

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

# Penetration Testing

# CSP010\_W \_EDUCON

PRESENTATION BY:  
CHRISTOS GRIGORIADIS (FOCAL POINT)



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

# Red Teaming

- 1. What is Red Teaming
- 2. Red Teaming vs Pentesting
- 3. Attack Lifecycle
- 4. MITRE ATT&CK
- 5. Atomic Red Introduction



# What is Red Teaming

## Red Team Operations

- Purpose of Red Team Operations: Simulate full-scope attacks to test security across digital infrastructure, employees, applications, and physical security.
- Simulating Real Adversaries: Replicate techniques used by real-world adversaries to uncover vulnerabilities and assess the company's defensive capabilities.
- Full Attack Lifecycle: Operations span the entire lifecycle of an attack, providing a comprehensive evaluation of security readiness.
- Revealing Vulnerabilities: Identifies multiple attack vectors and weaknesses not typically found in standard penetration tests.



# What is Red Teaming

## Impact and Integration with Blue Team

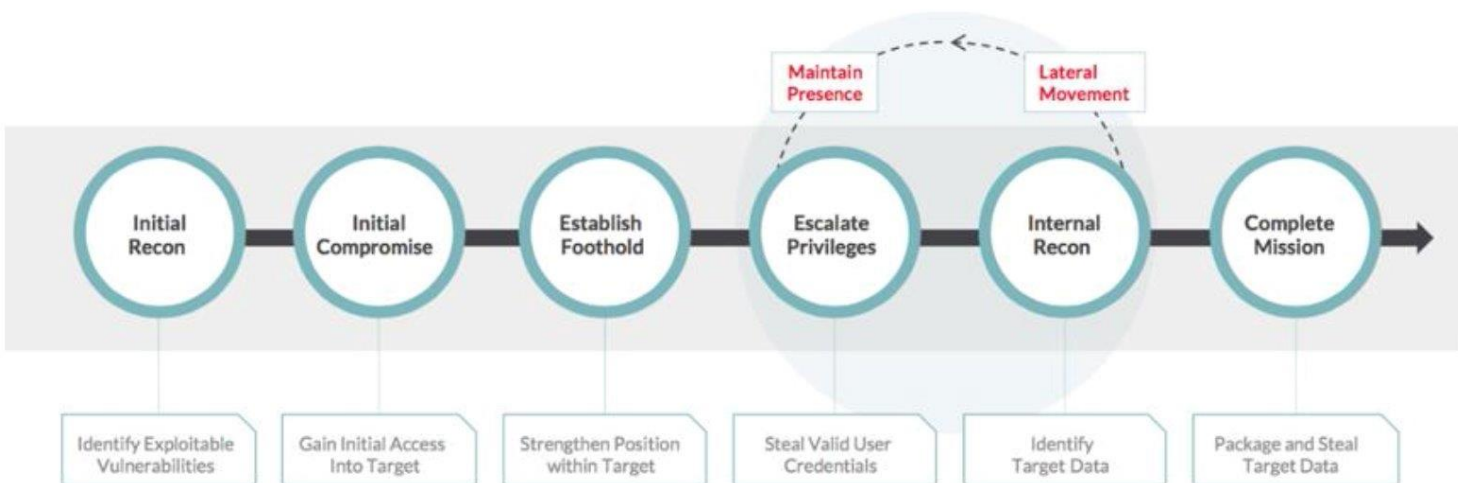
- Actionable Results: Red Team findings are used to improve security measures and prepare for potential threats.
- Blue Team Collaboration:
- Role of Blue Team: Security professionals tasked with vulnerability identification, remediation, and effectiveness verification.
- Utilizing Results: Develop signatures for malware, implement safeguards, and enhance infrastructure security.
- Training and Hardening:
- Train employees to resist social engineering.
- Patch vulnerabilities identified during operations.
- APT Emulation: Red Teams emulate techniques of Advanced Persistent Threats to test long-term defense mechanisms.



