Report di Analisi SOC

Indagine Dinamica di Malware – ANY.RUN

Ardelean Pop Catalin
Master in Cyber Security Specialist – Epicode

20 febbraio 2026

Indice

1 Riepilogo Esecutivo

Il file eseguibile **Jvczfhe.exe**, scaricato da un repository pubblico su GitHub, è stato sottoposto a sandbox dinamica tramite la piattaforma ANY.RUN.

L'analisi ha evidenziato comportamenti compatibili con:

- Malware di tipo **Dropper** o **Loader** modulare
- Tecniche di elusione di sandbox
- Esecuzione di comandi di sistema
- Attività potenziale di comunicazione verso server esterni

Livello di Gravità: ALTO Livello di Confidenza: Medio–Alto Impatto Potenziale: Compromissione iniziale con possibile payload secondario

2 Metadati del Campione

- Nome file: `Jvczfhe.exe`
- Fonte: Repository GitHub pubblico
- Sistema operativo sandbox: Windows 10 Pro x64
- Verdict ANY.RUN: *Malicious Activity*

Hash SHA256:

```
0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
```

2.1 Esecuzione dei Processi

Durante l'esecuzione in sandbox del file `Jvczfhe.exe`, è stata osservata la seguente catena di processi:

- `Jvczfhe.exe` (processo iniziale) – Eseguibile scaricato e lanciato manualmente nella sandbox.
- `Muadnrd.exe` (processo figlio) – Creato da `Jvczfhe.exe` tramite `CreateProcess`, indicativo di rilascio di payload secondario.
- `cmd.exe` (Command Prompt) – Invocato dal processo figlio per eseguire comandi batch e script, potenzialmente per configurare l'ambiente o eseguire payload aggiuntivi.
- `timeout.exe` (ritardo controllato) – Utilizzato per introdurre un ritardo prima dell'esecuzione di ulteriori azioni, tipico comportamento di **sandbox evasion**.

Osservazioni dettagliate SOC:

1. **Processo iniziale (`Jvczfhe.exe`):**
   - Avvio manuale nella sandbox ha innescato la creazione di processi figli.
   - Comportamento tipico di loader/dropper, che prepara il sistema per il rilascio di ulteriori componenti.
   - Potenziale raccolta di informazioni sull'ambiente locale prima di eseguire payload secondari (es. verifica OS, privilegi utente, presenza di strumenti di sicurezza).
2. **Processo figlio (`Muadnrd.exe`):**
   - Creato tramite API Windows `CreateProcess`, indicativo di modularità: loader e payload separati.
   - Potenziale esecuzione di ulteriori comandi batch o script.
   - Analisi comportamentale evidenzia tentativi di bypassare protezioni standard dell'OS.
   - Mapping MITRE ATT&CK: **T1105 – Ingress Tool Transfer** (trasferimento di strumenti o componenti aggiuntivi).
3. **Shell invocata (`cmd.exe`):**
   - Invocazione diretta dalla catena malware indica capacità di eseguire comandi arbitrari.
   - Possibile uso per configurazioni temporanee, esecuzione script di persistence o raccolta informazioni.
   - MITRE ATT&CK mapping: **T1059 – Command and Scripting Interpreter**.
4. **Ritardo controllato (`timeout.exe`):**
   - Inserimento di delay artificiale per evitare rilevamento da sandbox automatizzate.
   - Tecnica comune di **sandbox evasion** (MITRE ATT&CK: **T1497 – Virtualization/Sandbox Evasion**).
   - La temporizzazione può anche servire per sincronizzare il rilascio di payload secondari o la comunicazione con C2.

Indicazioni operative SOC:

- La sequenza di processi suggerisce un malware modulare con capacità di **pre-esecuzione di ricognizione** e evasione.
- La creazione di processi non standard e l'uso di shell estende la superficie di attacco, richiedendo monitoraggio tramite EDR per processi sospetti.
- Ogni processo nella catena può generare indicatori di compromissione (IOC) separati: file drop, parent-child relationship, comandi batch.
- Raccomandato attivare regole di rilevamento su eventi di processo (EventID 4688/4689) per tracciare genesi e fine dei processi non di sistema.
- L'analisi suggerisce che il malware è pronto per azioni post-compromise, come raccolta informazioni, comunicazioni C2 e deploy di ulteriori payload.

