Università degli Studi di Camerino

Scuola di Scienze e Tecnologie

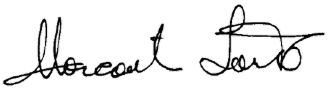
Corso di Laurea in Informatica (Classe L-31)

Profilazione degli avversari nel panorama del cyberspazio

Laureando
Alessandro Bernaschi

Matricola 109325

Relatore
Fausto Marcantoni



Correlatore
Alessandro Rossetti

A.A. 2021/2022

Indice

Elenco dei codici

Elenco delle figure

Elenco delle tabelle

1. Introduzione

Sapere è potere. Spesso non ci rendiamo conto dell'importanza di questa frase, specialmente se riferita al panorama delle informazioni che circolano sul Web. E non parlo di informazioni nell'accezione più generalista del termine, ma parlo delle *nostre* informazioni: del "like" spensierato che lasciamo su un post, di una notizia che leggiamo su La Repubblica, di un commento ad un articolo del nostro partito politico preferito ecc. L'essere umano spesso e volentieri desidera sentirsi potente e al sicuro, tanto da credere che basti selezionare "Rifiuta" all'interno dell'avviso dei Cookies, che appare ogni volta che si visita un sito, per sentirsi protetto dal pericolo che qualcuno possa in qualche modo risalire a lui.

Viviamo in un mondo, virtualmente parlando, in cui enormi quantità di informazioni circolano ovunque alla velocità della luce, e, oltre alle multinazionali, che scambiano i dati dei cittadini tra di loro o li vendono a compagine terze, ci sono anche persone o gruppi di persone, chiamati "avversari", che usano le suddette informazioni per realizzare i propri obiettivi. Le aziende vengono continuamente bersagliate da nuove tipologie di gruppi avversari organizzati. Non è più come una volta, in cui individui singoli si destreggiavano nello sperimentare nuovi metodi per eludere la sicurezza. Questi gruppi avversari agiscono secondo dei modelli di business ben precisi e sofisticati. Difendersi è sempre più difficile, ma con il progresso che avanza siamo in grado di studiare i comportamenti di questi gruppi e di costruire delle difese ad-hoc. Come vedremo più avanti, alla base di tutto questo c'è una lezione fondamentale, ossia di quanto il *sapere*, accennato in precedenza, sia importante, perché in questo contesto, come nella vita, è con la conoscenza che possiamo elevarci, riuscendo a prevenire e a difenderci dai pericoli nel migliore dei modi.

1.1 Obiettivi

In questa tesi parleremo dell'Intelligence applicata al cyberspazio, dell'uso di varie metodologie e strumenti messi in atto per prevenire e mitigare varie tipologie di attacchi informatici e, infine, di come è composto un report e dello sviluppo di un applicativo che sarà in grado, in base alle TTP(Tattiche, Tecniche, Procedure) di un gruppo avversario, di fornire una probabilità di appartenenza ad un determinato gruppo.

1.2 Struttura della Tesi

Dopo l'introduzione del primo capitolo si parlerà, nel secondo capitolo, del concetto di Intelligence: parleremo del Ciclo di vita dell'Intelligence, delle varie metodologie per recuperare le informazioni (INTS) e infine di come è strutturata l'Intelligence in Italia.

Nel terzo capitolo entreremo più nel dettaglio, parlando di una delle tante branche dell'Intelligence, ovvero la Cyberthreat Intelligence; le sue tipologie, come è composta e delle varie tipologie di avversari.

Il quarto capitolo parla del framework MITRE ATT&CK, verrà analizzato nel dettaglio e ci fornirà una maggiore conoscenza di tutto il panorama della cybersicurezza, parlando di delle tattiche utilizzate dagli avversari, degli strumenti che hanno utilizzato, nomi dei gruppi ecc.

Il quinto ed ultimo capitolo parlerà di come è composto un report per la profilazionedi un avversario e della creazione di un applicativo che sarà in grado, una volta inserite le TTP (Tattiche, Tecniche e Procedure) di un gruppo avversario, di fornirci una percentuale di appartenenza ad un determinato gruppo.

2. L'Intelligence

L'Intelligence è il prodotto dell'elaborazione di una o più notizie di interesse per la sicurezza nazionale. In questa accezione, corrisponde al termine informazione. Il vocabolo, largamente impiegato anche in ambito nazionale, ha valenza generica; viene quindi spesso accompagnato da aggettivi intesi a specificarne finalità (strategica, tattica, operativa), natura (situazionale o previsionale), fonte di provenienza o materia cui si riferisce (economico-finanziaria, militare, etc.). [9]

Figura 2.1: [15]

La frase sottocitata è stata scritta dallo stratega cinese Sun Tzu. Egli era rinomato per per la propria capacità di condurre campagne militari il cui successo era dovuto in gran parte alla propria capacità di raccogliere efficacemente informazioni ed al conseguente processo decisionale guidato dall'intelligence.

"Se un illuminato sovrano ed un saggio
generale sconfiggono il nemico ogni volta
e le loro imprese sono così meravigliose
da apparire sovrumane, tutto ciò lo
si deve alle previsioni derivate dalle
informazioni sulla situazione nemica".
(Sun Tzu, L'arte della guerra)

Come esempio a noi più vicino abbiamo la storia di Alan Turing. Considerato uno dei padri dell'informatica, fu uno dei più brillanti crittoanalisti che operavano in Inghilterra durante la Seconda Guerra Mondiale, per decifrare i messaggi scambiati dalle Potenze dell'Asse. Ideò una serie di tecniche per violare i cifrari nemici, consentendo al controspionaggio inglese di *decifrare* i messaggi tedeschi *codificati* con la macchina "Enigma". Tra le sue innumerevoli scoperte annoveriamo la "Macchina di Turing", potente strumento teorico largamente usato nella teoria della calcolabilità e nello studio della complessità degli algoritmi, ed il "Test di Turing", criterio su cui si basa buona parte dei successivi studi sull'intelligenza artificiale. I frutti del suo ingegno non gli valsero, peraltro, né fama né fortuna: condannato per omosessualità, morì suicida. Nel 2009 il Governo inglese si è scusato per il trattamento che gli venne riservato secondo le leggi dell'epoca.

2.1 Il Ciclo di Intelligence

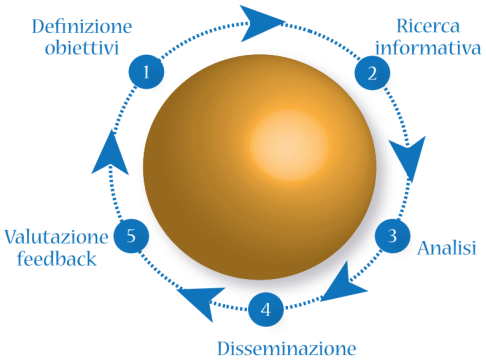


Figura 2.2: Ciclo Intelligence

Il ciclo di Intelligence è composto da 5 fasi: [8]

1. **Definizione obiettivi:** si determinano gli obiettivi e si identificano le migliori fonti da utilizzare per trovare le informazioni che si stanno cercando.

2. **Ricerca informativa:** inizia la ricerca di informazioni riguardanti gli obiettivi prefissati. Ci sono varie applicazioni del ciclo sulla base delle informazioni provenienti da fonti differenti: Osint, Humint, Sigint, Geoint, Technint, Masint.

3. **Analisi:** Questa fase è un passaggio chiave, in quanto, trasforma i dati e le notizie raccolte in un prodotto finito impiegabile, ed è anche il primo momento nel quale è possibile riorientare la ricerca delle informazioni. Ci sono due tipi di analisi: analisi tattica, circoscritta ad un ambiente specifico e serve per dare risposte utilizzabili nell'immediatezza, ed analisi strategica che ha invece l'obiettivo di valutare le possibili linee di sviluppo, ed individuare i fattori che daranno forma al futuro in modo che i decisori possano pianificare le proprie strategie e implementare le relative politiche.

4. **Disseminazione:** La quarta fase, la disseminazione, prevede che i risultati ottenuti vengano comunicati ai destinatari in modo breve, preciso e conciso.

5. **Valutazione feedback:** L'ultima fase, il feedback, produce un resoconto di come si sia svolta l'attività di ricerca, riorientandola ed effettuando una valutazione delle fonti e del processo di analisi che sono stati applicati. Il feedback viene eseguito alla fine di ogni fase.

2.1.1 Le metodologie INTs

Le cosiddette "INTs" accennate nel paragrafo precedente, sono metodologie che guidano la ricerca e l'analisi delle notizie a seconda delle risorse impiegate e delle fonti dalle quali tali notizie provengono. Si distinguono in:

- Humint (Human Intelligence): per le notizie provenienti da persone fisiche
- Sigint (Signals Intelligence): per i segnali e/o le emissioni elettromagnetiche

- Geoint (Geospatial Intelligence): per dati ed immagini georeferenziati
- Masint (Measurement and Signature Intelligence): per i dati metrici, angolari, spaziali, di lunghezza d'onda, etc. di eventi ed obiettivi di interesse informativo
- Osint (Open Source Intelligence): per le informazioni tratte da fonti aperte
- CTI (Cyber Threat Intelligence): la disciplina volta all'acquisizione, elaborazione e analisi di dati al fine di avere un quadro più chiaro delle minacce e comprendere le motivazioni, gli obiettivi e le modalità operative degli avversari.[5]

2.2 L'Intelligence in Italia

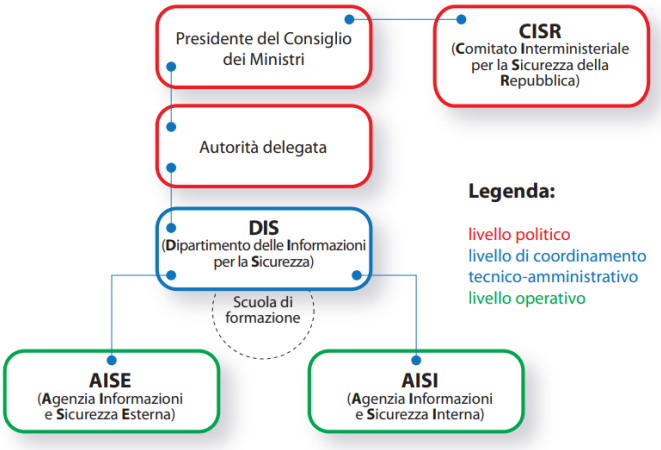


Figura 2.3: Struttura Intelligence in Italia

La comunità intelligence italiana è stata costruita dal Legislatore come un "sistema", il Sistema di informazione per la sicurezza della Repubblica. Il vertice del Sistema è il Presidente del Consiglio dei ministri che, tra l'altro, presiede il Comitato Interministeriale per la Sicurezza della Repubblica (CISR), l'organo collegiale cui spetta anche definire gli obiettivi informativi, quegli obiettivi, cioè, su cui concentrare l'attività di intelligence.