# Red Teaming vs Pentesting

Pentesting	Red Teaming
Defined scope	No defined scope
Used to identify and exploit vulnerabilities	Emulates adversary behavior
Provides a report of findings that are consequently used by companies to patch, harden and secure their infrastructure	Used to assess the resilience of an organization against adversaries attacks.
Preventative as opposed to detective. Penetration tests are useful at identifying vulnerabilities and threats, however, they do not provide actionable results that can be used for proactive detection of threats in the future.	Provides actionable results that can be used for detection.

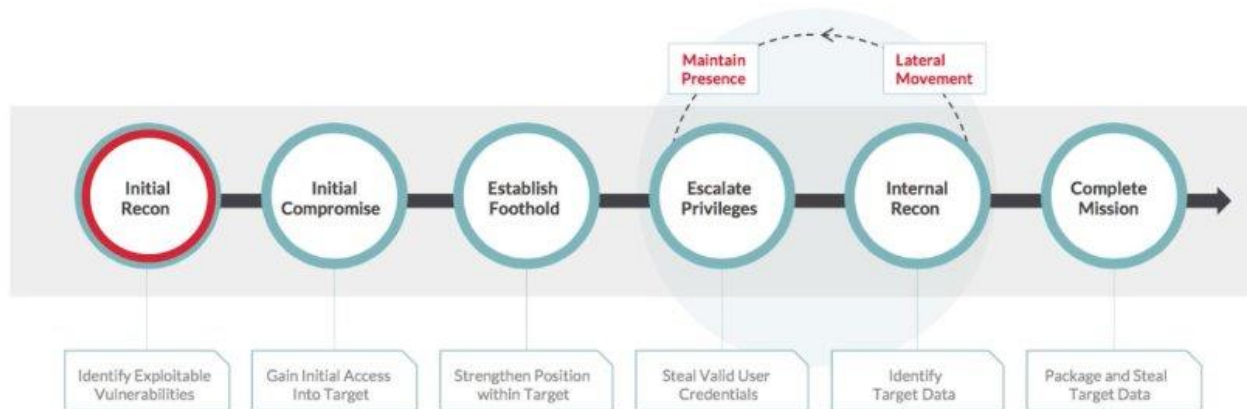
# Attack Lifecycle



# Attack Lifecycle

## Attack Lifecycle – Initial Reconnaissance

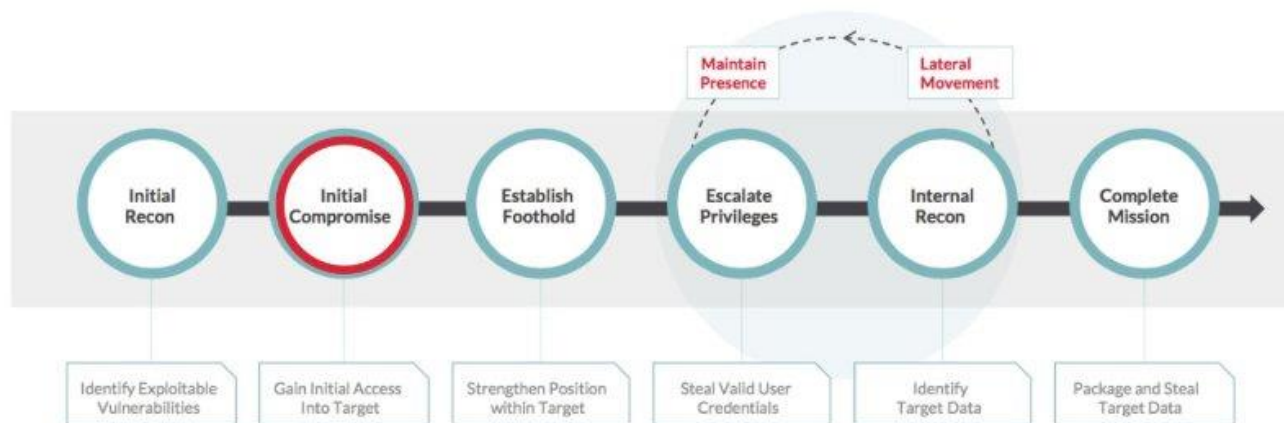
- Open source intelligence gathering
- Network and application reconnaissance
- Remote access identification



