Ασφάλεια Τηλεπικοινωνιακών Συστημάτων

Ασφάλεια διαδικτύου: Hacking, Hactivism, e-booling, trafficking, fake e-business, impersonation, ransomwares, κλοπή ψηφιακής ταυτότητας κοινωνικού δικτύου (πχ να κλαπεί η ταυτότητα ενός χρήστη και να αρχίσουν μέσω αυτής να εκτίθενται εικόνες που τον διαβάλλουν).

Διαδίκτυο:

1. Υποδομές παροχής πληροφορίας
-Whatever-pedia
-eBooks
-sites offering how to...
-Pictures shares
-News
-ePress
Etc

2. Υποδομές Παροχής Υπηρεσιών
-VoIP
-TvoIP
-eGoverment
-eClass
-ePresence
-eService

3. Νεφοϋπολογιστικές Υπηρεσίες
-Cloud Computing
-Cloud Service
-Cloud whatever

Δεδομένα (Data):

1. Data is:
Aggregated
Concentrated

2. Data is:
Transmitted
Processed
Aggregated
Concentrated

3. Data is:
Distributed
Transmitted
Processed
Aggregated

Κίνδυνοι στο διαδίκτυο

1. Ιοί
2. Σκουλήκια
3. Δούρειοι Ίπποι
4. Κερκόπορτες
5. Bots
6. ransomwares
7. rootkits
8. keyloggers

etc

Κακόβουλο Λογισμικό

Απειλές στο διαδίκτυο

1. Ψάρεμα
2. Απάτη
3. Πλαστοπροσωπεία
4. Κλοπή προσωπικών δεδομένων
5. Κλοπή περιουσιακών στοιχείων

-οικονομικά δεδομένα

-πνευματικά δεδομένα

6. Κυβερνοπειρατεία
7. Κυβερνο-ακτιβισμός
8. Κυβερνοέγκλημα
9. Κυβερνοτρομοκρατία

Ιός - virus

Λογισμικό εκτελέσιμου προγράμματος

1. **Χαρακτηριστικά**:
α. Αόρατο από το λειτουργικό σύστημα / χρήστη
β. Κρυφή Λειτουργικότητα
γ. Αναπαραγωγή, διασπορά, διάδοση σε άλλα λογισμικά του Η/Υ ερήμην του χρήστη
δ. ύπνωση / ενσωμάτωσή του σε νόμιμα λογισμικά

2. **Σκοπός**
α. Αθώα επιβεβαίωση του κατασκευαστή
β. Δολιοφθορά
γ. Στοχευμένη επίθεση
δ. κλοπή ευαίσθητων προσωπικών δεδομένων

3. **Εύρος διάδοσης**
α. Προσωπικοί Υπολογιστές / προσωπικές συσκευές
β. Δίκτυα υπολογιστικών συστημάτων (μεγάλα, μεσαία, μικρά)
γ. Εξυπηρετητές δικτύων
δ. Εξυπηρετητές Ηλεκτρονικού Ταχυδρομείου

Σκουλήκι - Worm

Αυτόνομο λογισμικό εκτελέσιμου προγράμματος

1. **Χαρακτηριστικά**:
α. Αόρατο από λειτουργικά συστήματα
β. Λειτουργικότητα
γ. Αναπαραγωγή, διασπορά, διάδοση σε άλλους Η/Υ
δ. ύπνωση / ενσωμάτωσή του σε νόμιμα λογισμικά

2. **Σκοπός**
α. Αθώα επιβεβαίωση του κατασκευαστή
β. Δολιοφθορά
γ. Διάδοση σε όσο το δυνατόν περισσότερα υπολογιστικά συστήματα
δ. κλοπή ευαίσθητων προσωπικών δεδομένων
ε. Κατασκευή coverts

3. **Εύρος διάδοσης**
α. Δίκτυα υπολογιστικών συστημάτων (μεγάλα, μεσαία, μικρά)

Δούρειοι Ίπποι – Trojan Horses

Αυτόνομο λογισμικό εκτελέσιμου προγράμματος, που συνήθως παραπλανά τους χρήστες του, καθώς διαφημίζεται για άλλη χρήση από αυτήν που κάνει

1. **Χαρακτηριστικά**:
α. Ορατό Λογισμικό
β. Κρυφή λειτουργικότητα που ενδεχομένως να συνυπάρχει με την διαφημιζόμενη

2. **Σκοπός**
α. Καταλογισμός ευθύνης για πειρατικό λογισμικό
β. Κλοπή ευαίσθητων προσωπικών δεδομένων
γ. Κυβερνοέγκλημα
δ. Κυβερνοτρομοκρατία
κοκ

3. **Εύρος διάδοσης**
α. Προσωπικοί Υπολογιστές / προσωπικές συσκευές
β. Δίκτυα υπολογιστικών συστημάτων (μεγάλα, μεσαία, μικρά)
γ. Εξυπηρετητές δικτύων
δ. Εξυπηρετητές Ηλεκτρονικού Ταχυδρομείου

Λογισμικό κατάσκοπος – Spyware

Κακόβουλο λογισμικό που έχει στόχο να συλλέξει κρυφά πληροφορίες για ένα πρόσωπο ή έναν οργανισμό, χωρίς τη γνώση τους, και στη συνέχεια ενδεχομένως να στείλει αυτές τις πληροφορίες σε μια τρίτη οντότητα, χωρίς την συγκατάθεσή τους.

1. **Χαρακτηριστικά**:
α. Αόρατο / κρυφό Λογισμικό
β. Κρυφή λειτουργικότητα
γ.

2. **Σκοπός**
α. Κλοπή ευαίσθητων προσωπικών δεδομένων
β. Κατασκοπεία

3. **Εύρος διάδοσης**
α. Προσωπικοί Υπολογιστές / προσωπικές συσκευές

Παράνομοι Διαφημιστές – Adware

Κακόβουλο λογισμικό που έχει στόχο να εισαγάγει, διασπείρει και ενσωματώσει διαφημίσεις σε άλλα λογισμικά, χωρίς την επίγνωση ή τη συγκατάθεση των νόμιμων χρηστών τους.

