ΠΑΝΕΠΙΣΤΗΜΙΟ ΠΕΛΟΠΟΝΝΗΣΟΥ ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

ΑΣΦΑΛΕΙΑ ΥΠΟΛΟΓΙΣΤΙΚΩΝ ΣΥΣΤΗΜΑΤΩΝ

ΖΟΡΜΠΑΣ ΘΕΟΔΩΡΟΣ

ΚΟΚΟΒΙΚΑΣ ΓΕΩΡΓΙΟΣ

ΕΠΙΒΛΕΠΩΝ: ΠΑΡΑΣΚΕΥΑΣ ΚΙΤΣΟΣ

ΠΑΤΡΑ 2021

Υπεύθυνη Δήλωση Φοιτητών

Βεβαιώνουμε ότι είμαστε συγγραφείς αυτής της εργασίας και ότι κάθε βοήθεια την οποία είχαμε για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης έχουμε αναφέρει τις όποιες πηγές από τις οποίες κάναμε χρήση δεδομένων, ιδεών ή λέξεων, είτε αυτές αναφέρονται ακριβώς είτε παραφρασμένες. Επίσης βεβαιώνουμε ότι αυτή η εργασία προετοιμάστηκε από εμάς προσωπικά ειδικά για τη συγκεκριμένη διπλωματική εργασία.

Η έγκριση της διπλωματικής εργασίας από το Τμήμα Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών του Πανεπιστημίου Πελοποννήσου δεν υποδηλώνει απαραιτήτως και αποδοχή των απόψεων του συγγραφέα εκ μέρους του Τμήματος.

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία των φοιτητών που την εκπόνησαν. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης ο συγγραφέας/δημιουργός εκχωρεί στο Πανεπιστήμιο Πελοποννήσου, μη αποκλειστική άδεια χρήσης του δικαιώματος αναπαραγωγής, προσαρμογής, δημόσιου δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσής τους διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος και για όλο το χρόνο διάρκειας των δικαιωμάτων πνευματικής ιδιοκτησίας. Η ανοικτή πρόσβαση στο πλήρες κείμενο για μελέτη και ανάγνωση δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, αποθήκευση, πώληση, εμπορική χρήση, μετάδοση, διανομή, έκδοση, εκτέλεση, «μεταφόρτωση» (downloading), «ανάρτηση» (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού. Ο συγγραφέας/δημιουργός διατηρεί το σύνολο των ηθικών και περιουσιακών του δικαιωμάτων.

Περίληψη

Πολλές πολιτικές ασφάλειας υπολογιστών γράφονται σχετικά αόριστα. Με πολλούς τρόπους, αυτό είναι σκόπιμο να επιτρέπει ευκολότερη πρόσβαση σε όλες τις λειτουργίες του δικτύου υπολογιστών. Ωστόσο, η υπερβολική ευελιξία επιτρέπει στους χρήστες, χωρίς να χρειάζεται να έχουν πρόσβαση σε πολλές από τις λειτουργίες του δικτύου, τη δυνατότητα εκτέλεσης λειτουργιών που ενδέχεται να προκαλέσουν βλάβη στο σύστημα ή να παρέχουν πρόσβαση σε πληροφορίες που δεν χρειάζεται να δουν. Έχοντας αυτό κατά νου, αυτή η πτυχιακή εργασία ρίχνει μια ματιά στην ασφάλεια των υπολογιστικών συστημάτων. Ξεκινά με ένα σύντομο ιστορικό ασφάλειας υπολογιστών και συνεχίζει με μια ματιά στην εσωτερική ασφάλεια. Δεδομένου ότι η εστίαση είναι στην κακή χρήση και τον εντοπισμό υπολογιστών, μια ματιά στην εσωτερική ασφάλεια παρέχει μια ματιά στους λόγους για τους οποίους πρέπει να γίνει προσπάθειαπαρακολούθησηςστις δραστηριότητες των χρηστών. Η ανίχνευση κακής χρήσης απαιτεί τουλάχιστον δύο δυνατότητες. Αυτές είναι η ικανότητα ελέγχου και δημιουργίας προφίλ. Όταν οι λειτουργίες ελέγχου είναι ενεργοποιημένες στο λειτουργικό σύστημα, μπορούν να δημιουργηθούν τεράστια αρχεία. Με την καθιέρωση προφίλ χρήσης προσωπικού, οι αυτοματοποιημένες δυνατότητες ελέγχου μπορούν να σαρώσουν γρήγορα αρχεία ελέγχου, να αναζητήσουν χρήση που βρίσκεται εκτός από το τι είναι καθορισμένο να είναι φυσιολογικό, να ειδοποιεί τους διαχειριστές και να διαγράφει παλιά δεδομένα ελέγχου. Ένα σύστημα εντοπισμού κακής χρήσης, όπως το σύστημα ανίχνευσης κακής χρήσης υπολογιστή που διατίθεται στο εμπόριο από τα ODsNetworks, μπορεί να εφαρμοστεί και να ενσωματωθεί σε μια ολοκληρωμένη πολιτική ασφάλειας.

Περιεχόμενα

Περίληψη 4

Περιεχόμενα 5

Εισαγωγή 6

Κεφάλαιο 1ο: Ιστορικά δεδομένα ασφάλειας υπολογιστικών συστημάτων 7

1.1. Επισκόπηση 7

1.2. Θεμέλια ασφάλειας υπολογιστικών συστημάτων 7

1.3. Απειλές και ευπάθειες 9

1.4. Εξέλιξη των σύγχρονων περιβαλλόντων 10

1.5. Προσπάθειες ασφαλείας 13

Κεφάλαιο 2ο: Κακόβουλο λογισμικό 19

2.1. Τύποι κακόβουλου λογισμικού (Malware) 20

2.2. ΠροχωρημένηΕπίμονηΑπειλή (Advanced Persistent Threat) 24

2.3. Διάδοση – ΜολυσμένοΠεριεχόμενο – Ιοί (Propagation – Infected Content – Viruses) 25

2.4. Διάδοση – Εκμετάλλευση Ευπάθειας – Υπολογιστικό Σκουλήκι (Worms) 33

2.5. Διάδοση – Κοινωνική Μηχανική - Ανεπιθύμητα Μηνύματα Ηλεκτρονικού Ταχυδρομείου, Δούρειος Ίππος (TrojanHorse – Trojans) 44

2.6. Ωφέλιμο Φορτίο – Διαφθορά Συστήματος 48

2.7. Ωφέλιμο Φορτίο – Επιθέσεις DDoS – Zombies, Bots 51

2.8. Ωφέλιμο Φορτίο – Κλοπή Πληροφοριών – Keyloggers, Phising, Spyware 54

2.9. Ωφέλιμο Φορτίο – Κρυφή Κλοπή (Stealthing) – Backdoors, Rootkits 58

2.10. Αντίμετρα 63

Κεφάλαιο 3ο: Ασφάλεια Λειτουργικού Συστήματος 74

3.1. Εισαγωγή στην Ασφάλεια Λειτουργικού Συστήματος 75

3.2. Σχεδιασμός Ασφάλειας Συστήματος 75

3.3. Σκλήρυνση Λειτουργικών Συστημάτων 77

3.4. Ασφάλεια Εφαρμογών 84

3.5. Συντήρηση ασφαλείας 86

3.6. Παράδειγμα ασφάλειας (WINDOWS) 88

ΣΥΜΠΕΡΑΣΜΑΤΑ 93

Βιβλιογραφία 94

Εισαγωγή

Καθώς πλησιάζει το τέλος του εικοστού αιώνα, ο κόσμος βρίσκεται στη μέση μιας τεχνολογικής επανάστασης με ολοένα αυξανόμενη εξάρτηση από υπολογιστές και συστήματα υπολογιστών. Με αυτήν την αυξανόμενη εξάρτηση, η ανάγκη προστασίας αυτών των συστημάτων και των δεδομένων που περιέχονται στις βάσεις δεδομένων τους έχει καταστεί σημαντική προτεραιότητα για τις κυβερνήσεις και την ιδιωτική βιομηχανία.

Μία πτυχή αυτής της προστασίας είναι η ανάγκη σωστού εντοπισμού προσωπικού που έχει πρόσβαση σε ευαίσθητες πληροφορίες και η αποτροπή εκείνου που δεν έχει πρόσβαση σε αυτές τις πληροφορίες. Με την συνεχώς αυξανόμενη συνδεσιμότητα μεταξύ των δικτύων εσωτερικών προς μια επιχείρηση και μεταξύ των επιχειρήσεων, η έννοια του προφίλ του χρήστη συνεχίζει να εξελίσσεται. Το προφίλ δεν είναι νέο και έχει χρησιμοποιηθεί σε πολλούς τομείς εκτός από τη διαχείριση συστημάτων πληροφοριών. Οι υπηρεσίες της Ομοσπονδιακής Κυβέρνησης ενδιαφέρονται ιδιαίτερα για την ανάπτυξη προφίλ υπολογιστή σε επίπεδο χρήστη για τις ολοένα αυξανόμενες βάσεις δεδομένων ομάδων, υποομάδων και μεμονωμένων χρηστών.

Μια καλά καθορισμένη πολιτική ασφάλειας υπολογιστών είναι το θεμέλιο ενός επιτυχημένου προγράμματος ασφαλείας. Επομένως, προκειμένου να επωφεληθούμε από την πιθανή ισχύ της πρόσβασης σε προφίλ χρηστών, είναι υψίστης σημασίας η ενσωμάτωση του προφίλ στην πολιτική ασφάλειας υπολογιστών ενός οργανισμού. Η ενσωμάτωση των χρηστών παρακολούθησης μαζί με την περιοδική εκπαίδευση θα ενισχύσει σημαντικά ένα πρόγραμμα ασφάλειας συστημάτων.

Η αξιολόγηση και ο έλεγχος ενός εμπορικά διαθέσιμου λογισμικού προφίλ υπολογιστών πραγματοποιήθηκε για να καθοριστεί εάν το προϊόν μπορεί να αποδώσει όπως διαφημίζεται σε συστήματα υπολογιστών τύπου Υπουργείου Άμυνας. Αφού εξετάσαμε αρκετά πακέτα λογισμικού, επιλέξαμε ένα υποδειγματικό πακέτο εφαρμογών που παρείχε τα απαραίτητα εργαλεία που απαιτούνται για την εκτέλεση του προφίλ των χρηστών. Το Σύστημα Ανίχνευσης Κατάχρησης Υπολογιστών (CMDS), που αναπτύχθηκε από την ODsNetworksInc., παρέχει ανίχνευση εισβολών, εγκληματολογία δεδομένων, διαχείριση ελέγχου και ένα ολοκληρωμένο σύστημα προφίλ χρήστη. Ο δεύτερος στόχος μας ήταν να ενσωματώσουμε ένα πρόγραμμα παρακολούθησης στην πολιτική ασφάλειας υπολογιστών ενός οργανισμού.

Κεφάλαιο 1ο: Ιστορικά δεδομένα ασφάλειας υπολογιστικών συστημάτων

1.1. Επισκόπηση

Οι υπολογιστές χρησιμοποιούνται σήμερα περισσότερο από ποτέ για να πραγματοποιούν επιχειρηματικές συναλλαγές, να αποθηκεύουν ευαίσθητα δεδομένα και να εκτελούν προσωπικές εργασίες στο σπίτι. Η ικανότητα ανταλλαγής πληροφοριών έχει αυξηθεί σημαντικά καθώς οι υπολογιστές συνδέονται με δίκτυα, δημιουργώντας συστήματα υπολογιστών. Οι πληροφορίες που περιέχονται σε αυτά τα συστήματα υπολογιστών είναι το κύριο επίκεντρο των σημερινών πολιτικών ασφάλειας υπολογιστών. Ποιες είναι αυτές οι πληροφορίες; Είναι πληροφορίες που σχετίζονται με κάθε λεπτομέρεια της ζωής μας - ιατρικά αρχεία, δεδομένα ποινικής έρευνας, τραπεζικές συναλλαγές και αρχεία προσωπικού. Είναι πληροφορίες που θέλουμε να διατηρήσουμε απόρρητες. Κάθε οργανισμός θα έχει μια μοναδική πολιτική ασφάλειας υπολογιστή προσαρμοσμένη στις συγκεκριμένες ανάγκες του οργανισμού. Προκειμένου να κατανοήσουμε πλήρως την τρέχουσα κατεύθυνση που οδηγεί η ασφάλεια του υπολογιστή, όσον αφορά την τεχνολογία προφίλ, είναι σημαντικό να εξετάσουμε τις αρχές του. Αυτό το κεφάλαιο αφηγείται εν συντομία την αξιολόγηση σε περιβάλλοντα υπολογιστών και την ασφάλεια του υπολογιστή που ακολούθησε αναπόφευκτα.

1.2. Θεμέλια ασφάλειας υπολογιστικών συστημάτων

Το πρώτο βήμα για την ανάπτυξη οποιασδήποτε πολιτικής είναι ο καθορισμός του στόχου, στην περίπτωσή μας πολιτικής ασφάλειας υπολογιστών. Τι είναι η ασφάλεια του υπολογιστή; Με απλά λόγια - είναι η προστασία του συστήματος υπολογιστή και όλου του σχετικού εξοπλισμού. Αυτό περιλαμβάνει τόσο φυσικές όσο και λογικές αποθήκες δεδομένων.

Υπάρχουν τρεις θεμελιώδεις ακρογωνιαίοι λίθοι της ασφάλειας του υπολογιστή - εμπιστευτικότητα, ακεραιότητα και διαθεσιμότητα. Η εμπιστευτικότητα διασφαλίζει ότι τα δεδομένα που είναι αποθηκευμένα σε ένα σύστημα υπολογιστή προστατεύονται και απελευθερώνονται μόνο σε εξουσιοδοτημένους χρήστες. Περιλαμβάνει στοιχεία όπως πληροφορίες μισθοδοσίας, επίσημο email ή δεδομένα προσωπικού για υπαλλήλους. Έχει σημαντική σημασία σε ένα στρατιωτικό περιβάλλον. Για παράδειγμα, η κυκλοφορία μηνυμάτων που αποθηκεύεται κεντρικά και μπορεί να προσεγγιστεί από το προσωπικό εντολών σε διάφορα

επίπεδα ταξινόμησης που κυμαίνονται από το μη ταξινομημένο έως το απόρρητο. Είναι εξαιρετικά σημαντικό μόνο το προσωπικό με την κατάλληλη άδεια ασφαλείας να είναι σε θέση να διαβάζει μηνύματα, στο ή «κάτω» από το επίπεδο ασφάλειας.

Η ακεραιότητα επικεντρώνεται στην αποτροπή μη εξουσιοδοτημένης τροποποίησης δεδομένων. Για παράδειγμα, η ακεραιότητα είναι εξαιρετικά σημαντική για τα τραπεζικά ιδρύματα, των οποίων οι πελάτες απαιτούν ακρίβεια στον υπολογισμό και την αποθήκευση πολύ οικονομικών συναλλαγών. Μέσα στον στρατό, είναι ύψιστης σημασίας να διασφαλιστεί ότι η επισκεψιμότητα των μηνυμάτων που λαμβάνεται είναι ακριβής και δεν έχει τροποποιηθεί από χάκερ. Οι επιχειρησιακοί διοικητές πρέπει να γνωρίζουν ότι τα μηνύματα που παρέχουν συντεταγμένες για επιθέσεις πυραύλων δεν έχουν τροποποιηθεί από το. μη εξουσιοδοτημένοparty. Ένα ανακριβές μήνυμα θα μπορούσε να οδηγήσει σε αποτυχημένη αποστολή, απώλειες πολιτών ή να έχει σημαντικές πολιτικές επιπτώσεις. Επιπλέον, οι εχθρικοί χάκερ θα μπορούσαν να υποκλέψουν και να παραποιήσουν πληροφορίες όπως αριθμούς στρατευμάτων, τοποθεσία ή πιθανά σχέδια επίθεσης.

Η διαθεσιμότητα έχει δεδομένα και άλλους υπολογιστικούς πόρους εύκολα προσβάσιμους κατά παραγγελία. Μια εταιρεία Διαδικτύου θα ήταν γρήγορα εκτός επιχείρησης εάν οι πελάτες δεν μπορούσαν να έχουν πρόσβαση σε δεδομένα στον ιστότοπο της εταιρείας. Οι υπολογιστές είναι ο ακρογωνιαίος λίθος των περισσότερων στρατιωτικών συστημάτων όπλων. Αυτά τα συστήματα πρέπει να έχουν υψηλό ποσοστό διαθεσιμότητας για την άμεση διεξαγωγή στρατιωτικών επιχειρήσεων.

Εκτός από αυτές τις θεμελιώδεις ιδιότητες, υπάρχουν πολλές δευτερεύουσες ανησυχίες που πρέπει επίσης να ληφθούν υπόψη κατά την ανάπτυξη μιας πολιτικής ασφάλειας, όπως η συνέπεια, ο έλεγχος και οι έλεγχοι. Η συνέπεια συνεπάγεται τη διασφάλιση της συμπεριφοράς του συστήματος όπως αναμενόταν. Ο έλεγχος ρυθμίζει την πρόσβαση στο σύστημά σας. Οι έλεγχοι διενεργούνται για την παρακολούθηση της χρήσης του συστήματος από τους υπαλλήλους καθώς και την πρόσβαση από εξωτερικά συμφέροντα.

1.3. Απειλές και ευπάθειες

Όλα τα συστήματα υπολογιστών είναι ευαίσθητα σε ορισμένες απειλές και είναι ευάλωτα σε κάποιο βαθμό επιθέσεων. Η ασφάλεια των υπολογιστών ασχολείται με την προστασία των συστημάτων από διάφορες απειλές και τον εντοπισμό τρωτών σημείων του συστήματος. Οτιδήποτε μπορεί να προκαλέσει ζημιά σε ένα σύστημα θεωρείται απειλή. Οι απειλές εμπίπτουν σε τρεις διαφορετικές κατηγορίες: φυσικές, ακούσιες και εκ προθέσεως. (Russell&Gangemi, 1991) Οι φυσικές απειλές είναι απρόβλεπτα γεγονότα όπως πυρκαγιές, πλημμύρες ή απροσδόκητες εξελίξεις. Αθέλητες απειλές κατά κύριο λόγο μπορεί να προκύψουν λόγω της κακής εκπαίδευσης ασφαλείας. Για παράδειγμα, σημαντικές απειλές για τα συστήματα υπολογιστών μπορεί να προέρχονται από έναν απρόσεκτο χρήστη που δίνει τον κωδικό πρόσβασής του σε έναν φίλο ή έναν διαχειριστή συστήματος που δεν κατανοεί πλήρως την πολιτική ασφαλείας ή πώς να διατηρήσει, μηχανισμούς ασφαλείας (π.χ., τείχη προστασίας). Ωστόσο, υπάρχουν πολλές εκ προθέσεως απειλές που μπορούν να προκαλέσουν καταστροφικές ζημιές σε οργανισμούς. Οι εκ προθέσεως απειλές μπορεί να είναι είτε εξωτερικές είτε εσωτερικές και προέρχονται από μεγάλη ποικιλία πηγών. Οι εξωτερικές απειλές είναι αυτές που οι περισσότεροι άνθρωποι γνωρίζουν και αποτελούνται από κράκερ, χάκερ, τρομοκράτες, εταιρικούς επιδρομείς ή ξένους πράκτορες πληροφοριών. Διεισδύουν σε συστήματα χρησιμοποιώντας μια ποικιλία μεθόδων, από απομακρυσμένα ηλεκτρονικά διαλείμματα έως δωροδοκία υπαλλήλων για ενημέρωση. Οι εσωτερικές απειλές προέρχονται από προσωπικό που έχει πρόσβαση στο σύστημα και για κάποιο λόγο, πιθανώς λόγω κακίας, αποφασίζει να διακόψει ή να κλέψει πληροφορίες. Αυτές οι απειλές μπορούν να προέλθουν από καταβολή κατασκοπικών εταιρειών για απόκτηση εταιρικών μυστικών ή απλώς δυσαρεστημένους υπαλλήλους. Έχει εκτιμηθεί ότι το 80% των διεισδύσεων του συστήματος προέρχονται από προσωπικό που είχε πλήρη πρόσβαση στο σύστημα που εκτελεί μη εξουσιοδοτημένες λειτουργίες. (Russell&Gangemi, 1991)

Δεν υπάρχει κανένα απόλυτα ασφαλές σύστημα υπολογιστών: κάθε σύστημα υπολογιστή έχει μια Αχίλλειο Πτέρνα. Είναι σημαντικό να κατανοήσουμε τις ευπάθειες ενός συστήματος κατά την ανάπτυξη μιας πολιτικής ασφάλειας. Τα τρωτά σημεία του συστήματος μπορούν να χωριστούν στις ακόλουθες κατηγορίες: (Russell&Gangemi, 1991)

- Φυσικές ευπάθειες: Το κτίριο γραφείων και οι αίθουσες υπολογιστών πρέπει να είναι ασφαλείς για την αποφυγή εισβολών από εισβολείς. Πολλές συσκευές είναι διαθέσιμες για να εμποδίσουν τους εισβολείς να αποκτήσουν πρόσβαση. «Κλειδαριές» κρυπτογράφησης, σάρωση αμφιβληστροειδούς, φωνητικό αποτύπωμα, δακτυλικό αποτύπωμα και συναγερμοί ασφαλείας όλα παρέχουν ένα αποτελεσματικό αποτρεπτικό.
- Φυσικές ευπάθειες: Φυσικές καταστροφές όπως πλημμύρες, πυρκαγιές ή υπερτάσεις που μπορούν να προκαλέσουν απώλεια δεδομένων.
- Ευπάθειες λογισμικού: Οι αστοχίες λογισμικού μπορεί να προκαλέσουν βλάβη στο σύστημα του υπολογιστή σας. Μπορεί επίσης να περιέχουν "τρύπες" και / ή "πόρτες παγίδας" που μπορούν να επιτρέψουν σε έναν εισβολέα πρόσβαση στο σύστημα και τις πληροφορίες σας.
- Ευπάθειες Emanation: Ο ευαίσθητος ηλεκτρονικός εξοπλισμός που αποτελεί ένα σύστημα υπολογιστή είναι εξαιρετικά ευάλωτος σε ηλεκτρομαγνητικές επιθέσεις. Επιπλέον, όλοι οι υπολογιστές εκπέμπουν ηλεκτρομαγνητική ακτινοβολία που περιέχει πληροφορίες. Αυτές οι πληροφορίες, με τον κατάλληλο εξοπλισμό, μπορούν να συλλεχθούν και να καταγραφούν.
- Ευπάθειες επικοινωνίας: Κάθε υπολογιστής που είναι συνδεδεμένος σε δίκτυο διατρέχει τον κίνδυνο διείσδυσης από απομακρυσμένη τοποθεσία.
- Ανθρώπινα θέματα ευπάθειας: Οι εργαζόμενοι είναι η κύρια αιτία πολλών προβλημάτων ασφαλείας και αυτό τους καθιστά μία από τις μεγαλύτερες ευπάθειες σε ένα σύστημα υπολογιστή.

1.4. Εξέλιξη των σύγχρονων περιβαλλόντων

Στις πρώτες μέρες της πληροφορικής, τα συστήματα υπολογιστών ήταν μεγάλα και εξαιρετικά ακριβά. Πολλές φορές, ολόκληρα συστήματα αφιερώθηκαν σε μεμονωμένους χρήστες ή το πολύ σε επιλεγμένους λίγους, οι οποίοι απλά έπρεπε να καθαρίσουν τη μνήμη του υπολογιστή, να σηκώσουν τις κασέτες του υπολογιστή τους, τις κάρτες διάτρησης και να κλειδώσουν το γραφείο στο τέλος της εργάσιμης ημέρας για να προστατεύσουν και τα δύο – συστήματα και πληροφορίες από εισβολείς. (Myers, 1980) Ο χρήστης είχε τον πλήρη έλεγχο του

περιβάλλοντος λειτουργίας. Η ασφάλεια των υπολογιστών ήταν απλώς μέρος του φυσικού σχεδίου ασφάλειας του οργανισμού. Οι κύριες ανησυχίες για την ασφάλεια του οργανισμού επικεντρώνονται σε φυσικές διακοπές, κλοπή του πραγματικού εξοπλισμού υπολογιστών και κλοπή δίσκων υπολογιστή, κυλίνδρων ταινιών ή καρτών διάτρησης.

Πριν από τη δεκαετία του 1980, ο φόβος για μια απειλή εσωτερικού ήταν η μικρότερη ανησυχία για τους περισσότερους οργανισμούς. Πολύ λίγοι άνθρωποι ήταν έμπειροι χρήστες υπολογιστών και οι επιλεγμένοι λίγοι που πραγματικά δούλευαν στους υπολογιστές το έκαναν σε ασφαλείς τοποθεσίες. Οι περισσότεροι χρήστες δεν είδαν ποτέ τα συστήματα υπολογιστών που εκτελούσαν τις καθημερινές τους εργασίες. Οι χρήστες υπέβαλαν διαλεγμένες εργασίες επεξεργασίας παρτίδων και ανέκτησαν τα αποτελέσματα.

Καθώς άλλαξαν οι καιροί, η τεχνολογία των υπολογιστών εξελίχθηκε επίσης. Στα τέλη της δεκαετίας του 1960, οι χρήστες άρχισαν να αλληλεπιδρούν με τους υπολογιστές πιο συχνά και άρχισαν να απαιτούν καλύτερη χρήση πόρων υπολογιστών. Το υπολογιστικό περιβάλλον άρχισε να μετατοπίζεται από τον κεντρικό έλεγχο σε αποκεντρωμένη πληροφορική. Αυτή η αλλαγή στα υπολογιστικά παραδείγματα παρείχε στους χρήστες μεγαλύτερο έλεγχο των υπολογιστικών τους πόρων, ανοίγοντας παράλληλα την πόρτα για νέες πιθανότητες κακής χρήσης υπολογιστών.

Η ικανότητα πρόσβασης σε υπολογιστές από απομακρυσμένες τοποθεσίες έφερε επανάσταση στην εποχή του υπολογιστή. Με την αύξηση των τηλεπικοινωνιών, τα «δίκτυα» υπολογιστών αυξήθηκαν σε μέγεθος και πολυπλοκότητα. Πολλές μεγάλες επιχειρήσεις άρχισαν να αυτοματοποιούν και να αποθηκεύουν πληροφορίες σχετικά με τους πελάτες, τους πωλητές και τις εμπορικές συναλλαγές τους.

Η πρόσβαση στον υπολογιστή μέσω δικτύου είχε δραματικό αντίκτυπο στην εκπαίδευση. Τα κολέγια και τα πανεπιστήμια σε ολόκληρη τη χώρα βρήκαν πλέον δυνατό να συνδεθούν με μεγάλα δίκτυα υπολογιστών και κεντρικές βάσεις δεδομένων υπολογιστών. Το πρώτο μεγάλο δίκτυο για εκπαίδευση και κυβερνητική χρήση ήταν το Arpanet, το οποίο αργότερα εξελίχθηκε στο Διαδίκτυο. Αυτή η έκρηξη στη διαθεσιμότητα υπολογιστών παρείχε στους μαθητές την ευκαιρία να πειραματιστούν και να εργαστούν με υπολογιστές για πρώτη φορά. Αυτό δημιούργησε ένα φαινόμενο «χιονοστιβάδας» που οδηγεί σε τεράστια αύξηση του συνολικού αριθμού ατόμων που χρησιμοποιούν υπολογιστές. Το μυστήριο ενός ανοιχτού υπολογιστικού

περιβάλλοντος άρχισε να ξεθωριάζει αργά, καθώς οι απειλές και οι επιθέσεις έγιναν, συνηθισμένες.

Η εισαγωγή του προσωπικού υπολογιστή κατά τη διάρκεια της δεκαετίας του 1980 παρείχε πρόσβαση σε ακόμη μεγαλύτερο αριθμό ατόμων. Ο προσωπικός υπολογιστής άρχισε να εμφανίζεται σε γραφεία τόσο στο χώρο εργασίας όσο και στο σπίτι. Καθώς η τιμή των υπολογιστών άρχισε να μειώνεται σταθερά, πολλές μικρές επιχειρήσεις το είδαν ως ευκαιρία να αυτοματοποιήσουν τις δραστηριότητές τους για να παραμείνουν ανταγωνιστικές με μεγαλύτερες εταιρείες. Η έλευση και η διαθεσιμότητα του προσωπικού υπολογιστή παρουσίασαν μια άλλη πρόκληση για την ασφάλεια του υπολογιστή. Οι άνθρωποι μπορούν τώρα να δημιουργήσουν προγράμματα στο σπίτι για να κλέψουν πληροφορίες ή να διακόψουν τις λειτουργίες. Επιπλέον, τα δεδομένα που έπρεπε να μεταφερθούν μεταξύ των συστημάτων αποθηκεύτηκαν σε δισκέτες και θα μπορούσαν τώρα να μεταφορτωθούν και να κλαπούν εύκολα.

Στα τέλη της δεκαετίας του 1980 και στις αρχές της δεκαετίας του 1990, η χρήση του προσωπικού υπολογιστή, αυξήθηκε με εκθετικό ρυθμό. Καθώς αυτή η χρήση αυξήθηκε, το ίδιο έκανε και η χρήση δικτύων, ηλεκτρονικού ταχυδρομείου και πινάκων ανακοινώσεων. Αυτές οι νέες εξελίξεις στον υπολογιστή αύξησαν την ικανότητα των χρηστών να επικοινωνούν μεταξύ τους και με άλλα συστήματα υπολογιστών. Αυτή η νέα ελευθερία στον υπολογισμό ανοίγει μια εντελώς νέα «παιδική χαρά» για τους χάκερ. Πριν από την ευρεία χρήση των δικτύων, ένας χάκερ μπορεί να είναι σε θέση να διεισδύσει σε ένα σύστημα τη φορά μέσω μόντεμ. Τώρα ένας υποψήφιος χάκερ έχει τη δυνατότητα να έχει πρόσβαση σε πολλά συστήματα με ένα μόνο διάλειμμα και έχει τη δυνατότητα να διαταράξει τα συστήματα υπολογιστών σε όλο τον κόσμο.

Η δεκαετία του 1990 είδε την εμφάνιση ανοικτών συστημάτων καθώς και την αυξανόμενη εξάρτηση από δίκτυα και την ανάγκη κοινής χρήσης δεδομένων, εφαρμογών και πόρων υλικού. Στο παρελθόν, η ασφάλεια δεν θεωρήθηκε σημαντική ανησυχία, αλλά με την έλευση του Διαδικτύου, η ικανότητα "προσέγγισης και επαφής" ενός δικτύου έχει γίνει παγκόσμια.

1.5. Προσπάθειες ασφαλείας

Οι πρώτες δραστηριότητες ασφάλειας που σχετίζονται με τον υπολογιστή ξεκίνησαν τη δεκαετία του 1950. Η κυβέρνηση των Ηνωμένων Πολιτειών, κατανοώντας τους πιθανούς κινδύνους ασφαλείας που σχετίζονται με υπολογιστές · έλαβε μερικά αρχικά μέτρα για την προστασία των κυβερνητικών υπολογιστικών πόρων. Το πρώτο πρότυπο ασφαλείας TEMPEST (TransientElectromagneticPulseEmanationStandard) σχεδιάστηκε για να εκμεταλλευτεί το γεγονός ότι όλος ο ηλεκτρονικός εξοπλισμός εκπέμπει σήματα που μπορούν να ληφθούν εκτός του συστήματος. Επιπλέον, ο πρώτος κυβερνητικός οργανισμός ασφαλείας, το Συμβούλιο Ασφαλείας Επικοινωνιών των Ηνωμένων Πολιτειών (COMSEC), ιδρύθηκε για να επιβλέπει την προστασία διαβαθμισμένων πληροφοριών και αποτελείται από εκπροσώπους πολλών διαφορετικών κλάδων της κυβέρνησης.

Αυτή η μέτρια προσπάθεια για την ασφάλεια του υπολογιστή αποτέλεσε το θεμέλιο πάνω στο οποίο σημειώθηκαν πρόοδοι στην ασφάλεια του υπολογιστή. Το Υπουργείο Άμυνας, ο Οργανισμός Εθνικής Ασφάλειας και το Εθνικό Γραφείο Προτύπων ξεκίνησαν όλες τις πρωτοβουλίες ασφαλείας. Αυτές οι πρωτοβουλίες σε συνδυασμό με την πρώτη ευαισθητοποίηση του κοινού για την ασφάλεια προέκυψαν προς τα τέλη της δεκαετίας του 1960.

Α) Δημόσια Ευαισθητοποίηση

Η πρώτη μεγάλη ευαισθητοποίηση του κοινού για την ασφάλεια των υπολογιστών ήρθε από την Ανοιξιάτικη Κοινή Διάσκεψη Υπολογιστών του 1967. Αυτό το συνέδριο αναγνωρίζεται γενικά ως η πρώτη ολοκληρωμένη παρουσίαση ασφάλειας υπολογιστών σε τεχνικό κοινό. Την παρουσίαση προήδρευσε ο WillisH. Ware της RANDCorporation και ασχολήθηκε με τα περίπλοκα ζητήματα που αφορούν την ευπάθεια της κοινής χρήσης πόρων και των συστημάτων υπολογιστών απομακρυσμένης πρόσβασης. Τα θέματα περιλάμβαναν ηλεκτρομαγνητική ακτινοβολία, καλωδιώσεις σε γραμμές επικοινωνίας, μη εξουσιοδοτημένους προγραμματιστές και πρόσβαση χρηστών σε συστήματα και δεδομένα.

Β) Πρωτοβουλίες Υπουργείου Άμυνας

Το Υπουργείο Άμυνας ήταν ένας από τους πρώτους οργανισμούς που χρησιμοποίησαν υπολογιστικά συστήματα και είχε έντονο ενδιαφέρον για την προστασία των διαβαθμισμένων πληροφοριών που είναι αποθηκευμένα σε αυτά τα συστήματα. Τον Οκτώβριο του 1967, το

Υπουργείο Άμυνας ίδρυσε μια ειδική ομάδα στο πλαίσιο του AdvancedResearchProjectsAgency (ARPA). Ο στόχος της ειδικής ομάδας ήταν να μελετήσει διάφορα συστήματα και δίκτυα υπολογιστών, να εντοπίσει τρωτά σημεία και απειλές και να κάνει συστάσεις για την προστασία και τον έλεγχο της πρόσβασης σε υπολογιστές, συστήματα, δίκτυα και πληροφορίες του Υπουργείου Άμυνας. Μετά από πάνω από δύο χρόνια εξέτασης του προβλήματος, η ομάδα εργασίας δημοσίευσε το διαβαθμισμένο έγγραφο που ονομάζεται Έλεγχος Ηλεκτρονικών Υπολογιστών για Συστήματα Υπολογιστών το 1970. Αυτό το έγγραφο ήταν το πρώτο του είδους αυτού και αποτέλεσε τη βάση για πολλά προγράμματα ασφαλείας που ακολούθησαν, αφιερωμένα στην προστασία διαβαθμισμένη πληροφορία.

