Comprehensive Malware Analysis Report: Malware_U3_W2_L5.exe

Executive Summary

This detailed analysis report is prepared to provide insights into the characteristics, behavior, and impact of the malware known as `Malware_U3_W2_L5.exe`. The analysis was conducted using advanced static and dynamic techniques to determine the malware's capabilities and recommend strategic countermeasures. The tools used include CFF Explorer for initial assessments, IDA Pro for in-depth disassembly, and OllyDbg for observing runtime behavior.

1. Tools and Methodology

- CFF Explorer: Analyzed the executable's headers, sections, and dependencies.
- IDA Pro: Disassembled the malware to study its code structure and flow.
- OllyDbg: Performed runtime analysis to observe the malware's interactions with the system and its behavior under execution conditions.

2. File Overview

General File Information:

- File Name: Malware_U3_W2_L5.exe
- File Type: Portable Executable 32-bit
- Compiled With: Microsoft Visual C++ 6.0
- Size: 40 KB (40960 bytes)
- Checksums:
  - MD5: C0B543E18E81392F28D17FAFF3D454
  - SHA-1: BB6F01B1FEF7A49CFC83EC2303D1F4F92A671F3C

3. PE Structure Analysis

PE Sections Analysis:

- .text: Contains executable code, crucial for the malware’s operation.
- .rdata: Holds read-only data and import tables.

- .data: Stores initialized data used by the malware.

4. Import Analysis

The malware imports several critical APIs from system DLLs, which are crucial for its malicious operations. Key dependencies include Kernel32.dll for system manipulation and WinInet.dll for network communications.

5. Behavioral Analysis

During execution, the malware exhibits behaviors typical of advanced persistent threats (APTs), including stealth operations, data exfiltration, and command execution from remote servers.

Runtime Malicious Behaviors:

- Network Activity: Initiates connections to remote servers for command and control.
- File Manipulation: Modifies system files and registries to achieve persistence.
- Evasion Techniques: Employs anti-debugging techniques to thwart analysis efforts.

6. Disassembly Analysis

Detailed disassembly highlighted several key functions intended for spying, data theft, and maintaining unauthorized access. Code analysis indicates sophisticated encryption routines aimed at securing its communication with C&C servers.

7. Threat Classification and Impact

Based on the observed behaviors and capabilities, the malware is classified as a Trojan/Backdoor. It poses a high threat due to its capabilities to perform unauthorized actions, such as data theft, system monitoring, and downloading additional payloads.

Malware Capabilities:

- Remote Access: Allows attackers remote control over the infected system.
- Data Exfiltration: Can steal sensitive information and transmit it to attackers.

- Persistence: Maintains presence through system reboots via registry modifications.

- Evasion: Uses advanced techniques to avoid detection and analysis.

8. Recommendations

- Deploy Advanced Endpoint Protection: Implement solutions with heuristic and behavior-based detection capabilities.

- Enhance Network Defenses: Use firewalls and intrusion detection systems to monitor and control incoming and outgoing traffic.

- Conduct Regular Security Audits: Regularly review system and network security settings to identify and mitigate vulnerabilities.

- Educational Programs: Train employees on cybersecurity best practices and the importance of recognizing phishing attempts.

9. Conclusion

The analysis of `Malware_U3_W2_L5.exe` reveals a well-engineered piece of malware designed to infiltrate systems, exfiltrate data, and provide remote access to attackers. Mitigating its threat requires a combination of advanced technical defenses and user awareness strategies.