# Attack Lifecycle

## *Attack Lifecycle – Initial Compromise*

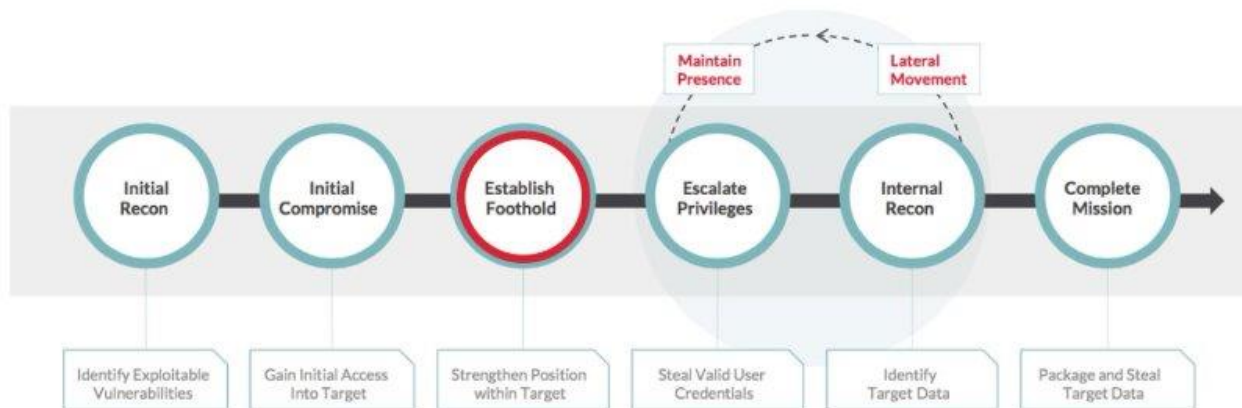
- Social engineering
- Internet-based attack
- Leverage service provider



