Progetto S11 – L5

Analisi dinamica tramite AnyRun

Executive Summary

L’attività di Studio IOC ha previsto **l’analisi dinamica di un file eseguibile sospetto tramite la piattaforma AnyRun**. L’osservazione del comportamento del file **ha evidenziato il download di un eseguibile da repository GitHub pubblico, l’assenza di firma digitale valida e tentativi di esecuzione potenzialmente pericolosi**.
L’analisi ha permesso di individuare **indicatori di compromissione (IOC) e possibili tecniche utilizzate**, valutando il rischio associato al file analizzato.

Introduzione

L’obiettivo dell’esercizio è **analizzare un campione sospetto utilizzando un ambiente sandbox (AnyRun) per osservare il comportamento del file in esecuzione**. Attraverso l’analisi dei processi, del traffico di rete e degli avvisi di sicurezza generati dal sistema, **è stato possibile identificare attività anomale e raccogliere indicatori utili alla valutazione della minaccia** in ottica cybersecurity.

---

1. Descrizione generale della minaccia

Ho analizzato il task AnyRun relativo all’esecuzione del file:
Jvczfhe.exe

Il file viene scaricato da un repository GitHub pubblico:
https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe

L’analisi è stata effettuata in ambiente Windows 10 a 64 bit con durata totale di 300 secondi.

Il comportamento osservato è coerente con un file eseguibile sospetto potenzialmente utilizzato come **downloader** o **backdoor**.

Il comportamento osservato è coerente con una minaccia di tipo downloader, in quanto **il file viene scaricato da una sorgente remota e successivamente eseguito nel sistema analizzato**.
Questo schema operativo è tipico delle fasi iniziali di compromissione.

---

2. Comportamento osservato

2.1 Accesso al repository GitHub

Durante l’analisi il processo `firefox.exe` accede al repository GitHub contenente l’eseguibile sospetto.

Questo indica una fase di **Ingress Tool Transfer**, cioè il trasferimento di uno strumento da una sorgente remota.

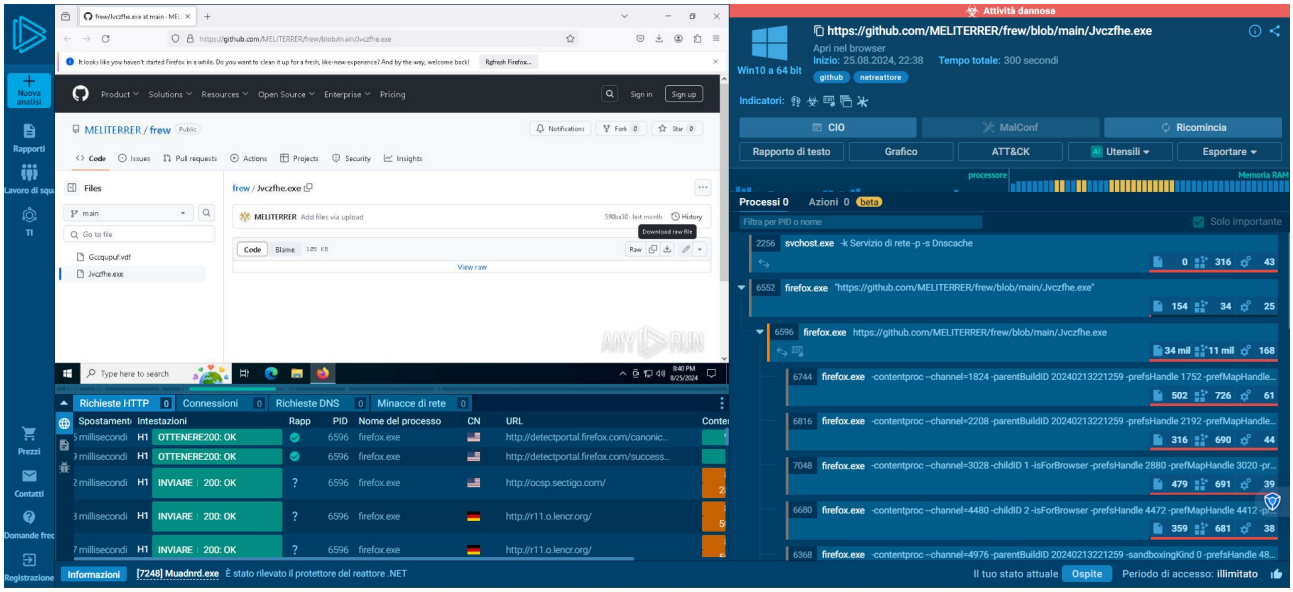

Figura 1 – Accesso al repository GitHub contenente l’eseguibile Jvczfhe.exe.

