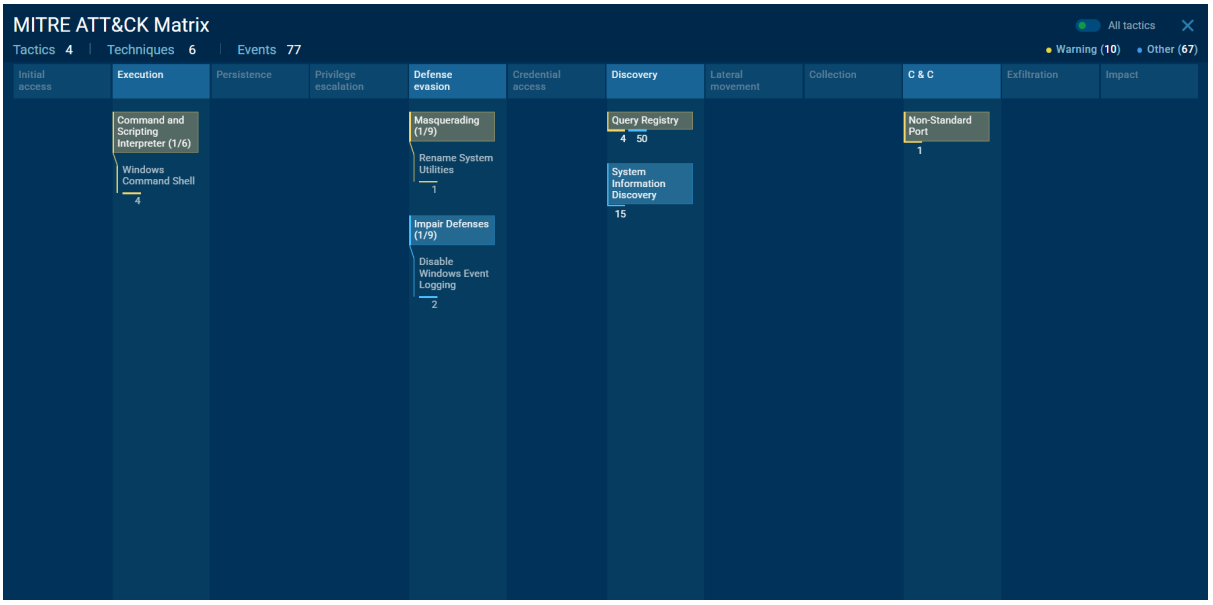
Introduzione

In questa relazione, analizzo le tecniche utilizzate dagli avversari per ottenere informazioni sul sistema, evadere i meccanismi di difesa, eseguire processi malevoli ed eseguire altre attività correlate alla matrice **MITRE ATT&CK.** L'obiettivo è spiegare in modo chiaro e comprensibile le metodologie osservate durante l'analisi di un caso reale, seguendo l'ordine delle tattiche mostrate nel report.



La matrice **MITRE ATT&CK** (Adversarial Tactics, Techniques, and Common Knowledge) è un quadro di riferimento globale e aperto che descrive i comportamenti, le tattiche e le tecniche utilizzate dagli attori delle minacce informatiche per condurre attacchi e compromettere sistemi. È ampiamente utilizzata da professionisti della sicurezza informatica per analizzare e difendersi da attacchi sofisticati.

Tattiche: Rappresentano gli obiettivi generali che un attaccante cerca di raggiungere, come "Initial Access" (Accesso Iniziale), "Execution" (Esecuzione) o "Defense Evasion" (Evasione delle Difese).

A proposito ho notato diverse tattiche utilizzate dagli attaccanti in questo file che ho esaminato

Considerazioni Iniziali

Text Report

Ho osservato che il Text Report fornisce una panoramica chiara delle attività, segmentando gli eventi per tattiche e tecniche. Questo è stato fondamentale per identificare i punti critici dell'attacco e le sue fasi principali.

