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.

Introduzione

Premessa

L'obiettivo principale di questo esercizio di ricerca di vulnerabilità è acquisire dimestichezza con l'utilizzo della Threat Intelligence (TI) in un contesto reale. Attraverso l'analisi di un comune italiano immaginario, ci si propone di:

- Comprendere le potenzialità della TI nell'identificare le minacce e le vulnerabilità più rilevanti per un'organizzazione.
- Applicare le tecniche e gli strumenti della TI per acquisire informazioni utili a migliorare la sicurezza informatica.
- Sviluppare capacità di analisi critica per valutare le informazioni raccolte e trarre conclusioni significative.

Threat Intelligence

La Threat Intelligence è un insieme di informazioni, analisi e conoscenze relative a:

- **Minacce informatiche:** Attacchi, malware, vulnerabilità e altre forme di minacce che possono colpire un sistema informatico.
- **Attacchi:** Tattiche, tecniche e procedure (TTP) utilizzate dagli hacker per compiere gli attacchi.
- **Attori:** Gruppi di hacker e individui che compiono attacchi informatici.

La TI non è una semplice raccolta di dati, ma un processo continuo di:

- **Raccolta di informazioni:** da diverse fonti, come report, blog, forum, social media e dark web.
- **Analisi delle informazioni:** per identificare le minacce più rilevanti e comprenderne le implicazioni.
- **Diffusione delle informazioni:** agli stakeholder interessati, in modo che possano prendere le opportune decisioni per proteggersi.

La TI può essere categorizzata in tre tipologie principali:

1. Strategic Intelligence:

- Ha come obiettivo primario quello di fornire informazioni sulle minacce e sui potenziali attori delle minacce.
- Fornisce alle compagnie una vista complessiva su come e da chi difendersi.
- Si basa su analisi di lungo termine e trend emergenti.

Esempi:

- Report annuali sulle minacce informatiche.
- Analisi del panorama geopolitico e delle sue implicazioni sulla sicurezza informatica.

2. Tactical Intelligence:

- Include dettagli tecnici e comportamentali sulle minacce.
- Viene condivisa con gli esperti di security per mettere in atto le azioni di risposta.
- Si concentra su minacce specifiche e immediate.

Esempi:

- Indicatori di compromissione (IOC) per un nuovo tipo di malware.
- Analisi di un attacco informatico mirato a un settore specifico.

3. Operational Intelligence:

- Include dettagli specifici per prevenire e rispondere a una singola minaccia.
- Contiene informazioni precise sugli attori della minaccia, la sua provenienza e i potenziali vettori d'attacco.
- Viene utilizzata per la gestione in tempo reale degli incidenti informatici.

Esempi:

- Indicazioni su come mitigare una vulnerabilità specifica.

L'esercizio si concentrerà su alcune specifiche aree di analisi:

- Analisi del panorama delle minacce: Identificazione delle minacce informatiche più diffuse nel settore della pubblica amministrazione.
- Valutazione delle vulnerabilità: Analisi dei sistemi e delle infrastrutture informatiche del comune immaginario per identificare le vulnerabilità sfruttabili dagli hacker.
- Sviluppo di un piano di rimedio: Definizione di azioni concrete per mitigare le vulnerabilità identificate e migliorare la sicurezza informatica del comune.

