AL2025_27 Fake Microsoft Office Add-ins Distribute Malware via SourceForge (June 11, 2025)

Description

A new malware campaign has been uncovered exploiting the SourceForge platform to distribute fake Microsoft Office add-in tools. These malicious files are designed to both mine and steal cryptocurrency from infected systems. The attack masquerades as a legitimate project called officepackage, cloning the appearance and content of Microsoft's real Office-Addin-Scripts GitHub repository. The campaign has reportedly impacted over 4,600 systems globally, primarily in Russia.

While SourceForge is generally a trusted site for open-source development, its open submission model allowed this malicious project to be listed temporarily. Although swiftly removed, the project had already been indexed by search engines and appeared in search results for Office add-ins, luring unsuspecting users into downloading the malware.

Attack Details

The initial entry point for this malware campaign involves users searching online for Microsoft Office add-ins. These victims are redirected to a fraudulent SourceForge project page, 'officepackage.sourceforge.io', which convincingly mimics a legitimate developer resource. The page displays familiar-looking elements such as "Office Add-ins" and "Download" buttons, increasing the likelihood that users will trust and interact with it.

When the user clicks the download button, they receive a ZIP file containing a password-protected archive named installer.zip, along with a text file revealing the password. Inside this archive lies a bloated 700MB installer.msi file, intentionally oversized to bypass antivirus scanning. Once executed, this installer drops two files onto the system: UnRAR.exe and 51654.rar. It also runs a Visual Basic script designed to fetch and execute a batch file (confvk.bat) hosted on GitHub. This script performs environment checks, including detection of sandboxing or antivirus software, before proceeding to download an additional script named confvz.bat.

The second batch script (confvz.bat) enables persistence on the infected machine by modifying the Windows Registry and creating new services. It also unpacks the contents

of the RAR file, deploying several key components of the malware. These include Input.exe (an AutoIT script interpreter), ShellExperienceHost.exe (a Netcat-based reverse shell), and two malicious DLLs: Icon.dll and Kape.dll.

Once active, the malware exhibits multiple capabilities. It includes a cryptocurrency miner that exploits the system's processing power to generate digital currency for the attacker. Additionally, it features clipper malware, which monitors the system clipboard for copied cryptocurrency wallet addresses and stealthily replaces them with attacker-controlled addresses. Lastly, the malware collects system data and transmits it to the attacker via Telegram API, which also serves as a channel for deploying further malicious payloads to the compromised machine.

Indicators of Compromise (IoCs)

File Names:

- installer.zip, installer.msi, UnRAR.exe, 51654.rar, Input.exe, ShellExperienceHost.exe, Icon.dll, Kape.dll
- Batch Scripts: confvk.bat, confvz.bat

Domains/URLs:

- officepackage.sourceforge.io
- GitHub URLs hosting confvk.bat and confvz.bat (exact URLs not disclosed)

Behavioral Indicators:

- Large MSI files (700MB) used to bypass AV
- Registry modifications and new Windows services
- Connections to Telegram API endpoints

Remediation

Immediate Actions:

- Isolate and investigate systems showing signs of infection.
- Terminate suspicious services and scheduled tasks added by malware.

- Delete malicious files and restore from backups if system compromise is confirmed.

Preventive Measures:

- Only download tools and software from official and verified sources (e.g., Microsoft's GitHub).
- Avoid downloading from unfamiliar project subdomains like *.sourceforge.io.
- Employ updated antivirus and endpoint detection systems capable of behavioral analysis.
- Monitor clipboard activity if dealing with cryptocurrency transactions frequently.

Organizational Controls:

- Block known malicious IoCs at the network and endpoint level.
- Regularly update group policies to prevent execution of unauthorized scripts and batch files.
- Educate users on verifying file origins and checking digital signatures.

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

References

- FadilpaŠI, S. (2025, April 9). Beware, these dangerous fake Microsoft Office add-ons are spreading malware. Retrieved from TechRadar. https://www.techradar.com/pro/security/beware-these-dangerous-fake-microsoft-office-add-ons-are-spreading-malware
- Toulas, B. (2025, April 9). Fake Microsoft Office add-in tools push malware via SourceForge. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/fake-microsoft-office-add-in-tools-push-malware-via-sourceforge/