RELAZIONE SULL'ANALISI DI ATTIVITA' SOSPETTE TRAMITE ANY.RUN

Introduzione

Questa relazione tecnica è il risultato dell'analisi effettuata in data **25/08/2024 alle ore 22:38:59** tramite la piattaforma **ANY.RUN**, su un sistema operativo **Windows 10 Pro**.
L'obiettivo dell'analisi è stato l'esame comportamentale di due file eseguibili sospetti: `Jvczfhe.exe` e `Muadnrd.exe`.

Nonostante l'assenza di segnali inequivocabilmente classificabili come *malevoli*, l'analisi ha rivelato numerose attività sospette, che giustificano un approfondimento per determinare il reale impatto sulla sicurezza del sistema e l'eventuale compromissione.

Svolgimento

1. Dati tecnici del file sospetto

- **Tipo di minaccia**: **Attiva (potenzialmente dannosa)**
- **File analizzati**: `Jvczfhe.exe`, `Muadnrd.exe`
- **Sistema operativo**: **Windows 10 Pro**

Hash identificativi:

- **MD5**: `00B5E91B42712471CDFBDB37B715670C`
- **SHA1**: `D9550361E5205DB1D2DF9D02CC7E30503B8EC3A2`
- **SHA256**: `0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3F0`

2. Operazioni rilevate dei file sospetti `.exe`

I due file `Jvczfhe.exe` e `Muadnrd.exe` risultano coinvolti in una serie di operazioni sospette, che mostrano comportamenti potenzialmente dannosi o di tipo evasivo. Le attività svolte da questi eseguibili includono:

- **Avvio del prompt dei comandi (`cmd.exe`)** per eseguire comandi di sistema.
- **Utilizzo di `timeout.exe`** per ritardare l'esecuzione e aggirare analisi comportamentali.
- **Controllo delle impostazioni di sicurezza di Windows e Internet Explorer** per identificare eventuali barriere o vulnerabilità.
- **Connessioni a porte non standard**, potenzialmente per comunicazioni con server remoti non autorizzati.
- **Verifica delle impostazioni di trust** per valutare privilegi utente o presenza di certificati attendibili.
- **Lettura di variabili ambientali, nome macchina e GUID del sistema** per ottenere fingerprint univoci dell'host.
- **Disabilitazione dei log di tracciamento**, comportamento tipico per nascondere le proprie attività.
- **Crash intenzionali e autolanciamento**, potenziali indicatori di tentativi di persistenza o di sfruttamento.

Queste operazioni mostrano un livello di complessità e intenzionalità tale da richiedere una valutazione approfondita, pur non essendo esplicitamente etichettate come "malevole".

---

3. Attività comportamentali rilevate

L'analisi è stata suddivisa in due sezioni principali:

Sezione "SUSPICIOUS" – Comportamenti sospetti

Attività che, pur non essendo malevoli in senso stretto, possono suggerire comportamenti anomali:

- **Esecuzione di `cmd.exe` da file non noti** (`Jvczfhe.exe`, `Muadnrle.exe`)
  → Potenziale tentativo di eseguire comandi arbitrari senza interazione diretta dell'utente.

- **Utilizzo di `timeout.exe` per ritardare l’esecuzione**
  → Tecnica comune per aggirare i controlli automatici o simulare un comportamento umano.

- **Connessione a porte non standard** da parte di `InstallUtil.exe` e `Muadnrle.exe`
  → Potenziale attività di *command and control* o comunicazione cifrata non convenzionale.

- **Avvio autonomo dei processi** (`Muadnrle.exe`)
  → Indicatore che il file potrebbe cercare di mantenere la persistenza nel sistema.

- **Verifica delle impostazioni di trust e sicurezza di Windows**
  → Spesso utilizzata da malware per valutare la possibilità di operare in modalità elevata.

- **Crash volontari di applicazioni**
  → Potenziale tentativo di sfruttamento di vulnerabilità tramite *buffer overflow* o comportamenti anomali forzati.

Sezione "INFO" – Attività informative rilevate

Attività che non sono direttamente sospette, ma che aiutano a comprendere il comportamento dei file:

- **Accesso a chiavi di registro di Office e impostazioni proxy**
  → Potrebbe indicare un tentativo di raccogliere dati sull'ambiente utente o di manipolare il traffico.

- **Lettura del nome macchina, GUID e variabili d’ambiente**
  → Attività ricorrente nei malware per la profilazione del sistema compromesso.

- **Disabilitazione dei log di traccia**
  → Tecnica usata per ostacolare eventuali indagini post-infezione.

- **Uso di protezione con `.NET Reactor`**
  → Meccanismo di offuscamento e protezione anti-reverse engineering, tipico di tool dannosi.

Conclusione

Sebbene l’analisi **non abbia etichettato esplicitamente alcuna attività come "MALICIOUS"**, il comportamento dei file analizzati è **fortemente sospetto** e compatibile con tecniche comunemente utilizzate da malware avanzati per eludere il rilevamento, ottenere informazioni di sistema, ed eseguire codice arbitrario.

Elementi critici osservati:

- Avvio autonomo e interazione con `cmd.exe` da file sconosciuti
- Comunicazione tramite porte non standard
- Tentativi di raccolta informazioni sul sistema e disabilitazione dei log
- Presenza di protezione software `.NET Reactor` – che ostacola le indagini

---

Raccomandazioni operative

1. **Isolare il sistema analizzato** per evitare eventuali diffusioni laterali.
2. **Eseguire una scansione completa** con antivirus avanzati e strumenti EDR.
3. **Raccogliere ed esaminare i file rilasciati da Firefox e i comandi eseguiti da `cmd.exe`**.
4. **Monitorare le porte di rete non convenzionali** coinvolte nell’analisi.
5. **Verificare la provenienza dei file sospetti (`Jvczfhe.exe`, `Muadnrle.exe`)** e bloccarli su tutta l'infrastruttura, se non riconosciuti.
6. **Conservare i log e creare una timeline degli eventi** per ulteriori indagini forensi.