

# Esercitazione W19D1 - Pratica 1

## Threat intelligence

Fabio Benevento - 12/03/2024

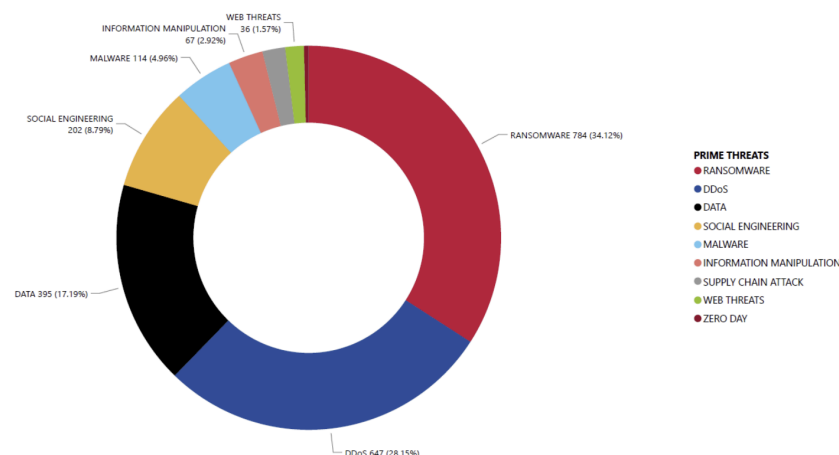
### Traccia

Creare un elenco di minacce comuni che possono colpire un'azienda, ad esempio phishing, malware, attacchi DDoS, furto di dati.

- Inizia raccogliendo informazioni sulle minacce alla sicurezza informatica, utilizzando fonti aperte, i siti web di sicurezza informatica e i forum di discussione.
- Analizza ciascuna minaccia in dettaglio, cercando di comprendere il modo in cui può essere utilizzata per compromettere la sicurezza informatica e i danni che può causare.
- Utilizza queste informazioni per creare un elenco delle minacce più comuni, tra cui malware, attacchi di phishing e attacchi DDoS aggiungendo tutte le informazioni raccolte dall'analisi.

### Implementazione

Secondo il rapporto annuale ENISA, i principali attacchi subiti dalle aziende nel corso del 2023 sono stati gli attacchi di tipo Ransomware, seguiti a stretto giro dagli attacchi di tipo DDoS e da quelli di tipo Data, i quali ricoprono nell'insieme circa l'80% del totale degli attacchi come riportato in figura.



Il ransomware è un tipo di malware che cripta i dati dell'azienda e richiede un pagamento di riscatto per ripristinarli. È una delle minacce più dannose per le aziende in quanto può causare gravi interruzioni delle operazioni e perdite di dati irreversibili.

Gli attacchi di DDos sono un tipo di attacco informatico in cui un grande numero di dispositivi, spesso compromessi e parte di una botnet, invia un elevato volume di traffico alla destinazione desiderata, come un sito web o un server. L'obiettivo principale di un attacco DDoS è sovraccaricare le risorse del sistema di destinazione, rendendolo inaccessibile ai suoi utenti legittimi.

Gli attacchi di tipo "data" si concentrano principalmente sulla manipolazione, il furto o la compromissione dei dati aziendali, compresi dati sensibili, informazioni finanziarie, informazioni personali dei clienti e altro ancora. Questi tipi di attacchi mirano a ottenere accesso non autorizzato ai dati o ad alterarli per danneggiare l'azienda o ottenere un vantaggio illegittimo.

Sempre dal rapporto annuale ENISA, è possibile individuare quelle che sono le principali tecniche di attacco per le tipologie indicate in precedenza riportate nella seguente tabella.

