Malware Analysis Report - Gen:Variant.Zusy.286543

Malware Analysis Report

==========

Malware Name: Gen:Variant.Zusy.286543

Hash (SHA-256): ef58e181ed97435e2b9795d4d15a65e7059e419da67e397c34721942c98e9365

1. Detection Overview

- "Gen:Variant.Zusy" is a heuristic detection name used by antivirus engines to identify a generic variant of the Zusy (Zeus) banking Trojan family.
- Often indicates malware with suspicious behavior patterns rather than signature matches.

2. Static Characteristics (Typical)

- Encrypted or packed payloads.
- API calls related to:
  - Network operations (winsock, InternetOpen)
  - Browser injection (DLL hooking)
  - Persistence (registry modifications)
- Embedded strings or encrypted configurations.

3. Dynamic Behavior (Expected)

- Network Communication: Opens socket connections to C2 servers.

- Credential Theft: Hooks into browser processes to steal data.

- Persistence: Creates autorun registry entries or scheduled tasks.

- Process Injection: Injects into legitimate processes to avoid detection.

4. Analysis Workflow (Suggested)

Static Analysis:

- Check for hashes, import tables, and embedded strings.

- Unpack if needed (e.g., UPX).

Dynamic Analysis:

- Use sandbox (ANY.RUN, Hybrid Analysis, Joe Sandbox).

- Monitor:

  - File and registry changes

  - Network traffic

  - Process behavior and injections

5. Cleanup and Mitigation

- Use antivirus tools like Malwarebytes, ESET, or Defender.

- Perform scans in Safe Mode.

- Remove persistence mechanisms manually.

- Change all passwords (especially banking and email).

- Consider OS reinstall if infection is severe.

6. Conclusion

Gen:Variant.Zusy.286543 is a heuristic Trojan detection resembling Zeus banking malware. It is capable of stealing sensitive information, establishing remote connections, and maintaining persistence. Behavioral and sandbox analysis are recommended for deeper inspection.

For more information, submit the hash to: VirusTotal, Hybrid Analysis, ANY.RUN.