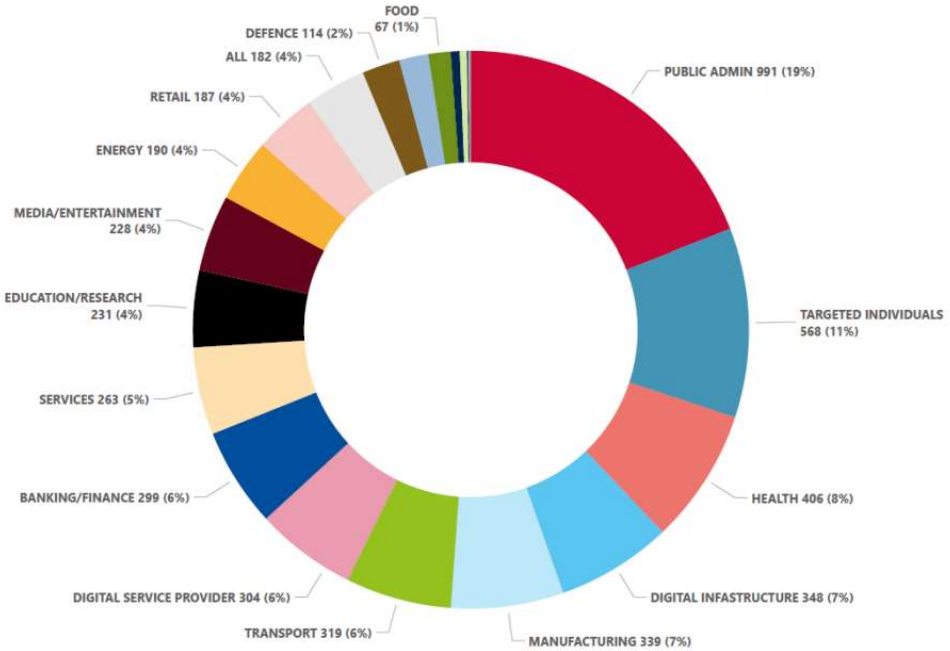
L'utilizzo della TI nell'esercizio permetterà di ottenere una visione più completa e approfondita delle minacce e delle vulnerabilità a cui è esposto il comune immaginario. Questo approccio consentirà di indirizzare le attività di ricerca e di rimedio in modo più efficace e di ottenere risultati più concreti.

Strategic Intelligence

Per la fase di raccolta informazioni utilizzeremo l' ENISA(Agenzia dell'Unione europea per la cibersicurezza) Threat Landscape (ETL), una relazione annuale sullo stato del panorama delle minacce alla sicurezza informatica. Identifica le principali minacce, i principali trend osservati in relazione alle minacce, agli attori delle minacce e alle tecniche di attacco, nonché analisi di impatto e motivazione. Descrive inoltre appropriate misure di mitigazione.

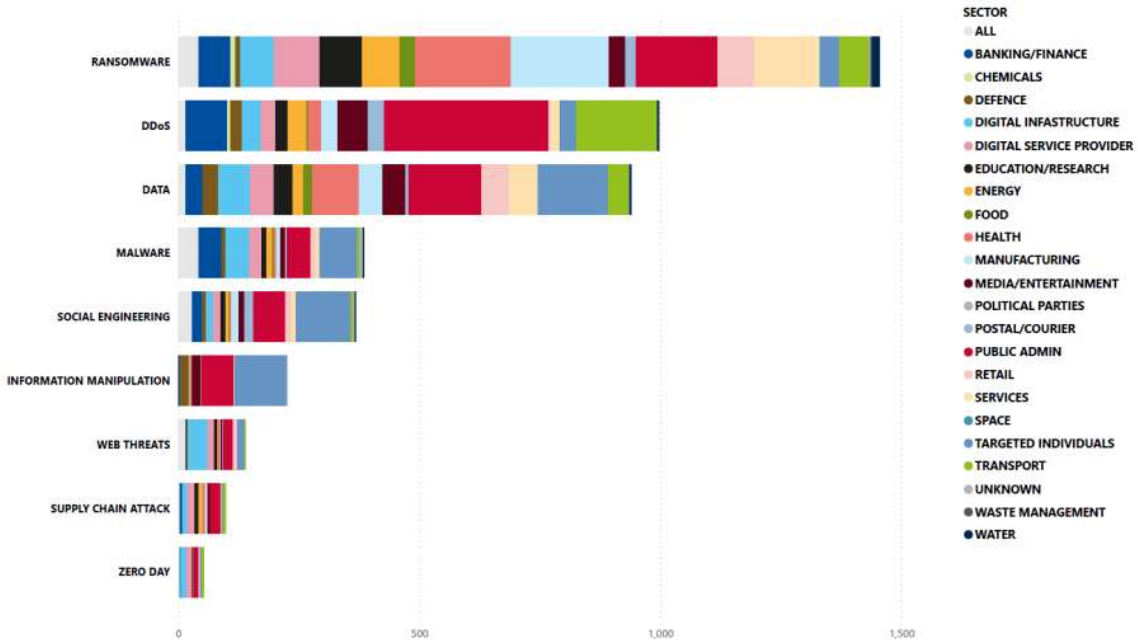
L'analisi dei grafici relativi ai settori colpiti e alle tipologie di attacco per settore è utile per ottenere una panoramica delle minacce più rilevanti per il comune immaginario.

