Rapporto di Analisi Approfondita del Malware

Data del Rapporto: 13 Giugno 2025

Redatto da: Stefano Gugliota

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

Data Analisi Campione: 25 Agosto 2024 alle 22:38:59

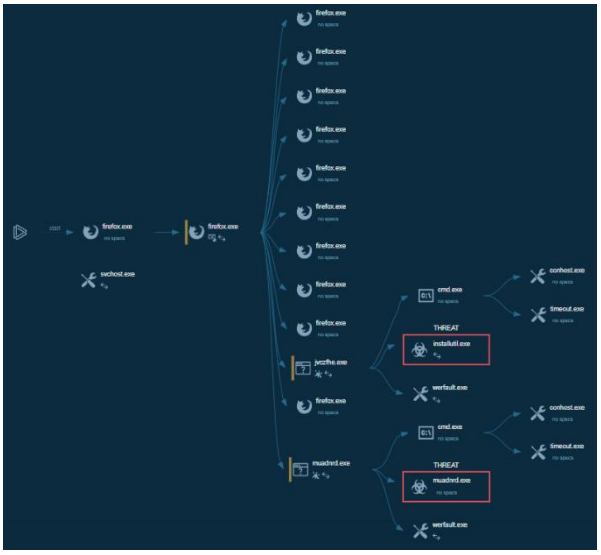
---

1. Sintesi Esecutiva

Il presente rapporto espone i risultati dell'analisi comportamentale di un campione di malware (jvczfhe.exe), osservato tramite un ambiente di sandbox dinamica. L'indagine ha confermato la natura malevola dell'eseguibile, classificato come "Malicious activity", che funge da *downloader* e *loader* per componenti aggiuntivi. La minaccia si distingue per l'impiego di tecniche di evasione del rilevamento (.NET Reactor), l'abuso di processi di sistema legittimi (Living off the Land) e la comunicazione con infrastrutture di rete sospette per la raccolta di informazioni e la potenziale esfiltrazione di dati. Il file analizzato presenta specifici hash crittografici che ne consentono l'identificazione univoca.

2. Contesto e Metodologia

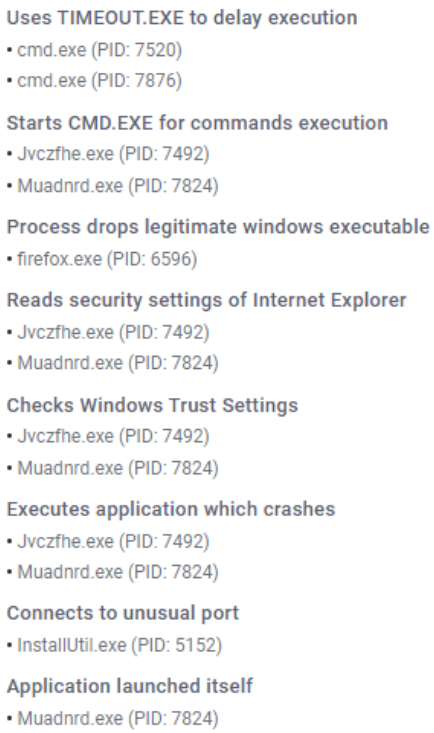
L'analisi è stata condotta esaminando una serie di catture di schermata (screenshot) provenienti da un'esecuzione controllata del campione di malware in un ambiente di analisi dinamica (Any.Run), con data di analisi del campione il 25 Agosto 2024. Il sistema operativo di riferimento è Windows 10 Professional (build: 19045, 64 bit). Questa metodologia ha consentito di osservare il comportamento in tempo reale del malware, inclusa la sua interazione con il sistema operativo, le operazioni sui processi e le comunicazioni di rete. Le informazioni dettagliate fornite dagli screenshot hanno permesso di delineare un profilo robusto delle tattiche, tecniche e procedure (TTPs) impiegate dall'aggressore.



