Malware Analysis – Proof of Concept Document

Name:Kirti Koltharkar Inter ID:246

POC: Static & Dynamic Analysis of Malware Sample W32.HfsAdware.5066

1.Objective

The purpose of this POC is to analyze the provided malware sample (W32.HfsAdware.5066) to understand its behavior, indicators of compromise (IOCs), and potential impact. The goal is to demonstrate the process of malware analysis for educational and security awareness purposes.

1.Tools Used

- Static Analysis:

- PEiD – Identify packers and compilers

- PEStudio – Analyze PE file structure and suspicious strings

- VirusTotal – Check file hash against known databases

- Strings Utility – Extract readable text from binary

- Dynamic Analysis:

- Cuckoo Sandbox – Automated malware behavior analysis

- Wireshark – Network traffic monitoring

- Process Monitor (Procmon) – File system and registry monitoring

- Regshot – Registry change comparison

2.Malware Sample Information

- Sample Name: W32.HfsAdware.5066

- Hash (MD5): 27c6adc401e509a9e76633df6d3ccb3e9

- Hash (SHA1): b3d60ed1cb65d522f32efc9e97f238

- File Type: Windows Executable (.exe)

- Category: Adware

- Delivery Method: Likely through bundled software downloads

2.Methodology

1.Static Analysis:

- Verified file hashes using sha256sum and checked against VirusTotal.

- Extracted ASCII and Unicode strings to identify suspicious domains, API calls, and registry paths.

- Inspected PE headers for anomalies, imports, and suspicious functions (e.g., URLDownloadToFileA, ShellExecuteA).

2.Dynamic Analysis:

- Executed malware in an isolated Windows VM (no internet access).

- Captured file system modifications, new files, and altered registry keys.

- Monitored network traffic for suspicious outbound connections or C2 server communication.

3.Findings

- Static Observations:

- Embedded suspicious URLs pointing to ad servers.

- API imports linked to persistence and browser injection.

Signs of UPX packing, suggesting obfuscation.

- Dynamic Observations:

-Created registry entries under

- Dropped additional executable files in %AppData%\Local\Temp.

- Generated outbound HTTP requests to suspicious domains for fetching ad content.

- Modified browser settings to inject advertisements.

4.Indicators of Compromise (IOCs)

- File Hash: 27c6adc401e509a9e76633df6d3ccb3e9

- Registry Keys Modified:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Updater

- Dropped Files:

- %AppData%\Local\Temp\adupdate.exe

- Suspicious Domains:

- ads-track-server[.]com

- clickredir[.]net

5.Mitigation

- Block listed domains in firewall and DNS filters.

- Remove persistence registry entries.

- Quarantine and delete dropped files.

- Deploy endpoint protection to detect similar adware variants.

- Educate users to avoid downloading software from untrusted sources.

Signs of UPX packing, suggesting obfuscation.

- Dynamic Observations:

- Created registry entries under HKCU\Software\Microsoft\Windows\CurrentVersion\Run for persistence.

- Dropped additional executable files in %AppData%\Local\Temp.

- Generated outbound HTTP requests to suspicious domains for fetching ad content.

- Modified browser settings to inject advertisements.

2. Indicators of Compromise (IOCs)

- File Hash: 27c6adc401e509a9e76633df6d3ccb3e9

- Registry Keys Modified:

- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Updater

- Dropped Files:

- %AppData%\Local\Temp\adupdate.exe

- Suspicious Domains:

- ads-track-server[.]com

- clickredir[.]net

5.Mitigation

- Block listed domains in firewall and DNS filters.

- Remove persistence registry entries.

- Quarantine and delete dropped files.

- Deploy endpoint protection to detect similar adware variants.

- Educate users to avoid downloading software from untrusted sources.