωνούν απευθείας όταν χρησιμοποιούν τείχος προστασίας εφαρμογής proxy. Τα τείχη προστασίας που περιλαμβάνονται στην κατηγορία αυτή λειτουργούν στο επίπεδο εφαρμογής του μοντέλου του δικτύου TCPIP. Δίνουν τη δυνατότητα ελέγχου του περιεχομένου και της επικύρωσης του πρωτοκόλλου εφαρμογής.

4.4. Συστήματα Ανίχνευσης Εισβολέων

Τα συστήματα ανίχνευσης εισβολέων (IDS) μπορεί καλύτερα να θεωρηθεί ένας συνδυασμός ενός προγράμματος ανίχνευσης ιών και sniffer δικτύου. Ένα τέτοιο σύστημα έχει ρυθμιστεί με μια βάση δεδομένων υπογραφών για γνωστό κακόβουλο κώδικα και για ύποπτη συμπεριφορά. Ένα IDS παρακολουθεί το σύνολο της κίνησης για το τμήμα του δικτύου στο οποίο είναι συνδεδεμένο και κάθε πακέτο έχει σαρωθεί με τη βάση δεδομένων υπογραφών. Εάν βρεθεί μια αντιστοιχία, ο διαχειριστής μπορεί να προειδοποιείτε για την παρουσία ύποπτων δραστηριοτήτων στο δίκτυο. Μερικά IDSs είναι αρκετά περίπλοκα για να φιλτράρουν τις ύποπτες κυκλοφορίες ή να τις εκτρέψουν σε μια απομονωμένη τοποθεσία όπου δεν μπορούν να κάνουν κακό.

4.5. Τείχη Προστασίας – Host

Τα τείχη προστασίας – Host εγκαθίστανται μεταξύ των εφαρμογών ενός κεντρικού υπολογιστή και του δικτύου. Επιβάλουν τους κανόνες που καθορίζουν τον τρόπο με τον οποίο συγκεκριμένες εφαρμογές μπορούν να χρησιμοποιούν το δίκτυο. Ένα τέτοιο εργαλείο ενδιαφέρεται για τις συνδέσεις στο δίκτυο, τις μεταφορές, καθώς και για layers εφαρμογών του πρωτοκόλλου TCP / IP μοντέλο και είναι χρήσιμο στην παρεμπόδιση worms που κάνουν ασυνήθιστες συνδέσεις. Είναι σημαντικό να έχουμε κατά νου ότι τα host τείχη προστασίας δεν μπορούν να ανιχνεύσουν κακόβουλες δραστηριότητες που φαίνεται να συνάδουν με τη συνήθη συμπεριφορά του χρήστη δεδομένου ότι αυτά τα τείχη αναπτύσσουν τους δικούς τους κανόνες, παρακολουθώντας την ομαλή τους ροή στο δικτύου του χρήστη.

4.6. Εικονικά Μηχανήματα

Μπορούν να χρησιμοποιηθούν δυνητικά για την πρόληψη κακόβουλων λογισμικών από τη χρήση του λειτουργικού συστήματος για παράνομες ενέργειες. Είναι τυπικά μεταξύ του λειτουργικού συστήματος και του φυσικού υλικού. Αυτό το στρώμα της διαμεσολάβησης μεταξύ του λογισμικού και του υλικού είναι ένα ισχυρό χαρακτηριστικό γνώρισμα που εμποδίζει δυνητικά κακόβουλο λογισμικό να διασυνδεθεί άμεσα με το πραγματικό υλικό.

4.7. Διαμόρφωση

Στο πλαίσιο αυτό, η διαμόρφωση αναφέρεται σε οποιαδήποτε εφαρμογή ή ρύθμιση του λειτουργικού συστήματος που μπορεί να προσαρμόζεται ώστε να καταστεί το περιβάλλον πιο ανθεκτικό στην επίθεση. Έχουμε περιορίσει το πεδίο εφαρμογής των ρυθμίσεων διαμόρφωσης σε εκείνα που είναι εύκολα να αλλαχθούν μέσα από εργαλεία, οδηγούς, και τα μενού. Εμείς δεν περιλαμβάνουμε προηγμένες ρυθμίσεις που συνήθως πραγματοποιούνται από έναν έμπειρο τεχνικό που χρησιμοποιεί ατεκμηρίωτα χαρακτηριστικά ή κάνει εκτεταμένες αλλαγές στο κώδικα. Τυπικές πτυχές μιας ισχυρής διαμόρφωσης περιλαμβάνουν αυστηρότερες ρυθμίσεις της εφαρμογής, περιορίζοντας τη χρήση των θυρών του δικτύου, που τρέχουν μόνο τις απαιτούμενες υπηρεσίες, καθώς και τον καθορισμό των πιο περιοριστικών δικαιωμάτων στο αρχείο του συστήματος και του μητρώου.

4.8. Anti-virus Heuristics

Παραδοσιακά antivirus προϊόντα έχουν μια κακώς γνωστή υπογραφής προσέγγισης. Περιέχουν υπογραφές, οι οποίες χρησιμοποιούνται για τον προσδιορισμό του κακόβουλου κώδικα. Οι προμηθευτές λογισμικού αντιμετώπισης ιών ενημερώνουν για τις υπογραφές αυτές σε τακτά χρονικά διαστήματα, συνήθως κάθε εβδομάδα ή ανάλογα με τις ανάγκες. Πολλά από τα προϊόντα antivirus απασχολούν επίσης heuristics στην αναζήτηση του κακόβουλου κώδικα. Τα προϊόντα εντοπισμού ιών μπορούν να εντοπίσουν νέο κακόβουλο κώδικα που λειτουργεί με τρόπο παρόμοιο με γνωστούς ιών και worms. Τα Heuristics επιτρέπουν την ανίχνευση των ιών και worms που ενδεχομένως δεν έχουν μελετηθεί από ερευνητές antivirus.

4.9. Host-Based Συστήματα Ανίχνευσης Εισβολέων

Τα Host-Based Συστήματα Ανίχνευσης Εισβολέων(HIPS) συνήθως χαρακτηρίζουν τις αιτήσεις από τους πόρους που χρειάζονται κατά τη διάρκεια της κανονικής λειτουργίας. Τέτοια συστήματα συνήθως λειτουργούν από προκαθορισμένους κανόνες που περιγράφουν το τι αποτελεί νομική συμπεριφορά για συγκεκριμένες εφαρμογές. Τα συστήματα αυτά συνήθως δίνουν πολιτική επιβολή στο εμπρόσθιο άκρο του ζωτικής σημασίας λειτουργικού συστήματος. Για παράδειγμα, ένα HIPS θα μπορούσε να μεσολαβήσει στη βασική δημιουργία Registry key, έτσι ώστε η παρέμβαση των worms που τρέχουν με κλειδιά θα μπορούσε να σταματήσει. Τέτοιου είδους συστήματα αντιδρούν σε επικίνδυνες αιτήσεις στο λειτουργικό σύστημα με την καταγραφή τους, αφαιρώντας τα οριστικά, ή ρωτώντας τον χρήστη για την έγκριση να συνεχίσουν τη δράση. Μια πιθανή δράση των HIPS είναι να τερματίσει το επιτιθέμενο πρόγραμμα. Η δράση αυτή θα σκοτώσει ευθέως το worm που προσπαθεί να χρησιμοποιήσει χωρίς άδεια πόρους του συστήματος.

4.10. Έλεγχος Ακεραιότητας

Κάνουν χρήση μιας αξιόπιστης αναφοράς των αρχείων στο σύστημα. Κρατούν γενικά κρυπτογραφική hashes των γνωστών καλών instances των αρχείων, έτσι ώστε οι συγκρίσεις ακεραιότητας να μπορούν να γίνουν ανά πάσα στιγμή. Μερικά έχουν τη δυνατότητα να αποκαταστήσουν τα αρχεία που ενδέχεται να έχουν τροποποιηθεί από ένα worm.

4.11. Stackguarding

Οι τεχνολογίες Stackguarding[20] έχουν ως στόχο να καταστήσουν τα προγράμματα ανθεκτικά σε buffer overflow επιθέσεις. Με τη συμπερίληψη ειδικών βιβλιοθηκών ή χρησιμοποιώντας ειδικά compilers, ο προγραμματιστής παράγει λογισμικό που δεν μπορεί να αξιοποιηθεί από μακριά. Το Stackguarding δεν αφαιρεί την υπερχείλιση των σφαλμάτων κωδικοποίησης, αλλά την αποτρέπει από το να αξιοποιηθεί.

[20] C. Cowan, C. Pu, D. Maier, H. Hilton, j. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, Q. Zhang, “StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks”

5. ΕΠΙΘΕΣΕΙΣ ΕΝΑΝΤΙΑ ΤΩΝ ΑΜΥΝΩΝ

Το σύστημα μας με τις ιδιότητες των επιθέσεων παρέχει ένα πλαίσιο μέσα στο οποίο κατατάση τα worms με τις κατάλληλες αμυντικές τεχνολογίες. Τα χαρακτηριστικά των επιθέσεων ταξινομούν, πώς λειτουργούν τα worms, και προτείνουν τις άμυνες που θα είναι πιο αποτελεσματικές. Για παράδειγμα, πολλά worms αλλάζουν τα Run κλειδιά, εντός του μητρώου (χαρακτηριστική επίθεση: τροποποιώντας τις ρυθμίσεις του συστήματος). Αυτό το χαρακτηριστικό μπορεί να προστατευθεί, κλειδώνοντας τα ευάλωτα κλειδιά μητρώου (αμυντική τεχνολογία: διαμόρφωση). Με το ταίριασμα τον αμυντικών χαρακτηριστικών τεχνολογιών για όλα τα worms που μελετήθηκαν, είχα την ευκαιρία να αναπτύξω ένα σχεδόν ολοκληρωμένο αμυντικό πίνακα.

Οι σειρές του πίνακα άμυνας αντιπροσωπεύουν τις δεκατέσσερις ιδιότητες επίθεσης και οι στήλες αντιπροσωπεύουν τις άμυνες. Οι πρώτες τέσσερις ιδιότητες αφορούν μόνο στη μόλυνση, ενώ οι υπόλοιπες δέκα μπορούν να εφαρμοστούν σε οποιαδήποτε λειτουργία ζωής του worm. Η τομή ενός χαρακτηριστικού και μιας άμυνας αντιπροσωπεύει την κλάση προστασίας που παρέχει η εν λόγω άμυνα να αντιμετωπίσει αυτό το χαρακτηριστικό επίθεσης. Αυτές οι κατηγορίες είναι οι εξής:

- **D – Ανίχνευση (Detect)** : Η άμυνα μπορεί να ανιχνεύσει την επίθεση, αλλά δεν μπορεί να κάνει τίποτα για να τη σταματήσει. Για παράδειγμα, το file integrity checkers μπορούν να ανιχνεύσουν ότι ένα αρχείο έχει τροποποιηθεί, αλλά δεν μπορεί να εμποδίσει την τροποποίηση.

- **P - Παρέχει Μερική Προστασία (Provides Partial Protection)** : Κάποιες άμυνες είναι καλές στην πρόληψη ορισμένων επιθέσεων, αλλά μπορούν να παρεκτραπούν, ανάλογα με τις ακριβείς λεπτομέρειες της εφαρμογής της επίθεσης τους. Για παράδειγμα, οι διακομιστές αλληλογραφίας μπορούν να ρυθμιστούν ώστε να φιλτράρουν τα συνημμένα που περιέχουν εκτελέσιμα αρχεία. Αυτό παρέχει μερική μόνο προστασία από worms που κοροϊδεύουν τον χρήστη, επειδή τα αρχεία μπορούν να φτάσουν στο χρήστη μέσω άλλων δικτύων εκτός από ηλεκτρονικό ταχυδρομείο.