1. **Χαρακτηριστικά**:
α. Αόρατο / κρυφό Λογισμικό
β. Κρυφή λειτουργικότητα

2. **Σκοπός**
α. Διασπορά διαφημίσεων

3. **Εύρος διάδοσης**
α. Προσωπικοί Υπολογιστές / προσωπικές συσκευές

Αντικλείδια – rootkits

Κακόβουλο λογισμικό που έχει στόχο να δώσει πρόσβαση σε μη εξουσιοδοτημένους χρήστες για δεδομένα, λογισμικό, ή λειτουργίες που υπό κανονικές συνθήκες δεν έχουν.

1. **Χαρακτηριστικά**:
α. Αόρατο / κρυφό Λογισμικό
β. Κρυφή λειτουργικότητα

2. **Σκοπός**
α. Απόδοση δικαιωμάτων για λογισμικά, υπηρεσίες
β. ξεκλείδωμα Η/Υ
γ. Πρόσβαση σε δεδομένα

3. **Εύρος διάδοσης**
α. Προσωπικοί Υπολογιστές / προσωπικές συσκευές
β. Δίκτυα υπολογιστικών συστημάτων (μεγάλα, μεσαία, μικρά)

Κερκόπορτες – Backdoors

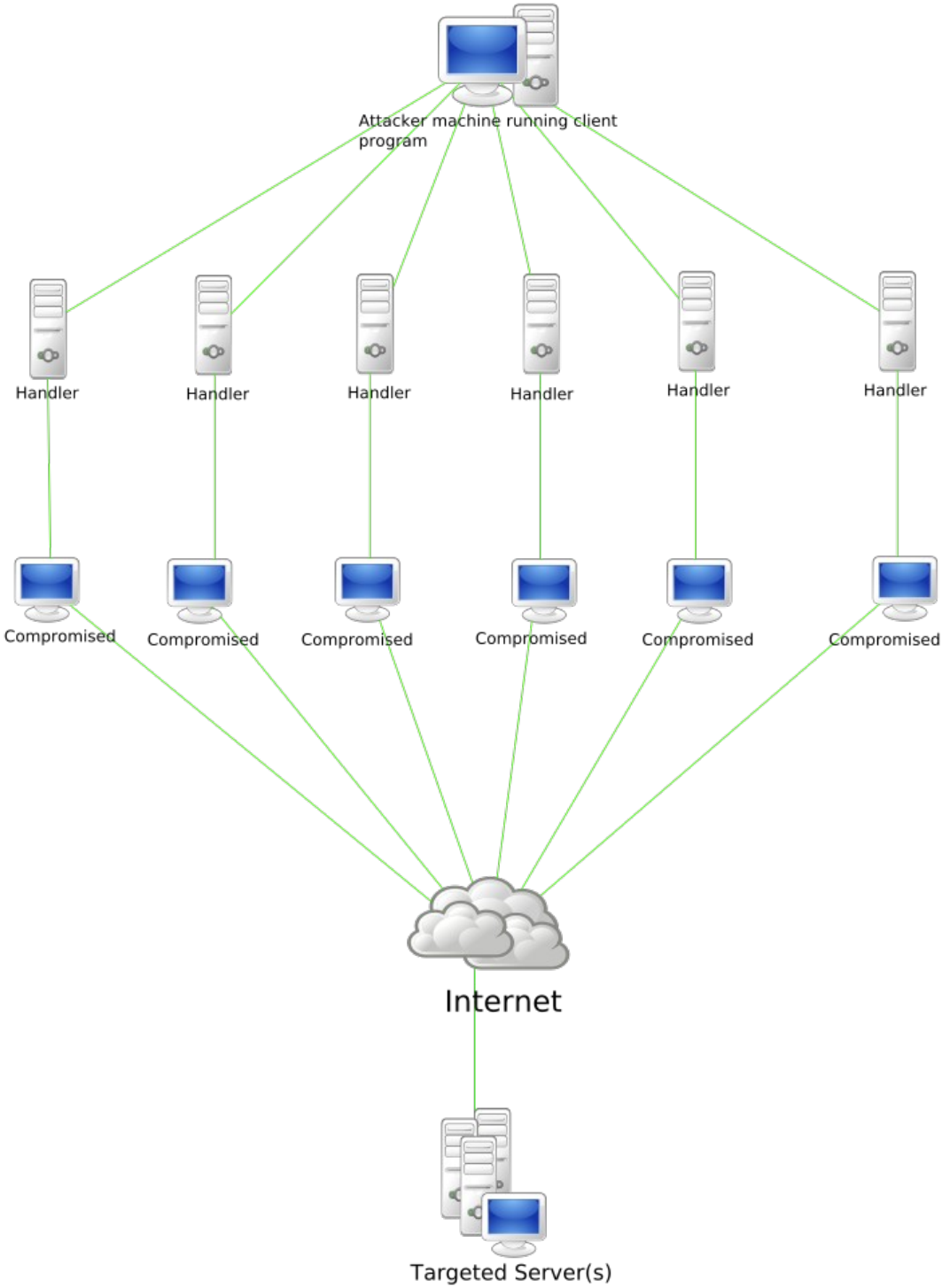
Τεχνικές παράκαμψης των οντοτήτων ασφαλείας (firewalls, antivirus, κρυπτογραφικά συστήματα, κρυπτογραφικά πρωτόκολλα κοκ), που έχουν τοποθετηθεί σκόπιμα από τους κατασκευαστές, με σκοπό την πιθανή μελλοντική αξιοποίησή τους.

1. **Χαρακτηριστικά**:
α. Αόρατο / κρυφό Λογισμικό
β. Κρυφή λειτουργικότητα

2. **Σκοπός**
α. Παράκαμψη των μέτρων ασφαλείας
αλλότριοι

3. **Εύρος διάδοσης**
α. Λογισμικό ασφαλείας
β. Υποδομές ασφαλείας υπολογιστικών συστημάτων

Botnets


Attacker machine running client program
Handler
Handler
Handler
Handler
Handler
Handler
Compromised
Compromised
Compromised
Compromised
Compromised
Compromised
Internet
Targeted Server(s)

“Προστασία” – Rogue security software, scareware

Κακόβουλο λογισμικό που έχει στόχο να διαδώσει ψευδώς ότι ένας ή περισσότεροι Η/Υ έχουν μολυνθεί από ιό, ώστε να αγοραστεί ένα συγκεκριμένο λογισμικό προστασίας (συνήθως ψευδές που καταστρέφει την μέχρι τότε υπάρχουσα υποδομή ασφαλείας)

1. **Χαρακτηριστικά**:
α. Ορατό Λογισμικό
β. Κρυφή λειτουργικότητα

2. **Σκοπός**
α. Απόδοση δικαιωμάτων για λογισμικά, υπηρεσίες
β. ξεκλείδωμα Η/Υ
γ. Πρόσβαση σε δεδομένα

3. **Εύρος διάδοσης**
α. Προσωπικοί Υπολογιστές / προσωπικές συσκευές
β. Δίκτυα υπολογιστικών συστημάτων (μεγάλα, μεσαία, μικρά)

Λύτρα – Ransomware

Κακόβουλο λογισμικό που κρυπτογραφεί τα δεδομένα ενός Η/Υ ή υπολογιστικού συστήματος, χωρίς τη συγκατάθεση του χρήστη και στη συνέχεια απαιτούνται λύτρα για να ξεκλειδώσει την κρυπτογράφηση.