3. Analisi Dettagliata del Comportamento e dei Processi

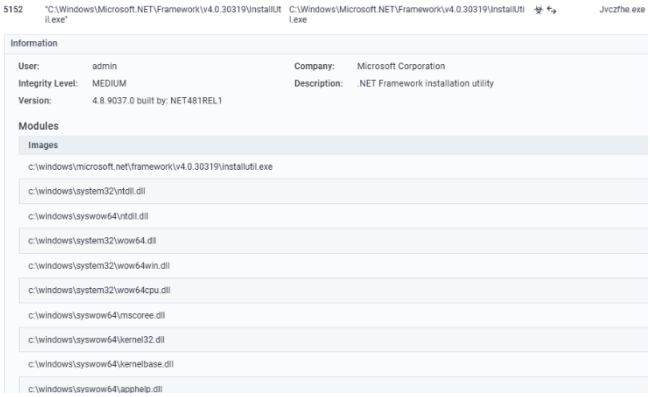
L'infezione ha avuto inizio con l'avvio del processo jvczfhe.exe (Process ID non visibile nel grafico principale, ma menzionato come padre in altri screenshot come 7492). Questo eseguibile, classificato come "Malicious activity", ha manifestato un

comportamento sospetto fin da subito, cercando di scaricare file da una risorsa ospitata su GitHub (https://github.com/MELITERER/frew/blob/main/jvczfhe.exe), una tattica comune per la distribuzione di malware che sfrutta la reputazione di domini legittimi.



La progressione dell'attacco si è articolata come segue, come evidenziato dal grafico dei processi e dai dettagli comportamentali:

- **Punto di Ingresso e Downloader (jvczfhe.exe):** Agisce come primo stadio della catena di infezione, responsabile del recupero e dell'esecuzione di ulteriori componenti dannosi.
- **Generazione di Processi Figli Malevoli:** Il dropper iniziale ha generato processi secondari critici per la fase successiva dell'attacco:
    - **installutil.exe (PID: 5152):** L'utilizzo di installutil.exe, uno strumento legittimo di Microsoft .NET Framework, rappresenta un chiaro esempio di "Living off the Land" (LotL). Il malware abusa di binari di sistema noti per svolgere compiti dannosi e sfuggire al rilevamento, mostrando un livello di integrità "MEDIUM".



    - **muadnd.exe (PID: 7824):** Un altro eseguibile malevolo e classificato come "THREAT" nel grafico dei processi, probabilmente il payload principale o un modulo ausiliario.

- **Abuso di Utilità di Sistema:** L'analisi ha rilevato l'invocazione di cmd.exe per l'esecuzione di comandi (screen 2.png) e l'uso di TIMEOUT.EXE per ritardare l'esecuzione dei processi (spesso per eludere le sandbox o rallentare l'analisi). La presenza di WerFault.exe (PID: 1356), il gestore degli errori di Windows (screen 3.png), avviato in un contesto sospetto (jvczfhe.exe come padre), potrebbe indicare crash indotti dal malware o un ulteriore abuso per mascherare attività.
- **Interazione con l'Ambiente Utente e Browser:** Il grafico dei processi mostra numerose istanze di firefox.exe. Sebbene firefox.exe sia stato rilevato "dropping legitimate windows executable", la sua massiccia presenza potrebbe essere legata all'attività del malware. Il malware "Reads security settings of Internet Explorer" e

"Checks Windows Trust Settings", indicando una ricerca di vulnerabilità o tentativi di manipolare le configurazioni di sicurezza del browser o del sistema.

- **Comportamenti Aggiuntivi Rilevati:**
    - **Connessione a Porta Insolita:** InstallUtil.exe (PID: 5152) "Connects to unusual port", suggerendo una comunicazione non standard, potenzialmente per il C2.
    - **Auto-Avvio (Application launched itself):** muadnd.exe (PID: 7824) ha mostrato la capacità di auto-avviarsi, indicando la creazione di un meccanismo di persistenza sul sistema.
    - **Crash di Applicazioni:** Il malware "Executes application which crashes", un comportamento che può essere usato per disorientare l'analisi o per sfruttare vulnerabilità in software specifico.

4. Analisi dell'Attività di Rete

Le attività di rete sono fondamentali per tracciare le origini dei payload e le comunicazioni del malware con la sua infrastruttura di Comando e Controllo (C2).

- **Download di Payload Iniziale:**
    - https://github.com/MELITERER/frew/blob/main/jvczfhe.exe: Questa URL è stata la fonte del jvczfhe.exe. La reputazione "shared" per github.com nelle richieste DNS evidenzia come gli aggressori sfruttino domini legittimi per la distribuzione di malware.