Settori target per numero di incidenti



Il grafico “Settori target per numero di incidenti” mostra che il settore della pubblica amministrazione è il settore più colpito dagli attacchi informatici, con una percentuale del 19% e un totale di 991 attacchi subiti nel periodo da Luglio 2022 a Giugno 2023. Questo dato evidenzia la necessità per il comune immaginario di rafforzare le proprie misure di sicurezza informatica.

Eventi osservati relativi alle principali minacce ETL in termini di settore interessato



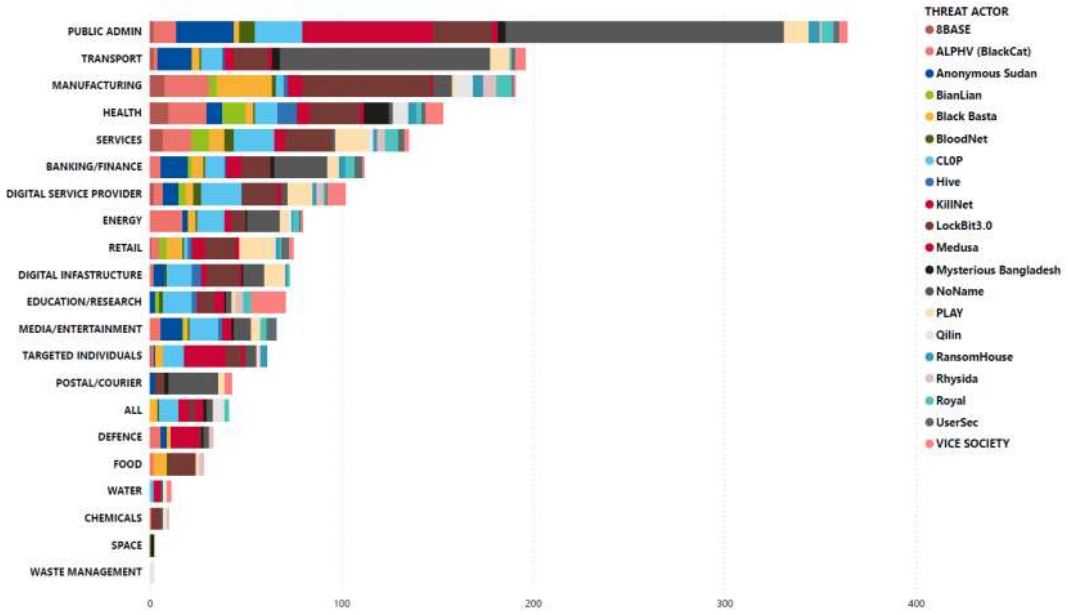
Dall'analisi del grafico “Eventi osservati relativi alle principali minacce ETL in termini di settore interessato” emerge che la pubblica amministrazione ha subito un'ampia varietà di minacce ETL, con una prevalenza di:

- **Ransomware**: attacchi che criptano i dati e richiedono un riscatto per la loro decrittografia.
- **DDoS (Distributed Denial-of-Service):** attacchi che mirano a sovraccaricare i sistemi informatici con un volume eccessivo di traffico, rendendoli inaccessibili.
- **Data (Data Breach, Data Leak e Data Manipulation)**: violazioni che causano la perdita, il furto o la modifica di dati sensibili.