Sintesi MITRE ATT&CK correlate alla catena processi:

- **T1059** – Command and Scripting Interpreter (cmd.exe)
- **T1105** – Ingress Tool Transfer (Muadnrd.exe)
- **T1497** – Virtualization/Sandbox Evasion (timeout.exe)
- **T1082** – System Information Discovery (azioni di ricognizione iniziale)

3 Attività sul File System

Durante l'esecuzione in sandbox del campione `Jvczfhe.exe`, sono state osservate le seguenti attività sul file system:

- **Creazione di file temporanei e artefatti:** il malware ha generato file temporanei nelle directory utente e di sistema (`C:\Users\<utente>\AppData\Local\Temp`). Questi artefatti possono essere utilizzati per staging di payload o caching di informazioni di processo.
- **Drop di eseguibili secondari:** sono stati creati file eseguibili figli (es. `Muadnrd.exe`) in percorsi accessibili all'utente, indicativi di comportamento modulare e potenziale preparazione di payload addizionali.
- **Interazione con directory utente:** il malware ha eseguito letture/scritture in directory dell'utente corrente, compatibile con raccolta di file sensibili o configurazioni locali.

- **Potenziale tentativo di sovrascrittura di file legittimi:** osservati accessi a file di configurazione o eseguibili presenti nelle directory comuni, comportamento tipico per persistence o attacco di tipo "file replacement".

Valutazione SOC:

- La creazione di artefatti temporanei e drop di file secondari è tipica dei **loader e dropper**, utilizzati per separare il codice iniziale dal payload principale.
- L'interazione con directory utente indica potenziale raccolta di dati sensibili e preparazione all'esfiltrazione.
- Il tentativo di sovrascrittura di file legittimi rappresenta un indicatore di rischio per alterazioni del sistema operativo o dei software installati.

MITRE ATT&CK correlati:

- **T1070.004** – Indicatori di pulizia: File Deletion/Temporary Files
- **T1036.005** – Masquerading: Match Legitimate Name or Location
- **T1105** – Ingress Tool Transfer

Raccomandazioni operative:

- Monitorare la creazione di eseguibili in percorsi non standard (AppData, Temp)
- Tracciare modifiche ai file esistenti e sovrascritture sospette
- Bloccare hash di file sospetti su EDR/AV

4 Attività sul Registro di Sistema

Durante l'analisi dinamica, il malware ha eseguito le seguenti operazioni sul registro di sistema:

- **Lettura delle impostazioni di sicurezza di Internet Explorer:** per identificare configurazioni di protezione e possibili bypass.
- **Interrogazione delle zone di sicurezza di Windows:** utile per determinare quali URL o directory sono considerate sicure, influenzando l'esecuzione di script e payload.
- **Ricognizione dei parametri di policy:** lettura delle Group Policy locali e parametri di sicurezza per individuare restrizioni su esecuzione di software o accesso a risorse.

Valutazione SOC:

- Queste azioni rappresentano una fase di **ricognizione dell'ambiente locale**, utile al malware per adattare il proprio comportamento evitando sistemi protetti.
- La lettura selettiva delle configurazioni di sicurezza indica tecniche avanzate di evasione e fingerprinting del sistema.
- Comportamento coerente con malware modulare o loader preparatorio per payload secondario.

MITRE ATT&CK correlati:

- **T1082** – System Information Discovery
- **T1012** – Query Registry
- **T1497** – Virtualization/Sandbox Evasion (verifica impostazioni di sicurezza per rilevare ambiente sandbox)

Raccomandazioni operative:

- Audit dei log di accesso al registro di sistema per processi non autorizzati
- Monitoraggio di query sospette su chiavi relative a sicurezza e policy
- Applicazione di regole EDR per bloccare modifiche/letture non autorizzate del registro

5 Attività di Rete

Durante l'esecuzione del campione `Jvczfhe.exe`, sono state osservate le seguenti attività di rete:

- **Query DNS:** il malware ha effettuato richieste DNS verso domini generati dinamicamente o potenzialmente sospetti. Questa attività è compatibile con tecniche di **Domain Generation Algorithm (DGA)** o tentativi di risolvere C2.
- **Tentativi di comunicazione HTTP:** pacchetti in uscita su protocolli standard (HTTP/HTTPS) verso host non riconosciuti. Il payload potrebbe tentare beaconing periodico per rilevare connessioni C2.
- **Connessioni su porte non standard:** sono state tentate connessioni TCP verso porte non convenzionali, comportamento tipico per bypassare firewall o monitoraggio di rete.