- **R - Αντιδραστική Προστασία (Reactive Protection)** : Η άμυνα μπορεί να ανιχνεύσει και να νικήσει την επίθεση, αλλά μόνο αφού η επίθεση γίνει γνωστή. Αντιδραστική άμυνες βασίζονται στις υπογραφές, όπως είναι τα συστήματα ανίχνευσης εισβολής.

- **B – Μπλοκάρει την Επίθεση (Blocks Attack)** : Η άμυνα μπλοκάρει αποτελεσματικά την επίθεση.

Η κενή εγγραφή δείχνει ότι η άμυνα δεν παρέχει αποτελεσματική προστασία από το ανάλογο χαρακτηριστικό επίθεσης.

5.1. Πίνακας Άμυνας

Ιδιότητες Άμυνας / Ιδιότητες Επίθεσης	Τείχη Προστασίας - Φιλτράρισμα Πακέτων	Τείχη Προστασίας - Stateful	Τείχη Προστασίας - Εφαρμογή Proxy	Συστήματα Ανίχνευσης Εισβολέων	Τείχη Προστασίας - Host	Εικονικά Μηχανήματα	Διαμόρφωση	Anti-virus Heuristics	Host-Based Συστήματα Ανίχνευσης Εισβολέων	Έλεγχος Ακεραιότητας	Stackguarding
Εκμετάλλευση Ευάλωτου Κώδικα Δικτύου	R	R	B	R	R		B				B
Παραπλάνηση του Χρήστη			B		B		P				
Εκμετάλλευση Ευάλωτων Ρυθμίσεων	B	B	B		B		B				
Εκμετάλλευση Μιας Υπάρχουσας Πίσω Πόρτας	B	B	B		B			B			
Αλλαγές σε Αρχείο του Συστήματος							B		B	D	
Αλλαγές στις Ρυθμίσεις του Συστήματος							B		B	D	
Τροποποίηση μιας Διεργασίας							B		B		
Πρόσβαση στο Δίκτυο	P	P	P		B				B		
Απαίτηση Ανεπτυγμένων Προνομίων							B		B		B
Διενεργεί Ανώμαλες Αναζητήσεις							B		B		
Επικαλείται Κρίσιμα APIs						B			B		
Προκαλεί Πλημμύρες Δικτύου	B	B	B		B				B		
Επιβραδύνει το Τοπικό Σύστημα									P		
Να Περιέχει Υπογραφές Worms			P	P				P			

Πίνακας 4 – Λεπτομερής Πίνακας Άμυνας

5.2. Παρατηρήσεις επί του Πίνακα Άμυνας

Στην ιδανική περίπτωση, τα worms θα πρέπει να εμποδίζονται από το να μολύνουν το σύστημα. Ο αμυντικός πίνακας δείχνει ότι η τεχνολογία που χρησιμοποιεί το stackguarding είναι ένα λογικό πρώτο βήμα. Αυτό θα καλύψει πολλές από τις αδυναμίες που εκμεταλλεύονται τα worms. Ο πίνακας δείχνει επίσης ότι τα τείχη προστασίας παρέχουν την πιο ολοκληρωμένη προστασία από τις τέσσερις λοίμωξης που συνδέονται με τα χαρακτηριστικά. Τα τείχη προστασίας, ωστόσο, παρέχουν πολύ περιορισμένη προστασία από τα αρχεία που εισέρχονται στο σύστημα "νόμιμα" και ξεγελούν τον χρήστη ώστε να μολύνει τον εαυτό του. Επίσης, δεν μπορεί να προστατεύσει από άγνωστες λογικές πλημμύρες που εκτίθενται σε διασυνδέσεις του δικτύου. Έτσι οι περιμετρικές άμυνες και μόνο είναι ανεπαρκείς για την παροχή πλήρους προστασίας από επιθέσεις worms.

Τα υπόλοιπα δέκα χαρακτηριστικά επίθεσης φαίνονται να παρέχουν καλύτερη προστασία από τα Host-Based συστήματα ανίχνευσης εισβολέων και την ορθή διαμόρφωση του συστήματος. Αυτές οι δύο άμυνες μπλοκάρουν ή υπερασπίζουν εννέα από τα δέκα μη μολυσμένα χαρακτηριστικά, και καλύπτουν επίσης 12 από την πλήρη λίστα των 14.

Επιλέγοντας από τις άμυνες στο πίνακα, είναι δυνατή η θέσπιση ενός πολυεπίπεδου συστήματος προστασίας που μπορεί να αντιμετωπίσει κάθε είδους χαρακτηριστικό επίθεσης. Αν η επιλεγμένη αμυντική στρατηγική χρησιμοποιεί άμυνες που μπλοκάρουν τελείως τα χαρακτηριστικά, μπορεί να είναι δυνατό να μπλοκάρουν ακόμη και zero-day worm.

Παρακάτω, θα εξηγήσω κάθε στήλη του αμυντικού πίνακα μήτρας και θα περιγράψω τον τρόπο που κάθε άμυνα ασχολείται με κάθε χαρακτηριστικό επίθεσης.

5.2.1. Τείχη Προστασίας – Φιλτράρισμα Πακέτων

Η ορθή ρύθμιση του τείχους προστασίας είναι κρίσιμη για την παροχή αποτελεσματικής προστασίας. Η κατευθυντήρια αρχή της διαμόρφωσης του τείχους προστασίας είναι να μπλοκάρει όλη την εισερχόμενη κίνηση εκτός αυτών που είναι απαραίτητων για τη λειτουργία του δικτύου. Περιορίζοντας την έκθεση των εσωτερικών χώρων του δικτύου μειώνετε η πιθανότητα ότι μια ευπάθεια ή μια πίσω πόρτα μια εσωτερική μηχανή μπορεί να αξιοποιηθεί από μακριά.

Το φιλτράρισμα πακέτων λαμβάνει αποφάσεις που βασίζονται σε IP διευθύνσεις και αριθμούς θύρας, δεν μπορεί να προστατεύσει τις θύρες που πρέπει να παραμείνουν ανοικτές. Εάν μια θύρα χρησιμοποιείται από μια υπηρεσία δικτύου που είναι ευάλωτη, μπορεί να κλειστεί από έναν διαχειριστή ως προσωρινή λύση σε βάρος της νόμιμης κυκλοφορίας.

Το φιλτράρισμα πακέτων μπορεί επίσης να προστατεύσει από τη κακή ρύθμιση παραμέτρων των συστημάτων υποδοχής. Για παράδειγμα, μια θύρα με μια αχρείαστη υπηρεσία δικτύου να προστατεύεται από ένα φιλτράρισμα του τείχους προστασίας. Ρεαλιστικά, κάποιες υπηρεσίες δεν μπορούν να αποκλειστούν γιατί είναι αναγκαίες. Αυτή η τεχνολογία δεν μπορεί να μειώσει όλες τις πτυχές μιας κακής ρύθμισης, όπως το τρέξιμο απαιτούμενων υπηρεσιών με υψηλότερα προνόμια από ότι απαιτούνται.

Μέσα από την καταγραφή των δυνατοτήτων τους, το φιλτράρισμα πακέτων μπορεί επίσης να βοηθήσει να εντοπιστούν οι πλημμύρες του δίκτυο που είναι ενδεικτικό της διάδοσης του worm. Μόλις μια τέτοια επίθεση έχει εντοπιστεί, το τείχος είναι σε θέση

να την αποτρέψει. Αυτό επηρεάζει επίσης τη νόμιμη κίνηση προσπαθώντας να περάσει το τείχος.

Επιπλέον, ένα πακέτο φιλτραρίσματος μπορεί να μπλοκάρει την πρόσβαση στο εξωτερικό δίκτυο. Αυτό δεν προσφέρει καμία προστασία στο πλαίσιο του δικτύου που προστατεύονται από το τείχος. Το φιλτράρισμα της εξερχόμενης κίνησης διαταράσσει το φυσιολογικό μοντέλο λειτουργίας του δικτύου και δεν είναι μια λογική λύση.

5.2.2. Τείχη Προστασίας – Stateful

Ένα τέτοιο τείχος προστασίας παρέχει την βασική προστασία ενός τείχους φιλτραρίσματος πακέτων και εξασφαλίζει ότι μόνο τα πακέτα που σχετίζονται με μια εσωτερική σύνδεση επιτρέπονται. Πρόκειται για μια βελτιωμένη λύση, δεδομένου ότι επιτρέπει το φιλτράρισμα με βάση τις συνθήκες και όχι απλώς το κλείδωμα ή επιτρεπόμενα συναλλαγών.

5.2.3. Τείχη Προστασίας – Εφαρμογή Proxy

Τα τείχη προστασίας με εφαρμογή Proxy είναι παρόμοια με τις δύο προηγούμενες τεχνολογίες με την έννοια ότι μπορεί να φιλτράρει την κυκλοφορία βασίζεται σε θύρες και σε διευθύνσεις IP. Έχουν επίσης την ικανότητα να φιλτράρουν την κυκλοφορία με βάση το περιεχόμενό της, η οποία παρέχει πρόσθετη προστασία από τα worms. Μπορούν να βεβαιώσουν ότι όλα τα πεδία έχουν έγκυρα μήκη και επιτρεπόμενη περιεκτικότητα γιατί κατανοούν τους υψηλότερους ορισμούς επιπέδου πρωτόκολλο. Το πεδίο μήκος φιλτραρίσματος μπορεί να αποτρέψει την υπερχείλιση που εκμεταλλεύεται αυτούς τους τομείς. Το φιλτράρισμα περιεχομένου, μπορεί να διασφαλίσει ότι οι τομείς έχουν νόμιμα δεδομένα. Χρησιμοποιώντας αυτές τις τεχνικές, τα συγκεκριμένα τείχη μπορούν να διαγράψουν τα πακέτα που περιέχουν εκμετάλλευση ή κώδικα κέλυφος.

Αυτά τα τείχη μπορούν να χρησιμοποιηθούν για να φιλτράρουν όλα τα εκτελέσιμα συνημμένα αρχεία. Η προστασία αυτή έχει τα όριά της, επειδή τη μετονομασία των συννημένων ή τη κρυπτογράφηση του ηλεκτρονικού ταχυδρομείου μπορεί να την παρακάμψει. Δυστυχώς, αυτή η αυστηρή προνοητική ικανότητα φιλτραρίσματος περιορίζει τους χρήστες στο να μοιραστούν νόμιμα μη κακόβουλα αρχεία. Αυτή η εφαρμογή προσφέρει ένα επιπλέον όφελος όταν χρησιμοποιείται κατασταλτικά. Έχουν τη δυνατότητα να φιλτράρουν τα μηνύματα που ταιριάζουν με γνωστές κακές τιμές. Προστατεύοντας έτσι τα συστήματα από worms που αποκτούν τον έλεγχο από την εξαπάτηση του χρήστη.

