REPORT ANALITICO ESERCIZIO 2: STUDIO IOC

Studente: Nicola Cassandra
Data: 20/02/2026
Obiettivo: Studio e analisi di minacce rilevate attraverso un'analisi dettagliata degli Indicatori di Compromissione (IoC) tramite Any.Run

---

1. Executive Summary

L'analisi dinamica del sample ha confermato l'esecuzione di un malware di tipo *loader/stealer* che sfrutta tecniche avanzate di evasione (approccio **Living off the Land**) per iniettare codice malevolo all'interno di processi di sistema legittimi. La compromissione ha permesso alla minaccia di effettuare una ricognizione silente dell'host e di stabilire con successo una connessione Command & Control (C2) verso un server esterno non standard, minacciando direttamente la confidenzialità e l'integrità dell'endpoint.

---

2. Scope & Toolchain

Di seguito la tabella riepilogativa dell'ambiente di analisi e degli strumenti impiegati durante l'investigazione:

Ambito / Target	**Strumento Utilizzato**	**Scopo Tecnico**
Endpoint Windows Sandbox	**Any.Run**	Esecuzione sicura, analisi comportamentale dinamica e tracciamento dell'albero dei processi.
91.92.253.47 (C2 Server)	**Network Tracker integrato**	Rilevamento di anomalie nel traffico TCP/UDP in uscita.
Comportamento Malware	**MITRE ATT&CK Framework**	Mappatura standardizzata delle tattiche di evasione, *discovery* ed esfiltrazione.

---

3. Analisi Tecnica e Attack Chain

L'esecuzione del malware è stata analizzata cronologicamente per comprenderne a fondo le meccaniche di persistenza ed evasione.

1. **Infezione Iniziale (Initial Access & Execution)**
   Il vettore d'infezione origina dalla navigazione web compromessa tramite il processo browser. Il download iniziale porta al salvataggio e all'esecuzione automatica dei payload primari, identificati con i nomi **jvczfhe.exe** e **muadnrd.exe**. Il ruolo di questi eseguibili è fungere da *dropper* per i moduli successivi.