Altri tipi di minacce ETL osservate includono:

- Malware
- Social Engineering
- Information Manipulation
- Web Threat
- Supply Chain Attack
- Zero Day

Attori delle minacce per settore

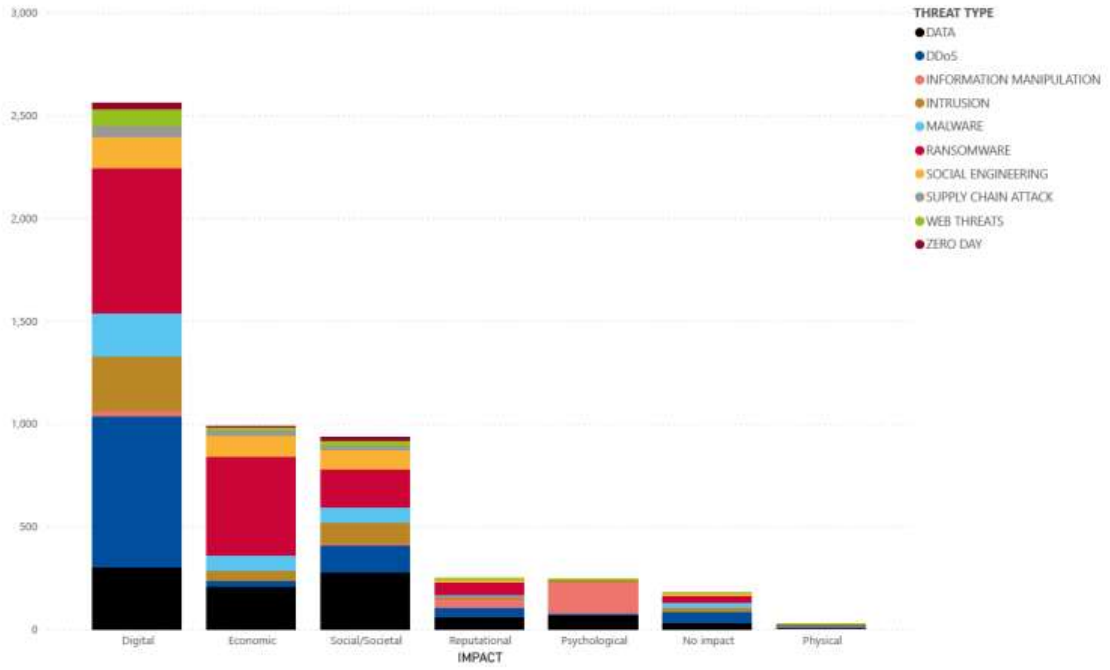


L'analisi del grafico “Attori delle minacce per settore" evidenzia come i gruppi di cybercriminalità organizzata siano gli attori delle minacce più prevalenti nella pubblica amministrazione.

Noname è un gruppo di hacker filorussi che ha rivendicato la responsabilità di diversi attacchi DDoS contro siti web italiani nel 2022 e 2023. Tuttavia, l'impatto di questi attacchi è stato generalmente basso e non ha causato danni significativi.

Focus geografico: Noname sembra concentrarsi principalmente su attacchi contro obiettivi ucraini e occidentali. L'Italia non è stata un bersaglio primario del gruppo.

Ripartizione dei tipi di minacce per impatto



L'analisi del grafico "Ripartizione dei tipi di minacce per impatto" ci permette di identificare impatti per ogni tipologia di attacco, ad esempio prendendo in esame i Ransomware, possiamo stabilire che hanno avuto prevalentemente 3 tipologie di impatto:

1. **Impatto digitale:**
   - Danneggiamento o indisponibilità di sistemi informatici, con conseguente interruzione dei servizi erogati alla cittadinanza.
   - Corruzione di file di dati, con la perdita di informazioni sensibili o di interesse pubblico.
   - Esfiltrazione di dati, con il rischio di violazioni della privacy e di danni reputazionali.

