BONUS 1

Analisi del Malware - Muadrnd.exe

---

1. Introduzione

Questa analisi si concentra sul file **Muadrnd.exe**, individuato su un repository GitHub. Il file è stato eseguito all'interno di una sandbox su **Any.Run** per studiarne il comportamento.

L'obiettivo è identificare **indicatori di compromissione (IoC)** e valutare le potenziali minacce.

2. Dati di Base

- **Nome del file**: Muadrnd.exe
- **Dimensione**: 106 KB
- **Provenienza**: GitHub (Link)
- **Protezione rilevata**: .NET Reactor Protector → **Possibile offuscamento del codice**

3. Indicatori di Compromissione (IoC)

A. Processi Eseguiti

- **Jxcfthe.exe** → Probabile payload principale
- **cmd.exe** → Possibile esecuzione di comandi malevoli
- **cohost.exe -Offffffff -ForceV1** → Processo sospetto, potrebbe essere usato per evasione
- **Muadrnd.exe** → Il file originale analizzato
- **InstallUtil.exe** → Strumento spesso abusato da malware per eseguire payload

B. Connessioni di Rete

- **Domini contattati**:
  - `http://10.1a.lonorg/`
  - `http://dcop.safegtp.com/`
  - `http://siscobaypan.org/...`
  - `http://sitectportal.firefox.com/...`
- **Tecniche sospette**:
  - Numerose **richieste GET e POST**, possibili comunicazioni C2 (Command & Control)
  - **Download di file binari e compressi**, segno di possibile esfiltrazione dati

4. Tecniche di Evasione

- Uso di **InstallUtil.exe** per eseguire codice senza essere rilevato
- **Offuscamento tramite .NET Reactor** per rendere difficile l'analisi
- **Cohost.exe con parametri anomali** per bypassare controlli di sicurezza

5. Possibili Impatti

- **Esfiltrazione di dati**: Il malware potrebbe inviare informazioni sensibili ai server remoti
- **Persistenza**: Uso di tecniche per rimanere attivo sul sistema
- **Scaricamento di ulteriori payload**: Possibile download di malware secondario

6. Mitigazioni e Raccomandazioni

- **Bloccare gli IoC identificati** nelle liste di sicurezza (domini, file sospetti)
- **Analizzare ulteriormente Jxcfthe.exe** per capire il payload effettivo
- **Verificare sistemi compromessi** per tracce di InstallUtil.exe e cmd.exe
- **Implementare regole di detection** per anomalie nei processi e connessioni

---

Conclusione: Il file **Muadrnd.exe** mostra segni evidenti di attività malevole, tra cui **evasione dei controlli, comunicazione con server sospetti e possibile esfiltrazione di dati**. È necessaria un'azione immediata per prevenire eventuali compromissioni di sistema.