Δοκιμές διείσδυσης

CSP010_W_EDUCON

ΠΑΡΟΥΣΊΑΣΗ ΑΠΌ:
ΧΡΉΣΤΟΣ ΓΡΗΓΟΡΙΆΔΗΣ

CyberSecPro

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

Κόκκινη Ομάδα

01. Τι είναι η κόκκινη ομάδα

02. Κόκκινη ομάδα vs δοκιμή διείσδυσης

03. Κύκλος ζωής επίθεσης

04. MITRE ATT&CK

05. Εισαγωγή στο «ατομικό κόκκινο»

Τι είναι η κόκκινη ομάδα

Λειτουργίες της Κόκκινης Ομάδας

- Σκοπός των λειτουργικών επιχειρήσεων 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

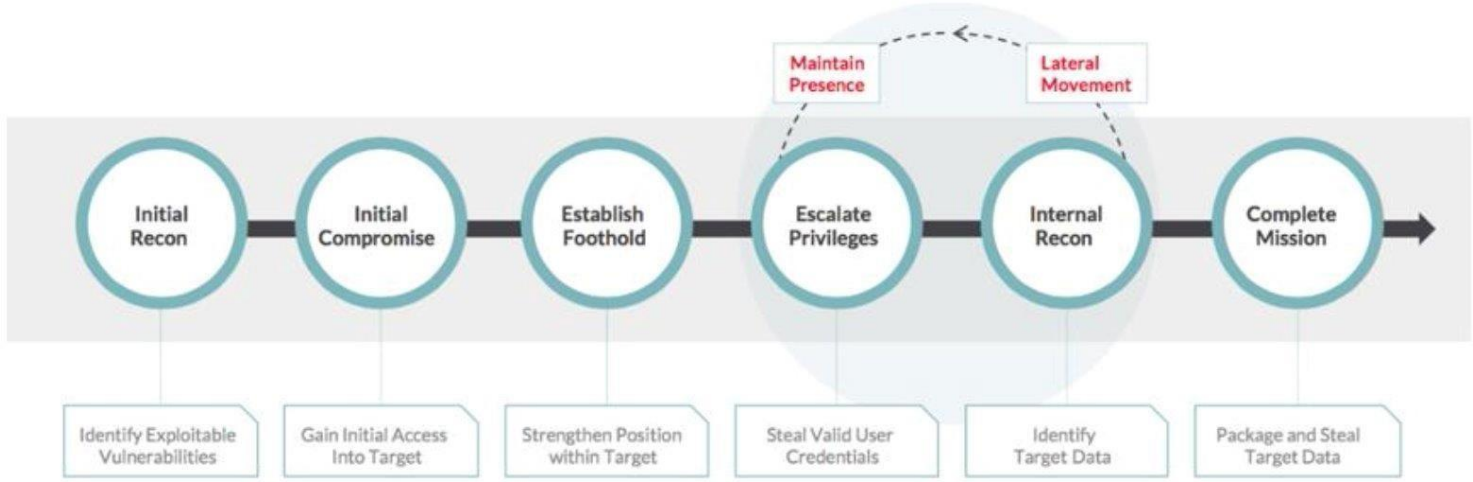
Επίδραση και ενσωμάτωση με την μπλε ομάδα

- 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:
  - Εκπαιδεύστε 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

Δοκιμή διείσδυσης	Κόκκινη ομάδα
Καθορισμένο πεδίο εφαρμογής	Χωρίς καθορισμένο πεδίο εφαρμογής
Χρησιμοποιείται για τον εντοπισμό και την εκμετάλλευση ευπαθειών	Εξομοιώνει τη συμπεριφορά των αντιπάλων
Παρέχει αναφορά ευρημάτων που χρησιμοποιούνται κατά συνέπεια από τις εταιρείες για να επιδιορθώσουν, 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 προδραστική ανίχνευση απειλών στο μέλλον.	Παρέχει αξιοποιήσιμα αποτελέσματα που μπορούν να χρησιμοποιηθούν για την ανίχνευση.