Il Presidente del Consiglio può delegare ad un Ministro senza portafoglio o ad un Sottosegretario di Stato, che assumono la denominazione di Autorità delegata, le funzioni che non gli sono attribuite in via esclusiva.

Rispondono tutti al livello politico gli organismi informativi veri e propri: il Dipartimento delle Informazioni per la Sicurezza (DIS), incaricato di assicurare unitarietà all'attività di informazione per la sicurezza, coordinando l'azione dell'Agenzia Informazioni e Sicurezza Esterna (AISE) e dell'Agenzia Informazioni e Sicurezza Interna (AISI), entrambe chiamate a proteggere gli "interessi politici, militari, economici, scientifici ed industriali dell'Italia", l'una gravitando all'esterno del territorio italiano, l'altra all'interno dei confini nazionali.

L'attività di intelligence è sottoposta ad una serie di controlli. Particolarmente pregnante e significativo il controllo politico-parlamentare affidato a COPASIR che, presieduto da un esponente dell'opposizione, verifica in modo sistematico e continuativo che l'attività del Sistema di informazione per la sicurezza si svolga nel rispetto della Costituzione e delle leggi, nell'esclusivo interesse e per la difesa della Repubblica e delle sue Istituzioni.[10]

In aggiunta allo schema 2.3, si considera fondamentale il ruolo dell'ACN (Agenzia per la cybersicurezza nazionale) e il ruolo della CNAIPIC (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche):

- **ACN:** è un ente di diritto pubblico italiano, istituito a tutela degli interessi nazionali nel campo della cybersicurezza. Viene presieduto da un'Autorità delegata e il suo compito è quello di analizzare tutte le operazioni di cyber-intelligence che gli sono state pervenute da agenzie di intelligence, così da poter utilizzare

questi dati nel campo, favorendo specifici percorsi formativi per lo sviluppo della forza lavoro nel settore, e sostenendo campagne di sensibilizzazione, oltre che una diffusa cultura della cybersicurezza.[16]

- **CNAIPIC:** è l'unità specializzata, interna al Servizio di polizia postale e delle comunicazioni, dedicata alla prevenzione e repressione dei crimini informatici diretti ai danni delle infrastrutture critiche nazionali.[17]

3. Cyber Threat Intelligence

La Cyber Threat Intelligence (CTI), consiste nell'attività di raccolta, elaborazione e analisi di dati provenienti da varie fonti in merito agli attacchi informatici che colpiscono o sono potenzialmente in grado di offendere la sicurezza di un'organizzazione.

Il patrimonio conoscitivo acquisito viene messo a disposizione di tutti gli stakeholder in modo da poter attuare consapevolmente strategie ed azioni utili alla prevenzione, alla mitigazione e all'eliminazione delle minacce, a partire da una corretta valutazione dei rischi.

Grazie al crescente grado di consapevolezza sull'argomento, sia i tecnici che i decisori non tecnici possono dare il giusto valore alle procedure di sicurezza ed assumere un atteggiamento strategicamente proattivo, che si traduce in una operatività concreta ed efficiente nel rilevare e prevenire gli attacchi informatici.[14]

3.1 Tipologie

Diverse sono le procedure individuate per la raccolta e analisi dei dati per informare in maniera dettagliata gli stakeholder. Esistono fondamentalmente quattro differenti approcci tipologici, aventi scopi differenti nell'informazione, sia per quanto riguarda l'oggetto d'indagine, sia riguardo al modo di comunicare il risultato delle analisi.[14]

1. **Cyber Threat Intelligence strategica**

   Ha l'obiettivo di individuare i potenziali attacchi informatici e le loro conseguenze per comunicarli ad un pubblico non tecnico, come nel caso dei decisori che risultano decisivi nel destinare i fondi necessari affinché le attività di sicurezza siano svolte nel modo migliore. L'approccio strategico deriva dalla volontà di far comprendere al meglio le dinamiche delle minacce e le possibili conseguenze nel caso in cui dovessero concretizzarsi i relativi rischi. Il risultato di questa attività generalmente si concretizza nella produzione di report e insight per descrivere nel dettaglio i rischi e le tendenze delle cyberminacce a livello globale, con un livello di attenzione specifico per le possibili ricadute nel contesto aziendale.

2. **Cyber Threat Intelligence tattica**

   Il focus della componente tattica risiede nel rilevare i comportamenti, le TTP (Tattiche, Tecniche e Procedure) e gli indicatori di compromissione che gli avversari adottano per dare forma ai loro attacchi. Il pubblico di riferimento in questo caso è composto dagli analisti CTI interni all'azienda, impegnati nella protezione di sistemi e dati.

Questa tipologia di Intelligence permette ai team di Cybersecurity di capire come la loro organizzazione potrebbe essere attaccata o compromessa, i modi migliori per difendersi e mitigare un attacco.

3. **Cyber Threat Intelligence tecnica**

   L'approccio tecnico si concentra soprattutto sui possibili indicatori di un attacco informatico, con particolare attenzione nei confronti di quelli che vengono definiti attacchi social engineering, che mirano a sfruttare l'ignoranza e la disattenzione dei dipendenti per ottenere informazioni riservate e dati sensibili, come le credenziali di accesso per i servizi dell'azienda, oltre a procedere con dei veri e propri furti di identità. Un classico esempio è costituito da tutta l'attività che ruota intorno al Phishing e a tutte le sue sottovarianti.

   La cyberthreat intelligence tecnica tramite la cybersecurity mira ad informare con costanza e precisione i dipendenti delle aziende sui possibili attacchi di cui potrebbero rimanere vittime.

4. **Cyber Threat Intelligence operativa**

   La CTI operativa punta a fornire conoscenza sugli attacchi informatici, sulle vulnerabilità, su eventi o campagne e quindi sfruttare tali informazioni per avviare attività di cybersecurity mirate, con lo scopo di mettere in sicurezza il perimetro contro tali minacce. Coloro che lavorano all'interno dei SOC (Security Operations Center) o dei CERT (Computer Emergency Response Team) sono i maggiori consumatori di intelligence operativa in quanto si occupano principalmente della gestione delle vulnerabilità, della risposta agli incidenti e del monitoraggio delle minacce.

3.2 Life Cycle

A livello operativo, nel corso degli anni, sono stati definiti vari framework per offrire le linee guida utili ai SOC (Security Operation Center) e agli IRT (Incident Response Team) per svolgere le loro attività investigative sui sistemi di sicurezza aziendali. Uno di questi, forse il più celebre, è il framework MITRE ATT&CK, acronimo di Adversarial Tactics, Tecniques and Common Knowledge.

Generalizzando i contenuti di un framework, vediamo quali sono i cinque step tipo di un possibile lifecycle di threat intelligence.

1. **Raccolta dei dati:** in questa fase, vengono raccolti dati e informazioni provenienti da diverse fonti, come feed di intelligence, fonti aperte, dati interni dell'organizzazione e collaborazioni con partner esterni. La raccolta dei dati può comprendere informazioni su vulnerabilità, indicatori di compromissione, minacce emergenti, comportamenti anomali, campagne di attacco, strumenti malware e altro ancora.

2. **Analisi:** i dati raccolti vengono analizzati per estrarre informazioni significative e rilevanti. Questa fase coinvolge l'identificazione di modelli, correlazioni e tendenze all'interno dei dati per comprendere meglio le minacce e le loro caratteristiche. L'analisi può essere condotta utilizzando metodi manuali o automatizzati, e spesso coinvolge l'uso di strumenti e tecnologie specializzate.

3. **Produzione:** in questa fase, i risultati dell'analisi vengono tradotti in intelligence utile e comprensibile. Le informazioni rilevanti vengono organizzate e formattate in modo da facilitare la loro comprensione e utilizzo da parte dei destinatari. Questa fase può includere la creazione di report, avvisi di sicurezza, feed di intelligence, indicatori di compromissione e altri prodotti intellettuali.

4. **Distribuzione:** l'intelligence prodotta viene distribuita agli utenti interessati, che possono essere sia interni che esterni all'organizzazione. La distribuzione può avvenire attraverso canali come avvisi di sicurezza, feed di intelligence, sistemi di gestione delle minacce, piattaforme di condivisione delle informazioni o tramite rapporti diretti alle parti interessate. È importante garantire che le informazioni raggiungano le persone giuste al momento giusto.

5. **Utilizzo:** le informazioni di intelligence vengono utilizzate per migliorare la sicurezza dell'organizzazione. Gli utenti dell'intelligence possono adottare misure proattive o reattive per mitigare le minacce, proteggere i sistemi e le reti, individuare e rispondere agli attacchi in corso, informare la pianificazione delle difese e migliorare le strategie di sicurezza complessive.

È importante sottolineare che il ciclo di vita della CTI è un processo continuo e iterativo. Le informazioni ottenute dall'utilizzo vengono utilizzate per raffinare le fasi successive del ciclo, migliorando così la capacità di rilevare, prevenire e rispondere alle minacce informatiche.

3.3 Protocollo TLP

Il protocollo TLP (Traffic Light Protocol) è un sistema utilizzato per la condivisione e la gestione delle informazioni riservate. È ampiamente utilizzato nel contesto della sicurezza informatica e dell'interoperabilità tra organizzazioni e agenzie governative.

Il TLP definisce quattro livelli di sensibilità delle informazioni, o label colorate, che indicano come le informazioni possono essere condivise e gestite. Di seguito sono elencate le quattro tipologie di label colorate utilizzate nel protocollo TLP[1]:

- **TLP:CLEAR**

  I destinatari possono diffonderla a livello globale, non c'è limite alla divulgazione. Le fonti[1] possono essere classificate TLP:CLEAR quando le informazioni comportano il rischio minimo o non prevedibile di uso improprio, in conformità con le regole e le procedure applicabili per il rilascio pubblico. Soggette alla legislazione sul copyright, le informazioni TLP:CLEAR possono essere condivise senza restrizioni.

