BONUS 1
Analisi malware con Anyrun.

General Info

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 26, 2024 at 06:38:59
OS:	Windows 10 Professional (build: 19045, 64 bit)
Tags:	github netreactor
Indicators:	
MD5:	00B5E91B42712471CDFBDB37B715670C
SHA1:	D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2
SHA256:	0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
SSDEEP:	3:N8tEd7QyQ3FJMERCNuN:2uRQyQ3zMsCNa

Da una prima visione dell'analisi, si possono notare diversi IOC (indicatori di compromissione), che suggeriscono attività malevole nel sistema:

1. Jvczfhe.exe (PID: 7492): questo eseguibile è stato identificato come il punto di origine degli eventi anomali.

Il suo comportamento include:

- Lettura delle impostazioni di sicurezza di Internet Explorer e delle trust settings di Windows, probabilmente per verificare o bypassare restrizioni di sicurezza.
- Avvio di cmd.exe, che esegue una serie di comandi malevoli.
- Tra i processi figli di cmd.exe, sono stati individuati:
  conhost.exe → Componente legittimo di Windows, utilizzato per gestire le finestre della console.
  timeout.exe → Comando di Windows che introduce ritardi nell'esecuzione. Il malware potrebbe sfruttarlo per eludere analisi automatiche.

2. InstallUtil.exe (PID: 5152):

- Questo processo (legittimo) ha segnalato una connessione su una porta anomala, suggerendo un possibile tentativo di evasione dei firewall o di stabilire una comunicazione con un server remoto.
- InstallUtil.exe è spesso sfruttato dai malware per eseguire codice malevolo in modo stealth, poiché fa parte del framework .NET di Windows.

3. Muadnrd.exe (PID: 7824) potrebbe essere una variante del file malevolo principale
   Simile a Jvczfhe.exe, ma con una differenza: si avvia autonomamente senza necessità di ulteriori trigger.

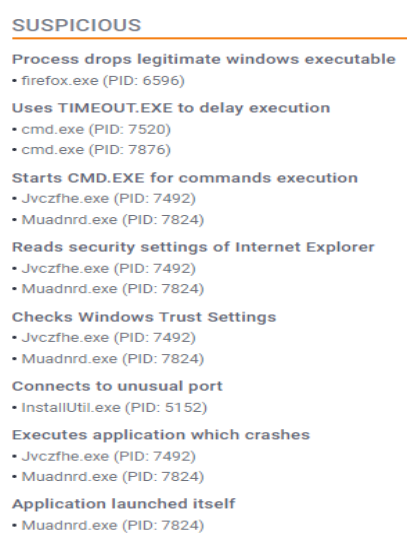
- Anche in questo caso, viene avviato cmd.exe, con i relativi sottoprocessi:
  conhost.exe
  timeout.exe

4. WerFault.exe (PID: 7584)

- Questo processo, solitamente usato da Windows per la gestione degli errori, sembra essere stato sfruttato per alterare le configurazioni del sistema.
- È stato osservato creare nuovi file e cartelle, segnalando potenziali modifiche persistenti nel sistema.

Analizzando meglio il report prodotto da Anyrun, tra le attività comportamentali, abbiamo notato delle attività sospette, tra cui:

- **Il processo rilascia un eseguibile legittimo di Windows**
  firefox.exe (PID: 6596)
- **Utilizza TIMEOUT.EXE per ritardare l'esecuzione**
  cmd.exe (PID: 7520)
  cmd.exe (PID: 7876)
- **Avvia CMD.EXE per eseguire comandi**
  Jvczfhe.exe (PID: 7492)
  Muadnrd.exe (PID: 7824)
- **Legge le impostazioni di sicurezza di Internet Explorer**
  Jvczfhe.exe (PID: 7492)
  Muadnrd.exe (PID: 7824)
- **Controlla le impostazioni di attendibilità di Windows**
  Jvczfhe.exe (PID: 7492)
  Muadnrd.exe (PID: 7824)
- **Si connette a una porta insolita**
  InstallUtil.exe (PID: 5152)
- **Esegue un'applicazione che poi si arresta in modo anomalo**
  Jvczfhe.exe (PID: 7492)
  Muadnrd.exe (PID: 7824)
- **L'applicazione si avvia autonomamente**
  Muadnrd.exe (PID: 7824)