# Attack Lifecycle

## Attack Lifecycle – Establish Foothold

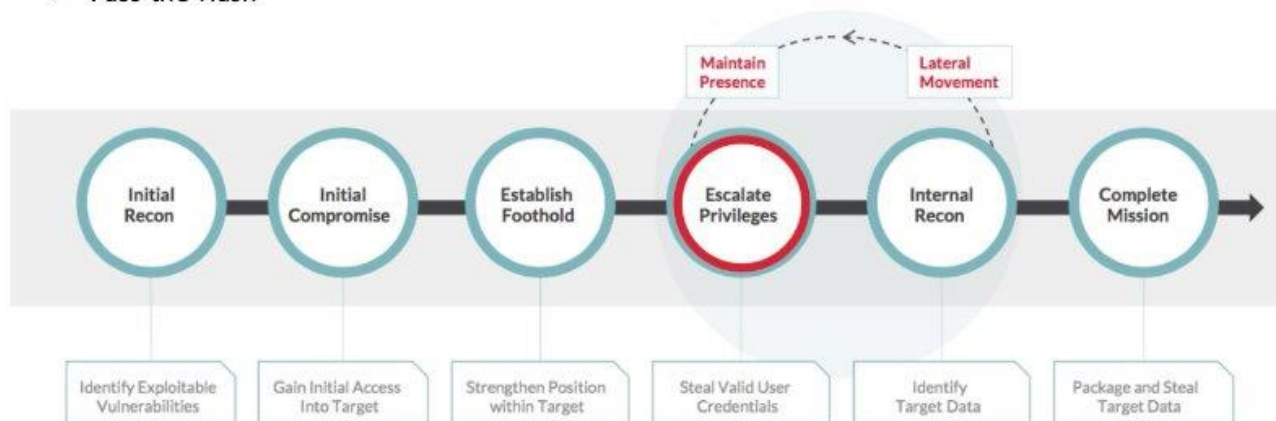
- Backdoors
- Remote access subversion



# Attack Lifecycle

## *Attack Lifecycle – Escalate Privileges*

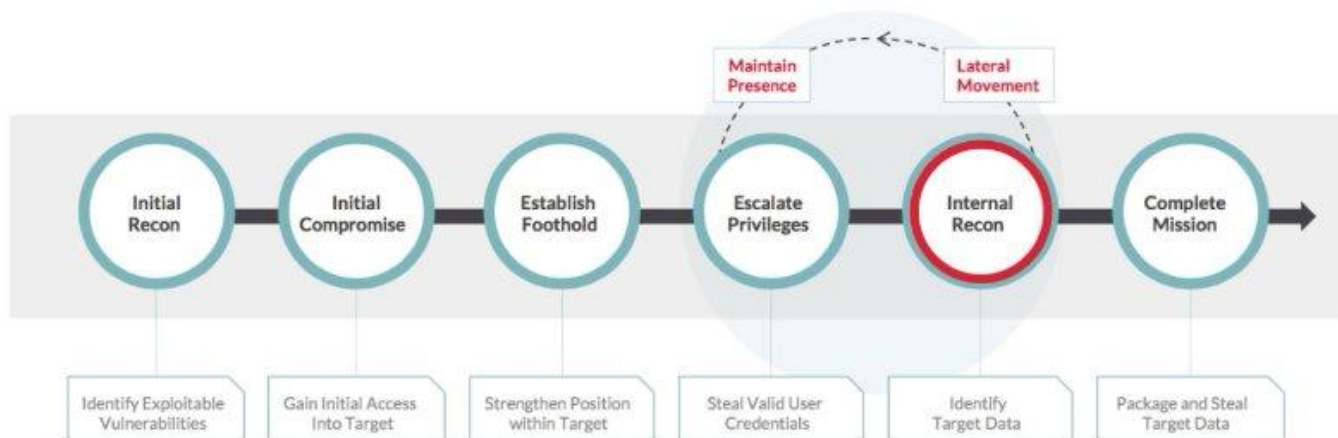
- Credential harvesting
- Password cracking
- Pass-the-Hash



# Attack Lifecycle

## *Attack Lifecycle – Internal Reconnaissance*

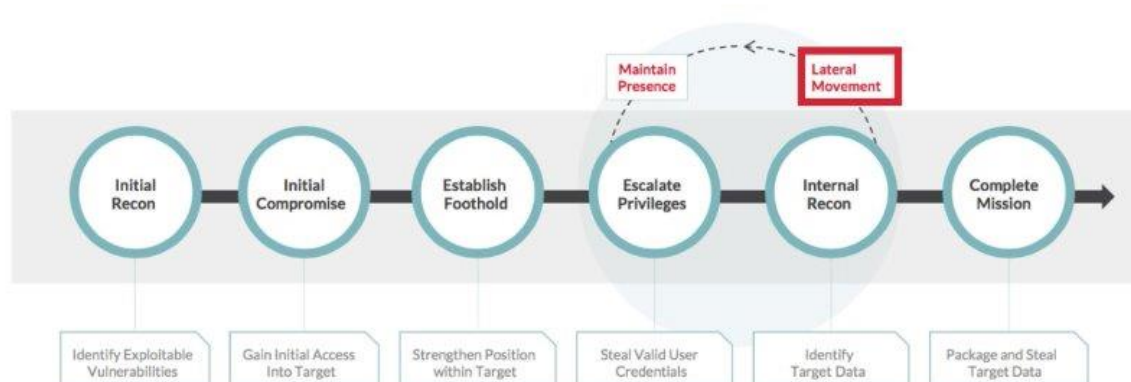
- Critical system identification
- System enumeration
- Account and password enumeration