- **TLP:GREEN**

  Divulgazione limitata, i destinatari possono diffonderla all'interno della loro comunità. Le fonti possono essere classificate TLP:GREEN quando le informazioni sono utili per aumentare la consapevolezza all'interno della loro comunità più ampia. I destinatari possono condividere le informazioni TLP:GREEN con colleghi e organizzazioni partner all'interno della loro comunità, ma non pubblicamente. Le informazioni non possono essere condivise al di fuori della comunità. Nota: con comunità intendiamo quella della sicurezza/difesa informatica.

- **TLP:AMBER**

  Divulgazione limitata, i destinatari possono diffonderla solo in caso di necessità all'interno della loro organizzazione e dei suoi clienti. TLP:AMBER+STRICT limita la condivisione solo all'organizzazione. Le fonti possono essere classificate TLP:AMBER quando le informazioni richiedono supporto, da parte dei clienti, per essere utilizzate efficacemente, ma comportano rischi per la privacy, la reputazione o le operazioni se condivise al di fuori delle organizzazioni coinvolte. I destinatari possono condividere le informazioni TLP:AMBER con i membri della propria organizzazione e dei suoi clienti, ma solo in caso di necessità per proteggere la loro organizzazione e i suoi clienti e prevenire ulteriori danni.

- **TLP:RED**

  Solo per gli occhi e le orecchie dei singoli destinatari, nessuna ulteriore divulgazione. Le fonti possono utilizzare TLP:RED quando non è possibile agire efficacemente sulle informazioni senza rischi significativi per la privacy, la reputazione o operazioni delle organizzazioni coinvolte. I destinatari non possono quindi condividere le informazioni TLP:RED con nessuno altro. Nel contesto di una riunione, ad esempio, le informazioni TLP:RED sono limitate ai presenti alla riunione.

[1]Per fonti si intende informazioni generate. Può accadere che a determinate informazioni prodotte con un certo grado di TLP, potrebbe essere aggiunto, dopo una valutazione che trova nuovi dettagli, un grado più alto di quello riportato precedentemente. È importante che questi vincoli vengano rispettati o si può ricorrere in sanzioni.

3.4 Pyramid of Pain

La Pyramid of Pain è una rappresentazione dei tipi di indicatori di compromissione (IoC[2]) che misura la potenziale utilità della threat intelligence e si concentra sulla risposta agli incidenti e sulla ricerca delle minacce.[11]

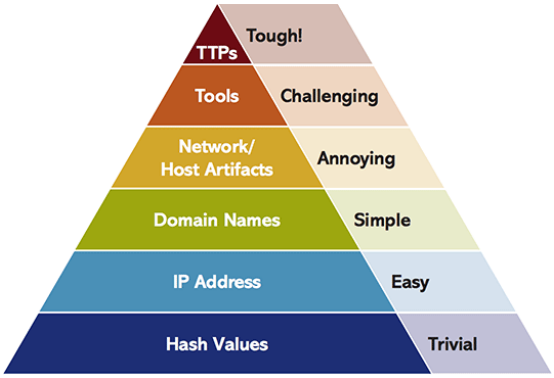


Figura 3.1: David Bianco Pyramid of Pain

- **Trivial (banale): valori hash**

  Un valore hash viene generato da algoritmi come MD5 e SHA e rappresenta un file dannoso specifico. Gli hash forniscono riferimenti specifici a malware e file sospetti utilizzati dagli utenti malintenzionati per l'intrusione.

- **Easy (facile): indirizzi IP**

  Gli indirizzi IP sono uno degli indicatori fondamentali di un attacco dannoso, ma un indirizzo IP è possibile modificarlo facilmente e frequente tramite proxy o VPN.

- **Simple (semplice): nomi di dominio**

  Potrebbe essere presente un nome di dominio[3] o persino un tipo di sotto-dominio registrato, pagato e ospitato. Tuttavia, molti service provider DNS hanno reso meno rigidi gli standard di registrazione.

- **Annoying (fastidioso): artefatti di rete/host**

  Gli artefatti di rete sono attività che possono identificare un utente malintenzionato e distinguerlo da un utente legittimo. Uno standard potrebbe essere un modello URI o informazioni C2 incorporate nei protocolli di rete. Gli artefatti host sono elementi osservabili causati da attività "avversarie" su un host che identifica attività dannose e le distingue dalle attività legittime. Tali identificatori includono chiavi o valori di registro noti per essere creati da malware o file/directory rilasciati in determinate aree.

[2]L'indicatore di compromissione è, nella informatica forense, un artefatto osservato in una rete o all'interno di un sistema che con un'alta probabilità è correlabile, o indica, un'intrusione.[18]

[3]In genere un dominio viene offuscato all'interno di un file dannoso per renderne difficile il rilevamento

- **Challenging (problematico): strumenti**

  Gli strumenti includono minacce che creano documenti dannosi per attacchi spear phishing, strumenti di password cracking o altre utility che sono in grado di compromettere il sistema.

- **Tough (Difficile): TTP**

  Tattiche, tecniche e procedure sono in cima alla piramide. Riguardano l'intero processo in base al quale gli avversari portano a compimento la loro missione, dall'inizio della fase di ricerca fino all'esfiltrazione dei dati, comprendendo tutte le operazioni nel mezzo.

  Questo processo viene svolto dal framwork ATT&CK di MITRE che è diviso in due parti:

  1. **ATT&CK:** possiede una raccolta di tutte le TTP (Tattiche, Tecniche e procedure) di un avversario, a differenza di molti framework ATT&CK va molto nel dettaglio nella descrizione di ogni singola tecnica con le sue sotto-tecniche.
  2. **D3FEND:** possiede una knowledge base delle tecniche di contromisura per la sicurezza informatica. È un insieme di tecniche difensive correlate con tecniche offensive/avversarie che ritroviamo in ATT&CK. L'obiettivo principale di D3FEND è aiutare a standardizzare il vocabolario utilizzato per descrivere la funzionalità della tecnologia di sicurezza informatica difensiva.

3.5 Studio degli Avversari

Sono 4 i gruppi di attori nel mondo della cybersecurity che sono stati individuati [6]:

1. **State-Sponsored**

   Gli attacchi state-sponsored sono attacchi informatici effettuati da uno stato-nazione contro un altro governo, organizzazione o individuo. Questi attacchi possono essere motivati da obiettivi politici, economici o militari. Costituiscono una preoccupazione crescente sia per le imprese che per i governi di tutto il mondo e sono svolti da gruppi con ampie risorse, spesso altamente sofisticate, da cui è spesso difficile difendersi.

   Questi attacchi state-sponsored hanno il potenziale per prendere di mira e distruggere infrastrutture critiche, come reti elettriche e sistemi finanziari e causare danni economici diffusi. Mentre alcuni attacchi sono progettati per rubare informazioni o interrompere le operazioni, altri hanno lo scopo di seminare il caos e causare danni economici. Le organizzazioni prese di mira da tali attacchi possono subire gravi perdite economiche, danni alla loro reputazione e, in alcuni casi, anche causare morte.[2]

   Uno degli attacchi più noti è la massiccia epidemia del ransomware NotPetya che, secondo alcuni ricercatori, è ancora considerato l'incidente di sicurezza informatica più costoso della storia. Un piccolo retroscena: il conflitto tra Ucraina e Russia ha portato molte volte il braccio informatico del Cremlino a raggiungere l'Ucraina oltre il confine russo. Ciò ha causato interruzioni di corrente e ha distrutto terabyte di dati dell'Ucraina. La tensione politica e la guerra non dichiarata andavano avanti da quattro anni. Usando l'Ucraina come banco di prova per le sue tattiche di guerra informatica, la Russia ha lasciato le porte aperte sotto forma di vulnerabilità del software in cui potevano rientrare quando volevano.

   I danni causati da NotPetya hanno colpito magnati delle spedizioni globali, aziende farmaceutiche multinazionali, organizzazioni di servizi finanziari e produttori di alimenti. Ha causato danni per 10 miliardi di dollari in tutto il mondo.

   I moderni attacchi informatici State-Sponsored vanno più lontano di quanto potrebbe mai fare la guerra tradizionale e i risultati possono essere catastrofici in tutti i settori. NotPetya ha sfruttato una vulnerabilità del software che aveva una soluzione nota: molte delle organizzazioni interessate da NotPetya avrebbero potuto evitare questo destino se avessero corretto questa vulnerabilità. Sebbene non esista un'unica risposta per difendersi dagli State-Sponsored, una delle difese più semplici è l'applicazione di patch e l'aggiornamento dei sistemi non appena è disponibile una correzione.

2. **Cybercriminali Organizzati**

   I Cybercriminali organizzati sono motivati dai profitti, sono più interessati a rubare informazioni come numeri di carte di credito, credenziali di account, etc. Ruberanno direttamente alle loro vittime o ruberanno informazioni e/o accessi che possono essere vendute illegalmente nei siti del Deep Web e utilizzeranno qualsiasi mezzo per raggiungere questo obiettivo: phishing, ransomware, cryptominer, trojan ad accesso remoto, exploit kit, social media, furto di dati/finanziario, estorsione e ricatto.

Il gruppo di hacker Fin7 ha preso di mira principalmente i settori della vendita al dettaglio, della ristorazione e dell'ospitalità negli Stati Uniti. Chipotle, Trump Hotels e Whole Foods sono stati vittime del malware di Fin7, violando oltre cinque milioni di numeri di carte di credito e di debito. Grazie alla loro natura altamente organizzata, i Fin7 possono operare in modo efficiente, con un profitto che è arrivato a $ 50 milioni al mese. I Fin7 utilizzano il phishing per diffondere malware sviluppato e testato dai suoi numerosi dipartimenti. Dopo aver scoperto una vulnerabilità nelle applicazioni Microsoft, ai Fin7 è bastato solo un giorno per creare un attacco malware, progettato per rubare il maggior numero possibile di numeri di carte di credito.

