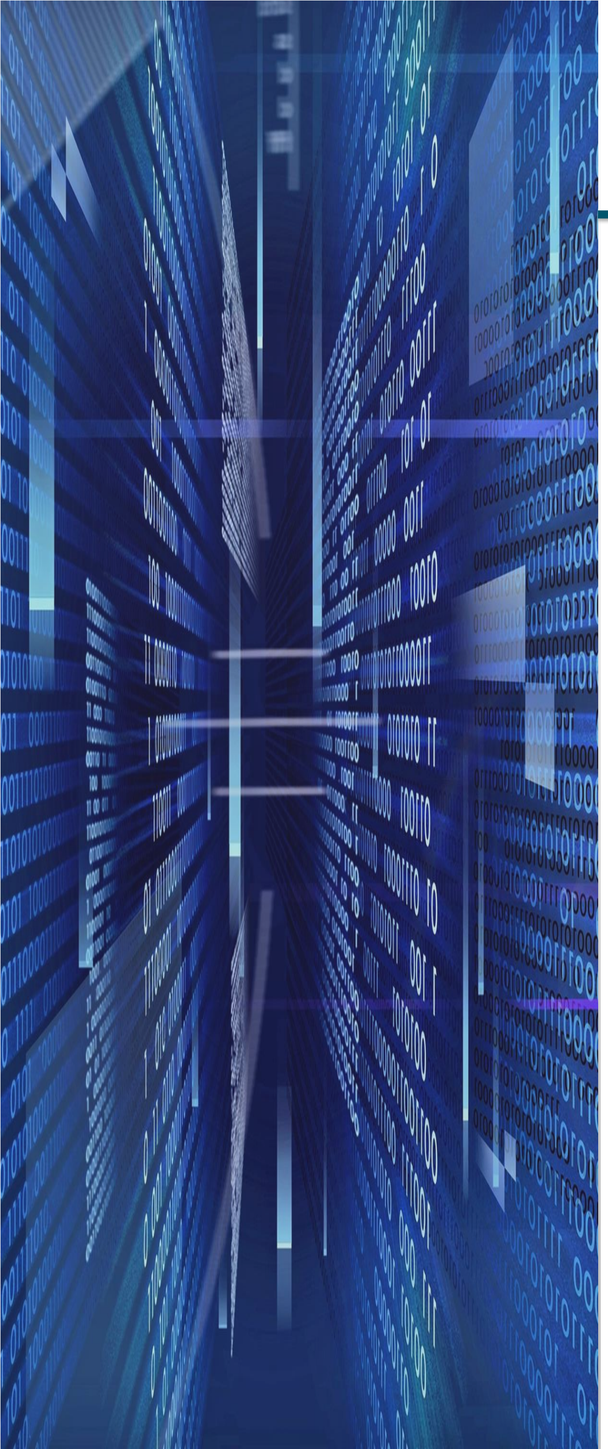


Cyber Kill Chain

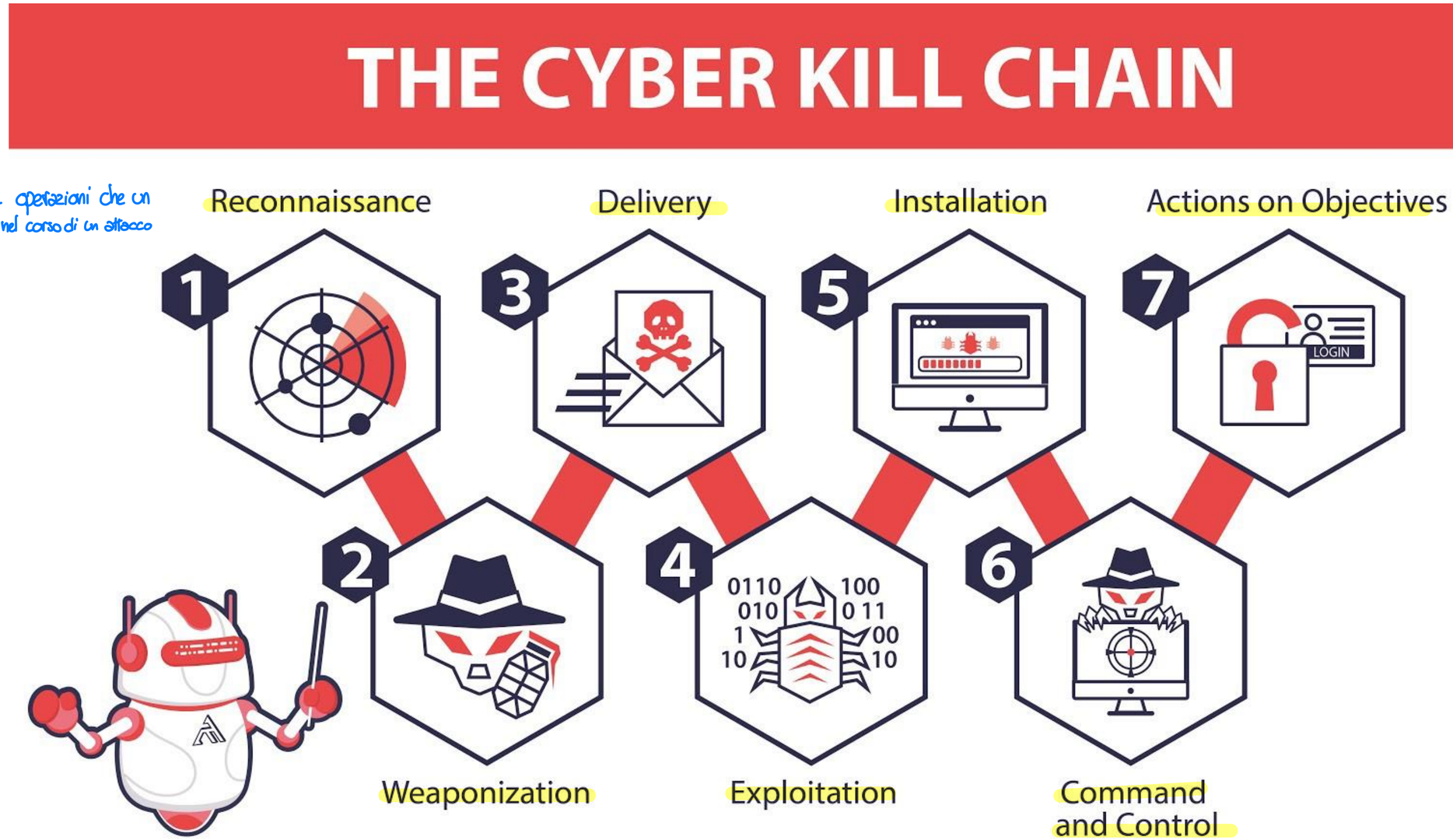
Prof. Federica Paci

Lecture Outline

- Cyber kill chain
  - Reconnaissance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command and Control
  - Actions on Objectives
- Trickbot's Cyber Kill Chain

What is the cyber kill chain?

É la sequenza delle operazioni che un attaccante può eseguire nel corso di un attacco



Reconnaissance

Goal: Select and gather information about the target

Possiamo avere due tipi di reconaissance:

1. **Passive:** gather information without interacting with target
   - **Tools**: whois, Shodan, Google, Social Media, Mantego

2. **Active**: gather information with interacting with target
   - **Tools**: nmap, port scanning, vulnerability scanners

Weaponization

Goal: Find or create the attack to exploit a weakness

Tools:

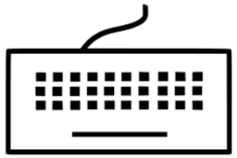
- Metasploit
- Exploit DB
- Veil Framework
- Social Engineering Toolkit
- Cain and Abel
- Aircrack
- SQL Map

Deliver

Goal: Select which venue to deliver the exploit

Web site

Social Media



User Input

Email

USB

Exploitation

Goal: Exploit an existing vulnerability

Examples

- SQL Injection
- Buffer overflow
- Malware
- Javascript hijacking
- User exploitation

Installation

Goal: Maintain persistence inside the environment

Techniques

- DLL Hijacking
- Meterpreter
- Remote Access Trojan
- Registry Changes
- PowerShell commands

Command and Control (C2)

Goal: Establish a command and control channel (C2) with the attacker to remotely manipulate the victim

Examples

- Open two way communications channel to C2 infrastructure
- Most common C2 channels are over web, DNS, and email protocols
- C2 infrastructure may be adversary owned or another victim network itself

