

7 – Κυβερνοεπιθέσεις ευρείας κλίμακας

Εθνική Σχολή Δημόσιας Διοίκησης & Αυτοδιοίκησης
Μάιος 2021

Ενότητες

- ▶ Η Περίπτωση του Ιομορφικού Λογισμικού Flame
- ▶ Ανάλυση Χαρακτηριστικών και Ταξινόμηση
- ▶ Συμπεράσματα

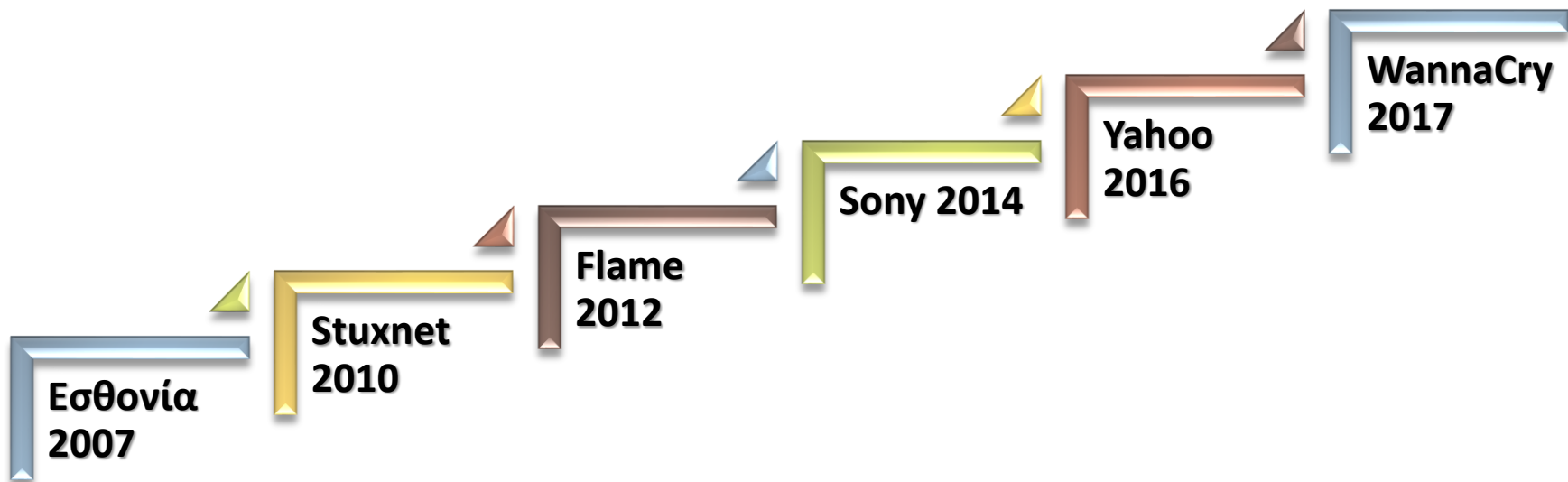
Εισαγωγή

- ▶ Το **Διαδίκτυο** αποτελεί το πέμπτο πεδίο συγκρούσεων και επίδειξης ισχύος σε διεθνή κλίμακα, το οποίο έρχεται να προστεθεί στα τέσσερα παραδοσιακά πεδία πολεμικών επιχειρήσεων: **ξηρά, θάλασσα, αέρας και διάστημα**

Εισαγωγή

- ▶ Απαιτείται μια νέα **μεθοδολογική προσέγγιση** στην προστασία της πληροφορίας η οποία θα πρέπει να περιλαμβάνει διαφορετικές διαστάσεις σε:
 - ▶ πολιτικό
 - ▶ νομικό
 - ▶ οργανωτικό
 - ▶ τεχνολογικό επίπεδο