1. **Χαρακτηριστικά**:
α. Ιός, αόρατο λογισμικό
β. Κρυφή λειτουργικότητα

2. **Σκοπός**
α. Κρυπτογράφηση και κλείδωμα Η/Υ

3. **Εύρος διάδοσης**
α. Προσωπικοί Υπολογιστές / προσωπικές συσκευές
β. Δίκτυα υπολογιστικών συστημάτων (μεγάλα, μεσαία, μικρά)
γ. Βάσεις δεδομένων
δ. Αποθηκευτικοί χώροι δεδομένων

Zombie

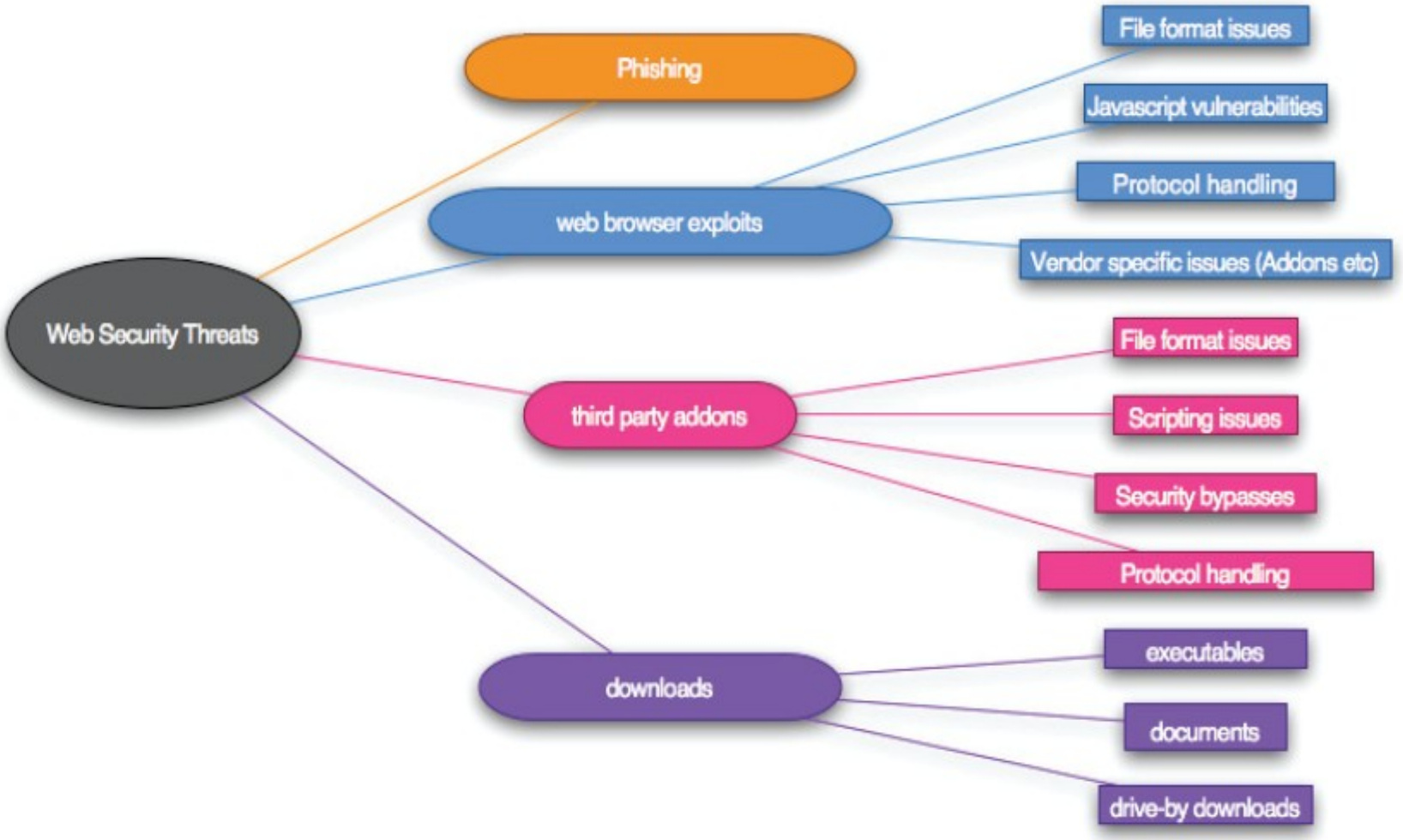
Υπολογιστής συνδεδεμένος στο διαδίκτυο, που έχει τεθεί υπό τον έλεγχο ενός hacker, χωρίς την συγκατάθεση ή την επίγνωση του νόμιμου χρήστη.

1. **Χαρακτηριστικά**:
α. Ιός, αόρατο λογισμικό
β. Κρυφή λειτουργικότητα

2. **Σκοπός**
α. Επιστράτευση του Η/Υ για κακόβουλη χρήση
β. Υπαγωγή του Η/Υ σε botnets

3. **Εύρος διάδοσης**
α. Προσωπικοί Υπολογιστές / προσωπικές συσκευές

Απειλές Ασφαλείας



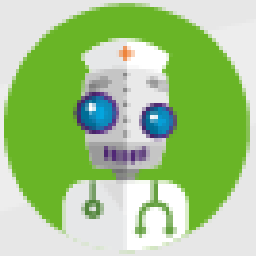
BOTS AND WEB SCRAPING

BOTS AND WEB SCRAPING

Τα bots είναι αυτοματοποιημένες διεργασίες στο διαδίκτυο που διενεργούνται από Εταιρείες ή Ομίλους εταιρειών για συγκεκριμένο σκοπό. Τα πιο γνωστά είναι τα bots που εκτελούν αυτοματοποιημένες διεργασίες αναζήτησης, όπως το Googlebot.