Actions and Objectives

Goal: Take actions to achieve their original objectives

Possible actions

- Collect user credentials
- Privilege escalation
- Internal reconnaissance
- Lateral movement through environment
- Collect and exfiltrate data
- Destroy systems
- Overwrite or corrupt data
- Surreptitiously modify data

Trickbot's key features

TrickBot is an advanced Trojan that malicious actors spread primarily by **spearphishing campaigns** using tailored emails that contain malicious attachments or links, which—if enabled—execute malware

Recent attacks use phishing emails, claiming to contain proof of a traffic violation, to steal sensitive information. The phishing emails contain links that redirect to a website hosted on a compromised server that prompts the victim to click on photo proof of their traffic violation

In clicking the photo, the victim unknowingly downloads a malicious **JavaScript file** that, when **opened,** automatically communicates with the malicious actor's command and control (C2) server to **download TrickBot** to the victim's system

Trickbot's key features

Attackers can use TrickBot to:

- Drop other malware, such as Ryuk and Conti ransomware, or
- Serve as an Emotet downloader

- Trickbot has a modular structure
- TrickBot's modules spread the malware laterally across a network by abusing the Server Message Block (SMB) Protocol.
- TrickBot is capable of data exfiltration over a hardcoded C2 server, cryptomining, and host enumeration (e.g., reconnaissance of Unified Extensible Firmware Interface or Basic Input/Output System [UEFI/BIOS] firmware)
- For host enumeration, operators deliver TrickBot in modules containing a configuration file with specific tasks.

