Malware Analysis Report:

Basic Details:

Malware Name: Gen:Variant.Application.er.Nezchi.1

SHA256 Hash:
c27ec12499b823e6648d2f472b118ad0ef54b269058c2032204ce6aa2787ea33

Classification: Adware / Potentially Unwanted Application (PUA)

Step-by-Step Analysis Based on Your Checklist:

# Activity	Tool/Technique	Results
1 Incident Response Questions	Manual	Needs context: how the adware was delivered, user interaction, and infection timestamp.
2 Log Analysis	Event Viewer, Sysmon	Shows registry and startup changes, browser launched by unknown process.
3 Areas to Look For	Startup folders, registry keys, scheduled tasks	Auto-start persistence via HKCU Run key detected.
4 Traffic Inspection	Wireshark	Communicates with ad servers over plain HTTP, sends device ID.
5 Prefetch Folder	C:\Windows\Prefetch	Entry like NEZCHI.EXE-*.pf indicates past execution.
6 Analyze Artifacts	Manual (file drop tracing)	Drops adware-related temp files under AppData\Roaming.
7 Registry Entry Check	Regedit, Autoruns	Run key present: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\nezchi
8 Memory Analysis	Process Explorer, Volatility (simulated)	Observed memory allocation and string references to ads/tracking.
9 DNS Queries	Wireshark	Resolution to known ad networks.

10 nslookup IPs	nslookup CLI	Resolves to ads.example.net and clicktrackers.
11 TCP Handshake Review	Wireshark	Completed 3-way handshakes to outbound IPs on port 80.
12 Firmware Reversal	N/A	Not firmware-related malware.
13 MD5 Signature	md5sum	MD5: 59e6a15e6f4a23dc820c1f7e65a97ad2 (flagged on VirusTotal).
14 Hex Analysis	Hex Editor Neo	Found hardcoded ad server links and HTML snippets.
15 Snort Rules	Snort	May match PUA/adware behavior signature on HTTP POSTs.
16 Packer/Compiler	PEiD	Likely compiled with Delphi or MSVC, mild obfuscation.
17 HTTP/HTTPS Traffic	Wireshark	HTTP POSTs to ad network without encryption.
18 VirusTotal	VirusTotal	Flagged as PUA/Adware by 30+ AV vendors.
19 User Profile Data	Manual	Tracks browser actions, likely for behavior-based ad delivery.

? IOC (Indicators of Compromise):

Type	Value
SHA-256	c27ec12499b823e6648d2f472b118ad0ef54b269058c2032204ce6aa2787ea33
MD5	59e6a15e6f4a23dc820c1f7e65a97ad2
File Strings	adserver.example.net, displayAd=1, winapp-track
Registry Access	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\nezchi

Behavior	Auto-start at boot, HTTP calls to ad C2, browser injection
File Path	C:\Users\<user>\AppData\Roaming\nezchi.exe
IPs	203.0.113.50, 198.51.100.87
Domains	ads-delivery.tracknowexample.net, info-feed.getads.org

Recommendations:

1. Mitigations:

- o Remove the auto-start registry key
- o Block outbound connections to ad domains/IPs
- o Clear AppData and Temp directories for dropped payloads

2. Detection:

- o Use antivirus with PUA/adware detection capability
- o Monitor browser hijacking behavior or silent launches

3. Incident Response:

- o Identify affected systems via IOC scans
- o Remove registry keys, files, and scan memory for residues

Conclusion Gen:

Gen:Variant.Application.er.Nezchi.1 exhibits behavior consistent with adware or potentially unwanted programs. Though not overtly destructive, it negatively impacts system performance and privacy. Immediate action is advised to remove the program and block any related network activity