3. **Hacktivisti**

   L'hacktivismo include individui o gruppi che usano l'hacking per influenzare il cambiamento politico o sociale. Questi attori fondono l'attivismo politico tradizionale con Internet, consentendo loro di esprimere il malcontento sociale e politico attraverso il cyberspazio. Il panorama degli attivisti informatici è vario e comprende individui e gruppi di vari livelli di competenze e capacità. È noto che gli attivisti informatici utilizzano malware, attacchi DDoS, "doxing", deturpazione di pagine Web e social media per esporre informazioni dannose sul loro obiettivo, da pratiche commerciali ingiuste alla custodia di segreti governativi. Gli attivisti informatici sono attivi dalla metà degli anni '90. L'hacktivismo moderno è stato fortemente plasmato dal gruppo Anonymous per tutto l'ultimo decennio. A differenza dei criminali informatici organizzati Fin7, Anonymous è polimorfo, composto da molte organizzazioni diverse, proxy e hacker affiliati.

   Negli ultimi anni, il gruppo ha preso di mira la campagna presidenziale del 2016 del presidente degli Stati Uniti Donald Trump, nonché lo Stato islamico e il Ku Klux Klan. Dopo gli attacchi dello Stato islamico a Parigi nel 2015, Anonymous ha deciso di smantellare la vasta rete di account sui social media dello Stato islamico per soffocare la diffusione della propaganda. Sebbene il loro motivo fosse per la giustizia sociale, i loro metodi furono messi in discussione poiché avrebbero potuto causare più danni che benefici. È altamente improbabile che Anonymous abbia le competenze antiterrorismo per controllare adeguatamente questi account e promuovere la rimozione di quest'ultimi e degli svariati forum dello Stato islamico ostacolando le operazioni di intelligence di veri esperti di antiterrorismo e di tutta la comunità dell'intelligence che lavora in questo campo.

   Parlando del conflitto russo-ucraino, in Italia abbiamo avuto gli attacchi di "Noname", un gruppo filorusso che tramite attacchi DDOS ha attacco il sito Web del ministero del Lavoro e delle Politiche sociali e quello del Consiglio superiore della magistratura. Ha eseguito inoltre attacchi ai siti Web dei Carabinieri, del ministero degli Esteri, di quello della Difesa e di altre società private italiane.[4]

   Un altro gruppo è Killnet, che ha rivendicato la responsabilità degli attacchi DDoS ai danni della Nato.[19]

   IT Army of Ukraine è invece un gruppo Ukraino arruolato ufficialmente dal governo Ucraino che prende di mira il governo russo. Hanno lanciato una campagna globale di cyber warfare (guerra cibernetica) contro obiettivi collegati a Mosca, che inaspettatamente e in breve tempo ha creato notevoli disagi.[3]

4. **Lupi Solitari**

   I lupi solitari sono una forza potente nell'underground del crimine informatico e sono molto difficili da rintracciare. La ragione? Operano individualmente (in rari casi lavorano con altri complici) e operano sul Dark Web, noto per l'anonimato che fornisce. Un esempio è "gookee", uno sviluppatore di malware probabilmente russo, che opera su un forum di criminalità informatica dal gennaio 2018, vendendo il suo malware ad altri criminali informatici meno esperti. Come molti altri attori, gookee fornisce il crimine informatico come servizio e sul suo forum sono addirittura presenti le recensioni dei clienti sui propri prodotti. Il suo malware "du jour" è un exploit ATM che consente ai suoi compratori di estrarre manualmente contanti dagli sportelli automatici. Questi tipi di avversari risultano difficili da fermare a causa del loro modello di business, che consente loro di prendere le distanze dai crimini commessi dai loro clienti.

3.6 Processo di attribuzione

La determinazione della relazione tra un attacco informatico e uno stato o uno specifico avversario è noto come "attribuzione". Questa attività si basa sull'analisi di una moltitudine di aspetti, come la tipologia di malware, le tipologie di offuscamento del codice o l'infrastruttura, l'analisi geopolitica del Paese dove si trova la vittima ecc.

I principali attori nelle attività di attribuzione oltre ai governi sono le società di cybersecurity; anche se queste non hanno accesso a specifiche fonti e dati riservati, possono contare su avanzate infrastrutture tecnologiche dotate di algoritmi di intelligenza artificiale e machine learning, che consentono di elaborare automaticamente e su larga scala un'enorme mole di dati provenienti dalla telemetria, ossia informazioni ottenute tramite le soluzioni di cybersecurity installate presso i clienti.

Inoltre, algoritmi avanzati permettono di correlare malware e dati contenuti in enormi database. Proprio per questo motivo le società di cybersecurity investono annualmente svariati milioni in ricerca e sviluppo con lo scopo di creare prodotti e servizi di qualità, che permettano alle società e ai governi di individuare tempestivamente attacchi e intrusioni.

L'attribuzione di un attacco può essere fatta a diversi livelli. Quella più semplice potrebbe essere eseguita dal team di cybersecurity della società colpita, a patto che ci sia un processo strutturato, un team di Threat Intelligence e che gli artefatti trovati nei sistemi compromessi (noti come indicatori di compromissione, loC) siano già noti e associati ad un attore di minaccia.

Il livello successivo riguarda l'identificazione della nazione dietro uno specifico attacco ma, prima che l'attribuzione sia fattibile, bisogna analizzare e correlare una moltitudine di attacchi similari. [5]

Per questo motivo sono stati creati svariati framework, uno dei più famosi, tra l'altro utilizzato per la profilazione di un avversario, è ATT&CK di MITRE.

4. MITRE ATT&CK

MITRE ATT&CK è una knowledge base accessibile a livello globale di tattiche, tecniche e procedure avversarie (TTP) basate su osservazioni del mondo reale. La knowledge base di ATT&CK viene utilizzata come base per lo sviluppo di specifici modelli e metodologie di minaccia nel settore privato, nel governo e nella comunità di prodotti e servizi di sicurezza informatica. ATT&CK fornisce una tassonomia comune sia per l'attacco che per la difesa ed è diventato un utile strumento concettuale in molte discipline di sicurezza informatica per trasmettere informazioni sulle minacce, eseguire test tramite red teaming o emulazione dell'avversario e migliorare le difese di rete e di sistema contro le intrusioni.[7]

Figura 4.1: Logo del framework ATT&CK

4.1 Background

MITRE ATT&CK è stato creato nel 2013 come risultato del Fort Meade Experiment (FMX) di MITRE, in cui i ricercatori hanno istituito un laboratorio per emulare il comportamento sia dell'avversario che del difensore nel tentativo di migliorare il rilevamento post-compromissione delle minacce attraverso la telemetria e l'analisi comportamentale. La domanda chiave per i ricercatori era "Stiamo procedendo bene nel rilevare il comportamento documentato di un avversario?" Per rispondere a questa domanda, i ricercatori hanno sviluppato ATT&CK, utilizzato come strumento per classificare il comportamento dell'avversario.[7]

4.2 Come viene utilizzato e da chi?

- **Emulazione dell'avversario**

  ATT&CK può essere utilizzato come strumento per creare scenari di emulazione per testare e verificare le difese contro tecniche avversarie comuni. I profili per specifici gruppi di avversari possono essere costruiti a partire dalle informazioni documentate in ATT&CK. Questi profili possono essere utilizzati anche dai difensori e dagli hunting team per allineare e migliorare le misure difensive.

- **Red Teaming**

  "Il Red Teaming è una metodologia appartenente alla sfera dell'hacking etico che permette di eseguire un attacco simulato a una specifica organizzazione per studiarne i punti deboli. Lo scopo è quello di fornire un'immagine del livello di rischio reale a cui una compagnia è soggetta." [12] ATT&CK può essere utilizzato come strumento per creare piani di red teaming e organizzare operazioni per penetrare determinate misure difensive. Può anche essere utilizzato come roadmap di ricerca per sviluppare nuovi modi di eseguire attacchi che potrebbero essere non rilevati dalle difese comuni.

- **Sviluppo di analisi comportamentali**

  Andando oltre i tradizionali indicatori di compromissione (IoC), l'analisi del rilevamento comportamentale può essere utilizzata per identificare attività potenzialmente dannose all'interno di un sistema o di una rete, che potrebbero non fare affidamento sulla conoscenza precedente di strumenti e indicatori sugli avversari. È un modo per identificare e collegare insieme attività sospette indipendenti da specifici strumenti che possono essere utilizzati dagli avversari.

- **Valutazione del gap difensivo**

  Una valutazione del gap difensivo consente a un'organizzazione di determinare quali parti della propria azienda di riferimento mancano di difese. Queste lacune rappresentano punti ciechi per potenziali vettori che consentono a un avversario di ottenere l'accesso alle sue reti senza essere rilevato o mitigato. ATT&CK può essere utilizzato come modello adversary-focused per valutare gli strumenti, il monitoraggio e le mitigazioni delle difese esistenti all'interno di un'azienda. Le lacune identificate sono utili per dare la priorità agli investimenti per il miglioramento del programma di sicurezza.

- **Valutazione della maturità dei SOC**

  il Security Operations Center di un'organizzazione è una componente fondamentale di molte reti aziendali di medie e grandi dimensioni che monitorano continuamente le minacce contro la rete. Comprendere la maturità di un SOC è importante per determinarne la sua efficacia. ATT&CK può essere utilizzato come misura per determinare l'efficacia di un SOC nel rilevare, analizzare e rispondere alle intrusioni. Analogamente alla valutazione del gap difensivo, una valutazione della maturità del SOC si concentra sui processi utilizzati per rilevare, comprendere e rispondere alle mutevoli minacce nella propria rete nel tempo.

- **Utilità per la Cyber Threat Intelligence**

  La Cyber Threat Intelligence studia le minacce informatiche e i gruppi di avversari che hanno un impatto sulla sicurezza informatica. Include informazioni su

malware, strumenti, TTP, tradecraft, comportamento e altri indicatori associati alle minacce. ATT&CK è utile per comprendere e documentare i profili dei gruppi avversari da una prospettiva comportamentale agnostica rispetto agli strumenti che il gruppo potrebbe utilizzare. Analisti e difensori possono comprendere meglio i comportamenti comuni di molti gruppi e mappare in modo più efficace le loro difese e porsi domande tipo: "come posso difendermi contro il gruppo avversario APT3?". Il formato strutturato di ATT&CK può aggiungere valore ai report di segnalazione delle minacce categorizzando il comportamento al di là degli indicatori standard.