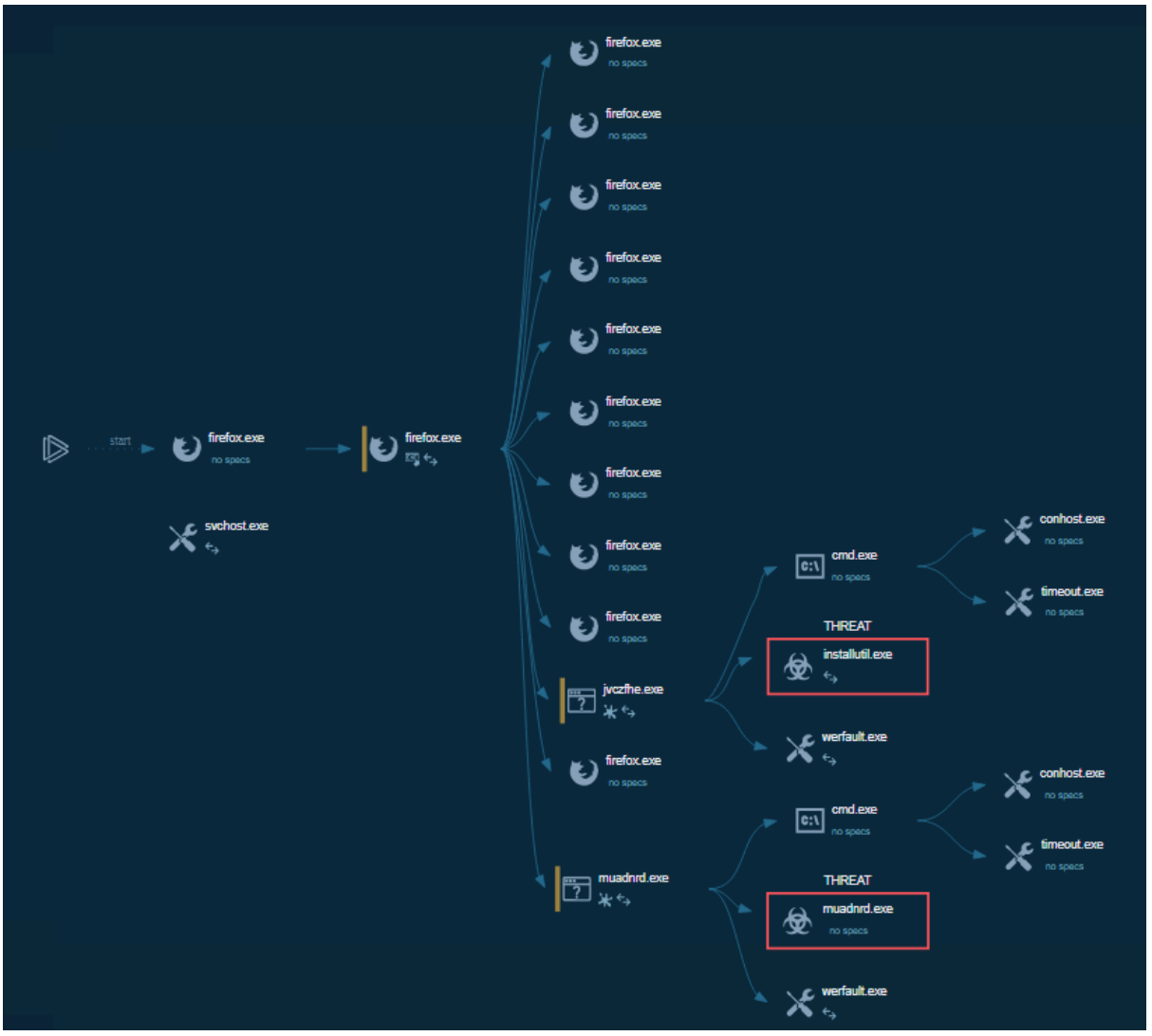

Fig. 1. L'albero dei processi evidenzia l'intera catena di esecuzione iniziale partita dal browser, che ha portato al lancio dei binari malevoli primari.

Evasione Temporale (Anti-Sandbox / Evasion)
Per evitare l'analisi dinamica e simulare l'inattività, il malware esegue una chiamata al processore dei comandi di Windows, istruendolo ad avviare l'utility nativa timeout.exe. Il motivo tecnico (il "perché") di questa azione è ingannare i timer di timeout delle sandbox di analisi automatizzata, bloccando l'esecuzione del codice malevolo fino alla scadenza del timer.

```
DOS
cmd.exe /c timeout /t <valore_in_secondi>
```

2. **Nota per il Blue Team:** L'invocazione di processi figli in sequenza rapida come cmd.exe -> timeout.exe da parte di eseguibili scaricati da percorsi non attendibili (es. la cartella Download) è un forte indicatore comportamentale di evasione temporale.
3. **Process Injection (Living off the Land)**
   Superata la fase di evasione, l'attaccante inietta il proprio codice maligno all'interno di un processo di sistema legittimo per aggirare l'Application Whitelisting (es. AppLocker). Viene preso di mira il file nativo del framework .NET: **C:\Windows\Microsoft.NET\Framework\v4.0.30319\InstallUtil.exe**. Questo processo viene "svuotato" (*Process Hollowing*) e utilizzato come maschera per l'esecuzione del payload.