2. **Impatto economico:**
   - Perdite finanziarie dirette per il pagamento dei riscatti.
   - Costi di ripristino dei sistemi informatici e dei dati danneggiati.
   - Danni alla sicurezza nazionale in caso di perdita di dati sensibili o di sistemi critici.

3. **Impatto sociale:**
   - Disagio e frustrazione per i cittadini che non possono accedere ai servizi essenziali.
   - Preoccupazione per la sicurezza dei propri dati personali.
   - Danno alla fiducia nelle istituzioni pubbliche.

Tactical Intelligence

La tactical intelligence si concentra sul qui e ora, fornendo informazioni immediate e specifiche sulle minacce informatiche in atto. Grazie a questa conoscenza, i team di sicurezza possono:

- Rilevare tempestivamente intrusioni e attacchi in corso.
- Comprendere le tattiche, tecniche e procedure (TTP) utilizzate dagli avversari.
- Accelerare la risposta agli incidenti e minimizzare i danni.
- Ottenere una visione approfondita del panorama delle minacce in tempo reale.

Il grafico ANNEX: MAPPING TO MITRE ATT&CK FRAMEWORK mappa le TTP utilizzate dagli avversari alle tattiche e tecniche descritte nel MITRE ATT&CK Framework.

RANSOMWARE

The current table highlights the techniques in the MITRE ATT&CK® Framework associated with ransomware software, ransomware groups or both, according to Ransomware techniques in ATT&CK[MS]. Note that this is a dynamic representation based on actual observations. These can change over time as groups evolve and use new techniques. Every threat actor uses its own specific tools and attack patterns. This overview groups all common techniques, starting from initial access.

Tactic	Technique	Mitigation
TA0001: Initial Access	T1190: Exploit Public-Facing Application T1133: External Remote Services T1566: Phishing T1199: Trusted Relationship	M1048: Application Isolation and Sandboxing M1050: Exploit Protection M1030: Network Segmentation M1026: Privileged Account Management M1051: Update Software M1016: Vulnerability Scanning M1042: Disable or Remove Feature or Program M1035: Limit Access to Resource Over Network M1032: Multi-factor Authentication M1049: Antivirus/Antimalware M1031: Network Intrusion Prevention M1021: Restrict Web-Based Content M1054: Software Configuration M1017: User Training M1018: User Account Management
TA0002: Execution	T1106: Native API T1047: Windows Management Instrumentation	M1040: Behaviour Prevention on Endpoint M1038: Execution Prevention M1026: Privileged Account Management M1018: User Account Management
TA0003: Persistence	T1197: BITS Jobs T1554: Compromise Client Software Binary T1136: Create Account T1133: External Remote Services	M1037: Filter Network Traffic M1028: Operating System Configuration M1018: User Account Management M1045: Code Signing M1030: Network Segmentation M1032: Multi-factor Authentication M1026: Privileged Account Management M1042: Disable or Remove Feature or Program M1035: Limit Access to Resource Over Network
TA0004: Privilege Escalation	T1134: Access Token Manipulation T1068: Exploitation for Privilege Escalation T1055: Process Injection	M1018: User Account Management M1026: Privileged Account Management M1048: Application Isolation and Sandboxing

Operational Intelligence

Oltre a quanto già descritto, il grafico ANNEX: MAPPING TO MITRE ATT&CK FRAMEWORK può essere utilizzato per verificare l'efficacia delle operazioni di mitigazione messe in atto contro le minacce informatiche.

Processo di verifica:

- Identificare le TTP utilizzate in un attacco.
- Mappare le TTP alle tattiche e tecniche del MITRE ATT&CK Framework.
- Valutare le difese in atto contro le TTP identificate.
- Identificare le eventuali lacune nelle difese.
- Implementare le misure di mitigazione necessarie per colmare le lacune.