5.2.4. Συστήματα Ανίχνευσης Εισβολέων

Τέτοια συστήματα μπορούν καλύτερα να θεωρηθούν ως ένας συνδυασμός προγράμματος ανίχνευσης ιών και sniffer δικτύου. Με λίγες εξαιρέσεις, τα εν λόγω συστήματα λειτουργούν σε ένα αντιδραστικό τρόπο, αναλαμβάνουν δράση μετά από τη ζημιά που έχει προκληθεί. Αυτό τα καθιστά καλά για να ειδοποιήσουν τους διαχειριστές σχετικά με την παρουσία γνωστού κακόβουλου κώδικα ή ύποπτης συμπεριφοράς που επιδιώκει να εκμεταλλευτεί ευάλωτο κώδικα δικτύου. Είναι αρκετά άχρηστα για τον εντοπισμό άγνωστης εκμετάλλευσης , άγνωστων worms, ή / και πολυμορφικών worms και ιών που είναι ικανοί να κρυπτογραφήσουν τον εαυτό τους για να αποφευχθεί η μέθοδος ανίχνευσης με βάση την υπογραφή.

5.2.5. Τείχη Προστασίας – Host

Τα τείχη προστασίας- Host επιβάλλουν μια πολιτική η οποία καθορίζει τις διαδικασίες μπορούν να έχουν πρόσβαση στο δίκτυο. Εξαιτίας αυτού που μπορούν να αποκλείσουν τον ιό τύπου worm που θα δημιουργήσει προγράμματα που επιχειρούν να στείλουν πακέτα. Μπορούν επίσης να αποκλείσουν επικίνδυνα προγράμματα που πλημμυρίζουν το δίκτυο. Αυτό προϋποθέτει ότι η διαδικασία που επικαλείται από το worm δεν είναι μεταμφιεσμένη σαν εκείνη που μπορεί να στηριχθεί το δίκτυο.

Εκτός από τις εξερχόμενες συνδέσεις, μπορούν επίσης να φιλτράρουν την εισερχόμενη κίνηση βασίζεται σε πρωτόκολλα, διευθύνσεις IP, και θύρες. Αυτό περιλαμβάνει τις αιτήσεις για τις πίσω πόρτες και τις υπηρεσίες που δεν πρέπει να εκτίθενται.

Τα ανεπτυγμένα τείχη προστασίας-host μπορούν να σαρώσουν κακόβουλες υπογραφές, συνήθως σε συνεργασία με την τεχνολογία anti-virus. Ενώ σαρώνουν εισερχόμενα e-mail, υψηλού κινδύνου, τα συνημμένα μπορεί επίσης να εγκαταλειφθούν. Η προστασία αυτή έχει τον ίδιο περιορισμό όπως η εφαρμογή Proxy μετονομάζοντας το συννημενο ή κρυπτογραφώντας το e-mail για να παρακάμψει την ασφάλεια.

5.2.6. Εικονικά Μηχανήματα

Οι εικονικές μηχανές, συνήθως παρέχουν εικονικούς πόρους του λειτουργικού συστήματος. Τα worms που επιχειρούν να τρέξουν σε ένα τέτοιο περιβάλλον μπορούν να βλάψουν μόνο τους εικονικούς πόρους και όχι το αληθινό του λειτουργικό σύστημα ή hardware. Για παράδειγμα, ο Mgistr θα ήταν σε θέση να αντικαταστήσει τα πραγματικά BIOS του συστήματος, εάν αυτός εκτελούνταν σε μια εικονική μηχανή. Με τον τρόπο αυτό, οι εικονικές μηχανές προστατεύουν από worms που επικαλούνται το κρίσιμο APIs, αν και μόνο αυτές επιχειρούν να αγγίξουν το hardware. Οι εικονικές μηχανές μπορούν επίσης να βοηθήσουν τον χρήστη να ανακτήσει το σύστημά του, από τη στιγμή που ανιχνεύετε μια επίθεση. Συχνά, έχουν τη δυνατότητα να επαναφέρουν το σύστημα σε μια προηγούμενη, απαλλαγμένη από το worm κατάσταση.

5.2.7. Διαμόρφωση

Μια ανθεκτική διαμόρφωση προστατεύει από τρωτά σημεία, κλειδώνοντας τις υπηρεσίες και απενεργοποιώντας όποιες δεν είναι απαραίτητες.

Με ασφαλή ρύθμιση, οι προνομιούχοι λογαριασμοί μπορούν να χρησιμοποιούνται μόνο όταν απαιτούνται για την ολοκλήρωση του έργου ή την εκτέλεση της υπηρεσίας. Αν η εκμεταλλεύσιμη υπηρεσία δεν απαιτεί δικαιώματα του συστήματος και η "αρχή του ελάχιστου προνομίου" έχει εκτελεστεί, το worm δεν θα είναι σε θέση να χρησιμοποιήσει τα προηγμένα προνόμια. Βάζοντας περιοριστικά δικαιώματα μπορεί επίσης να αποτρέψει ένα worm από το να τροποποιήσει άλλη διεργασία που εκτελείται ή εκτελεί ανώμαλα ερωτήματα.

Κάνοντας πιο σκληρές τις εφαρμογές ηλεκτρονικού ταχυδρομείου, αποτρέποντας την αυτόματη εκτέλεση των συνημμένων, βοηθά στην αποφυγή worms που διαδίδονται μέσω ηλεκτρονικού ταχυδρομείου.

Επιβάλλοντας ισχυρά δικαιώματα στο σύστημα αρχείων, καθώς και στο μητρώο μπορούν να περιορίσουν τον αριθμό των αλλαγών που ένα worm θα είναι σε θέση να προβεί στις ρυθμίσεις του συστήματος. Αυτό περιορίζει επίσης την ποσότητα των πληροφοριών που τα worms μπορούν να λάβουν από ένα τέτοιο σύστημα.

Κάποιες ρυθμίσεις ασφαλείας μπορεί να είναι δύσκολο να εφαρμοστούν αποτελεσματικά, διότι όλοι οι χρήστες μπορεί να έχουν μια νόμιμη ανάγκη για πρόσβαση σε ορισμένα αρχεία. Ρυθμίζοντας τα περιοριστικά δικαιώματα μπορούν να τα καταστήσουν απρόσιτα για όλους τους χρήστες. Υπό αυτές τις συνθήκες, μια προσεκτική ισορροπία πρέπει να υπάρχει, ώστε να παρέχετε στους χρήστες πρόσβαση σε ακριβώς αυτά που χρειάζονται και τίποτα περισσότερο.

5.2.8. Anti-virus Heuristics

Σωστά ενημερωμένα εργαλεία antivirus μπορούν να εντοπίζουν, να απομονώνουν, ακόμη και να καθαρίζουν γνωστά worms. Επίσης, είναι σε θέση να εκτελούν τα ίδια δράση κατά Trojan πίσω πορτών προγραμμάτων και άλλων τέτοιων κακόβουλων κωδίκων. Το μειονέκτημα αυτής της προσέγγισης είναι ότι οι ερευνητές antivirus πρέπει να μελετήσουν κάθε τύπο worm και να δημοσιεύουν τις υπογραφές που μπορούν να τα εντοπίσουν. Στη συνέχεια, πρέπει οι χρήστες να ενημερώσουν τα αρχεία με τις υπογραφές ώστε να εξασφαλίσουν ότι οι υπογραφές τους στις βάσεις δεδομένων είναι ενημερωμένες. Φυσικά, αυτό το είδος του προγράμματος αντιμετώπισης ιών προστατεύει μόνο από γνωστές απειλές και δεν είναι σε θέση να εντοπίσει τα worms για τα οποία οι προμηθευτές λογισμικού αντιμετώπισης ιών δεν έχουν αναπτύξει ακόμη υπογραφές. Για να βοηθήσει κατά αυτό τον τύπο απειλής, τα περισσότερα σύγχρονα προϊόντα καταπολέμησης του ιού επίσης αναζητήσουν για heuristics. Πρόκειται για ένα σύνολο worms ή ιών, όπως τμήματα κώδικα (μορφές κώδικα που φαίνεται να είναι κοινές σε κακόβουλο κώδικα). Αν και αυτό είναι μια καλή τεχνολογία για να έχουμε, (οι συγγραφείς worms γνωρίζουν την ύπαρξή του) και το είδος των προτύπων που αναζητούνται και μπορούν να τα νικήσουν εύκολα.

Αξίζει να σημειωθεί ότι προϊόντα antivirus εργάζονται κατά κανόνα σε επίπεδο αρχείου συστήματος, πράγμα που σημαίνει ότι παρακολουθούν και ανιχνεύουν τα αρχεία καθώς μια διεργασία τα προσβάλει. Μερικά worms, όπως ο CodeRed, υπάρχουν μόνο στη μνήμη και ποτέ δεν γράφουν τον εαυτό τους στο σύστημα αρχείων. Στην ουσία, δεν προσπαθούν να διατηρήσουν τον έλεγχο που έχουν καταλάβει. Αν και αυτή η συμπεριφορά καθιστά αυτό το worm ευκολότερο να καθαριστεί, τόσο πιο δύσκολο είναι να εκτοπιστούν από τα περισσότερα προϊόντα antivirus.

5.2.9. Host-Based Συστήματα Ανίχνευσης Εισβολέων

Αυτά τα συστήματα μπορούν να διαμεσολαβήσουν στα αρχεία του συστήματος, δικτύου, registry, διαδικασίες και προνομιούχα αιτήματα. Μπορούν να αναγνωρίσουν ιδιαιτερότητες, όπως είναι τα φυσιολογικά ερωτήματα ή οι πλημμύρες δικτύου, και τις αρνούνται. Μπορούν να εντοπίσουν επίσης αιχμές κατά των τοπικών δραστηριοτήτων του συστήματος με προσοχή για την υπερβολική δραστηριότητα των αρχείων του συστήματος ή χρήση μνήμης. Μόλις εντοπιστούν, μπορούν να σταματήσουν τις παράνομες διαδικασίες. Αυτή είναι η μόνη τεχνολογία που έχει κάποια δυνατότητα να αποτρέψει ένα worm από την εξευτελιστική απόδοση του στο σύστημα.

Τα συστήματα αυτά μπορούν επίσης να αποκλείσουν την πρόσβαση σε πόρους συστήματος που δεν προστατεύονται από ισχυρή διάρθρωση, να σταματήσουν πίσω πόρτες, και την πρόληψη των κακόβουλων ενεργειών του worm, ακόμη και αν ένας χρήστης έχει παρασυρθεί ώστε να ξεκινήσει τη μόλυνση. Όλα αυτά είναι δυνατά, επειδή επικυρώνουν ειδικές δράσεις. Προστατεύουν επίσης από τις ευπάθειες του κώδικα δικτύου, καθώς τα προγράμματα αυτά θα πρέπει να περιορίζονται στην εκτέλεση μόνο αναμενόμενων λειτουργιών τους.

5.2.10. Έλεγχος Ακεραιότητας

Ένας έλεγχος ακεραιότητας μπορεί να εντοπίσει τυχόν αλλαγές που έγιναν στο σύστημα αρχείων από ένα worm. Αλλαγές που θα μπορούσαν να αποκαλύψουν την παρουσία ενός worm θα «πιάνονταν» από τα συστήματα αυτά που περιλαμβάνουν την εισαγωγή των εκτελέσιμων αρχείων, όπως οι Trojan πίσω πόρτες, και η τροποποίηση των αρχείων ρυθμίσεων. Αυτά τα αρχεία συνήθως τροποποιούνται ώστε να καταστεί δυνατή η επιβίωση του worm μέσα από επανεκκινήσεις. Το μειονέκτημα αυτής της τεχνολογίας είναι ο έλεγχος ακεραιότητας συνήθως εκτελείτε μόνο περιστασιακά.