In particolare abbiamo:

### **Ramsonware**

<b>Tactic</b>	<b>Technique</b>
TA0001: Initial Access	T1190: Exploit Public-Facing Application
	T1133: External Remote Services
	T1566: Phishing
	T1199: Trusted Relationship
TA0002: Execution	T1106: Native API
	T1047: Windows Management Instrumentation
TA0003: Persistence	T1197: BITS Jobs

	T1554: Compromise Client Software Binary
	T1136: Create Account
	T1133: External Remote Services
TA0004: Privilege Escalation	T1134: Access Token Manipulation
	T1068: Exploitation for Privilege Escalation
	T1055: Process Injection
TA0005: Defence Evasion	T1134: Access Token Manipulation
	T1197: BITS Jobs
	T1140: Deobfuscate/Decode Files or Information
	T1480: Execution Guardrails
	T1036: Masquerading
	T1112: Modify Registry
	T1027: Obfuscated Files or Information
	T1055: Process Injection
	T1620: Reflective Code Loading
	T1497: Virtualisation/Sandbox Evasion
TA0006: Credential Access	T1555: Credentials from Password Stores
	T1539: Steal Web Session Cookie
TA0007: Discovery	T1087: Account Discovery
	T1217: Browser Bookmark Discovery
	T1135: Network Share Discovery
	T1069: Permission Groups Discovery

	T1057: Process Discovery
	T1012: Query Registry
	T1518: Software Discovery
	T1614: System Location Discovery
	T1033: System Owner/User Discovery
	T1124: System Time Discovery
	T1497: Virtualisation/Sandbox Evasion
TA0008: Lateral Movement	T1210: Exploitation of Remote Services
	T1080: Taint Shared Content
TA0009: Collection	T1560: Archive Collected Data
	T1530: Data from Cloud Storage Object
	T1213: Data from Information Repositories
	T1039: Data from Network Shared Drive
	T1113: Screen Capture
TA0011: Command and Control	T1568: Dynamic Resolution
	T1095: Non-Application Layer Protocol
	T1071: Non-Standard Port
	T1072: Protocol Tunnelling
	T1090: Proxy
	T1102: Web Service
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel
TA0040: Impact	T1485: Data Destruction
	T1499: Endpoint Denial of Service


Gli attacchi di tipo ransomware ricoprono la gran parte delle tattiche del MITRE. In primo luogo, troviamo la tattica “Initial Access” ovvero l’insieme delle tecniche per ottenere il primo accesso al sistema. Per quanto concerne il 2023, le tecniche più utilizzate in questo ambito sono state quelle dello sfruttamento di servizi remoti (External Remote Services) o applicazioni (Exploit Public-Facing Application) che presentano bug software o errori di configurazione che consentono l’accesso al sistema. Altre tecniche sono quelle di Phishing, ovvero l’invio di messaggi tramite vari canali spacciandosi per un servizio/organizzazione conosciuto, o quelle di Trusted Relationship, sfruttando quindi per l’accesso sistemi di terze parti conosciuti dal target e quindi con minori controlli.

La tattica di “Execution” riguarda invece le tecniche utilizzate per l’esecuzione del codice malevolo. Tra queste troviamo l’esecuzione diretta tramite API del sistema operativo (Native API) e quella di Windows Management Instrumentation, ovvero mediante i sistemi di amministrazione dei sistemi Windows.

Per quanto riguarda la persistenza (Persistence), ovvero il mantenimento dell’accesso ai sistemi anche in caso di riavvio, modifica delle credenziali e altre interruzioni che potrebbero interrompere l’accesso, le tecniche più in voga nello scorso anno sono state quelle di BITS job sempre nei sistemi Windows, quella di creazione di account (Create account) o utilizzo di servizi esposti (External Remote Services) o l’utilizzo di backdoor modificando il sorgente binario di un software sul client.

La tattica di “Defence evasion” consiste nelle tecniche che gli avversari utilizzano per evitare il rilevamento durante la loro compromissione. Le tecniche utilizzate per l’evasione della difesa includono la disinstallazione/disabilitazione del software di sicurezza o l’offuscamento/crittografia di dati e script. Gli avversari sfruttano e abusano anche dei processi affidabili per nascondere e mascherare il loro malware.

Per quanto riguarda i ransomware, le tecniche più utilizzate sono state quelle di BITS Job vista in precedenza, quella di Access Token Manipulation, ovvero di modifica dei token per eludere i controlli nell’accesso al sistema, o di modifica



del registro di sistema nei sistemi Windows (Modify Registry), così come l'utilizzo di malware (Deobfuscate/Decode Files and Information) o tramite l'intrusione in un processo esistente (Process Injection). Un'altra tecnica è quella di Virtualization/Sandbox evasion, ovvero di evasione dell'attacco da una macchina virtuale al sistema host.