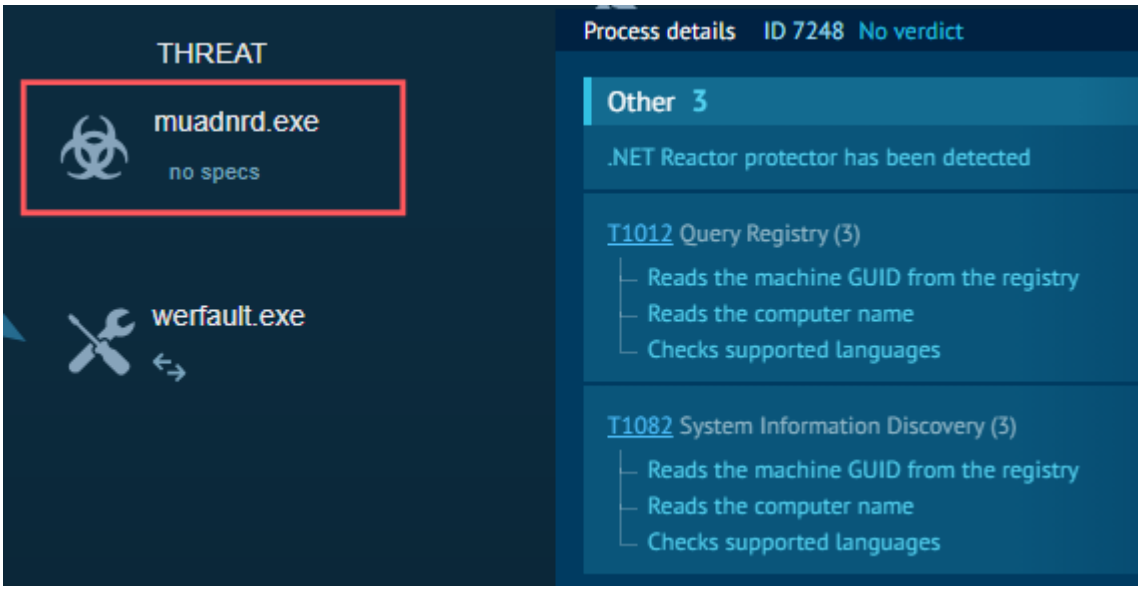

Fig. 2. I riquadri rossi di diagnostica della piattaforma Any.Run identificano come minaccia critica il processo teoricamente legittimo InstallUtil.exe, confermando l'avvenuta iniezione di codice.

Ricognizione e Command & Control (C2)
Operando sotto le spoglie di **InstallUtil.exe**, il malware interroga le chiavi di registro locali per estrarre identificatori unici, nello specifico il **Machine GUID** e il nome del computer. Lo scopo è profilare la macchina compromessa. Terminata la profilazione, viene generato traffico di rete in uscita per collegarsi all'infrastruttura dell'attaccante situata all'indirizzo IP **91.92.253.47**, utilizzando la porta anomala **7702**.
PowerShell
Esempio concettuale di ciò che il malware cerca di leggere tramite API di sistema:
Get-ItemProperty -Path "HKLM:\SOFTWARE\Microsoft\Cryptography" -Name "MachineGuid"