# Attack Lifecycle

## *Attack Lifecycle – Lateral Movement*

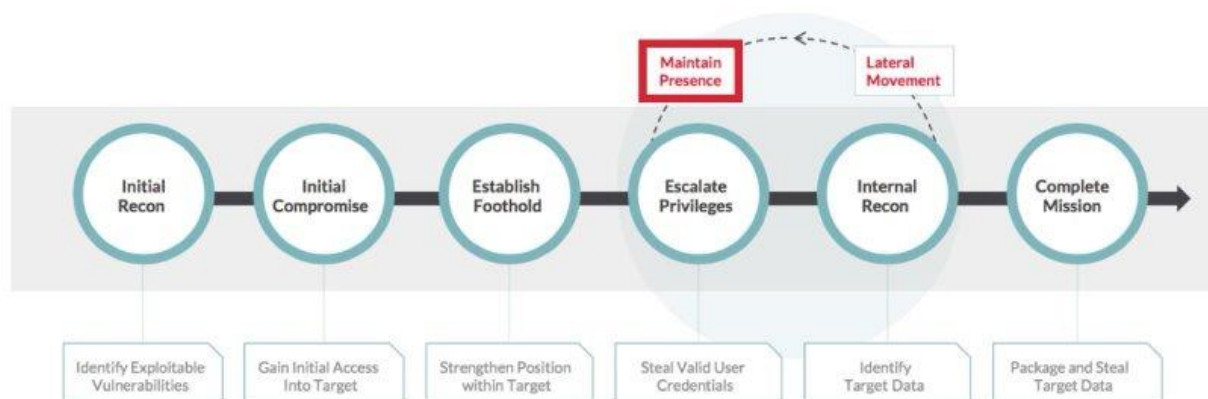
- Remote command execution
- Remote administration tools



# Attack Lifecycle

## Attack Lifecycle – Maintain Presence

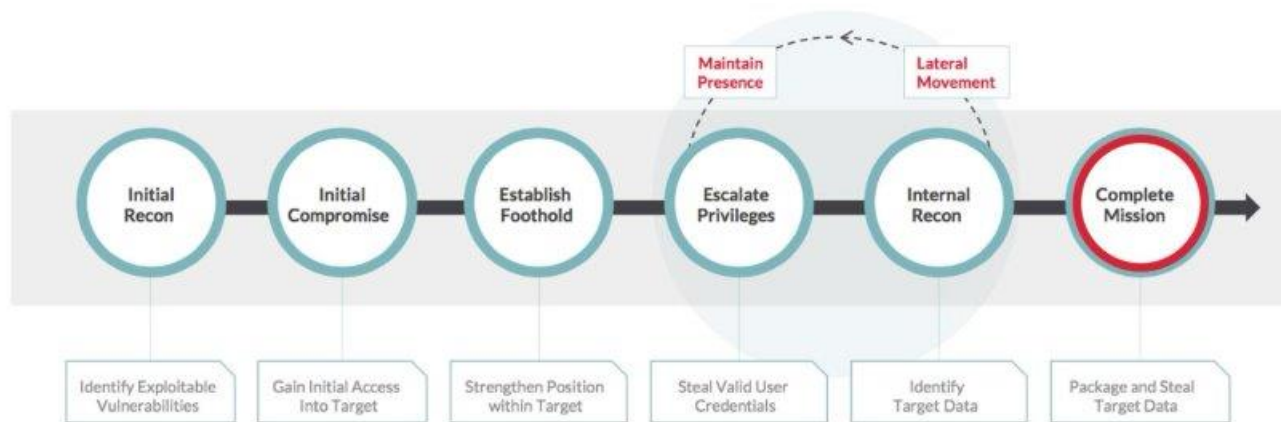
- Command and control
- Remote access subversion
- Account abuse