5.2.11. Stackguarding

Η τεχνολογία Stackguarding καθιστά εξαιρετικά δύσκολο για τους επιτιθέμενους να εκμεταλλευτούν την υπερχείλιση στο buffer ,το πιο κοινό είδος της ευπάθειας ανακαλύπτετε στο κώδικα του δικτύου. Από τις δεκατρείς ευπάθειες, που εξετάστηκαν από το σύνολο των worms μας, μόνο τα έξι είχαν υπερχειλίση μνήμης. Η τεχνολογία Stackguarding μπορεί επίσης να αποτρέψει τα worms από το να αποκτήσουν αυξημένα προνόμια στο σύστημα. worms που αποκτούν τον έλεγχο του λογαριασμού των χαμηλών προνομιών μπορεί να προσπαθήσουν να ανυψώσουν το προνόμιο τους. Η τεχνολογία αυτή μπορεί επίσης να υπερασπιστεί έναντι αυτού του είδους επίθεσης.

6. ΑΠΟΤΕΛΕΣΜΑΤΑ

6.1. Άμυνα σε Βάθος

Πολλές αμυντικές τεχνολογίες έχουν αναπτυχθεί για την καταπολέμηση της εξάπλωσης των worms του διαδικτύου. Δυστυχώς, δεν υπάρχει καμία ενιαία τεχνολογία που προστατεύει από όλους τους τύπους των κακόβουλων αυτών ιών. Πολλές επιχειρήσεις βασίζονται μόνο σε ένα μικρό σύνολο προστατευτικών τεχνολογιών για την προστασία των περιουσιακών τους στοιχείων, όπως τα τείχη προστασίας και τα προγράμματα ανίχνευσης ιών. Η μελέτη δείχνει ότι μια πολλών επιπέδων αμυντική λύση θα ήταν πιο αποτελεσματική στην πρόληψη απέναντι σε όλους τους γνωστούς φορείς ιών τύπου worm και, ενδεχομένως, σε πολλούς άγνωστους επίσης.

Το συμπέρασμα αυτό βασίζεται στην μελέτη μιας μεγάλης ποικιλίας από worms στο διαδίκτυο και τους αμυντικούς μηχανισμούς τους. Ως μέρος της έρευνάς, ανάπτυξα ένα σύστημα για την περιγραφή worms και μέτρησης κατά πόσο οι άμυνες μπορούν να τα σταματήσουν. Πιστεύω ότι η μέθοδος αυτή συλλαμβάνει τα κρίσιμα χαρακτηριστικά που καθορίζουν τα τρέχοντα worms καθώς και τα χαρακτηριστικά που θα μπορούσαν να εμφανίσουν στο μέλλον. Το σύστημά δείχνει ότι δεν υπάρχουν ενιαίες άμυνες που να λειτουργούν εις βάρος όλων των worms και ότι μόνο πολλαπλά επίπεδα αμυνών παρέχουν ισχυρή προστασία.

Η άμυνα σε βάθος βοηθά στην υπεράσπιση ενάντια όχι μόνο των worms, αλλά και σε άλλες απειλές του διαδικτύου, όπως δούρειους ίππους, κακόβουλους εισβολείς και χάκερς οι οποίοι έχουν μαντέψει κωδικούς πρόσβασης ή έχουν εισβάλλει στο σύστημα μέσω ατελειών του κώδικα δικτύου. Ενισχύεται η ασφάλεια με λύσεις οι οποίες είναι αποτελεσματικές, ακόμη και χωρίς περαιτέρω γνώση καμίας επίθεσης Τέτοιες λύσεις ασφάλειας λειτουργούν ακόμη και σε zero-day επιθέσεων [21], οι οποίες είναι οι επιθέσεις που κάνουν χρήση των άγνωστων τρωτών σημείων. Αντιδραστικές άμυνες, όπως η υπογραφή που βασίζεται σαρωτές ιών και των αυτοματοποιημένων συστημάτων είναι ακόμη αναγκαία, αλλά είναι αναποτελεσματικά εναντίον ραγδαίων εξελισσόμενων worms ή zero-day επιθέσεων.

Τα worms αποτελούν όλο και περισσότερο αναμειγνυομένων απειλών[22] που χρησιμοποιούν πολλές διαφορετικές μεθόδους για να επιτεθούν στα συστήματα Στην πραγματικότητα, χρησιμοποιούν μια επίθεση σε βάθος στρατηγική, προκειμένου να επιτύχουν την αποστολή τους. Ενιαίο σημείο λύσης μπορεί να είναι αν είμαστε σε θέση να εμποδίσουμε μερικούς από τους φορείς της επίθεσης, αλλά δεν θα είμαστε σε θέση να τους σταματήσουμε όλους.

[21] zero day attack είναι μια νέα, καινούρια ευπάθεια που ο προμηθευτής κάποιας εφαρμογής δεν γνωρίζει ακόμα και επομένως δεν υπάρχει το αντίστοιχο patch

[22] Symantec Security Response Glossary

6.2. Τι έκανα

Η μεθοδολογία μου περιλαμβάνει τη μελέτη μερικών από των πιο παραγωγικών σε ζημιά και εξελιγμένων worms των τελευταίων ετών. Αναπτύχτηκε μια μέθοδος κατάταξης των worms που βασίζεται στα χαρακτηριστικά που εμφανίζουν, την οποία αποκαλούμε «λειτουργίες της ζωής». Από τα χαρακτηριστικά αυτά, δημιούργησα ένα μεγάλο σύνολο χαρακτηριστικών επιθέσεων οι οποίες αντιπροσωπεύουν τις κατηγορίες των μέτρων που λαμβάνονται από τα worms για να εξασφαλιστεί η επιτυχής μόλυνση, επιβίωση και αναπαραγωγή. Τα χαρακτηριστικά των επιθέσεων ενάντια σε αμυντικές τεχνολογίες παρουσιάζονται στον πίνακα (Πίνακας **5**) που ονομάζεται «Πίνακας Άμυνας».

Ο πίνακας αποκαλύπτει ότι ορισμένοι αμυντικοί μηχανισμοί λειτουργούν καλύτερα σε βάρος συγκεκριμένων λειτουργιών της ζωής του worm. Αλλά για να επιτευχθεί η καλύτερη και ευρύτερη κάλυψη από την απειλή του worm μόνο μια άμυνα σε βάθος θα είναι αρκετή. Συγκεκριμένα, οι παραδοσιακές άμυνες περιμέτρου, όπως τα τείχη προστασίας, θα πρέπει να συμπληρώνεται με host-based σύστημα προστασίας.

Η μελέτη έδειξε πως οι επιθέσεις worms γίνονται σε βασικές δομικές μονάδες του συστήματος. Εξέτασα πάνω από 30 είδη worms και είδα ποιες συνθήκες και ενέργειες χρειάζονται για να επιτύχουν, παρατήρησα πάνω από 200 διαφορετικές συνθήκες. Μείωσα τις συνθήκες αυτές σε 14 γενικές κατηγορίες, τις οποίες τις ονομάζω «Γνωρίσματα της Επίθεσης Των Ίων Τύπου Worm». Πιστεύω ότι με το φράξιμο των εν λόγω δεκατεσσάρων κατηγοριών θα μπορούμε να ελέγξουμε τα worms.

Επίσης δείχνω πόσο καλά έντεκα κοινές άμυνες συμπεριφέρνονται για την καταπολέμηση του προβλήματος κατηγοριοποιώντας τες με βάση τα χαρακτηριστικά των επιθέσεων στον παρακάτω πίνακα. Ο Πίνακας 5, με τα χαρακτηριστικά επίθεσης από τη μια και τις άμυνες από την άλλη, δείχνει κατά πόσο μια άμυνα προσφέρει ελπίδα παρατηρώντας ή υπερασπίζοντας αυτό το σημείο τις επίθεσης. Η ένδειξη οδηγεί στο συμπέρασμα ότι κάποια προστασία παρέχεται ανάλογα με τα χαρακτηριστικά της επίθεσης.

Ιδιότητες Άμυνας / Ιδιότητες Επίθεσης	Τείχη Προστασίας - Φιλτράρισμα Πακέτων	Τείχη Προστασίας	Τείχη Προστασίας - Εφαρμογή Proxy	Συστήματα Ανίχνευσης Εισβολέων	Τείχη Προστασίας - Host	Virtual Μηχανήματα	Anti-virus Heuristics	AV with Heuristics	Host-Based Συστήματα Ανίχνευσης Εισβολέων	Integrity Έλεγχος	Stackguarding
Εκμετάλλευση Ευάλωτου Κώδικα Δικτύου	X	X	X	X	X		X				X
Παραπλάνηση του Χρήστη			X		X		X				
Εκμετάλλευση Ευάλωτων Ρυθμίσεων	X	X	X		X		X				
Εκμετάλλευση μιας Υπάρχουσας Πίσω Πόρτας	X	X	X		X			X			
Αλλαγές σε Αρχείο του Συστήματος							X		X	X	
Αλλαγές στις Ρυθμίσεις του συστήματος							X		X	X	
Τροποποίηση μιας Διεργασίας							X		X		
Πρόσβαση στο Δίκτυο	X	X	X		X				X		
Απαίτηση Ανεπτυγμένων Προνομίων							X		X		X
Performs Anomalous Queries							X		X		
Επικαλείται Κρίσιμα APIs						X			X		
Προκαλώντας Πλημμύρες Δικτύου	X	X	X		X				X		
Επιβραδύνει το Τοπικό Σύστημα									X		
Να Περιέχει Υπογραφές Worms			X	X				X			

Πίνακας 5 – Πίνακας Άμυνας

Τα πρώτα τέσσερα χαρακτηριστικά επίθεσης στον πίνακα άμυνας αντιστοιχούν στην πρώτη φάση του κύκλου ζωής του worm, το οποίο ονομάζω λοίμωξη λειτουργιών ζωής. Αυτό είναι όπου τα worms αποκτούν τον αρχικό έλεγχο του συστήματος

πρώτα και έπειτα εκτελούν τον κώδικα του. Οι υπόλοιπες ιδιότητες μπορούν να εφαρμοστούν σε οποιοδήποτε από τα μετέπειτα στάδια της ζωής των worms, είτε πρόκειται για την επιβίωση ή τον πολλαπλασιασμό τους. Ο πίνακας δείχνει ότι ορισμένες άμυνες είναι πιο αποτελεσματικές στο να εμποδίσουν την μόλυνση, ενώ άλλες είναι καλύτερες σε μεταγενέστερα στάδια της ζωής του worm.

Οι περισσότεροι αμυντικοί μηχανισμοί που χρησιμοποιούνται σήμερα επικεντρώνονται στην πρόληψη της αρχικής μόλυνσης, ένα ισχυρό τείχος προστασίας ή stackguarding είναι κάποιες αποτελεσματικές τεχνικές στον τομέα αυτό. Δυστυχώς, όπως φαίνεται στον πίνακα, αυτές οι τεχνικές δεν είναι επαρκείς. Η πλειοψηφία των worms στο δείγμα που έχουν μολύνει μηχανήματα, είναι αποτέλεσμα απευθείας εκτέλεση του worm από το χρήστη[23]. Τα τείχη προστασίας από μόνα τους δεν μπορούν να αντιμετωπίσουν αυτό το μηχανισμό της μόλυνσης, δεδομένου ότι δεν μπορούν να εμποδίσουν όλα τα μέσα με τα οποία τα αρχεία εισέρχονται στο σύστημα. Είναι ρεαλιστικό να εκτιμηθεί ότι οι χρήστες θα γίνουν πιο προσεκτικοί με το να αποφεύγουν να τρέχουν στο σύστημα άγνωστα αρχεία.

