

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

# Test di penetrazione

# CSP010\_W \_EDUCON

PRESENTAZIONE DA PARTE DI:  
CHRISTOS GRIGORIADIS (FOCALE PUNTO)



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

- o1. Che cos'è il Red Teaming
- o2. Red Teaming vs Pentesting
- o3. Ciclo di vita dell'attacco
- o4. MITRE ATT&CK
- o5. Introduzione al rosso atomico



# Che cos'è il Red Teaming

## Operazioni della squadra rossa

- Scopo delle operazioni Red Team: Simulare attacchi a tutto campo per testare la sicurezza dell'infrastruttura digitale, dei dipendenti, delle applicazioni e della sicurezza fisica.
- Simulazione di avversari reali: Replicare le tecniche utilizzate dagli avversari reali per scoprire le vulnerabilità e valutare le capacità difensive dell'azienda.
- Ciclo di vita completo dell'attacco: Le operazioni coprono l'intero ciclo di vita di un attacco, fornendo una valutazione completa della preparazione alla sicurezza.
- Rivelazione delle vulnerabilità: Identifica molteplici vettori di attacco e punti deboli che non vengono tipicamente riscontrati nei test di penetrazione standard.



# Che cos'è il Red Teaming

## Impatto e integrazione con il Blue Team

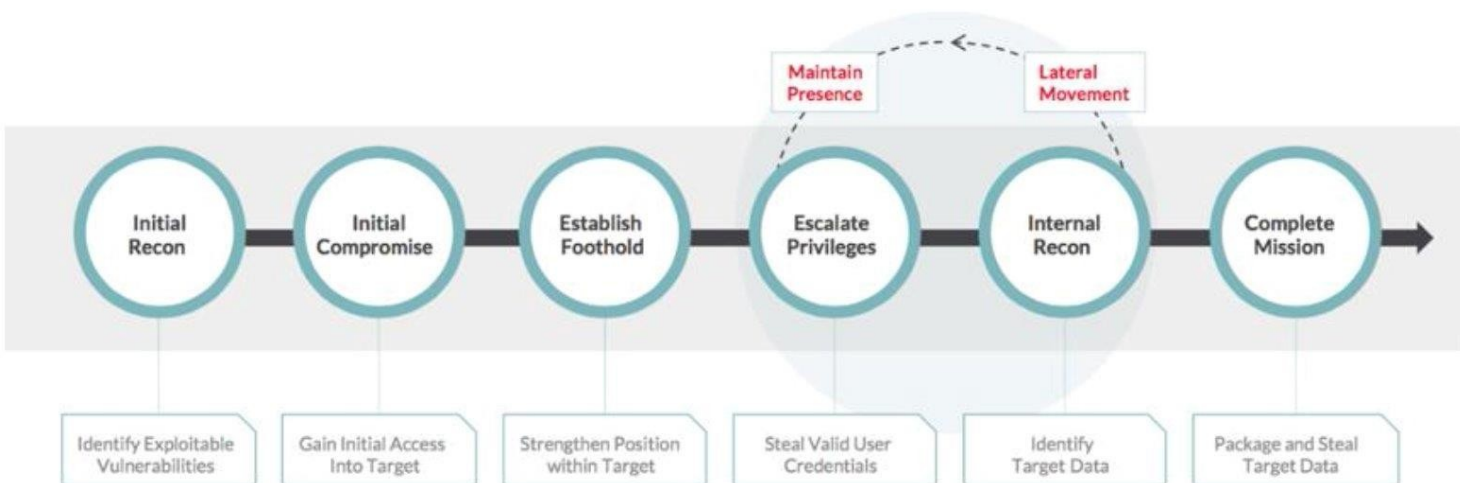
- Risultati attuabili: I risultati del Red Team vengono utilizzati per migliorare le misure di sicurezza e prepararsi a potenziali minacce.
- Collaborazione con il Blue Team:
- Ruolo del Blue Team: Professionisti della sicurezza incaricati dell'identificazione delle vulnerabilità, della correzione e della verifica dell'efficacia.
- Utilizzo dei risultati: Sviluppare firme per le minacce informatiche, implementare protezioni e migliorare la sicurezza delle infrastrutture.
- Addestramento e tempra:
- Formare i dipendenti a resistere all'ingegneria sociale.
- Rettificare le vulnerabilità identificate durante le operazioni.
- Emulazione APT: I Red Team emulano le tecniche delle Advanced Persistent Threats per testare i meccanismi di difesa a lungo termine.