# Attack Lifecycle

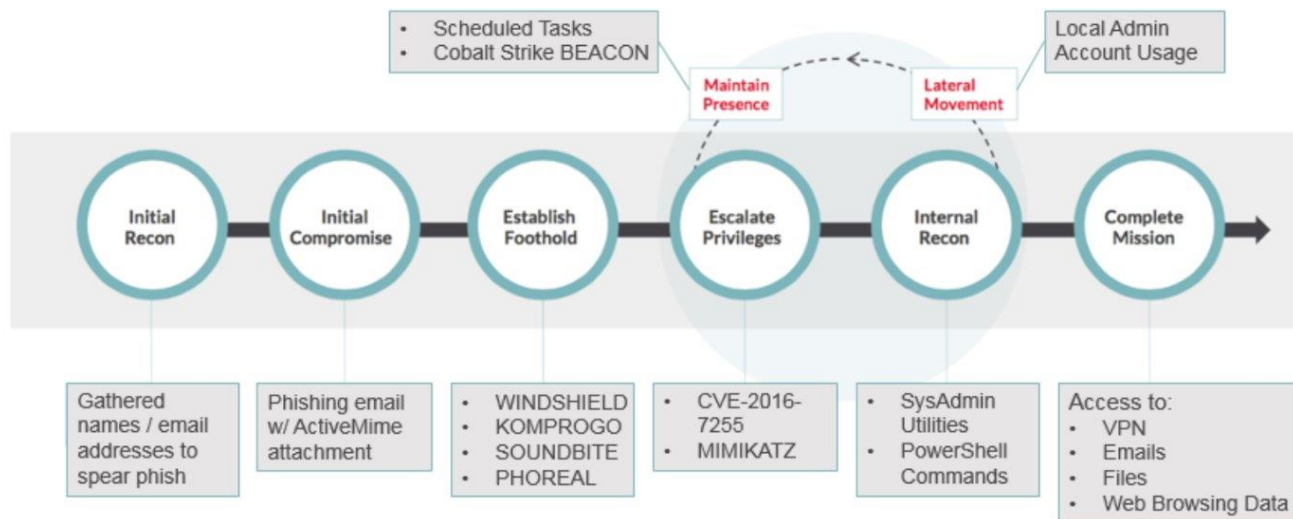
## Attack Lifecycle – Complete Mission

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



# Attack Lifecycle

## Attack Lifecycle – APT32



# MITRE ATT&CK & Atomic Red Team Exploration

Reconnaissance 14 techniques	Resource Development 8 techniques	Initial Access 12 techniques	Execution 14 techniques	Persistence 22 techniques	Privilege Escalation 14 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 12 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 14 techniques
Active Scanning <a href="#">↗</a>	Acquire Credentials <a href="#">↗</a>	Common Injection <a href="#">↗</a>	Cloud Administration Command <a href="#">↗</a>	Account Manipulation <a href="#">↗</a>	Abuse Elevation Control Mechanism <a href="#">↗</a>	Abuse Elevation Control Mechanism <a href="#">↗</a>	Adversary Infiltration <a href="#">↗</a>	Account Discovery <a href="#">↗</a>	Explanation of Remote Services <a href="#">↗</a>	Intercept the MDM <a href="#">↗</a>	Application Layer Protocol <a href="#">↗</a>	Automated Exfiltration <a href="#">↗</a>	Account Access Removal <a href="#">↗</a>
Cache Poisoning Information <a href="#">↗</a>	Device Hijacking <a href="#">↗</a>	Device Hijacking <a href="#">↗</a>	Command and Control <a href="#">↗</a>	API Abuse <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Browser Hijacking <a href="#">↗</a>	Application Window Discovery <a href="#">↗</a>	Hosts File Manipulation <a href="#">↗</a>	Application Collected Data <a href="#">↗</a>	Communication Through Removable Media <a href="#">↗</a>	Data Transfer to Cloud <a href="#">↗</a>	Data Destruction <a href="#">↗</a>
Cache Victim Memory Information <a href="#">↗</a>	Compromise Accounts <a href="#">↗</a>	Exploit Public Facing Application <a href="#">↗</a>	Command and Control <a href="#">↗</a>	API Abuse <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Browser Hijacking <a href="#">↗</a>	Browser Information Discovery <a href="#">↗</a>	Local Tool Transfer <a href="#">↗</a>	Audio Capture <a href="#">↗</a>	Communication Through Removable Media <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>	Reverse Remote Services <a href="#">↗</a>	Config Connector <a href="#">↗</a>	API Abuse <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Browser Hijacking <a href="#">↗</a>	Cloud Infrastructure Discovery <a href="#">↗</a>	Reverse Service Session Hijacking <a href="#">↗</a>	Automated Collection <a href="#">↗</a>	Content Injection <a href="#">↗</a>	Data Manipulation <a href="#">↗</a>	Defacement <a href="#">↗</a>