Δεν είναι όλα τα bots χρηστικά. Κάποια διενεργούν κακόβουλους σκοπούς:

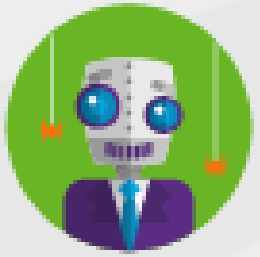
- Site scraping
- Vulnerability probing
- Launching DDoS attacks
- Distributing spam



1.2%

MONITORING BOTS

Health checkers that monitor website availability and the proper functioning of various online features.



2.9%

COMMERCIAL CRAWLERS

Spiders used for authorized data extractions, usually on behalf of digital marketing tools.

6.6%

SEARCH ENGINE BOTS

Bots that collect information for search engine algorithms, which they use to make ranking decisions.

12.2%

FEED FETCHERS

Bots that ferry website content to mobile and web applications, which they then display to their users.

24.3%

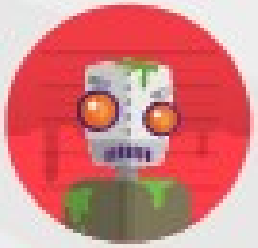
IMPERSONATORS

Bots that assume false identities to bypass security solutions. They are commonly used for DDoS assaults.

1.7%

SCRAPERS

Bots used for unauthorized data extraction and the reverse engineering of pricing models.



0.3%

SPAMMERS

Polluters that inject spam links into forums, discussions and comment sections.

2.6%

HACKER TOOLS

Scavengers that look for sites with vulnerabilities to exploit for data theft, malware injection, etc.

DDOS

Οι επιθέσεις DDOS (Distributed Denial of Service Attacks), είναι κατανεμημένες επιθέσεις που συμβαίνουν όταν συστήματα ζόμπι Η/Υ (από μερικές εκατοντάδες, έως και χιλιάδες μερικές φορές) επιτίθενται σε έναν μοναδικό στόχο. Επειδή η επίθεση προέρχεται από πολλά διαφορετικά IPs, το μπλοκάρισμα ενός IP δεν έχει αποτέλεσμα.

Διακρίνονται σε τρεις κατηγορίες:

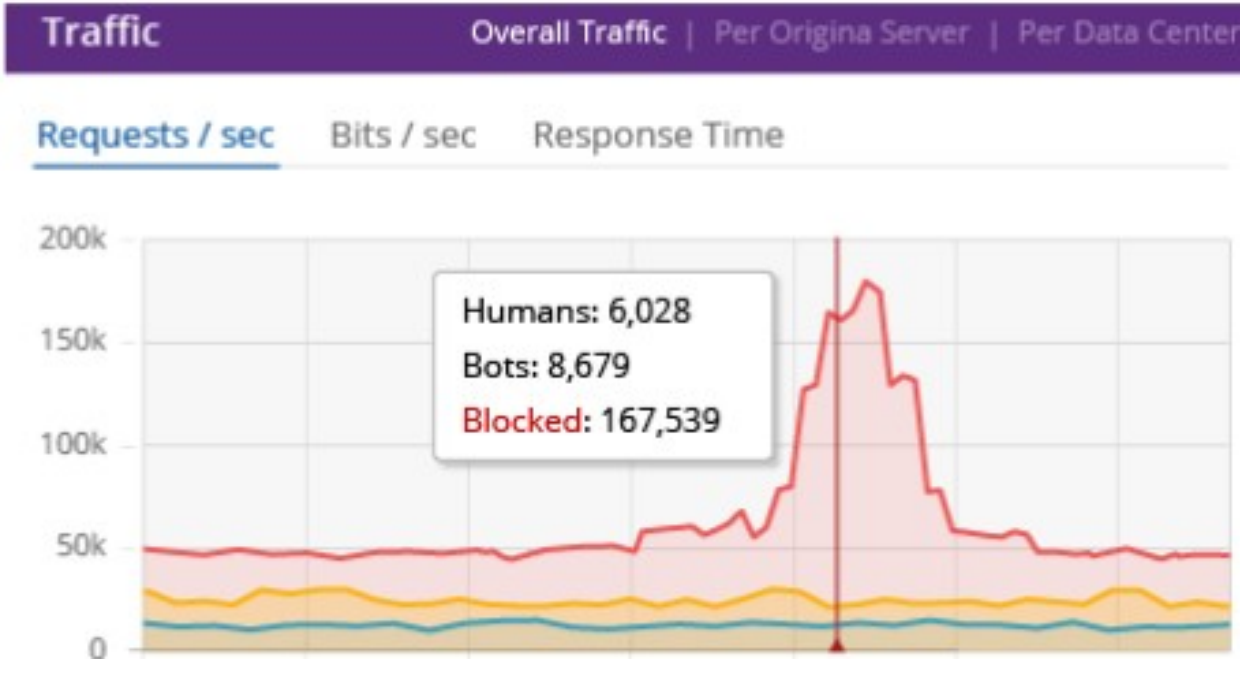
Volume Based Attacks Includes UDP floods, ICMP floods, and other spoofed-packet floods. The attack's goal is to saturate the bandwidth of the attacked site, and magnitude is measured in bits per second (Bps).

Protocol Attacks Includes SYN floods, fragmented packet attacks, Ping of Death, Smurf DDoS and more. This type of attack consumes actual server resources, or those of intermediate communication equipment, such as firewalls and load balancers, and is measured in packets per second (Pps).