4.3 Il modello ATT&CK

ATT&CK comprende una serie di tattiche, che vanno a descrivere in che modo gli avversari vogliono raggiungere uno o più obiettivi. Le varie tattiche sono formate al loro interno da un insieme di tecniche e sotto-tecniche che danno un ulteriore livello di dettaglio delle procedure e degli strumenti utilizzati per eseguire un attacco.[7]

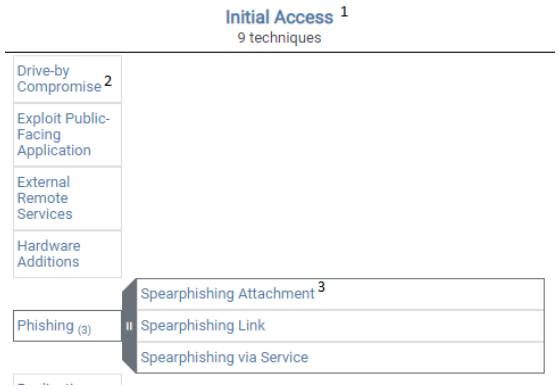


Figura 4.2: 1: Tattiche, 2: Tecniche, 3: Sotto-Tecniche

Ad oggi MITRE ha definito tre domini tecnologici: Enterprise (si basa sulle piattaforme Windows, Mac, Linux e sul cloud), Mobile(si basa su iOS e Android) e ICS (per i sistemi di controllo industriale ICS).

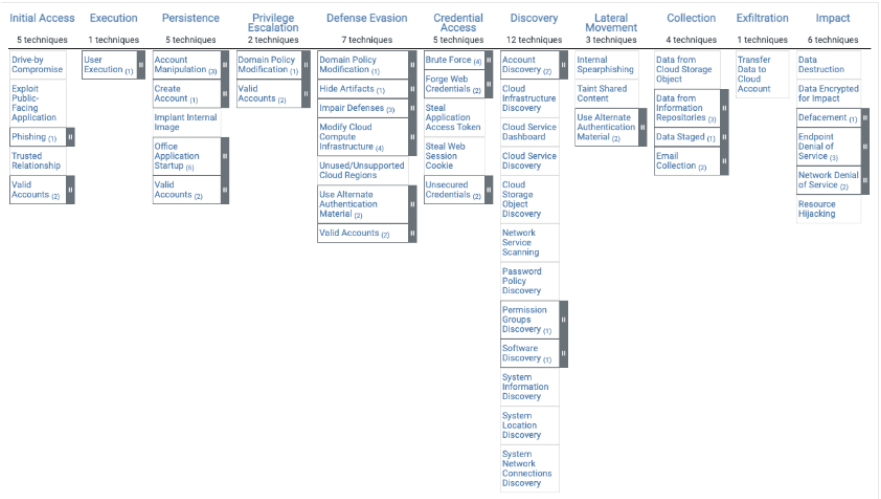


Figura 4.3: Matrice ATT&CK

4.4 ATT&CK vs Cyber Kill Chain

La Cyber Kill Chain è l'altro noto framework utilizzato per comprendere il comportamento degli avversari in un attacco informatico. Il modello Kill Chain è composto dalle seguenti fasi:[13, 5]

1. **Reconnaissance:** l'attaccante esegue delle azioni per identificare il target e i punti più vulnerabili.
2. **Weaponization:** creazione dell'arma digitale (malware o altro) più adattata per l'attacco.
3. **Delivery:** scelta su come avviare l'attacco (es. phishing, sfruttamento vulnerabilità).
4. **Exploitation:** attivazione dell'arma digitale (esecuzione del malware).
5. **Installation:** installazione di ulteriori componenti che funzionino come punto di accesso e persistenza (ad es. back-door).
6. **Command & Control (C2):** il dispositivo compromesso stabilisce una connessione con un server controllato dall'attaccante.
7. **Actions on Objectives:** l'attaccante intraprende azioni per raggiungere i propri obiettivi, l'esfiltrazione, la distruzione o la cifratura dei dati.

Ci sono due differenze principali tra il MITRE ATT&CK e la Cyber Kill Chain:

1. Il framework MITRE ATT&CK approfondisce notevolmente il modo in cui ogni fase viene condotta attraverso le tecniche e le sotto-tecniche; MITRE ATT&CK viene regolarmente aggiornato per stare al passo con le ultime tecniche in modo che i difensori aggiornino regolarmente le proprie difese e la modellazione degli attacchi.
2. La Cyber Kill Chain non tiene conto delle diverse tattiche e tecniche di un attacco. È un modello in grado di illustrare i più complessi attacchi informatici in maniera globale, così come un metodo di analisi delle intrusioni che genera uno schema semplice ed intuibile, da cui estrapolare informazioni fruibili ed universalmente comprensibili.

4.5 Tattiche

Le tattiche sono il mezzo utilizzato dall'avversario per raggiungere il suo obiettivo e rappresentano il "perché" di una tecnica o sotto-tecnica utilizzata. Ad oggi sono 14 le tattiche individuate che hanno dei "tag" all'interno di ATT&CK e una tabella contenente tecniche o sotto-tecniche associate, anch'esse con dei tag che possono appartenere a una o più tattiche.

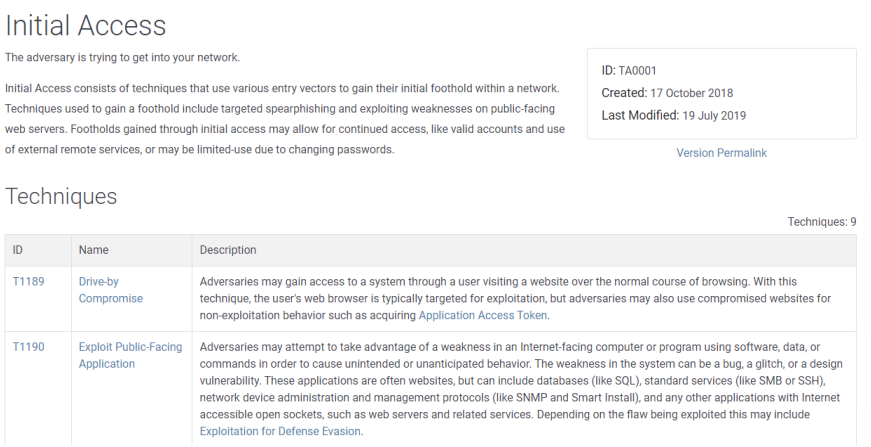


Figura 4.4: Tattica "Initial Access"

4.6 Tecniche e Sotto-Tecniche

Le tecniche rappresentano "come" un avversario raggiunge un obiettivo tattico e le singole azioni che va ad eseguire. Ad esempio, un avversario può eseguire il dump delle credenziali da un sistema operativo per ottenere l'accesso a credenziali utili all'interno di una rete. Le tecniche evidenziano anche quale tipo di informazioni un avversario sta cercando con una particolare azione.

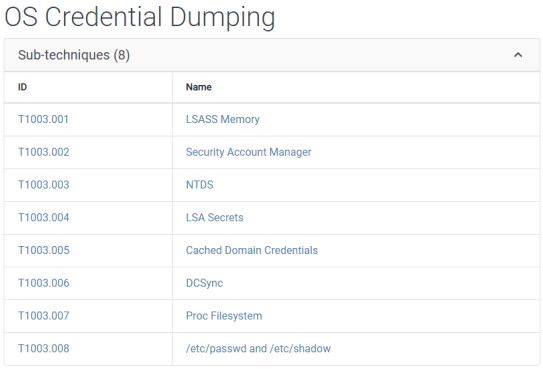


Figura 4.5: Tecnica con le sue sotto-tecniche

Le sotto-tecniche suddividono ulteriormente i comportamenti descritti dalle tecniche in descrizioni più specifiche di come il comportamento viene utilizzato per raggiungere un obiettivo. Ad esempio, con il dumping delle credenziali del sistema operativo, esistono diversi comportamenti più specifici in questa tecnica aventi tecniche secondarie

come: l'accesso alla memoria LSASS, al gestore dell'account di sicurezza o l'accesso a /etc/passwd e /etc/shadow.

4.6.1 Procedure

Le procedure sono un'altra componente importante del concetto di TTP (Tattiche, Tecniche, Procedure). All'interno di ATT&CK, le procedure sono l'implementazione specifica che gli avversari hanno utilizzato per le tecniche o sotto-tecniche. Le procedure sono documentate in ATT&CK nella sezione "Procedure Examples" delle pagine tecniche e sotto-tecniche. Ad esempio, una procedura potrebbe essere: APT28 sta utilizzando la PowerShell per iniettare lsass.exe e per eseguire il dump delle credenziali eseguendo lo scraping della memoria LSASS su una vittima.

Procedure Examples

ID	Name	Description
G0007	APT28	APT28 regularly deploys both publicly available (ex: Mimikatz) and custom password retrieval tools on victims.[1][2][3]
G0050	APT32	APT32 used GetPassword_x64 to harvest credentials.[4][5]
G0087	APT39	APT39 has used different versions of Mimikatz to obtain credentials.[6]
G0001	Axiom	Axiom has been known to dump credentials.[7]
S0030	Carbanak	Carbanak obtains Windows logon password details.[8]

Figura 4.6: Sezione "Procedure"

4.6.2 Mitigazioni

Le mitigazioni in ATT&CK rappresentano concetti di sicurezza e classi di tecnologie che possono essere utilizzati per impedire che una tecnica o sotto-tecnica venga eseguita con successo. Esistono 41 mitigazioni in ATT&CK for Enterprise che includono diversi tipi come: l'isolamento delle applicazioni e il sandboxing, il backup dei dati, la prevenzione dell'esecuzione e la segmentazione della rete. Le mitigazioni sono indipendenti dal prodotto del fornitore e descrivono solo categorie o classi di tecnologie, non soluzioni specifiche.