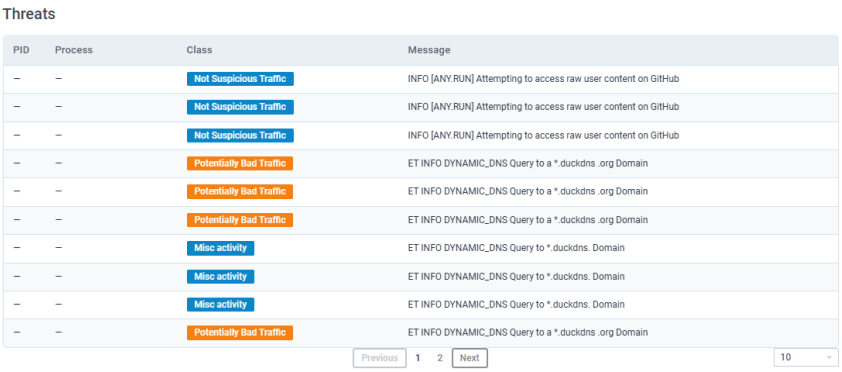
DNS requests

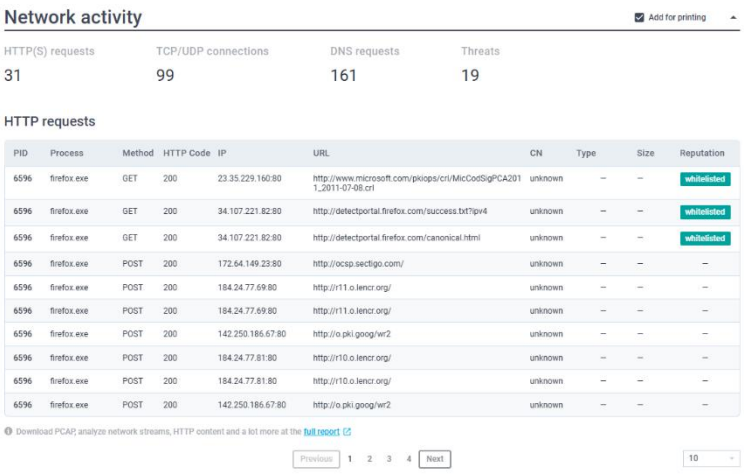
Domain	IP	Reputation
settings-win.data.microsoft.com	40.127.240.158 51.124.78.146	whitelisted
google.com	142.250.185.238	whitelisted
github.com	140.82.121.3	shared
detectportal.firefox.com	34.107.221.82	whitelisted
prod.detectportal.prod.cloudops.mozgcp.net	34.107.221.82 2600:1901:0:38d7::	whitelisted
example.org	93.184.215.14	whitelisted
ipv4only.arpa	192.0.0.170 192.0.0.171	whitelisted
contile.services.mozilla.com	34.117.188.166	whitelisted
spocs.getpocket.com	34.117.188.166	whitelisted
prod.ads.prod.webservices.mozgcp.net	34.117.188.166	unknown

Previous 1 2 3 4 5 6 7 8 Next 10

-

- **Connessioni Sospette/C2 e Attività DNS Anomale:**
    - Le minacce mostrano "Potentially Bad Traffic" legato a query DNS per domini *.duckdns.org. DuckDNS è un servizio di DNS dinamico spesso abusato da malware per stabilire connessioni C2 resilienti, poiché l'indirizzo IP associato al dominio può cambiare frequentemente.





    - Sebbene molti degli URL e IP nelle attività HTTP/S e connessioni siano legati a servizi legittimi (Microsoft, Mozilla Firefox, Google, Akamai, Sectigo) e classificati come "whitelisted" o "unknown", la loro presenza in un contesto di attività malevola merita un'attenta valutazione per escludere tecniche di mascheramento o di "fast-flux".
    - detectportal.firefox.com e contfile.services.mozilla.com sono legittimi, ma la loro frequenza o il contesto potrebbero essere monitorati per anomalie.

5. Indicatori di Compromissione (IoC)

Gli IoC sono artefatti critici per la rilevazione e la difesa contro questa minaccia.