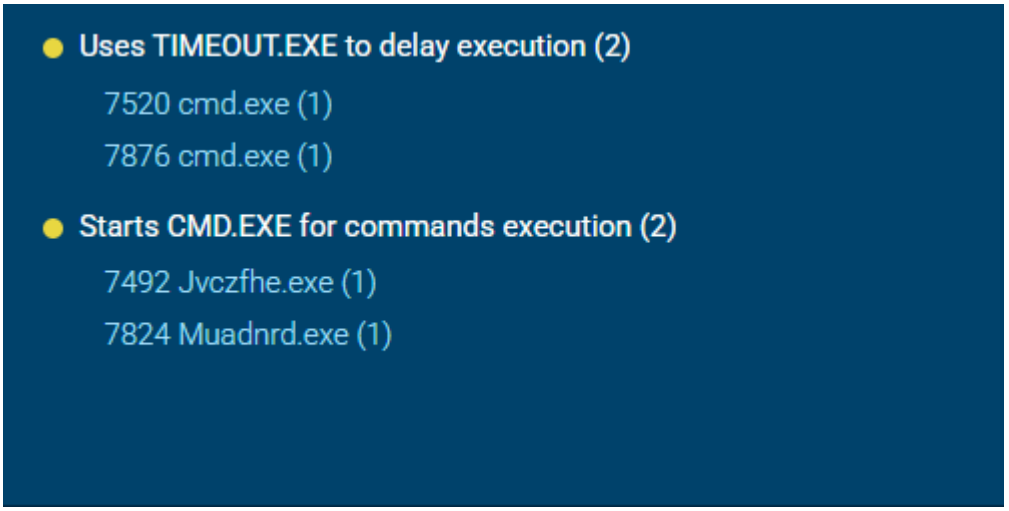
Processes Graph

Il Processes Graph ha rivelato le connessioni tra i vari processi coinvolti, evidenziando l'uso combinato di strumenti legittimi e malevoli. Questo grafico è stato essenziale per comprendere la logica e la struttura dell'attacco.

Execution

Che cos'è?

La categoria "Execution" riguarda l'avvio di processi malevoli sul sistema target. Gli avversari utilizzano questa tecnica per eseguire payload o per attivare strumenti già presenti nel sistema.



Esempi osservati

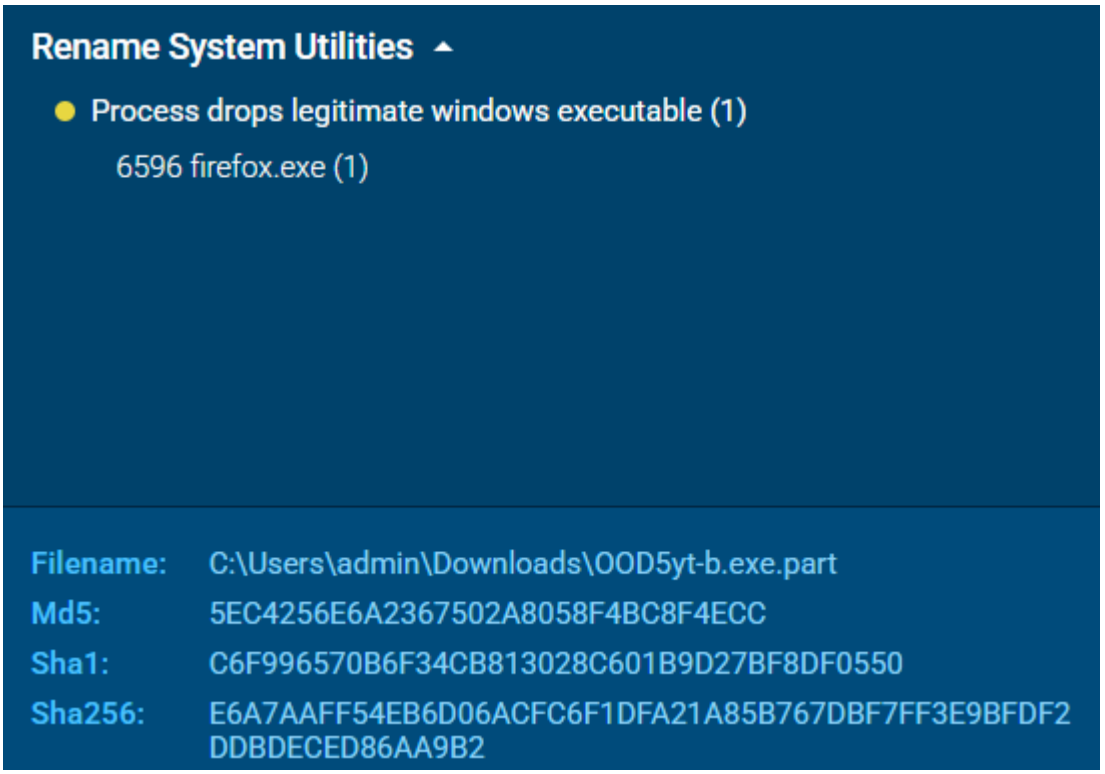
1. **Windows Command Shell**: Ho osservato 4 eventi che coinvolgono l'uso della shell dei comandi per eseguire script o comandi malevoli.
    - **Descrizione**: La shell è stata utilizzata per attivare strumenti malevoli come `Jvczfhe.exe` e `Muadrnd.exe`.