# Red Teaming vs Pentesting

Pentesting	Red Teaming
Ambito definito	Nessun ambito definito
Utilizzato per identificare e sfruttare le vulnerabilità	Emula il comportamento dell'avversario
Fornisce un rapporto sui risultati che vengono di conseguenza utilizzati dalle aziende per applicare patch, rinforzare e proteggere le loro infrastrutture.	Utilizzato per valutare la resilienza di un'organizzazione contro gli attacchi degli avversari.
Prevenzione anziché investigazione. I test di penetrazione sono utili per identificare le vulnerabilità e le minacce, ma non forniscono risultati utilizzabili per il rilevamento proattivo delle minacce in futuro.	Fornisce risultati utilizzabili per il rilevamento.

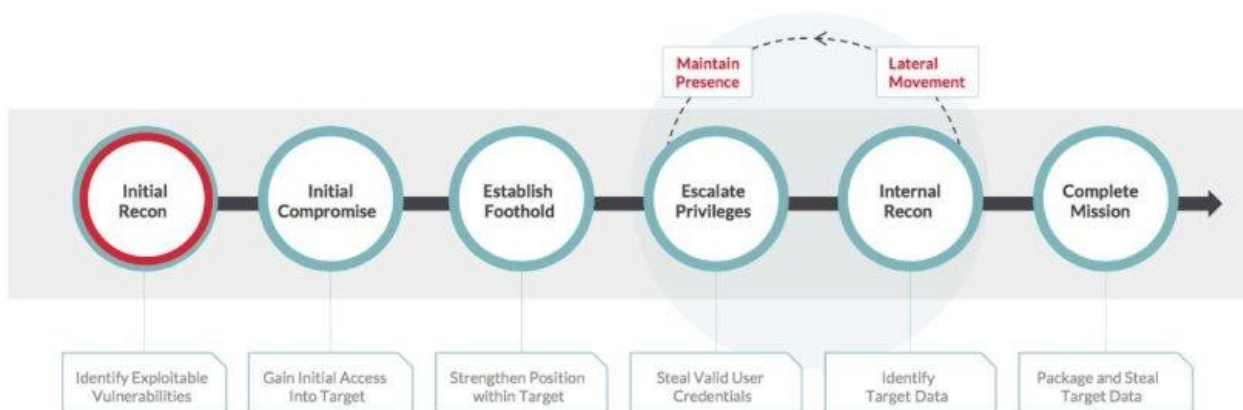
# Ciclo di vita dell'attacco



# Ciclo di vita dell'attacco

## *Attack Lifecycle – Initial Reconnaissance*

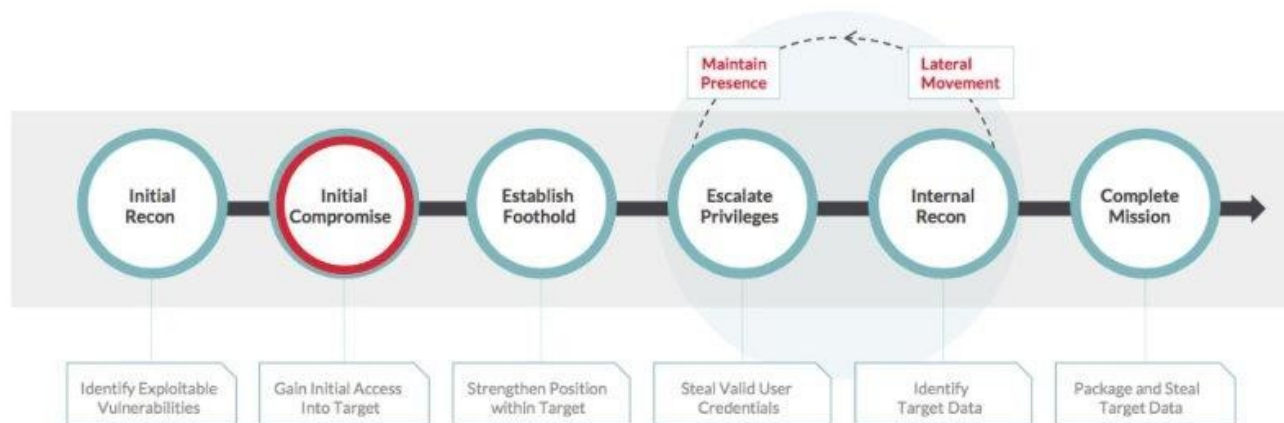
- Open source intelligence gathering
- Network and application reconnaissance
- Remote access identification