Valutazione SOC:

- Sebbene non sia stato confermato un server C2 attivo, la combinazione di query DNS, tentativi HTTP e connessioni su porte non standard rappresenta un **potenziale contatto esterno**, tipico di malware modulare in fase di staging.
- Possibile attività di **data exfiltration** o preparazione di canali di comando e controllo.
- Raccomandato attivare monitoraggio tramite IDS/IPS per traffico sospetto verso domini/host non autorizzati.

MITRE ATT&CK correlati:

- **T1071.001** – Application Layer Protocol: Web Protocols
- **T1071.002** – Application Layer Protocol: DNS
- **T1090** – Proxy, Tunneling e Beaconing
- **T1105** – Ingress Tool Transfer (seconde fasi di download)

6 Indicatori di Compromissione (IOC)

6.1 Hash del file

```
SHA256:
0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0
```

6.2 Processi sospetti

- `Jvczfhe.exe` – processo iniziale, loader/dropper
- `Muadnrd.exe` – payload secondario
- `cmd.exe` – eseguito da processo non di sistema, indicativo di esecuzione di comandi arbitrari

6.3 IOC Comportamentali

- Esecuzione di shell non standard
- Catena di processi sospetti con parent-child non convenzionali
- Ritardo controllato (`timeout.exe`) per elusione sandbox

- Drop di file secondari in percorsi utente temporanei
- Tentativi di connessioni esterne (DNS, HTTP) verso host sconosciuti

Raccomandazioni SOC:

- Bloccare e quarantinare hash del file sospetto su EDR/AV.
- Monitorare processi figlio generati da eseguibili non firmati.
- Implementare alert su creazione/esecuzione di file in directory temporanee.
- Analizzare log di rete per connessioni verso domini o IP non autorizzati.

7 Mappatura MITRE ATT&CK

Sulla base delle attività osservate, la seguente mappatura MITRE ATT&CK è stata identificata:

- **T1059** – Command and Scripting Interpreter (esecuzione di `cmd.exe`)
- **T1204** – User Execution (avvio manuale o involontario da parte dell'utente)
- **T1497** – Virtualization/Sandbox Evasion (`timeout.exe`)
- **T1105** – Ingress Tool Transfer (drop di eseguibili secondari)
- **T1082** – System Information Discovery (ricognizione dell'ambiente)
- **T1071** – Application Layer Protocol (HTTP, DNS)

8 Classificazione della Minaccia

In base all'analisi comportamentale e ai IOC rilevati, il campione può essere classificato come:

- **Loader di accesso iniziale** – finalizzato al rilascio e preparazione di payload secondari.
- **Framework dropper modulare** – con capacità di scaricare/eseguire componenti aggiuntivi.
- **Componente malware in fase di staging** – indicativo di attività preliminare, con possibile beaconing e raccolta informazioni.

Nota SOC: Non sono state osservate attività di cifratura dati (ransomware) o esfiltrazione massiva durante la sessione analizzata. Il rischio principale è legato all'installazione di ulteriori payload, potenziale persistenza e creazione di canali di comunicazione verso host esterni. Si raccomanda monitoraggio continuo dei processi e del traffico di rete sospetto per rilevare eventuali fasi successive.

9 Valutazione del Rischio

Impatto potenziale in un ambiente di produzione:

- Potenziale download di payload addizionali
- Possibilità di esecuzione remota di comandi
- Preparazione per movimento laterale
- Possibile installazione di meccanismi di persistenza

Livello di rischio: ALTO

10 Raccomandazioni per il SOC

10.1 Azioni Immediate

- Bloccare l'hash SHA256 nel sistema EDR
- Inserire il nome file nelle watchlist
- Monitorare la creazione di processi figli da eseguibili non affidabili
- Analizzare log proxy per eventuali connessioni verso indirizzi anomali