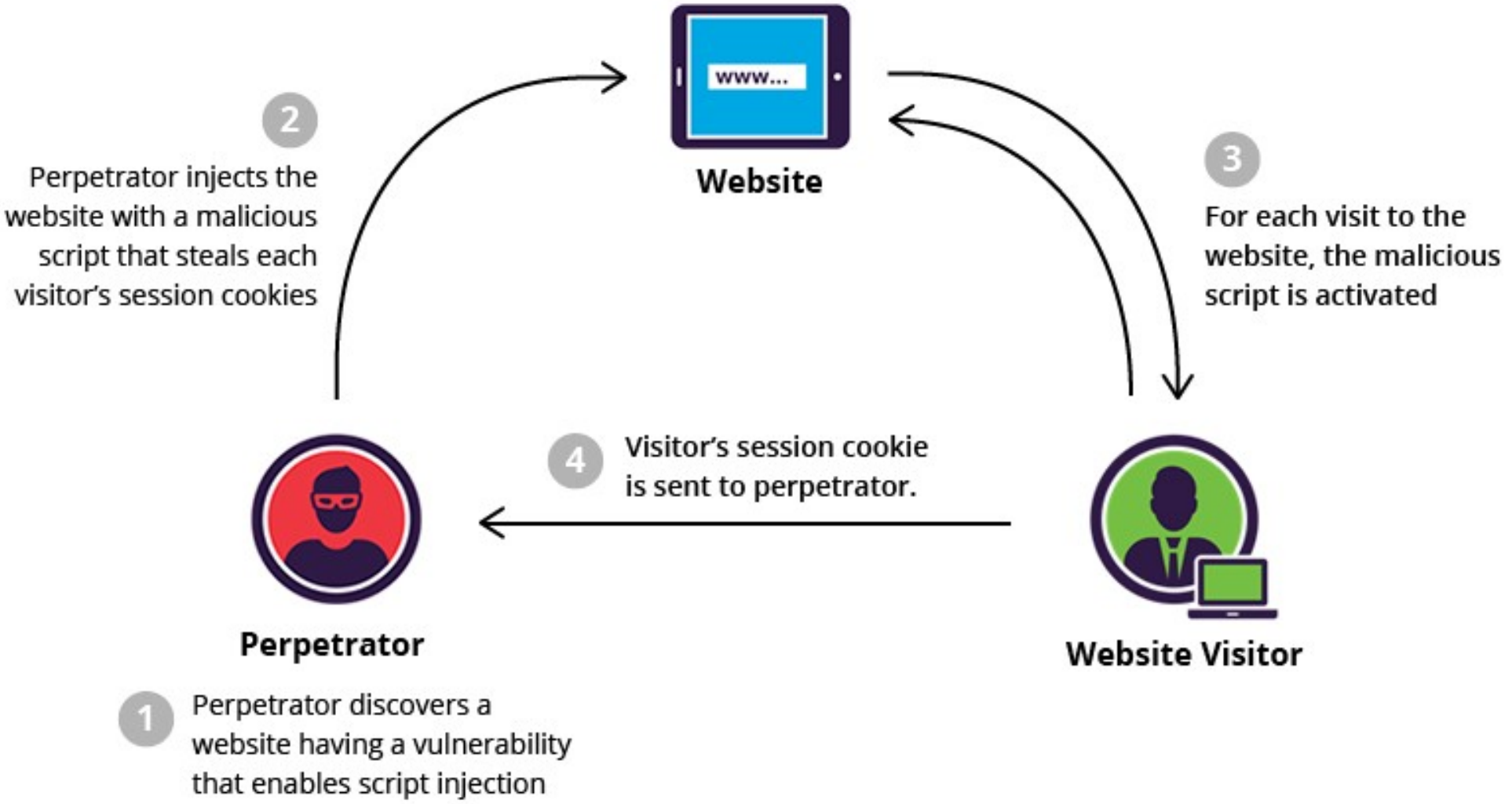
Application Layer Attacks Includes low-and-slow attacks, GET/POST floods, attacks that target Apache, Windows or OpenBSD vulnerabilities and more. Comprised of seemingly legitimate and innocent requests, the goal of these attacks is to crash the web server, and the magnitude is measured in Requests per second (Rps).

Κίνητρα για επιθέσεις DDOS:

- Ιδεολογία–"hacktivism“ Κυβερνοακτιβιστές επιτίθενται σε ιστοσελίδες με τις οποίες διαφωνούν.
- Εταιρικός ανταγωνισμός – Εταιρείες χρησιμοποιούν επιθέσεις DDoS ώστε στρατηγικά να θέσουν εκτός λειτουργίας συγκεκριμένες ιστοσελίδες ανταγωνιστών τους, ώστε για παράδειγμα να τους αποτρέψουν να λάβουν μέρος σε κάποιο γεγονός, όπως διαγωνισμοί κοκ. Ανία– Κυβερνοβάνδαλοι, χρησιμοποιούν scripts ώστε να αρχίσουν επιθέσεις DDOS.
- Εκβιασμός– Εκβιάζοντας τους ιδιοκτήτες ιστοσελίδων για χρήματα.
- Κυβερνοπόλεμος– Κυβερνήσεις διενεργούν επιθέσεις DDoS ώστε να αχρηστεύσουν ιστοσελίδες των αντιπάλων τους, και συνεκδοχικά τις υποδομές υπηρεσιών που εξυπηρετούνται από αυτές.



CROSS-SITE SCRIPTING (XSS)



CROSS-SITE SCRIPTING (XSS)

Ο αυτουργός μιας τέτοιας επίθεσης εμφιλοχωρεί τμήμα κακόβουλου λογισμικού σε ευάλωτες ιστοσελίδες, ανύποπτων ιδιοκτητών, χωρίς να στοχεύει τους ίδιους ή τις υπηρεσίες που επικουρούνται σε αυτές. Αντίθετα στοχεύει στους **επισκέπτες** των ιστοσελίδων αυτών.