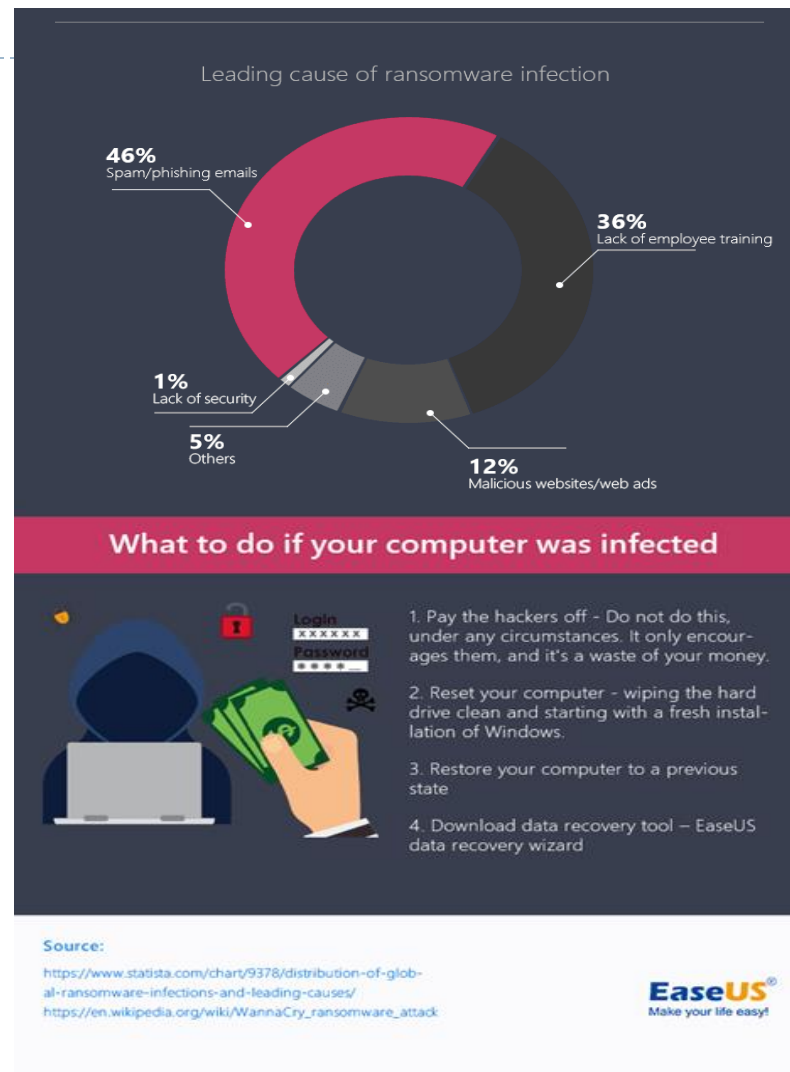
Κυβερνοεπιθέσεις



WannaCry

- ▶ **Ransomware** που προσέβαλε πάνω από 230.000 υπολογιστές σε περισσότερα από 150 κράτη το 2017, στοχεύοντας το λειτουργικό σύστημα των Windows
- ▶ Προκάλεσε σημαντικά προβλήματα στο Εθνικό Σύστημα Υγείας της Αγγλίας
- ▶ Κρυπτογραφούσε τα δεδομένα του υπολογιστή ζητώντας Bitcoins

Malware / RANSOMWARE : “WannaCry”



Yahoo

- ▶ Το 2016 η εταιρία ανακοίνωσε πως το 2014 σημειώθηκε περιστατικό παραβίασης 500 εκ. λογαριασμών χρηστών
- ▶ Ο επιτιθέμενος απέσπασε ονόματα χρηστών, κωδικούς πρόσβασης και στοιχεία επικοινωνίας
- ▶ Η Yahoo προέτρεψε τους χρήστες των υπηρεσιών της να δημιουργήσουν νέους κωδικούς πρόσβασης

