Rapporto di Analisi Malware – Versione Estesa (Solo Testo)

Riferimento: https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281/

# 1. Panoramica

Il presente rapporto fornisce un’analisi dettagliata di un campione malevolo identificato come jvczfhe.exe. L’analisi è stata effettuata tramite sandbox dinamica e ha evidenziato comportamenti tipici di un malware loader, in grado di scaricare, eseguire e facilitare l’esecuzione di altri payload dannosi. Il malware mostra tecniche avanzate di evasione e sfrutta infrastrutture legittime per eludere il rilevamento. Immagine che contiene testo, schermata, software, Software multimediale

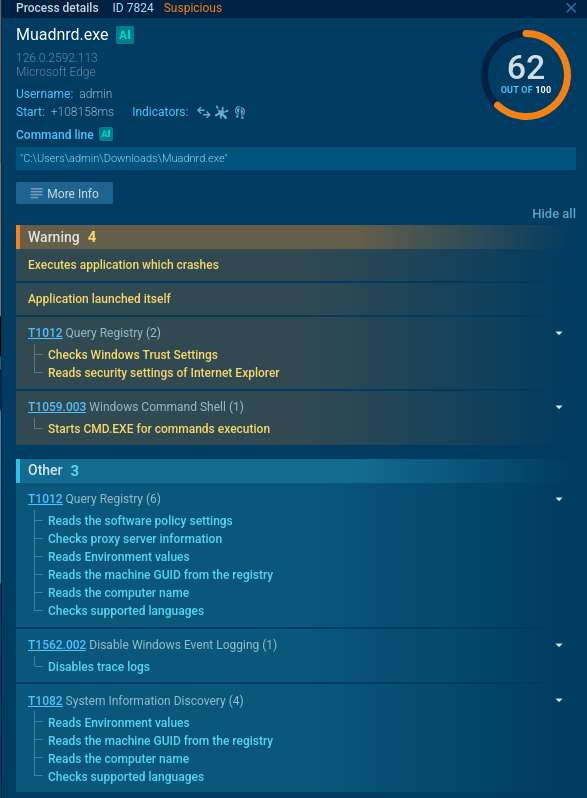
Il contenuto generato dall'IA potrebbe non essere corretto.

# 2. Tecniche e Metodologia

L'analisi si è svolta in ambiente virtualizzato con sistema operativo Windows 10 Professional (build 19045, 64 bit). È stato utilizzato Any.Run per monitorare l'esecuzione dinamica del campione, consentendo l’osservazione in tempo reale delle attività sospette, processi avviati, modifiche al sistema e comunicazioni di rete. La tecnica ha permesso di tracciare le principali TTPs del malware e la sua progressione in ambiente compromesso.

