AL2026_05 "Zombie ZIP" Technique Lets Malware Evade Security Scanning Tools (March 13th, 2026)

Description

Security researchers have identified a new technique dubbed **"Zombie ZIP"** that allows attackers to hide malicious payloads inside specially crafted ZIP archives capable of bypassing many antivirus (AV) and endpoint detection and response (EDR) solutions.

The technique manipulates ZIP archive headers so that security tools incorrectly interpret the contents of the file during scanning. As a result, malicious payloads may remain undetected even though the archive appears benign to automated inspection tools.

Because compressed archive files are commonly used to distribute documents and software, the technique could be abused in phishing campaigns or malware delivery operations targeting organizations and individual users.

Attack Details

The "Zombie ZIP" technique exploits inconsistencies in how security tools interpret ZIP archive metadata compared with how attackers process the archive payload.

Key characteristics include:

- **Header manipulation:** Attackers modify the ZIP file header so that the compression method is reported as "stored" (uncompressed) while the data is actually compressed using the DEFLATE algorithm.
- **Security scanning evasion:** Many antivirus engines trust the ZIP header and scan the file as raw uncompressed data. Because the actual contents are compressed, scanners analyze meaningless compressed bytes and fail to detect malicious signatures.
- **High detection bypass rate:** Testing against VirusTotal reportedly showed the technique bypassing the vast majority of antivirus engines, with only one out of 51 engines detecting the malicious sample.
- **Extraction errors:** Standard archive utilities such as WinRAR, unzip, or 7-Zip may fail to extract the archive due to inconsistencies in metadata such as the CRC checksum value.
- **Custom loaders:** Attackers can create specialized loaders that ignore the misleading ZIP metadata and correctly decompress the payload, allowing the malware to be recovered and executed.

The issue has been assigned **CVE-2026-0866**, and the CERT Coordination Center (CERT/CC) has issued guidance highlighting the risks of malformed archive files that bypass automated security scanning.

Remediation

Organizations should implement the following mitigation measures to reduce the risk of malware delivery through malicious archive files:

- **Treat suspicious archives cautiously:** Avoid opening ZIP files received from unknown or untrusted sources, especially if extraction tools report errors such as unsupported compression methods.
- **Update security tools:** Ensure antivirus and endpoint protection solutions are updated to the latest versions that include improved archive validation and inspection mechanisms.
- **Advanced archive inspection:** Configure security solutions to validate ZIP metadata against the actual file structure and enable deep archive analysis when available.
- **Email gateway filtering:** Configure email security gateways to scan and sandbox compressed attachments, particularly those received from external sources.
- **User awareness training:** Educate users about malicious archive-based attacks commonly delivered through phishing emails or file-sharing platforms.
- **Endpoint monitoring:** Deploy EDR solutions capable of detecting suspicious loader behavior, abnormal decompression routines, or attempts to execute payloads extracted from archives.
- **Incident response procedures:** If a suspicious archive is identified, isolate affected systems, scan for malicious processes or scripts, and analyze network activity for potential command-and-control communications.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

- Toulas, B. (2026, March 10). New “Zombie ZIP” technique lets malware slip past security tools. Retrieved from BleepingComputer: https://www.bleepingcomputer.com/news/security/new-zombie-zip-technique-lets-malware-slip-past-security-tools/