2.2 Download del file eseguibile

Il file viene scaricato e salvato nel percorso locale
C:\Users\admin\Downloads\Muadrnd.exe

L’azione dimostra che il file viene effettivamente trasferito sul sistema analizzato.

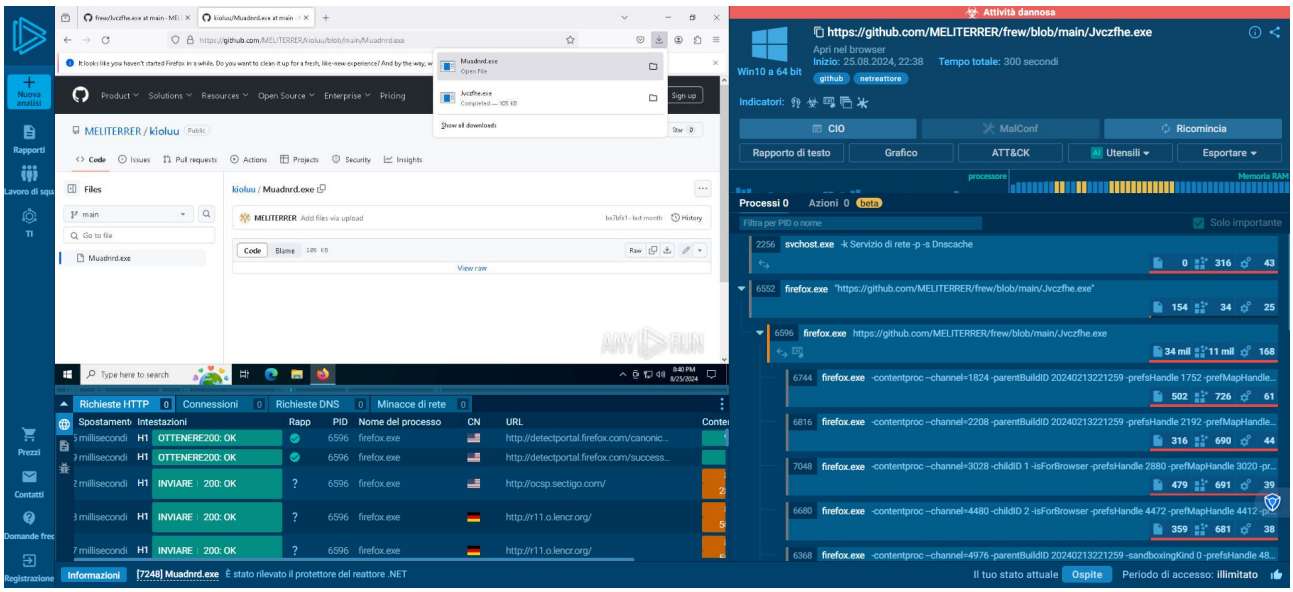

Figura 2 – Download del file Muadrnd.exe nel sistema locale.

2.3 Avviso di sicurezza Windows

Al momento dell'esecuzione, Windows mostra un avviso di sicurezza:

- Publisher: Unknown Publisher
- Firma digitale non valida

Questo rappresenta un forte indicatore di rischio.