Κύκλος ζωής επίθεσης

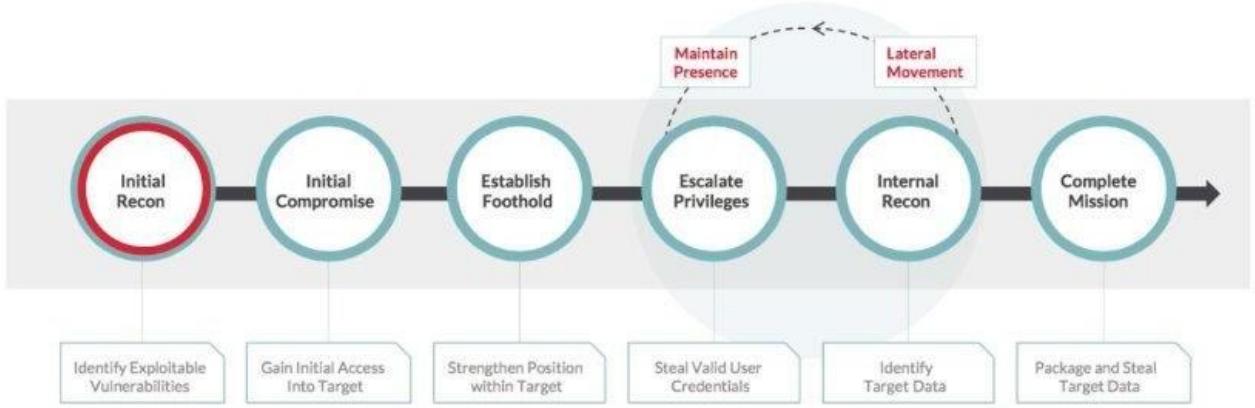


Στάδια μιας Τυπικής Κυβερνοεπίθεσης:
Αρχική Αναγνώριση (Initial Recon) & Εντοπισμός εκμεταλλεύσιμων ευπαθειών στον στόχο - Αρχική Διείσδυση (Initial Compromise) & Απόκτηση αρχικής πρόσβασης στο περιβάλλον του στόχου. - Εδραίωση Πρόσβασης (Establish Foothold) & Ενίσχυση της παρουσίας εντός του στόχου 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

Attack Lifecycle – Initial Reconnaissance

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

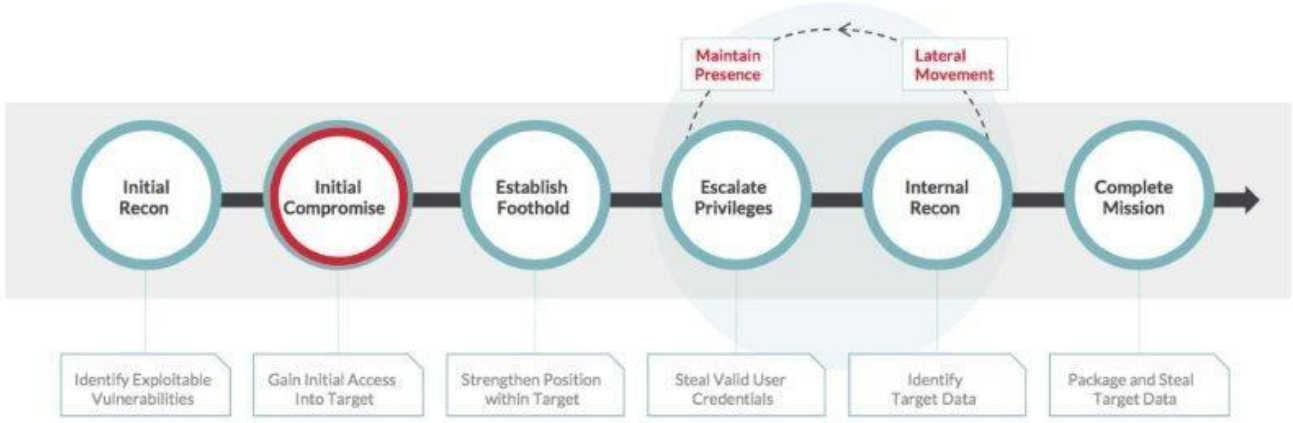


Συλλογή πληροφοριών από ανοικτές πηγές
Αναγνώριση δικτύου και εφαρμογών
Εντοπισμός δυνατοτήτων απομακρυσμένης πρόσβασης