10.2 Regole di Rilevamento Consigliate

Implementare rilevazioni per:

- Invocazioni di `cmd.exe` da processi non di sistema
- Esecuzioni di `timeout.exe` post lancio sospetto
- Drop di eseguibili in directory scrivibili dall'utente

10.3 Query di Hunting (EDR/SIEM)

```
EventID=4688 AND ParentImage!=C:\Windows\System32\*
AND NewProcessName=cmd.exe
```

```
ProcessName=timeout.exe AND ParentProcess!=explorer.exe
```

11 Conclusioni

L'analisi condotta in ambiente sandbox conferma che il file **Jvczfhe.exe** presenta caratteristiche altamente sospette e comportamenti tipici di malware modulare, con capacità di:

- Eseguire comandi di shell tramite `cmd.exe`, indicando possibilità di esecuzione di script arbitrari e operazioni a basso livello sul sistema.
- Droppare componenti secondari (`Muadnrd.exe`) in percorsi utente, segnalando architettura modulare e potenziale caricamento di payload aggiuntivi.
- Tentare comunicazioni di rete verso host esterni, comprese query DNS e richieste HTTP, compatibili con beaconing e tentativi di instaurare canali di comando e controllo (C2).
- Eludere tecniche di analisi automatizzata, come ritardi controllati (`timeout.exe`) e verifiche delle impostazioni di sicurezza locali.
- Effettuare ricognizione del file system e del registro di sistema, raccogliendo informazioni sull'ambiente operativo e su configurazioni di sicurezza.

Valutazione SOC approfondita:

- Il comportamento osservato indica che **Jvczfhe.exe** può agire come loader iniziale o dropper modulare, con alto potenziale di persistenza e diffusione all'interno di una rete compromessa.
- L'interazione con directory utente e file temporanei può rappresentare una fase preparatoria per esfiltrazione di dati o compromissione di account locali.
- Le attività di rete, sebbene non confermate come C2 attivo, suggeriscono preparazione a contatti esterni e possibili fasi successive di download di strumenti o dati sensibili.
- L'elusione di sandbox e la catena di processi sospetti indicano un tentativo di rendere difficoltosa l'analisi automatizzata, comportamento tipico di malware avanzati.

Impatto potenziale:

- **Compromissione del sistema locale:** esecuzione di comandi arbitrari e drop di file secondari possono permettere modifiche non autorizzate a file di sistema e applicazioni legittime.
- **Rischio di diffusione laterale:** se eseguito in un ambiente di rete, il malware potrebbe utilizzare credenziali o percorsi di rete per diffondersi ad altri host.
- **Preparazione a fasi avanzate:** la raccolta di informazioni di sistema e la comunicazione di rete suggeriscono che il malware potrebbe scaricare ulteriori payload o strumenti di esfiltrazione.
- **Riduzione della capacità di rilevamento:** le tecniche di elusione sandbox e i processi figlio mascherati complicano il rilevamento da parte di antivirus e sistemi di sicurezza.

Raccomandazioni strategiche e operative:

- Bloccare l'esecuzione del file **Jvczfhe.exe** su tutti i sistemi tramite hash noto e regole EDR/AV.
- Monitorare e allertare su creazione di processi figlio non autorizzati, drop di file in percorsi utente e directory temporanee.
- Implementare regole SIEM per rilevare tentativi di comunicazione verso domini o IP sconosciuti.
- Eseguire scansioni di rete e controlli di integrità dei file critici per rilevare eventuali compromissioni secondarie.
- Preparare piani di containment per isolare rapidamente macchine compromesse e limitare la diffusione laterale.
- Aggiornare procedure interne di awareness per gli utenti, prevenendo esecuzione di eseguibili sospetti.

Considerazioni finali: L'analisi suggerisce che **Jvczfhe.exe** rappresenta una minaccia concreta, con alto potenziale di compromissione se eseguito in un ambiente reale e non isolato.

Il comportamento modulare, le capacità di elusione, la raccolta informazioni e le comunicazioni di rete indicano che il file è parte di una strategia di malware avanzato in fase di staging.

L'adozione tempestiva di misure preventive, monitoraggio continuo e procedure di rilevamento avanzato è fondamentale per mitigare il rischio e prevenire impatti operativi e compromissioni dati.