Trickbot's cyber kill chain

RECONNAISSANCE

- Gathers information from public data sources to gather email addresses of specific and generic targets

WEAPONIZATION

- Builds out infrastructure, including previously compromised hosts, and creates weaponized malicious documents for upcoming campaigns

DELIVERY

- Generic Spear Phishing to create wide infection base in large scale campaigns
- Observed being deployed through Emotet as a secondary infection
- Spear phishing emails typically contain attachments that are XLS or DOC files with malicious macros embedded in them
- Emails range in themes and sophistication
- Little regard for prevention or detection
- Possible campaign based geographic targeting

EXPLOITATION

- Often after document/dropper is downloaded and opened, victim is tricked to “enable” features inside the program to allow for malicious code execution
- Trickbot has been noted going through extraordinary measures to evade sandboxing and implementing execution triggers to prevent analysis. Examples include the malware only executing upon an image zoom event in Microsoft word

INSTALLATION

- The malicious macros executes PowerShell code to stage the full Trickbot payload
- Multiple HTTP requests may be performed checking in to various command and control servers
- The HTTP requests are made directly to the server IPs resulting in Host headers of the IP addresses
- During installation, Trickbot has been observed checking its’ public IP address by making a request to various external public services

COMMAND + CONTROL

- C2 proxies typically previously compromised infrastructure – often appear to be residential ISPs
- Communicates to its’ command and control servers in a high volume manner, usually every 1-2 seconds. It will cycle through the command and control server list in a round robin fashion
- Communicates over the HTTP protocol with encrypted payloads inside of the protocol

ACTIONS ON OBJECTIVES

- **Primary:** Steals sensitive corporate information & credentials
- **Secondary:** Email harvesting for later spam use
- **NOTE:** Includes many other capabilities
- **Lateral:** Brute forcing using stolen credentials and at times using the ETERNALBLUE Exploit

Cybersecurity

Meccanismi e processi organizzativi che hanno come obbiettivo la protezione utilizzate all'interno di un azienda

Proprietà da garantire

1. Riservatezza e confidenzialità: protezione delle informazioni sensibili
2. Integrità: garantisce e protegge i servizi da modifiche
3. Disponibilità: garantisce che i servizi siano sempre disponibili
4. Autenticità: può essere associato sia agli utenti sia a un software, garantisce l'identità
5. Accountability: garantisce di sapere chi ha svolto le azioni
6. Safety: protezione

Assets

Comprende tutti i beni materiali o meno che hanno un valore per un organizzazione (sistemi, software, persone ....)

Gli assets possono contenere dei punti deboli, le vulnerabilità

→ sfruttate dai cyber threat

Attacco → uno o più cyberthreat che hanno conseguenze sul sistema

Cyber Kill Chain

① Reconnaissance → passiva: raccoglie informazioni senza interagire con l'obbiettivo (navigando in internet), strumenti: (whois, Shodan, Google, social media)

→ attiva: raccoglie informazioni interagendo con l'obbiettivo (nmap, portscanning, vulnerability scanning)

② Weaponization: trovare o creare l'attacco per sfruttare la vulnerabilità (Metasploit, Exploit DB) uses nmap

③ Delivery: scegliere la modalità di delivery dell'agente malevolo (website, social media, email, usb)

④ Exploitation: sfruttare una vulnerabilità presente (SQL injection, bufferoverflow, Malware, Javascript Hijacking, User Exploitation)

⑤ Installation: insediarsi persistentemente nel sistema, eventualmente tentare di elevare i propri privilegi (DLL Hijacking, Meterpreter, Remote Access Trojan)

⑥ Command and Controll: creare un nodo di comunicazione con l'attaccante del sistema infetto per manovrarlo, generalmente a due vie

- Esempio: incapsulare il traffico di rete in un altro protocollo in modo che non venga individuato

⑦ Azioni e Obbiettivi: fare azioni per raggiungere l'obbiettivo originale (ottenere credenziali utente, ottenere privilegi, riconoscimenti interni ....)