Conclusioni

In sintesi, i comportamenti che suggeriscono un'attività anomala indicano che il malware sta leggendo i dettagli del sistema e controllando le impostazioni di sicurezza, operazioni che spesso precedono l'esecuzione di azioni malevoli. Inoltre, scrive file e cartelle all'interno del sistema utilizzando strumenti legittimi come InstallUtil.exe, mascherando così la propria attività per evitare rilevamenti. Un altro comportamento sospetto è l'uso di timeout.exe per ritardare l'esecuzione, cercando di eludere i sistemi di rilevamento automatizzati. Il malware inoltre disabilita le impostazioni di tracing, bypassa il proxy e si assicura il controllo remoto della macchina target, sfruttando connessioni verso porte insolite per DNS sospetti come duckdns, il che potrebbe essere un tentativo di comunicare con server di comando e controllo per ricevere comandi ed inviare dati rubati.

Queste attività ci fanno ipotizzare che qualcuno abbia preso controllo del computer da remoto oppure che precedentemente sia stato caricato un loader (file malevolo che viene utilizzato per caricare altri malware o payload dannosi su una macchina compromessa) che abbia innescato la serie di comportamenti anomali descritti sopra.

Raccomandazioni per il caso specifico

1. Indagine approfondita e isolamento del sistema compromesso.
2. Verifica e rimozione dei file sospetti: I file sospetti come Jvczfhe.exe, Muadnrd.exe, e altre istanze che potrebbero risultare dannose devono essere rimosse.
3. Controllo dei registri di sistema: Esaminare e rimuovere eventuali modifiche ai registri effettuate dal malware, come quelle relative a HKEY_LOCAL_MACHINE o HKEY_CURRENT_USER, che potrebbero essere state utilizzate per persistere o per manipolare le configurazioni del sistema. In particolare, rivedere chiavi come quelle che riguardano la tracciabilità o la configurazione del proxy.
4. Rafforzare le configurazioni di sicurezza: Eseguire una revisione delle impostazioni di sicurezza di Internet Explorer, delle configurazioni di rete e dei firewall per garantire che siano correttamente configurati e che eventuali connessioni sospette (come quelle verso domini DDNS o porte non comuni) siano bloccate.

Raccomandazioni generali per la prevenzione

1. Formazione continua degli utenti: Fornire corsi di sensibilizzazione alla sicurezza per gli utenti, in modo che siano consapevoli delle minacce come phishing, malware e attacchi mirati. Questo è particolarmente utile per evitare che gli utenti eseguano involontariamente file sospetti o accedano a link dannosi.
2. Monitoraggio proattivo delle connessioni e del traffico di rete: Investire in strumenti di monitoraggio in tempo reale per osservare e analizzare il traffico di rete. In particolare, monitorare le connessioni che cercano di accedere a porte non standard o a domini sconosciuti potrebbe aiutare a rilevare connessioni verso server di comando e controllo.
3. Backup regolari e test di ripristino.
4. Segmentazione della rete e protezione degli endpoint: Implementare una segmentazione della rete per limitare l'accesso tra le diverse aree della rete aziendale. Utilizzare anche soluzioni di protezione endpoint avanzate che rilevino attività sospette e segnali di malware prima che possano causare danni significativi.
5. Rilevamento e risposta agli incidenti (IR): Avere un piano di rilevamento e risposta agli incidenti (IR) ben definito, che includa procedure per isolare e contenere gli attacchi, raccogliere evidenze, e ripristinare rapidamente i sistemi compromessi. È importante che questo piano venga testato regolarmente.