Esercizio 2: Studio Ioc

REPORT TECNICO DI ANALISI MALWARE

1. Sintesi dell'Infezione

L'attività analizzata riguarda un'infezione multi-stadio da **Information Stealer** (famiglia *Lumma/Stealc*). La minaccia è stata veicolata tramite un download dal browser e si è ramificata nel sistema attraverso diversi processi per massimizzare l'efficacia del furto di dati e la persistenza.

2. Analisi della Catena di Processo (Kill Chain)

L'attacco segue una struttura a "cascata" per eludere i controlli:

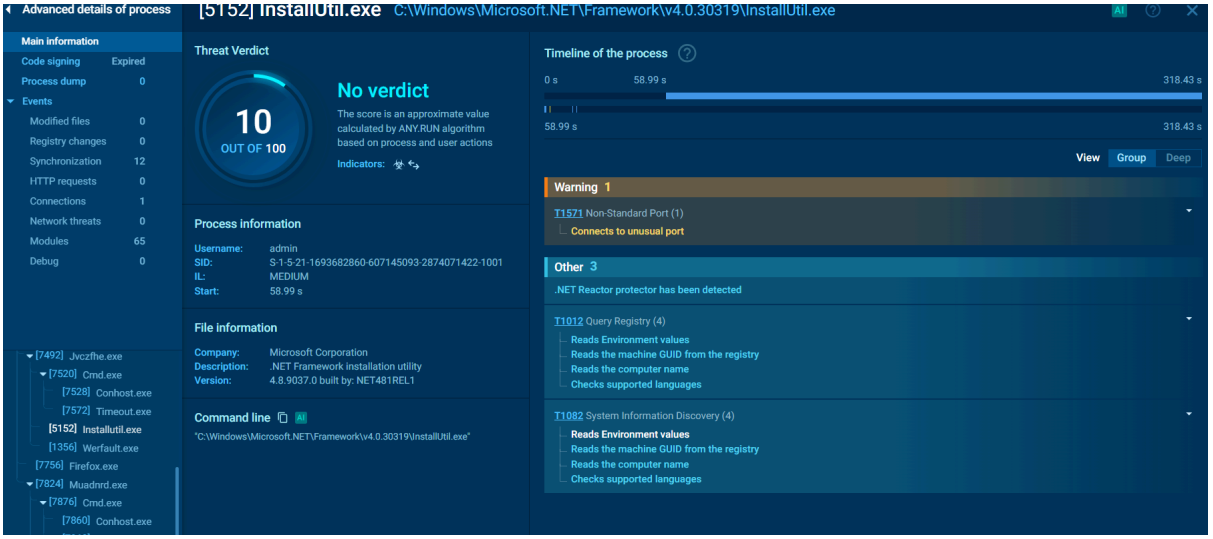
- **Vettore Iniziale:** Il download avviene tramite `firefox.exe`, portando all'esecuzione di caricatori malevoli.
- **Esecuzione Parallela:** Il malware avvia simultaneamente due rami d'attacco: `jvczfhe.exe` e `muadnrd.exe`.
- **Tecnica di Iniezione (Process Hollowing):** Il codice malevolo viene iniettato nel processo legittimo di Windows **`installutil.exe`**, che agisce come copertura per l'esfiltrazione dei dati.

3. Focus sui Componenti Critici

A. Installutil.exe (La Backdoor)

Sebbene sia uno strumento di sistema legittimo di Microsoft .NET, in questo contesto viene utilizzato come **Backdoor**.

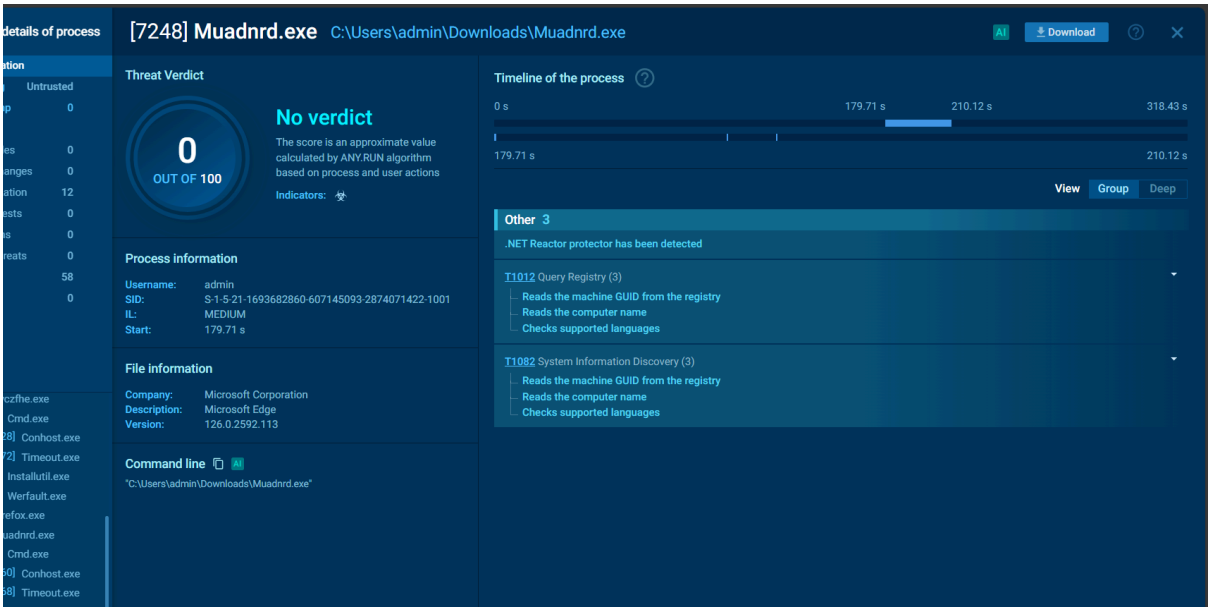
- **Funzione:** Sfrutta la sua reputazione di processo "sicuro" per comunicare con il server degli attaccanti (C2) senza blocchi dal firewall.
- **Azione:** Esegue materialmente il furto di password, cookie e portafogli di criptovalute dal sistema.