Πρέπει να υποτεθεί ότι τα worms θα είναι σε θέση να παρακάμπτουν περιμετρικές άμυνες και θα συνεχίσουν να παίρνουν τον έλεγχο των συστημάτων, όπως κάνουν τα τελευταία 15 χρόνια. Για τον λόγω αυτό, οι άμυνες πρέπει να προσανατολίζονται στο να μπλοκάρουν τα worms στα μεταγενέστερα στάδια της ζωής τους. Κατά τη διάρκεια της επιβίωσης και του πολλαπλασιασμού είναι τα στάδια όπου τα worms πρέπει γενικά να εκτελούν ενέργειες απευθείας στον μολυσμένο κεντρικό υπολογιστή. Προστασίες οι οποίες βρίσκονται κοντά στον κεντρικό υπολογιστή είναι καλύτερα προσαρμοσμένες για την υπεράσπιση ενάντια σε αυτές τις δράσεις του worm. Μόνο αυτές οι άμυνες είναι αρκετές για να κατανοήσουν τους πόρους του λειτουργικού συστήματος που χρησιμοποιείται από το worm.

Ο παραπάνω πίνακας δείχνει ότι τα **Host-Based Συστήματα Ανίχνευσης Εισβολέων** και η ισχυρή διαμόρφωση μπορούν να ανιχνεύσουν και να καταπολεμήσουν δώδεκα από τα δεκατέσσερα χαρακτηριστικά επίθεσης. Τα **Host-Based Συστήματα Ανίχνευσης Εισβολέων** προσφέρουν την καλύτερη προστασία ενάντια σε μεταγενέστερα στάδια της ζωής ενός worm. Επιβάλουν πολιτική συμπεριφοράς σε μια βάση ανά αίτηση. Αυτή η επιβολή της πολιτικής είναι ένα κρίσιμο στοιχείο της αμυντικής στρατηγικής μας, γιατί σχεδόν όλα τα worms επιδεικνύουν ανώμαλη συμπεριφορά σε σύγκριση με την αρχική τιμή της κανονικής λειτουργίας του συστήματος. Για παράδειγμα, προσβάλουν πόρους που θα πρέπει μόνο να αγγιχτούν μόνο κατά την εγκατάσταση του προγράμματος ή προσβάλουν πόρους που σχετίζονται με την επικοινωνία του δικτύου. Εργαλεία τα οποία παρέχουν προστασία κατά τα μεταγενέστερα στάδια της ζωής σε συνδυασμό με τα εργαλεία που εμποδίζουν αρχική λοίμωξη δεν αφήνουν κανένα χαρακτηριστικό επίθεσης που να μην μπορεί να προστατευθεί εναντίον τους.

6.3. Η Κατάσταση του Ιού Τύπου Worm

Αυτή η μελέτη έδωσε μια εικόνα για την κατάσταση της τεχνολογίας των worms. Κατά τη διάρκεια αυτής της μελέτης, είδα ένα ευρύ δείγμα των worms και μελέτησα τις συμπεριφορές τους. Από αυτή, κατάφερα να εκτιμήσω την πολυπλοκότητα του έργου τους και το μέλλον της τεχνολογίας τους. Από το ρυθμό με τον οποίο τα worms φαίνονται σε όλο το κόσμο και από τη δημοσιογραφική κάλυψη τους, θα μπορούσε να δημιουργηθεί η εντύπωση σε κάποιον ότι ο ιός τύπου worm είναι ένα πρόβλημα εκτός ελέγχου και είμαστε ανυπεράσπιστοι εναντίον του. Ενώ υπάρχουν πολλά worms που να έχουν ευρεία επιτυχία, καταλήγουμε στο συμπέρασμα ότι δεν εμφανίζουν συμπεριφορές που να μην μπορούν να αντιμετωπιστούν από ευρέως

[23] π.χ. κλικάρωντας πάνω του

διαθέσιμες άμυνες. Δυστυχώς, οι διαχειριστές συχνά αναπτύσσουν μόνο άμυνες που τείνουν να μην είναι τόσο «ενεργητικές» και δεν αντιμετωπίζουν επαρκώς όλες τις πτυχές του προβλήματος.

Έχει παρατηρηθεί κάποια πρόοδος στην κατάσταση των τεχνολογιών των worms. Έχουμε δει γρήγορα εξαπλωμένα worms, ιδιαίτερα καταστρεπτικά worms, με ειδικούς στόχους worms, τηλεκατευθυνόμενα worms, και βαριά θωρακισμένα worms (που είναι δύσκολο να αναλυθούν). Επιφανειακά, τα θέματα αυτά φαίνονται πολύ προχωρημένα, επανεξετάζοντας τα σε βάθος τον βαθμό πολυπλοκότητας τους παρατηρήσαμε ότι δεν έχουν κάνει τεράστια άλματα, αλλά η παρακολούθηση της τεχνολογίας που είναι διαθέσιμη μας δημιουργεί αυτήν την αίσθηση. Μόλις μια νέα τεχνολογία, όπως peer-to-peer δίκτυα, γίνει διαθέσιμη τότε οι μελετητές των worms θα τη χρησιμοποιήσουν για τη διάδοση και τον έλεγχο των worms.

Αν εξελιγμένοι αντίπαλοι έγραφαν τα worms, τότε θα περιμέναμε να δούμε περισσότερα worms που εκμεταλλεύονται τα κενά και δεν είναι γνωστά στο κοινό. Ο μικρός αριθμός αυτών των worms υποδηλώνει ότι οι συγγραφείς των ιών τύπου worm κάνουν απλώς χρήση των τρωτών σημείων που δημοσιεύονται στο Διαδίκτυο ώστε να οδηγήσουν την μόλυνση. Το οποίο επιβεβαιώνεται από τα συμπεράσματα. Τα worms που θεωρούνται παγκοσμίως τα πιο εξελιγμένα, δεν είναι αυτά που έχουν παρουσιάσει τις πιο προηγμένες τεχνικές, όπως να έχουν απομακρυσμένο έλεγχο, αλλά είναι αυτά που έχουν ενσωματώσει πιο αποτελεσματικά όλες τις διάφορες πτυχές των worms (τηλεχειριζόμενων, γρήγορη εξάπλωση, με ειδικούς στόχους, και ούτω καθεξής). Το Leave worm, για παράδειγμα, χρησιμοποιούσε πολλαπλούς φορείς μόλυνσης, που ήταν δύσκολο να αναλυθούν, χρησιμοποιούσε προηγμένη διοίκηση και έλεγχο καναλιών που διοχετευόταν μέσα από τα τείχη προστασίας, και ενεργοποιούσε ένα τηλεκατευθυνόμενο ελεγχόμενο πράκτορα για κάθε στόχο. Οι περιπτώσεις που μελέτησα δείχνουν ότι τα διάφορα στάδια της ζωής του Leave και άλλων worms μπορούν να προληφθούν με στρώση αμυνών.

7. ΠΑΡΑΔΕΙΓΜΑΤΑ: ΕΦΑΡΜΟΓΗΣ ΑΜΥΝΤΙΚΗΣ ΜΕΘΟΔΟΛΟΓΙΑΣ

Σε αυτή την ενότητα εφαρμόζω την μεθοδολογία μιας πολυεπίπεδης άμυνας σε πέντε επιθετικά ιστορικά worms για να δείξω πώς θα μπορούσαν να έχουν ηττηθεί.

7.1. YAHA.G

7.1.1. Μόλυνση

Περιγραφή

Ο Yaha χρησιμοποιεί δύο φορείς μόλυνσης για να κερδίσει τον αρχικό έλεγχο των συστημάτων που έχει θέσει ως στόχους. Πρώτον, προσπαθεί να εκμεταλλευτεί ένα λάθος στον τρόπο που οι κεφαλίδες MIME επεξεργάζονται μέσα στον Internet Explorer (οι πελάτες ηλεκτρονικού ταχυδρομείου της Microsoft χρησιμοποιούν τον Internet Explorer για την επεξεργασία των HTML μηνυμάτων ηλεκτρονικού ταχυδρομείου). Αυτή η ευπάθεια επιτρέπει σε έναν εισβολέα που χειρίζεται ορισμένες κεφαλίδες MIME να τρέχει αυτόματα ένα συνημμένο αρχείο binary. Ως αναπληρωματική λύση, ο Yaha μπορεί να αποκτήσει τον έλεγχο του συστήματος από την εξαπάτηση του χρήστη σε κλικ πάνω σε ένα εκτελέσιμο συνημμένο αρχείο.

Άμυνες

Τα ελαττώματα του MIME που εκμεταλλεύονται από τον Yaha θα μπορούσαν να μετριαστούν με την απενεργοποίηση λήψης αρχείων στο εσωτερικό των ζωνών ασφαλείας χαρακτηριστικό του Internet Explorer. Δεν υπάρχει γενική άμυνα για τη μόλυνση που προκαλεί ο χρήστης κάνοντας κλικ σε ένα συνημμένο. Ορισμένα τείχη προστασίας και διακομιστές αλληλογραφίας είναι σε θέση να φιλτράρουν το ηλεκτρονικό ταχυδρομείο και να αφαιρούν τον εκτελέσιμο κώδικα και scripts. Αυτό καθιστά την κατανομή των εκτελέσιμων αρχείων μέσω του ηλεκτρονικού ταχυδρομείου πιο δύσκολη, αλλά θα αποτρέψει αυτό το είδος του τύπου μόλυνσης.

7.1.2. Επιβίωση

Περιγραφή

Μετά την απόκτηση του ελέγχου της υποδοχής, ο Yaha αλλάζει το μητρώο και τον κατάλογο του συστήματος ώστε να εξασφαλίζεται ότι μπορεί να τρέχει συχνά. Συγκεκριμένα, τροποποιεί τα "HKLM \ exefile \ shell \ open \ command \ default" κλειδιά μητρώου και αντιγράφει τον εαυτό του στο κατάλογο συστήματος. Το worm μπορεί να επιχειρήσει να σκοτώσει οποιαδήποτε host-based τεχνολογία στην οποία στηρίζετε πριν την έναρξη της αναπαραγωγής του.

Άμυνες

Οι αλλαγές του αρχείο που κάνει ο Yaha στον κατάλογο του συστήματος ανιχνεύονται και από τον έλεγχο ακεραιότητας άλλα και από τα Host-Based συστήματα ανίχνευσης εισβολέων. Τα Host-Based συστήματα ανίχνευσης εισβολέων θα μπορούσαν να αποτρέψουν το αρχείο από το να εγγραφεί με επιτυχία, ενώ ο έλεγχος ακεραιότητας με το που εκτελούταν, θα μπορούσε να ανιχνεύσει τις αλλαγές. Οι ασφαλείς ρυθμίσεις, και με περιοριστικά δικαιώματα αρχείων, θα σταματούσαν επίσης τον Yaha από το να κάνει αλλαγές στο αρχείο.

Οι αλλαγές στο μητρώο από τον Yaha θα μπορούσαν να προληφθούν είτε από την ορθή διαμόρφωση ή από Host-Based συστήματα ανίχνευσης εισβολέων (HIPS). Η διαμόρφωση του συστήματος θα μπορούσε να αλλάξει για να περιορίσει την πρόσβαση σε ορισμένα κλειδιά μητρώου, έτσι θα αποτρεπόταν η απόπειρα του worm για να αποκτήσει πρόσβαση στο "exefile" κλειδί. Τα HIPS, επίσης, μπορούν να εξουδετερώσουν τις τροποποιήσεις του μητρώου σε μια πολιτική για την πρόληψη της πρόσβασης σε ορισμένα κλειδιά ή τις κυψέλες.