Το Υπουργείο Άμυνας άρχισε να αναπτύσσει κανονισμούς για την επιβολή της ασφάλειας των συστημάτων υπολογιστών, των δικτύων και των διαβαθμισμένων δεδομένων που χρησιμοποιούνται από το Υπουργείο Άμυνας και τους κυβερνητικούς εργολάβους, και το 1972 εξέδωσε την οδηγία DoD 5200.28, «Απαιτήσεις ασφαλείας για συστήματα αυτοματοποιημένης επεξεργασίας δεδομένων (ADP)». Αυτή η οδηγία καθιέρωσε μια συνεπή πολιτική DoD για τον έλεγχο του συστήματος υπολογιστών και ανέφερε τα ακόλουθα ως τη γενική πολιτική της:

«Το διαβαθμισμένο υλικό που περιέχεται σε ένα σύστημα ADP προστατεύεται από τη συνεχή χρήση προστατευτικών χαρακτηριστικών στο σχεδιασμό και τη διαμόρφωση του υλικού και του λογισμικού του συστήματος.» (Russell&Gangemi, 1991)

Αυτή η οδηγία ήταν το πρώτο επίσημο έγγραφο που καθιερώνει μια πολιτική ασφάλειας υπολογιστών για έναν οργανισμό. Ήταν μοναδικό στο γεγονός ότι όριζε ότι τα συστήματα προστατεύουν ειδικά, όχι μόνο τον εξοπλισμό υπολογιστών, αλλά και τα δεδομένα που περιέχονται στα συστήματα από τη σκόπιμη και ακούσια πρόσβαση σε διαβαθμισμένο υλικό από μη εξουσιοδοτημένα άτομα.

Καθ'όλη τη δεκαετία του 1970, αναπτύχθηκαν πολλές πρωτοβουλίες ασφάλειας υπολογιστών για την καλύτερη κατανόηση των τρωτών σημείων των υπολογιστικών συστημάτων και για την εξεύρεση τρόπου για την καταπολέμηση των απειλών. Οι πρωτοβουλίες χωρίστηκαν σε τρεις γενικές κατηγορίες: «ομάδες τίγρης», ερευνητικές μελέτες ασφάλειας και ανάπτυξη του πρώτου ασφαλούς λειτουργικού συστήματος.

- *«Ομάδες Τίγρης»*

Η δεκαετία του '70 είδε την εμφάνιση κυβερνητικών και βιομηχανικών ομάδων τίγρης. Οι ομάδες τίγρης αποτελούνταν από μια ομάδα χάκερ που προσπάθησαν να εισέλθουν σε συστήματα υπολογιστών για να εντοπίσουν αδυναμίες στους μηχανισμούς ασφαλείας. Μόλις εντοπιστούν αδυναμίες, η ομάδα θα αναπτύξει «μπαλώματα» για να ασφαλίσει τις τρύπες. Ενώ οι ομάδες τίγρης παρέχουν έναν αποτελεσματικό τρόπο εντοπισμού τρωτών σημείων, οι προσπάθειες των ομάδων ήταν συχνά ασυντόνιστες και δεν μπορούσαν απαραίτητα να βρουν όλα τα προβλήματα ασφαλείας που υπήρχαν σε οποιοδήποτε σύστημα. Συχνά οι ομάδες τίγρης βρήκαν ελαττώματα ασφαλείας που είχαν χαθεί από προηγούμενες ομάδες τίγρης. Επομένως, δεν θα μπορούσε κανείς να εγγυηθεί ένα ασφαλές σύστημα μόνο και μόνο επειδή μια ομάδα τίγρης δεν μπορούσε να διεισδύσει στο σύστημα. Η ιδέα της ομάδας τίγρης ήταν η πρώτη οργανωμένη προσπάθεια παροχής λύσης στο συνεχώς αυξανόμενο πρόβλημα των επιθέσεων στον υπολογιστή. Παρόλο που οι ομάδες τίγρης δεν ήταν πάντα αποτελεσματικές, έχουν δείξει πόσο εύκολα μπορούν να αξιοποιηθούν τα ελαττώματα ασφαλείας στα συστήματα. Έχουν επίσης πιέσει την ανάγκη για μια πιο αποτελεσματική και τυποποιημένη μέθοδο δοκιμής και αξιολόγησης τόσο της πολιτικής ασφάλειας όσο και της εφαρμογής της.

- *Μοντελοποίηση*

Ενώ οι ομάδες τίγρης ήταν απασχολημένες με τον εντοπισμό ελαττωμάτων ασφαλείας, διάφορες κυβερνητικές υπηρεσίες άρχισαν να χρηματοδοτούν πρωτοποριακά ερευνητικά προγράμματα. Αυτά τα έργα σχεδιάστηκαν για να αναλύσουν τις απαιτήσεις ασφάλειας, να κατασκευάσουν μοντέλα πολιτικής ασφαλείας και να παρέχουν συστάσεις σε κυβερνητικούς αξιωματούχους. Αρκετές σημαντικές απόψεις για την ασφάλεια των υπολογιστών προέκυψαν από αυτά τα ερευνητικά έργα. Το πρώτο από τα οποία ήταν η έννοια ενός μόνιτορ αναφοράς. Ο JamesP. Anderson ανέφερε για πρώτη φορά την οθόνη αναφοράς στη Μελέτη Προγραμματισμού Τεχνολογίας Ασφάλειας Υπολογιστών που γράφτηκε το 1972.

«Η οθόνη αναφοράς επιβάλλει την ασφάλεια, αναγκάζοντας όλα τα θέματα που επιθυμούν να έχουν πρόσβαση σε ένα αντικείμενο να το κάνουν μόνο μέσω της ίδιας της οθόνης.»(White, Fisch&Pooch, 1996)

Η έννοια της οθόνης αναφοράς καθίσταται εξαιρετικά σημαντική για την ανάπτυξη προτύπων και τεχνολογιών για ένα ασφαλές σύστημα. Η οθόνη αναφοράς λαμβάνει αποφάσεις ελέγχου πρόσβασης βάσει ενός συνόλου κανόνων, που περιγράφουν ποια θέματα μπορούν να

έχουν πρόσβαση σε ποια αντικείμενα. Οι κανόνες μπορούν να καθορίσουν ορισμένα αρχεία ή αντικείμενα και θα αντιπροσωπεύουν μια σύνοψη της πολιτικής ελέγχου πρόσβασης και του μοντέλου που έχει επιλεγεί για το σύστημα.

Επιπλέον, η πρώτη οργανωμένη προσπάθεια για τη δημιουργία ενός μοντέλου πολιτικής ασφάλειας ήταν από το Υπουργείο Άμυνας, το οποίο χρηματοδότησε πολλά έργα στα τέλη της δεκαετίας του 1970 με επίκεντρο την ανάπτυξη μαθηματικών μοντέλων ασφάλειας. Τα δύο πιο σημαντικά από τα μοντέλα είναι γνωστά ως το μοντέλο Bell-LaPadula και το μοντέλο Clark-Wilson.

Το μοντέλο Bell και LaPadula είχε μεγάλο ενδιαφέρον για το Υπουργείο Άμυνας, διότι επέβαλε τον στόχο του στρατού να εξαλείψει τη μη εξουσιοδοτημένη αποκάλυψη και να προβλέψει την αποχαρακτηρισμό ευαίσθητων πληροφοριών. Ενώ αυτό το μοντέλο ήταν εξαιρετικά χρήσιμο για στρατιωτικά συστήματα υπολογιστών, έθεσε πολλές προκλήσεις για εμπορικούς οργανισμούς των οποίων η επεξεργασία ευαίσθητων πληροφοριών διέφερε ουσιαστικά από αυτή των στρατιωτικών και των κοινοτήτων πληροφοριών.

Για να καλύψει τις ανάγκες της εμπορικής βιομηχανίας, ο DavidClark και ο DavidWilson ανέπτυξαν ένα μοντέλο ασφάλειας που επικεντρώθηκε στην ακεραιότητα των πληροφοριών παρά στην πραγματική του αποκάλυψη. Καθώς περισσότερες επιχειρήσεις άρχισαν να βασίζονται στην εμπορική επεξεργασία δεδομένων για να παρακολουθούν τα οικονομικά τους αρχεία, έγινε απαραίτητο να αποφευχθεί η μη εξουσιοδοτημένη τροποποίηση αυτών των δεδομένων. Χρησιμοποιεί δύο τύπους μηχανισμών για την επίτευξη αυτού του στόχου: καλά σχηματισμένες συναλλαγές και διαχωρισμός καθηκόντων.

Η καλά σχηματισμένη συναλλαγή είναι ένα ηλεκτρονικό αρχείο καταγραφής ελέγχου που διασφαλίζει ότι οι χρήστες δεν μπορούν να αλλάξουν τυχαία δεδομένα. Αυτό δίνει στον διαχειριστή του συστήματος τη δυνατότητα να αναδημιουργήσει τις ενέργειες ενός χρήστη σε περίπτωση παραβίασης της ασφάλειας του υπολογιστή και να επαναφέρει τα αρχικά δεδομένα, εάν χρειαστεί. Τα αρχεία καταγραφής ελέγχου δεν σταματούν φυσικά έναν υποψήφιο εισβολέα από την πρόσβαση και την αλλαγή δεδομένων, αλλά η γνώση που υπάρχει, ένα σύστημα μπορεί να την αποτρέψει.

Ο δεύτερος μηχανισμός που χρησιμοποιείται στο μοντέλο Clark-Wilson είναι ο διαχωρισμός των καθηκόντων. Ο στόχος του διαχωρισμού των καθηκόντων είναι να διατηρηθεί η ακεραιότητα των δεδομένων διαχωρίζοντας τις λειτουργίες που απαιτούνται για την τροποποίηση των δεδομένων σε διάφορα μέρη και απαιτώντας από διαφορετικούς χρήστες να εκτελούν κάθε μέροςξεχωριστά. Αυξάνοντας τον αριθμό των υπαλλήλων που απαιτούνται για την ολοκλήρωση της εργασίας, αυξάνει τη δυσκολία διάπραξης απάτης χωρίς να γίνει αντιληπτό.

Ο σκοπός αυτού του μοντέλου δεν είναι μόνο να εμποδίσει τους μη εξουσιοδοτημένους χρήστες από την τροποποίηση ευαίσθητων λογιστικών και οικονομικών δεδομένων, αλλά επίσης αντιμετωπίζει θέματα που σχετίζονται με εξουσιοδοτημένους χρήστες που έχουν πρόσβαση σε ευαίσθητες πληροφορίες. Ενώ η ασφάλεια των υπολογιστών, μέχρι αυτό το σημείο της ιστορίας, επικεντρώθηκε στην άρνηση πρόσβασης από εξωτερικές απειλές, αυτή ήταν η πρώτη σημαντική προσπάθεια για την καταπολέμηση της απειλής των εμπιστευτικών.

Με την πάροδο του χρόνου, άλλα μοντέλα αναπτύχθηκαν για την αντιμετώπιση πιο συγκεκριμένων προβλημάτων ασφάλειας. Για παράδειγμα, το μοντέλο Goguen-Meseguer αντιμετώπισε το ζήτημα της μη παρέμβασης μεταξύ των θεμάτων. Έχει σχεδιαστεί για να αποτρέπει τους χρήστες να παρεμβαίνουν μεταξύ τους.

- *<u>Η ανάπτυξη αξιόπιστων συστημάτων υπολογιστών</u>*

Ενώ πολλά έργα που χρηματοδοτήθηκαν από την κυβέρνηση επικεντρώθηκαν στην ανάπτυξη μοντέλων ασφαλείας στις αρχές του 970, άλλα άρχισαν να αναπτύσσουν τα πρώτα αξιόπιστα συστήματα. «Το κλειδί για την ανάπτυξη ενός αξιόπιστου συστήματος είναι ο πυρήνας ασφαλείας. Ο πυρήνας ασφαλείας είναι το μέρος του λειτουργικού συστήματος που ελέγχει την πρόσβαση σε όλους τους πόρους του υπολογιστή και είναι το κατώτατο επίπεδο σε ένα σχεδιασμό συστήματος πολλαπλών επιπέδων. Ο επίσημος ορισμός της ασφάλειας. Ο πυρήνας όπως ορίζεται στο "Πορτοκαλί βιβλίο" είναι: «Το υλικό, το υλικολογισμικό και τα στοιχεία λογισμικού μιας αξιόπιστης βάσης υπολογιστών που εφαρμόζουν την έννοια της οθόνης αναφοράς. Πρέπει να διαμεσολαβεί όλη την πρόσβαση, να προστατεύεται από τροποποίηση και να επαληθεύεται ως σωστή. (Russell&Gangemi, 1991)

Η πιο σημαντική ανάπτυξη του πυρήνα ασφαλείας ήρθε από ένα έργο που χρηματοδοτήθηκε από την Πολεμική Αεροπορία για το Σύστημα Multics (Multiplexed Information and ComputingSystem). Το Σύστημα Multics είναι σημαντικό στο γεγονός ότι επιτρέπει σε χρήστες με διαφορετικά περιθώρια ασφαλείας να έχουν ταυτόχρονα πρόσβαση σε πληροφορίες που έχουν ταξινομηθεί σε διαφορετικά επίπεδα και ήταν εξαιρετικά σημαντικές για την ανάπτυξη μελλοντικών αξιόπιστων συστημάτων. Διαθέτει ένα μεγάλης κλίμακας διαδραστικό σύστημα υπολογιστών που παρέχει εκτεταμένους κωδικούς πρόσβασης και στοιχεία ελέγχου σύνδεσης Πρόσθετα χαρακτηριστικά περιλαμβάνουν τα ακόλουθα: ασφάλεια δεδομένων μέσω λιστών ελέγχου πρόσβασης (ACLs), μηχανισμού απομόνωσης πρόσβασης (AIM), έλεγχος όλων των λειτουργιών πρόσβασης συστήματος, αποκεντρωμένη διαχείριση συστήματος, τμηματική εικονική μνήμη και αρχιτεκτονική διεργασιών.

Κεφάλαιο 2ο:Κακόβουλο λογισμικό

Κακόβουλο λογισμικό ή κακόβουλο λογισμικό, είναι αναμφισβήτητα μια από τις πιο σημαντικές κατηγορίες απειλών για τα συστήματα υπολογιστών. [SOUP13] ορίζει το κακόβουλο λογισμικό ως «ένα πρόγραμμα που εισάγεται σε ένα σύστημα, συνήθως κρυφά, με σκοπό να διακυβεύσει την εμπιστευτικότητα, την ακεραιότητα ή τη διαθεσιμότητα των δεδομένων, των εφαρμογών ή του λειτουργικού συστήματος του θύματος ή να ενοχλήσει ή να διαταράξει με άλλο τρόπο το θύμα». Ως εκ τούτου, ανησυχούμε για την απειλή που θέτει το κακόβουλο λογισμικό σε προγράμματα εφαρμογών, σε προγράμματα κοινής ωφέλειας, όπως προγράμματα επεξεργασίας και μεταγλωττιστές και σε προγράμματα σε επίπεδο πυρήνα. Ανησυχούμε επίσης για τη χρήση του σε παραβιασμένους ή κακόβουλους ιστότοπους και διακομιστές, ή σε ειδικά κατασκευασμένα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου ή άλλα μηνύματα, που στοχεύουν να εξαπατήσουν τους χρήστες να αποκαλύψουν ευαίσθητα προσωπικά στοιχεία.

Αυτό το κεφάλαιο εξετάζει το ευρύ φάσμα των απειλών και των αντιμέτρων κακόβουλου λογισμικού. Ξεκινά με μια έρευνα για διάφορους τύπους κακόβουλου λογισμικού και προσφέρει μια ευρεία ταξινόμηση που βασίζεται πρώτα στα μέσα που χρησιμοποιεί το κακόβουλο λογισμικό για να διαδώσει ή να διαδώσει, και στη συνέχεια στην ποικιλία των ενεργειών ή των ωφέλιμων φορτίων που χρησιμοποιούνται όταν το κακόβουλο λογισμικό έχει φτάσει σε έναν στόχο. Οι μηχανισμοί διάδοσης περιλαμβάνουν αυτούς που χρησιμοποιούνται από ιούς, σκουλήκια και δούρειους ίππους. Τα ωφέλιμα φορτία περιλαμβάνουν καταστροφή του

συστήματος, bots, phishing, spyware και rootkits. Η συζήτηση ολοκληρώνεται με μια ανασκόπηση των προσεγγίσεων αντιμέτρων.

2.1. Τύποι κακόβουλου λογισμικού (Malware)

Α) Μια Ευρεία Ταξινόμηση Κακόβουλου Λογισμικού

Ορισμένοι συγγραφείς προσπαθούν να ταξινομήσουν κακόβουλο λογισμικό, όπως φαίνεται στην έρευνα και την πρόταση του [HANS04]. Αν και μπορεί να χρησιμοποιηθεί μια σειρά από πτυχές, μια χρήσιμη προσέγγιση ταξινομεί το κακόβουλο λογισμικό σε δύο ευρείες κατηγορίες, με βάση πρώτα τον τρόπο με τον οποίο διαδίδεται ή διαδίδεται για να επιτύχει τους επιθυμητούς στόχους. και έπειτα στις ενέργειες ή τα ωφέλιμα φορτία εκτελεί μόλις επιτευχθεί ένας στόχος.

Name	Description
Advanced Persistent Threat (APT)	Cybercrime directed at business and political targets, using a wide variety of intrusion technologies and malware, applied persistently and effectively to specific targets over an extended period, often attributed to state-sponsored organizations.
Adware	Advertising that is integrated into software. It can result in pop-up ads or redirection of a browser to a commercial site.
Attack kit	Set of tools for generating new malware automatically using a variety of supplied propagation and payload mechanisms.
Auto-rooter	Malicious hacker tools used to break into new machines remotely.
Backdoor (trapdoor)	Any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality in a program, or onto a compromised system.
Downloaders	Code that installs other items on a machine that is under attack. It is normally included in the malware code first inserted on to a compromised system to then import a larger malware package.
Drive-by-download	An attack using code in a compromised Web site that exploits a browser vulnerability to attack a client system when the site is viewed.
Exploits	Code specific to a single vulnerability or set of vulnerabilities.
Flooders (DoS client)	Used to generate a large volume of data to attack networked computer systems, by carrying out some form of denial-of-service (DoS) attack.
Keyloggers	Captures keystrokes on a compromised system.
Logic bomb	Code inserted into malware by an intruder. A logic bomb lies dormant until a predefined condition is met; the code then triggers an unauthorized act.
Macro virus	A type of virus that uses macro or scripting code, typically embedded in a document, and triggered when the document is viewed or edited, to run and replicate itself into other such documents.
Mobile code	Software (e.g., script, macro, etc) that can be shipped unchanged to a heterogeneous collection of platforms and execute with identical semantics.
Rootkit	Set of hacker tools used after attacker has broken into a computer system and gained root-level access.
Spammer programs	Used to send large volumes of unwanted e-mail.
Spyware	Software that collects information from a computer and transmits it to another system by monitoring keystrokes, screen data, and/or network traffic; or by scanning files on the system for sensitive information.
Trojan horse	A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes it.
Virus	Malware that, when executed, tries to replicate itself into other executable machine or script code; when it succeeds, the code is said to be infected. When the infected code is executed, the virus also executes.
Worm	A computer program that can run independently and can propagate a complete working version of itself onto other hosts on a network, usually by exploiting software vulnerabilities in the target system.
Zombie, bot	Program activated on an infected machine that is activated to launch attacks on other machines.

Πίνακας 2.1.1: Ορολογία για κακόβουλο λογισμικό.

Οι μηχανισμοί διάδοσης περιλαμβάνουν μόλυνση υπάρχοντος εκτελέσιμου ή ερμηνευμένου περιεχομένου από ιούς που στη συνέχεια διαδίδεται σε άλλα συστήματα. αξιοποίηση ευπαθειών λογισμικού είτε τοπικά είτε μέσω δικτύου μέσω worm ή λήψεων μέσω Drive για να επιτρέπεται η αναπαραγωγή του κακόβουλου λογισμικού. και επιθέσεις κοινωνικής μηχανικής που πείθουν τους χρήστες να παρακάμψουν μηχανισμούς ασφαλείας για να εγκαταστήσουν Trojans ή να ανταποκριθούν σε επιθέσεις phishing.

Προηγούμενες προσεγγίσεις για την ταξινόμηση κακόβουλων προγραμμάτων διακρίνονταν μεταξύ εκείνων που χρειάζονται ένα πρόγραμμα φιλοξενίας, όπως ο παρασιτικός κώδικας όπως οι ιοί, και εκείνοι που είναι ανεξάρτητα, αυτοτελή προγράμματα που εκτελούνται στο σύστημα όπως worms, Trojans και bots. Μια άλλη διάκριση που χρησιμοποιήθηκε ήταν μεταξύ κακόβουλου λογισμικού που δεν αναπαράγεται, όπως Trojans και spame-mail και malware που κάνει, συμπεριλαμβανομένων ιών και worm.

Οι ενέργειες ωφέλιμου φορτίου που πραγματοποιούνται από κακόβουλο λογισμικό όταν φτάσουν σε ένα σύστημα στόχου μπορεί να περιλαμβάνουν καταστροφή αρχείων συστήματος ή δεδομένων. κλοπή υπηρεσίας προκειμένου να γίνει το σύστημα πράκτορας επίθεσης ζόμπι ως μέρος ενός botnet. κλοπή πληροφοριών από το σύστημα, ειδικά για συνδέσεις, κωδικούς πρόσβασης ή άλλα προσωπικά στοιχεία μέσω προγραμμάτων πληκτρολόγησης ή spyware. και κρυφά όπου το κακόβουλο λογισμικό κρύβει την παρουσία του στο σύστημα από προσπάθειες εντοπισμού και αποκλεισμού του.

Ενώ το πρώιμο κακόβουλο λογισμικό έτεινε να χρησιμοποιεί ένα μόνο μέσο διάδοσης για να παραδώσει ένα μόνο ωφέλιμο φορτίο, καθώς εξελίχθηκε, βλέπουμε μια ανάπτυξη συνδυασμένου κακόβουλου λογισμικού που ενσωματώνει μια σειρά τόσο μηχανισμών διάδοσης όσο και ωφέλιμων φορτίων που αυξάνουν την ικανότητά του να διαδίδει, να κρύβει και να εκτελεί εύρος δράσεων σε στόχους. Μια συνδυασμένη επίθεση χρησιμοποιεί πολλές μεθόδους μόλυνσης ή διάδοσης, για να μεγιστοποιήσει την ταχύτητα μετάδοσης και τη σοβαρότητα της επίθεσης. Ορισμένα κακόβουλα προγράμματα υποστηρίζουν ακόμη και έναν μηχανισμό ενημέρωσης που του επιτρέπει να αλλάζει το εύρος των μηχανισμών διάδοσης και ωφέλιμου φορτίου που χρησιμοποιούνται μόλις αναπτυχθεί.

Στις ακόλουθες ενότητες, εξετάζουμε αυτές τις διάφορες κατηγορίες κακόβουλου λογισμικού και μετά ακολουθούμε με μια συζήτηση σχετικά με τα κατάλληλα αντίμετρα.

Β) Σετ επίθεσης (AttackKits)

Αρχικά, η ανάπτυξη και ανάπτυξη κακόβουλου λογισμικού απαιτούσε σημαντική τεχνική ικανότητα από τους δημιουργούς λογισμικού. Αυτό άλλαξε με την ανάπτυξη εργαλείων δημιουργίας ιών στις αρχές της δεκαετίας του 1990 και στη συνέχεια αργότερα γενικότερων κιτ επίθεσης στη δεκαετία του 2000, που βοήθησαν σημαντικά στην ανάπτυξη και την ανάπτυξη κακόβουλου λογισμικού [FOSS10]. Αυτά τα πακέτα εργαλείων, συχνά γνωστά ως crimeware, περιλαμβάνουν τώρα μια ποικιλία μηχανισμών διάδοσης και ενοτήτων ωφέλιμου φορτίου που ακόμη και οι αρχάριοι μπορούν να συνδυάσουν, να επιλέξουν και να αναπτύξουν. Μπορούν επίσης εύκολα να προσαρμοστούν με τις πιο πρόσφατες ευπάθειες που ανακαλύφθηκαν, προκειμένου να εκμεταλλευτούν το παράθυρο ευκαιριών μεταξύ της δημοσίευσης μιας αδυναμίας και της εκτεταμένης ανάπτυξης ενημερωμένων εκδόσεων για να το κλείσουν. Αυτά τα κιτ διεύρυναν πολύ τον πληθυσμό των εισβολέων που ήταν σε θέση να αναπτύξουν κακόβουλο λογισμικό. Αν και το κακόβουλο λογισμικό που δημιουργήθηκε με τέτοιες εργαλειοθήκες τείνει να είναι λιγότερο εξελιγμένο από αυτό που έχει σχεδιαστεί από το μηδέν, ο τεράστιος αριθμός νέων παραλλαγών που μπορούν να δημιουργηθούν από εισβολείς που χρησιμοποιούν αυτές τις εργαλειοθήκες δημιουργεί ένα σημαντικό πρόβλημα για αυτά τα αμυντικά συστήματα εναντίον τους.

Η εργαλειοθήκη Zeuscrimeware είναι ένα εξέχον, πρόσφατο παράδειγμα ενός τέτοιου κιτ επίθεσης, το οποίο χρησιμοποιήθηκε για τη δημιουργία ενός ευρέος φάσματος πολύ αποτελεσματικών, κρυμμένων, κακόβουλων προγραμμάτων που διευκολύνουν μια σειρά εγκληματικών δραστηριοτήτων, ιδίως τη σύλληψη και την εκμετάλλευση τραπεζικών διαπιστευτηρίων [BINS10] . Άλλες ευρέως χρησιμοποιούμενες εργαλειοθήκες περιλαμβάνουν Blackhole, Sakura και Phoenix [SYMA13].

Γ) Πηγές επίθεσης

Μια άλλη σημαντική ανάπτυξη κακόβουλου λογισμικού τις τελευταίες δύο δεκαετίες είναι η αλλαγή από τους επιτιθέμενους να είναι άτομα, που συχνά παρακινούνται να αποδείξουν την τεχνική τους ικανότητα στους συνομηλίκους τους, σε πιο οργανωμένες και επικίνδυνες πηγές επίθεσης. Αυτά περιλαμβάνουν πολιτικά κίνητρα επιτιθέμενους, εγκληματίες και οργανωμένο έγκλημα. οργανισμούς που πωλούν τις υπηρεσίες τους σε εταιρείες και έθνη, καθώς και σε εθνικές κυβερνητικές υπηρεσίες. Αυτό άλλαξε σημαντικά τους διαθέσιμους πόρους και τα

κίνητρα πίσω από την εμφάνιση κακόβουλου λογισμικού, και όντως οδήγησε στην ανάπτυξη μιας μεγάλης υπόγειας οικονομίας που περιλαμβάνει την πώληση κιτ επίθεσης, την πρόσβαση σε παραβιασμένους κεντρικούς υπολογιστές και σε κλεμμένες πληροφορίες.

2.2. ΠροχωρημένηΕπίμονηΑπειλή (Advanced Persistent Threat)

Οι προηγμένες μόνιμες απειλές (APTs) έχουν αναδειχθεί τα τελευταία χρόνια. Αυτά δεν είναι ένας νέος τύπος κακόβουλου λογισμικού, αλλά μάλλον η συνεχής εφαρμογή μιας μεγάλης ποικιλίας τεχνολογιών εισβολής και κακόβουλου λογισμικού σε επιλεγμένους στόχους, συνήθως επιχειρηματικούς ή πολιτικούς. Τα APT συνήθως αποδίδονται σε κρατικούς οργανισμούς, με πιθανές επιθέσεις και από εγκληματικές επιχειρήσεις.

Οι APT διαφέρουν από άλλους τύπους επίθεσης λόγω της προσεκτικής επιλογής στόχων τους και των επίμονων, συχνά κρυφών, προσπαθειών εισβολής σε παρατεταμένες περιόδους. Μια σειρά από επιθέσεις υψηλού προφίλ, συμπεριλαμβανομένων των Aurora, RSA, APT1 και Stuxnet, αναφέρονται συχνά ως παραδείγματα. Ονομάζονται ως αποτέλεσμα αυτών των χαρακτηριστικών:

- Για προχωρημένους: Χρήση από τους εισβολείς μιας μεγάλης ποικιλίας τεχνολογιών εισβολής και κακόβουλου λογισμικού, συμπεριλαμβανομένης της ανάπτυξης προσαρμοσμένου κακόβουλου λογισμικού, εάν απαιτείται. Τα επιμέρους στοιχεία μπορεί να μην είναι απαραίτητα τεχνικά προηγμένα, αλλά επιλέγονται προσεκτικά για να ταιριάζουν στον επιλεγμένο στόχο.
- Μόνιμο: Προσδιορισμένη εφαρμογή των επιθέσεων σε μεγάλο χρονικό διάστημα έναντι του επιλεγμένου στόχου, προκειμένου να μεγιστοποιηθεί η πιθανότητα επιτυχίας. Μια ποικιλία επιθέσεων μπορεί να εφαρμοστεί σταδιακά, και συχνά κρυφά, έως ότου τεθεί σε κίνδυνο ο στόχος.
- Απειλές: Απειλές στους επιλεγμένους στόχους ως αποτέλεσμα των οργανωμένων, ικανών και καλά χρηματοδοτούμενων επιτιθέμενων που προτίθενται να θέσουν σε κίνδυνο τους συγκεκριμένους επιλεγμένους στόχους. Η ενεργός συμμετοχή των ανθρώπων στη διαδικασία αυξάνει σε μεγάλο βαθμό το επίπεδο απειλής από αυτό λόγω των εργαλείων αυτοματοποιημένων επιθέσεων και επίσης της πιθανότητας επιτυχούς επίθεσης.

Ο στόχος αυτών των επιθέσεων ποικίλλει από την κλοπή δεδομένων πνευματικής ιδιοκτησίας ή ασφάλειας και δεδομένων που σχετίζονται με την υποδομή έως τη φυσική διαταραχή της υποδομής. Οι τεχνικές που χρησιμοποιήθηκαν περιλαμβάνουν την κοινωνική μηχανική, τα ηλεκτρονικά μηνύματα ηλεκτρονικού ψαρέματος (phear-phishing) και τις μεταφορτώσεις από επιλεγμένους ιστότοπους που έχουν παραβιαστεί και είναι πιθανό να επισκεφθούν το προσωπικό του οργανισμού-στόχου. Ο σκοπός είναι να μολυνθεί ο στόχος με εξελιγμένο κακόβουλο λογισμικό με πολλαπλούς μηχανισμούς διάδοσης και ωφέλιμα φορτία. Μόλις αποκτήσουν αρχική πρόσβαση σε συστήματα στον οργανισμό-στόχο, χρησιμοποιείται ένα περαιτέρω εύρος εργαλείων επίθεσης για τη διατήρηση και την επέκταση της πρόσβασής τους.

Ως αποτέλεσμα, αυτές οι επιθέσεις είναι πολύ πιο δύσκολο να αμυνθούν λόγω αυτής της συγκεκριμένης στόχευσης και επιμονής. Απαιτεί έναν συνδυασμό τεχνικών αντιμέτρων, όπως θα συζητήσουμε αργότερα σε αυτό το κεφάλαιο, καθώς και εκπαίδευση ευαισθητοποίησης για να βοηθήσουμε το προσωπικό να αντισταθεί σε τέτοιες επιθέσεις, όπως συζητάμε στο Κεφάλαιο 17. Ακόμη και με τα τρέχοντα αντίμετρα βέλτιστης πρακτικής, η χρήση εκμεταλλεύσεων μηδενικής ημέρας και οι νέες προσεγγίσεις επίθεσης σημαίνει ότι μερικές από αυτές τις επιθέσεις είναι πιθανό να πετύχουν [SYMA13, MAND13]. Επομένως απαιτούνται πολλαπλά επίπεδα άμυνας, με μηχανισμούς για τον εντοπισμό, την απόκριση και τον μετριασμό τέτοιων επιθέσεων. Αυτά μπορεί να περιλαμβάνουν παρακολούθηση για την εντολή κακόβουλου λογισμικού και τον έλεγχο της κυκλοφορίας και τον εντοπισμό της κυκλοφορίας εξάλειψης.

2.3. Διάδοση – ΜολυσμένοΠεριεχόμενο – Ιοί (Propagation – Infected Content – Viruses)

Η πρώτη κατηγορία διάδοσης κακόβουλου λογισμικού αφορά παρασιτικά τμήματα λογισμικού που συνδέονται με κάποιο υπάρχον εκτελέσιμο περιεχόμενο. Το θραύσμα μπορεί να είναι κωδικός μηχανής που μολύνει κάποια υπάρχουσα εφαρμογή, βοηθητικό πρόγραμμα ή πρόγραμμα συστήματος ή ακόμη και τον κωδικό που χρησιμοποιείται για την εκκίνηση ενός συστήματος υπολογιστή. Πιο πρόσφατα, το τμήμα ήταν μια μορφή κώδικα δέσμης ενεργειών,

που χρησιμοποιείται συνήθως για την υποστήριξη ενεργού περιεχομένου σε αρχεία δεδομένων όπως έγγραφα MicrosoftWord, υπολογιστικά φύλλα Excel ή έγγραφα AdobePDF.

Α) Η φύση των ιών

Ο ιός του υπολογιστή είναι ένα λογισμικό που μπορεί να «μολύνει» άλλα προγράμματα, ή όντως οποιοδήποτε είδος εκτελέσιμου περιεχομένου, τροποποιώντας τα. Η τροποποίηση περιλαμβάνει την έγχυση του αρχικού κώδικα με μια ρουτίνα για τη δημιουργία αντιγράφων του κώδικα ιού, ο οποίος στη συνέχεια μπορεί να συνεχίσει να μολύνει άλλο περιεχόμενο. Οι ιοί υπολογιστών εμφανίστηκαν για πρώτη φορά στις αρχές της δεκαετίας του 1980 και ο ίδιος ο όρος αποδίδεται στον FredCohen. Ο Cohen είναι ο συγγραφέας ενός πρωτοποριακού βιβλίου για το θέμα [COHE94]. Ο ιός του εγκεφάλου, που πρωτοεμφανίστηκε το 1986, ήταν ένας από τους πρώτους που στοχεύουν συστήματα MSDOS και είχε ως αποτέλεσμα σημαντικό αριθμό λοιμώξεων για αυτή τη φορά.

Οι βιολογικοί ιοί είναι μικροσκοπικά θραύσματα γενετικού κώδικα - DNA ή RNA - που μπορούν να αναλάβουν τον μηχανισμό ενός ζωντανού κυττάρου και να τον ξεγελάσουν για να δημιουργήσουν χιλιάδες άψογες αντιγραφές του αρχικού ιού. Όπως και το βιολογικό αντίστοιχό του, ένας ιός υπολογιστών φέρει στον εκπαιδευτικό του κώδικα τη συνταγή για τη δημιουργία τέλειων αντιγράφων του. Ο τυπικός ιός ενσωματώνεται σε ένα πρόγραμμα ή φορέα εκτελέσιμου περιεχομένου, σε έναν υπολογιστή. Στη συνέχεια, κάθε φορά που ο μολυσμένος υπολογιστής έρχεται σε επαφή με ένα μη μολυσμένο κομμάτι κώδικα, ένα νέο αντίγραφο του ιού περνά στη νέα θέση. Έτσι, η μόλυνση μπορεί να εξαπλωθεί από υπολογιστή σε υπολογιστή, με τη βοήθεια μη ανυποψίαστων χρηστών, οι οποίοι ανταλλάσσουν αυτά τα προγράμματα ή αρχεία φορέα σε δίσκο ή USBstick. ή που τα στέλνουν ο ένας στον άλλο μέσω δικτύου. Σε ένα περιβάλλον δικτύου, η δυνατότητα πρόσβασης σε έγγραφα, εφαρμογές και υπηρεσίες συστήματος σε άλλους υπολογιστές παρέχει μια τέλεια κουλτούρα για την εξάπλωση αυτού του ιικού κώδικα.