# Ciclo di vita dell'attacco

## *Attack Lifecycle – Initial Compromise*

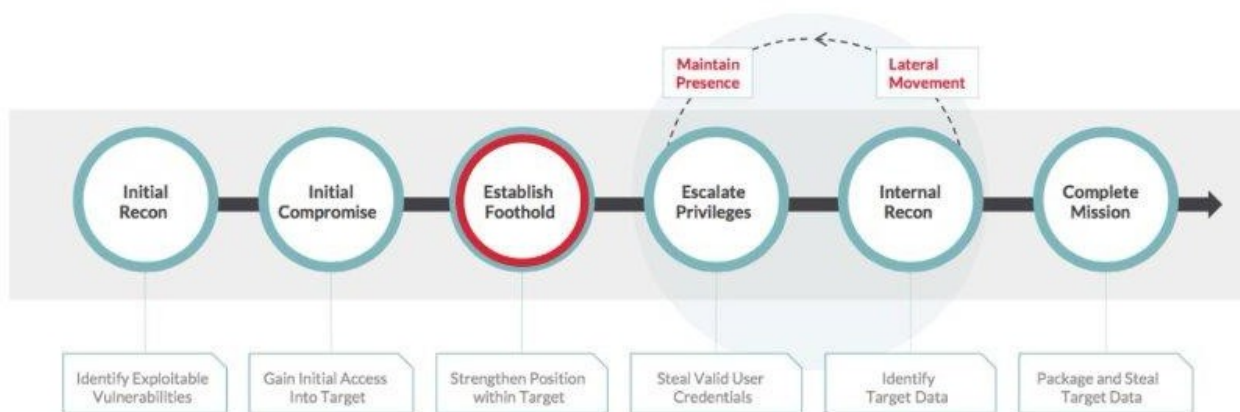
- Social engineering
- Internet-based attack
- Leverage service provider



# Ciclo di vita dell'attacco

## *Attack Lifecycle – Establish Foothold*

- Backdoors
- Remote access subversion



# Ciclo di vita dell'attacco

## *Attack Lifecycle – Escalate Privileges*

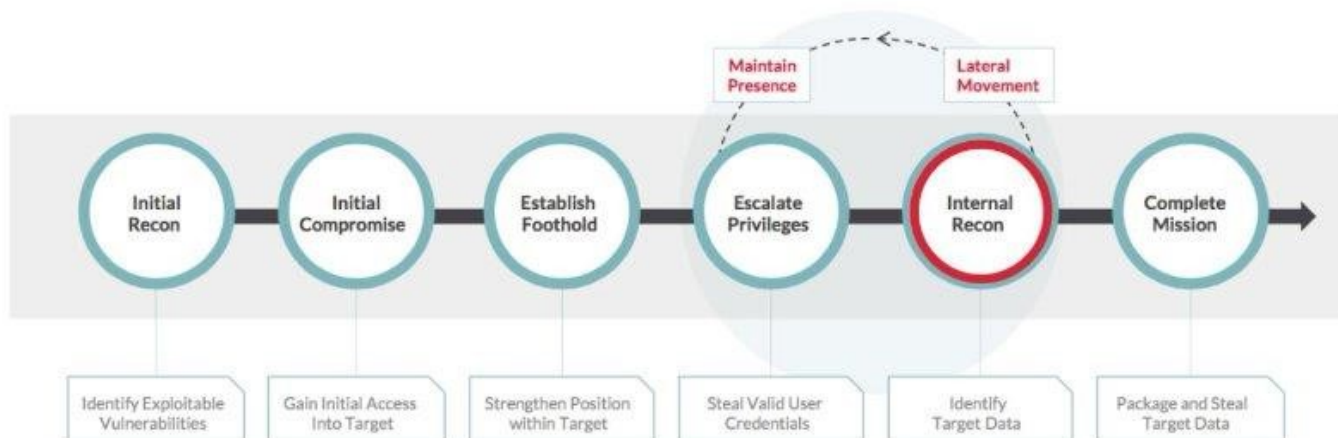
- Credential harvesting
- Password cracking
- Pass-the-Hash



