Malware Analysis Report

Malware Name: W32.PiretosLTR.Trojan

SHA-256 Hash:
3d653771933422f9a081ea122865da76edde83cdeb41b8b8e377833e75e21aca

Category: Trojan

Analysis Type: Static + Dynamic

Tools Used: Wireshark, Process Explorer, ProcMon, PEStudio, Any.Run (simulation)

1. Incident Response Interview Questions

Assume the malware was identified on a user's machine showing unusual network activity and performance degradation.

Key questions asked:

- When did the issue start?

- Any suspicious email or file downloaded?

- Was antivirus triggered? If yes, which file was detected?

2. Log Analysis

Examined logs from:

- Windows Event Viewer (Application and System Logs)

- Firewall logs

- Antivirus quarantine logs

Finding: Logs showed suspicious execution from `%TEMP%\svchost.exe` with elevated privileges.

3. Key Areas Investigated

- Auto-start entries (registry, scheduled tasks)

- Unknown processes and services

- Suspicious network connections

4. Network Traffic Inspection (Wireshark)

Tool Used: Wireshark

Captured malicious HTTP POST requests to an external command & control server.

Indicators:

- Unusual outbound connections to IP: 185.193.125.33

- Traffic on non-standard ports

5. Static Analysis

Tool Used: PEStudio

- File contains suspicious sections (.text, .rdata, .reloc)

- Packed using UPX (common in malware obfuscation)

- Detected API calls: LoadLibraryA, GetProcAddress, InternetOpen, etc.

- No digital signature present

6. Dynamic Analysis

Tool Used: Process Explorer, ProcMon

- Malware dropped a secondary payload in `%APPDATA%\Roaming\subdir`

- Created persistence via `HKCU\Software\Microsoft\Windows\CurrentVersion\Run`

- Created unusual file: `C:\Users\user\AppData\Roaming\syslog.dat`

- Connected to remote host repeatedly every 20 seconds

7. Conclusion

W32.PiretosLTR.Trojan is a downloader trojan that connects to a C2 server and may exfiltrate information or download further payloads. It uses registry persistence, process injection, and network beacons to remain active. Immediate containment and remediation are required.