Ένας ιός που συνδέεται με ένα εκτελέσιμο πρόγραμμα μπορεί να κάνει οτιδήποτε επιτρέπεται να κάνει το πρόγραμμα. Εκτελείται κρυφά όταν εκτελείται το πρόγραμμα υποδοχής. Όταν εκτελείται ο κωδικός ιών, μπορεί να εκτελέσει οποιαδήποτε λειτουργία, όπως διαγραφή αρχείων και προγραμμάτων, η οποία επιτρέπεται από τα δικαιώματα του τρέχοντος χρήστη. Ένας λόγος που οι ιοί κυριάρχησαν στη σκηνή του κακόβουλου λογισμικού τα προηγούμενα χρόνια ήταν η έλλειψη ελέγχου ταυτότητας χρήστη και ελέγχου πρόσβασης σε συστήματα

προσωπικών υπολογιστών εκείνη την εποχή. Αυτό επέτρεψε σε έναν ιό να μολύνει οποιοδήποτε εκτελέσιμο περιεχόμενο στο σύστημα. Η σημαντική ποσότητα προγραμμάτων που μοιράστηκαν σε δισκέτα επέτρεψε επίσης την εύκολη, αν και κάπως αργή, εξάπλωσή της. Η συμπερίληψη αυστηρότερων ελέγχων πρόσβασης σε σύγχρονα λειτουργικά συστήματα εμποδίζει σημαντικά την ευκολία μόλυνσης ενός τέτοιου παραδοσιακού, εκτελέσιμου από υπολογιστή κώδικα ιών. Αυτό είχε ως αποτέλεσμα την ανάπτυξη ιών μακροεντολών που εκμεταλλεύονται το ενεργό περιεχόμενο που υποστηρίζεται από ορισμένους τύπους εγγράφων, όπως αρχεία MicrosoftWord ή Excel ή έγγραφα AdobePDF. Τέτοια έγγραφα τροποποιούνται εύκολα και κοινοποιούνται από τους χρήστες ως μέρος της κανονικής χρήσης του συστήματος και δεν προστατεύονται από τα ίδια στοιχεία ελέγχου πρόσβασης με τα προγράμματα. Επί του παρόντος, ένας ιικός τρόπος μόλυνσης είναι συνήθως ένας από τους διάφορους μηχανισμούς διάδοσης που χρησιμοποιούνται από σύγχρονο κακόβουλο λογισμικό, το οποίο μπορεί επίσης να περιλαμβάνει δυνατότητες worm και Trojan.

[AYCO06] δηλώνει ότι ένας ιός υπολογιστή έχει τρία μέρη. Γενικότερα, πολλοί σύγχρονοι τύποι κακόβουλου λογισμικού περιλαμβάνουν επίσης μία ή περισσότερες παραλλαγές καθενός από αυτά τα στοιχεία:

- Μηχανισμός μόλυνσης: Τα μέσα με τα οποία ένας ιός εξαπλώνεται ή διαδίδεται, επιτρέποντάς του να αναπαραχθεί. Ο μηχανισμός αναφέρεται επίσης ως φορέας μόλυνσης.
- Trigger: Το συμβάν ή η συνθήκη που καθορίζει πότε ενεργοποιείται ή παραδίδεται το ωφέλιμο φορτίο, μερικές φορές γνωστή ως λογική βόμβα.
- Ωφέλιμο φορτίο: Τι κάνει ο ιός, εκτός από την εξάπλωση. Το ωφέλιμο φορτίο μπορεί να συνεπάγεται ζημιά ή μπορεί να περιλαμβάνει καλοήθη αλλά αισθητή δραστηριότητα.

Κατά τη διάρκεια της ζωής του, ένας τυπικός ιός περνά από τις ακόλουθες τέσσερις φάσεις:

• Αδρανοποιημένη φάση: Ο ιός είναι αδρανής. Ο ιός τελικά θα ενεργοποιηθεί από κάποιο συμβάν, όπως ημερομηνία, παρουσία άλλου προγράμματος ή αρχείου ή η χωρητικότητα του δίσκου που υπερβαίνει κάποιο όριο. Δεν έχουν όλοι οι ιοί αυτό το στάδιο.

• Φάση διάδοσης: Ο ιός τοποθετεί ένα αντίγραφο του εαυτού του σε άλλα προγράμματα ή σε ορισμένες περιοχές του συστήματος στο δίσκο. Το αντίγραφο ενδέχεται να μην είναι πανομοιότυπο με την έκδοση διάδοσης. Οι ιοί συχνά μεταμορφώνονται ώστε να αποφεύγουν την ανίχνευση. Κάθε μολυσμένο πρόγραμμα θα περιέχει τώρα έναν κλώνο του ιού, ο οποίος ο ίδιος θα εισέλθει σε μια φάση διάδοσης.

• Φάση ενεργοποίησης: Ο ιός ενεργοποιείται για την εκτέλεση της λειτουργίας για την οποία προοριζόταν. Όπως με την αδρανή φάση, η φάση ενεργοποίησης μπορεί να προκληθεί από μια ποικιλία συμβάντων του συστήματος, συμπεριλαμβανομένου του αριθμού των φορών που αυτό το αντίγραφο του ιού έχει δημιουργήσει αντίγραφα του εαυτού του.

• Φάση εκτέλεσης: Η λειτουργία εκτελείται. Η λειτουργία μπορεί να είναι ακίνδυνη, όπως ένα μήνυμα στην οθόνη ή καταστροφική, όπως η καταστροφή προγραμμάτων και αρχείων δεδομένων.

Οι περισσότεροι ιοί που μολύνουν εκτελέσιμα αρχεία προγράμματος εκτελούν τη δουλειά τους με τρόπο που είναι συγκεκριμένος για ένα συγκεκριμένο λειτουργικό σύστημα και, σε ορισμένες περιπτώσεις, συγκεκριμένοι για μια συγκεκριμένη πλατφόρμα υλικού. Έτσι, έχουν σχεδιαστεί για να εκμεταλλεύονται τις λεπτομέρειες και τις αδυναμίες συγκεκριμένων συστημάτων. Ωστόσο, οι ιοί μακροεντολών στοχεύουν συγκεκριμένους τύπους εγγράφων, οι οποίοι συχνά υποστηρίζονται σε μια ποικιλία συστημάτων.

*Εκτελέσιμη δομή ιών:*Σε έναν παραδοσιακό, εκτελέσιμο υπολογιστικό κώδικα, ο ιός μπορεί να προαχθεί ή να αναβληθεί σε κάποιο εκτελέσιμο πρόγραμμα ή μπορεί να ενσωματωθεί σε αυτόν με κάποιο άλλο τρόπο. Το κλειδί για τη λειτουργία του είναι ότι το μολυσμένο πρόγραμμα, όταν καλείται, θα εκτελέσει πρώτα τον κώδικα ιού και στη συνέχεια θα εκτελέσει τον αρχικό κώδικα του προγράμματος.

Το μολυσμένο πρόγραμμα ξεκινά με τον κωδικό του ιού και λειτουργεί ως εξής. Η πρώτη γραμμή κώδικα είναι ένας ειδικός δείκτης που χρησιμοποιείται από τον ιό για να προσδιορίσει εάν ένα πιθανό πρόγραμμα θύματος έχει ήδη μολυνθεί με αυτόν τον ιό. Όταν καλείται το πρόγραμμα, ο έλεγχος μεταφέρεται αμέσως στο κύριο μπλοκ δράσης που περιέχει τον κωδικό ιού. Ο ιός μπορεί πρώτα να αναζητήσει μη μολυσμένα εκτελέσιμα αρχεία και να τα μολύνει. Στη συνέχεια, ο ιός μπορεί να εκτελέσει το ωφέλιμο φορτίο του, εάν πληρούνται οι απαιτούμενες συνθήκες ενεργοποίησης, εάν υπάρχουν. Τέλος, ο ιός μεταφέρει τον έλεγχο στο αρχικό πρόγραμμα. Εάν η φάση μόλυνσης του προγράμματος είναι αρκετά γρήγορη, ένας χρήστης είναι απίθανο να παρατηρήσει οποιαδήποτε διαφορά μεταξύ της εκτέλεσης ενός μολυσμένου και ενός μη μολυσμένου προγράμματος.

Ένας ιός όπως αυτός που μόλις περιγράφηκε εντοπίζεται εύκολα επειδή μια μολυσμένη έκδοση ενός προγράμματος είναι μεγαλύτερη από την αντίστοιχη μη μολυσμένη.

Μόλις ένας ιός αποκτήσει είσοδο σε ένα σύστημα μολύνοντας ένα μόνο πρόγραμμα, είναι σε θέση να μολύνει μερικά ή όλα τα άλλα εκτελέσιμα αρχεία σε αυτό το σύστημα όταν εκτελείται το μολυσμένο πρόγραμμα, ανάλογα με τα δικαιώματα πρόσβασης που έχει το μολυσμένο πρόγραμμα. Έτσι, η ιογενής λοίμωξη μπορεί να προληφθεί εντελώς εμποδίζοντας την είσοδο του ιού στην πρώτη θέση. Δυστυχώς, η πρόληψη είναι εξαιρετικά δύσκολη, επειδή ένας ιός μπορεί να είναι μέρος οποιουδήποτε προγράμματος εκτός συστήματος. Επομένως, εκτός αν κάποιος είναι ικανοποιημένος να πάρει ένα απολύτως γυμνό κομμάτι σιδήρου και να γράψει όλα τα δικά του συστήματα και προγράμματα εφαρμογής, είναι ευάλωτο. Πολλές μορφές μόλυνσης μπορούν επίσης να αποκλειστούν με την άρνηση των κανονικών χρηστών του δικαιώματος τροποποίησης προγραμμάτων στο σύστημα.

Β) Ταξινόμηση ιών

Υπήρξε ένας συνεχής αγώνας όπλων μεταξύ συγγραφέων ιών και συγγραφέων λογισμικού προστασίας από ιούς από την πρώτη εμφάνιση των ιών. Καθώς αναπτύσσονται αποτελεσματικά αντίμετρα για υπάρχοντες τύπους ιών, αναπτύσσονται νεότεροι τύποι. Δεν υπάρχει απλό ή καθολικά συμφωνημένο σχήμα ταξινόμησης για ιούς. Σε αυτήν την ενότητα, ακολουθούμε το [AYCO06] και ταξινομούμε τους ιούς κατά μήκος δύο ορθογώνιων αξόνων: ο τύπος στόχου που

προσπαθεί να μολύνει ο ιός και η μέθοδος που χρησιμοποιεί ο ιός για να αποκρύψει τον εντοπισμό από χρήστες και λογισμικό προστασίας από ιούς.

Μια ταξινόμηση ιών κατά στόχο περιλαμβάνει τις ακόλουθες κατηγορίες:

- Infector τομέας εκκίνησης: Επηρεάζει μια κύρια εγγραφή εκκίνησης ή εγγραφή εκκίνησης και εξαπλώνεται όταν εκκινείται ένα σύστημα από το δίσκο που περιέχει τον ιό.
- Fileinfector: Επηρεάζει αρχεία που το λειτουργικό σύστημα ή το κέλυφος θεωρούν ότι είναι εκτελέσιμα.
- Macrovirus: Επηρεάζει αρχεία με κώδικα μακροεντολών ή scripting που ερμηνεύεται από μια εφαρμογή.
- Πολλαπλός ιός: Επηρεάζει αρχεία με πολλούς τρόπους. Συνήθως, ο ιός πολλαπλών μερών είναι ικανός να μολύνει πολλούς τύπους αρχείων, έτσι ώστε η εξάλειψη του ιού να αντιμετωπίζει όλες τις πιθανές τοποθεσίες μόλυνσης.

Μια ταξινόμηση ιών με στρατηγική απόκρυψης περιλαμβάνει τις ακόλουθες κατηγορίες:

- Κρυπτογραφημένος ιός: Μια μορφή ιού που χρησιμοποιεί κρυπτογράφηση για να αποκρύψει το περιεχόμενό του. Ένα τμήμα του ιού δημιουργεί ένα τυχαίο κλειδί κρυπτογράφησης και κρυπτογραφεί το υπόλοιπο του ιού. Το κλειδί αποθηκεύεται με τον ιό. Όταν καλείται ένα μολυσμένο πρόγραμμα, ο ιός χρησιμοποιεί το αποθηκευμένο τυχαίο κλειδί για την αποκρυπτογράφηση του ιού. Όταν ο ιός αναπαράγεται, επιλέγεται ένα διαφορετικό τυχαίο κλειδί. Επειδή το μεγαλύτερο μέρος του ιού είναι κρυπτογραφημένο με ένα διαφορετικό κλειδί για κάθε περίπτωση, δεν υπάρχει σταθερό μοτίβο bit που να παρατηρείται.
- Stealthvirus: Μια μορφή ιού που έχει σχεδιαστεί ρητά για να κρύβεται από την ανίχνευση από λογισμικό προστασίας από ιούς. Έτσι, ολόκληρος ο ιός, όχι μόνο ένα ωφέλιμο φορτίο είναι κρυμμένο. Μπορεί να χρησιμοποιήσει τεχνικές μετάλλαξης κώδικα, συμπίεσης ή rootkit για να το επιτύχει.
- Πολυμορφικός ιός: Μία μορφή ιού που δημιουργεί αντίγραφα κατά τη διάρκεια της αναπαραγωγής που είναι λειτουργικά ισοδύναμα αλλά έχουν σαφώς διαφορετικά

μοτίβα bit, προκειμένου να νικήσουν προγράμματα που ανιχνεύουν ιούς. Σε αυτήν την περίπτωση, η «υπογραφή» του ιού θα διαφέρει ανάλογα με κάθε αντίγραφο. Για να επιτευχθεί αυτή η παραλλαγή, ο ιός μπορεί να εισαγάγει τυχαία περιττές οδηγίες ή να αλλάξει τη σειρά ανεξάρτητων οδηγιών. Μια πιο αποτελεσματική προσέγγιση είναι η χρήση κρυπτογράφησης. Ακολουθείται η στρατηγική του ιού κρυπτογράφησης. Το τμήμα του ιού που είναι υπεύθυνο για τη δημιουργία κλειδιών και την εκτέλεση κρυπτογράφησης / αποκρυπτογράφησης αναφέρεται ως μηχανή μετάλλαξης. Η ίδια η μηχανή μετάλλαξης αλλάζειμεκάθεχρήση.

- Μεταμορφικός ιός: Όπως και με έναν πολυμορφικό ιό, ένας μεταμορφικός ιός μεταλλάσσεται με κάθε λοίμωξη. Η διαφορά είναι ότι ένας μεταμορφικός ιός ξαναγράφεται πλήρως σε κάθε επανάληψη, χρησιμοποιώντας πολλαπλές τεχνικές μετασχηματισμού, αυξάνοντας τη δυσκολία ανίχνευσης. Οι μεταμορφικοί ιοί μπορεί να αλλάξουν τη συμπεριφορά τους καθώς και την εμφάνισή τους.

Γ) Ιοί μακροεντολών και σεναρίων

Στα μέσα της δεκαετίας του 1990, οι ιοί κώδικα μακροεντολών ή scripting έγιναν μακράν ο πιο διαδεδομένος τύπος ιού. Οι ιοί μακροεντολών μολύνουν κώδικα δέσμης ενεργειών που χρησιμοποιείται για την υποστήριξη ενεργού περιεχομένου σε διάφορους τύπους εγγράφων χρήστη. Οι μακροίιοί απειλούνιδιαίτερα για διάφορουςλόγους:

1. Ο μακρο ιός είναι ανεξάρτητος από την πλατφόρμα. Πολλοί ιοί μακροεντολών μολύνουν ενεργό περιεχόμενο σε εφαρμογές που χρησιμοποιούνται συνήθως, όπως μακροεντολές σε έγγραφα του MicrosoftWord ή σε άλλα έγγραφα του MicrosoftOffice ή κώδικα δέσμης ενεργειών σε έγγραφα AdobePDF. Οποιαδήποτε πλατφόρμα υλικού και λειτουργικό σύστημα που υποστηρίζει αυτές τις εφαρμογές μπορεί να μολυνθεί.
2. Οι ιοί μακροεντολών μολύνουν έγγραφα, όχι εκτελέσιμα τμήματα κώδικα. Οι περισσότερες από τις πληροφορίες που εισάγονται σε ένα σύστημα υπολογιστή έχουν τη μορφή εγγράφων και όχι προγραμμάτων.
3. Οι μακροί ιοί εξαπλώνονται εύκολα, καθώς τα έγγραφα που εκμεταλλεύονται κοινοποιούνται σε κανονική χρήση. Μια πολύκοινήμέθοδοςείναι μέσωηλεκτρονικού ταχυδρομείου.

4. Επειδή οι ιοί μακροεντολών μολύνουν έγγραφα χρήστη και όχι προγράμματα συστήματος, τα παραδοσιακά στοιχεία ελέγχου πρόσβασης συστήματος αρχείων είναι περιορισμένης χρήσης για την αποτροπή της εξάπλωσής τους, καθώς οι χρήστες αναμένεται να τα τροποποιήσουν.

Οι ιοί μακροεντολών εκμεταλλεύονται την υποστήριξη για ενεργό περιεχόμενο χρησιμοποιώντας μια δέσμη ενεργειών ή μια γλώσσα μακροεντολών, ενσωματωμένα σε ένα έγγραφο επεξεργασίας κειμένου ή άλλο τύπο αρχείου. Συνήθως, οι χρήστες χρησιμοποιούν μακροεντολές για να αυτοματοποιήσουν τις επαναλαμβανόμενες εργασίες και επομένως να αποθηκεύσουν πατήματα πλήκτρων. Χρησιμοποιούνται επίσης για την υποστήριξη δυναμικού περιεχομένου, επικύρωσης φόρμας και άλλων χρήσιμων εργασιών που σχετίζονται με αυτά τα έγγραφα.

Οι διαδοχικές εκδόσεις προϊόντων MSOffice παρέχουν αυξημένη προστασία έναντι ιών μακροεντολών. Για παράδειγμα, η Microsoft προσφέρει ένα προαιρετικό εργαλείο προστασίας από ιούς μακροεντολών που εντοπίζει ύποπτα αρχεία Word και ειδοποιεί τον πελάτη για τον πιθανό κίνδυνο ανοίγματος ενός αρχείου με μακροεντολές. Διάφοροι προμηθευτές προϊόντων προστασίας από ιούς έχουν επίσης αναπτύξει εργαλεία για τον εντοπισμό και την αφαίρεση ιών μακροεντολών. Όπως και σε άλλους τύπους κακόβουλου λογισμικού, ο αγώνας όπλων συνεχίζεται στον τομέα των ιών μακροεντολών, αλλά δεν αποτελούν πλέον την κυρίαρχη απειλή κακόβουλου λογισμικού.

Ένας άλλος πιθανός κεντρικός υπολογιστής για κακόβουλο λογισμικό τύπου ιού είναι στα έγγραφα PDF της Adobe. Αυτά μπορούν να υποστηρίξουν μια σειρά ενσωματωμένων στοιχείων, συμπεριλαμβανομένου του Javascript και άλλων τύπων κώδικα δέσμης ενεργειών. Παρόλο που τα πρόσφατα προγράμματα προβολής PDF περιλαμβάνουν μέτρα για την προειδοποίηση των χρηστών όταν εκτελείται τέτοιος κώδικας, το μήνυμα που εμφανίζεται στον χρήστη μπορεί να χρησιμοποιηθεί για να τους εξαπατήσει ώστε να επιτρέψει την εκτέλεση του. Εάν συμβεί αυτό, ο κώδικας θα μπορούσε ενδεχομένως να λειτουργήσει ως ιός για να μολύνει άλλα έγγραφα PDF στα οποία ο χρήστης έχει πρόσβαση στο σύστημά του. Εναλλακτικά, μπορεί να εγκαταστήσει έναν Trojan ή να λειτουργήσει ως worm, όπως θα συζητήσουμε αργότερα [STEV11].

2.4. Διάδοση – Εκμετάλλευση Ευπάθειας – Υπολογιστικό Σκουλήκι (Worms)

Η επόμενη κατηγορία διάδοσης κακόβουλου λογισμικού αφορά την εκμετάλλευση ευπαθειών λογισμικού, όπως αυτά που συζητάμε στα Κεφάλαια 10 και 11, τα οποία συνήθως εκμεταλλεύονται τα worms υπολογιστών. Ένα σκουλήκι είναι ένα πρόγραμμα που αναζητά ενεργά περισσότερα μηχανήματα για να μολύνουν και στη συνέχεια κάθε μολυσμένο μηχάνημα χρησιμεύει ως αυτοματοποιημένο ταμπλό εκκίνησης για επιθέσεις σε άλλα μηχανήματα. Τα προγράμματα Worm εκμεταλλεύονται ευπάθειες λογισμικού σε προγράμματα πελάτη ή διακομιστή για να αποκτήσουν πρόσβαση σε κάθε νέο σύστημα. Μπορούν να χρησιμοποιούν συνδέσεις δικτύου για μετάδοση από σύστημα σε σύστημα. Μπορούν επίσης να εξαπλωθούν μέσω κοινόχρηστων μέσων, όπως μονάδες USB ή δίσκους δεδομένων CD και DVD. Τα σκουλήκια ηλεκτρονικού ταχυδρομείου εξαπλώνονται σε κώδικα μακροεντολής ή σεναρίου που περιλαμβάνονται σε έγγραφα που επισυνάπτονται σε ηλεκτρονικό ταχυδρομείο ή σε μεταφορές αρχείων άμεσων μηνυμάτων. Με την ενεργοποίηση, το σκουλήκι μπορεί να αναπαραχθεί και να εξαπλωθεί ξανά. Εκτός από τη διάδοση, το σκουλήκι φέρει συνήθως κάποια μορφή ωφέλιμου φορτίου.

Η ιδέα ενός σκουλήκι υπολογιστή παρουσιάστηκε στο μυθιστόρημα του JohnBrunner το 1975, TheShockwaveRider. Η πρώτη γνωστή εφαρμογή σκουληκιών έγινε στα εργαστήρια XeroxPaloAlto στις αρχές της δεκαετίας του 1980. Ήταν μη κακόβουλο, ψάχνοντας για αδράνεια συστήματα για χρήση για να εκτελέσετε μια υπολογιστικά εντατική εργασία.

Για να αναπαραχθεί, ένα worm χρησιμοποιεί κάποια μέσα για να αποκτήσει πρόσβαση σε απομακρυσμένα συστήματα. Αυτά περιλαμβάνουν τα ακόλουθα, τα περισσότερα από τα οποία εξακολουθούν να εμφανίζονται σε ενεργή χρήση [SYMA13]:

- Ηλεκτρονική αλληλογραφία ή εγκατάσταση ανταλλαγής άμεσων μηνυμάτων: Ένα worm στέλνει μέσω e-mail αντίγραφο του εαυτού του σε άλλα συστήματα ή αποστέλλεται ως συνημμένο μέσω υπηρεσίας άμεσων μηνυμάτων, έτσι ώστε ο κώδικάς του να εκτελείται κατά τη λήψη ή προβολή του e-mail ή του συνημμένου .
- Κοινή χρήση αρχείων: Ένα σκουλήκι δημιουργεί ένα αντίγραφο του εαυτού του ή μολύνει άλλα κατάλληλα αρχεία ως ιό σε αφαιρούμενα μέσα όπως μια μονάδα USB. Στη συνέχεια εκτελείται όταν η μονάδα δίσκου είναι συνδεδεμένη σε άλλο σύστημα

χρησιμοποιώντας το μηχανισμό αυτόματης εκτέλεσης εκμεταλλευόμενη κάποια ευπάθεια λογισμικού ή όταν ένας χρήστης ανοίγει το μολυσμένο αρχείο στο σύστημα προορισμού.

- Δυνατότητα απομακρυσμένης εκτέλεσης: Ένα worm εκτελεί ένα αντίγραφο του εαυτού του σε άλλο σύστημα, είτε χρησιμοποιώντας μια ρητή εγκατάσταση απομακρυσμένης εκτέλεσης είτε εκμεταλλευόμενος ένα ελάττωμα προγράμματος σε μια υπηρεσία δικτύου για να ανατρέψει τις λειτουργίες του (όπως συζητάμε στα Κεφάλαια 10 και 11).
- Απομακρυσμένη πρόσβαση αρχείων ή δυνατότητα μεταφοράς: Ένα worm χρησιμοποιεί απομακρυσμένη πρόσβαση αρχείων ή υπηρεσία μεταφοράς σε άλλο σύστημα για να αντιγράψει τον εαυτό του από το ένα σύστημα στο άλλο, όπου οι χρήστες σε αυτό το σύστημα μπορούν στη συνέχεια να το εκτελέσουν.
- Δυνατότητα απομακρυσμένης σύνδεσης: Ένα σκουλήκι συνδέεται σε ένα απομακρυσμένο σύστημα ως χρήστης και στη συνέχεια χρησιμοποιεί εντολές για να αντιγραφεί από το ένα σύστημα στο άλλο, όπου στη συνέχεια εκτελείται. Το νέο αντίγραφο του προγράμματος worm εκτελείται στη συνέχεια στο απομακρυσμένο σύστημα όπου, εκτός από τις λειτουργίες ωφέλιμου φορτίου που εκτελεί σε αυτό το σύστημα, συνεχίζει να διαδίδεται.

Ένα σκουλήκι χρησιμοποιεί συνήθως τις ίδιες φάσεις με τον ιό του υπολογιστή: αδρανής, διάδοση, ενεργοποίηση και εκτέλεση. Η φάση διάδοσης εκτελεί γενικά τις ακόλουθες λειτουργίες:

- Αναζήτηση κατάλληλων μηχανισμών πρόσβασης σε άλλα συστήματα για να μολύνουν εξετάζοντας πίνακες κεντρικού υπολογιστή, βιβλία διευθύνσεων, λίστες φίλων, αξιόπιστους συνομηλίκους και άλλα παρόμοια αποθετήρια λεπτομερειών πρόσβασης απομακρυσμένου συστήματος. με σάρωση πιθανών διευθύνσεων κεντρικού υπολογιστή στόχου · ή αναζητώντας κατάλληλες αφαιρούμενες συσκευές μέσων για χρήση.

- Χρησιμοποιήστε τους μηχανισμούς πρόσβασης που βρέθηκαν για να μεταφέρετε ένα αντίγραφο του στο απομακρυσμένο σύστημα και να προκαλέσετε την εκτέλεση του αντιγράφου.

Το σκουλήκι μπορεί επίσης να προσπαθήσει να προσδιορίσει εάν ένα σύστημα είχε προηγουμένως μολυνθεί πριν από την αντιγραφή του στο σύστημα. Σε ένα σύστημα πολλαπλού προγραμματισμού, μπορεί επίσης να συγκαλύψει την παρουσία του ονομάζοντας τον εαυτό του ως διαδικασία συστήματος ή χρησιμοποιώντας κάποιο άλλο όνομα που μπορεί να μην παρατηρηθεί από έναν χειριστή συστήματος. Τα πιο πρόσφατα σκουλήκια μπορούν ακόμη και να εισάγουν τον κώδικά τους σε υπάρχουσες διαδικασίες στο σύστημα και να τρέξουν χρησιμοποιώντας επιπλέον νήματα σε αυτήν τη διαδικασία, για να συγκαλύψουν περαιτέρω την παρουσία τους.

Α) Ανακάλυψη στόχου

Η πρώτη λειτουργία στη φάση διάδοσης ενός worm δικτύου είναι να αναζητά άλλα συστήματα που θα μολύνουν, μια διαδικασία γνωστή ως σάρωση ή δακτυλικό αποτύπωμα. Για τέτοια σκουλήκια, τα οποία εκμεταλλεύονται ευπάθειες λογισμικού σε απομακρυσμένες προσβάσιμες υπηρεσίες δικτύου, πρέπει να προσδιορίσει πιθανά συστήματα που εκτελούν την ευάλωτη υπηρεσία και, στη συνέχεια, να τα μολύνει. Τότε, συνήθως, ο κώδικας worm που είναι τώρα εγκατεστημένος στα μολυσμένα μηχανήματα επαναλαμβάνει την ίδια διαδικασία σάρωσης, έως ότου δημιουργηθεί ένα μεγάλο κατανεμημένο δίκτυο μολυσμένων μηχανών.

[MIRK04] παραθέτει τους ακόλουθους τύπους στρατηγικών σάρωσης διευθύνσεων δικτύου που μπορεί να χρησιμοποιήσει ένα τέτοιο worm:

- Τυχαία: Κάθε παραβιασμένος κεντρικός υπολογιστής ανιχνεύει τυχαίες διευθύνσεις στο χώρο διευθύνσεων IP, χρησιμοποιώντας διαφορετικό σπόρο. Αυτή η τεχνική παράγει

μεγάλο όγκο κίνησης στο Διαδίκτυο, το οποίο μπορεί να προκαλέσει γενικευμένη διακοπή πριν από την έναρξη της πραγματικής επίθεσης.

- Hit-List: Ο εισβολέας καταρτίζει πρώτα μια μακρά λίστα πιθανών ευάλωτων μηχανών. Αυτό μπορεί να είναι μια αργή διαδικασία που πραγματοποιείται για μεγάλο χρονικό διάστημα για να αποφευχθεί η ανίχνευση ότι μια επίθεση βρίσκεται σε εξέλιξη. Μόλις καταρτιστεί η λίστα, ο εισβολέας αρχίζει να μολύνει μηχανές στη λίστα. Σε κάθε μολυσμένο μηχάνημα παρέχεται ένα τμήμα της λίστας για σάρωση. Αυτή η στρατηγική οδηγεί σε μια πολύ σύντομη περίοδο σάρωσης, η οποία μπορεί να δυσκολεύει τον εντοπισμό της μόλυνσης.
- Τοπολογικά: Αυτή η μέθοδος χρησιμοποιεί πληροφορίες που περιέχονται σε ένα μολυσμένο μηχάνημα θύματος για να βρει περισσότερους κεντρικούς υπολογιστές για σάρωση.
- Τοπικό υποδίκτυο: Εάν ένας κεντρικός υπολογιστής μπορεί να μολυνθεί πίσω από ένα τείχος προστασίας, αυτός ο κεντρικός υπολογιστής αναζητά στόχους στο δικό του τοπικό δίκτυο. Ο κεντρικός υπολογιστής χρησιμοποιεί τη δομή διευθύνσεων υποδικτύου για να βρει άλλους κεντρικούς υπολογιστές που διαφορετικά θα προστατεύονταν από το τείχος προστασίας.

Β) Μοντέλο διάδοσης σκουληκιών

Ένα καλά σχεδιασμένο σκουλήκι μπορεί να εξαπλωθεί γρήγορα και να μολύνει τεράστιους αριθμούς ξενιστών. Είναι χρήσιμο να έχουμε ένα γενικό μοντέλο για τον ρυθμό διάδοσης των σκουληκιών. Οι ιοί υπολογιστών και τα σκουλήκια παρουσιάζουν παρόμοια συμπεριφορά αυτοδιπλασιασμού και διάδοσης με βιολογικούς ιούς. Έτσι μπορούμε να δούμε κλασικά επιδημικά μοντέλα για την κατανόηση της συμπεριφοράς του ιού του υπολογιστή και της διάδοσης των σκουληκιών. Ένα απλοποιημένο, κλασικό επιδημικό μοντέλο μπορεί να εκφραστεί ως εξής:

$$\frac{dI(t)}{dt} = \beta I(t)S(t)$$

όπου:

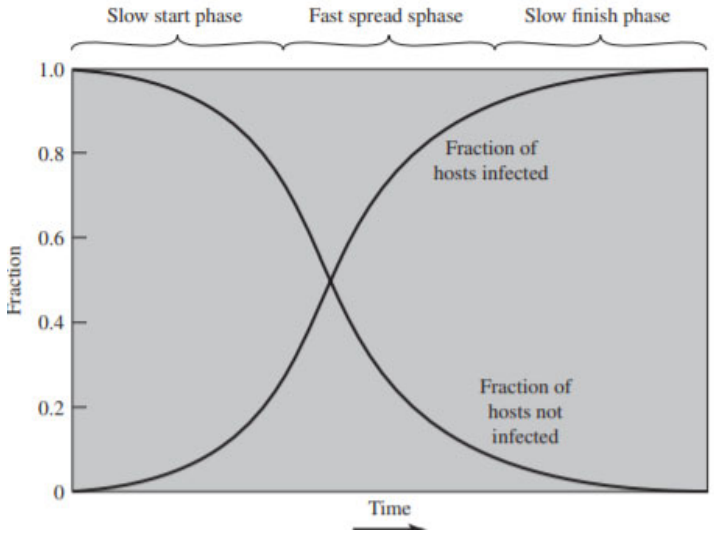
I(t) = αριθμός συστημάτων που έχουν μολυνθεί από το χρόνο t

S(t) = αριθμός ευπαθών συστημάτων (επιρρεπείς σε λοίμωξη αλλά δεν έχουν ακόμη μολυνθεί) τη στιγμή t

β = ποσοστόμόλυνσης

N = μέγεθος του πληθυσμού =>N = I(t) + S(t)

Σχήμα 2.4.1. δείχνει τη δυναμική της διάδοσης σκουληκιών χρησιμοποιώντας αυτό το μοντέλο. Η διάδοση προχωρά σε τρεις φάσεις. Στην αρχική φάση, ο αριθμός των κεντρικών υπολογιστών αυξάνεται εκθετικά. Για να δείτε ότι συμβαίνει αυτό, σκεφτείτε μια απλοποιημένη περίπτωση στην οποία ξεκινά ένα σκουλήκι από έναν μόνο κεντρικό υπολογιστή και μολύνει δύο κοντινούς κεντρικούς υπολογιστές. Κάθε ένας από αυτούς τους κεντρικούς υπολογιστές μολύνει δύο ακόμη κεντρικούς υπολογιστές, και ούτω καθεξής. Αυτό οδηγεί σε εκθετική ανάπτυξη. Μετά από λίγο καιρό, η μόλυνση των ξενιστών χάνει λίγο χρόνο επιτίθεται σε ήδη μολυσμένους ξενιστές, γεγονός που μειώνει το ποσοστό μόλυνσης. Κατά τη διάρκεια αυτής της μεσαίας φάσης, η ανάπτυξη είναι περίπου γραμμική, αλλά ο ρυθμός μόλυνσης είναι γρήγορος. Όταν οι περισσότεροι ευάλωτοι υπολογιστές έχουν μολυνθεί, η επίθεση εισέρχεται σε μια φάση αργής ολοκλήρωσης καθώς το worm αναζητά εκείνους τους υπόλοιπους κεντρικούς υπολογιστές που είναι δύσκολο να εντοπιστούν.



Πίνακας 2.4.1: Μοντέλο διάδοσης σκουληκιών (Worms)

Είναι σαφές ότι ο στόχος για την αντιμετώπιση ενός σκουληκιού είναι να πιάσει το σκουλήκι στη φάση της αργής εκκίνησης, σε μια στιγμή που λίγοι ξενιστές έχουν μολυνθεί.

[ZOU05] περιγράφουν ένα μοντέλο διάδοσης σκουληκιών που βασίζεται σε ανάλυση των επιθέσεων worm δικτύου εκείνη την εποχή. Η ταχύτητα διάδοσης και ο συνολικός αριθμός των μολυσμένων ξενιστών εξαρτώνται από διάφορους παράγοντες, συμπεριλαμβανομένου του τρόπου διάδοσης, της ευπάθειας ή των ευπαθειών που εκμεταλλεύονται και του βαθμού ομοιότητας με τις προηγούμενες επιθέσεις. Για τον τελευταίο παράγοντα, μια επίθεση που αποτελεί παραλλαγή μιας πρόσφατης προηγούμενης επίθεσης μπορεί να αντιμετωπιστεί πιο αποτελεσματικά από μια πιο νέα επίθεση. Το μοντέλο του Zou συμφωνεί στενά με το Σχήμα 2.4.1.