Κύκλος ζωής επίθεσης

Attack Lifecycle – Initial Compromise

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

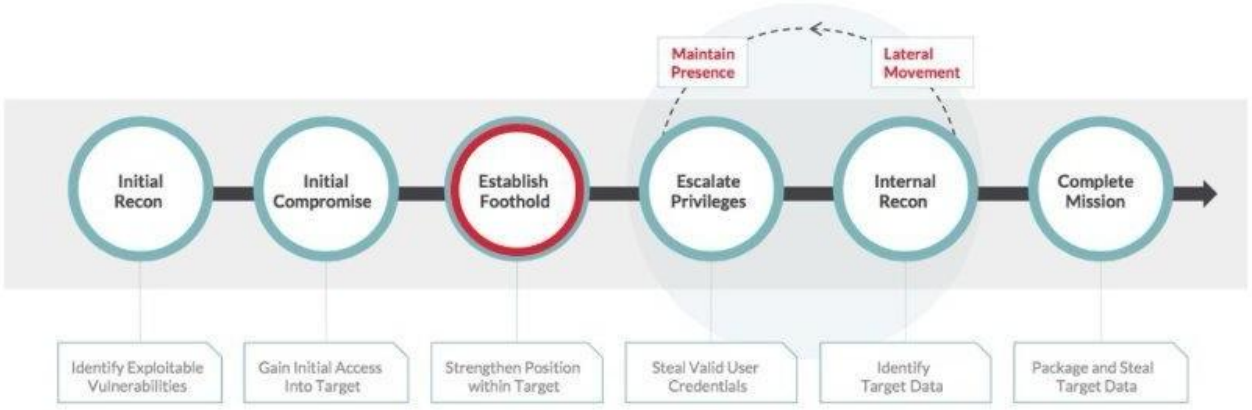


Κοινωνική μηχανική
Επίθεση μέσω διαδικτύου
Αξιοποίηση παρόχου υπηρεσιών

Κύκλος ζωής επίθεσης

Attack Lifecycle – Establish Foothold

- Backdoors
- Remote access subversion

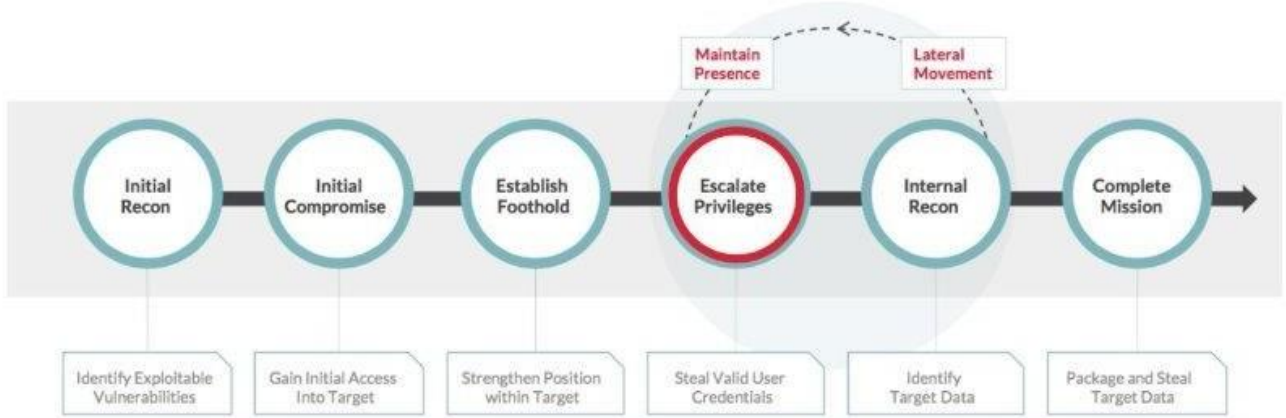


Κερκόπορτες (Backdoors)
Υπονόμευση απομακρυσμένης πρόσβασης

Κύκλος ζωής επίθεσης

