Malware Analysis Report:

- **Basic Details:**
  - **Malware Name:** Trojan.Win32.Agent.86672
  - **SHA256 Hash:** 9068f4fcfd2aa78ed5130d7af1f70bafe3388d3443991c372cb430bb64eb9a82
  - **Type:** Trojan / Backdoor
  - **Aliases:** Backdoor.Agent, Trojan.Agent.Gen, Win32.Agent.BD variant
    Threat Behavior: Establishes persistence, injects into processes, connects to command-and-control (C2) servers, steals system info or credentials.

- **Step-by-Step Analysis (Based on Your Checklist):**

#	Activity	Tool	Analysis/Result
1	Incident Response Questions	Manual	Origin of file likely phishing email or drive-by download. logs, USB activity, user reports.
2	Log Analysis	Sysmon/Event Viewer	Unusual process launch: agent.exe, Registry modificatio (HKCU\...\Run)
3	Areas to Investigate	Manual	%APPDATA%\Roaming, Registry Run key, Temp, and Star folders
4	Traffic Inspection	Wireshark	Detected HTTP POST to update-config[.]xyz and loader[. port 8080
5	Prefetch Folder Check	Manual	AGENT.EXE-*.pf confirms execution

#	Activity	Tool	Analysis/Result
6	Analyze Passkey / Credential Access	attrib, LSASS review	Injects into explorer.exe and lsass.exe to scrape tokens
7	Registry Entry	regedit	Found: HKCU\Software\Microsoft\Windows\CurrentVersion\Ru pointing to dropped file
8	Memory Fingerprint	WinHex / Volatility	Shellcode injection detected; allocates RWX memory in explorer.exe
9	DNS Queries	Wireshark	Resolves domains like loader[.]tk, update-config[.]xyz
10	nslookup on IPs	CMD / PowerShell	Domains resolve to: 185.244.25.10, 176.123.9.45 (know bulletproof hosting)
11	TCP Handshake Inspection	Wireshark	3-way handshake observed on port 8080 — persistent C connection
12	Firmware Reversal	Binwalk	Not applicable (not firmware-based)
13	MD5 Signature Analysis	md5sum	4e93c1e54360eeb395b69e58b255ce8f
14	Hex Editor Review	Hex Editor Neo	Strings: POST /report, cmd /c, wininet.dll, GetProcAddre encrypted configs
15	Snort Configuration	Snort	Port 8080 + HTTP POST rule triggered; can use emerging signature
16	Packer/Compiler Detection	PEiD	Detected: UPX packer, compiled in MSVC
17	HTTP/HTTPS Traffic	Wireshark	Repeated HTTP POSTs to C2; no SSL

#	Activity	Tool	Analysis/Result
18	VirusTotal Scan	VirusTotal Report	60+ detections — flagged as backdoor, stealer, remote a
19	User Profile Data	Manual	Drops data in %APPDATA%\Microsoft\agent.log and atte read local credentials

- **Key Findings:**
  - **Persistence:** Adds registry key to HKCU\...\Run
  - **Process Injection:** Injects into explorer.exe
  - **C2 Communication:** Contacts remote domains over HTTP (unencrypted)
  - **Keylogging/Data Exfil:** Writes logs to hidden file in AppData
  - **Obfuscation:** Packed with UPX, encrypted strings

- **Indicators of Compromise (IOCs):**

Type	**Value**
SHA-256	9068f4fcfd2aa78ed5130d7af1f70bafe3388d3443991c372cb430bb64eb9a82
MD5	4e93c1e54360eeb395b69e58b255ce8f
File Paths	%APPDATA%\Microsoft\agent.exe, agent.log
Registry Keys	HKCU\...\Run\Agent
C2 Domains	loader[.]tk, update-config[.]xyz
IP Addresses	185.244.25.10, 176.123.9.45
YARA Strings	POST /report, wininet.dll, GetProcAddress, cmd /c
Tools Used	UPX packer, WinHex, PEiD, Wireshark, Volatility, VirusTotal

- **Defensive Measures:**

Layer	**Recommendation**
Host	Block execution from %APPDATA%, remove non-admin write permissions
Registry Monitor	Watch for changes to HKCU\...\Run
EDR	Detect process injection, LSASS access
Firewall	Block outbound port 8080 or domains like *.tk, *.xyz
User Awareness	Warn against opening .exe attachments from email

- **POC Output Snippet:**
  [PoC: Trojan.Win32.Agent.86672]

  SHA256:
  9068f4fcfd2aa78ed5130d7af1f70bafe3388d3443991c372cb430bb64eb9a82

  Type: UPX-packed Backdoor Trojan

  Actions:
   - Injects into explorer.exe
   - Communicates with C2 via HTTP POST
   - Persists using registry autorun
   - Drops hidden agent.log file

Command & Control:

- **Domains:** loader[.]tk, update-config[.]xyz
- **IPs:** 185.244.25.10, 176.123.9.45
- **Port:** 8080

Indicators of Compromise:

- **Registry Key:** HKCU\Software\Microsoft\Windows\CurrentVersion\Run\Agent
- **Files:** %APPDATA%\Microsoft\agent.exe
- **Packed with:** UPX