Γ) Το σκουλήκι του Morris

Αναμφισβήτητα, η πρώτη σημαντική, και ως εκ τούτου γνωστή, μόλυνση από σκουλήκια κυκλοφόρησε στο Διαδίκτυο από τον RobertMorris το 1988 [ORMA03]. Το σκουλήκι Morris σχεδιάστηκε για να εξαπλωθεί σε συστήματα UNIX και χρησιμοποίησε διάφορες διαφορετικές τεχνικές για τη διάδοση. Όταν ξεκίνησε η εκτέλεση ενός αντιγράφου, το πρώτο του έργο ήταν να ανακαλύψει άλλους κεντρικούς υπολογιστές που είναι γνωστοί σε αυτόν τον κεντρικό υπολογιστή που θα επέτρεπαν την είσοδο από αυτόν τον κεντρικό υπολογιστή. Το worm πραγματοποίησε αυτήν την εργασία εξετάζοντας μια ποικιλία λιστών και πινάκων, συμπεριλαμβανομένων πινάκων συστήματος που δήλωσαν ότι άλλα μηχανήματα ήταν αξιόπιστα από αυτόν τον κεντρικό υπολογιστή, αρχεία προώθησης αλληλογραφίας χρηστών, πίνακες με τους οποίους οι χρήστες έδωσαν άδεια πρόσβασης σε απομακρυσμένους λογαριασμούς και από πρόγραμμα που ανέφερε την κατάσταση των συνδέσεων δικτύου. Για κάθε κεντρικό υπολογιστή που ανακαλύφθηκε, το worm δοκίμασε μια σειρά μεθόδων για να αποκτήσει πρόσβαση:

- Προσπάθησε να συνδεθεί σε έναν απομακρυσμένο κεντρικό υπολογιστή ως νόμιμος χρήστης. Σε αυτήν τη μέθοδο, το worm προσπάθησε πρώτα να σπάσει το τοπικό αρχείο κωδικού πρόσβασης και στη συνέχεια χρησιμοποίησε τους κωδικούς πρόσβασης που ανακαλύφθηκαν και τα αντίστοιχα αναγνωριστικά χρήστη. Η υπόθεση ήταν ότι πολλοί

χρήστες θα χρησιμοποιούν τον ίδιο κωδικό πρόσβασης σε διαφορετικά συστήματα. Για να αποκτήσετε τους κωδικούς πρόσβασης, το worm έτρεξε ένα πρόγραμμα διάσπασης κωδικού πρόσβασης που προσπάθησε:

1) Όνομα λογαριασμού κάθε χρήστη και απλές παραλλαγές αυτού
2) Μια λίστα με 432 ενσωματωμένους κωδικούς πρόσβασης που ο Μόρις πίστευε ότι είναι πιθανό υποψήφιοι
3) Όλες τις λέξεις στο λεξικό του τοπικού συστήματος.

- Εκμεταλλεύτηκε ένα σφάλμα στο πρωτόκολλο UNIX, το οποίο αναφέρει την τοποθεσία ενός απομακρυσμένου χρήστη.
- Εκμεταλλεύτηκε μια παγίδα στην επιλογή εντοπισμού σφαλμάτων της απομακρυσμένης διαδικασίας που λαμβάνει και στέλνει αλληλογραφία.

Εάν κάποια από αυτές τις επιθέσεις πέτυχε, το worm πέτυχε επικοινωνία με τον διερμηνέα εντολών του λειτουργικού συστήματος. Στη συνέχεια έστειλε σε αυτόν τον διερμηνέα ένα σύντομο πρόγραμμα bootstrap, εξέδωσε εντολή για την εκτέλεση αυτού του προγράμματος και στη συνέχεια αποσυνδέθηκε. Στη συνέχεια, το πρόγραμμα bootstrap κάλεσε ξανά το γονικό πρόγραμμα και κατέβασε το υπόλοιπο του worm. Στη συνέχεια εκτελέστηκε το νέο σκουλήκι.

Δ)Σύγχρονη κατάσταση σκουληκιών

Η τελευταία λέξη της τεχνολογίας των worms περιλαμβάνει τα εξής:

- Πολλαπλατφόρμα: Τα νεότερα σκουλήκια δεν περιορίζονται σε μηχανές Windows, αλλά μπορούν να επιτεθούν σε διάφορες πλατφόρμες, ειδικά στις δημοφιλείς ποικιλίες του UNIX. ή εκμεταλλευτείτε γλώσσες μακροεντολών ή scripting που υποστηρίζονται σε δημοφιλείς τύπους εγγράφων.
- Multi-exploit: Νέα worm διεισδύουν σε συστήματα με διάφορους τρόπους, χρησιμοποιώντας exploits σε διακομιστές Web, προγράμματα περιήγησης, e-mail, κοινή χρήση αρχείων και άλλες εφαρμογές που βασίζονται σε δίκτυο. ή μέσω κοινόχρηστων μέσων.

- Εξάπλωση Ultrafast: Αξιοποιήστε διάφορες τεχνικές για τη βελτιστοποίηση του ρυθμού εξάπλωσης ενός σκουληκιού για να μεγιστοποιήσετε την πιθανότητα εντοπισμού όσο το δυνατόν περισσότερων ευάλωτων μηχανών σε σύντομο χρονικό διάστημα.
- Πολυμορφικό: Για να αποφύγετε την ανίχνευση, να παραλείψετε τα προηγούμενα φίλτρα και να αποφύγετε την ανάλυση σε πραγματικό χρόνο, τα σκουλήκια υιοθετούν πολυμορφικές τεχνικές ιών Κάθε αντίγραφο του worm έχει νέο κώδικα που δημιουργείται εν κινήσει χρησιμοποιώντας λειτουργικά ισοδύναμες οδηγίες και τεχνικές κρυπτογράφησης.
- Μεταμόρφωση: Εκτός από την αλλαγή της εμφάνισής τους, τα μεταμορφικά σκουλήκια έχουν ένα ρεπερτόριο προτύπων συμπεριφοράς που εξαπολύονται σε διαφορετικά στάδια διάδοσης.
- Οχήματα μεταφοράς: Επειδή τα σκουλήκια μπορούν να θέσουν σε κίνδυνο έναν μεγάλο αριθμό συστημάτων, είναι ιδανικά για τη διάδοση μιας μεγάλης ποικιλίας κακόβουλων ωφέλιμων φορτίων, όπως κατανεμημένα bots άρνησης υπηρεσίας, rootkit, γεννήτριες ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου και spyware.
- Zero-dayexploit: Για να επιτευχθεί η μέγιστη έκπληξη και διανομή, ένα worm πρέπει να εκμεταλλευτεί μια άγνωστη ευπάθεια που ανακαλύπτεται μόνο από τη γενική κοινότητα του δικτύου όταν ξεκινά το worm.

Ε) Κωδικόςκινητώντηλεφώνων

Ο κωδικός για κινητά αναφέρεται σε προγράμματα (π.χ. σενάριο, μακροεντολή ή άλλη φορητή οδηγία) που μπορούν να αποσταλούν αμετάβλητα σε μια ετερογενή συλλογή πλατφορμών και να εκτελεστούν με την ίδια σημασιολογία [JANS08].

Ο κωδικός κινητής τηλεφωνίας μεταδίδεται από ένα απομακρυσμένο σύστημα σε ένα τοπικό σύστημα και στη συνέχεια εκτελείται στο τοπικό σύστημα χωρίς τη ρητή οδηγία του χρήστη [SOUP13]. Ο κωδικός κινητής τηλεφωνίας συχνά λειτουργεί ως μηχανισμός μετάδοσης

ιού, worm ή Trojanhorse στον σταθμό εργασίας του χρήστη. Σε άλλες περιπτώσεις, ο κώδικας κινητής τηλεφωνίας εκμεταλλεύεται τις ευπάθειες για την εκτέλεση των δικών του εκμεταλλεύσεων, όπως μη εξουσιοδοτημένη πρόσβαση δεδομένων ή συμβιβασμός ρίζας. Τα δημοφιλή οχήματα για κώδικα κινητής τηλεφωνίας περιλαμβάνουν εφαρμογές Java, ActiveX, JavaScript και VBScript. Οι πιο συνηθισμένες μέθοδοι χρήσης κώδικα κινητής τηλεφωνίας για κακόβουλες λειτουργίες σε τοπικό σύστημα είναι η δέσμη ενεργειών μεταξύ ιστότοπων, οι διαδραστικοί και δυναμικοί ιστότοποι, τα συνημμένα μηνύματα ηλεκτρονικού ταχυδρομείου και οι λήψεις από μη αξιόπιστους ιστότοπους ή μη αξιόπιστου λογισμικού.

Στ) Worms κινητού τηλεφώνου

Τα Worms εμφανίστηκαν για πρώτη φορά σε κινητά τηλέφωνα με την ανακάλυψη του σκουλήκι Cabir το 2004 και στη συνέχεια Lasco και CommWarrior το 2005. Αυτά τα σκουλήκια επικοινωνούν μέσω ασύρματων συνδέσεων Bluetooth ή μέσω της υπηρεσίας ανταλλαγής μηνυμάτων πολυμέσων (MMS). Ο στόχος είναι το smartphone, το οποίο είναι ένα κινητό τηλέφωνο που επιτρέπει στους χρήστες να εγκαταστήσουν εφαρμογές λογισμικού από άλλες πηγές εκτός του φορέα κινητής τηλεφωνίας. Όλα αυτά τα πρώιμα κινητά σκουλήκια στοχεύουν κινητά τηλέφωνα που χρησιμοποιούν το λειτουργικό σύστημα Symbian. Το πιο πρόσφατο κακόβουλο λογισμικό στοχεύει συστήματα Android και iPhone. Το κακόβουλο λογισμικό του κινητού τηλεφώνου μπορεί να απενεργοποιήσει εντελώς το τηλέφωνο, να διαγράψει δεδομένα στο τηλέφωνο ή να αναγκάσει τη συσκευή να στείλει δαπανηρά μηνύματα σε αριθμούς premium.

Το σκουλήκι CommWarrior αναπαράγεται μέσω Bluetooth σε άλλα τηλέφωνα στην περιοχή λήψης. Αποστέλλεται επίσης ως αρχείο MMS σε αριθμούς στο βιβλίο διευθύνσεων του τηλεφώνου και σε αυτόματες απαντήσεις σε εισερχόμενα μηνύματα κειμένου και μηνύματα MMS. Επιπλέον, αντιγράφεται στην αφαιρούμενη κάρτα μνήμης και εισάγεται στα αρχεία εγκατάστασης του προγράμματος στο τηλέφωνο.

Αν και αυτά τα παραδείγματα δείχνουν ότι είναι πιθανά τα σκουλήκια των κινητών τηλεφώνων, η συντριπτική πλειονότητα των κακόβουλων προγραμμάτων κινητής τηλεφωνίας που παρατηρούνται χρησιμοποιούν trojanapps για να εγκατασταθούν.

Ζ) Ευπάθειες από πλευράς πελατών και Drive-by-Downloads

Μια άλλη προσέγγιση για την εκμετάλλευση τρωτών σημείων λογισμικού περιλαμβάνει την εκμετάλλευση σφαλμάτων σε εφαρμογές χρηστών για την εγκατάσταση κακόβουλου λογισμικού. Μια κοινή τεχνική εκμεταλλεύεται τις ευπάθειες του προγράμματος περιήγησης, έτσι ώστε όταν ο χρήστης βλέπει μια ιστοσελίδα που ελέγχεται από τον εισβολέα, περιέχει κώδικα που εκμεταλλεύεται το σφάλμα του προγράμματος περιήγησης για λήψη και εγκατάσταση κακόβουλου λογισμικού στο σύστημα χωρίς τη γνώση ή τη συγκατάθεση του χρήστη. Αυτό είναι γνωστό ως drive-bydownload και είναι ένα κοινό πλεονέκτημα σε πρόσφατα κιτ επίθεσης. Στις περισσότερες περιπτώσεις, αυτό το κακόβουλο λογισμικό δεν διαδίδεται ενεργά όπως κάνει το worm, αλλά περιμένει ανυποψίαστους χρήστες να επισκεφθούν την κακόβουλη ιστοσελίδα για να εξαπλωθούν στα συστήματά τους.

Σε γενικές γραμμές, οι επιθέσεις drive-by-download στοχεύουν σε οποιονδήποτε επισκέπτεται έναν παραβιασμένο ιστότοπο και είναι ευάλωτος στα εκμεταλλεύματα που χρησιμοποιούνται. Οι επιθέσεις water-hole είναι μια παραλλαγή αυτής που χρησιμοποιείται σε επιθέσεις υψηλής στόχευσης [SYMA13]. Ο εισβολέας ερευνά τα προοριζόμενα θύματά του για να εντοπίσει ιστότοπους που είναι πιθανό να επισκεφθούν και, στη συνέχεια, σαρώνει αυτούς τους ιστότοπους για να εντοπίσει εκείνους με τρωτά σημεία που επιτρέπουν τον συμβιβασμό τους με μια επίθεση drive-by-download. Στη συνέχεια, περιμένουν ένα από τα προοριζόμενα θύματά τους να επισκεφθούν έναν από τους παραβιασμένους ιστότοπους. Ο κωδικός επίθεσής τους μπορεί ακόμη και να γραφτεί έτσι ώστε να μολύνει μόνο συστήματα που ανήκουν στον οργανισμό-στόχο και να μην προβεί σε καμία ενέργεια για άλλους επισκέπτες στον ιστότοπο. Αυτό αυξάνει σημαντικά την πιθανότητα παραβίασης του συμβιβασμού του ιστότοπου.

Η κακόβουλη διαφήμιση είναι μια άλλη τεχνική που χρησιμοποιείται για την τοποθέτηση κακόβουλου λογισμικού σε ιστότοπους χωρίς να τα θέτει σε κίνδυνο [SYMA13]. Ο εισβολέας πληρώνει για διαφημίσεις που είναι πολύ πιθανό να τοποθετηθούν στους προβλεπόμενους ιστότοπους προορισμού τους και στις οποίες ενσωματώνουν κακόβουλα προγράμματα. Χρησιμοποιώντας αυτές τις κακόβουλες προσθήκες, οι εισβολείς μπορούν να μολύνουν τους επισκέπτες σε ιστότοπους που τις εμφανίζουν. Και πάλι, ο κώδικας κακόβουλου λογισμικού

μπορεί να δημιουργηθεί δυναμικά είτε για τη μείωση της πιθανότητας εντοπισμού, είτε για μόλυνση συγκεκριμένων συστημάτων.

Οι σχετικές παραλλαγές μπορούν να εκμεταλλευτούν σφάλματα σε κοινούς πελάτες ηλεκτρονικού ταχυδρομείου, όπως το worm μαζικής αλληλογραφίας Klez που εμφανίστηκε τον Οκτώβριο του 2001, το οποίο στόχευσε ένα σφάλμα στο χειρισμό HTML στα προγράμματα Outlook και OutlookExpress της Microsoft για αυτόματη εκτέλεση. Εναλλακτικά, τέτοια κακόβουλα προγράμματα ενδέχεται να στοχεύουν σε κοινούς θεατές PDF να κάνουν λήψη και εγκατάσταση κακόβουλου λογισμικού χωρίς τη συγκατάθεση του χρήστη όταν βλέπουν ένα κακόβουλο έγγραφο PDF [STEV11]. Τέτοια έγγραφα μπορεί να εξαπλωθούν μέσω ανεπιθύμητου ηλεκτρονικού ταχυδρομείου ή να αποτελούν μέρος μιας στοχευμένης επίθεσης ηλεκτρονικού ψαρέματος (phishing), όπως συζητάμε στην επόμενη ενότητα.

Η) Clickjacking

Το Clickjacking, επίσης γνωστό ως επίθεση αποκατάστασης διεπαφής χρήστη (UI), είναι μια ευπάθεια που χρησιμοποιείται από έναν εισβολέα για τη συλλογή κλικ ενός μολυσμένου χρήστη. Ο εισβολέας μπορεί να αναγκάσει τον χρήστη να κάνει διάφορα πράγματα, από την προσαρμογή των ρυθμίσεων του υπολογιστή του χρήστη έως την ακούσια αποστολή του χρήστη σε τοποθεσίες Web που ενδέχεται να έχουν κακόβουλο κώδικα. Επίσης, εκμεταλλευόμενοι το AdobeFlash ή το JavaScript, ένας εισβολέας θα μπορούσε ακόμη και να τοποθετήσει ένα κουμπί κάτω από ή πάνω από ένα νόμιμο κουμπί, καθιστώντας δύσκολη την ανίχνευση των χρηστών. Μια τυπική επίθεση χρησιμοποιεί πολλαπλά διαφανή ή αδιαφανή στρώματα για να εξαπατήσει έναν χρήστη να κάνει κλικ σε ένα κουμπί ή να συνδεθεί σε μια άλλη σελίδα όταν σκοπεύει να κάνει κλικ στη σελίδα ανώτατου επιπέδου. Έτσι, ο εισβολέας εισβάλλει σε κλικ που προορίζονται για μία σελίδα και τα δρομολογεί σε άλλη σελίδα, που πιθανότατα ανήκει σε άλλη εφαρμογή, τομέα ή και τα δύο.

Χρησιμοποιώντας μια παρόμοια τεχνική, τα πλήκτρα μπορούν επίσης να παραβιαστούν. Με έναν προσεκτικά σχεδιασμένο συνδυασμό φύλλων στυλ, iframe και πλαισίων κειμένου, ένας χρήστης μπορεί να οδηγήσει να πιστέψει ότι πληκτρολογεί τον κωδικό πρόσβασης στο email ή

τον τραπεζικό λογαριασμό του, αλλά αντ 'αυτού πληκτρολογεί ένα αόρατο πλαίσιο που ελέγχεται από τον εισβολέα.

Υπάρχει μια μεγάλη ποικιλία τεχνικών για την επίθεση επίθεσης με κλικ, και αναπτύσσονται νέες τεχνικές καθώς εφαρμόζονται άμυνες σε παλαιότερες τεχνικές. [NIEM11] και [STON10] είναι χρήσιμες συζητήσεις.

2.5. Διάδοση – ΚοινωνικήΜηχανική - ΑνεπιθύμηταΜηνύματαΗλεκτρονικούΤαχυδρομείου, ΔούρειοςΊππος (TrojanHorse – Trojans)

Η τελική κατηγορία διάδοσης κακόβουλου λογισμικού που θεωρούμε αφορά την κοινωνική μηχανική, την «εξαπάτηση» των χρηστών για βοήθεια στον συμβιβασμό των δικών τους συστημάτων ή προσωπικών πληροφοριών. Αυτό μπορεί να συμβεί όταν ένας χρήστης προβάλλει και αποκρίνεται σε κάποιο SPAMe-mail ή επιτρέπει την εγκατάσταση και εκτέλεση κάποιου Trojanhorse προγράμματος ή κώδικα δέσμης ενεργειών.

Α) Ηλεκτρονικό ταχυδρομείο ανεπιθύμητων μηνυμάτων

Με την εκρηκτική ανάπτυξη του Διαδικτύου τις τελευταίες δεκαετίες, η ευρεία χρήση του e-mail και το εξαιρετικά χαμηλό κόστος που απαιτείται για την αποστολή μεγάλου όγκου e-mail, έχει προκύψει η αύξηση των ανεπιθύμητων μαζικών e-mail, κοινώς γνωστών ως ανεπιθυμητηαλληλογραφια. Ορισμένες πρόσφατες εκτιμήσεις υποδηλώνουν ότι τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου ενδέχεται να αντιπροσωπεύουν το 90% ή περισσότερο του συνόλου των email που αποστέλλονται. Αυτό επιβάλλει σημαντικό κόστος τόσο στην υποδομή δικτύου που απαιτείται για την αναμετάδοση αυτής της κίνησης, όσο και στους χρήστες που πρέπει να φιλτράρουν τα νόμιμα e-mail τους από αυτήν την πλημμύρα. Σε απάντηση σε αυτήν την εκρηκτική ανάπτυξη, υπήρξε η εξίσου ταχεία ανάπτυξη της βιομηχανίας κατά των ανεπιθύμητων μηνυμάτων που παρέχει προϊόντα για τον εντοπισμό και το φιλτράρισμα ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου. Αυτό οδήγησε σε μια κούρσα όπλων μεταξύ των spammers που επινοούν τεχνικές για να γλιστρήσουν το περιεχόμενό τους και με τις προσπάθειες των υπερασπιστών να τους αποκλείσουν [KREI09]

Τα τελευταία χρόνια, ο όγκος των ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου έχει αρχίσει να μειώνεται. Ένας λόγος είναι η ταχεία ανάπτυξη επιθέσεων, συμπεριλαμβανομένου του spam, που διαδίδονται μέσω δικτύων κοινωνικών μέσων. Αυτό αντικατοπτρίζει την ταχεία ανάπτυξη στη χρήση αυτών των δικτύων, τα οποία αποτελούν μια νέα αρένα για να εκμεταλλευτούν οι επιτιθέμενοι [SYMA13].

Ενώ ορισμένα ανεπιθύμητα μηνύματα αποστέλλονται από νόμιμους διακομιστές αλληλογραφίας, τα πιο πρόσφατα ανεπιθύμητα μηνύματα αποστέλλονται από botnetsχρησιμοποιώντας παραβιασμένα συστήματα χρηστών. Ένα σημαντικό μέρος του περιεχομένου ανεπιθύμητων μηνυμάτων ηλεκτρονικού ταχυδρομείου είναι απλώς διαφήμιση, προσπαθώντας να πείσει τον παραλήπτη να αγοράσει κάποιο προϊόν στο Διαδίκτυο, όπως φαρμακευτικά προϊόντα ή να χρησιμοποιηθεί σε απάτες, όπως απάτες μετοχών ή διαφημίσεις για δουλειά μου. Αλλά το spam είναι επίσης ένας σημαντικός φορέας κακόβουλου λογισμικού. Το ηλεκτρονικό ταχυδρομείο μπορεί να έχει συνημμένο έγγραφο, το οποίο, εάν ανοίξει, μπορεί να εκμεταλλευτεί μια ευπάθεια λογισμικού για την εγκατάσταση κακόβουλου λογισμικού στο σύστημα του χρήστη, όπως συζητήσαμε στην προηγούμενη ενότητα. Εναλλακτικά, μπορεί να έχει ένα συνημμένο πρόγραμμα Trojanhorse ή κώδικα δέσμης ενεργειών που, εάν εκτελείται, εγκαθιστά επίσης κακόβουλο λογισμικό στο σύστημα του χρήστη. Μερικοί Trojans αποφεύγουν την ανάγκη για συμφωνία χρήστη εκμεταλλευόμενοι μια ευπάθεια λογισμικού για να εγκατασταθούν, όπως συζητάμε στη συνέχεια. Τέλος, το ανεπιθύμητο περιεχόμενο μπορεί να χρησιμοποιηθεί σε μια επίθεση ηλεκτρονικού ψαρέματος (phishing), κατευθύνοντας συνήθως τον χρήστη είτε σε έναν ψεύτικο ιστότοπο που αντικατοπτρίζει κάποια νόμιμη υπηρεσία, όπως μια διαδικτυακή τοποθεσία τραπεζικής, όπου επιχειρεί να καταγράψει τα στοιχεία σύνδεσης και κωδικού πρόσβασης του χρήστη ή για να συμπληρώσετε κάποια φόρμα με επαρκή προσωπικά στοιχεία για να επιτρέψετε στον εισβολέα να πλαστοπροσωπεί τον χρήστη σε κλοπή ταυτότητας. Όλες αυτές οι χρήσεις καθιστούν τα ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου σημαντική ανησυχία για την ασφάλεια. Ωστόσο, σε πολλές περιπτώσεις, απαιτεί την ενεργή επιλογή του χρήστη να δει το ηλεκτρονικό ταχυδρομείο και οποιοδήποτε συνημμένο έγγραφο ή να επιτρέψει την εγκατάσταση κάποιου προγράμματος, προκειμένου να συμβεί ο συμβιβασμός.

Β) ΔούρειοςΊππος (Trojan Horse – Trojans)

Ένα Trojanhorse είναι ένα χρήσιμο, ή προφανώς χρήσιμο, πρόγραμμα ή βοηθητικό πρόγραμμα που περιέχει κρυφό κώδικα που, όταν καλείται, εκτελεί κάποια ανεπιθύμητη ή επιβλαβή λειτουργία.

Trojanhorse προγράμματα μπορούν να χρησιμοποιηθούν για την εκτέλεση λειτουργιών έμμεσα που ο εισβολέας δεν μπορούσε να επιτύχει άμεσα. Για παράδειγμα, για να αποκτήσετε πρόσβαση σε ευαίσθητα, προσωπικά στοιχεία που είναι αποθηκευμένα στα αρχεία ενός χρήστη, ένας εισβολέας θα μπορούσε να δημιουργήσει ένα πρόγραμμα Δούρειου ίππου που, όταν εκτελείται, σαρώνει τα αρχεία του χρήστη για τις επιθυμητές ευαίσθητες πληροφορίες και στέλνει ένα αντίγραφο αυτών στον εισβολέα. μέσω φόρμας Web ή e-mail ή γραπτού μηνύματος. Ο συγγραφέας θα μπορούσε στη συνέχεια να προσελκύσει τους χρήστες να εκτελέσουν το πρόγραμμα ενσωματώνοντάς το σε ένα παιχνίδι ή ένα χρήσιμο πρόγραμμα βοηθητικών προγραμμάτων και καθιστώντας το διαθέσιμο μέσω ενός γνωστού ιστότοπου διανομής λογισμικού ή ενός καταστήματος εφαρμογών. Αυτή η προσέγγιση χρησιμοποιήθηκε πρόσφατα με βοηθητικά προγράμματα που "ισχυρίζονται" ότι είναι ο τελευταίος ανιχνευτής προστασίας από ιούς ή ενημέρωση ασφαλείας, για συστήματα, αλλά στην πραγματικότητα είναι κακόβουλα Trojans, που συχνά μεταφέρουν ωφέλιμα φορτία όπως spyware που αναζητούν τραπεζικά διαπιστευτήρια. Ως εκ τούτου, οι χρήστες πρέπει να λάβουν προφυλάξεις για να επικυρώσουν την πηγή οποιουδήποτε λογισμικού που εγκαθιστούν.

Οι Δούρειοι Ίπποι ταιριάζουν σε ένα από τα τρία μοντέλα:

- Συνεχίζοντας να εκτελείτε τη λειτουργία του αρχικού προγράμματος και επιπλέον να εκτελείτε μια ξεχωριστή κακόβουλη δραστηριότητα.
- Συνέχιση της εκτέλεσης της λειτουργίας του αρχικού προγράμματος αλλά τροποποίηση της λειτουργίας για εκτέλεση κακόβουλης δραστηριότητας (π.χ., μια έκδοση Trojanhorse ενός προγράμματος σύνδεσης που συλλέγει κωδικούς πρόσβασης) ή για τη μεταμφίεση άλλης κακόβουλης δραστηριότητας (π.χ., μια έκδοση Trojanhorse μιας λίστας διαδικασίας πρόγραμμα που δεν εμφανίζει συγκεκριμένες διαδικασίες που είναι κακόβουλες).
- Εκτέλεση κακόβουλης λειτουργίας που αντικαθιστά πλήρως τη λειτουργία του αρχικού προγράμματος.

Μερικοί Trojans αποφεύγουν την απαίτηση για βοήθεια από τους χρήστες εκμεταλλευόμενοι κάποια ευπάθεια λογισμικού για να επιτρέψουν την αυτόματη εγκατάσταση και εκτέλεση τους. Σε αυτό μοιράζονται ορισμένα χαρακτηριστικά ενός σκουλήκι, αλλά σε αντίθεση με αυτό, δεν αναπαράγονται. Ένα σημαντικό παράδειγμα μιας τέτοιας επίθεσης ήταν το HydraqTrojan που χρησιμοποιήθηκε στην Επιχείρηση Aurora το 2009 και στις αρχές του 2010. Αυτό εκμεταλλεύτηκε μια ευπάθεια στον InternetExplorer για εγκατάσταση, και στοχεύει αρκετές εταιρείες υψηλού προφίλ [SYMA13]. Διανεμήθηκε συνήθως χρησιμοποιώντας είτε ανεπιθύμητο e-mail είτε μέσω ενός συμβιβασμένου ιστότοπου χρησιμοποιώντας μια επίθεση "watering-hole".

Γ) Trojans κινητού τηλεφώνου

Το κινητό τηλέφωνο Trojans εμφανίστηκε επίσης για πρώτη φορά το 2004 με την ανακάλυψη του Skuller. Όπως και με τα κινητά worms, ο στόχος είναι το smartphone και οι πρώτοι Trojans για κινητά στοχεύουν σε Symbian τηλέφωνα. Πιο πρόσφατα, ένας σημαντικός αριθμός Trojan έχουν εντοπιστεί που στοχεύουν τηλέφωνα Android και iPhone της Apple. Αυτά τα Trojans διανέμονται συνήθως μέσω ενός ή περισσοτέρων από τις αγορές εφαρμογών για το τηλέφωνο προορισμού O / S.

Το 2011, η Google κατάργησε έναν αριθμό εφαρμογών από το AndroidMarket που ήταν Trojans που περιείχαν κακόβουλο λογισμικό DroidDream. Αυτός είναι ένας ισχυρός πράκτορας ζόμπι που εκμεταλλεύτηκε τρωτά σημεία σε ορισμένες εκδόσεις του Android που χρησιμοποιούνται αυτήν τη στιγμή για να αποκτήσει πλήρη πρόσβαση στο σύστημα για την παρακολούθηση δεδομένων και την εγκατάσταση επιπλέον κώδικα. Ωστόσο, αυτή είναι μία από τις 49 οικογένειες κακόβουλου λογισμικού Android που αναλύθηκαν στο [ZHOU12]. Έλεγξαν πάνω από 1200 δείγματα κακόβουλου λογισμικού που βρέθηκαν σε διάφορες αγορές Android και σημείωσαν ότι το 90% αυτών είχε ως αποτέλεσμα την προσθήκη του παραβιασμένου τηλεφώνου σε ένα botnet, συχνά με υποστήριξη για πρόσβαση σε υπηρεσίες premium ή για τη συλλογή πληροφοριών χρήστη. Σημείωσαν επίσης ότι κανένα από τα κινητά προϊόντα κατά των ιών που εξέτασαν δεν μπόρεσε να εντοπίσει όλες αυτές τις οικογένειες. Ως εκ τούτου, απαιτείται περαιτέρω ανάπτυξη αυτών των προϊόντων, ειδικά δεδομένης της ταχείας εξέλιξης αυτής της κατηγορίας κακόβουλου λογισμικού.

Οι αυστηρότεροι έλεγχοι που επιβάλλει η Apple στο κατάστημα εφαρμογών τους, σημαίνει ότι τα περισσότερα iPhoneTrojans που φαίνεται να στοχεύουν μέχρι σήμερα τηλέφωνα «σπασμένα με φυλακή» και διανέμονται μέσω ανεπίσημων ιστότοπων. Ωστόσο, ορισμένες εκδόσεις του iPhoneO / S περιείχαν κάποια μορφή ευπάθειας γραφικών ή PDF. Πράγματι, αυτά τα τρωτά σημεία ήταν τα κύρια μέσα που χρησιμοποιήθηκαν για να «σπάσουν τις φυλακές» των τηλεφώνων. Αλλά παρείχαν επίσης μια διαδρομή που θα μπορούσε να χρησιμοποιήσει το κακόβουλο λογισμικό για να στοχεύσει τα τηλέφωνα. Ενώ η Apple έχει διορθώσει ορισμένες από αυτές τις ευπάθειες, συνέχισαν να ανακαλύπτονται νέες παραλλαγές. Αυτή είναι μια ακόμη εικόνα για το πόσο δύσκολο είναι, ακόμη και για οργανισμούς με καλή πηγή, να γράφουν ασφαλές λογισμικό σε ένα περίπλοκο σύστημα, όπως ένα λειτουργικό σύστημα.

2.6. Ωφέλιμο Φορτίο – Διαφθορά Συστήματος

Μόλις το κακόβουλο λογισμικό είναι ενεργό στο σύστημα προορισμού, η επόμενη ανησυχία είναι ποιες ενέργειες θα κάνει σε αυτό το σύστημα. Δηλαδή, τι μεταφέρει το ωφέλιμο φορτίο. Ορισμένα κακόβουλα προγράμματα έχουν ανύπαρκτο ή μη λειτουργικό ωφέλιμο φορτίο. Ο μόνος σκοπός του, είτε εσκεμμένος είτε λόγω τυχαίας πρόωρης απελευθέρωσης, είναι να εξαπλωθεί. Συνήθως, μεταφέρει ένα ή περισσότερα ωφέλιμα φορτία που εκτελούν κρυφές ενέργειες για τον εισβολέα.

Ένα πρώιμο ωφέλιμο φορτίο που παρατηρήθηκε σε διάφορους ιούς και σκουλήκια είχε ως αποτέλεσμα την καταστροφή δεδομένων στο μολυσμένο σύστημα όταν πληρούνται ορισμένες συνθήκες ενεργοποίησης [WEAV03]. Ένα σχετικό ωφέλιμο φορτίο είναι αυτό που εμφανίζει ανεπιθύμητα μηνύματα ή περιεχόμενο στο σύστημα του χρήστη όταν ενεργοποιείται. Πιο σοβαρά, μια άλλη παραλλαγή προσπαθεί να προκαλέσει ζημιά στον πραγματικό κόσμο στο σύστημα. Όλες αυτές οι ενέργειες στοχεύουν στην ακεραιότητα του λογισμικού ή του υλικού του συστήματος του υπολογιστή ή των δεδομένων του χρήστη. Αυτές οι αλλαγές ενδέχεται να μην πραγματοποιηθούν αμέσως, αλλά μόνο όταν πληρούνται συγκεκριμένες συνθήκες ενεργοποίησης που ικανοποιούν τον κώδικα λογικής-βόμβας.

Α) Καταστροφή Δεδομένων

Ο ιός του Τσερνομπίλ είναι ένα πρώιμο παράδειγμα ενός καταστροφικού ιού Windows-95 και 98 που παραμένει στην παρασιτική μνήμη, το οποίο εμφανίστηκε για πρώτη φορά το 1998. Μολύνει τα εκτελέσιμα αρχεία όταν ανοίγουν. Και όταν επιτευχθεί μια ημερομηνία ενεργοποίησης, διαγράφει δεδομένα για το μολυσμένο σύστημα αντικαθιστώντας τα πρώτα megabyte του σκληρού δίσκου με μηδενικά, με αποτέλεσμα μαζική καταστροφή ολόκληρου του συστήματος αρχείων. Αυτό συνέβη για πρώτη φορά στις 26 Απριλίου 1999, όταν οι εκτιμήσεις δείχνουν ότι επηρεάστηκαν περισσότεροι από ένα εκατομμύριο υπολογιστές.

Ομοίως, το σκουλήκι μαζικής αποστολής Klez είναι ένα πρώιμο παράδειγμα ενός καταστροφικού σκουλήκι που μολύνει τα συστήματα Windows-95 σε XP και εμφανίστηκε για πρώτη φορά τον Οκτώβριο του 2001. Διαδίδεται μέσω e-mail αντίγραφά του σε διευθύνσεις που βρίσκονται στο βιβλίο διευθύνσεων και στο αρχεία στο σύστημα. Μπορεί να σταματήσει και να διαγράψει ορισμένα προγράμματα προστασίας από ιούς που εκτελούνται στο σύστημα. Στις ημερομηνίες ενεργοποίησης, που είναι η 13η των αρκετών μηνών κάθε χρόνο, προκαλεί άδεια στα αρχεία του τοπικού σκληρού δίσκου.