- **File Hashes (del campione originale jvczfhe.exe - da screen 1.png):**
    - **MD5:** 00B5E91B42712471CDFBDB37B715670C
    - **SHA1:** D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
    - **SHA256:** 0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
    - **SSDEEP:** 3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa
- **URL/Domini Maligni o Sospetti:**

- https://github.com/MELITERER/frew/blob/main/jvczfhe.exe (Fonte del dropper)
- *.duckdns.org (Domini di C2 basati su DNS dinamico)

- **Nomi di File Maligni/Sospetti (o abusati):**
  - jvczfhe.exe
  - installutil.exe (uso sospetto/abuso di strumento legittimo)
  - muadnd.exe
  - WerFault.exe (uso sospetto/abuso di strumento legittimo)
  - cmd.exe, timeout.exe (abuso di strumenti di sistema)
- **Sistema Operativo Target:** Windows 10 Professional (build: 19045, 64 bit)

6. Tecniche di Evasione del Rilevamento

Il rilevamento del **".NET Reactor protector"** evidenzia che il malware è stato impacchettato e offuscato per complicare l'analisi statica del codice e eludere i sistemi di rilevamento basati su firme. I *packers* come .NET Reactor sono comunemente utilizzati per nascondere il vero intento del malware fino all'esecuzione, dove il codice si spacchetta in memoria, rendendo più difficile il reverse engineering e l'analisi automatica.

URL:	https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe
Full analysis:	https://app.any.run/tasks/9a158718-43fe-45ce-85b3-66203dbc2281
Verdict:	Malicious activity
Analysis date:	August 25, 2024 at 22:38:59
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	github netreactor
Indicators:	
MD5:	00B5E91B42712471CDFBDB37B715670C
SHA1:	D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
SHA256:	0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
SSDEEP:	3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

7. Impatto Potenziale e Raccomandazioni

Questo campione di malware, data la sua architettura a più stadi, le capacità di persistenza e la raccolta di informazioni, rappresenta una minaccia significativa. L'impatto potenziale su un sistema compromesso include, ma non si limita a: furto di credenziali e dati sensibili, deployment di ulteriori payload (es. ransomware, spyware), integrazione in botnet e l'utilizzo del sistema come punto di lancio per attacchi successivi.

Per mitigare questa minaccia e rafforzare la postura di sicurezza aziendale, si raccomandano le seguenti azioni:

1. **Aggiornamento e Implementazione delle Difese:**
    - Assicurarsi che le soluzioni di sicurezza per endpoint (EDR, Antivirus) e perimetrali (Firewall, IDS/IPS, proxy web) siano costantemente aggiornate e configurate per rilevare e bloccare gli IoC basati su hash, URL e domini identificati.
    - Implementare regole di blocco per i domini *.duckdns.org a livello di DNS o firewall.
2. **Monitoraggio Comportamentale Avanzato:**
    - Rafforzare il monitoraggio per l'esecuzione anomala di processi di sistema legittimi (installutil.exe, cmd.exe, WerFault.exe, timeout.exe), specialmente se avviati in contesti insoliti, da directory non standard o con parametri sospetti.
    - Monitorare le connessioni verso porte insolite o indirizzi IP non standard.
3. **Sicurezza degli Endpoint e Governance:**
    - Adottare politiche di sicurezza che limitino l'esecuzione di eseguibili non firmati o da fonti non attendibili (es. Software Restriction Policies, AppLocker).
    - Applicare il principio del privilegio minimo agli account utente e di sistema.
4. **Sensibilizzazione e Formazione degli Utenti:**
    - Conduce formazioni regolari sulla cybersecurity per educare gli utenti sui pericoli del phishing, dell'ingegneria sociale e del download di software da fonti non verificate, che rappresentano i vettori iniziali comuni per tali infezioni.
5. **Analisi Forense e Risposta agli Incidenti:**
    - In caso di rilevamento di attività simili, avviare immediatamente i protocolli di risposta agli incidenti, isolare i sistemi compromessi e condurre un'analisi forense approfondita per determinare l'estensione completa della compromissione.

---

8. Conclusioni

In sintesi, l'analisi del campione di malware jvczfhe.exe ha rivelato un'operazione complessa e ben congegnata, che sfrutta tattiche raffinate per stabilire una presenza persistente e raccogliere informazioni sul sistema target. L'utilizzo di .NET Reactor` per l'offuscamento, unitamente all'abuso di binari di sistema legittimi e all'uso di

infrastrutture di C2 dinamiche (DuckDNS), sottolinea la determinazione degli aggressori a eludere le difese e a mantenere il controllo.

Gli Indicatori di Compromissione (IoC) e i comportamenti identificati forniscono dati essenziali per le squadre di sicurezza per rilevare, analizzare e mitigare efficacemente questa specifica minaccia. L'implementazione proattiva delle raccomandazioni delineate è cruciale per rafforzare la resilienza organizzativa contro simili attacchi future e per mantenere una solida postura di sicurezza cibernetica.