Defense Evasion

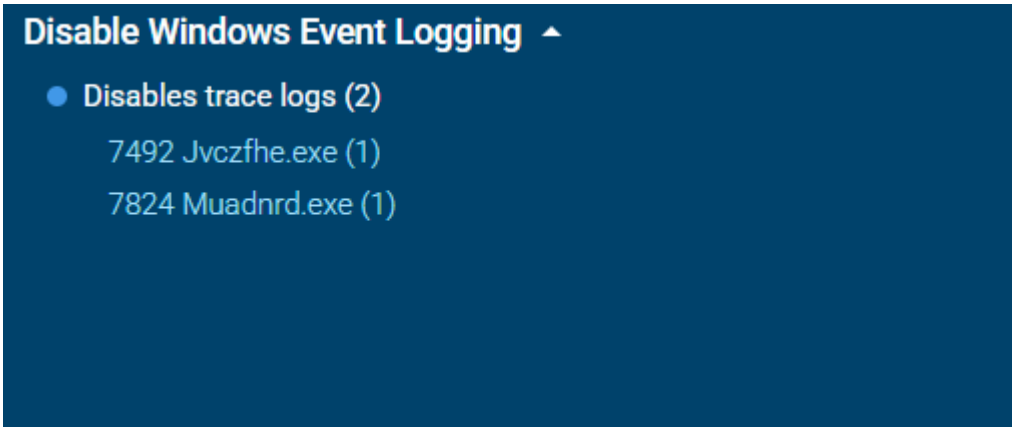
Che cos'è?

"Defense Evasion" comprende tecniche progettate per evitare il rilevamento da parte di soluzioni di sicurezza come antivirus, EDR (Endpoint Detection and Response) e firewall.

Esempi osservati

1. 

Masquerading: Gli attaccanti hanno rinominato utilità di sistema per confondere gli strumenti di sicurezza.
    - **Eventi rilevati**: 1 evento
    - **Esempio**: `InstallUtil.exe` è stato usato per nascondere attività malevole.

2. 

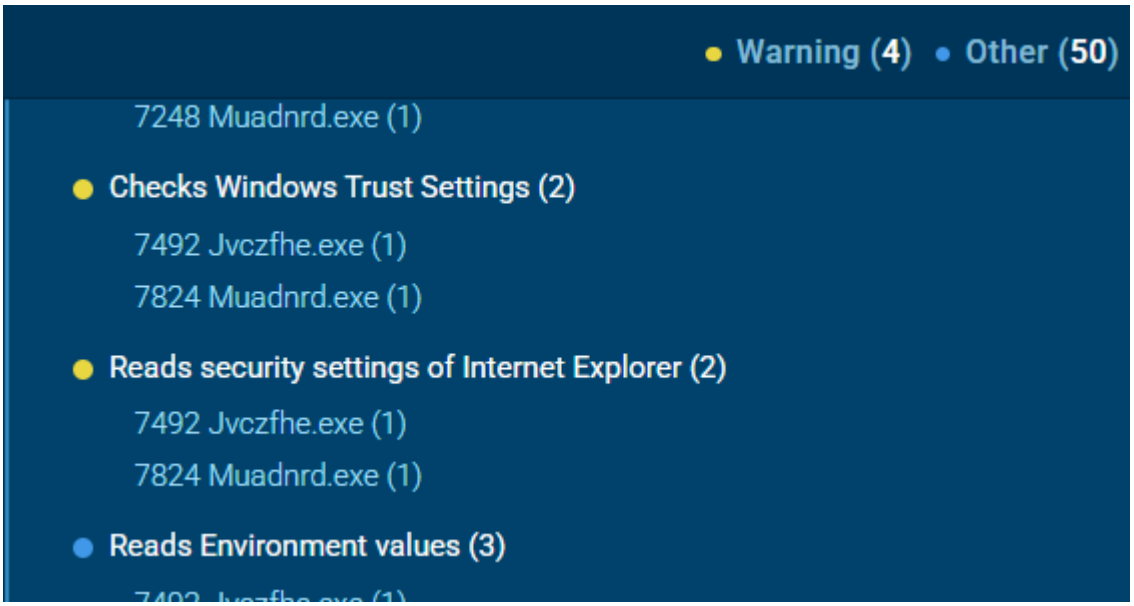
Impair Defenses: Gli avversari hanno disabilitato il logging degli eventi di Windows per evitare il rilevamento.
    - **Eventi rilevati**: 2 eventi
    - **Descrizione**: Disabilitazione del monitoraggio delle attività nel registro eventi di Windows.