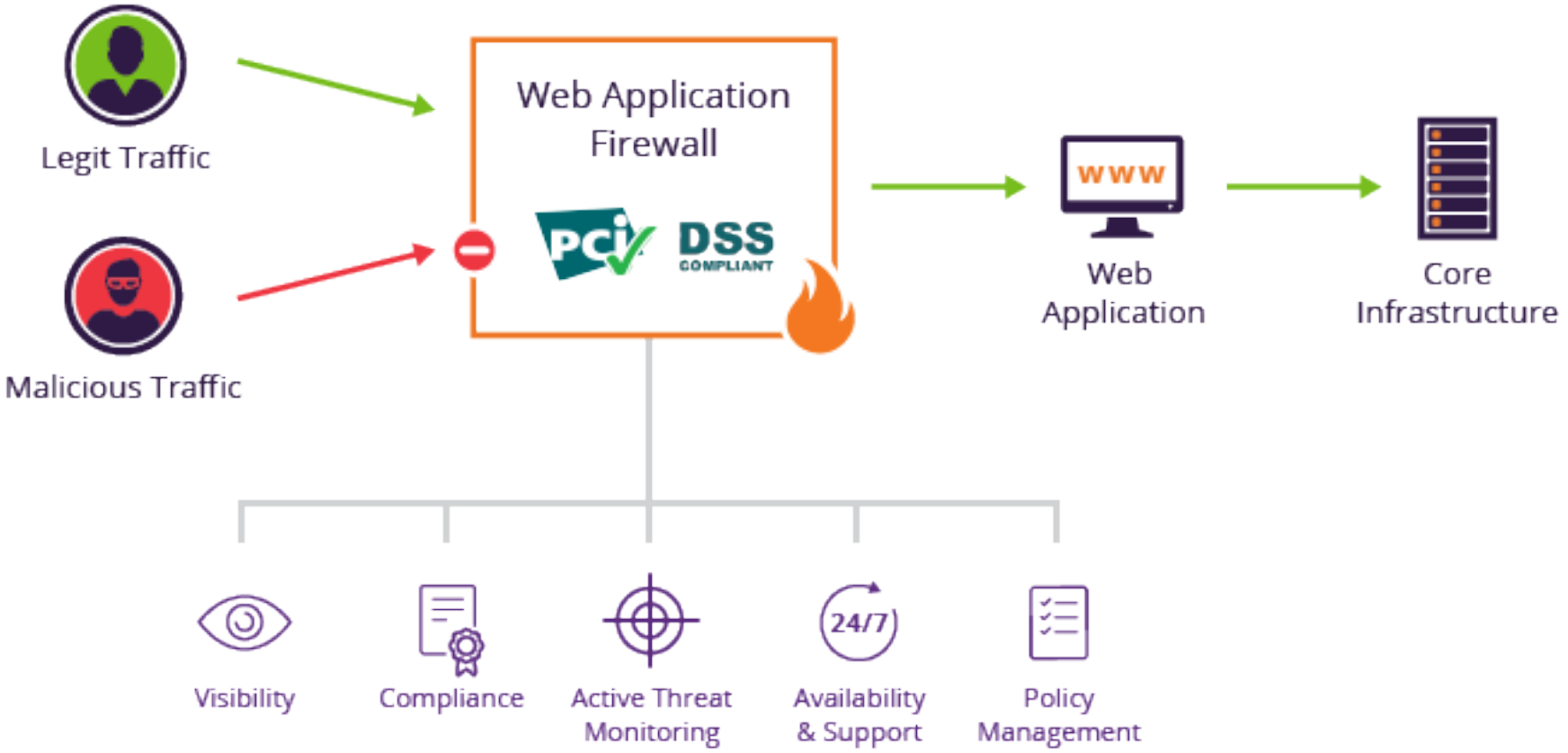
Τα αποτελέσματα μιας τέτοιας επίθεσης μπορεί να είναι ολέθρια για τη φήμη μιας εταιρείας και τις σχέσεις της με τους πελάτες-επισκέπτες των ιστοσελίδων της. Διακρίνονται σε:

Stored XSS, επίσης μόνιμες και οι πιο καταστροφικές. Το κακόβουλο script εγχέεται κατευθείαν στο λογισμικό εφαρμογής της ιστοσελίδας.

Reflected XSS το κακόβουλο script εγχέεται σε άλλη ιστοσελίδα, και ενεργοποιείται στην ιστοσελίδα στόχο ένας σύνδεσμος. Όταν αυτός ο σύνδεσμος επιλεγεί, τότε ο ανυποψίαστος επισκέπτης πηγαίνει σε άγνωστη για αυτόν ιστοσελίδα που τρέχει το κακόβουλο script.

Έγχυση κώδικα SQL

Ο επιτιθέμενος παρακάμπτει τα συστήματα πιστοποίησης χρήστη μιας ιστοσελίδας και εγχέει κώδικα SQL, χρησιμοποιώντας κακόβουλο λογισμικό, ώστε να θέσει ερωτήματα και συχνά να καταλάβει μια βάση δεδομένων. Συχνά αποκτάει πλήρη πρόσβαση σε δεδομένα που υπό κανονικές συνθήκες δεν θα έπρεπε να έχει, όπως ευαίσθητα εταιρικά δεδομένα, λίστες χρηστών, πνευματική ιδιοκτησία ή προσωπικά δεδομένα.