Ως εναλλακτική λύση στην απλή καταστροφή δεδομένων, ορισμένα κακόβουλα προγράμματα κρυπτογραφούν τα δεδομένα του χρήστη και απαιτούν πληρωμή προκειμένου να αποκτήσουν πρόσβαση στο κλειδί που απαιτείται για την ανάκτηση αυτών των πληροφοριών. Αυτό είναι μερικές φορές γνωστό ως ransomware. Το PCCyborgTrojan που εμφανίστηκε το 1989 ήταν ένα πρώιμο παράδειγμα αυτού. Ωστόσο, γύρω στα μέσα του 2006, εμφανίστηκαν ορισμένα worms και Trojans, όπως το GpcodeTrojan, που χρησιμοποίησαν κρυπτογραφία δημόσιου κλειδιού με όλο και μεγαλύτερα μεγέθη κλειδιών για την κρυπτογράφηση δεδομένων. Ο χρήστης έπρεπε να πληρώσει λύτρα ή να πραγματοποιήσει μια αγορά από συγκεκριμένους ιστότοπους, προκειμένου να λάβει το κλειδί για την αποκρυπτογράφηση αυτών των δεδομένων. Ενώ οι προηγούμενες περιπτώσεις χρησιμοποίησαν ασθενέστερη κρυπτογραφία που θα μπορούσε να σπάσει χωρίς να πληρώσει τα λύτρα, οι νεότερες εκδόσεις που χρησιμοποιούν κρυπτογραφία δημόσιου κλειδιού με μεγάλα μεγέθη κλειδιών δεν θα μπορούσαν να σπάσουν με αυτόν τον τρόπο. [SYMA13] σημειώνει ότι το ransomware είναι μια αυξανόμενη πρόκληση, συχνά διαδίδεται μέσω του "drive-by-downloads".

Β) Ζημία στον πραγματικό κόσμο

Μια άλλη παραλλαγή των ωφέλιμων φορτίων διαφθοράς στοχεύει να προκαλέσει ζημιά σε φυσικό εξοπλισμό. Το μολυσμένο σύστημα είναι σαφώς η πιο εύκολα στοχευμένη συσκευή. Ο ιός του Τσερνομπίλ που αναφέρθηκε παραπάνω όχι μόνο καταστρέφει τα δεδομένα, αλλά προσπαθεί να ξαναγράψει τον κωδικό BIOS που χρησιμοποιήθηκε για την αρχική εκκίνηση του υπολογιστή. Εάν είναι επιτυχής, η διαδικασία εκκίνησης αποτυγχάνει και το σύστημα δεν μπορεί να χρησιμοποιηθεί έως ότου το τσιπ BIOSεπαναπρογραμματιστεί ή αντικατασταθεί. Πιο πρόσφατα, το wormStuxnet που συζητήσαμε προηγουμένως στοχεύει σε κάποιο συγκεκριμένο λογισμικό βιομηχανικού συστήματος ελέγχου ως βασικό ωφέλιμο φορτίο του [CHEN11, KUSH13]. Εάν μολυνθούν συστήματα ελέγχου που χρησιμοποιούν συγκεκριμένο λογισμικό βιομηχανικού ελέγχου της Siemens με συγκεκριμένη διαμόρφωση συσκευών, τότε το σκουλήκι αντικαθιστά τον αρχικό κωδικό ελέγχου με κωδικό που οδηγεί σκόπιμα τον ελεγχόμενο εξοπλισμό εκτός του κανονικού εύρους λειτουργίας του, με αποτέλεσμα την αποτυχία του συνδεδεμένου εξοπλισμού. Οι φυγοκεντρητές που χρησιμοποιήθηκαν στο πρόγραμμα εμπλουτισμού του ιρανικού ουρανίου υποψιάστηκαν έντονα ως στόχο, με αναφορές πολύ υψηλότερες από τις κανονικές τιμές αστοχίας που παρατηρήθηκαν σε αυτά κατά την περίοδο κατά την οποία ήταν ενεργός αυτός ο σκουλήκι. Όπως σημειώθηκε στην προηγούμενη συζήτησή μας, αυτό έχει εγείρει ανησυχίες σχετικά με τη χρήση εξελιγμένου στοχευμένου κακόβουλου λογισμικού για βιομηχανικά σαμποτάζ.

Γ) Λογική Βόμβα (LogicBomb)

Ένα βασικό συστατικό του κακόβουλου λογισμικού που καταστρέφει τα δεδομένα είναι η λογική βόμβα. Η λογική βόμβα είναι κωδικός ενσωματωμένος στο κακόβουλο λογισμικό που έχει οριστεί να «εκραγεί» όταν πληρούνται ορισμένες προϋποθέσεις. Παραδείγματα συνθηκών που μπορούν να χρησιμοποιηθούν ως ενεργοποιητές για μια λογική βόμβα είναι η παρουσία ή απουσία ορισμένων αρχείων ή συσκευών στο σύστημα, μια συγκεκριμένη ημέρα της εβδομάδας ή την ημερομηνία, μια συγκεκριμένη έκδοση ή διαμόρφωση κάποιου λογισμικού ή μια συγκεκριμένη λειτουργία του χρήστη η εφαρμογή. Μόλις ενεργοποιηθεί, μια βόμβα μπορεί να αλλάξει ή να διαγράψει δεδομένα ή ολόκληρα αρχεία, να προκαλέσει διακοπή του μηχανήματος ή να προκαλέσει κάποια άλλη ζημιά.

Ένα εντυπωσιακό παράδειγμα του πώς μπορούν να χρησιμοποιηθούν οι λογικές βόμβες ήταν η περίπτωση του TimLloyd, ο οποίος καταδικάστηκε για τη δημιουργία μιας λογικής βόμβας που κόστισε στον εργοδότη του, την OmegaEngineering, πάνω από 10 εκατομμύρια δολάρια, εκτροχιάστηκε τη στρατηγική της εταιρικής ανάπτυξης και τελικά οδήγησε στην απόλυση 80 εργαζομένων [GAUD00]. Τελικά, ο Λόιντ καταδικάστηκε σε φυλάκιση 41 μηνών και διέταξε να πληρώσει 2 εκατομμύρια δολάρια σε αποζημίωση.

2.7. ΩφέλιμοΦορτίο – ΕπιθέσειςDDoS – Zombies, Bots

Η επόμενη κατηγορία ωφέλιμου φορτίου που συζητάμε είναι όπου το κακόβουλο λογισμικό ανατρέπει τους υπολογιστικούς πόρους και τους πόρους δικτύου του μολυσμένου συστήματος για χρήση από τον εισβολέα. Ένα τέτοιο σύστημα είναι γνωστό ως bot (ρομπότ), ζόμπι ή drone, και αποκτά κρυφά έναν άλλο συνδεδεμένο στο Διαδίκτυο υπολογιστή και στη συνέχεια χρησιμοποιεί αυτόν τον υπολογιστή για να ξεκινήσει ή να διαχειριστεί επιθέσεις που είναι δύσκολο να εντοπιστούν στον δημιουργό του bot. Το bot συνήθως φυτεύεται σε εκατοντάδες ή χιλιάδες υπολογιστές που ανήκουν σε ανυποψίαστους τρίτους. Η συλλογή των bots είναι συχνά ικανή να ενεργεί με συντονισμένο τρόπο. μια τέτοια συλλογή αναφέρεται ως botnet. Αυτός ο τύπος ωφέλιμου φορτίου επιτίθεται στην ακεραιότητα και τη διαθεσιμότητα του μολυσμένου συστήματος.

Α) Χρήσεις τωνBots

[HONE05] παραθέτει τις ακόλουθες χρήσεις των bots:

- Κατανεμημένες επιθέσεις άρνησης υπηρεσίας (DDoS): Μια επίθεση DDoS είναι μια επίθεση σε ένα σύστημα υπολογιστή ή δίκτυο που προκαλεί απώλεια υπηρεσίας στους χρήστες. Εξετάζουμε τις επιθέσεις DDoS στο Κεφάλαιο 7.
- Spamming: Με τη βοήθεια ενός botnet και χιλιάδων bots, ένας εισβολέας μπορεί να στείλει τεράστια ποσά μαζικών e-mail (spam).
- Sniffingtraffic: Τα bots μπορούν επίσης να χρησιμοποιήσουν ένα πακέτο sniffer για να παρακολουθήσουν ενδιαφέροντα δεδομένα cleartext που περνούν από έναν παραβιασμένο υπολογιστή. Τα sniffers χρησιμοποιούνται κυρίως για την ανάκτηση ευαίσθητων πληροφοριών όπως ονόματα χρήστη και κωδικούς πρόσβασης.
- Keylogging: Εάν το μηχάνημα που έχει παραβιαστεί χρησιμοποιεί κρυπτογραφημένα κανάλια επικοινωνίας (π.χ. HTTPS ή POP3S), τότε απλώς η εισπνοή των πακέτων δικτύου στον υπολογιστή του θύματος είναι άχρηστο επειδή λείπει το κατάλληλο κλειδί για την αποκρυπτογράφηση των πακέτων. Αλλά χρησιμοποιώντας ένα keylogger, το οποίο καταγράφει πατήματα πλήκτρων στο μολυσμένο μηχάνημα, ένας εισβολέας μπορεί να ανακτήσει ευαίσθητες πληροφορίες.
- Διάδοση νέου κακόβουλου λογισμικού: Τα botnets χρησιμοποιούνται για τη διάδοση νέων bots. Αυτό είναι πολύ εύκολο καθώς όλα τα bots εφαρμόζουν μηχανισμούς για λήψη και εκτέλεση ενός αρχείου μέσω HTTP ή FTP. Ένα botnet με 10.000 κεντρικούς υπολογιστές που λειτουργεί ως βάση εκκίνησης για έναν ιό worm ή mail επιτρέπει πολύ γρήγορη εξάπλωση και συνεπώς προκαλεί περισσότερη βλάβη.
- Εγκατάσταση πρόσθετων διαφημίσεων και αντικειμένων βοηθού προγράμματος περιήγησης (BHO): Μπορούν επίσης να χρησιμοποιηθούν botnets για την απόκτηση οικονομικών πλεονεκτημάτων. Αυτό λειτουργεί δημιουργώντας έναν ψεύτικο ιστότοπο με ορισμένες διαφημίσεις: Ο χειριστής αυτού του ιστότοπου διαπραγματεύεται μια συμφωνία με ορισμένες εταιρείες φιλοξενίας που πληρώνουν για κλικ σε διαφημίσεις. Με τη βοήθεια ενός botnet, αυτά τα κλικ μπορούν να «αυτοματοποιηθούν» έτσι ώστε αμέσως μερικές χιλιάδες bot να κάνουν κλικ στα αναδυόμενα παράθυρα. Αυτή η διαδικασία μπορεί να βελτιωθεί περαιτέρω εάν το bot παραβιάζει την αρχική σελίδα ενός παραβιασμένου μηχανήματος, έτσι ώστε τα «κλικ» να εκτελούνται κάθε φορά που το θύμα χρησιμοποιεί το πρόγραμμα περιήγησης.

- Επίθεση σε δίκτυα συνομιλίας IRC: Τα botnets χρησιμοποιούνται επίσης για επιθέσεις σε δίκτυα InternetRelayChat (IRC). Δημοφιλές στους επιτιθέμενους είναι ιδιαίτερα η επίθεση κλώνου: Σε αυτό το είδος επίθεσης, ο ελεγκτής διατάζει κάθε bot να συνδέσει μεγάλο αριθμό κλώνων στο δίκτυο IRC του θύματος. Το θύμα πλημμυρίζεται από αιτήματα υπηρεσίας από χιλιάδες ρομπότ ή χιλιάδες κανάλια από αυτά τα κλωνοποιημένα ρομπότ. Με αυτόν τον τρόπο, το δίκτυο IRC του θύματος κατεβαίνει, παρόμοιο με μια επίθεση DDoS.
- Χειρισμός διαδικτυακών δημοσκοπήσεων / παιχνιδιών: Οι διαδικτυακές δημοσκοπήσεις / παιχνίδια προσελκύουν όλο και περισσότερη προσοχή και είναι μάλλον εύκολο να τα χειριστείτε με botnets. Δεδομένου ότι κάθε bot έχει μια ξεχωριστή διεύθυνση IP, κάθε ψήφος θα έχει την ίδια αξιοπιστία με την ψήφο ενός πραγματικού ατόμου. Τα διαδικτυακά παιχνίδια μπορούν να χρησιμοποιηθούν με παρόμοιοτρόπο.

Β) Εγκατάσταση τηλεχειρισμού

Η εγκατάσταση του τηλεχειριστηρίου είναι αυτό που διακρίνει ένα bot από ένα σκουλήκι. Ένα worm διαδίδεται και ενεργοποιείται, ενώ ένα bot ελέγχεται από κάποια μορφή δικτύου διακομιστών εντολών και ελέγχου (C&C). Αυτή η επαφή δεν χρειάζεται να είναι συνεχής, αλλά μπορεί να ξεκινά περιοδικά όταν το bot παρατηρεί ότι έχει πρόσβαση στο δίκτυο.

Ένα πρώιμο μέσο εφαρμογής της εγκατάστασης τηλεχειριστηρίου χρησιμοποίησε έναν διακομιστή IRC. Όλα τα bots συμμετέχουν σε ένα συγκεκριμένο κανάλι σε αυτόν τον διακομιστή και αντιμετωπίζουν τα εισερχόμενα μηνύματα ως εντολές. Τα πιο πρόσφατα botnets τείνουν να αποφεύγουν τους μηχανισμούς IRC και να χρησιμοποιούν κρυφά κανάλια επικοινωνίας μέσω πρωτοκόλλων όπως το HTTP. Χρησιμοποιούνται επίσης κατανεμημένοι μηχανισμοί ελέγχου, χρησιμοποιώντας πρωτόκολλα peer-to-peer, για την αποφυγή ενός μόνο σημείου αποτυχίας.

Αρχικά αυτοί οι διακομιστές C&C χρησιμοποίησαν σταθερές διευθύνσεις, πράγμα που σήμαινε ότι θα μπορούσαν να εντοπιστούν και ενδεχομένως να αναληφθούν ή να καταργηθούν από τις υπηρεσίες επιβολής του νόμου. Μερικές πιο πρόσφατες οικογένειες κακόβουλου

λογισμικού έχουν χρησιμοποιήσει τεχνικές όπως η αυτόματη δημιουργία πολύ μεγάλων αριθμών ονομάτων τομέα διακομιστή με τα οποία θα προσπαθήσει να επικοινωνήσει το κακόβουλο λογισμικό. Εάν ένα όνομα διακομιστή έχει παραβιαστεί, οι εισβολείς μπορούν να ρυθμίσουν έναν νέο διακομιστή με άλλο όνομα που γνωρίζουν ότι θα δοκιμαστεί. Για να το νικήσουμε αυτό απαιτείται από τους αναλυτές ασφαλείας να αναστρέψουν τον αλγόριθμο δημιουργίας ονομάτων και στη συνέχεια να προσπαθήσουν να αποκτήσουν τον έλεγχο όλων των εξαιρετικά μεγάλων αριθμών πιθανών τομέων. Μια άλλη τεχνική που χρησιμοποιείται για την απόκρυψη των διακομιστών είναι το fast-fluxDNS, όπου η διεύθυνση που σχετίζεται με ένα δεδομένο όνομα διακομιστή αλλάζει συχνά, συχνά κάθε λίγα λεπτά, για να περιστρέφεται πάνω από ένα μεγάλο αριθμό διακομιστών μεσολάβησης, συνήθως άλλων μελών του botnet. Τέτοιες προσεγγίσεις εμποδίζουν τις προσπάθειες των υπηρεσιών επιβολής του νόμου να ανταποκριθούν στην απειλή botnet.

Μόλις δημιουργηθεί μια διαδρομή επικοινωνίας μεταξύ μιας μονάδας ελέγχου και των bots, η μονάδα ελέγχου μπορεί να διαχειριστεί τα bots. Στην απλούστερη μορφή του, η μονάδα ελέγχου εκδίδει απλώς εντολή στο bot που κάνει το bot να εκτελεί ρουτίνες που έχουν ήδη εφαρμοστεί στο bot. Για μεγαλύτερη ευελιξία, η μονάδα ελέγχου μπορεί να εκδώσει εντολές ενημέρωσης που δίνουν εντολή στα bot να κατεβάσουν ένα αρχείο από κάποια τοποθεσία στο Διαδίκτυο και να το εκτελέσουν. Το bot σε αυτήν την τελευταία περίπτωση γίνεται ένα πιο γενικό εργαλείο που μπορεί να χρησιμοποιηθεί για πολλαπλές επιθέσεις. Η ηλεκτρονική μονάδα ελέγχου μπορεί επίσης να συλλέξει πληροφορίες που συλλέγονται από τα bots που μπορεί στη συνέχεια να εκμεταλλευτεί ο εισβολέας.

2.8. ΩφέλιμοΦορτίο – ΚλοπήΠληροφοριών – Keyloggers, Phising, Spyware

Εξετάζουμε τώρα τα ωφέλιμα φορτία όπου το κακόβουλο λογισμικό συλλέγει δεδομένα που είναι αποθηκευμένα στο μολυσμένο σύστημα για χρήση από τον εισβολέα. Ένας κοινός στόχος είναι τα διαπιστευτήρια σύνδεσης και κωδικού πρόσβασης του χρήστη σε τραπεζικά, τυχερά παιχνίδια και συναφείς ιστότοπους, τα οποία στη συνέχεια χρησιμοποιεί ο εισβολέας για να πλαστοπροσωπήσει τον χρήστη για πρόσβαση σε αυτούς τους ιστότοπους για κέρδος. Λιγότερο συχνά, το ωφέλιμο φορτίο μπορεί να στοχεύει έγγραφα ή λεπτομέρειες διαμόρφωσης

συστήματος για λόγους αναγνώρισης ή κατασκοπείας. Αυτές οι επιθέσεις στοχεύουν στην εμπιστευτικότητα αυτών των πληροφοριών.

Α) Κλοπή διαπιστευτηρίων, Keyloggers και Spyware

Συνήθως, οι χρήστες αποστέλλουν τα διαπιστευτήρια σύνδεσης και κωδικού πρόσβασης σε τραπεζικά, τυχερά παιχνίδια και σχετικούς ιστότοπους μέσω κρυπτογραφημένων καναλιών επικοινωνίας (π.χ. HTTPS ή POP3S), τα οποία τους προστατεύουν από τη λήψη μέσω παρακολούθησης πακέτων δικτύου. Για να παρακάμψει αυτό, ένας εισβολέας μπορεί να εγκαταστήσει ένα πληκτρολόγιο, το οποίο καταγράφει πατήματα πλήκτρων στο μολυσμένο μηχάνημα για να επιτρέψει σε έναν εισβολέα να παρακολουθεί αυτές τις ευαίσθητες πληροφορίες. Δεδομένου ότι αυτό θα είχε ως αποτέλεσμα ο εισβολέας να λάβει ένα αντίγραφο όλου του κειμένου που έχει εισαχθεί στον υπολογιστή που έχει παραβιαστεί, οι keyloggers συνήθως εφαρμόζουν κάποια μορφή μηχανισμού φιλτραρίσματος που επιστρέφει μόνο πληροφορίες κοντά στις επιθυμητές λέξεις-κλειδιά (π.χ. «σύνδεση» ή «κωδικός πρόσβασης» ή «paypal.com) ").

Σε απάντηση στη χρήση των keyloggers, ορισμένοι τραπεζικοί και άλλοι ιστότοποι άλλαξαν τη χρήση γραφικής μικροεφαρμογής για την εισαγωγή κρίσιμων πληροφοριών, όπως κωδικών πρόσβασης. Δεδομένου ότι αυτά δεν χρησιμοποιούν κείμενο που εισάγεται μέσω του πληκτρολογίου, τα παραδοσιακά πληκτρολόγια δεν συλλαμβάνουν αυτές τις πληροφορίες. Σε απάντηση, οι επιτιθέμενοι ανέπτυξαν γενικότερα ωφέλιμα φορτία spyware, τα οποία ανατρέπουν τον παραβιασμένο υπολογιστή για να επιτρέπουν την παρακολούθηση ενός ευρέος φάσματος δραστηριοτήτων στο σύστημα. Αυτό μπορεί να περιλαμβάνει παρακολούθηση του ιστορικού και του περιεχομένου της δραστηριότητας περιήγησης, ανακατεύθυνση συγκεκριμένων αιτημάτων ιστοσελίδας σε πλαστούς ιστότοπους που ελέγχονται από τον εισβολέα και δυναμική τροποποίηση δεδομένων που ανταλλάσσονται μεταξύ του προγράμματος περιήγησης και συγκεκριμένων ιστότοπων που ενδιαφέρουν. Όλα αυτά μπορούν να οδηγήσουν σε σημαντικό συμβιβασμό των προσωπικών στοιχείων του χρήστη.

Το ZeusbankingTrojan, που δημιουργήθηκε από την εργαλειοθήκη crimeware, είναι ένα εξέχον παράδειγμα τέτοιου λογισμικού υποκλοπής spyware που έχει αναπτυχθεί ευρέως τα

τελευταία χρόνια [BINS10]. Κλέβει τραπεζικά και οικονομικά διαπιστευτήρια χρησιμοποιώντας ένα keylogger και καταγράφει και πιθανώς αλλάζει δεδομένα φόρμας για συγκεκριμένους ιστότοπους. Συνήθως αναπτύσσεται χρησιμοποιώντας ανεπιθύμητα μηνύματα ηλεκτρονικού ταχυδρομείου ή μέσω ενός συμβιβασμένου ιστότοπου στο "drive-by-download".

Β) Ηλεκτρονικό ψάρεμα (Phising) και κλοπή ταυτότητας

Μια άλλη προσέγγιση που χρησιμοποιείται για την καταγραφή των διαπιστευτηρίων σύνδεσης και κωδικού πρόσβασης ενός χρήστη είναι η συμπερίληψη μιας διεύθυνσης URL σε ένα ανεπιθύμητο ηλεκτρονικό ταχυδρομείο που συνδέεται με έναν ψεύτικο ιστότοπο που ελέγχεται από τον εισβολέα, αλλά μιμείται τη σελίδα σύνδεσης ορισμένων τραπεζικών, παιχνιδιών ή παρόμοιων ιστότοπων. Αυτό συνήθως περιλαμβάνεται σε κάποιο μήνυμα που υποδηλώνει ότι απαιτείται από τον χρήστη επείγουσα ενέργεια για τον έλεγχο ταυτότητας του λογαριασμού του, για να αποφευχθεί ο αποκλεισμός του. Εάν ο χρήστης είναι απρόσεκτος και δεν συνειδητοποιήσει ότι παραβιάζεται, τότε ακολουθώντας τον σύνδεσμο και παρέχοντας τις ζητούμενες λεπτομέρειες σίγουρα θα έχει ως αποτέλεσμα οι εισβολείς να εκμεταλλευτούν το λογαριασμό τους χρησιμοποιώντας τα καταγεγραμμένα διαπιστευτήρια.

Γενικότερα, ένα τέτοιο ανεπιθύμητο e-mail μπορεί να κατευθύνει έναν χρήστη σε μια πλαστή τοποθεσία Web που ελέγχεται από τον εισβολέα, ή να συμπληρώσει κάποια εσωκλειόμενη φόρμα και να επιστρέψει σε ένα e-mailπροσβάσιμο από τον εισβολέα, το οποίο χρησιμοποιείται για τη συλλογή ιδιωτικών , προσωπικές, πληροφορίες για τον χρήστη. Δεδομένων επαρκών λεπτομερειών, ο εισβολέας μπορεί στη συνέχεια να "αναλάβει" την ταυτότητα του χρήστη με σκοπό την απόκτηση πίστωσης ή ευαίσθητη πρόσβαση σε άλλους πόρους. Αυτό είναι γνωστό ως επίθεση ηλεκτρονικού ψαρέματος (phishing) και εκμεταλλεύεται την κοινωνική μηχανική για να αξιοποιήσει την εμπιστοσύνη των χρηστών μεταμφιέζοντας ως επικοινωνίες από μια αξιόπιστη πηγή [GOLD10].

Τέτοια γενικά ανεπιθύμητα e-mail συνήθως διανέμονται ευρέως σε πολύ μεγάλο αριθμό χρηστών, συχνά μέσω botnet. Παρόλο που το περιεχόμενο δεν θα ταιριάζει με τις κατάλληλες αξιόπιστες πηγές για ένα σημαντικό μέρος των παραληπτών, οι εισβολείς βασίζονται σε αυτό,

προσεγγίζοντας επαρκείς χρήστες της ονομασμένης αξιόπιστης πηγής, ένα ευχάριστο τμήμα του οποίου θα ανταποκριθεί, ώστε να είναι κερδοφόρο.

Μια πιο επικίνδυνη παραλλαγή αυτού είναι η επίθεση ψαρέματος-ψαρέματος. Και πάλι αυτό είναι ένα e-mail που ισχυρίζεται ότι προέρχεται από αξιόπιστη πηγή. Ωστόσο, οι παραλήπτες ερευνούνται προσεκτικά από τον εισβολέα και κάθε ηλεκτρονικό ταχυδρομείο είναι προσεκτικά σχεδιασμένο ώστε να ταιριάζει ειδικά στον παραλήπτη του, αναφέροντας συχνά μια σειρά πληροφοριών για να τους πείσει για την αυθεντικότητά του. Αυτό αυξάνει σημαντικά την πιθανότητα του παραλήπτη να ανταποκριθεί όπως επιθυμεί ο εισβολέας. Αυτός ο τύπος επίθεσης χρησιμοποιείται ιδιαίτερα σε βιομηχανικές και άλλες μορφές κατασκοπείας από οργανισμούς με καλή πηγή [SYMA13].

Γ) Αναγνώριση, κατασκοπεία και αποβολή δεδομένων

Η κλοπή διαπιστευτηρίων και η κλοπή ταυτότητας είναι ειδικές περιπτώσεις ενός γενικότερου ωφέλιμου φορτίου αναγνώρισης, το οποίο στοχεύει στη λήψη συγκεκριμένων τύπων επιθυμητών πληροφοριών και την επιστροφή τους στον εισβολέα. Αυτές οι ειδικές περιπτώσεις είναι σίγουρα οι πιο κοινές. Ωστόσο, είναι γνωστοί άλλοι στόχοι. Η επιχείρηση Aurora το 2009 χρησιμοποίησε ένα Trojan για να αποκτήσει πρόσβαση και ενδεχομένως να τροποποιήσει τα αποθετήρια πηγαίου κώδικα σε μια σειρά εταιρειών υψηλής τεχνολογίας, ασφάλειας και άμυνας [SYMA13]. Το Stuxnetworm που ανακαλύφθηκε το 2010 περιελάμβανε τη σύλληψη λεπτομερειών διαμόρφωσης υλικού και λογισμικού για να προσδιοριστεί εάν είχε θέσει σε κίνδυνο τα συγκεκριμένα επιθυμητά συστήματα στόχου. Οι πρώτες εκδόσεις αυτού του worm επέστρεψαν τις ίδιες πληροφορίες, οι οποίες στη συνέχεια χρησιμοποιήθηκαν για την ανάπτυξη των επιθέσεων που αναπτύχθηκαν σε μεταγενέστερες εκδόσεις [CHEN11, KUSH13].

Οι επιθέσεις APT μπορεί να οδηγήσουν στην απώλεια μεγάλου όγκου ευαίσθητων πληροφοριών, οι οποίες αποστέλλονται, αποβάλλονται από τον οργανισμό-στόχο, στους επιτιθέμενους. Για την ανίχνευση και τον αποκλεισμό τέτοιων δεδομένων, απαιτείται η κατάλληλη τεχνική αντίληψη «απώλειας δεδομένων» που διαχειρίζεται είτε την πρόσβαση σε αυτές τις πληροφορίες είτε τη μετάδοσή της μέσω της περιμέτρου δικτύου του οργανισμού.

2.9. ΩφέλιμοΦορτίο – ΚρυφήΚλοπή (Stealthing) – Backdoors, Rootkits

Η τελική κατηγορία ωφέλιμου φορτίου που συζητάμε αφορά τεχνικές που χρησιμοποιούνται από κακόβουλο λογισμικό για την απόκρυψη της παρουσίας του στο μολυσμένο σύστημα και για την παροχή μυστικής πρόσβασης σε αυτό το σύστημα. Αυτός ο τύπος ωφέλιμου φορτίου επιτίθεται επίσης στην ακεραιότητα του μολυσμένου συστήματος.

A) Backdoors

Ένα backdoor, επίσης γνωστό ως trapdoor, είναι ένα μυστικό σημείο εισόδου σε ένα πρόγραμμα που επιτρέπει σε κάποιον που γνωρίζει την πόρτα να αποκτήσει πρόσβαση χωρίς να περάσει από τις συνήθεις διαδικασίες πρόσβασης ασφαλείας. Οι προγραμματιστές έχουν χρησιμοποιήσει νόμιμα backdoors για πολλά χρόνια για να εντοπίσουν σφάλματα και να δοκιμάσουν προγράμματα. μια τέτοια πίσω πόρτα ονομάζεται γάντζος συντήρησης. Αυτό γίνεται συνήθως όταν ο προγραμματιστής αναπτύσσει μια εφαρμογή που έχει μια διαδικασία ελέγχου ταυτότητας ή μια μακρά ρύθμιση, που απαιτεί από τον χρήστη να εισαγάγει πολλές διαφορετικές τιμές για την εκτέλεση της εφαρμογής. Για τον εντοπισμό σφαλμάτων του προγράμματος, ο προγραμματιστής μπορεί να επιθυμεί να αποκτήσει ειδικά προνόμια ή να αποφύγει όλες τις απαραίτητες ρυθμίσεις και έλεγχο ταυτότητας. Ο προγραμματιστής μπορεί επίσης να θέλει να διασφαλίσει ότι υπάρχει μια μέθοδος ενεργοποίησης του προγράμματος σε περίπτωση που κάτι δεν πάει καλά με τη διαδικασία ελέγχου ταυτότητας που ενσωματώνεται στην εφαρμογή. Η πίσω πόρτα είναι κώδικας που αναγνωρίζει κάποια ειδική ακολουθία εισόδου ή ενεργοποιείται από την εκτέλεση από ένα συγκεκριμένο αναγνωριστικό χρήστη ή από μια απίθανη ακολουθία συμβάντων.

Οι υπαίθριοι χώροι γίνονται απειλές όταν οι αδίστακτοι προγραμματιστές τα χρησιμοποιούν για να αποκτήσουν μη εξουσιοδοτημένη πρόσβαση. Το backdoor ήταν η βασική ιδέα για την ευπάθεια που απεικονίζεται στην ταινία WarGames. Ένα άλλο παράδειγμα είναι ότι κατά την ανάπτυξη του Multics, διενεργήθηκαν δοκιμές διείσδυσης από μια «ομάδα τίγρης» της Πολεμικής Αεροπορίας (προσομοίωση αντιπάλων). Μια τακτική που χρησιμοποιήθηκε ήταν να στείλετε μια ψευδή ενημέρωση του λειτουργικού συστήματος σε έναν ιστότοπο που εκτελεί Multics. Η ενημέρωση περιείχε ένα Δούρειο άλογο που θα μπορούσε να ενεργοποιηθεί από μια πίσω πόρτα και που επέτρεψε στην ομάδα τίγρης να αποκτήσει πρόσβαση. Η απειλή

εφαρμόστηκε τόσο καλά που οι προγραμματιστές Multics δεν μπορούσαν να τη βρουν, ακόμα και αφού ενημερώθηκαν για την παρουσία της [ENGE80].

Τις πιο πρόσφατες φορές, ένα backdoor συνήθως εφαρμόζεται ως υπηρεσία δικτύου που ακούει σε κάποια μη τυπική θύρα στην οποία ο εισβολέας μπορεί να συνδεθεί και να εκδώσει εντολές για να εκτελεστεί στο παραβιασμένο σύστημα.

Είναι δύσκολο να εφαρμοστούν χειριστήρια λειτουργικού συστήματος για backdoors σε εφαρμογές. Τα μέτρα ασφαλείας πρέπει να εστιάζονται στην ανάπτυξη προγραμμάτων και στις δραστηριότητες ενημέρωσης λογισμικού και σε προγράμματα που επιθυμούν να προσφέρουν μια υπηρεσία δικτύου.

B) Rootkits

Το rootkit είναι ένα σύνολο προγραμμάτων που είναι εγκατεστημένα σε ένα σύστημα για τη διατήρηση της μυστικής πρόσβασης σε αυτό το σύστημα με δικαιώματα διαχειριστή (ή root) 3, ενώ κρύβεται η απόδειξη της παρουσίας του στο μεγαλύτερο δυνατό βαθμό. Αυτό παρέχει πρόσβαση σε όλες τις λειτουργίες και τις υπηρεσίες του λειτουργικού συστήματος. Το rootkit τροποποιεί την τυπική λειτουργία του κεντρικού υπολογιστή με κακόβουλο και κρυφό τρόπο. Με πρόσβαση root, ένας εισβολέας έχει τον πλήρη έλεγχο του συστήματος και μπορεί να προσθέσει ή να αλλάξει προγράμματα και αρχεία, να παρακολουθεί τις διαδικασίες, να στέλνει και να λαμβάνει κίνηση στο δίκτυο και να έχει πρόσβαση στο backdoor κατόπιν αιτήματος.

Ένα rootkit μπορεί να κάνει πολλές αλλαγές σε ένα σύστημα για να κρύψει την ύπαρξή του, καθιστώντας δύσκολο για τον χρήστη να προσδιορίσει ότι το rootkit είναι παρόν και να εντοπίσει ποιες αλλαγές έχουν γίνει. Στην ουσία, ένα rootkit κρύβεται ανατρέποντας τους μηχανισμούς που παρακολουθούν και αναφέρουν τις διαδικασίες, τα αρχεία και τα μητρώα σε έναν υπολογιστή.

Ένα rootkit μπορεί να ταξινομηθεί χρησιμοποιώντας τα ακόλουθα χαρακτηριστικά:

- Μόνιμο: Ενεργοποιείται κάθε φορά που ξεκινά το σύστημα. Το rootkit πρέπει να αποθηκεύει κώδικα σε ένα μόνιμο κατάστημα, όπως το μητρώο ή το σύστημα αρχείων, και να διαμορφώνει μια μέθοδο με την οποία εκτελείται ο κώδικας χωρίς

παρέμβαση του χρήστη. Αυτό σημαίνει ότι είναι ευκολότερο να εντοπιστεί, καθώς μπορεί να σαρωθεί το αντίγραφο σε μόνιμη αποθήκευση.

- Βάση μνήμης: Δεν έχει επίμονο κώδικα και ως εκ τούτου δεν μπορεί να επιβιώσει από την επανεκκίνηση. Ωστόσο, επειδή είναι μόνο στη μνήμη, μπορεί να είναι πιο δύσκολο να εντοπιστεί.
- Λειτουργία χρήστη: Παρεμποδίζει κλήσεις σε API (διεπαφές προγράμματος εφαρμογής) και τροποποιεί τα αποτελέσματα που επιστρέφονται. Για παράδειγμα, όταν μια εφαρμογή εκτελεί μια λίστα καταλόγων, τα αποτελέσματα επιστροφής δεν περιλαμβάνουν καταχωρήσεις που προσδιορίζουν τα αρχεία που σχετίζονται με το rootkit.
- Λειτουργία πυρήνα: Μπορεί να παρακολουθεί κλήσεις σε εγγενή API σε λειτουργία πυρήνα. Το rootkit μπορεί επίσης να αποκρύψει την παρουσία μιας διαδικασίας κακόβουλου λογισμικού αφαιρώντας την από τη λίστα ενεργών διεργασιών του πυρήνα.
- Βασική εικονική μηχανή: Αυτός ο τύπος rootkit εγκαθιστά μια ελαφριά οθόνη εικονικής μηχανής και, στη συνέχεια, εκτελεί το λειτουργικό σύστημα σε μια εικονική μηχανή πάνω από αυτήν. Το rootkit μπορεί στη συνέχεια να παρακολουθεί με διαφάνεια και να τροποποιεί καταστάσεις και συμβάντα που συμβαίνουν στο εικονικοποιημένο σύστημα.
- Εξωτερική λειτουργία: Το κακόβουλο λογισμικό βρίσκεται εκτός του κανονικού τρόπου λειτουργίας του στοχευμένου συστήματος, σε λειτουργία BIOS ή διαχείρισης συστήματος, όπου μπορεί να έχει άμεση πρόσβαση σε υλικό.