# Ciclo di vita dell'attacco

## *Attack Lifecycle – Internal Reconnaissance*

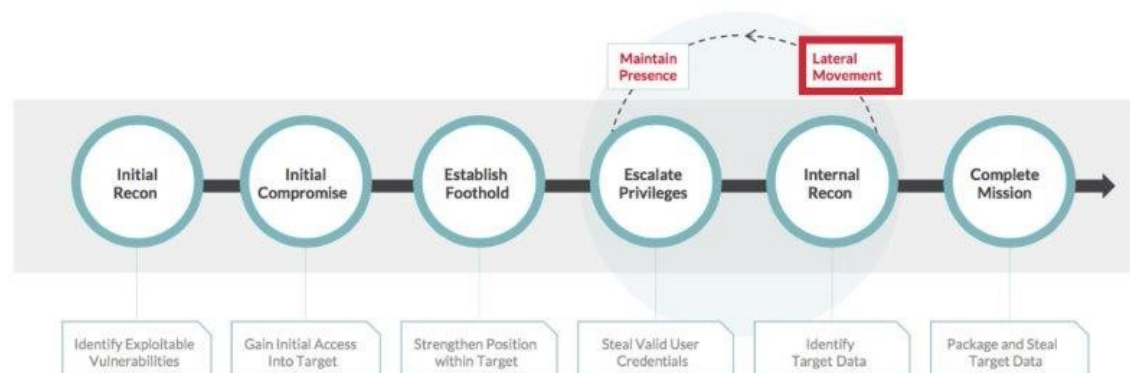
- Critical system identification
- System enumeration
- Account and password enumeration



# Ciclo di vita dell'attacco

## *Attack Lifecycle – Lateral Movement*

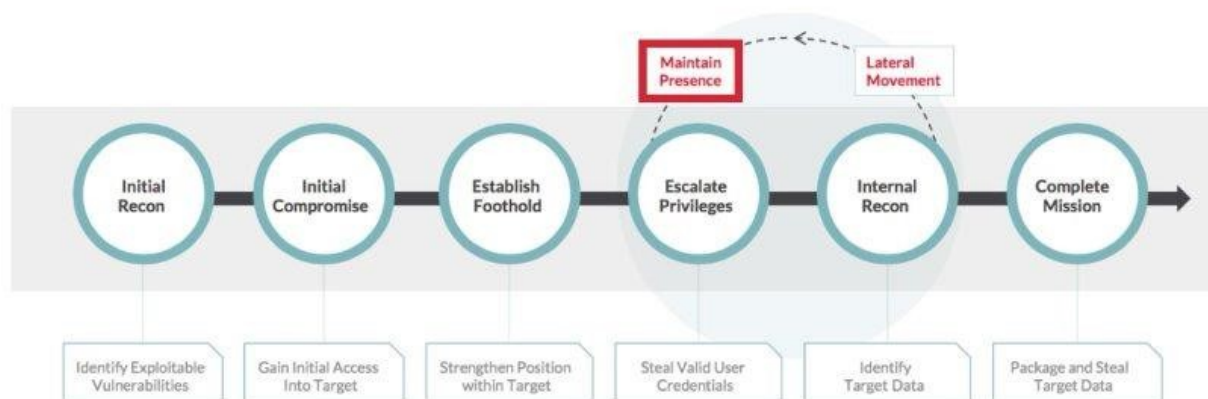
- Remote command execution
- Remote administration tools



# Ciclo di vita dell'attacco

## *Attack Lifecycle – Maintain Presence*

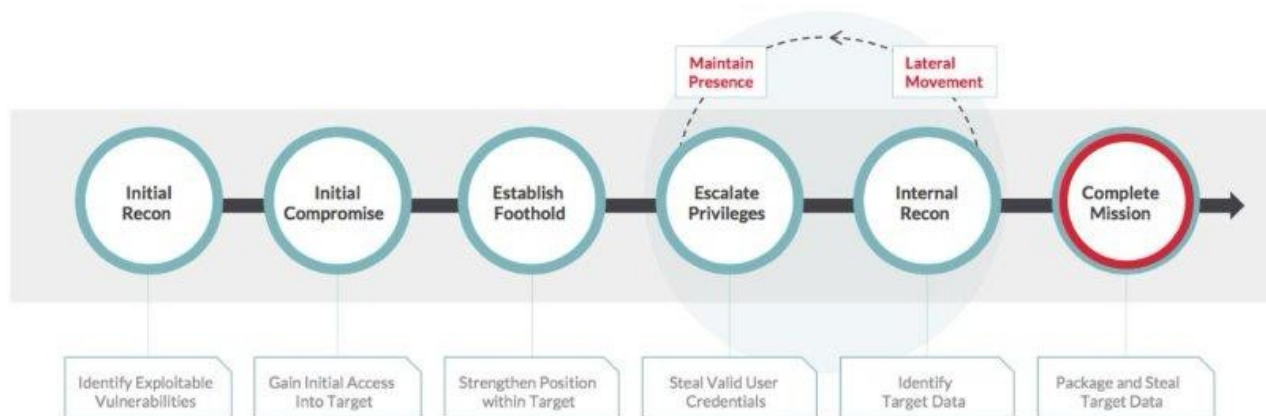
- Command and control
- Remote access subversion
- Account abuse