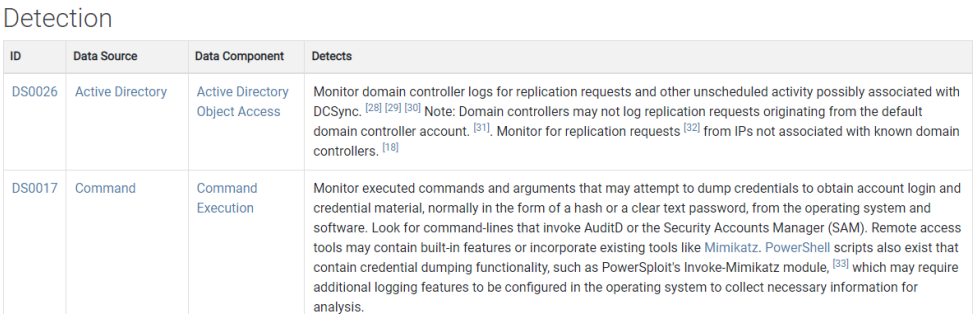
Mitigations

ID	Mitigation	Description
M1015	Active Directory Configuration	Manage the access control list for "Replicating Directory Changes" and other permissions associated with domain controller replication. [18] [19] Consider adding users to the "Protected Users" Active Directory security group. This can help limit the caching of users' plaintext credentials.[20]
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to secure LSASS and prevent credential stealing. [21]

Figura 4.7: Sezione "Mitigazioni"

4.6.3 Rilevamenti

La sezione rilevamenti descrive come sia possibile accorgersi delle varie tecniche e sotto-tecniche che sono state messe in atto.



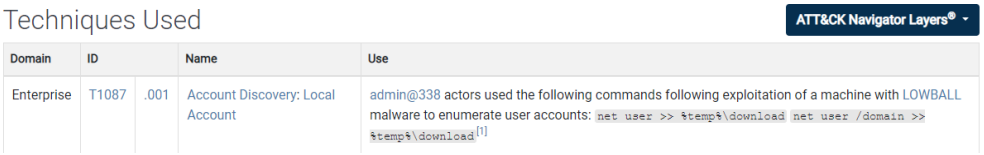
Detection

ID	Data Source	Data Component	Detects
DS0026	Active Directory	Active Directory Object Access	Monitor domain controller logs for replication requests and other unscheduled activity possibly associated with DCSync. [28] [29] [30] Note: Domain controllers may not log replication requests originating from the default domain controller account. [31]. Monitor for replication requests [32] from IPs not associated with known domain controllers. [18]
DS0017	Command	Command Execution	Monitor executed commands and arguments that may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Look for command-lines that invoke AuditD or the Security Accounts Manager (SAM). Remote access tools may contain built-in features or incorporate existing tools like Mimikatz. PowerShell scripts also exist that contain credential dumping functionality, such as PowerSploit's Invoke-Mimikatz module, [33] which may require additional logging features to be configured in the operating system to collect necessary information for analysis.

Figura 4.8: Sezione "Rilevamenti"

4.7 Gruppi e Software

Gli avversari noti vengono monitorati all'interno di ATT&CK sotto la componente "Gruppi". I gruppi possono utilizzare le tecniche direttamente o impiegare software che le implementano. Per ogni gruppo è prevista una descrizione ed una sottosezione di tecniche e software usati.

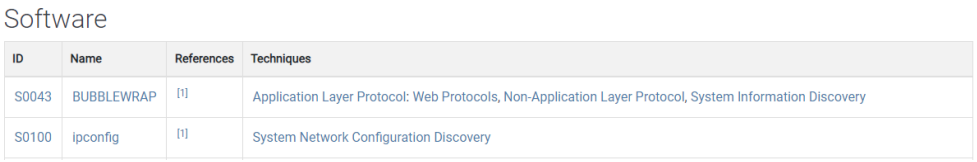


Techniques Used

ATT&CK Navigator Layers

Domain	ID		Name	Use
Enterprise	T1087	.001	Account Discovery: Local Account	admin@338 actors used the following commands following exploitation of a machine with LOWBALL malware to enumerate user accounts: `net user >> %temp%\download` `net user /domain >> %temp%\download` [1]

Figura 4.9: Sezione "Tecniche Usate"



Software

ID	Name	References	Techniques
S0043	BUBBLEWRAP	[1]	Application Layer Protocol: Web Protocols, Non-Application Layer Protocol, System Information Discovery
S0100	ipconfig	[1]	System Network Configuration Discovery

Figura 4.10: Sezione "Software"

Gli avversari usano comunemente diversi tipi di software durante le intrusioni. Il software può rappresentare un'istanza di una tecnica o di una sotto-tecnica, quindi è anche necessario classificarlo all'interno di ATT&CK. Il software è suddiviso in due categorie di alto livello: tools e malware.

- **Tools:** software commerciale, open-source, integrato o pubblicamente disponibile che potrebbe essere utilizzato da un difensore, un pen tester, un Red Teamer o un avversario. Questa categoria comprende sia il software che generalmente non si trova su un sistema aziendale, sia il software solitamente disponibile come parte di un sistema operativo già presente in un ambiente. Gli esempi includono PsExec, Metasploit, Mimikatz, nonché utilità di Windows come Net, netstat, Tasklist, ecc.

- **Malware:** software commerciale, personalizzato a codice chiuso o open source, destinato a essere utilizzato per scopi dannosi dagli avversari. Gli esempi includono PlugX, CHOPSTICK, ecc

4.8 ATT&CK Navigator

ATT&CK Navigator[1] è stato progettato per navigare la matrice ATT&CK e permettere delle annotazioni. Una delle molte funzioni utili di ATT&CK Navigator è l'utilizzo dei filtri forniti per evidenziare le tecniche utilizzate da un particolare gruppo di avversari. Nell'immagine 4.11 si può osservare la presenza di vari strumenti utili per personalizzare la nostra matrice.

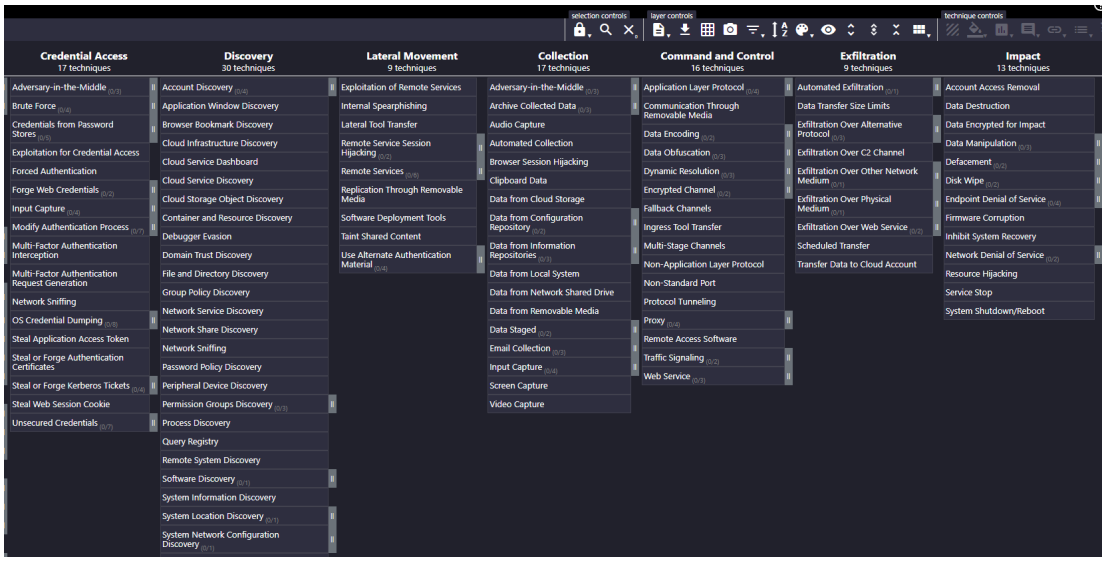


Figura 4.11: ATT&CK Navigator matrix

Nell'esempio sono stati creati tre layer: il primo contenente le TTP del gruppo APT-39, nel secondo le TTP del gruppo Barmanou e nel terzo layer una combinazione dei precedenti layer per vedere le differenze dei TTP usati ed eventualmente se alcune TTP si sovrappongono:

Figura 4.12: Layer

[1] https://mitre-attack.github.io/attack-navigator/

Come possiamo vedere nella figura 4.13 per i gruppi APT-39 (rosso) e Barmanou (giallo), le TTP evidenziate in verde sono quelle che si sovrappongono.

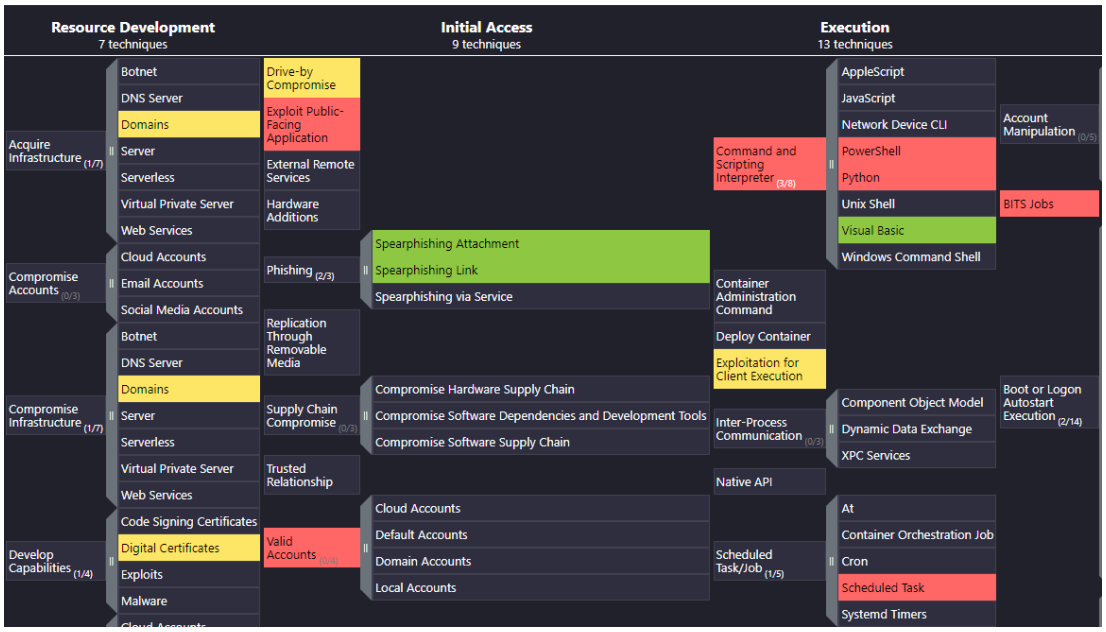


Figura 4.13: Overlap delle TTP

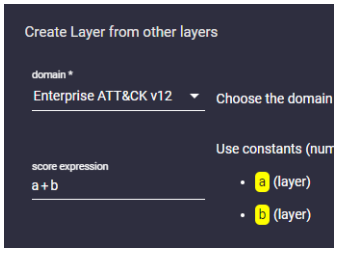


Figura 4.14: Formula per unire i layer (a+b)

5. Profilazione Avversario

In questo capitolo vedremo le procedure che saranno messe in atto per analizzare e catalogare le TTP di un avversario. Come primo step si andrà ad analizzare un report. In genere i report vengono scritti in lingua inglese da società di cybersecurity. Nei report saranno descritti, più dettagliatamente o meno, tutti i passaggi che un avversario ha compiuto per eseguire l'attacco. Come si può notare nell'immagine 5.1, un report è generalmente strutturato come segue: un titolo (rettangolo rosso), un riepilogo dell'attacco (rettangolo verde) e un'analisi tecnica (rettangolo in blu), sezione dove vengono spiegati tutti i passaggi, arricchita anche con immagini.

