UAC-0099 Uses Fake Notepad++ Plugin to Deploy MATCHBOIL.V2 Malware

***Author**: Portia S. Cole – CTI Researcher*

TL;DR

The Russia-aligned threat group UAC-0099 is using phishing emails and a malicious Notepad++ plugin to compromise Windows systems and deploy MATCHBOIL.V2.

The campaign currently targets organizations in Ukraine, but the delivery method could be reused against other organizations across various regions.

Overview

UAC-0099 (a Russian threat actor) is distributing a malicious Notepad++ plugin through phishing emails that contain an image linked to a ZIP archive. The archive contains a Visual Basic Script (VBScript) disguised as a PDF using a double file extension and additional spaces before the .vbs extension.

If the recipient opens the script, it displays a legitimate PDF as a decoy while downloading a second archive named Evernote.zip. This archive contains a working copy of Notepad++ 8.8.3, a malicious plugin named NppExport.dll, a password-protected archive and the legitimate WinRAR executable.

The script launches Notepad++, which loads the malicious plugin through the application's normal plugin-loading process. CERT-UA identifies the plugin as LUNCHPOKE. It extracts the BURNYBEAR and MATCHBOIL.V2 loaders and creates a scheduled task that runs the malware every three minutes.

MATCHBOIL.V2 can update its command-and-control configuration, download additional payloads and create additional scheduled tasks. CERT-UA has not disclosed the final payload delivered during the observed attacks or the campaign's ultimate objective.

This campaign does not involve a confirmed compromise of Notepad++ or its official update infrastructure. The attackers bundle a legitimate copy of the application with their own malicious plugin and rely on the recipient to launch the disguised script. Although the campaign currently targets organizations in Ukraine, the same attack method could be used against organizations in other regions, particularly those that support Ukraine.

Aspire Protects

- Block or quarantine VBScript files delivered through email, downloaded archives and file-sharing services unless there is a documented business need.
- Configure Windows to display complete file extensions to help users identify double-extension files.
- Alert on notepad++.exe running from %PUBLIC% or other unexpected directories.
- Monitor for Notepad++ loading unfamiliar plugin DLLs, particularly NppExport.dll.
- Update Notepad++, WinRAR and 7-Zip through approved software-management channels.
- If the malicious script was executed, isolate the system and investigate for scheduled tasks, additional payloads and outbound command-and-control activity.
    - Removing the downloaded archive alone will not remove the persistence mechanism.

TTPs to Watch

Initial Access

- Phishing: Spearphishing Link [T1566.002] – An attacker may send a phishing email containing an image linked through a URL-shortening service to a file-sharing site hosting a malicious ZIP archive.

Execution

- User Execution: Malicious Link [T1204.001] – An attacker may rely on the recipient to click the image or link that leads to the malicious archive.
- User Execution: Malicious File [T1204.002] – An attacker may rely on the recipient to extract the archive and execute a VBScript disguised as a PDF.
- Command and Scripting Interpreter: Visual Basic [T1059.005] – An attacker may use VBScript to download additional files, display a decoy PDF and launch the malware chain.

Persistence

- Scheduled Task/Job: Scheduled Task [T1053.005] – An attacker may create a scheduled task that runs BURNYBEAR every three minutes to maintain persistence and execute MATCHBOIL.V2.

Defense Evasion/Stealth

- Masquerading: Double File Extension [T1036.007] – An attacker may disguise a VBScript as a PDF by using a .pdf.vbs double extension and inserting spaces before the final extension.

Command and Control

- Ingress Tool Transfer [T1105] – An attacker may use the initial VBScript and MATCHBOIL.V2 to download additional archives, malware components and follow-on payloads.

IoCs

Files

- NppExport.dll
- RemoteLibUpdater.exe
- InitTest.dll
- Evernote.zip
- updater.rar
- Background.exe

SHA-256 Hashes

- c270432a3f16241c24d0b57838b17b2fa438a24eebf29dcbda08622de725fe21
- 838512a8a88f584a5d9a61cff17da0db7fa5886cccce2f84652ccb6e7808b090
- 78cb23c739d24513b25f477183566c9fce0b329696e05482065f1bf01629c606

File Paths and System Artifacts

- %PUBLIC%\Libs_<random>\Notepad\
- %PUBLIC%\Libraries\<random>\RemoteLibUpdater.exe
- %PUBLIC%\Wallpapers\Background.exe
- \W1n3r-U09oTy-Ap5\Updates
- RemoteLibUpdater.exe setup nodisplay

***Note**: This is not a Notepad++ vulnerability or supply-chain compromise. The attackers are distributing their own packaged copy of Notepad++ with a malicious plugin already placed inside it.*

Targeted Industries

UAC-0099 has historically targeted the following industries:

- Government
- Defense

Aspire Service Offerings

- **Aspire Managed XDR (MXDR)**
  - Aspire Managed XDR (MXDR) combines next-generation eXtended Detection and Response (XDR) technology, a 24x7 security operations center (SOC), and the expertise of a US-based team of security professionals to identify and respond to threats across a broader attack surface.
  - Building on the existing capabilities of Managed Detection and Response (MDR), Aspire Managed XDR integrates and correlates telemetry from endpoints, network, cloud, email, identity, and more. This advanced platform creates valuable context enabling end-to-end visibility across all threat vectors.
  - Experienced security analysts and incident responders deliver 24x7 threat detection, analysis, and investigations – with both automated and human-led response actions to quickly mitigate cyber attacks.
- **Aspire Incident Response**
  - The ability to respond effectively to data breaches is critical to every organization. When attacks occur, IT leaders need a process that will ultimately maintain business continuity, protect the company reputation, and avoid fines, legal fees, and remediation costs.
  - Aspire offers incident response services to help you prepare for, manage, and recover from data breaches and network attacks. An experienced team uses industry-leading threat intelligence and the most current security technology to quickly respond to attacks, reduce damage, and minimize exposure.

Supporting Documentation

CERT-UA

UAC-0099 threat actors employ malicious HTA files for MatchBoil loader delivery