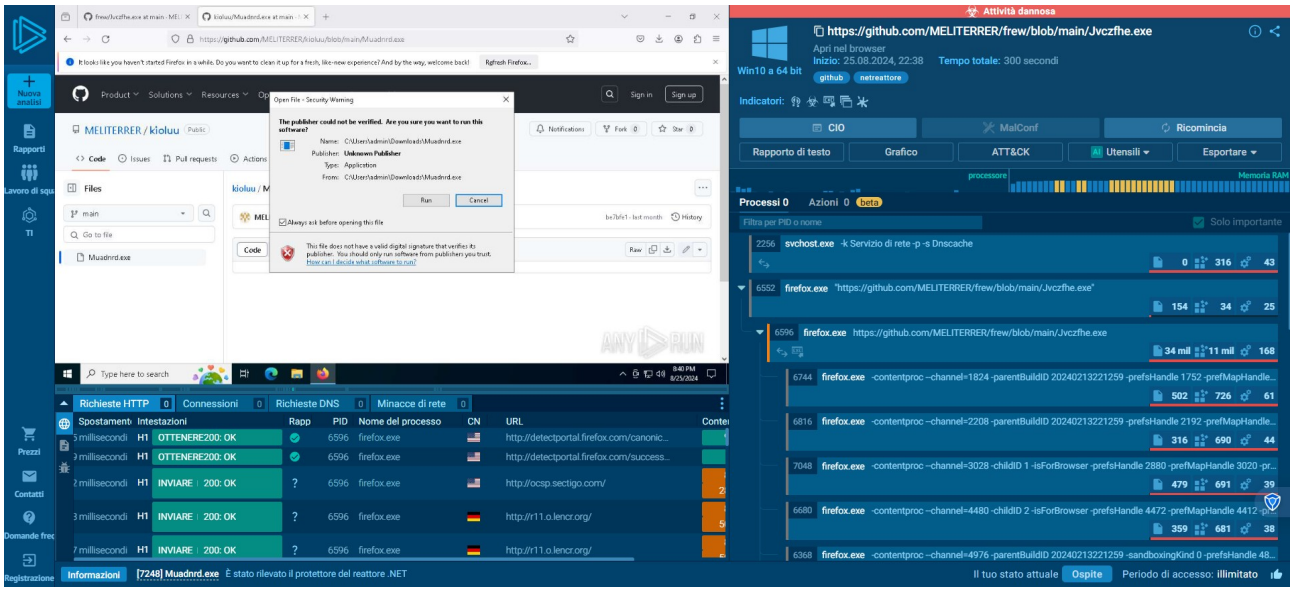

Figura 3 – Avviso di sicurezza Windows: publisher non verificato.

2.4 Analisi dei processi

Nel pannello AnyRun vengono visualizzati i processi attivi durante l’esecuzione:

- firefox.exe
- svchost.exe
- eventuali processi figli

Non si osservano connessioni persistenti evidenti nel breve intervallo analizzato, ma il comportamento è coerente con una fase iniziale di staging.