Ο Yaha επιχειρεί επίσης να σκοτώσει οποιαδήποτε πρόγραμμα τείχους προστασίας που θα βρει, υπό την προϋπόθεση ότι πρόκειται για μια εκδοχή του Yaha που ξέρει πώς να σκοτώσει (Όπως διάφορες παραλλαγές αυτού του worm προσπαθούν να απενεργοποιήσουν διάφορα προγράμματα της άμυνας). Ορισμένα τείχη προστασίας υποδοχής προειδοποιούν το χρήστη καθώς κλείνουν και του επιτρέπουν να εγκαταλείψει μια τέτοια ενέργεια, αυτό είναι ένα καλό χαρακτηριστικό που θα μπορούσε να αμβλύνει τους κινδύνους ενός κακόβουλου προγράμματος κλείνοντας ένα host-based τείχος προστασίας. Τα HIPS μπορούν επίσης να είναι αποτελεσματικά στην περίπτωση αυτή, καθώς τα εν λόγω συστήματα είναι σε θέση να εντοπίσουν ή να προλάβουν μια ενιαία διαδικασία που προσπαθεί να τροποποιήσει ή να ελέγξει κάποιο άλλο.

7.1.3. Διάδοση

Περιγραφή

Ο Yaha δημιουργεί μια λίστα με τις διευθύνσεις ηλεκτρονικού ταχυδρομείου, που έχει βάλει στόχο, από την αναζήτηση μέσω του Windows Address Book, το MSN Messenger, το ICQ, και άλλων πόρων email. Από τη στιγμή που έχει συλλέξει τα στοιχεία που χρειάζεται, ο Yaha προσπαθεί να βρει την προεπιλογή του διακομιστή SMTP ανατρέχοντας στα "HKCU \ Software \ Microsoft \ Internet Account Manager \ Accounts" κλειδιά μητρώου. Εάν δεν βρει την προεπιλογή του SMTP server, τοτε ο Yaha χρησιμοποιεί έναν προκαθορισμένο εξωτερικό διακομιστή και συνδέεται σε αυτόν χρησιμοποιώντας τη θύρα SMTP (TCP port25).

Άμυνες

Η αναγνώριση του Yaha για τις διευθύνσεις ηλεκτρονικού ταχυδρομείου θα μπορούσε να παρεμποδίζεται από ένα HIPS ρυθμισμένος να σταματάει τις προσβάσεις σε αρχεία ή κλειδιά μητρώου που περιέχουν διευθύνσεις ηλεκτρονικού ταχυδρομείου. Ομοίως, αυστηροί έλεγχοι σχετικά με την πρόσβαση στο μητρώο θα μπορούσαν να αποτρέψουν τέτοια αναγνώριση. Η πρόσβαση του worm στους SMTP servers είναι δυνατόν να προληφθεί με host-based και proxy που μπλοκάρουν τις συνδέσεις χωρίς άδεια. Ένα HIPS θα μπορούσε επίσης να συσταθεί για να αποτρέψει επικίνδυνα προγράμματα από την έκδοση εντολών για να συνδεθούν σε ένα διακομιστή SMTP.

7.1.4. Ωφέλιμο Φορτίο

Περιγραφή

Περιοδικά, ο Yaha προσπαθεί να συνδεθεί με το σύστημα www.pak.sov.pk που έχει θέσει ως στόχο.

Άμυνες

Αν πολλαπλά αντίγραφα του Yaha τρέχουν στο ίδιο τμήμα δικτύου, μια αξιοσημείωτη ποσότητα της κυκλοφορίας στο δίκτυο δημιουργείται. Αυτό μπορεί να ανιχνευθεί με IDSs και firewalls. Εάν ο διαχειριστής παρατηρήσει μια URL να δέχεται επιθέσεις,

μπορεί να ρυθμίσει firewalls ή HIPS για να εμποδίσει τις αιτήσεις προς τον προορισμό αυτό.

7.2. SLAMMER

7.2.1. Μόλυνση

Περιγραφή

Ο Slammer αποκτά τον έλεγχο του συστήματος χρησιμοποιώντας υπερχείλιση μνήμης στο SQL Server Resolution Service της Microsoft SQL Server και MSDE 2000 (ένα desktop data engine component που μοιράζεται κώδικα με τον SQL Server).

Άμυνες

Η ευαισθησία που εκμεταλλεύεται ο Slammer ήταν γνωστή και ένα patch ήταν διαθέσιμο τον Ιανουάριο του 2003, όταν ο ιός κυκλοφόρησε. Η τεράστια επίδραση και η ταχεία εξάπλωση του ιού είναι μια καλή ένδειξη του πόσο λίγοι διαχειριστές του συστήματος είχαν εφαρμόσει τα patches.

Η μόλυνση του Slammer θα μπορούσε να είχε μειωθεί σημαντικά αν περισσότερα συστήματα είχαν ρυθμιστεί σωστά. Γενικά δεν είναι απαραίτητο ότι ο SQL Server Resolution Service να είναι ορατός από το Internet, ούτε να τρέχει με τα ίδια δικαιώματα του συστήματος. Εάν αυτή η υπηρεσία δεν είναι ορατή από έξω τότε ο Slammer δεν μπορεί να εισβάλει. Εάν η υπηρεσία λειτουργεί ως μία απλού χρήστη, τότε η βλάβη του περιορίζεται από το λειτουργικό σύστημα αδειών.

Ένα σωστά ρυθμισμένο φιλτράρισμα των πακέτων του τείχους προστασίας θα μπορούσε να σταματήσει, τη λοίμωξη του Slammer κλειδώνοντας εισερχόμενα πακέτα που στοχεύουν το SQL Server Resolution Service. Υπάρχει σπάνια νόμιμος λόγος για την υπηρεσία να είναι προσβάσιμη μέσω του Διαδικτύου.

Η εκμετάλλευση της υπερχείλισης της μνήμης στην υπηρεσία θα μπορούσε να αποφευχθεί με stackguarding. Εναλλακτικά, ένα proxy τείχος θα μπορούσε να διενεργεί έλεγχο σχετικά με την εγκυρότητα του τομέα, που ξεχειλίζει ο Slammer.

7.2.2. Επιβίωση

Περιγραφή

Ο Slammer κατοικεί στη μνήμη και δεν κάνει μόνιμες αλλαγές στο μητρώο των Windows ή σε αρχεία του συστήματος για να εξασφαλίσει την επιβίωσή του στη μηχανή των στόχων του.

Άμυνες

Ο Slammer δεν προσπαθεί να αλλοιώσει το σύστημα. Δεν αμύνεται από host-oriented προστασίες που αναζητούν κατεστραμμένους πόρους.

7.2.3. Διάδοση

Περιγραφή

Διαδίδεται μέσω της παραγωγής μικρών πακέτων που εκμεταλλεύονται την ευπάθεια του SQL Resolution Service και τα αποστέλλουν στη IP διεύθυνση στο Internet. Η επιθετική διάδοση του Slammer δημιούργησε τεράστια ποσά κυκλοφορίας που πλημμύρισαν γρήγορα δίκτυα σε όλο τον κόσμο.

Άμυνες

Η διάδοση μπορεί να σταματήσει στις πύλες του δικτύου με σωστά ρυθμισμένο φιλτράρισμα των πακέτων του τείχους προστασίας. Εάν ξεφύγει από τα τείχη, ένα IDS μπορεί να είναι σε θέση να ανιχνεύσει τις πλημμύρες των πακέτων. Υπάρχουν λίγα που μπορούν να γίνουν σε ένα μολυσμένο υπολογιστή, εκτός από την αποσύνδεση του από το δίκτυο, την επανεκκίνηση του, καθώς και την εγκατάσταση νέων patches.

7.2.4. Ωφέλιμο Φορτίο

Περιγραφή

Ο Slammer δεν έχει ωφέλιμο φορτίο. Η διάδοση του worm κάνει όλη τη ζημιά.

Άμυνες

Ο Slammer δεν έχει ωφέλιμο φορτίο, έτσι δεν υπάρχει τίποτα για να αμυνθεί ενάντια.

7.3. BUGBEAR

7.3.1. Μόλυνση

Περιγραφή

Ο Bugbear εξαπλώνεται κυρίως από την εκτέλεση ενός συνημμένου αρχείου ηλεκτρονικού ταχυδρομείου που περιέχει το worm. Η εκτέλεση μπορεί να ξεκινήσει από ένα ανυποψίαστο χρήστη ή να ενεργοποιείτε μέσω μιας ευπάθειας στην MIME κεφαλίδα επεξεργάζοντας τον κώδικα στον Internet Explorer (το ίδιο ελάττωμα εκμεταλλεύεται και ο Yaha).

Άμυνες

Το φιλτράρισμα του ηλεκτρονικού ταχυδρομείου για την αφαίρεση του εκτελέσιμου συνημμένου και απενεργοποίηση λήψεις αρχείων του Internet Explorer είναι αποτελεσματικά μέτρα ενάντια στους φορείς μόλυνσης του Bugbear.

7.3.2. Επιβίωση

Περιγραφή

Ο Bugbear αντιγραφεί τον εαυτό του κατάλογο του συστήματος και τον θέτει στο φάκελο εκκίνησης, έτσι ώστε να εκτελεστεί κάθε φορά που το σύστημα κάνει επανεκκίνηση. Το RunOnce κλειδί στο μητρώο έχει οριστεί σε σημείο τέτοιο ώστε ο Bugbear να το χρησιμοποιεί ως εφεδρικό μέτρο για την εξασφάλιση ότι θα εκτελείται κατά την εκκίνηση του συστήματος.

Όπως και ο Yaha, έτσι και ο Bugbear επιχειρεί να θέσει εκτός λειτουργίας το λογισμικό ασφάλειας στον κεντρικό υπολογιστή. Απενεργοποιεί επίσης τις αυτόματες ειδοποιήσεις σε διάφορα σημεία, ώστε ο χρήστης να μην ειδοποιείται.

Άμυνες

Τα βήματα επιβίωσης που λαμβάνονται από τον Bugbear θα μπορούσαν να ελλατωθούν μέσω σφιχτών δικαιωμάτων στο μητρώο και το σύστημα αρχείων. Το μητρώο θα μπορούσε να ρυθμιστεί έτσι ώστε να περιορίσει την πρόσβαση σε κλειδιά που περιέχουν διευθύνσεις ηλεκτρονικού ταχυδρομείου. Περιοριστικά δικαιώματα βοηθούν μόνο εάν ο λογαριασμός πάνω στον οποίο τρέχει ο Bugbear δεν απαιτεί κανονικά πρόσβαση.

Τα HIPS μπορούν να παρεμποδίσουν τις λειτουργίες επιβίωσης του Bugbear, οι οποίες αποτελούνται από τροποποιήσεις στο μητρώο και το σύστημα αρχείων. Θα μπορούσαν, επίσης να μειώσουν τις προσπάθειες παύσης των antivirus και των host-based τειχών προστασίας, δεδομένου ότι μπορούν να ελέγξουν τη διαδικασία που συνδέεται με API.

7.3.3. Διάδοση

Περιγραφή

Ο Bugbear διαδίδεται από μηνύματα ηλεκτρονικού ταχυδρομείου που περιέχουν μολυσμένα συνημμένα αρχεία. Ο ιός χρησιμοποιεί διάφορα αντικείμενα όπως ονόματα σύνδεσης, καθώς και διευθύνσεις ηλεκτρονικού ταχυδρομείου προορισμού. Αυτό το καθιστά δύσκολο να φιλτράρετε με τείχη προστασίας που ελέγχουν το περιεχόμενο.

Εκτός από τη χρήση ηλεκτρονικού ταχυδρομείου ως μέθοδο πολλαπλασιασμού, ο Bugbear προσπαθεί να διαδοθεί μέσω ανοιχτών κοινόχρηστων αρχείων.