Discovery

Che cos'è?

La categoria "Discovery" si concentra sull'acquisizione di informazioni sul sistema target per supportare altre fasi dell'attacco.

Esempi osservati

1. 

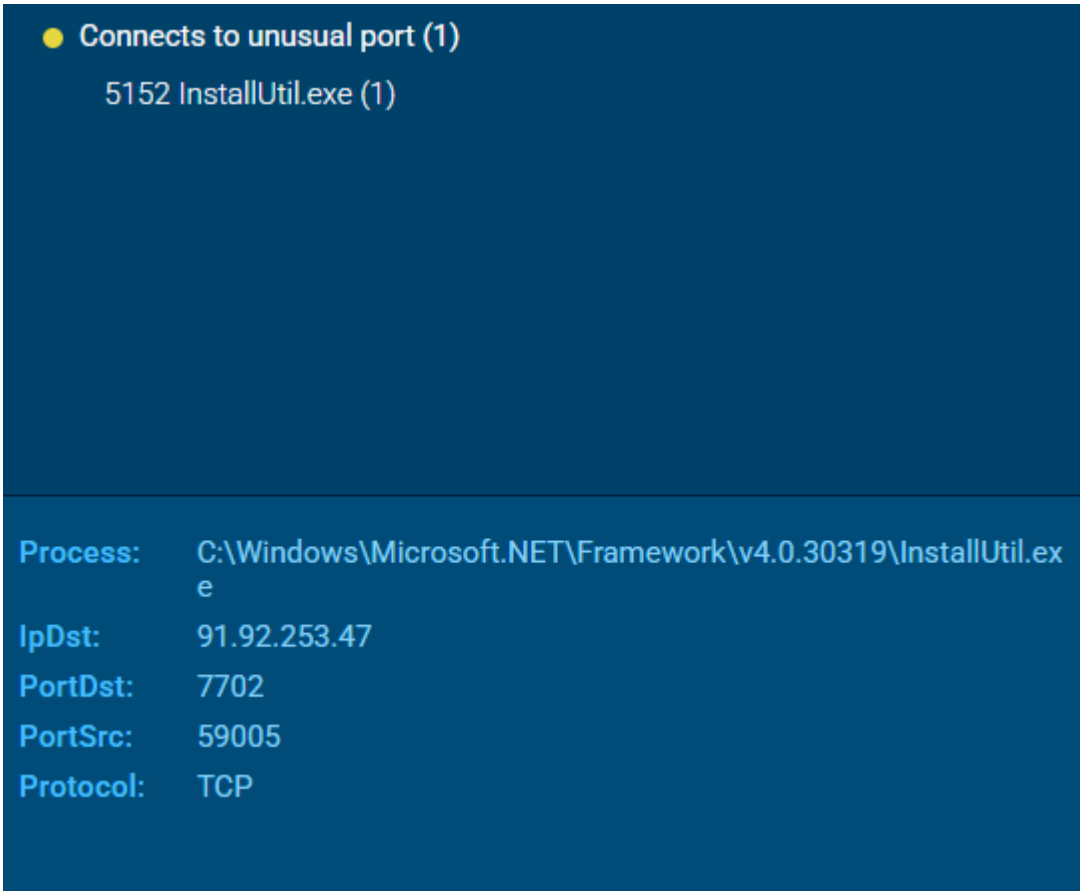
Query Registry: Ho rilevato 54 eventi (50 blu e 4 gialli) relativi alla lettura di informazioni dal registro di sistema.

    - **Descrizione**: Gli avversari hanno recuperato informazioni come nome del computer, configurazione linguistica e GUID della macchina.
    - **Chiavi di registro**:
        - `HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\ComputerName\ActiveComputerName`
        - `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography`
2. **System Information Discovery**: Ho osservato 15 eventi relativi all'acquisizione di dettagli sul sistema operativo e sull'hardware.
    - **Descrizione**: Lettura di informazioni come tipo di installazione e configurazione ambientale.
    - **Chiavi di registro**:
        - `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows NT\CurrentVersion`

Command and Control (C&C)

Che cos'è?