Αυτή η ταξινόμηση δείχνει μια συνεχιζόμενη κούρσα όπλων μεταξύ των συγγραφέων rootkit, οι οποίοι εκμεταλλεύονται όλο και πιο κρυφά μηχανισμούς για να κρύψουν τον κώδικά τους, και εκείνους που αναπτύσσουν μηχανισμούς για να σκληρύνουν τα συστήματα ενάντια σε μια τέτοια ανατροπή ή για να εντοπίσουν πότε έχει συμβεί. Μεγάλο μέρος αυτής της προόδου σχετίζεται με την εύρεση μορφών επίθεσης «κάτω-κάτω». Τα πρώτα rootkits δούλεψαν σε λειτουργία χρήστη, τροποποιώντας βοηθητικά προγράμματα και βιβλιοθήκες για να

αποκρύψουν την παρουσία τους. Οι αλλαγές που πραγματοποίησαν μπορούσαν να εντοπιστούν με κωδικό στον πυρήνα, καθώς αυτό λειτουργούσε στο επίπεδο κάτω από τον χρήστη.

Γ) KernelModeRootkits

Η επόμενη γενιά rootkits μετακίνησε ένα επίπεδο, κάνοντας αλλαγές στον πυρήνα και συνυπάρχει με τον κώδικα των λειτουργικών συστημάτων, προκειμένου να κάνει την ανίχνευσή τους πολύ πιο δύσκολη. Κάθε πρόγραμμα «anti-virus» θα υπόκειται πλέον στις ίδιες τροποποιήσεις «χαμηλού επιπέδου» που χρησιμοποιεί το rootkit για να αποκρύψει την παρουσία του. Ωστόσο, αναπτύχθηκαν μέθοδοι για τον εντοπισμό αυτών των αλλαγών.

Τα προγράμματα που λειτουργούν σε επίπεδο χρήστη αλληλεπιδρούν με τον πυρήνα μέσω κλήσεων συστήματος. Έτσι, οι κλήσεις συστήματος είναι πρωταρχικός στόχος rootkit σε επίπεδο πυρήνα για την επίτευξη απόκρυψης. Ως παράδειγμα του τρόπου λειτουργίας των rootkit, εξετάζουμε την εφαρμογή των κλήσεων συστήματος στο Linux. Στο Linux, σε κάθε κλήση συστήματος εκχωρείται ένας μοναδικός αριθμός syscall. Όταν μια διαδικασία λειτουργίας χρήστη εκτελεί μια κλήση συστήματος, η διαδικασία αναφέρεται στην κλήση συστήματος με αυτόν τον αριθμό. Ο πυρήνας διατηρεί έναν πίνακα κλήσεων συστήματος με μία καταχώρηση ανά ρουτίνα κλήσεων συστήματος. κάθε καταχώρηση περιέχει ένα δείκτη στην αντίστοιχη ρουτίνα. Ο αριθμός syscall χρησιμεύει ως ευρετήριο στον πίνακα κλήσεων συστήματος.

[LEVI06] παραθέτει τρεις τεχνικές που μπορούν να χρησιμοποιηθούν για την αλλαγή κλήσεων συστήματος:

- ✓ Τροποποίηση του πίνακα κλήσεων συστήματος: Ο εισβολέας τροποποιεί επιλεγμένες διευθύνσεις syscall που είναι αποθηκευμένες στον πίνακα κλήσεων συστήματος. Αυτό επιτρέπει στο rootkit να κατευθύνει μια κλήση συστήματος από τη νόμιμη ρουτίνα στην αντικατάσταση του rootkit. Το σχήμα 6.4 δείχνει πώς το επιτυγχάνει αυτό το κιτ rootkit.
- ✓ Τροποποίηση στόχων πίνακα κλήσεων συστήματος: Ο εισβολέας αντικαθιστά επιλεγμένες νόμιμες ρουτίνες κλήσεων συστήματος με κακόβουλο κώδικα. Ο πίνακας κλήσεων συστήματος δεν αλλάζει.

- ✓ Ανακατεύθυνση του πίνακα κλήσεων συστήματος: Ο εισβολέας ανακατευθύνει τις αναφορές σε ολόκληρο τον πίνακα κλήσεων συστήματος σε έναν νέο πίνακα σε μια νέα θέση μνήμης πυρήνα.

Δ) Εικονική μηχανή και άλλα εξωτερικά Rootkits

Η τελευταία γενιά rootkit χρησιμοποιεί κώδικα που είναι εντελώς αόρατο στο στοχευμένο λειτουργικό σύστημα. Αυτό μπορεί να γίνει χρησιμοποιώντας μια αδίστακτη ή παραβιασμένη οθόνη εικονικής μηχανής ή έναν επόπτη, που συχνά υποστηρίζεται από την υποστήριξη εικονικοποίησης υλικού που παρέχεται σε πρόσφατους επεξεργαστές. Στη συνέχεια, ο κώδικας rootkit εκτελείται εντελώς κάτω από την ορατότητα ομοιόμορφου κώδικα πυρήνα στο στοχευμένο λειτουργικό σύστημα, το οποίο τώρα εκτελείται άγνωστα σε μια εικονική μηχανή και μπορεί να παρακολουθείται σιωπηλά και να δέχεται επίθεση από τον παρακάτω κώδικα [SKAP07].

Πολλά πρωτότυπα των εικονικοποιημένωνrootkits επιδείχθηκαν το 2006. Το SubVirt επιτέθηκε σε συστήματα Windows που λειτουργούν είτε με εικονικούς υπολογιστές της Microsoft είτε με VMwareWorkstationhypervisors τροποποιώντας τη διαδικασία εκκίνησης που χρησιμοποίησαν. Αυτές οι αλλαγές κατέστησαν δυνατή την ανίχνευση της παρουσίας του rootkit.

Ωστόσο, το rootkit του BluePill μπόρεσε να ανατρέψει ένα εγγενές σύστημα WindowsVista εγκαθιστώντας ένα λεπτό hypervisor κάτω από αυτό και στη συνέχεια συνεχίζοντας απρόσκοπτα την εκτέλεση του συστήματος Vista σε μια εικονική μηχανή. Καθώς απαιτούσε μόνο την εκτέλεση ενός αδίστακτου προγράμματος οδήγησης από τον πυρήνα Vista, αυτό το rootkit θα μπορούσε να εγκατασταθεί όταν εκτελούσε το στοχευμένο σύστημα και είναι πολύ πιο δύσκολο να εντοπιστεί. Αυτός ο τύπος rootkit αποτελεί ιδιαίτερη απειλή για συστήματα που λειτουργούν σε σύγχρονους επεξεργαστές με υποστήριξη εικονικοποίησης υλικού, αλλά όπου δεν χρησιμοποιείται υπεύθυνος.

Άλλες παραλλαγές εκμεταλλεύονται τη Λειτουργία διαχείρισης συστήματος σε επεξεργαστές Intel που χρησιμοποιείται για έλεγχο υλικού χαμηλού επιπέδου ή τον κωδικό BIOS που χρησιμοποιείται κατά την πρώτη εκκίνηση του επεξεργαστή. Ένας τέτοιος κώδικας έχει άμεση πρόσβαση σε συνδεδεμένες συσκευές υλικού και είναι γενικά αόρατος στον κώδικα που εκτελείται εκτός αυτών των ειδικών λειτουργιών [EMBL08]. Για την άμυνα έναντι αυτών των τύπων rootkits, ολόκληρη η διαδικασία εκκίνησης πρέπει να είναι ασφαλής, διασφαλίζοντας ότι το λειτουργικό σύστημα έχει φορτωθεί και ασφαλιστεί από την εγκατάσταση αυτών των τύπων κακόβουλου κώδικα. Αυτό πρέπει να περιλαμβάνει παρακολούθηση της φόρτωσης οποιουδήποτε κώδικα υπεύθυνου για να διασφαλιστεί ότι είναι νόμιμος.

2.10. Αντίμετρα

Εξετάζουμε τώρα πιθανά αντίμετρα για κακόβουλο λογισμικό. Αυτοί είναι γενικά γνωστοί ως «αντι-ιικοί» μηχανισμοί, καθώς αναπτύχθηκαν για να στοχεύουν συγκεκριμένα τις μολύνσεις από ιούς. Ωστόσο, έχουν εξελιχθεί για την αντιμετώπιση των περισσότερων τύπων κακόβουλου λογισμικού που συζητάμε σε αυτό το κεφάλαιο.

Α) Προσεγγίσεις αντιμετώπισης κακόβουλου λογισμικού

Η ιδανική λύση για την απειλή του κακόβουλου λογισμικού είναι η πρόληψη: Μην αφήνετε το κακόβουλο λογισμικό να εισέλθει αρχικά στο σύστημα ή να αποκλείσετε την ικανότητά του να τροποποιεί το σύστημα. Αυτός ο στόχος είναι, γενικά, σχεδόν αδύνατο να επιτευχθεί, αν και η λήψη κατάλληλων αντιμέτρων για τη σκλήρυνση των συστημάτων και των χρηστών στην πρόληψη της μόλυνσης μπορεί να μειώσει σημαντικά τον αριθμό των επιτυχημένων επιθέσεων κακόβουλου λογισμικού. [SOUP13] προτείνει ότι υπάρχουν τέσσερα κύρια στοιχεία πρόληψης: πολιτική, ευαισθητοποίηση, μετριασμός ευπάθειας και μετριασμός απειλών. Η ύπαρξη κατάλληλης πολιτικής για την αντιμετώπιση της πρόληψης κακόβουλου λογισμικού παρέχει τη βάση για την εφαρμογή κατάλληλων προληπτικών αντιμέτρων.

Η ιδανική λύση για την απειλή του κακόβουλου λογισμικού είναι η πρόληψη: Μην αφήνετε το κακόβουλο λογισμικό να εισέλθει αρχικά στο σύστημα ή να αποκλείσετε την ικανότητά του να τροποποιεί το σύστημα. Αυτός ο στόχος είναι, γενικά, σχεδόν αδύνατο να επιτευχθεί, αν και η λήψη κατάλληλων αντιμέτρων για τη σκλήρυνση των συστημάτων και των

χρηστών στην πρόληψη της μόλυνσης μπορεί να μειώσει σημαντικά τον αριθμό των επιτυχημένων επιθέσεων κακόβουλου λογισμικού. [SOUP13] προτείνει ότι υπάρχουν τέσσερα κύρια στοιχεία πρόληψης: πολιτική, ευαισθητοποίηση, μετριασμός ευπάθειας και μετριασμός απειλών. Η ύπαρξη κατάλληλης πολιτικής για την αντιμετώπιση της πρόληψης κακόβουλου λογισμικού παρέχει τη βάση για την εφαρμογή κατάλληλων προληπτικών αντιμέτρων.

Ένα από τα πρώτα αντίμετρα που πρέπει να εφαρμοστούν είναι να διασφαλιστεί ότι όλα τα συστήματα είναι όσο το δυνατόν πιο σύγχρονα, με όλες τις ενημερώσεις κώδικα που εφαρμόζονται, προκειμένου να μειωθεί ο αριθμός των τρωτών σημείων που ενδέχεται να αξιοποιηθούν στο σύστημα. Το επόμενο είναι να ορίσετε κατάλληλα στοιχεία ελέγχου πρόσβασης στις εφαρμογές και τα δεδομένα που είναι αποθηκευμένα στο σύστημα, για να μειώσετε τον αριθμό των αρχείων στα οποία μπορεί να έχει πρόσβαση οποιοσδήποτε χρήστης και, ως εκ τούτου, να μολύνει ή να καταστρέψει, ως αποτέλεσμα της εκτέλεσης κάποιου κώδικα κακόβουλου λογισμικού. Αυτά τα μέτρα στοχεύουν άμεσα τους βασικούς μηχανισμούς διάδοσης που χρησιμοποιούνται από σκουλήκια, ιούς και ορισμένους Τρώες. Ο τρίτος κοινός μηχανισμός διάδοσης, που στοχεύει τους χρήστες σε μια επίθεση κοινωνικής μηχανικής, μπορεί να αντιμετωπιστεί χρησιμοποιώντας την κατάλληλη ευαισθητοποίηση και εκπαίδευση των χρηστών. Αυτό έχει ως στόχο να εξοπλίσει τους χρήστες να γνωρίζουν περισσότερο αυτές τις επιθέσεις και λιγότερο πιθανό να αναλάβουν ενέργειες που οδηγούν σε συμβιβασμό. Το [SOUP13] παρέχει παραδείγματα κατάλληλων θεμάτων ευαισθητοποίησης.

Εάν η πρόληψη αποτύχει, τότε μπορούν να χρησιμοποιηθούν τεχνικοί μηχανισμοί για την υποστήριξη των ακόλουθων επιλογών μετριασμού των απειλών:

- ✓ Ανίχνευση: Μόλις εμφανιστεί η μόλυνση, προσδιορίστε ότι έχει συμβεί και εντοπίστε το κακόβουλο λογισμικό.
- ✓ Αναγνώριση: Μόλις επιτευχθεί η ανίχνευση, εντοπίστε το συγκεκριμένο κακόβουλο λογισμικό που έχει μολύνει το σύστημα.
- ✓ Αφαίρεση: Μόλις εντοπιστεί το συγκεκριμένο κακόβουλο λογισμικό, αφαιρέστε όλα τα ίχνη ιού κακόβουλου λογισμικού από όλα τα μολυσμένα συστήματα, ώστε να μην μπορεί να εξαπλωθεί περαιτέρω.

Εάν η ανίχνευση επιτύχει, αλλά δεν είναι δυνατή η αναγνώριση ή η αφαίρεση, τότε η εναλλακτική λύση είναι να απορρίψετε τυχόν μολυσμένα ή κακόβουλα αρχεία και να φορτώσετε

εκ νέου μια καθαρή έκδοση αντιγράφου ασφαλείας. Στην περίπτωση ορισμένων ιδιαίτερα δυσάρεστων λοιμώξεων, αυτό μπορεί να απαιτεί πλήρη σκούπισμα όλης της αποθήκευσης και ανοικοδόμηση του μολυσμένου συστήματος από γνωστά καθαρά μέσα.

Αρχικά, ας εξετάσουμε ορισμένες απαιτήσεις για αποτελεσματικά αντίμετρα κακόβουλου λογισμικού:

- Γενικότητα: Η προσέγγιση που ακολουθεί πρέπει να είναι σε θέση να χειριστεί μια μεγάλη ποικιλία επιθέσεων.
- Επικαιρότητα: Η προσέγγιση πρέπει να ανταποκρίνεται γρήγορα έτσι ώστε να περιορίζεται ο αριθμός των μολυσμένων προγραμμάτων ή συστημάτων και η συνακόλουθη δραστηριότητα.
- Ανθεκτικότητα: Η προσέγγιση πρέπει να είναι ανθεκτική στις τεχνικές διαφυγής που χρησιμοποιούν οι εισβολείς για να κρύψουν την παρουσία του κακόβουλου λογισμικού τους.
- Ελάχιστο κόστος άρνησης υπηρεσίας: Η προσέγγιση θα πρέπει να έχει ως αποτέλεσμα την ελάχιστη μείωση της χωρητικότητας ή της υπηρεσίας λόγω των ενεργειών του λογισμικού αντιμέτρων και δεν θα πρέπει να διαταράξει σημαντικά την κανονική λειτουργία.
- Διαφάνεια: Το λογισμικό και οι συσκευές αντιμέτρων δεν πρέπει να απαιτούν τροποποίηση σε υπάρχοντα (παλαιού τύπου) λειτουργικά συστήματα, λογισμικό εφαρμογών και υλικό.
- Παγκόσμια και τοπική κάλυψη: Η προσέγγιση πρέπει να είναι σε θέση να αντιμετωπίσει τις πηγές επιθέσεων τόσο από το εξωτερικό όσο και από το εταιρικό δίκτυο.

Η επίτευξη όλων αυτών των απαιτήσεων συχνά απαιτεί τη χρήση πολλαπλών προσεγγίσεων, σε μια στρατηγική άμυνας σε βάθος.

Η ανίχνευση της παρουσίας κακόβουλου λογισμικού μπορεί να συμβεί σε διάφορες τοποθεσίες. Μπορεί να συμβεί στο μολυσμένο σύστημα, όπου εκτελείται κάποιο πρόγραμμα "anti-virus" που βασίζεται σε κεντρικό υπολογιστή, παρακολουθώντας δεδομένα που εισάγονται

στο σύστημα και την εκτέλεση και τη συμπεριφορά των προγραμμάτων που εκτελούνται στο σύστημα. Ή, μπορεί να πραγματοποιηθεί ως μέρος των περιμετρικών μηχανισμών ασφαλείας που χρησιμοποιούνται στα συστήματα εντοπισμού τείχους προστασίας και εισβολής (IDS) ενός οργανισμού. Τέλος, η ανίχνευση μπορεί να χρησιμοποιεί κατανεμημένους μηχανισμούς που συλλέγουν δεδομένα τόσο από αισθητήρες που βασίζονται σε κεντρικούς υπολογιστές όσο και από αισθητήρες περιμέτρου, ενδεχομένως μέσω μεγάλου αριθμού δικτύων και οργανισμών, προκειμένου να αποκτήσουν τη μεγαλύτερη προβολή της κίνησης του κακόβουλου λογισμικού. Εξετάζουμε τώρα καθεμία από αυτές τις προσεγγίσεις με περισσότερες λεπτομέρειες.

Β) Σαρωτές βάσει κεντρικού υπολογιστή

Η πρώτη τοποθεσία όπου χρησιμοποιείται λογισμικό προστασίας από ιούς είναι σε κάθε τελικό σύστημα. Αυτό δίνει στο λογισμικό τη μέγιστη πρόσβαση σε πληροφορίες όχι μόνο για τη συμπεριφορά του κακόβουλου λογισμικού καθώς αλληλεπιδρά με το στοχευμένο σύστημα, αλλά και για τη μικρότερη συνολική άποψη της δραστηριότητας κακόβουλου λογισμικού. Η χρήση λογισμικού προστασίας από ιούς σε προσωπικούς υπολογιστές είναι πλέον διαδεδομένη, εν μέρει λόγω της εκρηκτικής αύξησης του όγκου και της δραστηριότητας κακόβουλου λογισμικού. Αυτό το λογισμικό μπορεί να θεωρηθεί ως μια μορφή συστήματος εντοπισμού εισβολής που βασίζεται σε κεντρικό υπολογιστή, το οποίο συζητάμε γενικότερα στην Ενότητα 8.4. Οι εξελίξεις στην τεχνολογία ιών και άλλων κακόβουλων προγραμμάτων, καθώς και στην τεχνολογία προστασίας από ιούς και άλλα αντίμετρα, συμβαδίζουν. Το πρώιμο κακόβουλο λογισμικό χρησιμοποίησε σχετικά απλό και εύκολα εντοπισμένο κώδικα, και ως εκ τούτου θα μπορούσε να αναγνωριστεί και να καθαριστεί με σχετικά απλά πακέτα λογισμικού προστασίας από ιούς. Καθώς η φυλή κακόβουλου λογισμικού έχει εξελιχθεί, τόσο ο κώδικας κακόβουλου λογισμικού όσο και, κατ 'ανάγκη, το λογισμικό προστασίας από ιούς έχει εξελιχθεί πιο περίπλοκο και εξελιγμένο.

[STEP93] προσδιορίζει τέσσερις γενιές λογισμικού προστασίας από ιούς:

- Πρώτη γενιά: απλοί σαρωτές
- Δεύτερη γενιά: ευρετικοί σαρωτές
- Τρίτη γενιά: παγίδες δραστηριότητας
- Τέταρτη γενιά: πλήρης προστασία

Ένας σαρωτής πρώτης γενιάς απαιτεί υπογραφή κακόβουλου λογισμικού για την αναγνώριση του κακόβουλου λογισμικού. Η υπογραφή μπορεί να περιέχει "μπαλαντέρ" αλλά ταιριάζει ουσιαστικά με την ίδια δομή και μοτίβο bit σε όλα τα αντίγραφα του κακόβουλου λογισμικού. Τέτοιοι σαρωτές ειδικής υπογραφής περιορίζονται στην ανίχνευση γνωστών κακόβουλων προγραμμάτων. Ένας άλλος τύπος σαρωτή πρώτης γενιάς διατηρεί αρχείο για τη διάρκεια των προγραμμάτων και αναζητά αλλαγές στο μήκος ως αποτέλεσμα λοίμωξης από ιούς.

Ένας σαρωτής δεύτερης γενιάς δεν βασίζεται σε συγκεκριμένη υπογραφή. Αντίθετα, ο σαρωτής χρησιμοποιεί ευρετικούς κανόνες για την αναζήτηση πιθανών παρουσιών κακόβουλου λογισμικού. Μια κατηγορία τέτοιων σαρωτών αναζητά τμήματα κώδικα που συχνά σχετίζονται με κακόβουλο λογισμικό. Για παράδειγμα, ένας σαρωτής μπορεί να αναζητήσει την αρχή ενός βρόχου κρυπτογράφησης που χρησιμοποιείται σε έναν πολυμορφικό ιό και να ανακαλύψει το κλειδί κρυπτογράφησης. Μόλις εντοπιστεί το κλειδί, ο σαρωτής μπορεί να αποκρυπτογραφήσει το κακόβουλο λογισμικό για να το εντοπίσει και, στη συνέχεια, να αφαιρέσει τη μόλυνση και να επιστρέψει το πρόγραμμα στην υπηρεσία.

Μια άλλη προσέγγιση δεύτερης γενιάς είναι ο έλεγχος ακεραιότητας. Ένα άθροισμα ελέγχου μπορεί να προσαρτηθεί σε κάθε πρόγραμμα. Εάν το κακόβουλο λογισμικό αλλάζει ή αντικαθιστά κάποιο πρόγραμμα χωρίς να αλλάξει το άθροισμα ελέγχου, τότε ένας έλεγχος ακεραιότητας θα εντοπίσει αυτήν την αλλαγή. Για την αντιμετώπιση κακόβουλου λογισμικού που είναι αρκετά εξελιγμένο για να αλλάξει το άθροισμα ελέγχου όταν αλλάζει ένα πρόγραμμα, μπορεί να χρησιμοποιηθεί μια κρυπτογραφημένη συνάρτηση κατακερματισμού. Το κλειδί κρυπτογράφησης αποθηκεύεται ξεχωριστά από το πρόγραμμα έτσι ώστε το κακόβουλο λογισμικό να μην μπορεί να δημιουργήσει νέο κωδικό κατακερματισμού και να το κρυπτογραφήσει. Χρησιμοποιώντας μια συνάρτηση κατακερματισμού και όχι απλούστερου αθροίσματος ελέγχου, το κακόβουλο λογισμικό αποτρέπεται από την προσαρμογή του προγράμματος ώστε να παράγει τον ίδιο κωδικό κατακερματισμού όπως πριν. Εάν διατηρηθεί μια προστατευμένη λίστα προγραμμάτων σε αξιόπιστες τοποθεσίες, αυτή η προσέγγιση μπορεί επίσης να εντοπίσει απόπειρες αντικατάστασης ή εγκατάστασης απατεώνου κώδικα ή προγραμμάτων σε αυτές τις τοποθεσίες.

Τα προγράμματα τρίτης γενιάς είναι προγράμματα που ζουν στη μνήμη και εντοπίζουν κακόβουλα προγράμματα από τις ενέργειές του και όχι τη δομή του σε ένα μολυσμένο πρόγραμμα. Τέτοια προγράμματα έχουν το πλεονέκτημα ότι δεν είναι απαραίτητο να αναπτυχθούν υπογραφές και ευρετικά για ένα ευρύ φάσμα κακόβουλου λογισμικού. Αντίθετα, είναι απαραίτητο μόνο να προσδιοριστεί το μικρό σύνολο ενεργειών που υποδεικνύουν ότι επιχειρείται κακόβουλη δραστηριότητα και στη συνέχεια να παρέμβει.

Τα προϊόντα τέταρτης γενιάς είναι πακέτα που αποτελούνται από μια ποικιλία τεχνικών κατά των ιών που χρησιμοποιούνται σε συνδυασμό. Αυτά περιλαμβάνουν στοιχεία σάρωσης και παγίδας δραστηριότητας. Επιπλέον, ένα τέτοιο πακέτο περιλαμβάνει δυνατότητα ελέγχου πρόσβασης, η οποία περιορίζει την ικανότητα του κακόβουλου λογισμικού να διεισδύει σε ένα σύστημα και στη συνέχεια περιορίζει τη δυνατότητα ενός κακόβουλου λογισμικού να ενημερώνει αρχεία προκειμένου να διαδώσει.

Ο αγώνας όπλων συνεχίζεται. Με τα πακέτα τέταρτης γενιάς, χρησιμοποιείται μια πιο περιεκτική στρατηγική άμυνας, διευρύνοντας το πεδίο της άμυνας σε πιο γενικά σκοπού μέτρα ασφαλείας υπολογιστών. Αυτές περιλαμβάνουν πιο εξελιγμένες προσεγγίσεις κατά των ιών. Τώρα επισημαίνουμε δύο από τα πιο σημαντικά.

Γ) Γενικήαποκρυπτογράφηση

Η τεχνολογία γενικής αποκρυπτογράφησης (GD) επιτρέπει στο πρόγραμμα προστασίας από ιούς να εντοπίζει εύκολα ακόμη και τους πιο πολύπλοκους πολυμορφικούς ιούς και άλλα κακόβουλα προγράμματα, διατηρώντας παράλληλα γρήγορες ταχύτητες σάρωσης [NACH97]. Θυμηθείτε ότι όταν εκτελείται ένα αρχείο που περιέχει έναν πολυμορφικό ιό, ο ιός πρέπει να αποκρυπτογραφηθεί για να ενεργοποιηθεί. Προκειμένου να εντοπιστεί μια τέτοια δομή, εκτελέσιμα αρχεία εκτελούνται μέσω ενός σαρωτή GD, ο οποίος περιέχει τα ακόλουθα στοιχεία:

- Εξομοιωτής CPU: Ένας εικονικός υπολογιστής που βασίζεται σε λογισμικό. Οι οδηγίες σε ένα εκτελέσιμο αρχείο ερμηνεύονται από τον εξομοιωτή αντί να εκτελούνται στον υποκείμενο επεξεργαστή. Ο εξομοιωτής περιλαμβάνει εκδόσεις λογισμικού όλων των καταχωρητών και άλλου υλικού επεξεργαστή, έτσι ώστε ο

υποκείμενος επεξεργαστής να μην επηρεάζεται από προγράμματα που ερμηνεύονται στον εξομοιωτή.

- Σαρωτής υπογραφής ιών: Μια λειτουργική μονάδα που σαρώνει τον κώδικα-στόχο αναζητώντας γνωστές υπογραφές κακόβουλου λογισμικού.
- Μονάδα ελέγχου προσομοίωσης: Ελέγχει την εκτέλεση του κώδικα στόχου.

Στην αρχή κάθε προσομοίωσης, ο εξομοιωτής αρχίζει να ερμηνεύει οδηγίες στον κώδικα προορισμού, μία κάθε φορά. Έτσι, εάν ο κώδικας περιλαμβάνει μια ρουτίνα αποκρυπτογράφησης που αποκρυπτογραφεί και ως εκ τούτου εκθέτει το κακόβουλο λογισμικό, αυτός ο κώδικας ερμηνεύεται. Στην πραγματικότητα, το κακόβουλο πρόγραμμα λειτουργεί για το πρόγραμμα προστασίας από ιούς εκθέτοντας τον εαυτό του. Περιοδικά, η μονάδα ελέγχου διακόπτει την ερμηνεία για να σαρώσει τον κώδικα προορισμού για υπογραφές κακόβουλου λογισμικού. Κατά τη διάρκεια της ερμηνείας, ο κωδικός στόχος δεν μπορεί να προκαλέσει ζημιά στο πραγματικό περιβάλλον του προσωπικού υπολογιστή, επειδή ερμηνεύεται σε ένα πλήρως ελεγχόμενο περιβάλλον. Το πιο δύσκολο πρόβλημα σχεδίασης με έναν σαρωτή GD είναι να καθοριστεί πόσο καιρό θα εκτελείται κάθε ερμηνεία. Συνήθως, τα στοιχεία κακόβουλου λογισμικού ενεργοποιούνται αμέσως μετά την έναρξη ενός προγράμματος, αλλά αυτό δεν ισχύει. Όσο περισσότερο ο σαρωτής εξομοιώνει ένα συγκεκριμένο πρόγραμμα, τόσο πιο πιθανό είναι να εντοπίσει οποιοδήποτε κρυφό κακόβουλο λογισμικό. Ωστόσο, το πρόγραμμα προστασίας από ιούς μπορεί να καταλάβει μόνο περιορισμένο χρόνο και πόρους προτού οι χρήστες παραπονούνται για υποβαθμισμένη απόδοση του συστήματος.

Δ) Λογισμικό αποκλεισμού συμπεριφοράς βάσει κεντρικού υπολογιστή

Σε αντίθεση με τους ευρετικούς ή σαρωτές βάσει δακτυλικών αποτυπωμάτων, το λογισμικό αποκλεισμού συμπεριφοράς ενσωματώνεται στο λειτουργικό σύστημα ενός κεντρικού υπολογιστή και παρακολουθεί τη συμπεριφορά του προγράμματος σε πραγματικό χρόνο για κακόβουλες ενέργειες [CONR02, NACH02]. Είναι ένας τύπος συστήματος πρόληψης εισβολής που βασίζεται σε κεντρικό υπολογιστή, το οποίο συζητάμε περαιτέρω στην Ενότητα 9.6. Το λογισμικό αποκλεισμού συμπεριφοράς στη συνέχεια αποκλείει δυνητικά κακόβουλες ενέργειες

προτού έχουν την ευκαιρία να επηρεάσουν το σύστημα. Οι ελεγχόμενες συμπεριφορές μπορούν να περιλαμβάνουν:

- Προσπάθειες ανοίγματος, προβολής, διαγραφής και / ή τροποποίησης αρχείων.
- Προσπάθειες για μορφοποίηση μονάδων δίσκου και άλλων λειτουργιών δίσκου που δεν μπορούν να ανακτηθούν.
- Τροποποιήσεις στη λογική των εκτελέσιμων αρχείων ή μακροεντολών
- Τροποποίηση κρίσιμων ρυθμίσεων συστήματος, όπως ρυθμίσεις εκκίνησης
- Σενάριο πελατών e-mail και άμεσων μηνυμάτων για αποστολή εκτελέσιμου περιεχομένου
- Έναρξη επικοινωνιώνδικτύου.

Επειδή ένας αποκλειστής συμπεριφοράς μπορεί να αποκλείσει ύποπτο λογισμικό σε πραγματικό χρόνο, έχει ένα πλεονέκτημα σε σχέση με τέτοιες καθιερωμένες τεχνικές ανίχνευσης ιών όπως το δακτυλικό αποτύπωμα ή το ευρετικό. Υπάρχουν κυριολεκτικά τρισεκατομμύρια διαφορετικοί τρόποι για να αποκρύψετε και να αναδιατάξετε τις οδηγίες ενός ιού ή ενός σκουλήκι, πολλοί από τους οποίους θα αποφύγουν την ανίχνευση από έναν σαρωτή δακτυλικών αποτυπωμάτων ή ευρετικό. Αλλά τελικά, κακόβουλος κώδικας πρέπει να υποβάλει ένα σαφώς καθορισμένο αίτημα στο λειτουργικό σύστημα. Δεδομένου ότι ο αποκλειστής συμπεριφοράς μπορεί να υποκλέψει όλα αυτά τα αιτήματα, μπορεί να εντοπίσει και να αποκλείσει κακόβουλες ενέργειες, ανεξάρτητα από το πόσο ασαφής φαίνεται η λογική του προγράμματος.

Ο αποκλεισμός συμπεριφοράς από μόνο του έχει περιορισμούς. Επειδή ο κακόβουλος κώδικας πρέπει να εκτελείται στο μηχάνημα προορισμού προτού εντοπιστούν όλες οι συμπεριφορές του, μπορεί να προκαλέσει βλάβη προτού εντοπιστεί και αποκλειστεί. Για παράδειγμα, ένα νέο στοιχείο κακόβουλου λογισμικού ενδέχεται να ανακατέψει ορισμένα φαινομενικά ασήμαντα αρχεία γύρω από τον σκληρό δίσκο πριν τροποποιήσετε ένα μόνο αρχείο και μπλοκαριστεί. Παρόλο που η πραγματική τροποποίηση αποκλείστηκε, ο χρήστης ενδέχεται να μην μπορεί να εντοπίσει τα αρχεία του, προκαλώντας απώλεια στην παραγωγικότητα ή πιθανώς χειρότερη.

Ε) Ανίχνευση και αφαίρεση spyware

Παρόλο που τα γενικά προϊόντα προστασίας από ιούς περιλαμβάνουν υπογραφές για την ανίχνευση spyware, η απειλή που δημιουργεί αυτός ο τύπος κακόβουλου λογισμικού και η χρήση τεχνικών stealthing, σημαίνει ότι υπάρχει μια σειρά ειδικών βοηθητικών προγραμμάτων εντοπισμού και αφαίρεσης spyware. Αυτά ειδικεύονται στην ανίχνευση και την αφαίρεση του spyware και παρέχουν πιο ισχυρές δυνατότητες. Έτσι, συμπληρώνουν και πρέπει να χρησιμοποιούνται μαζί με γενικότερα προϊόντα κατά των ιών.

ΣΤ) Αντιμετώπιση Rootkit

Τα ριζικά κιτ μπορεί να είναι εξαιρετικά δύσκολο να εντοπιστούν και να εξουδετερωθούν, ειδικά για τα rootkit σε επίπεδο πυρήνα. Πολλά από τα εργαλεία διαχείρισης που θα μπορούσαν να χρησιμοποιηθούν για την ανίχνευση ενός rootkit ή τα ίχνη του μπορούν να παραβιαστούν από το rootkit ακριβώς έτσι ώστε να μην είναι ανιχνεύσιμο.

Η αντιμετώπιση των rootkits απαιτεί μια ποικιλία εργαλείων ασφαλείας σε επίπεδο δικτύου και υπολογιστή. Τόσο τα IDS που βασίζονται σε δίκτυο όσο και σε κεντρικό υπολογιστή μπορούν να αναζητήσουν τις υπογραφές κώδικα γνωστών επιθέσεων rootkit στην εισερχόμενη κίνηση. Το λογισμικό προστασίας από ιούς που βασίζεται σε κεντρικό υπολογιστή μπορεί επίσης να χρησιμοποιηθεί για την αναγνώριση των γνωστών υπογραφών.

Φυσικά, υπάρχουν πάντα νέα rootkit και τροποποιημένες εκδόσεις υπαρχόντων rootkit που εμφανίζουν νέες υπογραφές. Για αυτές τις περιπτώσεις, ένα σύστημα πρέπει να αναζητήσει συμπεριφορές που θα μπορούσαν να υποδεικνύουν την παρουσία ενός rootkit, όπως η παρακολούθηση των κλήσεων συστήματος ή ένα πληκτρολόγιο που αλληλεπιδρά με ένα πρόγραμμα οδήγησης πληκτρολογίου. Αυτή η ανίχνευση συμπεριφοράς δεν είναι καθόλου απλή. Για παράδειγμα, το λογισμικό προστασίας από ιούς συνήθως παρακολουθεί κλήσεις συστήματος.

