Observe Behavior Indicators

Malware Hash Analyzed (SHA-256)

`4218214f32f946a02b7a7bebe3059af3dd87bcd130c0469aeb21b58299e2ef9a`

Tool Used

VirusTotal (Static + Dynamic Sandbox Analysis)

Observed Behavior Indicators (From VirusTotal Report)

The behavior indicators were identified from the **Behavior**, **Relations**, **Graph Summary**, and **MITRE ATT&CK** sections.

---

1. High Malicious Detection

- **61 out of 70 security vendors** flagged the file as malicious.
- Community score is **negative**, indicating high threat confidence.
- Multiple sandboxes classified it as:
  - **Ransomware**
  - **Trojan**
  - **Stealer**
  - **Phishing**
  - **Evader**

📌 *This confirms the file is highly dangerous.*

---

2. File Type & Execution Behavior

- File type: **Win32 DLL (PE32 executable)**
- Designed to run as a **Dynamic Link Library**, often used for:
  - Process injection
  - Stealthy execution inside legitimate processes

Behavior Tags Observed:

- `runtime-modules`

- `overlay`
- `signed`
- `checks-user-input`

📌 *DLL malware is commonly used to hide malicious code execution.*

---

3. Dropped Files (Payload Activity)

- Malware dropped **multiple files (10+ files)** after execution.
- Dropped file types include:
  - `.exe`
  - `.doc`
  - `.js`
  - `.bmp`
  - `.text`
  - `.zlib`

📌 *Dropping additional files indicates payload delivery and secondary infection.*

---

4. Persistence Mechanisms

From **MITRE ATT&CK – Persistence**:

- **Boot or Logon Autostart Execution (T1547)**
- **Hijack Execution Flow (T1574)**

📌 *This ensures the malware runs automatically after reboot.*

---

5. Defense Evasion Techniques

Observed **multiple evasion behaviors**, including:

- **Detect Debug Environment**
- **Obfuscated Files or Information (T1027)**
- **Masquerading (T1036)**
- **Hide Artifacts (T1564)**
- **Long Sleeps (Anti-sandbox delay)**

📌 *These techniques help malware avoid detection by security tools.*

6. Process Injection & Privilege Abuse

From **Privilege Escalation & Execution**:

- **Process Injection (T1055)**
- **Shared Modules (T1129)**
- **Command & Scripting Interpreter (T1059)**
- **Windows Management Instrumentation – WMI (T1047)**

📌 *Indicates advanced malicious control over system processes.*

---

7. Network Communication (C2 Activity)

The malware contacted:

Domains (4)

- `arc.msn.com`
- `ocsp.sectigo.com`
- `crl.sectigo.com`
- `msftstore.s.llnwi.net`

IP Addresses (3)

- IPs located in **China, USA, and Ireland**

📌 *Network communication suggests Command & Control (C2) behavior.*

---

8. Data Collection & Impact

From **MITRE ATT&CK**:

- **Data from Local System (T1005)**
- **Input Capture (T1056)**
- **System & Network Discovery**
- **Data Encrypted for Impact (T1486)**

📌 *Confirms ransomware-style encryption and data theft.*

Graph Summary Interpretation

- 7 bundled files
- 10+ dropped files
- 3 contacted IPs
- 4 contacted domains
- 2 execution parents

📌 *Shows multi-stage malware behavior.*

The observed behavior indicators clearly show that the analyzed file is a **high-risk multi-functional malware** exhibiting characteristics of **Trojan, Ransomware, Stealer, and Defense-Evasion malware**. The malware performs file dropping, process injection, persistence, data encryption, network communication, and sandbox evasion, confirming its malicious nature.