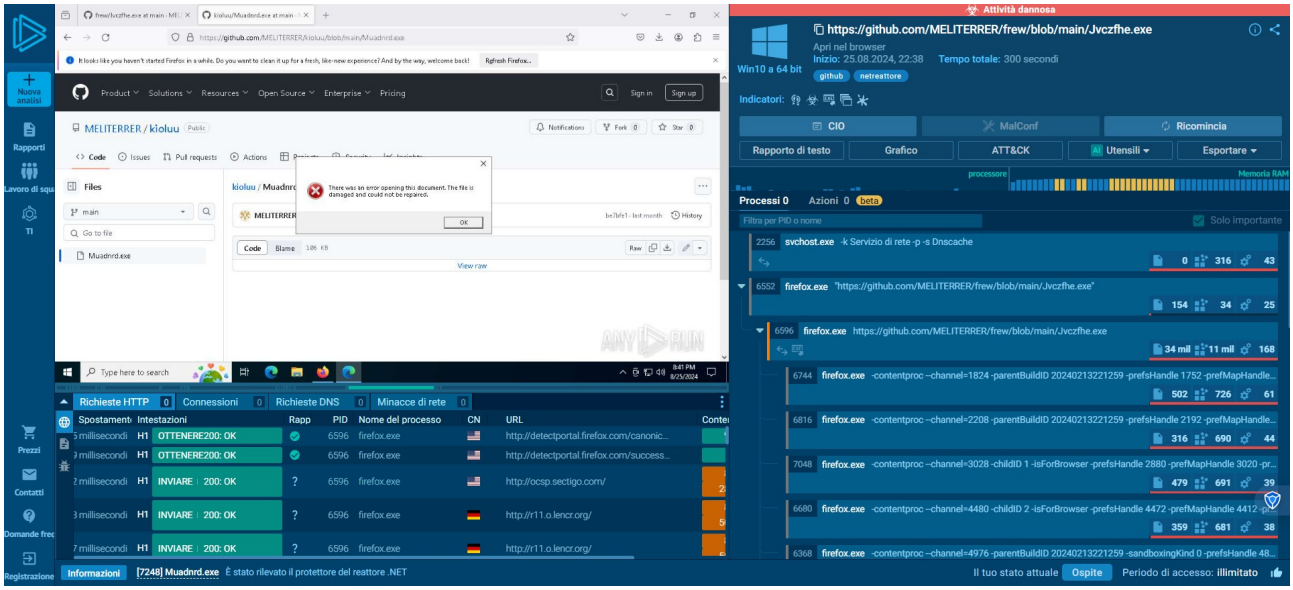

Figura 4 – Vista dei processi attivi durante l’analisi dinamica.

2.5 Traffico di rete

A seguire, nel pannello richieste HTTP e DNS si osservano:

- Connessioni HTTP
- Richieste DNS
- Attività legata al download del file

Il traffico verso GitHub indica il recupero del payload.

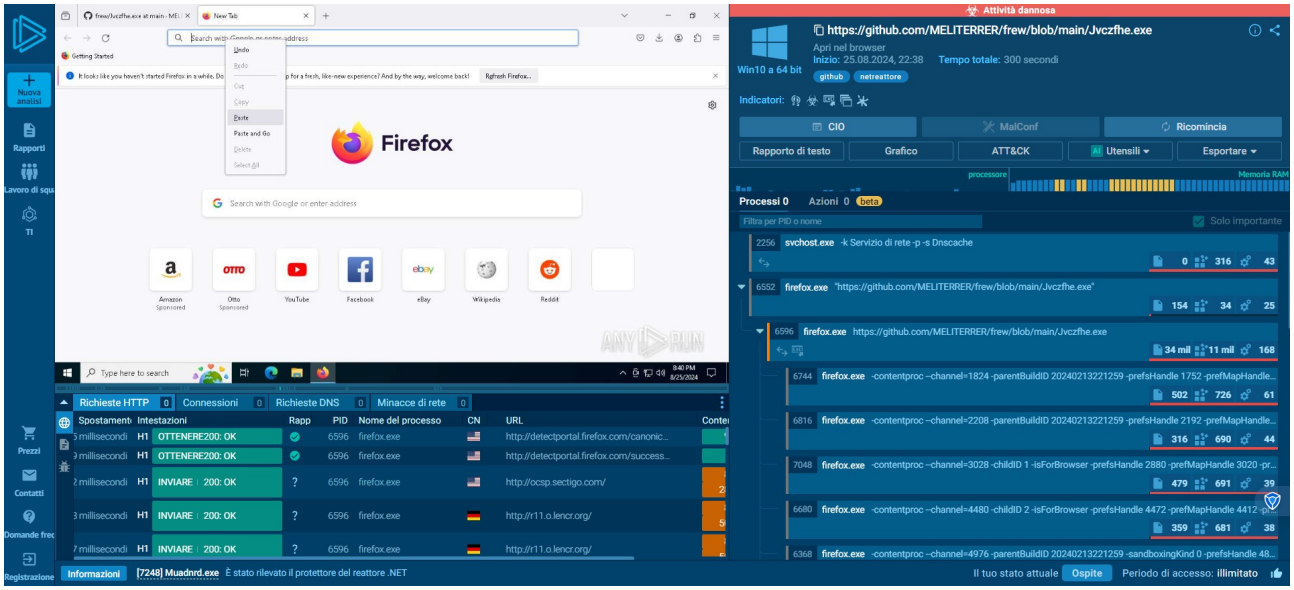

Figura 5 – Monitoraggio richieste HTTP e DNS durante l'analisi.