Questa categoria si riferisce alle tecniche utilizzate dagli avversari per comunicare con i sistemi compromessi e mantenere il controllo remoto.



Esempi osservati

1. **Non-Standard Port**: Ho rilevato 1 evento di comunicazione su una porta non standard (7702).
    - **Descrizione**: Gli avversari hanno utilizzato la porta 7702 per evitare il rilevamento da parte dei sistemi di monitoraggio del traffico di rete, che solitamente si concentrano su porte standard come 80 o 443.

Analisi delle Connessioni

Considerazioni

Durante l'analisi delle connessioni, ho rilevato alcuni punti sospetti:

1. **Connessioni a domini poco comuni**:
    - **DuckDNS**: Sono state osservate connessioni frequenti verso domini associati a `*.duckdns.org`. Questi servizi di DNS dinamico, sebbene legittimi, sono spesso sfruttati per attività malevole.
2. **Abuso di processi legittimi**:
    - Il processo `svchost.exe` è stato usato per effettuare connessioni ripetute verso indirizzi IP esterni.

    - Il processo `InstallUtil.exe` ha comunicato su una porta non standard (7702).
3. **Traffico su provider cloud**:
    - Traffico verso domini come `raw.githubusercontent.com`, potenzialmente utilizzati per scaricare script o payload.
4. **Portate dati anomale**:
    - Connessioni con upload/download significativi rispetto alla norma potrebbero indicare esfiltrazioni di dati.

Analisi delle Richieste DNS

L'analisi delle richieste DNS ha rivelato attività sospette che potrebbero essere indicative di compromissioni.

1. **Connessioni a DuckDNS**
    - Sono state rilevate richieste verso il dominio `egehgdehjbhjtre.duckdns.org`. DuckDNS, sebbene legittimo, è spesso sfruttato da attaccanti per configurare server di comando e controllo (C&C). Alcune richieste non hanno ricevuto risposta IP, suggerendo l'uso di infrastrutture temporanee.
2. **Abuso di piattaforme cloud**
    - Richieste verso domini come `cloudfront.net` e `akamai.net` potrebbero essere utilizzate per distribuire payload malevoli o esfiltrare dati, sfruttando la reputazione di questi servizi legittimi.
3. **Richieste a GitHub**
    - Le connessioni verso `collector.github.com` e API di GitHub sollevano il sospetto che la piattaforma sia stata utilizzata per scaricare script o payload dannosi.

Implicazioni

Questi elementi suggeriscono l'uso di tecniche avanzate per comunicare con infrastrutture malevole sfruttando servizi legittimi.

Raccomandazioni:

- Monitorare le richieste DNS verso domini sospetti.
- Limitare l'uso di DuckDNS se non strettamente necessario.
- Controllare i file scaricati da piattaforme cloud o GitHub.

Conclusioni

L'analisi del caso ha evidenziato una strategia sofisticata da parte degli attaccanti, che hanno sfruttato una combinazione di tecniche per compromettere il sistema.

1. **Punti chiave delle minacce identificate**:
    - L'uso di strumenti di sistema come `InstallUtil.exe` e `svchost.exe` ha permesso di mascherare attività malevole e mantenere la persistenza nel sistema.
    - La raccolta di informazioni dettagliate tramite il registro di sistema ha fornito agli attaccanti un quadro chiaro delle configurazioni del sistema.
    - La comunicazione su porte non standard ha dimostrato un tentativo deliberato di evitare i controlli di rete tradizionali.
2. **Importanza dell'identificazione precoce**:
    - Le tecniche di "Query Registry" e "System Information Discovery" indicano che gli attaccanti erano in fase di ricognizione per pianificare ulteriori attacchi.

Raccomandazioni

Per proteggersi da queste minacce, consiglio di:

- **Implementare sistemi di monitoraggio avanzati**: Adottare soluzioni EDR per identificare comportamenti anomali legati all'uso di strumenti di sistema.
- **Segmentare la rete**: Limitare la comunicazione tra sistemi critici e implementare politiche di accesso rigorose.
- **Monitorare il traffico di rete**: Analizzare le connessioni su porte non standard e configurare avvisi per attività sospette.
- **Eseguire audit regolari**: Controllare regolarmente i registri di sistema e le configurazioni per identificare anomalie.

Questa analisi dimostra l'importanza di un approccio proattivo alla sicurezza informatica per mitigare le minacce avanzate e salvaguardare le infrastrutture critiche.