# Ciclo di vita dell'attacco

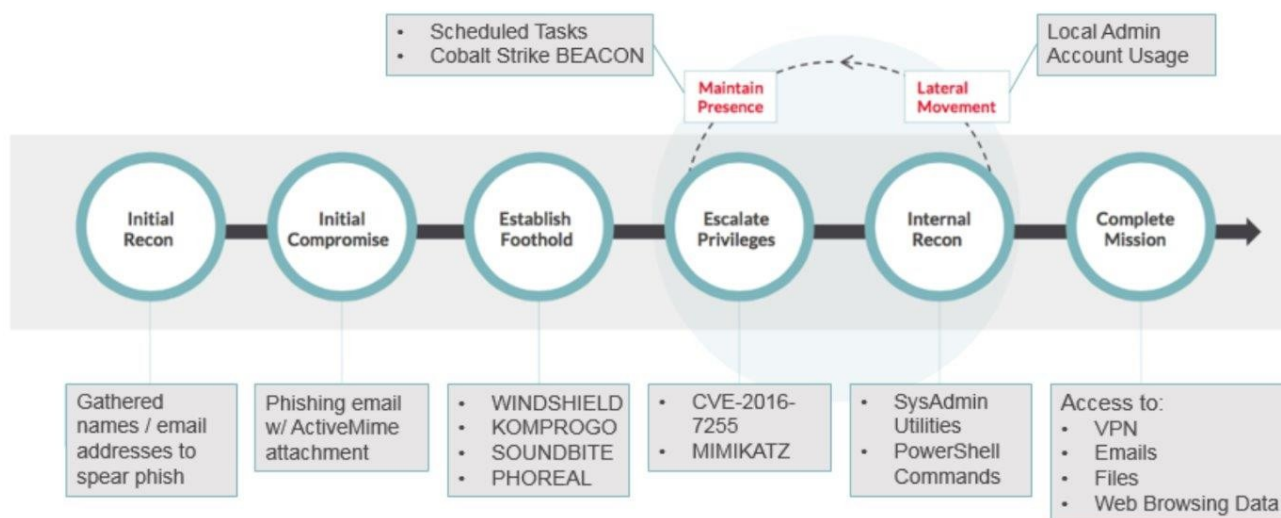
## Attack Lifecycle – Complete Mission

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



# Ciclo di vita dell'attacco

Attack Lifecycle – APT32



# MITRE ATT&CK e l'esplorazione della squadra rossa atomica

Reconnaissance 14 techniques	Resource Development 8 techniques	Initial Access 14 techniques	Execution 14 techniques	Persistence 23 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="#">1</a>	Acquire Credentials <a href="#">1</a>	Common Injection <a href="#">1</a>	Cloud Administration Command <a href="#">1</a>	Account Manipulation <a href="#">1</a>	Abuse Elevation Control Mechanism <a href="#">1</a>	Abuse Elevation Control Mechanism <a href="#">1</a>	Adversary Infiltration <a href="#">1</a>	Account Discovery <a href="#">1</a>	Exploitation of Remote Services <a href="#">1</a>	Infrastructure Discovery <a href="#">1</a>	Application Layer Protocol <a href="#">1</a>	Automated Exfiltration <a href="#">1</a>	Account Access Removal <a href="#">1</a>
Cache Poisoning Information <a href="#">1</a>	Device Interception <a href="#">1</a>	Service to Computer <a href="#">1</a>	Command and Control <a href="#">1</a>	API Jobs <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Cloud Backlog <a href="#">1</a>	Application Vulnerability Discovery <a href="#">1</a>	Host-to-Host Tunneling <a href="#">1</a>	Application Layer Protocol <a href="#">1</a>	Communication Through Removable Media <a href="#">1</a>	Data Transfer Over Cloud <a href="#">1</a>	Data Destruction <a href="#">1</a>
Cache Victim Memory Information <a href="#">1</a>	Competitive Advertising <a href="#">1</a>	Signal Public Facing Application <a href="#">1</a>	Command Administration Command <a href="#">1</a>	API Jobs <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Cloud Backlog <a href="#">1</a>	Business Information Discovery <a href="#">1</a>	Local Tool Transfer <a href="#">1</a>	Application Layer Protocol <a href="#">1</a>	Communication Through Removable Media <a href="#">1</a>	Data Encrypted for Impact <a href="#">1</a>	Data Manipulation <a href="#">1</a>
Cache Victim Network Information <a href="#">1</a>	Competitive Advertising <a href="#">1</a>	Reverse Remote Services <a href="#">1</a>	Config Console <a href="#">1</a>	API Jobs <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Cloud Backlog <a href="#">1</a>	Cloud Infrastructure Discovery <a href="#">1</a>	Reverse Service Session Hijacking <a href="#">1</a>	Application Layer Protocol <a href="#">1</a>	Communication Through Removable Media <a href="#">1</a>	Data Encrypted for Impact <a href="#">1</a>	Data Manipulation <a href="#">1</a>
Cache Victim Org Information <a href="#">1</a>	Device Interception <a href="#">1</a>	Hardware Additions <a href="#">1</a>	Exploitation for Client Execution <a href="#">1</a>	API Jobs <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Cloud Backlog <a href="#">1</a>	Cloud Service Dashboard <a href="#">1</a>	Reverse Service Session Hijacking <a href="#">1</a>	Application Layer Protocol <a href="#">1</a>	Communication Through Removable Media <a href="#">1</a>	Data Encrypted for Impact <a href="#">1</a>	Data Manipulation <a href="#">1</a>