Per quanto concerne la tattica di Credential Access le tecniche sono l'accesso tramite password salvate in precedenza dall'utente o tramite cookies.

La fase di Discovery consiste nelle tecniche che un avversario può utilizzare per acquisire conoscenze sul sistema e sulla rete interna. Queste tecniche aiutano gli avversari a osservare l'ambiente e a orientarsi prima di decidere come agire.

La ricerca può riguardare gli account (Account Discovery), i bookmark dell'utente nel browser (Browser Bookmark Discovery), la rete (Network Share Discovery), i permessi utente (Permission Groups Discovery), i software presenti sulla macchina e i processi in esecuzione, così come il file system locale.

Tramite la tattica di Lateral movement è possibile, una volta violata una prima macchina, attaccare altri dispositivi sulla stessa rete. In questo caso le tecniche più utilizzate sono quelle di accesso mediante servizi esposti (Exploitation of Remote Services) o tramite l'iniezione di codice malevolo che punta a cartelle condivise (Taint Shared Content).

La raccolta (Collection) consiste nelle tecniche che gli avversari utilizzano per raccogliere e rubare le informazioni. La raccolta può riguardare dispositivi di rete (Data from Network Shared Drive), cloud (Data from Cloud Storage Object) o repository di informazioni (Data from Information Repositories). Rientrano in questa categoria anche lo screenshot dello schermo dell'utente. Il comando e il controllo consistono in tecniche che gli avversari possono utilizzare per comunicare con i sistemi sotto il loro controllo all'interno di una rete vittima. Di solito gli avversari cercano di simulare il traffico normale e previsto per evitare il rilevamento. Esistono molti modi in cui un avversario può stabilire il comando e il controllo, con vari livelli di furtività a seconda della struttura e delle difese della rete della vittima. Relativamente ai Ransomware, le tecniche più utilizzate sono state mediante Web Service, Proxy, Protocol Tunneling, Non-standard Port, Non-ApplicationLayer protocol, e di Dynamic Resolution.

La fase di Exfiltration riguarda invece la fase di prelievo delle informazioni raccolte vero e proprio. Relativamente ai Ransomware tipicamente questa fase avviene mediante un C2 channel ovvero un doppio canale dati e controllo

instaurato in precedenza.

Infine troviamo la tattica di Impact ovvero delle tecniche per malipolare, interrompere o distruggere il sistema target.

Tramite i Ransomware ciò avviene mediante distruzione dei dati (Service Stop), interruzione di un servizio (Service stop) o inibizione dell'accesso tramite rete (Endpoint Denial of Service).

## DDos

Tactic	Technique
TA0042: Resource Development	T1583: Acquire Infrastructure
	T1584: Compromise Infrastructure
TA0005: Defence Evasion	T1553: Subvert Trust Controls
TA0040: Impact	T1485: Data Destruction
	T1489: Service Stop
	T1499: Endpoint Denial of Service
	T1498: Network Denial of Service

La tattica di "Resource Development" è una tattica all'interno del MITRE ATT&CK Framework che riguarda lo sviluppo e l'ottenimento di risorse aggiuntive o strumenti che possono essere utilizzati dagli attaccanti per sostenere e facilitare ulteriori attività dannose. Questa tattica è utilizzata dagli attaccanti per preparare il terreno per attacchi futuri o per migliorare l'efficacia delle loro operazioni di hacking.

Tra di esse troviamo la tecnica "Acquire Infrastructure" e la tecnica "Compromise Infrastructure". La prima tecnica consiste, da parte degli attaccanti, nell'acquistare, affittare o noleggiare infrastrutture che possono essere utilizzate durante il targeting. Una tecnica alternativa invece è quella di compromettere l'infrastruttura per utilizzarla successivamente per gli attacchi, evitando quindi l'acquisto/affitto illustrato in precedenza.