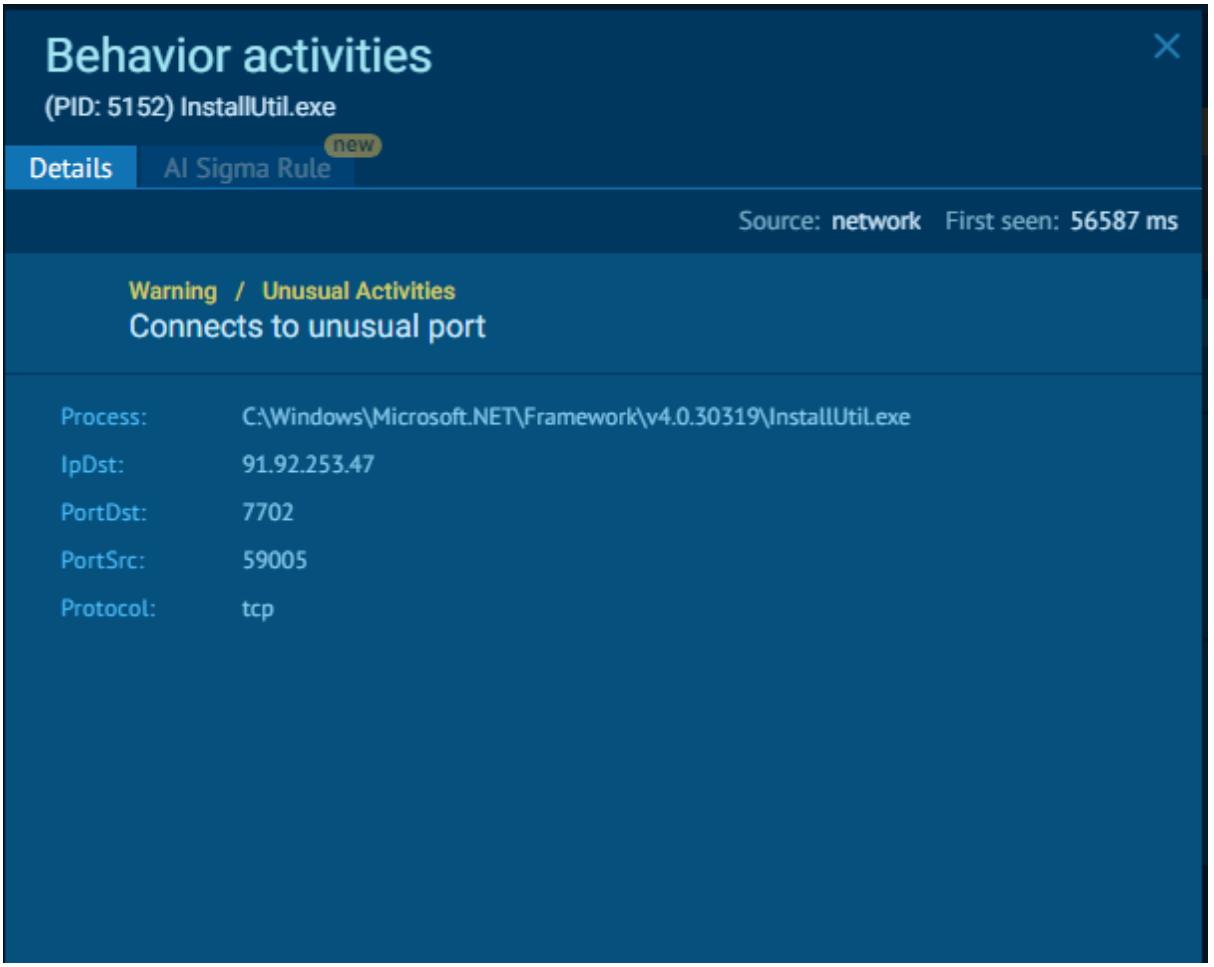

Fig. 3. Evidenza della scheda comportamentale (Behavior activities) che conferma il tentativo di connessione TCP in uscita, contrassegnata come "Connects to unusual port", verso il server C2.

---

4. Vulnerabilità Sfruttate

Il malware analizzato non fa affidamento sullo sfruttamento di falle del codice (come *Buffer Overflow* tradizionali), bensì sull'abuso sistematico di architetture e *trust* del sistema operativo (Misconfiguration/Design abuse).

Vulnerabilità / Tecnica	**Riferimento Identificativo**	**Descrizione Dettagliata**
Process Injection / Hollowing	MITRE **T1055.012**	Iniezione di codice malevolo in memoria all'interno dell'eseguibile di sistema legittimo **InstallUtil.exe** per mascherare le attività ai software EDR.

Abuse of System Functionality	**CWE-426** (Untrusted Search Path / Abuso)	Sfruttamento di utility native firmate (come cmd.exe e timeout.exe) per implementare l'approccio *Living off the Land* ed eludere l'analisi euristica.
System Information Discovery	MITRE **T1082**	Accesso non autorizzato alle chiavi di registro di Windows per estrarre il GUID della macchina ed evadere le sandbox.

---

5. Remediation (Mitigazione)

Per difendere l'infrastruttura aziendale da vettori di attacco di questa tipologia, è essenziale applicare un approccio di *Defense in Depth*. Di seguito le raccomandazioni strategiche e tecniche per il contenimento:

- **Hardening degli EDR (Endpoint Detection and Response):**
  Implementare logiche di rilevamento (es. tramite regole *Sigma* o *YARA*) incentrate sul monitoraggio dei processi legittimi sfruttati impropriamente. Generare avvisi critici qualora **InstallUtil.exe** o RegAsm.exe generino comunicazioni di rete in uscita o vengano spawnati come processi figli da eseguibili atipici situati in percorsi utente (es. %APPDATA% o cartella Download).
- **Restrizioni Firewall (Egress Filtering):**
  Riconfigurare il firewall perimetrale applicando politiche di *Default Deny* per il traffico in uscita. Tutto il traffico TCP/UDP verso porte non standard (come la porta **7702** evidenziata nell'attacco) deve essere bloccato e generare un alert per i team del SOC.
- **Aggiornamento delle Threat Intelligence (IoC):**
  Inserire istantaneamente in blocklist all'interno del SIEM, del firewall e degli apparati IDS/IPS l'indirizzo IP del Command and Control scoperto: **91.92.253.47**.
- **Application Control (WDAC/AppLocker):**
  Abilitare e configurare rigorosamente l'Application Whitelisting impedendo l'esecuzione di eseguibili o script non preventivamente approvati e non firmati digitalmente che originano dai profili utente, neutralizzando così l'azione dei *dropper* primari (come **jvczfhe.exe**).