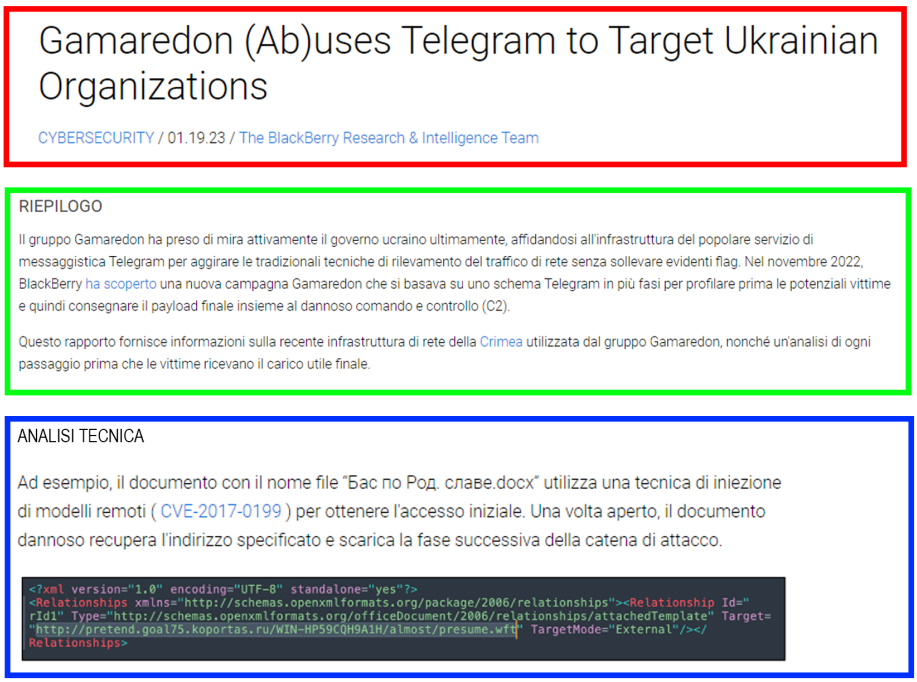


Figura 5.1: Esempio di Report

Il nostro obiettivo è quello di estrapolare questi passaggi e di catalogarli grazie all'uso del framework ATT&CK di MITRE.

Nello Stage formativo svolto presso TS-Way S.r.l. mi sono avvalso della loro piattaforma proprietaria "TS-Intelligence" per scegliere i report da analizzare.

Una volta analizzato il report, tutte le TTP di un avversario verranno raccolte e riportate in un foglio Excel ben strutturato 5.2. Per motivi di segretezza relativi all'azienda, non è possibile vedere la matrice originale con i rispettivi dati, così è stata

creata una matrice di esempio con dati fittizzi.

ATT&CK Tactic Category	techniques	subtechniques	descrizione attività
Initial Access - Phishing (T1566)	Spearphishing Attachment (T1566.001)	Office File	email attachment -->.docx
Execution - User Execution (T1204)	Malicious File (T1204.002)		
Command and Control - Ingress Tool Transfer (T1105)			.rar
Discovery - System Location Discovery (T1614)		IP Geolocalization	ukranian IP
Execution - Command and Scripting Interpreter (T1059)	PowerShell (T1059.001)		
Exfiltration - Exfiltration Over C2 Channel (T1041)			

Figura 5.2: Matrice TTP in Excel

La matrice è formata da: una data di quando è stato prodotto il report, un link al report presente nella piattaforma dell'azienda "TS-Intelligence", una fonte del report vero e proprio, un link riferito agli indicatori di compromissione (IoC), le tattiche, le tecniche e le sotto-tecniche della matrice ATT&CK (in realtà l'azienda TS-Way ha scelto in questa matrice di raggruppare le tecniche insieme alle tattiche, questo per permettere di inserire un ulteriore dettaglio di analisi nel campo "sotto-tecniche") e infine la descrizione delle attività.

Oltre al foglio, che raccoglierà le TTP, è presente anche un ulteriore foglio contenente una versione più dettagliata della matrice ATT&CK sviluppato dall'azienda, per rendere possibile una catalogazione più accurata di tutte le TTP usate, specialmente nel campo delle sotto-tecniche, come riportato in precedenza.

5.1 Applicativo profilazione TTP

Per dare un ulteriore utilità nell'analisi di un avversario, è stata creata un'applicazione web che, una volta inserite le TTP di un avversario, sarà in grado di fornire, sotto forma di percentuale, una probabilità di appartenenza ad uno o più gruppi avversari.

5.1.1 Tecnologie usate

L'applicazione web è stata sviluppata utilizzando il framework Angular e Firebase per le comunicazioni con il database.

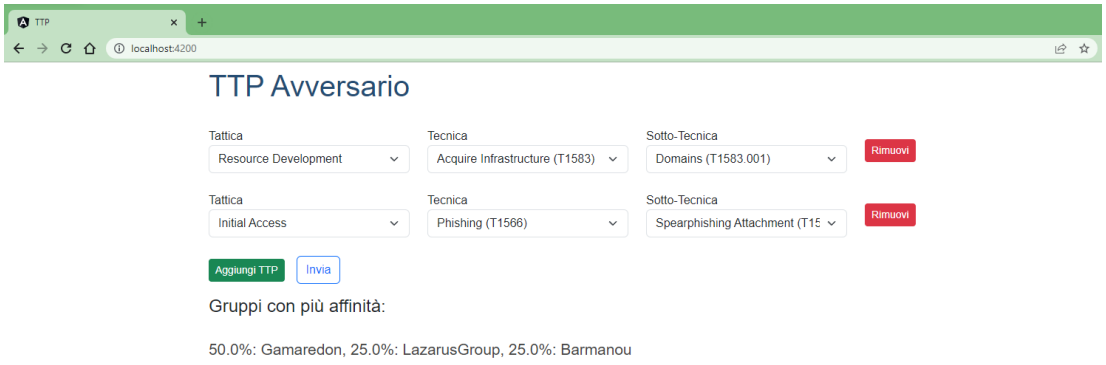


Figura 5.3: Interfaccia applicativo in Angular

L'utente ha la possibilità di inserire una o più TTP e, una volta premuto il bottone "Invia", avverrà il confronto con le TTP associate ai vari gruppi nel database.

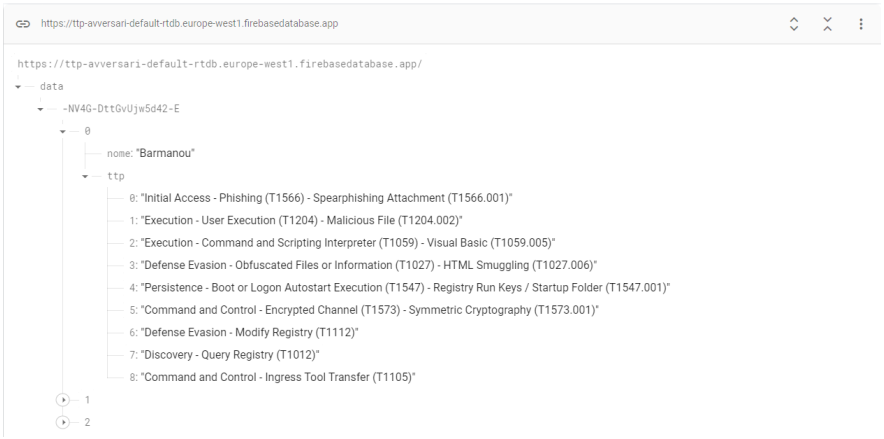


Figura 5.4: Database con i gruppi avversari e le loro TTP

Nel codice, il confronto è stato sviluppato, come si può notare nella figura 5.5 alla riga 185, creando un array di punteggi, contenente ognuno un punteggio per ogni gruppo avversario. Per registrare i punteggi è stata usata una variabile chiamata "count" (riga 186). Questa variabile, ogni volta che verrà trovata una corrispondenza tra i campi inseriti dall'utente e delle TTP nel database, aumenterà il suo valore di 1.

```
184  // Per ogni gruppo, calcolo il numero di ttp in comune con i parametri
185  const punteggi = ttp_db[0].map((data: any) => {
186    let count = 0;
187
188    for(let i=0; i<ttp_field[0].length;i++){
189      for(let k=0; k<data.ttp.length; k++){
190
191        //se non è stata inserita la sotto-tecnica valuta solo la tattica e la tecnica
192        if(ttp_field[0][i].sottotecnica == "" || ttp_field[0][i].sottotecnica == null){
193          if((ttp_field[0][i].tattica +" - "+ ttp_field[0][i].tecnica) == data.ttp[k]){
194            count++;
195          }
196        }
197
198        //nel caso fosse presente anche la sotto-tecnica
199        if((ttp_field[0][i].tattica +" - "+ ttp_field[0][i].tecnica +" - "+ ttp_field[0][i].sottotecnica) == data.ttp[k]){
200          count++;
201        }
202
203      }
204    }
205
206    return count;
207  })
```