Άμυνες

Εξερχόμενα e-mail θα μπορούσαν να φιλτράρονται από ένα διακομιστή αλληλογραφίας ή προχωρημένο proxy τείχος προστασίας , το οποίο «πιάνει» τα εκτελέσιμα συνημμένα αρχεία.

Τα HIPS προφυλάσσουν από αναπληρωματικούς μηχανισμούς πολλαπλασιασμού του Bugbear, εξασφαλίζοντας ότι μόνο οι νόμιμες διαδικασίες έχουν πρόσβαση σε κοινόχρηστα αρχεία.

7.3.4. Ωφέλιμο Φορτίο

Περιγραφή

Ο Bugbear εγκαθιστά μια «πίσω πόρτα» που προαιρετικά να ακούει τις θύρες TCP 36794 και 1080. Η «πίσω πόρτα» ακούει τις εντολές που εκδίδονται από το συντάκτη του. Ένας keystroke logger εγκαθίσταται επίσης σε μολυσμένα μηχανήματα και δημιουργεί αρχεία στον κατάλογο του συστήματος.

Άμυνες

Ο καλύτερος τρόπος για την καταπολέμηση των ωφέλιμων φορτίων του Bugbear είναι να τα εμποδίσουν από το να εγκατασταθούν και να τρέξουν. Η σωστή ρύθμιση θα μπορούσε να κλειδώσει τους καταλόγους που χρησιμοποιεί το worm για να εγκαταστήσει την πίσω πόρτα και το keylogger. Τα HIPS θα μπορούσαν να προσέξουν για αλλαγές του συστήματος που εισάγουν αυτά τα ωφέλιμα φορτία.

Υποθέτοντας ότι τα στοιχεία του ωφέλιμου φορτίου τρέχουν, το φιλτράρισμα πακέτων (που πραγματοποιείται από οποιοδήποτε από τα διάφορα είδη των firewalls) θα μπορούσε να εμποδίσει τις εντολές από το να φτάσουν στην «πίσω πόρτα». Δυστυχώς, κλείνοντας μια από αυτές τις θύρες, 1080, απενεργοποιείται μια νόμιμη υπηρεσία και μπορεί να επηρεαστεί η λειτουργία του συστήματος. Αν όλα έχουν αποτύχει και η πίσω πόρτα μπορεί να καθοδηγηθεί από το έξω, οι εντολές που η πίσω πόρτα εκτελεί κατά πάσα πιθανότητα θα είναι out-of-character και συνεπώς θα στηριχθεί αμυντικά από HIPS. Τα keystroke logger επίσης, θα πραγματοποιήσουν ενέργειες οι οποίες μπορούν να ανιχνευθούν στην θύρα υποδοχής.

7.4. LEAVE

7.4.1. Μόλυνση

Περιγραφή

Ο Leave χρησιμοποιεί δύο βασικές τεχνικές για να μολύνει έναν κεντρικό υπολογιστή. Η κύρια μέθοδος της λοίμωξης είναι να επωφεληθεί από τον subSeven Trojan. Αυτή η μέθοδος της λοίμωξης απαιτεί από το θύμα να έχει προηγουμένως τεθεί σε κίνδυνο από μια έκδοση του SubSeven που έχει το συστατικό της πίσω πόρτας ενεργό.

Η δεύτερη μέθοδος του Leave δεσμεύει τον ίδιο τον εαυτό του σε ένα εκτελέσιμο αρχείο. Όταν ένα μολυσμένο πρόγραμμα εκτελείται, συνήθως εξαπατώντας τον χρήστη, ο Leave εκχειλίζεται και μολύνει το σύστημα.

Άμυνες

Το κύριο μέσο μόλυνσης του είναι χρησιμοποιώντας τον SubSeven Trojan. Ο SubSeven ήταν δυνατό να εντοπιστεί από λογισμικό ιών πολύ πριν την εμφάνιση του Leave. Εάν οι χρήστες είχαν ενημερωμένο λογισμικό προστασίας από ιούς, θα ήταν απαλλαγμένοι από τον SubSeven Trojan και θα είχαν ανοσία σε λοιμώξεις από τον Leave μέσω αυτής της μεθόδου. Επιπλέον, τα firewalls θα μπορούσαν να έχουν ρυθμιστεί ώστε να αποκλείουν τη θύρα που χρησιμοποιείται από την πίσω πόρτα του SubSeven.

7.4.2. Επιβίωση

Περιγραφή

Μόλις ο Leave διαπεράσει ένα σύστημα, λαμβάνει αμέσως μέτρα για να αποτρέψει την ανίχνευση και την αφαίρεση του. Επιλέγει κοινές εφαρμογές των Windows όπως το σημειωματάριο και ο Internet Explorer και επισυνάπτεται στα εκτελέσιμα αρχεία τους. Κάθε φορά που ένα από αυτά τα τροποποιημένα προγράμματα εκτελείται, ο Leave είναι σε θέση να ξαναμολύνει το σύστημα.

Επιπλέον, ο Leave τροποποιεί διάφορα κλειδιά μητρώου για να εξασφαλίσει ότι τα Windows θα τον εκτελούν κατά την εκκίνηση του συστήματος. Εάν αυτά τα κλειδιά μητρώου αναιρούνται, τότε η εκτέλεση μίας μολυσμένης εφαρμογής τα αποκαθιστά.

Άμυνες

Οι μηχανισμοί επιβίωσης του Leave μπορούν να μετριαστούν μέσω HIPSs και αρχείων ακεραιότητας του συστήματος. Τα HIPSs μπορούν να χρησιμοποιηθούν για την ανίχνευση και πρόληψη του Leave που επιχειρεί να τροποποιήσει τα κλειδιά μητρώου του συστήματος. Καθώς ο Leave βασίζεται σε κλειδιά μητρώου για να εκτελούν το λειτουργικό σύστημα, δεν θα εκτελούνται κατά την εκκίνηση, αν αυτά τα κλειδιά δεν είναι παρόντα.

Επίσης βασίζεται δεσμεύοντας τον εαυτό του με διάφορα προγράμματα που χρησιμοποιούνται συνήθως. Αρχεία ελέγχου ακεραιότητας του συστήματος μπορούν να ειδοποιήσουν αμέσως τον χρήστη όταν ένα πρόγραμμα επιχειρεί να τροποποιήσει άλλα εκτελέσιμα αρχεία.

7.4.3. Διάδοση

Περιγραφή

Ο αρχικός υιός Leave έχει τόσο ενεργό και παθητικό φορέα διάδοσης. Η ενεργή μέθοδος του πολλαπλασιασμού του περιλαμβάνει σάρωση του Διαδικτύου για υπολογιστές που έχουν μολυνθεί με τον SubSeven Trojan. Όταν ένα μολυσμένο μηχάνημα βρίσκεται, ο Leave χρησιμοποιεί τι πίσω πόρτα του SubSeven για να αντιγράψει τον εαυτό του στο απομακρυσμένο μηχάνημα. Οι εφαρμογές που μολύνει όταν διεισδύει σε ένα σύστημα μπορούν επίσης να χρησιμοποιηθούν και ως φορείς διάδοσης. Αν εκτελεστούν σε έναν άλλο υπολογιστή, τότε μολύνουν το νέο σύστημα.

Άμυνες

Ο Leave είναι εξαιρετικά οικείος με το δίκτυο. Ανιχνεύει για πιθανά θύματα στο διαδίκτυο και χρησιμοποιεί το IRC, HTTP, και NTP πρωτόκολλα κατά την κανονική λειτουργία του. Στηρίζεται στο δίκτυο σχεδόν σε όλες τις πτυχές του κύκλου ζωής του. Ένα τείχος θα αρνούταν αυτές τις δυνατότητες. Σε περίπτωση που ο Leave προσπαθήσει να έχει πρόσβαση σε οποιοδήποτε μέρος του δικτύου, τότε το τείχος προστασίας θα παρεμποδίσει αμέσως τη δράση αυτή και θα ειδοποιήσει τον χρήστη, ενώ οι δυνατότητες του δικτύου του θα είναι εντελώς σε κίνδυνο.

7.4.4. Ωφέλιμο Φορτίο

Περιγραφή

Ο Leave προσφέρει στο συντάκτη του τη δυνατότητα να έχει σχεδόν τον πλήρη έλεγχό ενός μολυσμένου μηχανήματος. Αφού διασφαλίζει την επιβίωσή του, συγχρονίζει το ρολόι συστήματος με διάφορους προσιτούς στο κοινό NTP (Network Time-Proiocol) servers. Συνδέεται με διάφορες ιστοσελίδες και κατεβάζει μια λίστα εντολών που μπορεί ο συγγραφέας του ιού να έχει δημοσιεύσει.

Συνδέεται επίσης με ένα ιδιωτικό κανάλι IRC και περιμένει εντολές που αποστέλλονται απευθείας από το δημιουργό. Οι εντολές που υποστηρίζει περιλαμβάνουν την δυνατότητα να τροποποιήσει το τοπικό σύστημα αρχείων, αντιγραφεί αρχεία, ανεβάζει/κατεβάζει και τροποποιεί αρχεία, επιτίθεται σε νέες θύρες και πολλά άλλα. Ο Leave μπορεί να λειτουργήσει ως ένα κακόβουλο εργαλείο απομακρυσμένης διαχείρισης με λίγους περιορισμούς.

Άμυνες

Ο Leave δεν έχει καμία πρόθεση να καταστρέψει τα δεδομένα στον κεντρικό υπολογιστή. Στην πραγματικότητα, αφαιρεί την SubSeven «πίσω πόρτα» για να αποτραπεί νέα προσβολή ή μόλυνση από ένα άλλο worm. Δεδομένου ότι όλες οι εντολές και ο έλεγχος πραγματοποιείται μέσω του δικτύου, ένα host-based firewall θα άφηνε τον Leave έξω από το δίκτυο.

7.5. NIMDA

7.5.1. Μόλυνση

Περιγραφή

Ο Nimda έχει τέσσερις φορείς λοίμωξης. Η πρώτη τεχνική λοίμωξης του είναι να εκμεταλλευτεί την ίδια κεφαλίδα MIME ευπάθειας στον Internei Explorer που χρησιμοποιήθηκε στον Yaha και στον Bugbear. Σε άλλα σενάρια μπορεί να προσπαθήσει να παραπλανήσει έναν χρήστη ώστε να εκτελέσει χειροκίνητα ένα συνημμένο ή να λάβει ένα αρχείο από το Internet. Ο τέταρτος φορέας λοίμωξη είναι η απομακρυσμένη εκμετάλλευση στην υπερχείλιση μνήμης στο www Microsoft Server IIS (Internet Information Services).

Άμυνες

Η κεφαλίδα MIME μεταγλωττίζει ευπαθή αποτελέσματα σε συνημμένα στο στάδιο της εκτέλεσης χωρίς κάποια ενέργεια του χρήστη. Αυτή η ευπάθεια μπορεί να εξαλειφθεί με την κατάλληλη πολιτική μεταγλώττισης. Φιλτράρισμα των συνημμένων, το οποίο γίνεται στο mail server ή firewall, μπορεί να καταργήσει κάθε παρόμοια συνημμένα πριν φτάσουν στον πελάτη. Η απενεργοποίηση λήψεων αρχείων στις Ζώνες ασφαλείας του Internet Explorer θα μπορούσε να αποτρέψει τους πελάτες από τυχαία λήψη οποιουδήποτε περιεχομένου από ένα μολυσμένο διακομιστή IIS.

