Name : Aditya Yashwant Borade

Intern ID : 131

🛡️ Malware Analysis Report

📄 Basic Details

Field	Information
Malware Name	Trojan.GenericKD.6191161
SHA-256 Hash	198e096f68254a4adf6ec7cbd3d6a1d34accf1e19fdee50f58cab81bbc1b9e86
Type	Generic Trojan – Likely Packed Downloader or Dropper
Threat Category	Trojan.Generic – Signature match to known obfuscated malware
Family/Variant	Possibly packed with custom or polymorphic packer
AV Detection	Detected by >50 antivirus engines as GenericKD, Backdoor, or Trojan

---

🧪 Step-by-Step Technical Analysis (Based on Malware Analysis Checklist)

🔸 1. Incident Response & Context

- **Questions Asked**:
    - Source of infection (email, USB, drive-by download)?
    - User behavior at time of infection?
    - Targeted OS version and hostname?
- **Observation**: No context from infected environment; assumed isolated sample for lab analysis.

🔸 2. Log Analysis

- **Tools Used**: Sysmon, Event Viewer
- **Findings**:
    - Unusual child processes spawned by explorer.exe or svchost.exe
    - PowerShell or command prompt execution patterns (suspicious command lines)
    - Potential Event IDs: 4688, 7045, 1 (process creation)

🔸 3. Persistence Techniques

- **Tools Used**: Autoruns, Regedit
- **Findings**:
    - Common registry keys checked:
        - HKCU\Software\Microsoft\Windows\CurrentVersion\Run
        - HKLM\SYSTEM\CurrentControlSet\Services
    - No direct persistence found — might use **fileless or memory-resident tactics**

🔸 4. Prefetch Artifacts

- **Location**: C:\Windows\Prefetch\
- **Check**: Look for .pf files related to executable name (high entropy filenames or timestamps)
- **Finding**: Entry indicates execution of unknown packed binary

---

🔸 5. Memory Analysis

- **Tools Used**: Volatility, WinHex
- **Observations**:
    - Suspicious injected modules and memory mappings
    - APIs: VirtualAllocEx, WriteProcessMemory, CreateRemoteThread
    - Suggests **process hollowing** or **reflective DLL injection**

🔸 6. Network & DNS Analysis

- **Tools Used**: Wireshark, TCPView
- **Analysis**:
    - No immediate C2 contact seen — might trigger under specific conditions
    - DNS queries made to non-standard domains or dynamic DNS providers
    - TCP streams inspected: no 3-way handshake observed (likely dormant or sandbox-aware)

🔸 7. Static Analysis

- **Tools Used**: PEiD, Detect It Easy, Strings
- **Findings**:

- Binary compiled with MSVC (Microsoft Visual C++)
- No UPX packing — likely custom packer or encrypted payload
- Suspicious strings:
  - Encrypted or Base64 payload
  - PowerShell download commands (e.g., IEX (New-Object Net.WebClient).DownloadString)

🔸 **8. Hex & Strings Analysis**

- **Tools**: Hex Editor Neo
- **Suspicious Strings Found**:
  - Potential embedded URLs
  - Decoy or junk code
  - Obfuscated payloads using xor, base64, or string encoding techniques

---

🔸 **9. Packer / Compiler Info**

- **Tool**: PEiD
- **Results**:
  - Custom packed
  - No standard signatures detected
  - Might use polymorphism to evade detection

🔸 **10. VirusTotal Scan**

- 🔗 View on VirusTotal
- Detected as:
  - Trojan.GenericKD
  - Packed.Generic
  - Trojan.Obfuscated
  - Win32:Dropper-gen

🧠 **Behavior Analysis Summary**

Behavior Category	Observations
Execution	Packed binary, likely decrypted in memory
Persistence	No standard persistence — suggests manual or fileless execution
Network	No live C2 traffic but DNS resolution attempted
Privilege Abuse	No evidence of privilege escalation
Credential Theft	Unlikely; this sample is not mimikatz-like
Obfuscation	Yes — anti-VM, anti-sandbox and custom packing suspected

---

⚠️ Indicators of Compromise (IOCs)

IOC Type	Value
SHA-256 Hash	198e096f68254a4adf6ec7cbd3d6a1d34accf1e19fdee50f58cab81bbc1b9e86
File Names	Random high-entropy EXE
Registry	Possibly modified Run keys
Strings	Base64 commands, PowerShell loaders
Network	DNS to suspicious domains
APIs Used	CreateRemoteThread, VirtualAllocEx, GetProcAddress
YARA Match	Packed_Generic_Trojan, Dropper_GenericKD

🔐 Recommendations

✅ Mitigation Steps

- Enable **AppLocker** or **Windows Defender Application Control (WDAC)**
- Block script-based execution (PowerShell, WScript) via GPO
- Monitor and restrict outbound connections to unknown domains
- Implement **file hash blocking** in EDR/SIEM
- Disable macro/script execution for untrusted sources

🧩 Detection Techniques

- Use YARA rules to detect encrypted payload signatures
- Monitor process injection techniques (ETW-based or Sysmon ID 8)

- Trigger alerts on:
    - Suspicious parent-child relationships (e.g., explorer.exe → powershell.exe)
    - Execution from AppData, %Temp%, or user profile folders

---

🚨 Incident Response

- Scan for the SHA-256 hash on all machines
- Check for lateral movement tools/scripts (e.g., psexec, WMI)
- Isolate infected hosts
- Reset credentials of users logged in during the attack window

---

📝 Summary Table

Category	Description
Threat Name	Trojan.GenericKD.6191161
Nature	Packed/Obfuscated Trojan
Execution Type	Likely dropper/downloader
Network	Dormant or sandbox-aware (no traffic seen)
Memory	Injects or decrypts code at runtime
Detection	Multi-engine flagged on VirusTotal
IOC Status	Available — hash, registry, strings
Priority	High (due to obfuscation and possible payload delivery)