Sony

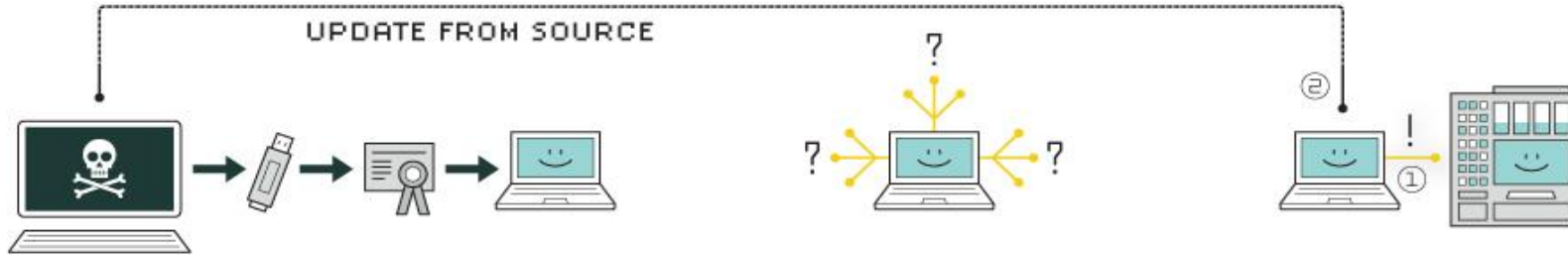
- ▶ Το 2014 σημειώθηκε υποκλοπή δεδομένων από τους εξυπηρετητές της Sony Pictures από τους hackers Guardians of Peace
- ▶ Τα δεδομένα αφορούσαν προσωπικά στοιχεία εργαζομένων, μηνύματα ηλεκτρονικού ταχυδρομείου, αρχεία μισθοδοσίας και υλικό ταινιών που δεν είχαν ακόμη βγει στην αγορά
- ▶ Οι δράστες ζήτησαν να μην προβληθεί στις αίθουσες η ταινία «The Interview», που αφορούσε τη δολοφονία του ηγέτη της Βόρειας Κορέας

Stuxnet

- ▶ Κυβερνοεπίθεση το 2010 με στόχο τα βιομηχανικά συστήματα αυτοματισμού SCADA του πυρηνικού προγράμματος του Ιράν
- ▶ Η ιομορφή προσβάλλει το λειτουργικό σύστημα των Windows με στόχο λογισμικό λειτουργίας των συσκευών φυγοκέντρισης της Siemens
- ▶ Αρχικά διαδίδεται μέσω USB και εξαπλώνεται μέσω δικτύου

HOW STUXNET WORKED

UPDATE FROM SOURCE



1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

Stuxnet raises the spin rate to 1410Hz for 15 mins.

Then sleeps for 27 days.

Then slows the spin rate to 2Hz for 50 mins.

Then sleeps for 27 days.

Stuxnet repeats this process over and over.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.

5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

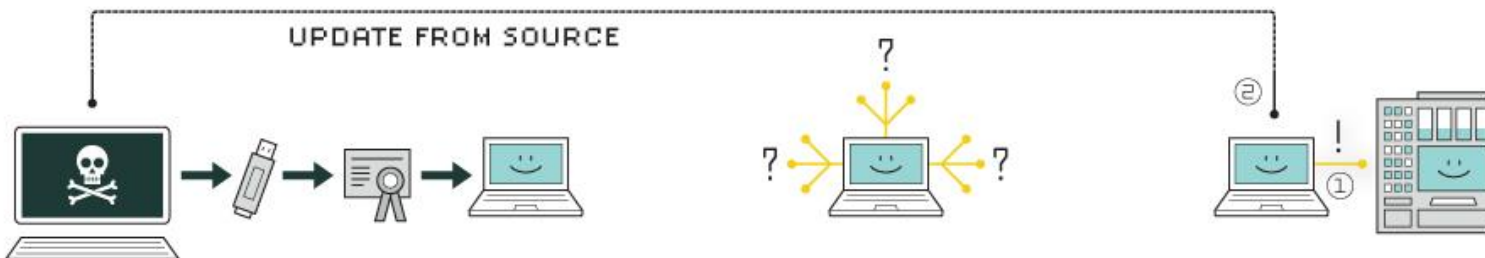
6. deceive and destroy

Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Αξιοποίηση 3 0-day exploits & 2 κλεμμένα digital certificates από Taiwan

HOW STUXNET WORKED

UPDATE FROM SOURCE



1. infection

WORM:

Χρήση αληθοφανούς
Πιστοποιητικού (Taiwan)
Μετάδοση μέσω USB

2. search

Είναι σε H/Y Siemens SCADA?
ΟΧΙ: αναμετάδοση μέσω USB

3. update

H/Y Siemens SCADA
Σύνδεση Internet ?
UPDATE + Λήψη εντολών



4. compromise

3 x ZERO-DAY τρωτότητες

5. control

Παρακολούθηση λειτουργίας
Συλλογή δεδομένων

6. deceive and destroy

Ψευδή στοιχεία
λειτουργίας
«Υπερφόρτωση»

Stuxnet raises the spin rate
to 1410Hz for 15 mins.

Then sleeps for 27 days.

Then slows the spin rate
to 2Hz for 50 mins.

Then sleeps for 27 days.

Stuxnet repeats this
process over and over.

Αξιοποίηση 3 0-day exploits & 2 κλεμμένα digital certificates από Taiwan

Εσθονία

- ▶ Κυβερνοεπίθεση DDoS ευρείας κλίμακας στην Εσθονία το 2007, διάρκειας τριών εβδομάδων, με στόχο την πλήρη κατάρρευση των υποδομών του κράτους
- ▶ Η επίθεση αποδόθηκε στη Ρωσία, ωστόσο δεν ήταν δυνατόν να εξακριβωθεί εάν πίσω από αυτήν βρισκόταν η ρωσική κυβέρνηση ή hackers που έδρασαν αυτόνομα

Ιομορφικό Λογισμικό Flame

- ▶ Αποτελεί ένα από τα πιο εξελιγμένα κακόβουλα προγράμματα που έχουν γραφτεί ποτέ
- ▶ Χρησιμοποιήθηκε ως ένα ολοκληρωμένο εργαλείο διεθνής κατασκοπείας στον κυβερνοχώρο
- ▶ Μεταδίδεται μέσω τοπικών δικτύων υπολογιστών ή μέσω USB sticks και μπορεί να καταγράψει ήχο, οθόνη, πληκτρολόγηση και δικτυακή κίνηση
- ▶ Επίσης, μπορεί να καταγράψει συζητήσεις που διεξάγονται μέσω Skype

Ιομορφικό Λογισμικό Flame

- ▶ Αποκαλύφθηκε το **Μάιο του 2012** όταν η Διεθνής Ένωση Τηλεπικοινωνιών (International Telecommunication Union – ITU) ζήτησε από την εταιρία **Kaspersky** να εξετάσει αναφορές από χώρες της Μέσης Ανατολής σχετικά με περιστατικά προσβολής της ασφάλειας πληροφοριακών συστημάτων από ιομορφικό λογισμικό

Ιομορφικό Λογισμικό Flame

- ▶ Ονομάστηκε **Flame** από το όνομα μίας από τις κύριες λειτουργικές του μονάδες
- ▶ Χρησιμοποιήθηκε αρχικά το 2010
- ▶ Η ανάπτυξη της πλατφόρμας του κώδικα των **Command & Control (C&C) servers** ξεκίνησε το 2006

Ανάλυση Χαρακτηριστικών & Ταξινόμηση

- ▶ Ο Flame είναι ένα **εργαλείο κατασκοπείας** στον **κυβερνοχώρο**, το οποίο δίνει τη δυνατότητα στον επιτιθέμενο να υποκλέψει μία πληθώρα δεδομένων από το στόχο του

Κύρια Χαρακτηριστικά

- ▶ Διαθέτει **αρθρωτή δομή** που περιλαμβάνει πλούσια συλλογή τεχνολογιών κατασκοπείας σε μία και μόνο ιομορφή
- ▶ Στοχεύει σε συστήματα με λειτουργικό σύστημα **Microsoft Windows** και ενσωματώνει πολλαπλές τεχνικές διάδοσης, επίθεσης και ενσωμάτωσης κώδικα