Μια άλλη προσέγγιση είναι να κάνετε κάποιο είδος ελέγχου ακεραιότητας αρχείων. Ένα παράδειγμα αυτού είναι το RootkitRevealer, ένα πακέτο δωρεάν λογισμικού από το SysInternals. Το πακέτο συγκρίνει τα αποτελέσματα μιας σάρωσης συστήματος χρησιμοποιώντας API με την πραγματική προβολή του χώρου αποθήκευσης χρησιμοποιώντας οδηγίες που δεν περνούν μέσω API. Επειδή ένα rootkit κρύβεται τροποποιώντας την προβολή του χώρου αποθήκευσης που φαίνεται από τις κλήσεις διαχειριστή, το RootkitRevealer εντοπίζει τη διαφορά.

Εάν εντοπιστεί rootkit σε επίπεδο πυρήνα, ο μόνος ασφαλής και αξιόπιστος τρόπος ανάκτησης είναι να κάνετε μια εντελώς νέα εγκατάσταση λειτουργικού συστήματος στο μολυσμένο μηχάνημα.

Ζ) Προσέγγισησάρωσηςπεριμέτρου

Η επόμενη τοποθεσία όπου χρησιμοποιείται λογισμικό προστασίας από ιούς είναι το τείχος προστασίας και το IDS ενός οργανισμού. Συνήθως περιλαμβάνεται σε υπηρεσίες διακομιστή μεσολάβησης e-mail και Web που εκτελούνται σε αυτά τα συστήματα. Μπορεί επίσης να συμπεριληφθεί στο στοιχείο ανάλυσης κίνησης ενός IDS. Αυτό δίνει στο λογισμικό προστασίας από ιούς πρόσβαση σε κακόβουλο λογισμικό κατά τη μεταφορά μέσω σύνδεσης δικτύου με οποιοδήποτε από τα συστήματα του οργανισμού, παρέχοντας μια ευρύτερη προβολή της δραστηριότητας κακόβουλου λογισμικού. Αυτό το λογισμικό μπορεί επίσης να περιλαμβάνει μέτρα πρόληψης εισβολής, μπλοκάρισμα της ροής τυχόν ύποπτης κίνησης, εμποδίζοντας έτσι την επίτευξη και τον κίνδυνο ορισμένου συστήματος στόχου, είτε εντός είτε εκτός του οργανισμού.

Ωστόσο, αυτή η προσέγγιση περιορίζεται στη σάρωση περιεχομένου κακόβουλου λογισμικού, καθώς δεν έχει πρόσβαση σε οποιαδήποτε συμπεριφορά που παρατηρείται όταν εκτελείται σε μολυσμένο σύστημα. Μπορούν να χρησιμοποιηθούν δύο τύποι λογισμικού παρακολούθησης:

- Οθόνες εισόδου: Αυτές βρίσκονται στα σύνορα μεταξύ του εταιρικού δικτύου και του Διαδικτύου. Μπορούν να αποτελούν μέρος του λογισμικού φιλτραρίσματος εισόδου ενός συνοριακού δρομολογητή ή εξωτερικού τείχους προστασίας ή μιας ξεχωριστής παθητικής οθόνης. Αυτές οι οθόνες μπορούν να χρησιμοποιήσουν ανωμαλία ή υπογραφή και ευρετικές προσεγγίσεις για τον εντοπισμό της κίνησης κακόβουλου λογισμικού, όπως συζητάμε περαιτέρω στο Κεφάλαιο 8. Ένα honeypot μπορεί επίσης να συλλάβει την εισερχόμενη κίνηση κακόβουλου λογισμικού. Ένα παράδειγμα τεχνικής ανίχνευσης για ένα μόνιτορ εισόδου είναι η αναζήτηση εισερχόμενης κίνησης σε μη χρησιμοποιημένες τοπικές διευθύνσεις IP.
- Οθόνες Egress: Αυτά μπορούν να βρίσκονται στο σημείο εξόδου μεμονωμένων LAN στο εταιρικό δίκτυο, καθώς και στα σύνορα μεταξύ του εταιρικού δικτύου και του Διαδικτύου. Στην προηγούμενη περίπτωση, η οθόνη εξόδου μπορεί να είναι μέρος του λογισμικού φιλτραρίσματος εξόδου ενός δρομολογητή ή διακόπτη LAN. Όπως με τις οθόνες εισόδου, το εξωτερικό τείχος προστασίας ή ένα honeypot μπορούν να φιλοξενήσουν το λογισμικό παρακολούθησης. Πράγματι, οι δύο τύποι οθονών μπορούν να εγκατασταθούν σε μία συσκευή. Η οθόνη εξόδου έχει σχεδιαστεί για να εντοπίζει την πηγή μιας επίθεσης κακόβουλου λογισμικού παρακολουθώντας την εξερχόμενη κίνηση για σημάδια σάρωσης ή άλλη ύποπτη συμπεριφορά. Αυτή η παρακολούθηση θα μπορούσε να αναζητήσει την κοινή συμπεριφορά διαδοχικής ή τυχαίας σάρωσης που χρησιμοποιείται από τα σκουλήκια και το όριο ρυθμού ή να το αποκλείσει. Μπορεί επίσης να είναι σε θέση να ανιχνεύσει και να ανταποκριθεί σε ασυνήθιστα υψηλή επισκεψιμότητα μέσω email, όπως αυτή που χρησιμοποιείται από σκουλήκια μαζικής αλληλογραφίας ή ανεπιθύμητα φορτία.

Η παρακολούθηση της περιμέτρου μπορεί επίσης να βοηθήσει στον εντοπισμό και την απόκριση στη δραστηριότητα botnet ανιχνεύοντας μη φυσιολογικά μοτίβα κυκλοφορίας που σχετίζονται με αυτήν τη δραστηριότητα. Μόλις ενεργοποιηθούν τα bots και μια επίθεση είναι σε εξέλιξη, μια τέτοια παρακολούθηση μπορεί να χρησιμοποιηθεί για τον εντοπισμό της επίθεσης. Ωστόσο, πρωταρχικός στόχος είναι να προσπαθήσουμε να εντοπίσουμε και να απενεργοποιήσουμε το botnet κατά τη φάση κατασκευής του, χρησιμοποιώντας τις διάφορες

τεχνικές σάρωσης που μόλις συζητήσαμε, εντοπίζοντας και αποκλείοντας το κακόβουλο λογισμικό που χρησιμοποιείται για τη διάδοση αυτού του τύπου ωφέλιμου φορτίου.

Η) Κατανεμημένες προσεγγίσεις συγκέντρωσης πληροφοριών

Η τελική τοποθεσία όπου χρησιμοποιείται το λογισμικό προστασίας από ιούς είναι σε κατανεμημένη διαμόρφωση. Συγκεντρώνει δεδομένα από μεγάλο αριθμό αισθητήρων που βασίζονται σε κεντρικούς υπολογιστές και περιμέτρων, μεταδίδει αυτή τη νοημοσύνη σε ένα κεντρικό σύστημα ανάλυσης ικανό να συσχετίσει και να αναλύσει τα δεδομένα, τα οποία στη συνέχεια μπορούν να επιστρέψουν ενημερωμένες υπογραφές και πρότυπα συμπεριφοράς για να επιτρέψουν σε όλα τα συντονισμένα συστήματα να ανταποκριθούν και υπερασπιστείτε από επιθέσεις κακόβουλου λογισμικού. Έχουν προταθεί ορισμένα τέτοια συστήματα. Αυτό είναι ένα συγκεκριμένο παράδειγμα ενός κατανεμημένου συστήματος πρόληψης εισβολών (IPS), με στόχο κακόβουλο λογισμικό.

Κεφάλαιο 3ο:Ασφάλεια Λειτουργικού Συστήματος

Τα συστήματα υπολογιστών-πελατών και διακομιστών αποτελούν κεντρικά στοιχεία της υποδομής πληροφορικής για τους περισσότερους οργανισμούς. Τα συστήματα πελατών παρέχουν πρόσβαση σε οργανωτικά δεδομένα και εφαρμογές, που υποστηρίζονται από τους διακομιστές που φιλοξενούν αυτά τα δεδομένα και τις εφαρμογές. Ωστόσο, δεδομένου ότι τα περισσότερα μεγάλα συστήματα λογισμικού θα έχουν σχεδόν σίγουρα ορισμένες αδυναμίες ασφαλείας, όπως συζητήσαμε στο Κεφάλαιο 6 και στα προηγούμενα δύο κεφάλαια, είναι επί του παρόντος απαραίτητο να διαχειριστούμε την εγκατάσταση και τη συνέχιση της λειτουργίας αυτών των συστημάτων για την παροχή κατάλληλων επιπέδων ασφάλεια παρά την αναμενόμενη παρουσία αυτών των τρωτών σημείων. Σε ορισμένες περιπτώσεις, ενδέχεται να είμαστε σε θέση να χρησιμοποιήσουμε συστήματα που έχουν σχεδιαστεί και αξιολογηθεί για να παρέχουν ασφάλεια από το σχεδιασμό.

3.1. Εισαγωγή στην Ασφάλεια Λειτουργικού Συστήματος

Όπως σημειώσαμε παραπάνω, τα συστήματα υπολογιστών-πελατών και διακομιστών αποτελούν κεντρικά στοιχεία της υποδομής πληροφορικής για τους περισσότερους οργανισμούς, ενδέχεται να διαθέτουν κρίσιμα δεδομένα και εφαρμογές και αποτελούν απαραίτητο εργαλείο για τη λειτουργία ενός οργανισμού. Συνεπώς, πρέπει να έχουμε επίγνωση της αναμενόμενης παρουσίας τρωτών σημείων σε λειτουργικά συστήματα και εφαρμογές όπως διανέμονται και την ύπαρξη σκουληκιών που ανιχνεύουν τέτοια τρωτά σημεία σε υψηλά ποσοστά, όπως συζητήσαμε στην Ενότητα 6.3. Έτσι, είναι πολύ πιθανό ένα σύστημα να παραβιαστεί κατά τη διάρκεια της διαδικασίας εγκατάστασης, προτού μπορέσει να εγκαταστήσει τις πιο πρόσφατες ενημερώσεις κώδικα ή να εφαρμόσει άλλα μέτρα σκλήρυνσης. Ως εκ τούτου, η κατασκευή και η ανάπτυξη ενός συστήματος πρέπει να είναι μια προγραμματισμένη διαδικασία σχεδιασμένη για την αντιμετώπιση μιας τέτοιας απειλής και για τη διατήρηση της ασφάλειας κατά τη διάρκεια της λειτουργίας του.

(Scarfone, 2008) δηλώνει ότι αυτή η διαδικασία πρέπει:

- Να αξιολογεί τους κινδύνους και να σχεδιάζει την ανάπτυξη του συστήματος.
- Να ασφαλίζει το υποκείμενο λειτουργικό σύστημα και στη συνέχεια τις βασικές εφαρμογές.
- Να βεβαιώνει ότι είναι ασφαλές οποιοδήποτε κρίσιμο περιεχόμενο.
- Να βεβαιώνει ότι χρησιμοποιούνται κατάλληλοι μηχανισμοί προστασίας δικτύου.
- Να βεβαιώνει ότι χρησιμοποιούνται κατάλληλες διαδικασίες για τη διατήρηση της ασφάλειας.

3.2. Σχεδιασμός Ασφάλειας Συστήματος

Το πρώτο βήμα στην ανάπτυξη νέων συστημάτων είναι ο προγραμματισμός. Ο προσεκτικός προγραμματισμός θα σας βοηθήσει να διασφαλίσετε ότι το νέο σύστημα είναι όσο το δυνατόν ασφαλέστερο και συμμορφώνεται με τις απαραίτητες πολιτικές. Αυτός ο σχεδιασμός πρέπει να ενημερώνεται από μια ευρύτερη αξιολόγηση ασφάλειας του οργανισμού, καθώς κάθε οργανισμός έχει ξεχωριστές απαιτήσεις ασφάλειας και ανησυχίες.

Ο στόχος της συγκεκριμένης διαδικασίας σχεδιασμού εγκατάστασης συστήματος είναι να μεγιστοποιήσει την ασφάλεια ενώ ελαχιστοποιεί το κόστος. Η ευρεία εμπειρία δείχνει ότι είναι πολύ πιο δύσκολο και δαπανηρό να "ρετρό-ταιριάζει" ασφάλεια αργότερα, από ό, τι είναι να το σχεδιάσετε και να το παρέχετε κατά τη διάρκεια της αρχικής διαδικασίας ανάπτυξης. Αυτή η διαδικασία σχεδιασμού πρέπει να καθορίσει τις απαιτήσεις ασφαλείας για το σύστημα, τις εφαρμογές και τα δεδομένα του, και των χρηστών του. Αυτό στη συνέχεια καθοδηγεί την επιλογή του κατάλληλου λογισμικού για το λειτουργικό σύστημα και τις εφαρμογές και παρέχει οδηγίες σχετικά με τις κατάλληλες ρυθμίσεις χρήστη και ρυθμίσεις ελέγχου πρόσβασης. Καθοδηγεί επίσης την επιλογή άλλων απαιτούμενων μέτρων σκλήρυνσης. Το σχέδιο πρέπει επίσης να προσδιορίσει το κατάλληλο προσωπικό για να εγκαταστήσει και να διαχειριστεί το σύστημα, λαμβάνοντας υπόψη τις απαιτούμενες δεξιότητες και οποιαδήποτε απαιτούμενη εκπαίδευση.

(Scarfone, 2008) παρέχει μια λίστα στοιχείων που πρέπει να ληφθούν υπόψη κατά τη διαδικασία σχεδιασμού ασφάλειας συστήματος. Ενώ επικεντρώνεται στην ασφαλή ανάπτυξη διακομιστή, μεγάλο μέρος της λίστας ισχύει εξίσου καλά για τη σχεδίαση συστήματος πελάτη. Αυτή η λίστα περιλαμβάνει την εξέταση:

- Ο σκοπός του συστήματος, ο τύπος αποθηκευμένων πληροφοριών, οι παρεχόμενες εφαρμογές και υπηρεσίες και οι απαιτήσεις ασφαλείας τους.
- Οι κατηγορίες χρηστών του συστήματος, τα προνόμια που έχουν και οι τύποι πληροφοριών στις οποίες έχουν πρόσβαση.
- Τρόπος ελέγχου ταυτότητας των χρηστών.
- Πώς διαχειρίζεται η πρόσβαση στις πληροφορίες που είναι αποθηκευμένες στο σύστημα.
- Τι πρόσβαση έχει το σύστημα σε πληροφορίες που είναι αποθηκευμένες σε άλλους κεντρικούς υπολογιστές, όπως διακομιστές αρχείων ή βάσεων δεδομένων, και πώς γίνεται αυτό.
- Ποιος θα διαχειριστεί το σύστημα και πώς θα διαχειριστεί το σύστημα (μέσω τοπικής ή απομακρυσμένης πρόσβασης).
- Τυχόν πρόσθετα μέτρα ασφαλείας που απαιτούνται στο σύστημα, συμπεριλαμβανομένης της χρήσης τείχους προστασίας κεντρικού υπολογιστή,

μηχανισμών προστασίας από ιούς ή άλλων κακόβουλων προγραμμάτων και καταγραφής.

3.3. Σκλήρυνση Λειτουργικών Συστημάτων

Το πρώτο κρίσιμο βήμα για την εξασφάλιση ενός συστήματος είναι η εξασφάλιση του βασικού λειτουργικού συστήματος στο οποίο βασίζονται όλες οι άλλες εφαρμογές και υπηρεσίες. Ένα καλό ίδρυμα ασφαλείας χρειάζεται ένα σωστά εγκατεστημένο, διορθωμένο και διαμορφωμένο λειτουργικό σύστημα. Δυστυχώς, η προεπιλεγμένη διαμόρφωση για πολλά λειτουργικά συστήματα μεγιστοποιεί την ευκολία χρήσης και τη λειτουργικότητα, παρά την ασφάλεια. Επιπλέον, δεδομένου ότι κάθε οργανισμός έχει τις δικές του ανάγκες ασφάλειας, το κατάλληλο προφίλ ασφαλείας και, συνεπώς, η διαμόρφωση, θα διαφέρει επίσης. Αυτό που απαιτείται για ένα συγκεκριμένο σύστημα πρέπει να προσδιοριστεί κατά τη φάση προγραμματισμού.

(Scarfone, 2008) προτείνει τα ακόλουθα βασικά βήματα που πρέπει να χρησιμοποιηθούν για την ασφάλεια ενός λειτουργικού συστήματος:

- Εγκαταστήστε και επιδιορθώστε το λειτουργικό σύστημα.
- Προστατέψτε και διαμορφώστε το λειτουργικό σύστημα ώστε να αντιμετωπίσετε επαρκώς τις προσδιορισμένες ανάγκες ασφαλείας του συστήματος με:
    1. Κατάργηση περιττών υπηρεσιών, εφαρμογών και πρωτοκόλλων.
    2. Διαμόρφωση χρηστών, ομάδων και αδειών.
    3. Διαμόρφωση ελέγχων πόρων.
- Εγκαταστήστε και διαμορφώστε πρόσθετα στοιχεία ελέγχου ασφαλείας, όπως anti-virus, τείχη προστασίας που βασίζονται σε κεντρικούς υπολογιστές και συστήματα ανίχνευσης εισβολής (IDS), εάν χρειάζεται.
- Ελέγξτε την ασφάλεια του βασικού λειτουργικού συστήματος για να βεβαιωθείτε ότι τα βήματα που λαμβάνονται ανταποκρίνονται επαρκώς στις ανάγκες ασφαλείας του.

<u>Α) Εγκατάσταση λειτουργικού συστήματος: Αρχική εγκατάσταση και ενημέρωση κώδικα</u>

Η ασφάλεια του συστήματος ξεκινά με την εγκατάσταση του λειτουργικού συστήματος. Όπως έχουμε ήδη σημειώσει, ένα δίκτυο συνδεδεμένο, χωρίς σύστημα, είναι ευάλωτο σε εκμετάλλευση κατά την εγκατάσταση ή τη συνεχιζόμενη χρήση του. Ως εκ τούτου, είναι σημαντικό το σύστημα να μην εκτίθεται ενώ βρίσκεται σε αυτήν την ευάλωτη κατάσταση. Ιδανικά, νέα συστήματα πρέπει να κατασκευάζονται σε προστατευμένο δίκτυο. Αυτό μπορεί να είναι ένα εντελώς απομονωμένο δίκτυο, με την εικόνα του λειτουργικού συστήματος και όλες τις διαθέσιμες ενημερώσεις κώδικα να μεταφέρονται σε αυτό χρησιμοποιώντας αφαιρούμενα μέσα όπως DVD ή μονάδες USB. Δεδομένης της ύπαρξης κακόβουλου λογισμικού που μπορεί να διαδώσει χρησιμοποιώντας αφαιρούμενα μέσα, απαιτείται προσοχή για να διασφαλιστεί ότι τα μέσα που χρησιμοποιούνται εδώ δεν είναι τόσο μολυσμένα. Εναλλακτικά, μπορεί να χρησιμοποιηθεί ένα δίκτυο με αυστηρά περιορισμένη πρόσβαση στο ευρύτερο Διαδίκτυο. Στην ιδανική περίπτωση, δεν θα πρέπει να έχει εισερχόμενη πρόσβαση και να έχει εξερχόμενη πρόσβαση μόνο στις βασικές τοποθεσίες που απαιτούνται για τη διαδικασία εγκατάστασης και διόρθωσης του συστήματος. Σε κάθε περίπτωση, η πλήρης διαδικασία εγκατάστασης και σκλήρυνσης πρέπει να πραγματοποιηθεί πριν το σύστημα αναπτυχθεί στην προβλεπόμενη, πιο προσιτή και, ως εκ τούτου, ευάλωτη τοποθεσία του.

Η αρχική εγκατάσταση θα πρέπει να εγκαταστήσει το ελάχιστο απαραίτητο για το επιθυμητό σύστημα, με πρόσθετα πακέτα λογισμικού που περιλαμβάνονται μόνο εάν απαιτούνται για τη λειτουργία του συστήματος. Εξετάζουμε τη λογική για ελαχιστοποίηση του αριθμού των πακέτων στο σύστημα σύντομα.

Η συνολική διαδικασία εκκίνησης πρέπει επίσης να είναι ασφαλής. Αυτό μπορεί να απαιτεί προσαρμογή επιλογών ή καθορισμό κωδικού πρόσβασης που απαιτείται για αλλαγές στον κωδικό BIOS που χρησιμοποιείται κατά την εκκίνηση του συστήματος. Μπορεί επίσης να απαιτεί περιορισμό από ποια μέσα επιτρέπεται συνήθως η εκκίνηση του συστήματος. Αυτό είναι απαραίτητο για να αποτραπεί ένας εισβολέας από την αλλαγή της διαδικασίας εκκίνησης για να εγκαταστήσει έναν κρυφό υπεύθυνο, ή για να εκκινήσει ένα σύστημα της επιλογής του από εξωτερικά μέσα προκειμένου να παρακάμψει τα κανονικά στοιχεία ελέγχου πρόσβασης συστήματος σε τοπικά αποθηκευμένα δεδομένα. Η χρήση ενός κρυπτογραφικού συστήματος αρχείων μπορεί επίσης να χρησιμοποιηθεί για την αντιμετώπιση αυτής της απειλής, όπως σημειώνουμε αργότερα.

Απαιτείται επίσης προσοχή με την επιλογή και εγκατάσταση οποιουδήποτε πρόσθετου κωδικού προγράμματος οδήγησης συσκευής, καθώς αυτό εκτελείται με πλήρη δικαιώματα σε επίπεδο πυρήνα, αλλά συχνά παρέχεται από τρίτο μέρος. Η ακεραιότητα και η πηγή αυτού του κωδικού προγράμματος οδήγησης πρέπει να επικυρωθεί προσεκτικά δεδομένου του υψηλού επιπέδου εμπιστοσύνης που έχει. Ένα κακόβουλο πρόγραμμα οδήγησης μπορεί δυνητικά να παρακάμψει πολλούς ελέγχους ασφαλείας για την εγκατάσταση κακόβουλου λογισμικού. Αυτό έγινε τόσο στο rootkit επίδειξης BluePill όσο και στο σκουλήκι Stuxnet.

Δεδομένης της συνεχιζόμενης ανακάλυψης λογισμικού και άλλων τρωτών σημείων για κοινά χρησιμοποιούμενα λειτουργικά συστήματα και εφαρμογές, είναι κρίσιμο το σύστημα να διατηρείται όσο το δυνατόν πιο ενημερωμένο, με όλα τα κρίσιμα patches που σχετίζονται με την ασφάλεια. Πράγματι, κάνοντας αυτό, αντιμετωπίζει μία από τις τέσσερις βασικές στρατηγικές μετριασμού ASD που αναφέραμε προηγουμένως. Σχεδόν όλα τα κοινά χρησιμοποιούμενα συστήματα παρέχουν πλέον βοηθητικά προγράμματα που μπορούν να κατεβάσουν και να εγκαταστήσουν αυτόματα ενημερώσεις ασφαλείας. Αυτά τα εργαλεία πρέπει να διαμορφωθούν και να χρησιμοποιηθούν για να ελαχιστοποιηθεί ο χρόνος που οποιοδήποτε σύστημα είναι ευάλωτο σε αδυναμίες για τις οποίες είναι διαθέσιμες ενημερώσεις κώδικα.

Να σημειωθεί ότι σε συστήματα ελεγχόμενης αλλαγής, δεν πρέπει να εκτελείτε αυτόματες ενημερώσεις, επειδή οι ενημερώσεις κώδικα ασφαλείας μπορούν, σε σπάνιες αλλά σημαντικές περιπτώσεις, να προκαλέσουν αστάθεια. Για συστήματα στα οποία η διαθεσιμότητα και ο χρόνος λειτουργίας είναι υψίστης σημασίας, επομένως, θα πρέπει να πραγματοποιήσετε και να επικυρώσετε όλες τις ενημερώσεις κώδικα σε δοκιμαστικά συστήματα πριν τα αναπτύξετε στην παραγωγή.

Β) Κατάργηση περιττών υπηρεσιών, εφαρμογών και πρωτοκόλλων

Επειδή οποιοδήποτε από τα πακέτα λογισμικού που εκτελούνται σε ένα σύστημα ενδέχεται να περιέχει ευπάθειες λογισμικού, σαφώς εάν υπάρχουν λιγότερα πακέτα λογισμικού για εκτέλεση, τότε ο κίνδυνος μειώνεται. Υπάρχει σαφώς μια ισορροπία μεταξύ χρηστικότητας, παρέχοντας σε όλο το λογισμικό που μπορεί να απαιτείται κάποια στιγμή, με ασφάλεια, και την επιθυμία να περιορίσετε την ποσότητα του εγκατεστημένου λογισμικού. Το εύρος των

απαιτούμενων υπηρεσιών, εφαρμογών και πρωτοκόλλων θα ποικίλλει πολύ μεταξύ των οργανισμών, και μάλιστα μεταξύ των συστημάτων εντός ενός οργανισμού. Η διαδικασία σχεδιασμού του συστήματος θα πρέπει να προσδιορίζει τι πραγματικά απαιτείται για ένα δεδομένο σύστημα, έτσι ώστε να παρέχεται ένα κατάλληλο επίπεδο λειτουργικότητας, ενώ ταυτόχρονα εξαλείφεται το λογισμικό που δεν απαιτείται για τη βελτίωση της ασφάλειας.

Η προεπιλεγμένη διαμόρφωση για τα περισσότερα κατανεμημένα συστήματα έχει οριστεί για να μεγιστοποιεί την ευκολία χρήσης και τη λειτουργικότητα, παρά την ασφάλεια. Κατά την εκτέλεση της αρχικής εγκατάστασης, οι παρεχόμενες προεπιλογές δεν πρέπει να χρησιμοποιούνται, αλλά μάλλον η εγκατάσταση θα πρέπει να προσαρμοστεί έτσι ώστε να εγκαθίστανται μόνο τα απαιτούμενα πακέτα. Εάν χρειαστούν πρόσθετα πακέτα αργότερα, μπορούν να εγκατασταθούν όταν απαιτούνται. (Scarfone, 2008) και πολλοί από τους οδηγούς σκλήρυνσης ασφαλείας παρέχουν λίστες υπηρεσιών, εφαρμογών και πρωτοκόλλων που δεν πρέπει να εγκατασταθούν εάν δεν απαιτείται.

(Scarfone, 2008) δηλώνει επίσης μια ισχυρή προτίμηση για τη μη εγκατάσταση ανεπιθύμητου λογισμικού, παρά την εγκατάσταση και στη συνέχεια την κατάργηση ή την απενεργοποίησή του. Υποστηρίζει αυτήν την προτίμηση, επειδή σημειώνουν ότι πολλά σενάρια απεγκατάστασης αποτυγχάνουν να αφαιρέσουν εντελώς όλα τα στοιχεία ενός πακέτου. Σημειώνουν επίσης ότι η απενεργοποίηση μιας υπηρεσίας σημαίνει ότι ενώ δεν είναι διαθέσιμη ως αρχικό σημείο επίθεσης, εάν ένας εισβολέας επιτύχει να αποκτήσει κάποια πρόσβαση σε ένα σύστημα, τότε το απενεργοποιημένο λογισμικό θα μπορούσε να ενεργοποιηθεί εκ νέου και να χρησιμοποιηθεί για περαιτέρω συμβιβασμό ενός συστήματος. Είναι καλύτερο για την ασφάλεια εάν δεν είναι εγκατεστημένο ανεπιθύμητο λογισμικό και, ως εκ τούτου, δεν είναι διαθέσιμο για χρήση καθόλου.

Γ) Ρύθμιση παραμέτρων χρηστών, ομάδων και ελέγχου ταυτότητας

Δεν έχουν όλοι οι χρήστες με πρόσβαση σε ένα σύστημα την ίδια πρόσβαση σε όλα τα δεδομένα και τους πόρους του συστήματος. Όλα τα σύγχρονα λειτουργικά συστήματα εφαρμόζουν ελέγχους πρόσβασης σε δεδομένα και πόρους. Σχεδόν όλοι παρέχουν κάποια μορφή διακριτικών ελέγχων πρόσβασης. Ορισμένα συστήματα ενδέχεται να παρέχουν μηχανισμούς

ελέγχου πρόσβασης με βάση το ρόλο ή υποχρεωτικούς. Η διαδικασία σχεδιασμού του συστήματος θα πρέπει να λαμβάνει υπόψη τις κατηγορίες των χρηστών στο σύστημα, τα προνόμια που έχουν, τους τύπους πληροφοριών στις οποίες μπορούν να έχουν πρόσβαση, καθώς και πώς και πού καθορίζονται και πιστοποιούνται. Ορισμένοι χρήστες θα έχουν αυξημένα δικαιώματα για τη διαχείριση του συστήματος. Άλλοι θα είναι κανονικοί χρήστες, μοιράζονται την κατάλληλη πρόσβαση σε αρχεία και άλλα δεδομένα, όπως απαιτείται. και μπορεί να υπάρχουν ακόμη και λογαριασμοί επισκεπτών με πολύ περιορισμένη πρόσβαση. Το τρίτο από τις τέσσερις βασικές στρατηγικές μετριασμού ASD είναι ο περιορισμός των αυξημένων δικαιωμάτων μόνο σε εκείνους τους χρήστες που τους χρειάζονται. Περαιτέρω, είναι ιδιαίτερα επιθυμητό αυτοί οι χρήστες να έχουν πρόσβαση σε αυξημένα δικαιώματα μόνο όταν χρειάζεται για να εκτελέσουν κάποια εργασία που τους απαιτεί και να έχουν διαφορετική πρόσβαση στο σύστημα ως κανονικός χρήστης. Αυτό βελτιώνει την ασφάλεια παρέχοντας ένα μικρότερο παράθυρο ευκαιρίας σε έναν εισβολέα να εκμεταλλευτεί τις ενέργειες τέτοιων προνομιούχων χρηστών. Ορισμένα λειτουργικά συστήματα παρέχουν ειδικά εργαλεία ή μηχανισμούς πρόσβασης για να βοηθήσουν τους διοικητικούς χρήστες να αυξήσουν τα προνόμιά τους μόνο όταν είναι απαραίτητο και να καταγράψουν κατάλληλα αυτές τις ενέργειες. Μια βασική απόφαση είναι εάν οι χρήστες, οι ομάδες στις οποίες ανήκουν και οι μέθοδοι ελέγχου ταυτότητας καθορίζονται τοπικά στο σύστημα ή θα χρησιμοποιούν έναν κεντρικό διακομιστή ελέγχου ταυτότητας. Όποιο κι αν είναι επιλεγμένο, οι κατάλληλες λεπτομέρειες διαμορφώνονται τώρα στο σύστημα. Επίσης, σε αυτό το στάδιο, τυχόν προεπιλεγμένοι λογαριασμοί που περιλαμβάνονται στο πλαίσιο της εγκατάστασης του συστήματος θα πρέπει να είναι ασφαλείς. Εκείνα που δεν απαιτούνται πρέπει να αφαιρεθούν ή τουλάχιστον να απενεργοποιηθούν. Οι λογαριασμοί συστήματος που διαχειρίζονται υπηρεσίες στο σύστημα πρέπει να οριστούν έτσι ώστε να μην μπορούν να χρησιμοποιηθούν για διαδραστικές συνδέσεις. Και οι κωδικοί πρόσβασης που έχουν εγκατασταθεί από προεπιλογή θα πρέπει να αλλάξουν σε νέες τιμές με κατάλληλη ασφάλεια. Οποιαδήποτε πολιτική που ισχύει για διαπιστευτήρια ελέγχου ταυτότητας, και ειδικά για την ασφάλεια κωδικού πρόσβασης, έχει επίσης ρυθμιστεί. Αυτό περιλαμβάνει λεπτομέρειες σχετικά με τις μεθόδους ελέγχου ταυτότητας που γίνονται αποδεκτές για διαφορετικές μεθόδους πρόσβασης στο λογαριασμό. Περιλαμβάνει λεπτομέρειες για το απαιτούμενο μήκος, την πολυπλοκότητα και την ηλικία που επιτρέπεται για τους κωδικούς πρόσβασης.

Δ) Διαμόρφωση στοιχείων ελέγχου πόρων

Μόλις καθοριστούν οι χρήστες και οι συσχετισμένες ομάδες τους, μπορούν να οριστούν κατάλληλα δικαιώματα σε δεδομένα και πόρους για να ταιριάζουν με την καθορισμένη πολιτική. Αυτό μπορεί να είναι για τον περιορισμό των χρηστών που μπορούν να εκτελέσουν ορισμένα προγράμματα, ειδικά εκείνα που τροποποιούν την κατάσταση του συστήματος. Ή μπορεί να είναι ο περιορισμός των χρηστών που μπορούν να διαβάσουν ή να γράψουν δεδομένα σε ορισμένα δέντρα καταλόγου. Πολλοί από τους οδηγούς σκλήρυνσης ασφαλείας παρέχουν λίστες με προτεινόμενες αλλαγές στην προεπιλεγμένη διαμόρφωση πρόσβασης για τη βελτίωση της ασφάλειας.

Ε) Εγκατάσταση πρόσθετων στοιχείων ελέγχου ασφαλείας

Περαιτέρω βελτίωση της ασφάλειας μπορεί να είναι δυνατή με την εγκατάσταση και διαμόρφωση πρόσθετων εργαλείων ασφαλείας, όπως λογισμικό προστασίας από ιούς, τείχη προστασίας που βασίζονται σε κεντρικούς υπολογιστές, λογισμικό IDS ή IPS ή λευκή λίστα εφαρμογών. Ορισμένες από αυτές ενδέχεται να παρέχονται ως μέρος της εγκατάστασης των λειτουργικών συστημάτων, αλλά δεν έχουν ρυθμιστεί και ενεργοποιηθεί από προεπιλογή. Άλλα είναι προϊόντα τρίτων που αποκτώνται και χρησιμοποιούνται.

Δεδομένης της διαδεδομένης επικράτησης κακόβουλου λογισμικού, όπως συζητάμε στο Κεφάλαιο 6, η κατάλληλη προστασία από ιούς (η οποία όπως αναφέρεται αναφέρεται σε ένα ευρύ φάσμα τύπων κακόβουλου λογισμικού) είναι ένα κρίσιμο στοιχείο ασφάλειας σε πολλά συστήματα. Τα προϊόντα κατά των ιών παραδοσιακά χρησιμοποιούνται σε συστήματα Windows, καθώς η υψηλή χρήση τους τα έκανε προτιμώμενο στόχο για τους εισβολείς. Ωστόσο, η ανάπτυξη σε άλλες πλατφόρμες, ιδίως smartphone, έχει οδηγήσει σε ανάπτυξη περισσότερων κακόβουλων προγραμμάτων για αυτούς. Ως εκ τούτου, τα κατάλληλα προϊόντα κατά των ιών πρέπει να λαμβάνονται υπόψη για οποιοδήποτε σύστημα ως μέρος του προφίλ ασφαλείας του.