La tattica di “Defence evasion” consiste nelle tecniche che gli avversari utilizzano per evitare il rilevamento durante la loro compromissione. Le tecniche utilizzate per l'evasione della difesa includono la disinstallazione/disabilitazione del software di sicurezza o l'offuscamento/crittografia di dati e script. Gli avversari sfruttano e abusano anche dei processi affidabili per nascondere e mascherare il loro malware.

La tecnica più utilizzata nel 2023 è quella di “Subvert Trust Control”.

L'avversario sta cercando di manipolare, interrompere o distruggere i vostri sistemi e dati.

La tattica “Impact” consiste nelle tecniche che gli avversari utilizzano per interrompere la disponibilità o compromettere l'integrità manipolando i processi aziendali e operativi. Tra le tecniche più utilizzate nell'anno scorso troviamo quella di distruzione dei dati (Data Destruction), di interruzione di un servizio (Service Stop), di degrado o blocco di accesso ad un servizio tramite attacco DDos al target (Endpoint Denial of Service) o alla rete, saturando la banda disponibile (Network Denial of Service)

## Data

Tactic	Technique
TA0003: Persistence	T1197: BITS Jobs
TA0005: Defence Evasion	T1197: BITS Jobs
	T1599: Network Boundary Bridging
TA0009: Collection	T1560: Archive Collected Data
	T1005: Data from Local System
	T1039: Data from Network Shared Drive
	T1025: Data from Removable Media
	T1074: Data Staged
TA0010: Exfiltration	T1020: Automated Exfiltration



	T1048: Exfiltration Over Alternative Protocol
	T1041: Exfiltration Over C2 Channel
	T1052: Exfiltration Over Physical Medium
	T1567: Exfiltration Over Web Service
	T1029: Scheduled Transfer
	T1537: Transfer Data to Cloud Account

La persistenza (“Persistence”) è costituita da tecniche che gli avversari utilizzano per mantenere l'accesso ai sistemi anche in caso di riavvio, modifica delle credenziali e altre interruzioni che potrebbero interrompere l'accesso.


Tra di esse troviamo la tecnica BITS job che sfrutta il Background Intelligent Transfer Service (BITS) di Windows .

Questa tecnica viene utilizzata anche per la tattica Defence Evasion che consiste nelle tecniche utilizzate dall’attaccante per evitare di essere rilevato durante la sua attività. Un’altra tecnica fortemente utilizzata nel 2023 è quella di Network Boundary Bridging tramite la quale gli avversari possono superare i confini della rete compromettendo i dispositivi di rete del perimetro o i dispositivi interni responsabili della segmentazione della rete.

La raccolta (Collection) consiste nelle tecniche che gli avversari possono utilizzare per raccogliere informazioni e nelle fonti da cui vengono raccolte le informazioni rilevanti per il conseguimento degli obiettivi dell'avversario. Spesso, l'obiettivo successivo alla raccolta dei dati è il loro furto (esfiltrazione). Questa fase di raccolta può riguardare il file system locale (Data from Local System), dispositivi di rete (Data from Shared Drive) o dispositivi rimovibili (Data from Removable Device).

Gli avversari possono conservare i dati raccolti in una locazione centralizzata in proprio possesso prima della fase di esfiltrazione (Data Stage). I dati possono essere archiviati prima di essere trasferiti al fine di offuscare i dati rubati e velocizzare la fase di trasferimento (Archive Collected Data).

Infine troviamo la tattica di “Exfiltration” ovvero la vera e propria fase in cui i dati vengono rubati. Questa fase può essere automatizzata (“Automated Exfiltration”) o



svolta manualmente tramite dispositivi fisici (“Exfiltration Over Physical Medium”), web service (“Exfiltration Over Web Service”), tramite un C2 channel ovvero un doppio canale, uno per i comandi e uno per i dati (“Exfiltration Over C2 Channel”) o tramite un protocollo proprietario (“Exfiltration Over Alternative Protocol”). Il processo di esfiltrazione può venire schedato successivamente (“Scheduled transfer”). I dati rubati possono venire copiati su cloud (“Transfer Data to Cloud Account”).