Δυνατότητες

Δυνατότητα αποτύπωσης πληκτρολογήσεων

Λήψη στιγμιότυπων της οθόνης ανά τακτά χρονικά διαστήματα

Ενεργοποίηση του μικροφώνου και της κάμερας για καταγραφή

Αναζήτηση στα αποθηκευτικά μέσα συνδεδεμένα με τον υπολογιστή

Παρακολούθηση και καταγραφή της δικτυακής κίνησης

Ενεργοποίηση Bluetooth για καταγραφή γειτονικών συσκευών

Χρήση του Bluetooth για την αποστολή δεδομένων

Κύρια Χαρακτηριστικά

- ▶ Λόγω του ότι καταλαμβάνει μεγάλο χώρο στο δίσκο, προστίθεται στο σύστημα στόχο **τμηματικά**
- ▶ Το κύριο συστατικό του που προσβάλλει ένα σύστημα έχει μέγεθος 6 MB και περιλαμβάνει μία σειρά από λειτουργικές μονάδες σε **συμπιεσμένη μορφή**

Κύρια Χαρακτηριστικά

- ▶ Μετά την εγκατάσταση του κύριου συστατικού στο σύστημα, αυτό **αποκρυπτογραφεί** και **αποσυμπιέζει** τις λειτουργικές μονάδες που περιλαμβάνει και τις τοποθετεί σε διάφορα σημεία του δίσκου
- ▶ Ο αριθμός των λειτουργικών μονάδων της κάθε μόλυνσης εξαρτάται από τους σκοπούς της παρακολούθησης του κάθε στόχου
- ▶ Στην πλήρη ανάπτυξή της η ιομορφή μπορεί να φτάσει έως και τα 20 MB

Κύρια Χαρακτηριστικά

- ▶ Χρησιμοποιεί τεχνικές **συμπίεσης** και **κρυπτογράφησης** προκειμένου να αποκρύψει τα αρχεία του
- ▶ Έχουν εντοπιστεί 5 διαφορετικές μέθοδοι κρυπτογράφησης (και παραλλαγές τους), 3 διαφορετικές τεχνικές συμπίεσης και τουλάχιστον 5 διαφορετικές μορφές αρχείων

Κύρια Χαρακτηριστικά

- ▶ Χρησιμοποιεί βάσεις δεδομένων SQLite και τις άγνωστες βάσεις δεδομένων CLAN, για την αποθήκευση ορισμένων από τις πληροφορίες που συγκεντρώνει

Κύρια Χαρακτηριστικά

- ▶ Χρησιμοποιεί μηχανισμούς ενσωμάτωσης κώδικα στις εκτελούμενες διεργασίες του συστήματος (όπως winlogon, services και explorer), οι οποίες δεν επιτρέπουν τον εντοπισμό του ενσωματωμένου κώδικα με τη χρήση κλασσικών μεθόδων, όπως την απαρίθμηση των λειτουργικών μονάδων της κάθε διεργασίας
- ▶ Οι σελίδες της μνήμης που χρησιμοποιεί είναι προστατευμένες με δικαιώματα READ, WRITE και EXECUTE έτσι ώστε να είναι απροσπέλαστες από τις εφαρμογές των χρηστών

Κύρια Χαρακτηριστικά

- ▶ Ελέγχει την παρουσία περισσοτέρων από 300 προϊόντων ασφάλειας τα οποία θα μπορούσαν να τον ανιχνεύσουν και τροποποιεί ανάλογα τη συμπεριφορά του, έτσι ώστε να αποφευχθεί ο εντοπισμός του
- ▶ Για παράδειγμα, ενώ συνήθως χρησιμοποιεί την επέκταση .ocx, στην περίπτωση που είναι εγκατεστημένο το McAfee Shield αλλάζει τις επεκτάσεις των αρχείων του σε .tmp

Κύρια Χαρακτηριστικά

- ▶ Διαθέτει ποικίλες μορφές αυτοαναπαραγωγής και εξάπλωσης σε τοπικά δίκτυα και USB sticks
- ▶ Δημιουργεί λογαριασμούς κερκόπορτες στους μολυσμένους υπολογιστές, εφόσον είναι διαθέσιμα τα απαραίτητα δικαιώματα