Cache Victim Org Information <a href="#">↗</a>	Desktop Capabilities <a href="#">↗</a>	Hardware Additions <a href="#">↗</a>	Device Configuration <a href="#">↗</a>	API Abuse <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Browser Hijacking <a href="#">↗</a>	Cloud Service Dashboard <a href="#">↗</a>	Reverse Service Session Hijacking <a href="#">↗</a>	Browser Session Hijacking <a href="#">↗</a>	Data Manipulation <a href="#">↗</a>	Data Manipulation <a href="#">↗</a>	Denial of Service <a href="#">↗</a>
Cloud Service Information <a href="#">↗</a>	Desktop Capabilities <a href="#">↗</a>	Hardware Additions <a href="#">↗</a>	Device Configuration <a href="#">↗</a>	API Abuse <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Browser Hijacking <a href="#">↗</a>	Cloud Service Dashboard <a href="#">↗</a>	Reverse Service Session Hijacking <a href="#">↗</a>	Browser Session Hijacking <a href="#">↗</a>	Data Manipulation <a href="#">↗</a>	Data Manipulation <a href="#">↗</a>	Denial of Service <a href="#">↗</a>
Search Open Technical Databases <a href="#">↗</a>	Desktop Capabilities <a href="#">↗</a>	Hardware Additions <a href="#">↗</a>	Device Configuration <a href="#">↗</a>	API Abuse <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Browser Hijacking <a href="#">↗</a>	Cloud Service Dashboard <a href="#">↗</a>	Reverse Service Session Hijacking <a href="#">↗</a>	Browser Session Hijacking <a href="#">↗</a>	Data Manipulation <a href="#">↗</a>	Data Manipulation <a href="#">↗</a>	Denial of Service <a href="#">↗</a>
Search Open Malware Domains <a href="#">↗</a>	Desktop Capabilities <a href="#">↗</a>	Hardware Additions <a href="#">↗</a>	Device Configuration <a href="#">↗</a>	API Abuse <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Browser Hijacking <a href="#">↗</a>	Cloud Service Dashboard <a href="#">↗</a>	Reverse Service Session Hijacking <a href="#">↗</a>	Browser Session Hijacking <a href="#">↗</a>	Data Manipulation <a href="#">↗</a>	Data Manipulation <a href="#">↗</a>	Denial of Service <a href="#">↗</a>
Search Victim-Owned Malware <a href="#">↗</a>	Desktop Capabilities <a href="#">↗</a>	Hardware Additions <a href="#">↗</a>	Device Configuration <a href="#">↗</a>	API Abuse <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Access Token Manipulation <a href="#">↗</a>	Browser Hijacking <a href="#">↗</a>	Cloud Service Dashboard <a href="#">↗</a>	Reverse Service Session Hijacking <a href="#">↗</a>	Browser Session Hijacking <a href="#">↗</a>	Data Manipulation <a href="#">↗</a>	Data Manipulation <a href="#">↗</a>	Denial of Service <a href="#">↗</a>



# Thank you for your attention

Presentation by:

Christos Grigoriadis  
(Focal Point)