Report di Analisi della Minaccia: `Jvczfhe.exe`

Michele Storelli

June 13, 2025

Questo report presenta un'analisi dettagliata delle attività malevole associate al file `Jvczfhe.exe`, come osservato in un'analisi sandbox su Any.run. Vengono evidenziate le tecniche di persistenza, le comunicazioni di rete e le tattiche di evasione impiegate dal malware.

1 Informazioni Generali sull'Analisi

L'analisi è stata condotta sulla piattaforma Any.run in data **25 Agosto 2024 alle 22:38:59** su un sistema **Windows 10 Professional (64 bit)**.

- **URL del file analizzato:** https://github.com/MELITERRER/frew/blob/main/Jvczfhe.exe
- **Verdetto:** Attività malevola
- **Hash SHA256:** `0307EE805DF8B94733598D5C3D62B28678EAEADBF1CA3689FA678A3780DD3DF0`
- **Tag associati:** `github`, `netreactor`

2 Attività Sospette e Minacce Identificate

L'analisi del comportamento del malware ha rivelato diverse attività malevole e indicatori di compromissione.

2.1 Creazione ed Esecuzione di File

Il malware manifesta la sua presenza creando ed eseguendo file nella directory temporanea dell'utente.

- Creazione ed esecuzione di `Jvczfhe.exe` in `C:`
  `Users`
  `admin`
  `AppData`
  `Local`
  `Temp`
  .
- Rilevata l'esecuzione di `123.bat` e `723.exe`.

2.2 Persistenza sul Sistema

Per assicurare la sua esecuzione ad ogni riavvio o accesso utente, il malware modifica il registro di sistema.

- Creazione della chiave di registro: `HKCU`
  `SOFTWARE`
  `Microsoft`
  `Windows`
  `CurrentVersion`
  `Run`
  `j`
- Valore associato: `C:`
  `Users`
  `admin`
  `AppData`
  `Local`
  `Temp`
  `j.exe`

Questo meccanismo garantisce che il malware si avvii automaticamente con la sessione utente.

2.3 Comunicazione di Rete (Comando e Controllo - C2)

Il malware tenta attivamente di comunicare con server esterni, probabilmente per ricevere istruzioni o esfiltrare dati.

- **Dominio sospetto:** `egehgdehjbhjtre.duckdns.org` (Indirizzo IP: `91.92.253.47`)
- Tentativi di connessione a diverse porte, inclusa la `443` (HTTPS), per camuffare il traffico malevolo.

La presenza di un dominio DuckDNS è un indicatore comune di infrastrutture C2 malevole, a causa della loro facilità di gestione e aggiornamento dinamico degli IP.

2.4 Tecniche di Evasione e Offuscamento

Il malware impiega tecniche avanzate per sfuggire al rilevamento e all'analisi.

- **Process Injection (NTDLL) / Process Hollowing (Native API):** Queste tecniche permettono al malware di iniettare codice in processi legittimi o di sostituire il codice di un processo legittimo con il proprio, rendendo più difficile l'identificazione della sua origine e attività.
- **Uso di NetReactor:** Il tag `netreactor` indica che il malware è stato offuscato utilizzando questo packer, rendendo l'analisi statica del codice più complessa.

- **Anti-analisi/Anti-debug:** Chiamate API come `NtGetContextThread` e `NtSetInformationThread` suggeriscono tentativi di rilevare o interferire con ambienti di debugging o sandbox.

2.5 Raccolta di Informazioni

Il malware tenta di raccogliere informazioni sul sistema operativo, come evidenziato dalla chiamata API `GetVersionExW`. Questa attività è spesso un precursore per la raccolta di dati più sensibili o per l'adattamento del comportamento malevolo all'ambiente specifico.

3 Conclusioni e Raccomandazioni

Il file `Jvczfhe.exe` è classificato come malware con un comportamento che mira alla persistenza, alla comunicazione con server di Comando e Controllo e all'evasione dei sistemi di sicurezza. Si tratta probabilmente di un trojan o di un loader, capace di scaricare payload aggiuntivi o di fornire accesso remoto ai malintenzionati.

3.1 Raccomandazioni per la Mitigazione

Per mitigare la minaccia e prevenire ulteriori compromissioni, si raccomanda di:

1. **Isolare il sistema:** Scollegare immediatamente il sistema compromesso dalla rete.
2. **Bloccare indicatori di compromissione (IoC):** Bloccare l'accesso al dominio `egehgdehjbhjtre.duckdns.org` e all'indirizzo IP `91.92.253.47` a livello di firewall, proxy o DNS.
3. **Scansione e Bonifica:** Eseguire una scansione approfondita del sistema con software antivirus e antimalware aggiornati.
4. **Ripristino:** Se possibile, ripristinare il sistema da un backup pulito per garantire la rimozione completa di tutte le infezioni e modifiche malevole.
5. **Analisi Forense:** Condurre un'analisi forense dettagliata per comprendere l'estensione della compromissione e identificare eventuali altri IoC.