Κύρια Χαρακτηριστικά

- ▶ Τα δεδομένα που συγκεντρώνει αποστέλλονται κρυπτογραφημένα σε απομακρυσμένους **Command & Control (C&C) Servers** χρησιμοποιώντας το πρωτόκολλο SSL, εφόσον υπάρχει διαθέσιμη διαδικτυακή σύνδεση
- ▶ Σε αντίθετη περίπτωση, τα συγκεντρωμένα δεδομένα μπορούν να αποσταλούν σε USB sticks, μέσω των οποίων μπορούν να μολυνθούν άλλοι υπολογιστές των οποίων η διαδικτυακή σύνδεση χρησιμοποιείται για την επικοινωνία με τους C&C Servers

Κύρια Χαρακτηριστικά

- ▶ Αξιοποιεί την scripting γλώσσα προγραμματισμού LUA για τη συγγραφή τμημάτων της ιομορφής και ενσωματώνει έναν διερμηνέα της γλώσσας, που επιτρέπει στους επιτιθέμενους να εμπλουτίσουν την λειτουργικότητά της μέσω διαφόρων scripts τα οποία αποστέλλονται από τους C&C Servers στους μολυσμένους υπολογιστές

Κύρια Χαρακτηριστικά

- ▶ Οι επιτιθέμενοι είναι σε θέση να αποστείλουν μία λειτουργική μονάδα “αυτοκτονίας” της ιομορφής, στην περίπτωση που αυτό καταστεί αναγκαίο
- ▶ Η λειτουργική αυτή μονάδα (browse32) εντοπίζει όλα τα ίχνη της ιομορφής, περιλαμβανομένων των αρχείων που περιλαμβάνουν τα δεδομένα που έχουν υποκλαπεί, και τα καταστρέφει