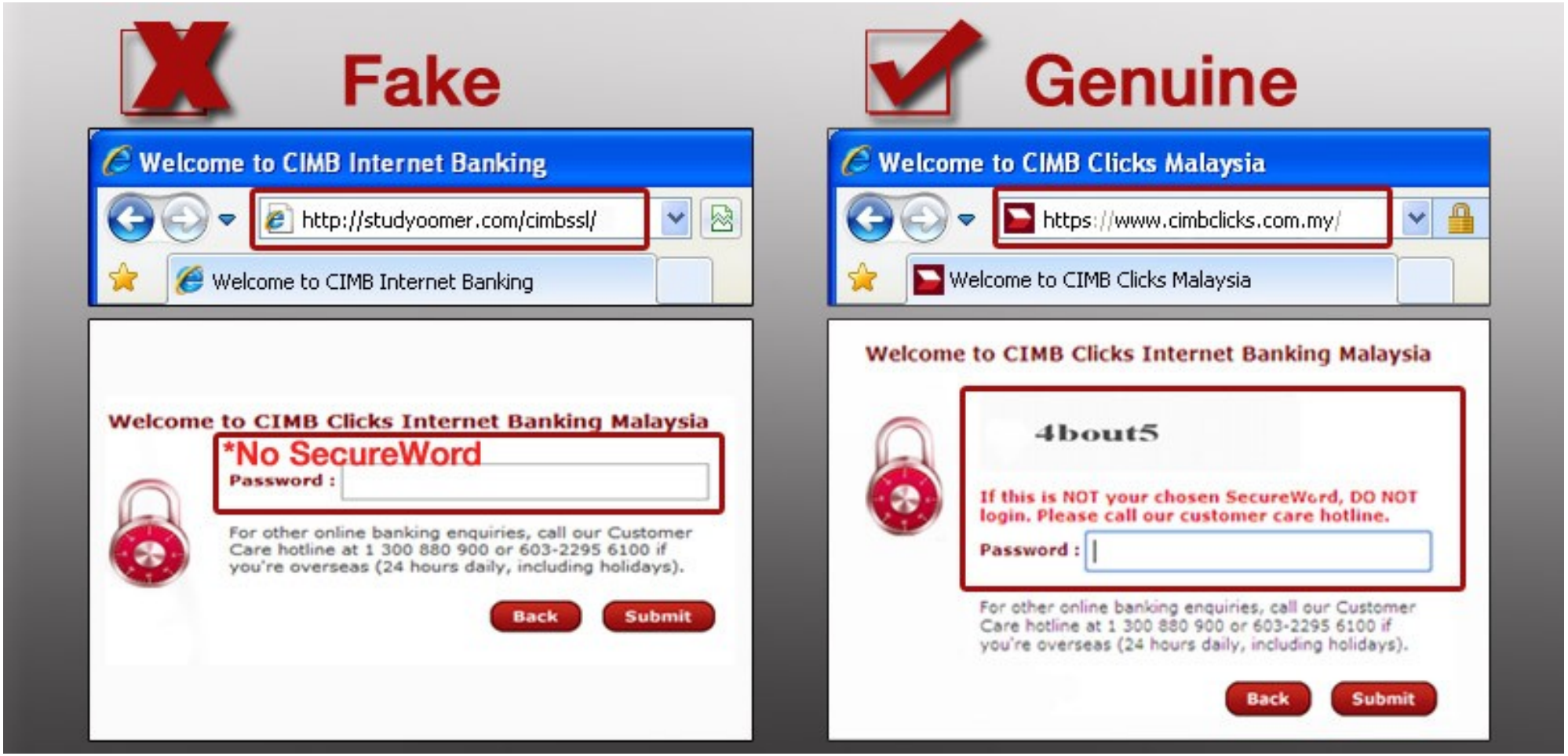
Απειλές στο διαδίκτυο

1. Ψάρεμα
2. Απάτη
3. Πλαστοπροσωπεία
4. Κλοπή προσωπικών δεδομένων
5. Κλοπή περιουσιακών στοιχείων
-οικονομικά δεδομένα
-πνευματικά δεδομένα
6. Κυβερνοπειρατεία
7. Κυβερνο-ακτιβισμός
8. Κυβερνοέγκλημα
9. Κυβερνοτρομοκρατία

Ψάρεμα - Phishing

Phishing: Ψευδές μήνυμα που υποτίθεται ότι έρχεται από εταιρεία-συνεργάτη και προειδοποιεί ότι μια υπηρεσία σύντομα λήγει. Προτρέπει σε ψευδή ιστοσελίδα που ζητάει από το χρήστη να δώσει προσωπικά δεδομένα.

Ψάρεμα - Phishing



Απάτη - Fraud

E-Commerce Fraud Types

- Credit Card Fraud
- Identity Theft
- Spam
- Scam/Solicitation
- Phishing
- Hacking
- Man-In-The-Middle Attacks
- Malicious Code
- Backdoor Attacks
- Skimming

Πλαστοπροσωπία - Impersonation

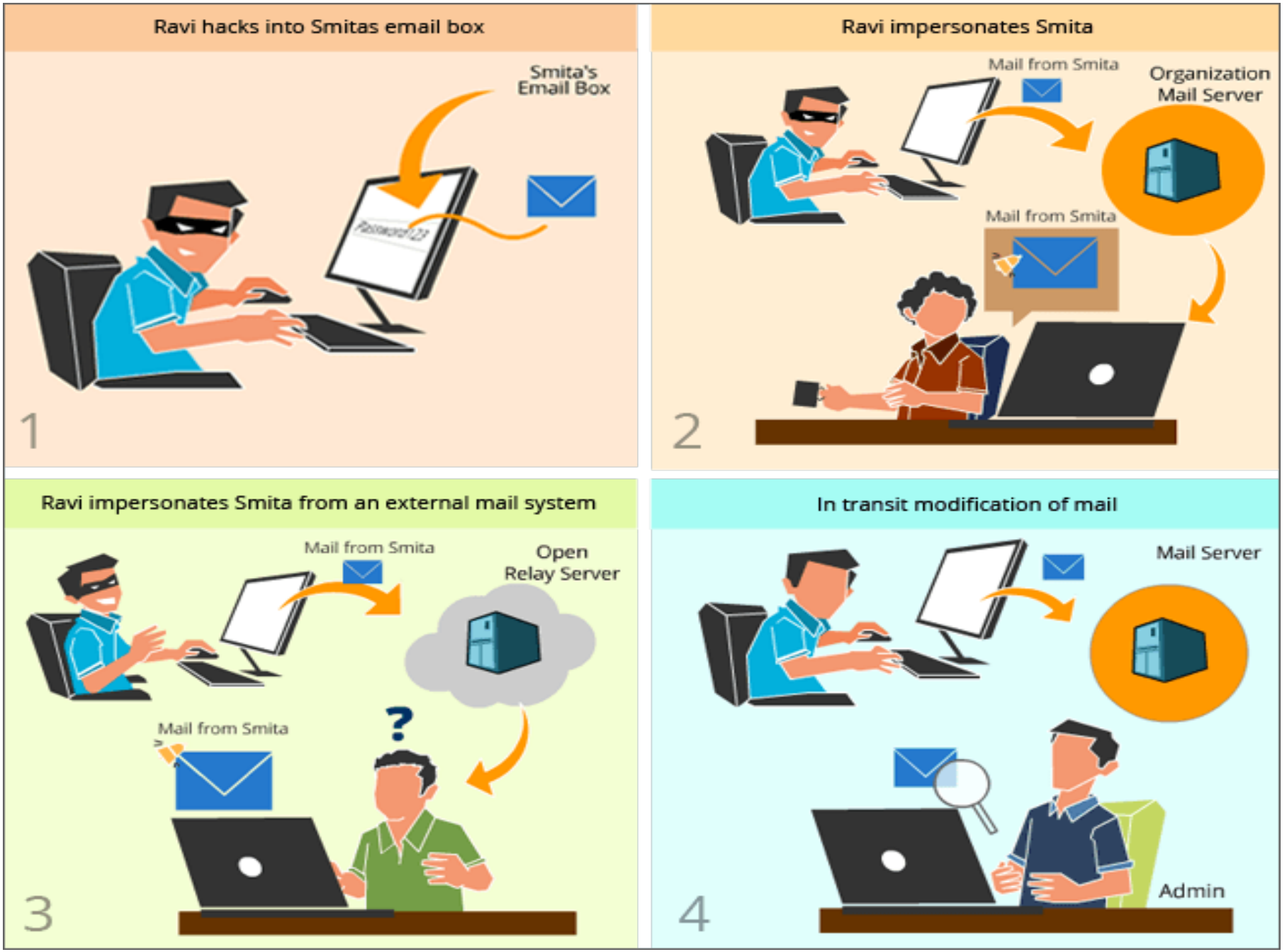
Πλαστοπροσωπία - Impersonation

Πλαστοπροσωπία - Impersonation

Ιστοσελίδες διάσημων προσώπων, περσόνες διασήμων, με στόχο τη σπίλωση, την εξαπάτηση κοκ.