---

3. Indicatori di Compromissione (IOC)

File sospetti

- Jvczfhe.exe
- Muadrnd.exe

URL

https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe

Dominio

- github.com

Percorso locale

C:\Users\admin\Downloads\

Caratteristiche sospette

- Eseguibile senza firma digitale
- Publisher sconosciuto
- Possibile offuscamento .NET
- Download diretto da repository pubblico

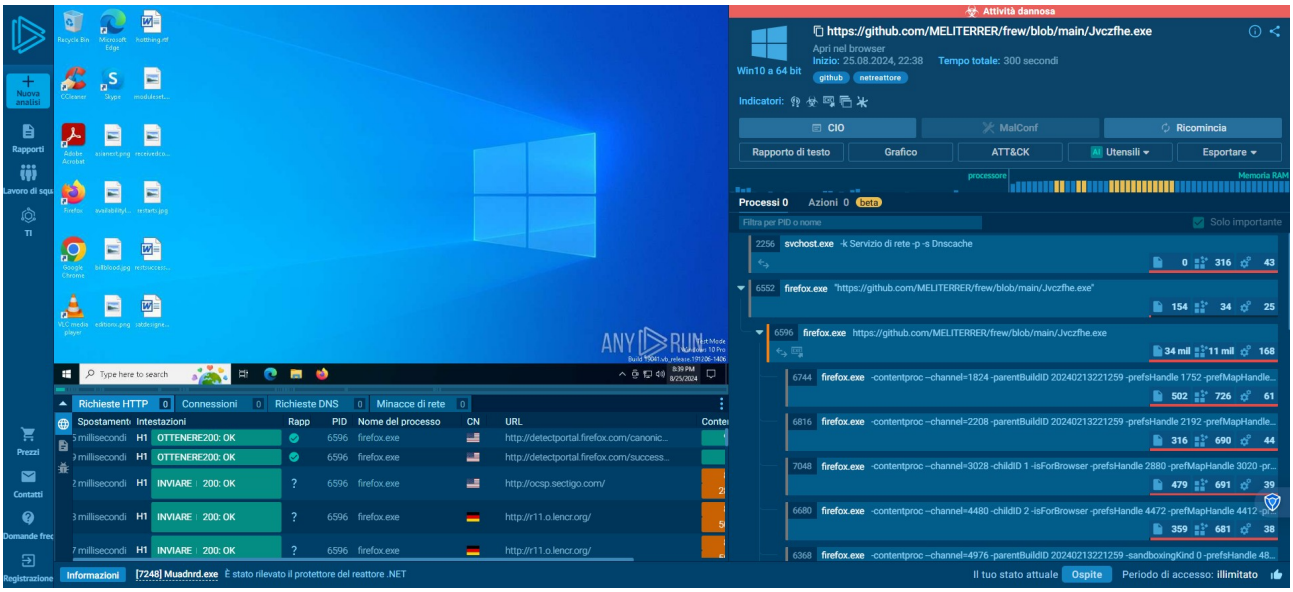

Figura 6 – Evidenza del file scaricato nel sistema analizzato.

---

4. Tecniche MITRE ATT&CK potenzialmente coinvolte

- **T1105 – Ingress Tool Transfer**
- **T1204 – User Execution**
- **T1027 – Obfuscated/Compressed Files**
- **T1059 – Command Execution (potenziale fase successiva)**

---

5. Impatto Potenziale

Se eseguito in ambiente reale, il file potrebbe:

- Installare ulteriori payload
- Stabilire meccanismi di persistenza
- Aprire una backdoor
- Consentire controllo remoto
- Scaricare moduli aggiuntivi

---

6. Conclusione

L’analisi dinamica effettuata su AnyRun evidenzia un comportamento sospetto legato al download e all’esecuzione di un eseguibile non firmato proveniente da repository GitHub pubblico.

La combinazione di:

- Download di file binario
- Assenza di firma digitale
- Publisher sconosciuto
- Potenziale offuscamento

indica un rischio elevato e compatibile con malware di tipo downloader o backdoor.

L’attività dimostra l’importanza dell’analisi dinamica per identificare indicatori di compromissione e valutare la pericolosità di file eseguibili prima dell’esecuzione in ambienti produttivi.