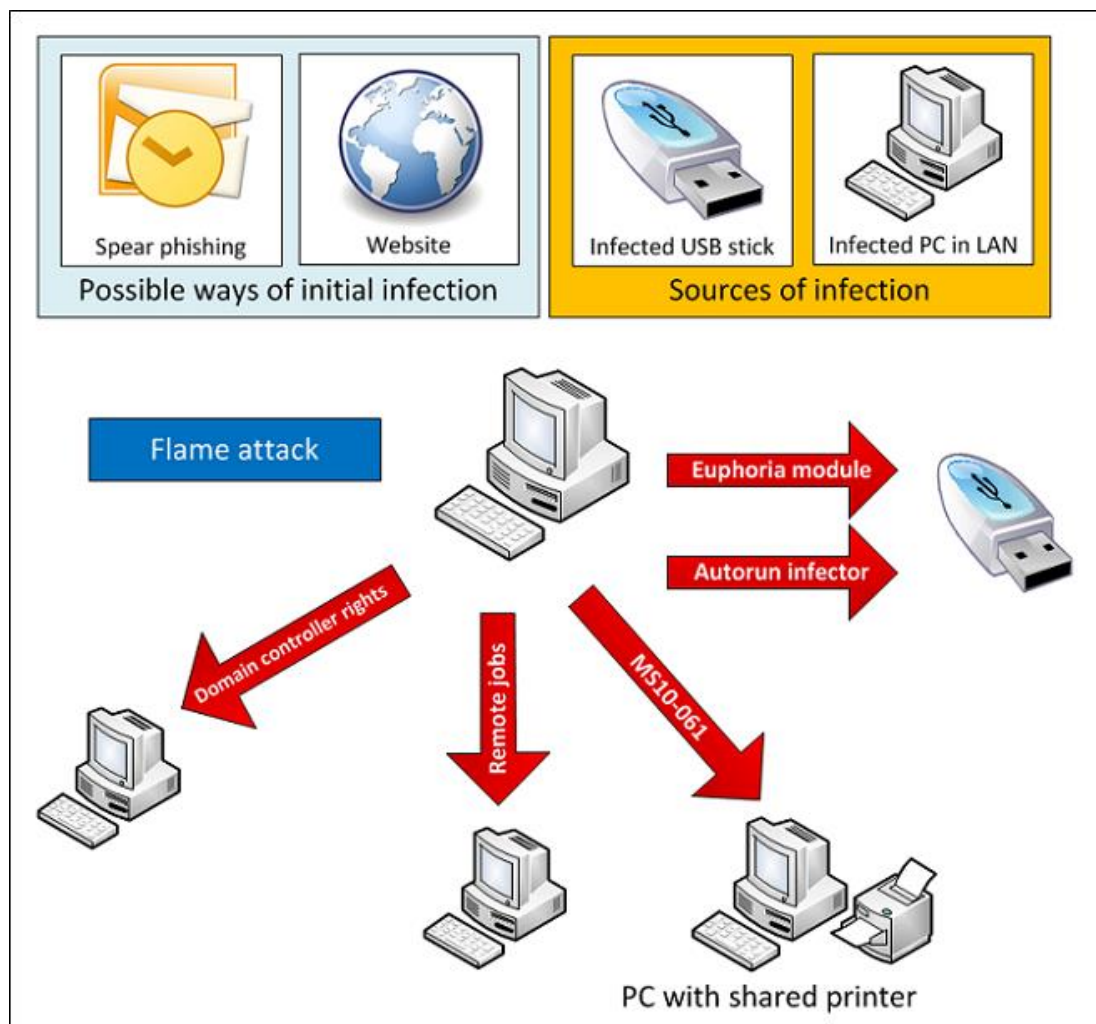
Κύρια Χαρακτηριστικά

- ▶ Οι λειτουργικές μονάδες του Flame έχουν τη δυνατότητα να συγκεντρώνουν έναν εξαιρετικά μεγάλο όγκο πληροφοριών από τον υπολογιστή που έχει προσβάλει, ο οποίος υπερβαίνει κατά πολύ τον όγκο πληροφοριών που μπορεί να συγκεντρωθεί από ιομορφές του παρελθόντος

Κύρια Χαρακτηριστικά

- ▶ Ο Flame μπορεί να συλλέξει μεταδεδομένα αρχείων και στη συνέχεια ο επιτιθέμενος, βάσει αυτών των πληροφοριών, να επιλέξει να υποκλέψει μόνο τα αρχεία που τον ενδιαφέρουν
- ▶ Το τεράστιο εύρος των λειτουργιών και το μέγεθός του τον κάνει να ξεχωρίζει από άλλα εργαλεία κατασκοπείας

Μέθοδοι Εξάπλωσης του Flame



Ταξινόμηση

- ▶ Ο Flame μπορεί να ταξινομηθεί κυρίως ως **Αναπαραγωγός**, λόγω του ότι διαθέτει το χαρακτηριστικό της αυτοαναπαραγωγής, ενώ ταυτόχρονα δεν απαιτείται για την αναπαραγωγή του η ενεργοποίηση κάποιου άλλου λογικού αντικειμένου (ξενιστής)

Ταξινόμηση

- ▶ Εξαιτίας της δυνατότητάς του να δημιουργεί λογαριασμούς κερκόπορτες, διαθέτει και τα χαρακτηριστικά **κερκόπορτας**
- ▶ Η δυνατότητα που έχει να εξαπλώνεται μέσω της παραβίασης του μηχανισμού Windows Update του προσδίδει και τα χαρακτηριστικά **Δούρειου Ίππου**

Συμπεράσματα

- ▶ Ο Flame είναι μία χαρακτηριστική περίπτωση ανάδειξης της ανεπάρκειας που διακρίνει τα παραδοσιακά συστήματα ασφάλειας, αναφορικά με την **προστασία κρίσιμων υποδομών**
- ▶ Το κυβερνοέγκλημα εξελίσσεται διαρκώς και επινοεί νέους τρόπους **παρακάμψης** των μηχανισμών ασφάλειας
- ▶ Οποιαδήποτε ιομορφή είναι καινούργια και άγνωστη, είναι πολύ πιθανό να καταφέρει να **παρακάμψει** τα παραδοσιακά συστήματα ασφάλειας