Figura 5.5: Porzione di codice che rappresenta il confronto

Per il calcolo della percentuale, nell'immagine 5.6 alla riga 233, è stato creato un array di tipo numerico in grado di memorizzare, per ogni gruppo, una percentuale. Tramite l'applicazione del metodo "reduce()", alla riga 235, è stata fatta la somma di tutti i punteggi, e successivamente è stata memorizzata nella variabile "sum". Con l'ausilio di un ciclo for, alla riga 237, andiamo a scorrere ogni singolo punteggio di ogni gruppo all'interno dell'array "punteggi". Infine, alla riga 239, ogni singolo punteggio è stato trasformato in percentuale, moltiplicandolo per 100 e dividendo il risultato per la somma, calcolata precedentemente, di tutti i punteggi.

```
232  calcoloPercentuale(punteggi: any, indice: any) : number{
233    let percentuali: number[] = [];
234    // Somma di tutti i punteggi
235    const sum = punteggi.reduce((a: any, b: any) => a + b, 0);
236    // Itero sull'array dei punteggi
237    for (let punteggio of punteggi){
238      // Per ogni percentuale, trasformo il punteggio in centesimi e lo divido per la somma dei punteggi
239      let percentuale = (punteggio * 100) / sum;
240      // Aggiungo la percentuale all'array delle percentuali
241      percentuali.push(percentuale);
242    }
243
244    return percentuali[indice];
245  }
```

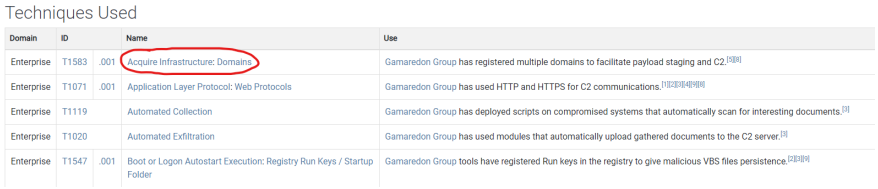
Figura 5.6: Porzione di codice che rappresenta la percentuale

Per mostrare l'output (immagine 5.7) è stato creato alla riga 211, un array di punteggi ordinati, in cui ogni punteggio è stato collegato con l'indice di ogni gruppo. Nel risultato che vogliamo ottenere, le percentuali con i rispettivi gruppi, devono essere visualizzate in ordine decrescente. Per fare questo, è stato creato un ciclo for, alla riga 218, che parte dall'ultima cella dell'array "punteggiOrdinati", e scorrerà finché non avrà visualizzato tutto l'array in ordine decrescente. L'output verrà salvato nella variabile "result" tramite il metodo "push", riga 224, ma come possiamo notare alla riga 222, è stato fatto un controllo, ovvero che verrà mostrata solo la percentuale di un gruppo a patto che sia maggiore o uguale del 25%.

```
210  // Ordina i punteggi in ordine crescente, mantenendo l'indice del gruppo associato
211  const punteggiOrdinati = punteggi.map((valore: any, indice: any) => ({ valore, indice }))
212                                    .sort((a: { valore: number; }, b: { valore: number; }) => a.valore - b.valore);
213
214  // Variabile che ci servirà per salvare i gruppi
215  let result: string[] = [];
216
217  // Itero sui gruppi permettendo di visualizzare i gruppi in ordine di probabilità
218    for (let i = punteggiOrdinati.length-1; i >= 0 ; i--) {
219
220      const { indice } = punteggiOrdinati[i];
221
222      if (this.calcoloPercentuale(punteggi,indice) >= 25.0) {
223
224        result.push("\n" + this.calcoloPercentuale(punteggi,indice).toFixed(1) + "%" + ": " + this.ttp_db[0][indice].nome);
225      }
226    }
227
228    return result;
```

Figura 5.7: Porzione di codice che rappresenta l'output

In conclusione, completiamo l'analisi confrontando le TTP con quelle appartenenti al gruppo trovato. In questo ci viene aiuto il sito del framework ATT&CK che, come possiamo vedere nell'immagine 5.8, ci fornisce una breve descrizione sulle modalità d'uso delle TTP durante un attacco da parte di un avversario.



Techniques Used

Domain	ID		Name	Use
Enterprise	T1583	.001	Acquire Infrastructure: Domains	Gamaredon Group has registered multiple domains to facilitate payload staging and C2.[5][8]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	Gamaredon Group has used HTTP and HTTPS for C2 communications.[1][2][3][4][6][8]
Enterprise	T1119		Automated Collection	Gamaredon Group has deployed scripts on compromised systems that automatically scan for interesting documents.[3]
Enterprise	T1020		Automated Exfiltration	Gamaredon Group has used modules that automatically upload gathered documents to the C2 server.[3]
Enterprise	T1547	.001	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder	Gamaredon Group tools have registered Run keys in the registry to give malicious VBS files persistence.[2][3][6]

Figura 5.8: Confronto sulla pagina del gruppo nel sito del framework ATT&CK

6. Conclusioni

Il mondo del cybercrime è in continua evoluzione ed è in grado di adattare dinamicamente le tecniche di attacco al fine di sfruttare al meglio anche le problematiche sociali del momento. Ad esempio, durante la pandemia Covid-19, lo sfruttamento di temi legati alla sanità ha fatto registrare una crescita esponenziale degli attacchi e di conseguenza degli introiti per i criminali informatici. Stessa cosa per i temi legati al conflitto russo-ucraino. I continui attacchi dimostrano una chiara carenza delle difese -sia del settore pubblico che di quello privato- nel monitorare e proteggere in modo adeguato il proprio perimetro. La regola fondamentale rimane quella di essere preparati e resilienti per rispondere in modo adeguato e incisivo, cercando il più possibile di implementare attività che riescano ad individuare in anticipo le minacce informatiche, così da prevenire un impatto potenzialmente critico sulle infrastrutture, i dati o le persone. La sicurezza è un'interazione che si realizza non solo tra processi e tecnologie, ma soprattutto tra le persone. L'essere umano, essendo prima di tutto un essere pensante, può essere vulnerabile a tutte quelle pratiche di *social engineering* che sfruttano la psiche umana, rappresentando così l'anello debole della catena della cybersecurity. I manager dovrebbero essere consci dei rischi legati alla criminalità informatica e del fatto che investire ingenti somme di denaro solo su nuove tecnologie di cybersecurity può non essere sufficiente, se a questo non si affianca la CTI. Bisogna considerare che una buona CTI, oltre a fornire informazioni ai team tecnici, permette di fornire informazioni strategiche al management, permettendo loro di prendere decisioni più rapidamente, investire in modo mirato, mitigare i rischi legati al business ed essere più efficienti nella protezione delle infrastrutture aziendali. [5]

Bibliografia

[1] CISA. *Traffic Light Protocol (TLP) Definitions and Usage*. URL: https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage.

[2] cybersecurity360.it. *Attacchi state-sponsored: cosa sono e come contrastarli migliorando le capacità di cyber difesa*. URL: https://www.cybersecurity360.it/nuove-minacce/attacchi-state-sponsored-cosa-sono-e-come-contrastarli-migliorando-le-capacita-di-cyber-difesa/.

[3] difesaesicurezza. *Cyber War, l'Ucraina arruola gli hacker volontari che combattono contro la Russia*. URL: https://www.difesaesicurezza.com/difesa-e-sicurezza/cyber-war-ucraina-arruola-gli-hacker-volontari-che-combattono-contro-la-russia/.

[4] Giornalettismo. *Chi sono gli hacker di NoName e quali siti istituzionali italiani hanno attaccato di recente*. URL: https://www.giornalettismo.com/noname-hacker-attacchi-siti-italiani/.

[5] Camilla Salini Giuseppe Brando Marco Di Costanzo. *Il ransomware nell'economia del cybercrime*. Roma: Themis, 2023.

[6] LookingGlass. *three common threat actors and the one you might not know about*. URL: https://lookingglasscyber.com/blog/threat-intelligence-insights/three-common-threat-actors-and-the-one-you-might-not-know-about/.

[7] MITRE. *MITRE ATT&CK*. URL: https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

[8] Alessandra Nicolosi. *Ciclo Intelligence*. URL: http://www.crimint.it/il-ciclo-di-intelligence/.

[9] Sistema di informazione per la sicurezza della Repubblica. *IL LINGUAGGIO DEGLI ORGANISMI INFORMATIVI*. URL: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2013/12/Glossario-intelligence-2013.pdf.

[10] Sistema di informazione per la sicurezza della repubblica. *Lezione Intelligence*. URL: https://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/05/lezione-intelligence.pdf.

[11] servicenow. *Che cos'è il framework MITRE ATT&CK?* URL: https://www.servicenow.com/it/products/security-operations/what-is-mitre-attack.html.

[12] sicurezza.net. *Cosa si intende con Red Teaming?* URL: https://sicurezza.net/cyber-security/red-teaming-cosa-e/#gref.

[13] Trellix. *What is mitre attack framework?* URL: https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html.

[14] Francesco La Trofa. *Cyberthreat Intelligence*. URL: https://universeit.blog/cyber-threat-intelligence/.

[15] UNODC. *Criminal Intelligence for Analysts*. URL: https://www.unodc.org/documents/organized-crime/Law-Enforcement/Criminal_Intelligence_for_Analysts.pdf.

[16] Wikipedia. *Agenzia per la cybersicurezza nazionale*. URL: https://it.wikipedia.org/wiki/Agenzia_per_la_cybersicurezza_nazionale.

[17] Wikipedia. *Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche*. URL: https://it.wikipedia.org/wiki/Centro_nazionale_anticrimine_informatico_per_la_protezione_delle_infrastrutture_critiche.

[18] Wikipedia. *Indicatore di compromissione*. URL: https://it.wikipedia.org/wiki/Indicatore_di_compromissione.

[19] Wired. *Che cosa sappiamo sull'attacco informatico alla Nato*. URL: https://www.wired.it/article/attacco-hacker-killnet-nato/.

Ringraziamenti

Ringrazio l'Università di Camerino, che mi ha dato la possibilità di perseguire e approfondire la mia passione per l'informatica.

La mia famiglia, che c'è sempre stata in tutto e per tutto, sia nei momenti felici che nei momenti più difficili.

Ringrazio nel complesso tutte quelle persone che hanno contribuito, direttamente ed indirettamente, al mio percorso formativo in ambito universitario.

Ringrazio il mio Tutor Aziendale che mi ha permesso di conoscere questa nuova branca dell'informatica.

Infine ringrazio mio Zio, che molto pazientemente ha visionato tutta la tesi andando a caccia di refusi ed errori ortografici.