

December, 2024

Corrupted ZIPs and Office Docs Bypass Security

Context

A sophisticated phishing campaign, leveraging corrupted ZIP archives and Microsoft Office files, is successfully bypassing traditional security defenses, including antivirus systems, sandboxes, and email spam filters. Active since August 2024, this attack exploits vulnerabilities in file recovery mechanisms within widely used applications such as Microsoft Word, Outlook, and WinRAR. When users open seemingly legitimate business communications, the malicious payloads are triggered, executing harmful code. What makes this threat particularly concerning is its ability to target trusted tools, allowing attackers to bypass security layers that rely on detecting suspicious file types or behaviors. The sophistication of the campaign reflects a deep understanding of how modern security defenses operate, posing a significant risk to organizational integrity. By exploiting trusted file formats and recovery features, attackers can establish a foothold in corporate environments, potentially leading to data breaches, ransomware deployment, or the theft of sensitive information. This campaign underscores the urgent need for organizations to move beyond reliance on a single layer of threat detection, such as Microsoft Defender, which many businesses depend on without validating its effectiveness or assessing potential evasion. Relying solely on one security measure leaves organizations vulnerable to sophisticated attacks that can bypass traditional defenses. To mitigate these risks, organizations should implement multi-layered security strategies, including advanced, behavior-based detection systems, and ensure that employees are trained to identify and avoid increasingly sophisticated social engineering tactics.

Mitigation

Defenses often fail or are evaded by sophisticated attacks, and when this occurs, organizations must be proactive in detecting breaches. To strengthen their response, they should implement the following controls:

1. **Forensic-Level Compromise Assessments:** Conduct these assessments at least once a day to ensure thorough examination of potential security incidents.
2. **Threat Hunting:** Proactively conduct threat hunting to validate in-memory and operating system artifacts that cannot be analyzed using existing security technologies.



Technical Details

Malware Delivery

Corrupted ZIP or Microsoft Office files containing malicious code are sent as attachments in phishing emails. These emails often mimic legitimate business correspondence. When these files are opened, built-in recovery mechanisms in software, such as Microsoft Word, Outlook, or WinRAR, activate thereby executing the malicious payload.

Malware Analysis

The malicious files evade detection by traditional security solutions by exploiting document recovery features. Security solutions fail to analyze the files because their extraction systems cannot access any readable content. However, when users open these files, recovery functions of applications trigger the execution of embedded malware. The payloads typically aim to steal sensitive data, compromise systems, and establish persistent access. This method ensures that only genuine user interaction initiates the attack, bypassing most automated defenses.

A potential zero-day attack evades detection by security tools

ANY.RUN


- 1

An email attachment is received, identified as a ZIP file or an MS Office document, but it is corrupted

```

Incorrect ZIP file header
00000000 50 4b c3 9d c3 8f ef be a0 e3 85 a4 e3 85 a4 e3  PK .....
00000010 85 a4 ef be a0 e3 85 a4 e3 85 a4 ef be a0 ef be .....
00000020 a0 e3 85 a4 e3 85 a4 ef be a0 ef be a0 ef be a0 .....
00000030 ef be a0 e3 85 a4 ef be a0 e3 85 a4 e3 85 a4 e3 .....
```
- 2

For instance, when opening a Word file, the application prompts to restore it. Let's see what happens if we press "Yes"


- 3

Word locates a valid header to reconstruct the file, as it contains critical archive information required for processing

```

Correct ZIP file header
00002cd0 be a0 e3 85 a4 e3 85 a4 20 7d ce 99 50 4b c3 9d ..... } PK...
00002ce0 74 83 99 98 83 80 72 59 74 59 8e 5b 75 10 63 01 ..... }tY (- c
00002cf0 00 85 00 00 03 00 00 00 5b 43 6f 6e 74 65 ..... [Conte
00002d00 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 85 54 09 nt.Types.xml
```

Compressed size

Uncompressed size

Source: ANY.RUN

Tactics, Techniques and Procedures

The following TTPs have been observed in relation to this attack:

Initial Tactic: Initial Access | Technique: Phishing (T1566.001)

Malicious ZIP and Office files delivered through phishing emails disguised as business correspondence.

Tactic: Execution | Technique: User Execution (T1204.002)

Malicious code runs when recovery mechanisms process corrupted files.

Tactic: Defense Evasion | Techniques: Obfuscated Files (T1027)

Files have corrupted metadata to bypass antivirus detection.

Tactic: Defense Evasion | Techniques: Deobfuscate/Decode Files (T1140)

Applications decode and execute the files via recovery features.

Tactic: Command and Control | Technique: Encrypted Channel (T1573):

Communication with attacker infrastructure occurs over encrypted channels

Cyber Threat Intelligence

ANY.RUN has uncovered that this attack technique has been utilized by threat actors since at least August 2024, identifying it as a potential zero-day vulnerability exploited to evade detection.

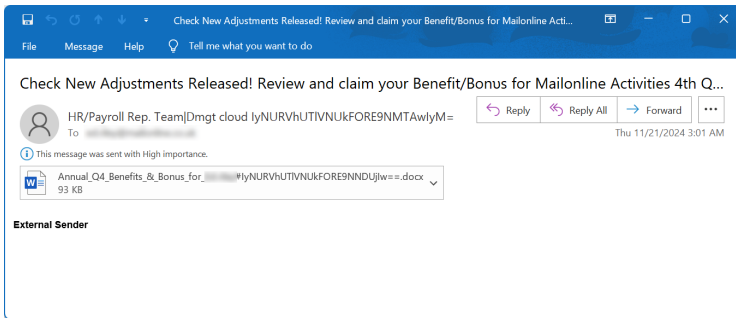
The primary objective of these attacks is to manipulate users into opening malicious documents, which contain QR codes that, when scanned, redirect victims to fraudulent websites designed for malware deployment or counterfeit login pages aimed at stealing credentials.

These findings underscore the persistent ingenuity of cybercriminals, who continuously seek novel methods to bypass email security defenses and ensure that their phishing emails successfully reach their targets' inboxes.

The corrupted state of the files prevents them from being flagged as suspicious or malicious by email filters and antivirus software. Despite this, the attack remains effective by exploiting the built-in recovery mechanisms of programs like Microsoft Word, Outlook, and WinRAR. These programs attempt to reopen the damaged files in recovery mode, inadvertently triggering the malicious payload.

References

Sample Phishing Email:



These attachments use a wide range of themes, all revolving around employee benefits and bonuses, including:

- Annual_Benefits_& Bonus_for_[name]_lyNURVhUTIVNUkFORE9NNDUjIw__.docx
- Annual_Q4_Benefits_& Bonus_for_[name]_lyNURVhUTIVNUkFORE9NNDUjIw__.docx.bin
- Benefits_& Bonus_for_[name]_lyNURVhUTIVNUkFORE9NNDUjIw__.docx.bin
- Due_& Payment_for_[name]_lyNURVhUTIVNUkFORE9NNDUjIw__.docx.bin
- Q4_Benefits_& Bonus_for_[name]_lyNURVhUTIVNUkFORE9NNDUjIw__.docx.bin

Source: BleepingComputer

Public Intelligence:

- <https://www.bleepingcomputer.com/news/security/novel-phishing-campaign-uses-corrupted-word-documents-to-evade-security/>
- <https://any.run/cybersecurity-blog/corrupted-files-attack/>

Act now to protect your business!

Contact CyberStash today to learn about eclipse.xdr and our round-the-clock managed detection and response service.