Συμπεράσματα

- ▶ Η πρακτική της λήψης μέτρων προστασίας κατόπιν της αναγνώρισης και επιβεβαίωσης των ιομορφικών προσβολών είναι ένα ξεπερασμένο μοντέλο, καθώς δίνει τη δυνατότητα στους επιτιθέμενους που χρησιμοποιούν μία νέα μέθοδο να πραγματοποιούν με επιτυχία τις επιθέσεις τους έως ότου γίνουν αντιληπτοί, αναγνωριστούν οι τεχνικές δράσης τους και ληφθεί ένα νέο μέτρο ασφάλειας
- ▶ Μέχρι τότε **όμως η ζημιά έχει ήδη γίνει**

Συμπεράσματα

- ▶ Ο ενδεδειγμένος τρόπος αντιμετώπισης, ειδικά για την προστασία κρίσιμων υποδομών, είναι η υιοθέτηση μίας **προληπτικής προσέγγισης**, μέσω του αυστηρού ελέγχου των εφαρμογών που εγκαθίστανται και εκτελούνται στα συστήματα και διατήρησης μίας whitelist με τις εγκεκριμένες εφαρμογές

Συμπεράσματα

- ▶ Υιοθετώντας μία **προσέγγιση άρνησης εκτέλεσης εξ ορισμού** (autorun) οποιουδήποτε λογισμικού δεν περιλαμβάνεται στη λίστα των εγκεκριμένων εφαρμογών, δεν θα επέτρεπε την εκτέλεση ιομορφών όπως ο Flame, ανεξάρτητα εάν αυτές εμφανίζονται ως αξιόπιστες και ψηφιακά υπογεγραμμένες
- ▶ Σε αντίθεση με τη λογική των παραδοσιακών ανιχνευτών ιών, η προσέγγιση του **whitelist** δίνει τη δυνατότητα στους διαχειριστές να ελέγχουν με λεπτομέρεια τις εφαρμογές που εκτελούνται σε κάθε σύστημα

Συμπεράσματα

- ▶ Εξετάζοντας την περίπτωση του Flame, παρατηρείται ένα μεγάλο χάσμα αναφορικά με τις πληροφορίες και γνώσεις που έχουν στη διάθεσή τους οι επιτιθέμενοι σε σχέση με τα θύματα της επίθεσης
- ▶ Η εγκατάσταση και λειτουργία ενός κατανεμημένου δικτύου από **honeypots** θα μπορούσε να συμβάλει στην ανίχνευση συντονισμένων επιθέσεων με τη συλλογή στοιχείων αναφορικά με τις νέες ιομορφικές προσβολές που θα εντοπίζονται εγκαίρως

Συμπεράσματα

- ▶ Ο Flame αποτελεί τμήμα μιας ευρύτερης επίθεσης και παρέμεινε ενεργός για ένα μεγάλο χρονικό διάστημα πριν αποκαλυφθεί από τους ερευνητές
- ▶ Αυτό οφείλεται στο γεγονός ότι δεν προκαλεί ορατές επιπλοκές στα συστήματα που προσβάλλει, χρησιμοποιώντας παράλληλα τεχνικές συμπίεσης και κρυπτογράφησης

Συμπεράσματα

- ▶ Ο Flame υποκλέπτει πληροφορίες με πολλαπλούς τρόπους και χρησιμοποιεί διάφορα εναλλακτικά μέσα επικοινωνίας για τη μετάδοση των πληροφοριών που συλλέγει στους επιτιθέμενους, καθώς και την αποστολή από αυτούς νέων τμημάτων κώδικα και εντολών

Συμπεράσματα

- ▶ Ένας έμπειρος διαχειριστής με τη χρήση κατάλληλων εργαλείων θα μπορούσε να είχε εντοπίσει τις ανωμαλίες που επιφέρει η εγκατάσταση του Flame στα συστήματα που έχει υπό την εποπτεία του
- ▶ Η αυστηρή συνεχής παρακολούθηση και οι τακτικοί έλεγχοι ορθής λειτουργίας πληροφοριακών συστημάτων και δικτύων αποτελούν βασική γραμμή άμυνας έναντι των κυβερνοεπιθέσεων

Ευχαριστώ για την προσοχή σας

Ερωτήσεις