Trickbot

Trojan avanzato diffuso tramite spearphishing, utilizzando email personalizzate contenenti elementi damosi che se attivati eseguono il malware

→ usati per rubare informazioni sensibili
↳ phishing attraverso siti web compromessi

→ la vittima scarica un Javascript damoso

Viene utilizzato per installare nuovi malware
Ha struttura modulare

Mitre Attack Matrix

→ Tassonomia con tutte le tattiche utilizzate negli attacchi

Enterprise Techniques

Reconnaissance

L'obbiettivo è ottenere informazioni per pianificare operazioni future
Le informazioni possono essere raccolte attivamente o passivamente, verranno poi utilizzate per l'attacco e durante le altre fasi

Informazioni → dettagli sull'organizzazione
↓ staff
↘ infrastruttura

Tecniche

- Active scanning
- Gather Victim Identity Information
- Gather Victim Host Information
- Phishing for Information
- Search Open Websites/Domains (Code Repositories)

Resource Development

L'attaccante sta cercando di creare risorse che possono essere utilizzate per supportare le operazioni di attacco

Consiste nella creazione o nel rubare account, infrastrutture e capacità.

Tecniche

- Acquire Access
- Acquire Infrastructure
- Compromise Accounts
- Compromise Infrastructure
- Establish Account

Initial Access

L'attaccante cerca di entrare nella rete, attraverso vari vettori di ingresso per ottenere la loro prima "presa" nella rete che poi permetterà di agire nelle fasi successive.

Tecniche

- Supply Chain compromise, compromise software dependencies and development tools
- Valid Account

Execution

L'attaccante tenta di lanciare codice malevolo
Obbiettivi possono essere l'esplorazione di una rete o il furto di dati

Tecniche

- Command and Scripting Interpreter
- Schedule Task / Schedule Job
- User Execution

Persistence

L'attaccante tenta di mantenere le prese acquisite
L'obbiettivo è mantenere l'accesso ai sistemi nonostante riavvii, modifiche delle credenziali e altre interruzioni che potrebbero interrompere il loro accesso

Tecniche

- Account Manipulation
- Boot or logon autostart execution
- Registry run Keys / startup folder
- Event Trigger Execution (Screen Saver, AppInit DLLs)

Privilege Escalation

L'attaccante tenta di elevare i propri permessi

Gli approcci comuni consistono nell'approfittare delle debolezze del sistema, delle errate configurazioni e delle vulnerabilità

Esempi:

- Livello system / root
- Amministratore locale
- Account utente con accesso simile a quello dell'amministratore
- Account utente con accesso a sistemi specifici o per svolgere funzioni specifiche

Spesso si sovrappongono alle tecniche di persistenza

Tecniche

- Bypass User Account Controll
- Token Impersonation / Theft
- Hijacking Execution Flow (DDL Search Order Hijacking)
  ↳ Dirottamento del flusso di esecuzione

Defense Evasion

L'attaccante tenta di eludere le difese e di non essere identificato
Le tecniche includono la disabilitazione e disinstallazione dei software di sicurezza o di offuscamento di dati e script. Gli attaccanti spesso utilizzano processi "sicuri" per nascondere e mascherare i propri malware

Tecniche

- Impair Defenses → obbiettivo disattivare la detection dai firewall e dai sistemi antivirus
- Disable Windows Event Logging
- Hide Artifacts → obbiettivo nascondere gli artefatti creati dal malware sulla macchina infetta
- NTFS file attributes
- Hidden Files and Directories
- Deobfuscate / Decode Files or Information
- Rootkit

Credential Access

L'attaccante cerca di rubare username e password
Le tecniche possono essere il keylogging o il credential dumping, usando credenziali legittime l'attaccante può dare accesso al sistema, risultando più difficile da individuare, può inoltre creare ulteriori account che permettano di raggiungere il goal

Tecniche

- Credential from password stores
- Input Capture → Key logging
- Man In the Middle (multifactor autentication)

Discovery

L'attaccante sta cercando di scoprire il tuo ambiente
L'attaccante utilizza tecniche per acquisire conoscenza sul sistema e sulla rete interna

Tecniche

- Account Discovery → Local Account
- Device Driver Discovery
- Password Policy Discovery

Lateral Movement

L'attaccante cerca di muoversi attraverso l'environment
L'obbiettivo è esplorare la rete alla ricerca dell'obbiettivo e successivamente riuscire ad accedervi

Tecniche

- Internal spearing

Collection

L'attaccante cerca di ottenere informazioni per il suo obbiettivo

Command and Controll

L'attaccante cerca di comunicare col sistema infetto e di controllarlo
L'attaccante cerca di simulare il traffico normale per evitare di essere rilevato

Exfiltration

L'attaccante cerca di rubare i dati

Impact

L'attaccante cerca di manipolare, interrompere o distruggere il sistema e i dati

Tecniche

- Data destruction
- Data Encrypted for Impact
- Defacment

Resources

Eric M. Hutchins, Michael J. Clopperty,Rohan M. Amin, Ph.D.z. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.