Τα τείχη προστασίας που βασίζονται σε κεντρικούς υπολογιστές, το λογισμικό IDS και το IPS ενδέχεται επίσης να βελτιώσουν την ασφάλεια περιορίζοντας την απομακρυσμένη

πρόσβαση δικτύου σε υπηρεσίες του συστήματος. Εάν δεν απαιτείται απομακρυσμένη πρόσβαση σε μια υπηρεσία, αν και κάποια τοπική πρόσβαση είναι απαραίτητη, τότε αυτοί οι περιορισμοί βοηθούν στη διασφάλιση τέτοιων υπηρεσιών από την απομακρυσμένη εκμετάλλευση από έναν εισβολέα. Τα τείχη προστασίας είναι παραδοσιακά διαμορφωμένα ώστε να περιορίζουν την πρόσβαση μέσω θύρας ή πρωτοκόλλου, από ορισμένα ή όλα τα εξωτερικά συστήματα. Ορισμένα ενδέχεται επίσης να έχουν ρυθμιστεί ώστε να επιτρέπουν την πρόσβαση από ή σε συγκεκριμένα προγράμματα στα συστήματα, να περιορίζουν περαιτέρω τα σημεία επίθεσης και να αποτρέπουν την εγκατάσταση και την πρόσβαση ενός εισβολέα από κακόβουλο λογισμικό. Το λογισμικό IDS και IPS μπορεί να περιλαμβάνει πρόσθετους μηχανισμούς, όπως παρακολούθηση της κυκλοφορίας, ή έλεγχο ακεραιότητας αρχείων για τον εντοπισμό και ακόμη και την απάντηση σε ορισμένους τύπους επιθέσεων.

Ένας άλλος πρόσθετος έλεγχος είναι στις εφαρμογές λευκής λίστας. Αυτό περιορίζει τα προγράμματα που μπορούν να εκτελεστούν στο σύστημα μόνο σε εκείνα σε μια ρητή λίστα. Ένα τέτοιο εργαλείο μπορεί να εμποδίσει έναν εισβολέα να εγκαταστήσει και να εκτελέσει το δικό του κακόβουλο λογισμικό και είναι η πρώτη από τις τέσσερις βασικές στρατηγικές μετριασμού ASD. Ενώ αυτό θα βελτιώσει την ασφάλεια, λειτουργεί καλύτερα σε περιβάλλον με ένα προβλέψιμο σύνολο εφαρμογών που απαιτούν οι χρήστες. Οποιαδήποτε αλλαγή στη χρήση λογισμικού θα απαιτούσε αλλαγή στη διαμόρφωση, η οποία μπορεί να οδηγήσει σε αυξημένες απαιτήσεις υποστήριξης πληροφορικής. Δεν θα είναι επαρκώς προβλέψιμοι όλοι οι οργανισμοί ή όλα τα συστήματα ώστε να ταιριάζουν σε αυτόν τον τύπο ελέγχου.

ΣΤ) Έλεγχος ασφάλειας συστήματος

Το τελευταίο βήμα στη διαδικασία της αρχικής εξασφάλισης του βασικού λειτουργικού συστήματος είναι ο έλεγχος ασφαλείας. Ο στόχος είναι να διασφαλιστεί ότι τα προηγούμενα βήματα διαμόρφωσης ασφαλείας εφαρμόζονται σωστά και να εντοπιστούν τυχόν πιθανές ευπάθειες που πρέπει να διορθωθούν ή να διαχειριστούν. Κατάλληλες λίστες ελέγχου περιλαμβάνονται σε πολλούς οδηγούς σκλήρυνσης ασφαλείας. Υπάρχουν επίσης προγράμματα ειδικά σχεδιασμένα για την αναθεώρηση ενός συστήματος για να διασφαλιστεί ότι ένα σύστημα πληροί τις βασικές απαιτήσεις ασφάλειας και για τη σάρωση για γνωστές ευπάθειες και κακές πρακτικές διαμόρφωσης. Αυτό πρέπει να γίνει μετά την αρχική σκλήρυνση του συστήματος και στη συνέχεια να επαναλαμβάνεται περιοδικά ως μέρος της διαδικασίας συντήρησης ασφαλείας.

3.4. ΑσφάλειαΕφαρμογών

Μόλις το βασικό λειτουργικό σύστημα εγκατασταθεί και ασφαλιστεί κατάλληλα, οι απαιτούμενες υπηρεσίες και εφαρμογές πρέπει στη συνέχεια να εγκατασταθούν και να διαμορφωθούν. Τα βήματα για αυτό αντικατοπτρίζουν σε μεγάλο βαθμό τη λίστα που έχει ήδη δοθεί στην προηγούμενη ενότητα. Η ανησυχία, όπως και με το βασικό λειτουργικό σύστημα, είναι η εγκατάσταση μόνο λογισμικού στο σύστημα που απαιτείται για την κάλυψη της επιθυμητής λειτουργικότητάς του, προκειμένου να μειωθεί ο αριθμός των θέσεων που μπορεί να βρεθούν ευπάθειες. Το λογισμικό που παρέχει απομακρυσμένη πρόσβαση ή υπηρεσία είναι ιδιαίτερα ανησυχητικό, καθώς ένας εισβολέας μπορεί να είναι σε θέση να το εκμεταλλευτεί για να αποκτήσει απομακρυσμένη πρόσβαση στο σύστημα. Επομένως, οποιοδήποτε τέτοιο λογισμικό πρέπει να επιλεγεί προσεκτικά και να διαμορφωθεί και να ενημερωθεί στην πιο πρόσφατη διαθέσιμη έκδοση.

Κάθε επιλεγμένη υπηρεσία ή εφαρμογή πρέπει να εγκατασταθεί και, στη συνέχεια, να διορθωθεί στην πιο πρόσφατη υποστηριζόμενη ασφαλή έκδοση κατάλληλη για το σύστημα. Αυτό μπορεί να προέρχεται από πρόσθετα πακέτα που παρέχονται με τη διανομή του λειτουργικού συστήματος ή από ξεχωριστό πακέτο τρίτων. Όπως με το βασικό λειτουργικό σύστημα, προτιμάται η χρήση ενός απομονωμένου, ασφαλούς δικτύου κατασκευής.

Α) Διαμόρφωση εφαρμογής

1878 / 5000

Αποτελέσματα μετάφρασης

Στη συνέχεια εκτελείται οποιαδήποτε ρύθμιση παραμέτρων για συγκεκριμένη εφαρμογή. Αυτό μπορεί να περιλαμβάνει τη δημιουργία και τον καθορισμό κατάλληλων περιοχών αποθήκευσης δεδομένων για την εφαρμογή και την πραγματοποίηση κατάλληλων αλλαγών στις προεπιλεγμένες λεπτομέρειες της εφαρμογής ή της υπηρεσίας. Ορισμένες εφαρμογές ή υπηρεσίες ενδέχεται να περιλαμβάνουν προεπιλεγμένα δεδομένα, σενάρια ή λογαριασμούς χρηστών. Αυτά πρέπει να αναθεωρηθούν και να διατηρηθούν μόνο αν απαιτείται και να ασφαλιστούν κατάλληλα. Ένα πολύ γνωστό παράδειγμα αυτού βρίσκεται στους διακομιστές Web, οι οποίοι συχνά περιλαμβάνουν έναν αριθμό παραδειγμάτων σεναρίων, αρκετά από τα οποία είναι γνωστό ότι είναι ανασφαλή. Αυτά δεν πρέπει να χρησιμοποιούνται όπως παρέχονται, αλλά θα πρέπει να αφαιρεθούν εκτός εάν χρειαστεί και ασφαλιστεί. Ως μέρος της διαδικασίας διαμόρφωσης, πρέπει να εξεταστεί προσεκτικά τα δικαιώματα πρόσβασης που παραχωρούνται στην εφαρμογή. Και πάλι, αυτό αφορά ιδιαίτερα τις υπηρεσίες που έχουν πρόσβαση από απόσταση, όπως υπηρεσίες Web και μεταφοράς αρχείων. Στην εφαρμογή διακομιστή δεν πρέπει να παραχωρηθεί το δικαίωμα τροποποίησης αρχείων, εκτός εάν απαιτείται συγκεκριμένη λειτουργία. Ένα πολύ κοινό σφάλμα διαμόρφωσης που εμφανίζεται στους διακομιστές μεταφοράς Ιστού και αρχείων είναι ότι όλα τα αρχεία που παρέχονται από την υπηρεσία ανήκουν στον ίδιο λογαριασμό "χρήστη" με τον οποίο εκτελείται ο διακομιστής. Η συνέπεια είναι ότι οποιοσδήποτε εισβολέας μπορεί να εκμεταλλευτεί κάποια ευπάθεια είτε στο λογισμικό του διακομιστή είτε σε ένα σενάριο που εκτελείται από το διακομιστή μπορεί να είναι σε θέση να τροποποιήσει οποιοδήποτε από αυτά τα αρχεία. Ο μεγάλος αριθμός επιθέσεων "Web defacing" αποτελεί σαφή ένδειξη αυτού του τύπου ανασφαλούς διαμόρφωσης. Μεγάλο μέρος του κινδύνου από αυτήν τη μορφή επίθεσης μειώνεται διασφαλίζοντας ότι τα περισσότερα από τα αρχεία μπορούν να διαβαστούν μόνο, αλλά όχι να γραφτούν, από τον διακομιστή. Μόνο εκείνα τα αρχεία που πρέπει να τροποποιηθούν, για να αποθηκεύσουν τα φορτωμένα δεδομένα φόρμας, για παράδειγμα, ή λεπτομέρειες καταγραφής, πρέπει να είναι εγγράψιμα από το διακομιστή. Αντ 'αυτού, τα αρχεία πρέπει κυρίως να ανήκουν και να τροποποιούνται από τους χρήστες του συστήματος που είναι υπεύθυνοι για τη διατήρηση των πληροφοριών.

Β) Τεχνολογία κρυπτογράφησης

Η κρυπτογράφηση είναι ένα κλειδί που επιτρέπει την τεχνολογία που μπορεί να χρησιμοποιηθεί για την ασφάλεια δεδομένων τόσο κατά τη μεταφορά όσο και κατά την αποθήκευση. Εάν απαιτούνται τέτοιες τεχνολογίες για το σύστημα, τότε πρέπει να διαμορφωθούν και να δημιουργηθούν, να υπογραφούν και να ασφαλιστούν τα κατάλληλα κλειδιά κρυπτογράφησης.

Εάν παρέχονται ασφαλείς υπηρεσίες δικτύου, κατά πάσα πιθανότητα χρησιμοποιώντας είτε TLS είτε IPsec, τότε πρέπει να δημιουργηθούν κατάλληλα δημόσια και ιδιωτικά κλειδιά για καθένα από αυτά. Στη συνέχεια, τα πιστοποιητικά X.509 δημιουργούνται και υπογράφονται από μια αρμόδια αρχή έκδοσης πιστοποιητικών, συνδέοντας κάθε ταυτότητα υπηρεσίας με το δημόσιο κλειδί που χρησιμοποιείται. Εάν παρέχεται ασφαλής απομακρυσμένη πρόσβαση χρησιμοποιώντας το SecureShell (SSH), τότε πρέπει ο κατάλληλος διακομιστής, και ενδεχομένως τα κλειδιά πελάτη, να δημιουργηθεί.

Τα κρυπτογραφικά συστήματα αρχείων είναι μια άλλη χρήση κρυπτογράφησης. Εάν θέλετε, τότε αυτά πρέπει να δημιουργηθούν και να ασφαλιστούν με κατάλληλα κλειδιά.

3.5. Συντήρηση ασφαλείας

Μόλις το σύστημα κατασκευαστεί, ασφαλιστεί και αναπτυχθεί κατάλληλα, η διαδικασία διατήρησης της ασφάλειας είναι συνεχής. Αυτό προκύπτει από το συνεχώς μεταβαλλόμενο περιβάλλον, την ανακάλυψη νέων τρωτών σημείων και, συνεπώς, την έκθεση σε νέες απειλές. (Scarfone, 2008) προτείνει ότι αυτή η διαδικασία συντήρησης ασφαλείας περιλαμβάνει τα ακόλουθα πρόσθετα βήματα:

- Παρακολούθηση και ανάλυση πληροφοριών καταγραφής
- Τακτική εκτέλεση αντιγράφων ασφαλείας
- Ανάκτηση από συμβιβασμούς ασφαλείας
- Τακτικόςέλεγχοςασφάλειαςσυστήματος
- Χρήση κατάλληλων διαδικασιών συντήρησης λογισμικού για την επιδιόρθωση και την ενημέρωση όλων των κρίσιμων λογισμικών και για την παρακολούθηση και την αναθεώρηση της διαμόρφωσης, όπως απαιτείται.

A) Logging

Ο (Scarfone, 2008) σημειώνει ότι "η καταγραφή είναι ο ακρογωνιαίος λίθος μιας στάσης ασφάλειας ήχου." Η καταγραφή είναι ένας αντιδραστικός έλεγχος που μπορεί να σας ενημερώσει μόνο για κακά πράγματα που έχουν ήδη συμβεί. Ωστόσο, η αποτελεσματική καταγραφή συμβάλλει στη διασφάλιση ότι σε περίπτωση παραβίασης ή αποτυχίας του συστήματος, οι διαχειριστές συστήματος μπορούν να εντοπίσουν πιο γρήγορα και με ακρίβεια τι συνέβη και, κατά συνέπεια, να επικεντρώσουν αποτελεσματικότερα τις προσπάθειες αποκατάστασης και ανάκτησης. Το κλειδί είναι να διασφαλίσετε ότι καταγράφετε τα σωστά δεδομένα στα αρχεία καταγραφής και, στη συνέχεια, μπορείτε να παρακολουθείτε και να αναλύετε κατάλληλα αυτά τα δεδομένα. Οι πληροφορίες καταγραφής μπορούν να δημιουργηθούν από το σύστημα, το δίκτυο και τις εφαρμογές. Το εύρος των δεδομένων καταγραφής που αποκτώνται πρέπει να προσδιοριστεί κατά τη διάρκεια του σταδίου σχεδιασμού του συστήματος, καθώς εξαρτάται από τις απαιτήσεις ασφαλείας και την ευαισθησία πληροφοριών του διακομιστή.

Η καταγραφή μπορεί να δημιουργήσει σημαντικούς όγκους πληροφοριών. Είναι σημαντικό να διατεθεί επαρκής χώρος για αυτούς. Θα πρέπει επίσης να διαμορφωθεί ένα κατάλληλο σύστημα αυτόματης περιστροφής καταγραφής και αρχειοθέτησης ώστε να βοηθά στη διαχείριση του συνολικού μεγέθους των πληροφοριών καταγραφής.

Η μη αυτόματη ανάλυση των αρχείων καταγραφής είναι κουραστική και δεν αποτελεί αξιόπιστο μέσο για την ανίχνευση ανεπιθύμητων ενεργειών. Μάλλον, προτιμάται κάποια μορφή αυτοματοποιημένης ανάλυσης, καθώς είναι πιο πιθανό να εντοπιστεί μη φυσιολογική δραστηριότητα.

Β) Δημιουργία αντιγράφων ασφαλείας και αρχείο δεδομένων

Η πραγματοποίηση τακτικών αντιγράφων ασφαλείας δεδομένων σε ένα σύστημα είναι ένας άλλος κρίσιμος έλεγχος που βοηθά στη διατήρηση της ακεραιότητας του συστήματος και των δεδομένων χρήστη. Υπάρχουν πολλοί λόγοι για τους οποίους μπορεί να χαθούν δεδομένα από ένα σύστημα, συμπεριλαμβανομένων αστοχιών υλικού ή λογισμικού ή τυχαίας ή σκόπιμης διαφθοράς. Μπορεί επίσης να υπάρχουν νομικές ή λειτουργικές απαιτήσεις για τη διατήρηση δεδομένων. Η δημιουργία αντιγράφων ασφαλείας είναι η διαδικασία δημιουργίας αντιγράφων δεδομένων σε τακτά χρονικά διαστήματα, επιτρέποντας την ανάκτηση χαμένων ή κατεστραμμένων δεδομένων σε σχετικά σύντομες χρονικές περιόδους από μερικές ώρες έως μερικές εβδομάδες. Το Αρχείο είναι η διαδικασία διατήρησης αντιγράφων δεδομένων για παρατεταμένες χρονικές περιόδους, που είναι μήνες ή χρόνια, προκειμένου να πληρούνται νομικές και λειτουργικές απαιτήσεις για την πρόσβαση σε προηγούμενα δεδομένα. Αυτές οι διαδικασίες συχνά συνδέονται και διαχειρίζονται μαζί, αν και καλύπτουν διαφορετικές ανάγκες.

Οι ανάγκες και η πολιτική που σχετίζονται με τη δημιουργία αντιγράφων ασφαλείας και το αρχείο πρέπει να προσδιορίζονται κατά το στάδιο του σχεδιασμού του συστήματος. Οι βασικές αποφάσεις περιλαμβάνουν εάν τα αντίγραφα ασφαλείας διατηρούνται στο διαδίκτυο ή εκτός σύνδεσης και εάν τα αντίγραφα αποθηκεύονται τοπικά ή μεταφέρονται σε απομακρυσμένο ιστότοπο. Οι αντισταθμίσεις περιλαμβάνουν ευκολία εφαρμογής και κόστους σε σχέση με μεγαλύτερη ασφάλεια και ανθεκτικότητα έναντι διαφορετικών απειλών.

Ένα καλό παράδειγμα των συνεπειών των κακών επιλογών εδώ παρατηρήθηκε στην επίθεση σε έναν Αυστραλό πάροχο φιλοξενίας στις αρχές του 2011. Οι εισβολείς κατέστρεψαν όχι μόνο τα ζωντανά αντίγραφα χιλιάδων ιστότοπων πελατών, αλλά και όλα τα αντίγραφα ασφαλείας στο διαδίκτυο. Ως αποτέλεσμα, πολλοί πελάτες που δεν είχαν τα δικά τους αντίγραφα ασφαλείας έχασαν όλο το περιεχόμενο και τα δεδομένα του ιστότοπού τους, με σοβαρές συνέπειες για πολλούς από αυτούς, καθώς και για τον πάροχο φιλοξενίας. Σε άλλα παραδείγματα, πολλοί οργανισμοί που διατηρούσαν μόνο αντίγραφα ασφαλείας επιτόπου έχουν χάσει όλα τα δεδομένα τους ως αποτέλεσμα πυρκαγιάς ή πλημμύρας στο κέντρο πληροφορικής τους. Αυτοί οι κίνδυνοι πρέπει να αξιολογηθούν κατάλληλα.

3.6. Παράδειγμα ασφάλειας (WINDOWS)

Εξετάζουμε τώρα ορισμένα συγκεκριμένα ζητήματα με την ασφαλή εγκατάσταση, διαμόρφωση και διαχείριση συστημάτων MicrosoftWindows. Αυτά τα συστήματα αποτελούν

εδώ και πολλά χρόνια ένα σημαντικό μέρος όλων των εγκαταστάσεων συστήματος «γενικού σκοπού». Ως εκ τούτου, έχουν στοχοθετηθεί ειδικά από επιτιθέμενους, και κατά συνέπεια απαιτούνται αντίμετρα ασφαλείας για την αντιμετώπιση αυτών των προκλήσεων. Η διαδικασία παροχής κατάλληλων επιπέδων ασφάλειας εξακολουθεί να ακολουθεί τη γενική περιγραφή που περιγράφουμε σε αυτό το κεφάλαιο.

Α) Διαχείριση ενημερωμένων εκδόσεων κώδικα

Η υπηρεσία "WindowsUpdate" και οι "Υπηρεσίες ενημέρωσης διακομιστή των Windows" βοηθούν στην τακτική συντήρηση του λογισμικού της Microsoft και πρέπει να διαμορφωθούν και να χρησιμοποιηθούν. Πολλές άλλες εφαρμογές τρίτων παρέχουν επίσης υποστήριξη αυτόματης ενημέρωσης και αυτές πρέπει να είναι ενεργοποιημένες για επιλεγμένες εφαρμογές.

Β) Διαχείριση χρηστών και έλεγχοι πρόσβασης

Οι χρήστες και οι ομάδες στα συστήματα Windows ορίζονται με ένα αναγνωριστικό ασφαλείας (SID). Αυτές οι πληροφορίες μπορούν να αποθηκευτούν και να χρησιμοποιηθούν τοπικά, σε ένα μόνο σύστημα, στο SecurityAccountManager (SAM). Μπορεί επίσης να διαχειρίζεται κεντρικά για μια ομάδα συστημάτων που ανήκουν σε έναν τομέα, με τις πληροφορίες που παρέχονται από ένα κεντρικό σύστημα ActiveDirectory (AD) χρησιμοποιώντας το πρωτόκολλο LDAP. Οι περισσότεροι οργανισμοί με πολλαπλά συστήματα θα τα διαχειρίζονται χρησιμοποιώντας τομείς. Αυτά τα συστήματα μπορούν επίσης να επιβάλουν κοινή πολιτική για τους χρήστες σε οποιοδήποτε σύστημα στον τομέα.

Τα συστήματα Windows εφαρμόζουν ελέγχους διακριτικής πρόσβασης σε πόρους συστήματος όπως αρχεία, κοινόχρηστη μνήμη και επώνυμους σωλήνες. Η λίστα ελέγχου πρόσβασης έχει έναν αριθμό καταχωρήσεων που ενδέχεται να εκχωρήσουν ή να αρνηθούν δικαιώματα πρόσβασης σε ένα συγκεκριμένο SID, το οποίο μπορεί να είναι για έναν μεμονωμένο χρήστη ή για κάποια ομάδα χρηστών. Τα WindowsVista και νεότερα συστήματα περιλαμβάνουν επίσης υποχρεωτικά στοιχεία ελέγχου ακεραιότητας. Αυτά επισημαίνουν όλα τα

αντικείμενα, όπως διαδικασίες και αρχεία, και όλους τους χρήστες, ως χαμηλό, μεσαίο, υψηλό ή επίπεδο ακεραιότητας συστήματος. Στη συνέχεια, όποτε τα δεδομένα γράφονται σε ένα αντικείμενο, το σύστημα διασφαλίζει πρώτα ότι η ακεραιότητα του θέματος είναι ίση ή υψηλότερη από το επίπεδο του αντικειμένου. Αυτό εφαρμόζει μια μορφή του μοντέλου BibaIntegrity που στοχεύει συγκεκριμένα το ζήτημα του μη αξιόπιστου απομακρυσμένου κώδικα που εκτελείται, για παράδειγμα στον WindowsInternetExplorer, προσπαθώντας να τροποποιήσει τοπικούς πόρους.

Τα συστήματα Windows ορίζουν επίσης προνόμια, τα οποία είναι ευρεία και παραχωρούνται σε λογαριασμούς χρηστών. Παραδείγματα προνομίων περιλαμβάνουν τη δυνατότητα δημιουργίας αντιγράφων ασφαλείας του υπολογιστή (που απαιτεί παράκαμψη των κανονικών ελέγχων πρόσβασης για την απόκτηση πλήρους αντιγράφου ασφαλείας) ή τη δυνατότητα αλλαγής της ώρας του συστήματος. Ορισμένα προνόμια θεωρούνται επικίνδυνα, καθώς ένας εισβολέας μπορεί να τα χρησιμοποιήσει για να καταστρέψει το σύστημα. Ως εκ τούτου, πρέπει να χορηγούνται με προσοχή. Άλλοι θεωρούνται καλοήθεις και ενδέχεται να χορηγούνται σε πολλούς ή όλους τους λογαριασμούς χρηστών.

Όπως με οποιοδήποτε σύστημα, η σκλήρυνση της διαμόρφωσης του συστήματος μπορεί να περιλαμβάνει περαιτέρω περιορισμό των δικαιωμάτων και των προνομίων που παρέχονται σε χρήστες και ομάδες στο σύστημα. Καθώς η λίστα ελέγχου πρόσβασης δίνει μεγαλύτερη προτεραιότητα στις καταχωρήσεις απόρριψης, μπορείτε να ορίσετε μια ρητή άδεια άρνησης για να αποτρέψετε τη μη εξουσιοδοτημένη πρόσβαση σε κάποιο πόρο, ακόμα και αν ο χρήστης είναι μέλος μιας ομάδας που παρέχει διαφορετικά πρόσβαση.

Κατά την πρόσβαση σε αρχεία σε έναν κοινόχρηστο πόρο, ένας συνδυασμός δικαιωμάτων κοινής χρήσης και NTFS μπορεί να χρησιμοποιηθεί για την παροχή πρόσθετης ασφάλειας και λεπτομερειών. Για παράδειγμα, μπορείτε να παραχωρήσετε πλήρη έλεγχο σε μια κοινή χρήση, αλλά πρόσβαση μόνο για ανάγνωση στα αρχεία που περιέχει. Εάν η απαρίθμηση βάσει πρόσβασης είναι ενεργοποιημένη σε κοινόχρηστους πόρους, μπορεί να αποκρύψει αυτόματα τυχόν αντικείμενα που δεν επιτρέπεται να διαβάζει ένας χρήστης. Αυτό είναι χρήσιμο με κοινόχρηστους φακέλους που περιέχουν, για παράδειγμα, τους οικιακούς καταλόγους πολλών χρηστών.

Οι χρήστες θα πρέπει επίσης να διασφαλίζουν ότι τα δικαιώματα διαχείρισης τους χρησιμοποιούν μόνο όταν απαιτείται, και διαφορετικά να έχουν πρόσβαση στο σύστημα ως κανονικός χρήστης. Ο έλεγχος λογαριασμού χρήστη (UAC) που παρέχεται στα Vista και νεότερα συστήματα βοηθά με αυτήν την απαίτηση. Αυτά τα συστήματα παρέχουν επίσης Λογαριασμούς Υπηρεσιών Χαμηλού Προνομίου που μπορούν να χρησιμοποιηθούν για διαδικασίες υπηρεσίας μεγάλης διάρκειας, όπως υπηρεσίες αρχείων, εκτύπωσης και DNS που δεν απαιτούν αυξημένα δικαιώματα.

Γ) Διαμόρφωση εφαρμογής και υπηρεσίας

Μεγάλο μέρος των πληροφοριών διαμόρφωσης στα συστήματα των Windows συγκεντρώνεται στο Μητρώο, το οποίο αποτελεί μια βάση δεδομένων με κλειδιά και τιμές που μπορούν να ερωτηθούν και να ερμηνευθούν από εφαρμογές σε αυτά τα συστήματα.

Αλλαγές σε αυτές τις τιμές μπορούν να γίνουν σε συγκεκριμένες εφαρμογές, ορίζοντας προτιμήσεις στην εφαρμογή που στη συνέχεια αποθηκεύονται στο μητρώο χρησιμοποιώντας τα κατάλληλα κλειδιά και τιμές. Αυτή η προσέγγιση αποκρύπτει τη λεπτομερή αναπαράσταση από τον διαχειριστή. Εναλλακτικά, τα κλειδιά μητρώου μπορούν να τροποποιηθούν απευθείας χρησιμοποιώντας τον "Επεξεργαστή μητρώου". Αυτή η προσέγγιση είναι πιο χρήσιμη για την πραγματοποίηση μαζικών αλλαγών, όπως αυτές που συνιστώνται στους οδηγούς σκλήρυνσης. Αυτές οι αλλαγές μπορούν επίσης να καταγραφούν σε ένα κεντρικό αποθετήριο και να απομακρυνθούν κάθε φορά που ένας χρήστης συνδέεται σε ένα σύστημα εντός τομέα δικτύου.

Δ) Άλλοι έλεγχοι ασφαλείας

Δεδομένης της κυριαρχίας του κακόβουλου λογισμικού που στοχεύει τα συστήματα των Windows, είναι απαραίτητο να εγκατασταθούν και να διαμορφωθούν κατάλληλα πακέτα λογισμικού προστασίας από ιούς, anti-spyware, προσωπικού τείχους προστασίας και άλλων κακόβουλων προγραμμάτων και ανίχνευσης και χειρισμού επιθέσεων. Αυτό είναι σαφώς απαραίτητο για συστήματα συνδεδεμένα στο δίκτυο, όπως φαίνεται από τους αριθμούς υψηλής συχνότητας σε αναφορές όπως το [SYMA13]. Ωστόσο, όπως δείχνουν οι επιθέσεις Stuxnet το

2010, ακόμη και μεμονωμένα συστήματα που ενημερώνονται με αφαιρούμενα μέσα είναι ευάλωτα, και επομένως πρέπει επίσης να προστατευθούν.

Τα σύγχρονα συστήματα Windows περιλαμβάνουν μερικές βασικές δυνατότητες αντιμετώπισης τείχους προστασίας και κακόβουλου λογισμικού, οι οποίες σίγουρα θα πρέπει να χρησιμοποιούνται τουλάχιστον. Ωστόσο, πολλοί οργανισμοί θεωρούν ότι πρέπει να αυξηθούν με ένα ή περισσότερα από τα πολλά διαθέσιμα εμπορικά προϊόντα. Ένα ζήτημα που προκαλεί ανησυχία είναι οι ανεπιθύμητες αλληλεπιδράσεις μεταξύ του ιού και άλλων προϊόντων από πολλούς προμηθευτές. Απαιτείται προσοχή κατά τον σχεδιασμό και την εγκατάσταση τέτοιων προϊόντων για τον εντοπισμό πιθανών ανεπιθύμητων αλληλεπιδράσεων και για να διασφαλιστεί ότι το σύνολο των προϊόντων που χρησιμοποιούνται είναι συμβατά μεταξύ τους.

Τα συστήματα Windows υποστηρίζουν επίσης μια σειρά κρυπτογραφικών λειτουργιών που μπορεί να χρησιμοποιηθούν όπου είναι επιθυμητό. Αυτές περιλαμβάνουν υποστήριξη για κρυπτογράφηση αρχείων και καταλόγων που χρησιμοποιούν το σύστημα αρχείων κρυπτογράφησης (EFS) και για κρυπτογράφηση πλήρους δίσκου με AES χρησιμοποιώντας το BitLocker.

Ε) Δοκιμήασφαλείας

Οι οδηγοί σκλήρυνσης του συστήματος, όπως αυτοί που παρέχονται από το "NSA - SecurityConfigurationGuides" περιλαμβάνουν επίσης λίστες ελέγχου ασφαλείας για διάφορες εκδόσεις των Windows.

Υπάρχουν επίσης πολλά εμπορικά και εργαλεία ανοιχτού κώδικα διαθέσιμα για την εκτέλεση σάρωσης ασφαλείας συστήματος και τον έλεγχο ευπάθειας των συστημάτων Windows. Το "MicrosoftBaselineSecurityAnalyzer" είναι ένα απλό, δωρεάν, εύχρηστο εργαλείο που στοχεύει να βοηθήσει τις μικρομεσαίες επιχειρήσεις να βελτιώσουν την ασφάλεια των συστημάτων τους ελέγχοντας τη συμμόρφωση με τις συστάσεις ασφαλείας της Microsoft. Οι μεγαλύτεροι οργανισμοί πιθανότατα εξυπηρετούνται καλύτερα χρησιμοποιώντας μία από τις μεγαλύτερες, κεντρικές, εμπορικές σουίτες ανάλυσης ασφάλειας που είναι διαθέσιμες.

ΣΥΜΠΕΡΑΣΜΑΤΑ

Η σημερινή τεχνολογία, μας προσφέρει διάφορα μέσα προστασίας. Πολλά από αυτά είναι απλά στην υλοποίησή τους και έχουν μικρό κόστος, ενώ άλλα είναι πολύπλοκα και έχουν κόστος αρκετά υψηλό. Όταν λοιπόν σχεδιάζουμε την ασφάλεια ενός πληροφοριακού συστήματος, επιλέγουμε ποια και πόσα από αυτά τα μέσα θα πρέπει να χρησιμοποιηθούν, ώστε να διασφαλίσουμε τη σωστή και αδιάκοπη λειτουργία του πληροφοριακού συστήματος.

Όπως είναι γνωστό, είναι αδύνατο να υπάρξει ένα τέλειο σύστημα ασφαλείας, το οποίο να μπορεί να μας διασφαλίσει από κάθε κίνδυνο. Υπάρχει λοιπόν η ανάγκη για κάθε μεθόδους και τεχνικές, οι οποίες μας βοηθούν στο να ξεκαθαρίσουμε το τι πρέπει και τι αξίζει να διαφυλάξουμε.

Στο 1ο Κεφάλαιο αναλύθηκαν γενικά τα υπολογιστικά συστήματα και οι ευπάθειες τους, ενώ στο 2ο Κεφάλαιο διερευνήθηκαν, υπογραμμίστηκαν και επεξηγήθηκαν πολλές από τις ευπάθειες (vulnerabilities) που μπορούν να βλάψουν ένα υπολογιστικό σύστημα, καθώς επίσης και μερικοί από τους τρόπους που είναι ικανοί να αντιμετωπίσουν αυτές τις ευπάθειες και να προλάβουν την κακόβουλη χρήση τους.

Τέλος στο 3ο Κεφάλαιο, αναλύθηκε η λειτουργική ασφάλεια των συστημάτων καθώς είναι η κύρια υπεύθυνη για την προστασία ενός πληροφοριακού συστήματος και δόθηκε παράδειγμααασφαλείας των Windowsγια να γίνει πιο προσιτό στον αναγνώστη.

Βιβλιογραφία

- [AYCO06] = Aycock, J. Computer Viruses and Malware. New York: Springer, 2006.
- [CASS01] = Cass, S. “Anatomy of Malice.” IEEE Spectrum, November 2001.
- [EMBL08] =Embleton, S.; Sparks, S.; and Zou, C. “SMM Rootkits: A New Breed of OS-Independent Malware.” Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, ACM, September 2008.
- [GEER06] = Geer, D. “Hackers Get to the Root of the Problem.” Computer, May 2006.
- [HOLZ05] =Holz, T. “A Short Visit to the Bot Zoo.” IEEE Security and Privacy, January–February 2005.
- [HYPP06] =Hypponen, M. “Malware Goes Mobile.” Scientific American, November 2006.
- [KEPH97] = Kephart, J.; Sorkin, G.; Chess, D.; and White, S. “Fighting Computer Viruses.” Scientific American, November 1997.
- [LEVI04] = Levine, J.; Grizzard, J.; and Owen, H. “A Methodology to Detect and Characterize Kernel Level Rootkit Exploits Involving Redirection of the System Call Table.” Proceedings, Second IEEE International Information Assurance Workshop, 2004.
- [LEVI06] = Levine, J.; Grizzard, J.; and Owen, H. “Detecting and Categorizing KernelLevel Rootkits to Aid Future Detection.” IEEE Security and Privacy, January–February 2006.
- [MAND13] = Mandiant “APT1: Exposing One of China’s Cyber Espionage Units,” 2013.
- [MCLA04] = McLaughlin, L. “Bot Software Spreads, Causes New Worries.” IEEE Distributed Systems Online, June 2004.
- [MOOR02] = Moore, D.; Shannon, C.; and Claffy, K. “Code-Red: A Case Study on the Spread and Victims of an Internet Worm.” Proceedings of the 2nd ACM SIGCOMM Workshop on Internet Measurement, November 2002.
- [NACH97] =Nachenberg, C. “Computer Virus-Antivirus Coevolution.” Communications of the ACM, January 1997.

- [SCAR08] =Scarfone, K.; Jansen, W.; and Tracy, M. Guide to General Server Security, NIST Special Publication 800-123, July 2008
- [SOUP13] =Souppaya, M., and Scarfone, K. Guide to Malware Incident Prevention and Handling for Desktops and Laptops. NIST Special Publication SP 800-83, July 2013.
- [SYMA13] = Symantec, “Internet Security Threat Report, Vol. 18.” April 2013.
- [SZOR05] =Szor, P. The Art of Computer Virus Research and Defense. Reading, MA: Addison-Wesley, 2005.
- [WEAV03] = Weaver, N., et al. “A Taxonomy of Computer Worms.” The First ACM Workshop on Rapid Malcode (WORM), 2003.
- [ZHOU12] = Zhou, Y.; and Jiang, X. “Dissecting Android Malware: Characterization and Evolution” Proceedings of the 33rd IEEE Symposium on Security and Privacy, May 2012.