Attack Lifecycle – Escalate Privileges

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

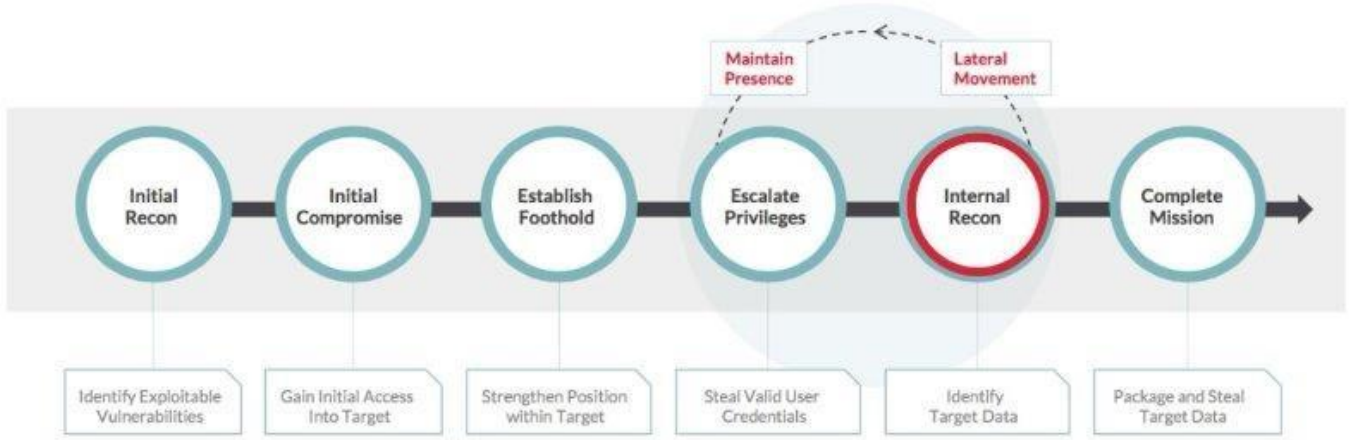


Συλλογή διαπιστευτηρίων
Σπάσιμο κωδικών πρόσβασης
Τεχνική Pass-the-Hash

Κύκλος ζωής επίθεσης

Attack Lifecycle – Internal Reconnaissance

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

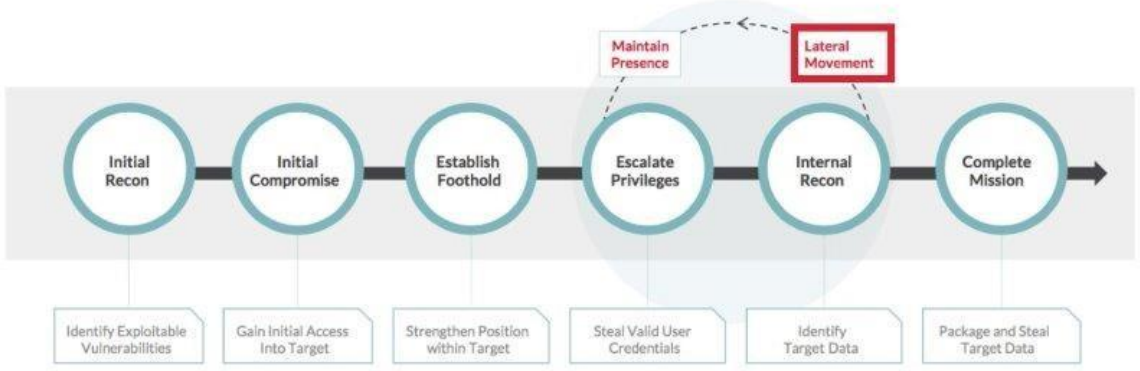


Αναγνώριση κρίσιμων συστημάτων
Καταγραφή/Απαρίθμηση συστημάτων
Καταγραφή/Απαρίθμηση λογαριασμών και κωδικών πρόσβασης