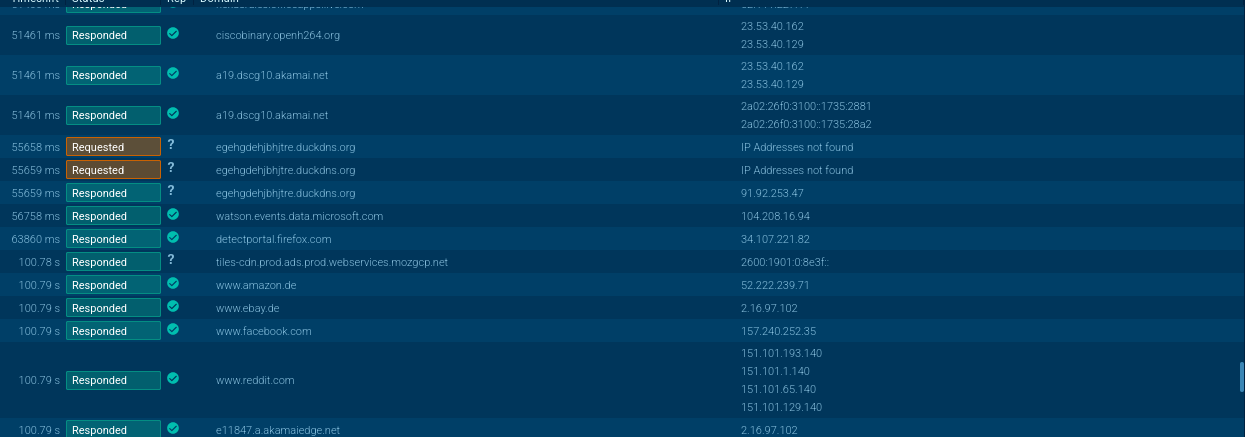
# 3. Dettagli Operativi del Malware

- Il file jvczfhe.exe viene scaricato da GitHub e lanciato sul sistema target.  
- Subito dopo l'avvio, avvia processi figli tra cui installutil.exe (Microsoft .NET tool legittimo, abusato come LotL) e muadnd.exe (payload classificato come minaccia).  
- Il malware utilizza cmd.exe per impartire comandi e timeout.exe per introdurre ritardi nell’esecuzione, spesso per confondere la sandbox.  
- WerFault.exe viene lanciato in maniera anomala, potenzialmente per simulare crash o mascherare attività.  
- Si osservano molteplici istanze di firefox.exe, utilizzate potenzialmente per accedere o manipolare impostazioni browser.  
- Viene effettuata la lettura delle impostazioni di sicurezza di Internet Explorer e dei Windows Trust Settings. Immagine che contiene testo, schermata, Carattere

Il contenuto generato dall'IA potrebbe non essere corretto.

# 4. Attività di Rete

- Il malware scarica il proprio codice da una repository GitHub pubblica.  
- Sono state individuate richieste DNS verso domini \*.duckdns.org, tipici di infrastrutture C2 dinamiche.  
- Le connessioni includono comunicazioni con domini Microsoft, Google, Mozilla e Akamai, che appaiono leciti, ma potrebbero essere mascherati o sfruttati in modo malevolo.  
- Alcune connessioni avvengono su porte non standard, suggerendo l’intento di aggirare controlli firewall e IDS.



# 5. Indicatori di Compromissione

Hash identificativi del file jvczfhe.exe:  
- MD5: 00B5E91B42712471CDFBDB37B715670C  
- SHA1: D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2  
- SHA256: 0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0  
  
Domini e URL sospetti:  
- https://github.com/MELITERER/frew/blob/main/jvczfhe.exe  
- \*.duckdns.org (C2)  
  
File associati:  
- jvczfhe.exe (malware principale)  
- installutil.exe (strumento legittimo abusato)  
- muadnd.exe (payload secondario)  
- cmd.exe, timeout.exe (comandi e delay)  
- WerFault.exe (simulazione crash?)

# 6. Tecniche di Evasione

- Uso di .NET Reactor per offuscare il codice, rendendo difficile l’analisi statica.  
- Attività LotL tramite installutil.exe per sfruttare binari di Windows firmati.  
- Persistenza implementata tramite meccanismi di auto-avvio.  
- Induzione crash per interrompere analisi automatizzate o far scattare eccezioni.  
- Comunicazioni criptiche e porta non standard per eludere analisi comportamentali di rete.



# 7. Impatto e Raccomandazioni

Impatto:  
- Furto di credenziali e informazioni sensibili  
- Download ed esecuzione di ransomware o spyware  
- Integrazione del sistema in botnet  
- Punto d’ingresso per attacchi futuri  
  
Raccomandazioni:  
- Aggiornamento costante di antivirus, EDR e firewall  
- Monitoraggio comportamentale di processi e connessioni anomale  
- Blocco DNS su domini \*.duckdns.org  
- Politiche restrittive su esecuzione software non firmato  
- Formazione continua degli utenti per mitigare phishing e social engineering  
- Prontezza nella risposta a incidenti e analisi forense su sistemi sospetti

# 8. Conclusione

Il malware jvczfhe.exe rappresenta una minaccia moderna, ben strutturata, che combina tecniche avanzate di evasione e persistenza. La sua capacità di sfruttare infrastrutture legittime e strumenti di sistema richiede un approccio difensivo basato sul comportamento e su una solida cultura della sicurezza informatica. L’implementazione delle misure indicate in questo rapporto è fondamentale per rafforzare la resilienza.