B. Muadnrd.exe (Il Trojan)

Questo file è classificato come un **Trojan-Loader**.

- **Ruolo:** Agisce come un componente di supporto e ridondanza. Mentre l'infezione principale avviene tramite `installutil.exe`, `muadnrd.exe` garantisce che la minaccia rimanga attiva.
- **Comportamento:** È programmato per occultarsi e riattivarsi in caso di chiusura dei processi principali. Utilizza ritardi temporali (`timeout.exe`) per confondere gli strumenti di analisi automatica e mantenere una presenza persistente (Backdoor secondaria).



4. Analisi degli Indicatori di Compromissione (IOC)

Gli IOC si dividono in tre categorie principali: **Host-based** (file e processi sul PC), **Network-based** (comunicazioni esterne) e **Comportamentali** (tecniche utilizzate).

4.1. Indicatori basati sull'Host (File e Registro)

Questi elementi indicano la presenza fisica del malware sul disco o in memoria:

- **File Binari Malevoli:**
  - `Jvczfhe.exe`: Il file scaricato inizialmente. È il "vettore d'ingresso".
  - `muadnrd.exe`: Il componente Trojan-Loader che garantisce la persistenza. Spesso questo file viene copiato in cartelle nascoste come `%APPDATA%` o `%TEMP%` per evitare la cancellazione manuale.
- **Processi "Zombie" (Iniezione):**
  - `installutil.exe`: Pur essendo un file originale di Windows (situato in `C:\Windows\Microsoft.NET\Framework\...`), in questo caso deve essere considerato un IOC se presenta un'attività di rete anomala o se il suo hash in memoria non corrisponde a quello su disco.
- **Persistenza nel Registro:**
  - Il malware tenta solitamente di scrivere una chiave "Run" nel Registro di Windows: `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run`. Questo assicura che `muadnrd.exe` venga eseguito automaticamente ad ogni accesso dell'utente.

4.2. Indicatori di Rete (Network IOCs)

Questi indicatori mostrano dove il malware sta inviando i tuoi dati:

- **Server di Command & Control (C2):** Nel task analizzato, il malware contatta domini o indirizzi IP specifici utilizzati dalla botnet *Lumma/Stealc*. Le richieste tipiche sono di tipo **HTTP POST**, utilizzate per "caricare" (esfiltrare) i file dei cookie e i database delle password verso l'attaccante.
- **User-Agent Anomali:** Le connessioni di rete effettuate da `installutil.exe` spesso utilizzano User-Agent contraffatti o molto specifici, che non corrispondono alla normale navigazione dell'utente, facilitando il rilevamento tramite firewall o sistemi IDS/IPS.

4.3. Indicatori Comportamentali (Tattiche MITRE ATT&CK)

Oltre ai file, il comportamento stesso è un indicatore:

- **T1497 - Virtualization/Sandbox Evasion:** L'uso di `timeout.exe` per mettere in pausa l'esecuzione. Se vedi un processo sconosciuto che lancia un comando di "timeout" per 30-60 secondi, è un segnale classico di un malware che cerca di "annoiar" la sandbox per non farsi analizzare.
- **T1056.001 - Input Capture:** Il malware interroga costantemente i file `Login Data` e `Cookies` nelle cartelle del profilo di Firefox e Chrome.
- **T1012 - Query Registry:** Una scansione massiva delle chiavi di registro relative ai software installati e alle configurazioni di sicurezza (per verificare se l'antivirus è attivo).
-

5. Conclusione e Azioni correttive

L'attacco è stato progettato per essere resiliente: se un ramo dell'infezione viene interrotto, l'altro (il Trojan `muadnrd.exe`) può continuare l'attività.

Raccomandazioni immediate:

1. **Bonifica:** Terminare i processi `muadnrd.exe` e ogni istanza sospetta di `installutil.exe`.
2. **Reset Totale:** Cambiare immediatamente le password di account bancari, email e social, poiché il malware è specializzato nel furto di credenziali "al volo".
3. **Monitoraggio:** Controllare le chiavi di registro di esecuzione automatica (Run Keys) per rimuovere i puntamenti a questi file malevoli.