Κύκλος ζωής επίθεσης

Attack Lifecycle – Lateral Movement

- Remote command execution
- Remote administration tools

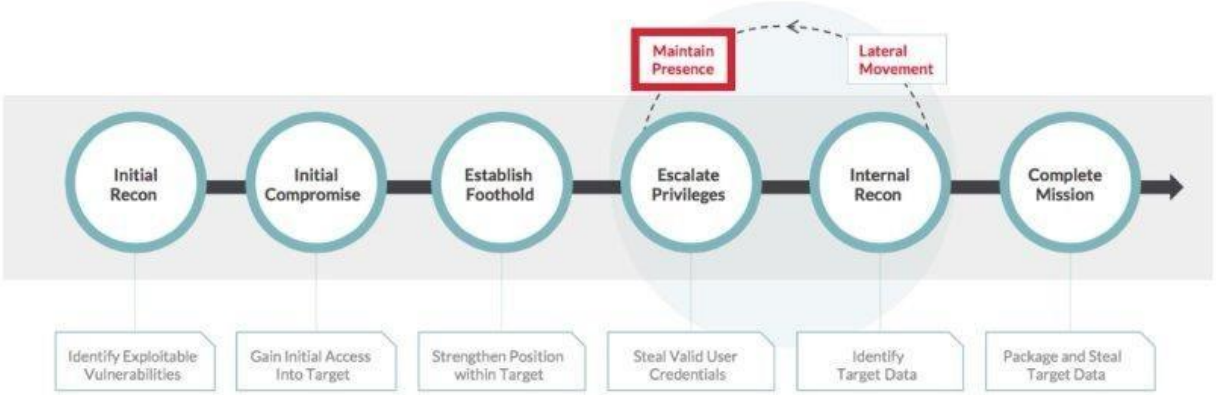


Απομακρυσμένη εκτέλεση εντολών
Εργαλεία απομακρυσμένης διαχείρισης

Κύκλος ζωής επίθεσης

Attack Lifecycle – Maintain Presence

- Command and control
- Remote access subversion
- Account abuse

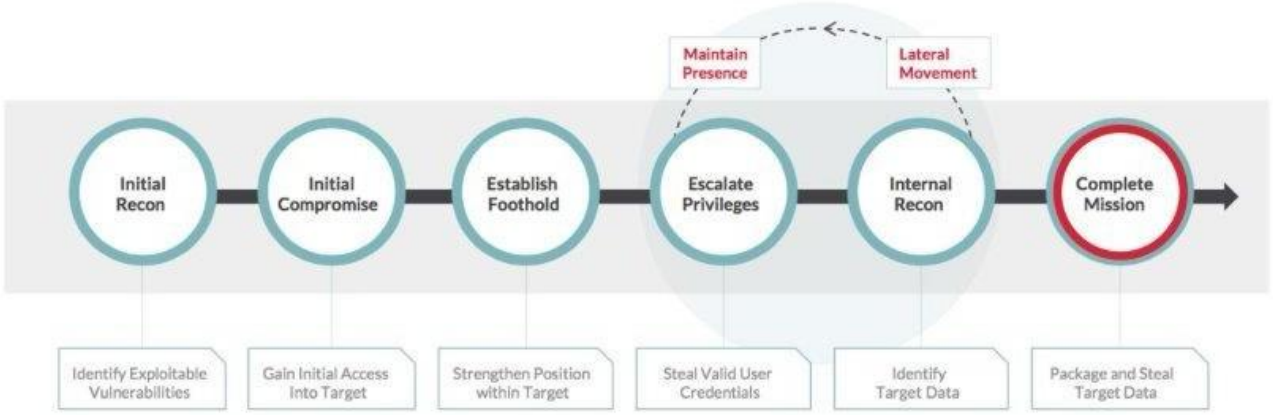


Έλεγχος και διοίκηση
Υπονόμευση απομακρυσμένης πρόσβασης
Κατάχρηση λογαριασμού

Κύκλος ζωής επίθεσης

Attack Lifecycle – Complete Mission

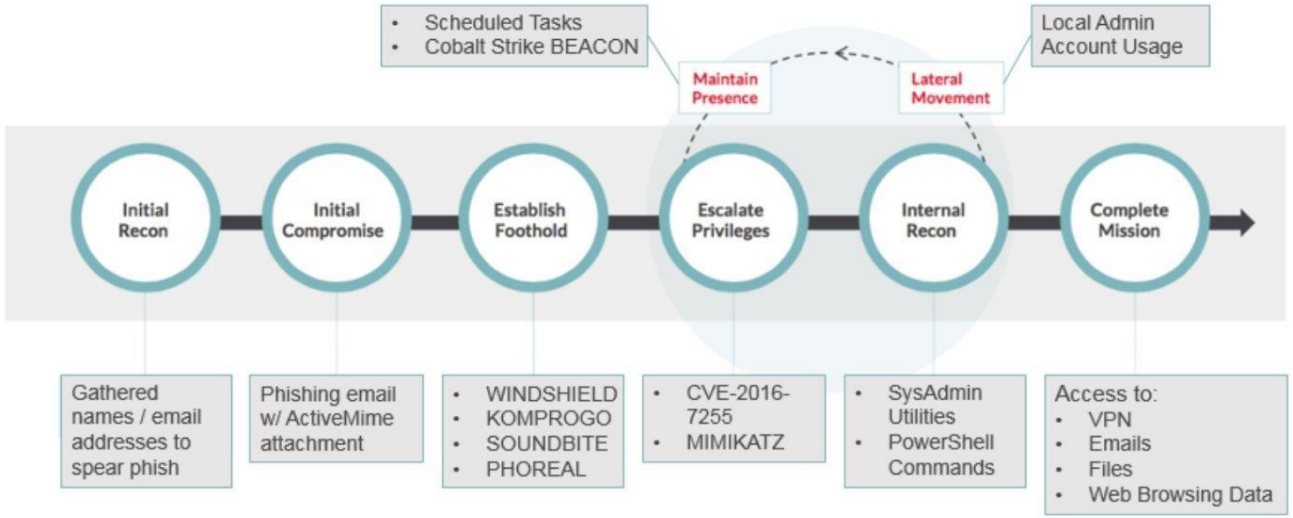
- Data staging
- Data exfiltration
- Data modification
- Data destruction



Προετοιμασία δεδομένων
Εξαγωγή δεδομένων
Τροποποίηση δεδομένων
Καταστροφή δεδομένων

Κύκλος ζωής επίθεσης

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
   Διατήρηση παρουσίας: Προγραμματισμένες Εργασίες,Cobalt Strike BEACON
5. Εσωτερική Αναγνώριση: SysAdmin Utilities, PowerShell Εντολές
   Πλευρική κίνηση: Χρήση τοπικών διαχειριστικών λογαριασμών
6. Ολοκλήρωση Αποστολής: Πρόσβαση σε: VPN, Email, Αρχεία, Δεδομένα περιήγησης

MITRE ATT&CK & Atomic Red Team Exploration

CyberSecPro

Σας ευχαριστώ για την προσοχή σας

Παρουσίαση από:

Χρήστος Γρηγοριάδης

CyberSecPro