Cloud Backlog <a href="#">1</a>	Device Interception <a href="#">1</a>	Hardware Additions <a href="#">1</a>	Exploitation for Client Execution <a href="#">1</a>	API Jobs <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Cloud Backlog <a href="#">1</a>	Cloud Service Dashboard <a href="#">1</a>	Reverse Service Session Hijacking <a href="#">1</a>	Application Layer Protocol <a href="#">1</a>	Communication Through Removable Media <a href="#">1</a>	Data Encrypted for Impact <a href="#">1</a>	Data Manipulation <a href="#">1</a>
Cloud Capabilities <a href="#">1</a>	Device Interception <a href="#">1</a>	Hardware Additions <a href="#">1</a>	Exploitation for Client Execution <a href="#">1</a>	API Jobs <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Cloud Backlog <a href="#">1</a>	Cloud Service Dashboard <a href="#">1</a>	Reverse Service Session Hijacking <a href="#">1</a>	Application Layer Protocol <a href="#">1</a>	Communication Through Removable Media <a href="#">1</a>	Data Encrypted for Impact <a href="#">1</a>	Data Manipulation <a href="#">1</a>
Cloud Open Technical Database <a href="#">1</a>	Device Interception <a href="#">1</a>	Hardware Additions <a href="#">1</a>	Exploitation for Client Execution <a href="#">1</a>	API Jobs <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Cloud Backlog <a href="#">1</a>	Cloud Service Dashboard <a href="#">1</a>	Reverse Service Session Hijacking <a href="#">1</a>	Application Layer Protocol <a href="#">1</a>	Communication Through Removable Media <a href="#">1</a>	Data Encrypted for Impact <a href="#">1</a>	Data Manipulation <a href="#">1</a>
Cloud Open Malware Database <a href="#">1</a>	Device Interception <a href="#">1</a>	Hardware Additions <a href="#">1</a>	Exploitation for Client Execution <a href="#">1</a>	API Jobs <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Cloud Backlog <a href="#">1</a>	Cloud Service Dashboard <a href="#">1</a>	Reverse Service Session Hijacking <a href="#">1</a>	Application Layer Protocol <a href="#">1</a>	Communication Through Removable Media <a href="#">1</a>	Data Encrypted for Impact <a href="#">1</a>	Data Manipulation <a href="#">1</a>
Cloud Victim Domain Metadata <a href="#">1</a>	Device Interception <a href="#">1</a>	Hardware Additions <a href="#">1</a>	Exploitation for Client Execution <a href="#">1</a>	API Jobs <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Access Token Manipulation <a href="#">1</a>	Cloud Backlog <a href="#">1</a>	Cloud Service Dashboard <a href="#">1</a>	Reverse Service Session Hijacking <a href="#">1</a>	Application Layer Protocol <a href="#">1</a>	Communication Through Removable Media <a href="#">1</a>	Data Encrypted for Impact <a href="#">1</a>	Data Manipulation <a href="#">1</a>



# Grazie per l'attenzione

Presentazione a cura di:

Christos Grigoriadis  
(Punto focale)