Παλαιότερα κάποιοι κτυπούσαν τις πόρτες και ζητούσαν ενίσχυση για θρησκευτικές ενορίες, για αντικαρκινικό έρανο, για τους οδοκαθαριστές, κοκ.

E-mail Spoofing



E-mail Spoofing

Warning: Your account has been limited!

paypal to me 7/26/12 Thu,

PayPal

Confirm your account with PayPal

Dear Member,

You account has been temporarily Iimited if you want unlock it

please check it from here

Unlock Your Account

- Receive cross-border payments from the many countries that PayPal serves.
- Withdraw your payments to the bank account you selected.
- Become verified and remove your spending limit.

Yours sincerely,
PayPal

Help Centre | Resolution Centre | Security Centre

Please do not reply to this email because we are not monitoring this inbox. To get in touch with us, log in to your

Διασπορά ψευδών ειδήσεων

Overseas Money Transfer Scam

Overseas Money Transfer Scam

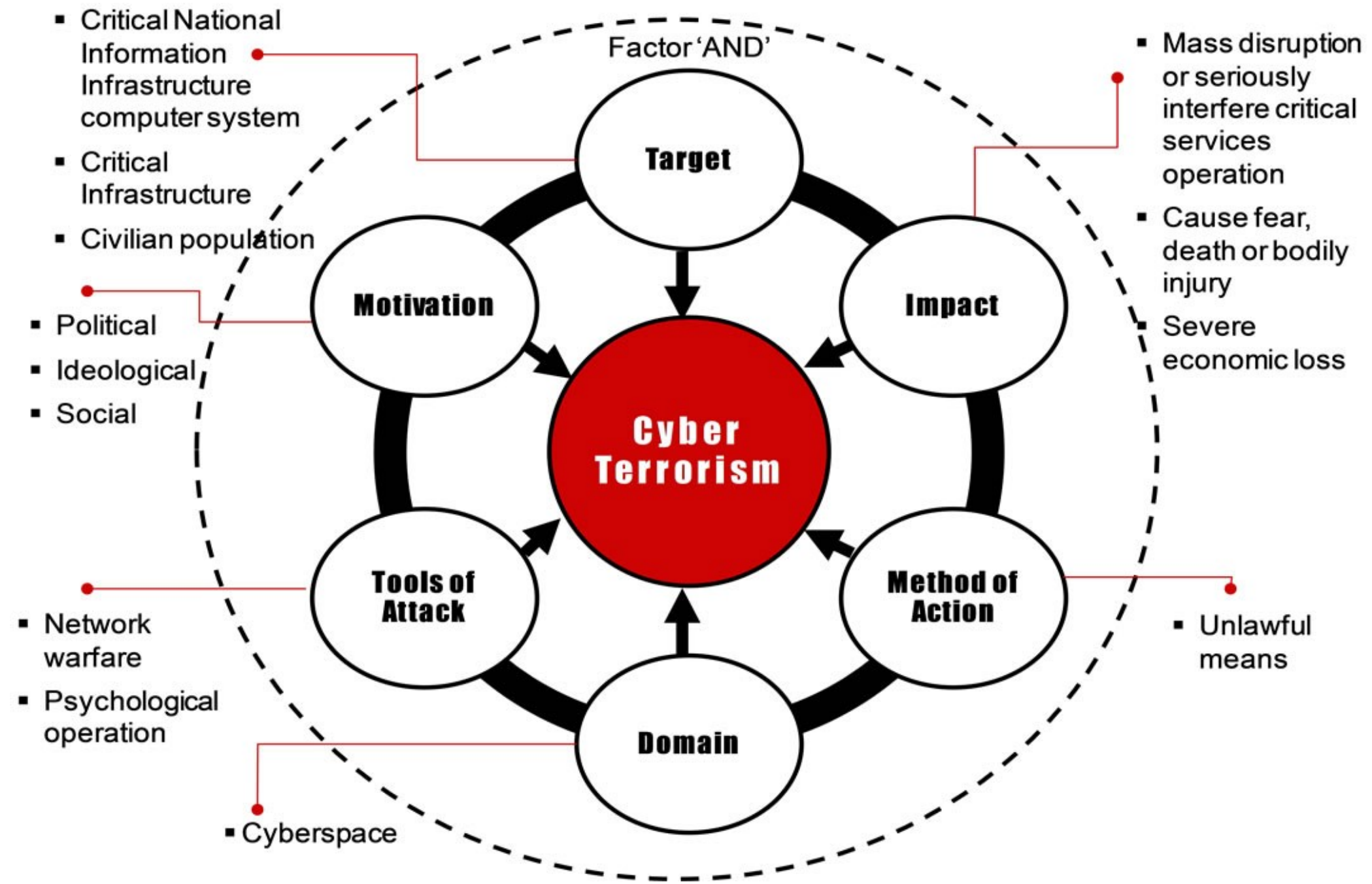
Κυβερνοπειρατία – Cyber Piracy

Κυβερνοπειρατία – Cyber Piracy

Software Piracy.

- ✓ Unauthorized software theft.
- ✓ Illegal copy / Counterfeiting.
- ✓ Illegal distribution of the same.
- ✓ No valid license .
- ✓ Almost impossible to stop.

Κυβερνοτρομοκρατία – Cyber Terrorism



The Haren Incident

The Haren Incident

The Haren Incident

The Haren Incident

MALWARE – Κακόβουλο Λογισμικό

Preparing the ground for the attack:

- Identifying the victim(s).
- Gathering background information.
- Selecting attack method(s).

Deceiving the victim(s) to gain a foothold:

- Engaging the target.
- Spinning a story.
- Taking control of the interaction.

Obtaining the information over a period of time:

- Expanding foothold.
- Executing the attack.
- Disrupting business or/and siphoning data.

Closing the interaction,
ideally without arousing suspicion:

- Bringing the charade to a natural end.
- Removing all traces of malware.
- Covering tracks.