Εάν ένας IIS συντάχθηκε με stackguarding, η υπερχείλιση του buffer στο IIS θα ήταν μη εκμεταλλεύσιμη, και για αυτό η μόλυνση αυτού του τομέα θα ήταν αναποτελεσματική.

7.5.2. Επιβίωση

Περιγραφή

Μετά την μόλυνση Nimda παίρνει πολλά μέτρα για να εξασφαλίσει ότι δεν μπορεί να αφαιρεθεί. Για την απόκρυψη της παρουσίας του, ο Nimda αντικαθιστά τις εφαρμογές του συστήματος, όπως mmc.exe (η Microsoft Management Console) στον κατάλογο των Windows. Στη συνέχεια, θα σαρώσει για έγγραφα του Microsoft Word και θα δημιουργήσει κακόβουλα αρχεία DLL (που περιέχουν ένα αντίγραφο του ιού) στους καταλόγους που βρίσκονται τα έγγραφα. Θα αλλάξει τις προτιμήσεις του χρήστη ώστε να μην εμφανίζονται γνωστές επεκτάσεις αρχείων ή κρυμμένα αρχεία έτσι ώστε το κακόβουλο DLLs δεν θα εμφανίζετε. Για να βεβαιωθεί ότι ο ιός εκτελείται κατά την εκκίνηση, ο Nimda τροποποιεί τις ρυθμίσεις μητρώου. Επίσης τροποποιεί τα αρχεία ρυθμίσεων, όπως το System.ini. Καταχωρείται επίσης ως μια υπηρεσία συστήματος, έτσι ώστε να είναι σε θέση να τρέξει ακόμη και όταν κανένας χρήστης δεν έχει εισέλθει.

Θα δημιουργήσει ανοιχτό κοινόχρηστο δίκτυο για όλους τους οδηγούς σχετικά με το μολυσμένο υπολογιστή. Τέλος, θα δημιουργήσει επίσης χρήστες που έχουν ενισχυμένα προνόμια για το μολυσμένο μηχάνημα και θα δώσει στους φιλοξενούμενους δικαιώματα διαχειριστή.

Άμυνες

Οι μηχανισμοί επιβίωσης του Nimda μπορούν να μετριαστούν με HIPSs, τα οποίο μπορούν να αμφισβητήσουν τις προσπάθειες του Nimda σχετικά με την τροποποίηση, τη δημιουργία και ή να διαγράψει τα αρχεία του συστήματος και τις ρυθμίσεις μητρώου. Μπορούν επίσης να αποτρέψουν ένα worm από τη δημιουργία επισφαλών λογαριασμών χρηστών με περιττά δικαιώματα, προκαλώντας κενά στη στάση της ασφάλειας. Τέλος, ένα HIPS μπορεί να ανιχνεύσει τις προσπάθειες που

κάνει ο Nimda ώστε να έχει πρόσβαση σε τμήματα του συστήματος μητρώου και αρχείων και τους αρνείται την πρόσβαση.

7.5.3. Διάδοση

Περιγραφή

Όταν ο Nimda προσπαθεί να διαδοθεί σε άλλα μηχανήματα, έχει μια ποικιλία μεθόδων στη διάθεσή του. Η πιο βασική τεχνική πολλαπλασιασμού του Nimda είναι ότι θα στείλει ένα αντίγραφο του εαυτού του σε μια διεύθυνση ηλεκτρονικού ταχυδρομείου, ελπίζοντας ότι ο απομακρυσμένος χρήστης θα είναι ευάλωτος σε μεταγλώττιση των MIME κεφαλίδων ή θα παρασυρθεί ώστε να εκτελέσει το συννημένο αρχείο. Ο Nimda έχει επίσης τη δυνατότητα αναζήτησης σε κοινόχρηστα στοιχεία δικτύου για έγγραφα του Microsoft Word και τη δημιουργία κακόβουλων αρχείων DLL που θα φορτωθούν από το Microsoft Word όταν ανοιχτούν τα έγγραφα.

Εάν ο χρήστης ανοίγοντας το έγγραφο βρίσκεται σε έναν απομακρυσμένο υπολογιστή, τότε θα μολύνεται και ο υπολογιστής. Ο Nimda επίσης αντιγράφει τον εαυτό του σε κοινόχρηστα στοιχεία δικτύου με την ελπίδα ότι οι απομακρυσμένοι χρήστες θα τα εκτελέσουν. Αφού ο Nimda ανιχνεύει για ευπαθείς διακομιστές IIS, μπορεί να εκμεταλλευτεί την υπερχείλιση μνήμης για να διαδοθεί σε ένα τέτοιο διακομιστή. Ο απομακρυσμένος server τότε θα μολυνθεί επίσης. Οι IIS servers που έχουν μολυνθεί με Nimda θα επιχειρήσουν να στείλουν αντίγραφα στους πελάτες του worm ιού όταν ζητούν περιεχόμενο.

Άμυνες

Οι περισσότερες από τις τεχνικές πολλαπλασιασμού Nimda περιλαμβάνουν αιτήματα για πρόσβαση στο δίκτυο. Αν τα αιτήματα αυτά είναι για να στείλουν μολυσμένα μηνύματα ηλεκτρονικού ταχυδρομείου ή να σαρώσουν για ευάλωτους διακομιστές IIS, ένα host-based τείχος θα μπορούσε να αποτρέψει αυτές τις ενέργειες. Όσο για την τροποποίηση των φακέλων σχετικά με το κοινόχρηστο δίκτυο, τα HIPS θα μπορούσαν να ανιχνεύσουν αυτή την ύποπτη συμπεριφορά και να προλάβουν τη σάρωση του δικτύου και την τροποποίηση των αρχείων συστήματος.

7.5.4. Ωφέλιμο Φορτίο

Περιγραφή

Αφού ο Nimda έχει μολύνει μια μηχανή, ξεκινά την εκτέλεση του ωφέλιμου φορτίου του. Κάθε δέκα ημέρες, ο Nimda υποκλέπτει διευθύνσεις ηλεκτρονικού ταχυδρομείου από το τοπικό μηχάνημα και αρχίζει τη μαζική αλληλογραφία σε αυτές τις διευθύνσεις. Αυτά τα μηνύματα έχουν ένα συνημμένο αρχείο που περιέχετε ο ιός. Ο Nimda θα μπορέσει να τον χρησιμοποιήσει για τη δική του μηχανή SMTP για να στείλει mail απευθείας σε ένα διακομιστή αλληλογραφίας, παρακάμπτοντας την ανάγκη για έναν πελάτη ηλεκτρονικού ταχυδρομείου επίσης θα εκδώσει αιτήσεις DNS MX για τον εντοπισμό διακομιστών ηλεκτρονικού ταχυδρομείου. Όταν ο Nimda αντιγράφει τον εαυτό του σε απομακρυσμένους διακομιστές IIS, θα ξεκινήσει ένας TFTP (Trivial File Transfer Protocol) server για να βοηθήσει στη λειτουργία αναπαραγωγής του.

Άμυνες

Ο Nimda θα τρέχει τη δική του μηχανή SMTP, εκτελώντας αναζητήσεις DNS, και θα αρχίσει έναν TFTP (Trivial File Transfer Protocol) server. Δεδομένου ότι κάθε μία από αυτές τις υπηρεσίες χρειάζεται πρόσβαση στο δίκτυο, μια αντιπυρική ζώνη υποδοχής θα μπορούσε να αρνηθεί αυτές τις αιτήσεις για πρόσβαση στο δίκτυο.

Άμυνα / Worm	Τείχη Προστασίας - Φιλτράρισμα Πακέτων	Τείχη Προστασίας - Stateful	Τείχη Προστασίας - Εφαρμογή Proxy	Συστήματα Ανίχνευσης Εισβολέων	Τείχη Προστασίας - Host	Εικονικά Μηχανήματα	Διαμόρφωση	Anti-virus Heuristics	Host-Based Συστήματα Ανίχνευσης Εισβολέων	Έλεγχος Ακεραιότητας	Stackguarding
YAHA			X		X		X		X	X	
SLAMMER	X	X	X	X	X		X			X	X
BUGBEAR			X		X		X		X	X	
LEAVE	X	X	X		X			X	X		
NIMDA			X	X	X		X		X	X	X

Πίνακας 6 – Σύνοψη των αποτελεσμάτων της υπόθεσης

ΒΙΒΛΙΟΓΡΑΦΙΑ – ΠΗΓΕΣ

- The Worm Information Center, http://www.networm.org/faq
- CERT Coordination Center, http://www.cert.org
- F-Secure Virus Info Center, http://www.f-secure.com/virus-info
- Kaspersky Labs Virus Encylopedia, http://www.viruslist.com
- Network Associates AVERT Virus Information Library, http://vil.nai.com
- Sophos Virus Information, http://www.sophos.com/virusinfo
- Symantec Security Response, http://www.securityresponse.symantec.com/avcenter
- Trend Micro Virus Encylopedia, http://www.trendmicro.com/vinfo
- Virus Bulletin, http://www.virusbtn.com/resources/viruses/index.xml
- MITRE Common Vulnearbilities, cve.mitre.org
- Microsoft Security Bulletins, http://www.microsoft.com/technet/security
- Symantec Security Response Glossary, http://securityrespone.symantec.com/avcenter/refa.html
- CAIDA analysis of Code Red. http://www.caida.org/analysis/security/code-red
- Eeye Blaste Analysis, http://www.eeye.com/Research/Advisories/AL20030811.html
- D. Moore, C. Shannon, K. Claffy, “Code Red: a case study on the spread and victims of an Internet worm”
- J. Van Hoogstraten, “Blasting Windows: An Analysis of the W32/Blaster Worm”, http://www.giac.org/practical/GCIH/John_VanHoogstraten_GCIH.pdf
- E. Manrique, “An Analysis of W32.Bugbear and the Technical Procedural Controls Needed for Protection”. http://www.giac.org/practical/GCIH/Edmundo_Manrique_GCIH.pdf
- A. Marinescu, “An Analysis of Simile”, http://www.securityfocus.com/infocus/1671
- P. Ferrie, “WHO? WHAT? WHERE? SWEN?”, http://pferrie.tripod.com/swen.pdf
- P. Ferrie, “Klez”, http://torondo.virusbtn.com/magazine/archives/200207/klez.xml
- Max Vision, “Lion Internet Worm Analysis”, http://www.whitehats.com/library/worms/lion
- Max Vision, “Ramen Internet Worms Analysis”, http://www.whithats.com/library/worms/ramen
- D. Moore, C. Shannon, G.M. Voelker, S. Savage, Internet Quarantine: Requirements for Containing Self-Propagating Code”, Infocom 2003
- S. Stanford, V. Paxson, N. Weaver, “How to own the Internet in Your Spare Time” in Proceedings of the 11th USENIX Security Symposium, San Francisco, CA, August 2002
- C. Cowan, C. Pu, D. Maier, H. Hilton, j. Walpole, P. Bakke, S. Beattie, A. Grier, P. Wagle, Q. Zhang, “StackGuard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks”
- E. Spafford, “Computer Viruses as Artificial Life”
- D. Chess, S. White, Än Undetectable Computer Virus”
- J. Nazario, J. Anderson, R. Wash, C. Connelly, “The Future of Internet Worms”, Crimelabs Research, http://www.crimelabs.net
- P. K. Singh “A Physiological Decomposition of Virus and Worms Programs”
- Tripwire Integrity Assurance Company, http://www.tripwire.com

- D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, V. Weaver, “The Spread of the Sapphire/Slammer Worm”, http://www.silicondefence.com/research/slammer