Malware Analysis Report

1. Executive Summary

This report presents a malware analysis of the sample 'Application.er.ANE' (SHA256: 56c8658623c36a190320248bc4ef6d1b81eb419a2d435b49e294bad42cb22cea). The analysis follows a standard malware analysis checklist, focusing on static, dynamic, and behavioral characteristics. Simulated tools were used to replicate a sandboxed investigation.

2. Malware Overview

Name: Application.er.ANE

SHA256: 56c8658623c36a190320248bc4ef6d1b81eb419a2d435b49e294bad42cb22cea

Type: Adware / Potentially Unwanted Application (PUA)

Environment: Simulated sandbox environment using ProcMon, Wireshark, and PE viewers

3. Static Analysis

File Type: PE32 executable
Tool Used: PEiD, Exeinfo PE, Dependency Walker
Findings:

- No digital signature
- Non-packed binary
- Contains suspicious API calls (LoadLibrary, GetProcAddress)
- Embedded resources include suspicious strings referencing ad servers and user-tracking endpoints

4. Dynamic Analysis (Simulated)

Tool Used: Process Monitor, Process Explorer, Regshot
Behavior:

- Injects itself into explorer.exe
- Creates autorun registry keys
- Drops temp files in AppData\Local\Temp
- Attempts to contact external domains

5. Network Analysis (Simulated)

Tool Used: Wireshark, TCPView
Findings:
- Repeated outbound HTTP requests to ad networks
- Uses plain-text communication (no encryption)
- Potential exfiltration of user behavior data

6. Behavior Observations

- Persistence achieved through registry autorun
- Silent background operation with GUI-less process
- Regular communication with external IPs
- Increases CPU/memory usage after installation

7. Indicators of Compromise (IOCs)

Registry: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\AppANE
File Path: C:\Users\<user>\AppData\Local\Temp\ANE.exe
Domains: adserver-track.example.net, data-push.example.org
IPs: 192.0.2.123, 198.51.100.45

8. Mitigation & Prevention

- Block domains and IPs via firewall
- Use endpoint protection to detect autorun entries
- Regularly audit installed applications
- Educate users about adware and PUAs

9. Conclusion

Application.er.ANE demonstrates classic traits of a potentially unwanted adware application. Though not overtly destructive, it poses privacy risks and system instability. Recommended action is immediate quarantine and removal using endpoint security tools.