Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Notepad++ Plugin Compromised to Inject Malicious Code

Date of Publication	Admiralty Code	TA Number
April 9, 2024	A1	TA2024135

Summary

Attack Began: April 2024
Attack Region: Worldwide
Attack: By tampering with a widely used Notepad++ plugin, hackers have injected malicious code that compromises users' systems. This attack targeted the “MIME Tools" plugin, a commonly utilized component within Notepad++. The attackers included the malicious MIMETools.dll file in the installation package of a particular version of Notepad++, disguising it as a legitimate package file to deceive users.

Attack Regions

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin

Attack Details

#1

Hackers exploited a widely-used Notepad++ plugin named MIME Tools, specifically responsible for encoding operations like Base64 encoding. They distributed a modified version of this plugin disguised as a regular package file within a specific Notepad++ installation package, tricking users into installing the malware onto their systems.

#2

Using a DLL hijacking technique, the attackers manipulated the basic plugin, inserting encrypted malicious shell code having decryption and execution instructions. This encrypted code was stored within the certificate.pem file. Upon loading, the malicious MIMETools.dll initiates its malicious activities automatically without requiring user interaction.

#3

The malware operates by initiating a process when the user runs Notepad++ and mimeTools.dll is loaded. It performs thread injection into explorer.exe, decrypts the certificate.pem file, modifies code in the BingMaps.dll->GetBingMapsFactory() function, and downloads additional shell code from a C2 server.

#4

The malware, triggered upon the loading of MIMETools.dll within Notepad++, performs thread injection into explorer.exe, decrypts the certificate.pem file, and alters the code in BingMaps.dll. ShellCode injected into the GetBingMapsFactory() function of BingMaps.dll detects analysis environments and terminates processes if specific conditions are met. However, if "explorer.exe" is identified, additional ShellCode is generated within its memory space, allowing the execution of malicious code. Furthermore, the malware downloads additional ShellCode from a C2 server, employing indirect syscall techniques to evade antivirus detection.

#5

This incident underscores the importance of downloading software from reputable platforms and exercising caution when using cracked software or obtaining materials from unknown sources.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Download from Trusted Sources: Only download software from trusted sources. Avoid downloading software from third-party websites or torrents, as they may contain malware or modified versions of the software.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0007 Discovery	**TA0010** Exfiltration	**TA0011** Command and Control	**T1566** Phishing
T1059 Command and Scripting Interpreter	**T1204** User Execution	**T1036** Masquerading	**T1574** Hijack Execution Flow
T1574.002 DLL Side-Loading	**T1132** Data Encoding	**T1132.001** Standard Encoding	**T1033** System Owner/User Discovery
T1069 Permission Groups Discovery	**T1614** System Location Discovery	**T1614.001** System Language Discovery	**T1124** System Time Discovery
T1497 Virtualization/Sandbox Evasion			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	c4ac3b4ce7aa4ca1234d2d3787323de2, 6136ce65b22f59b9f8e564863820720b, fe4237ab7847f3c235406b9ac90ca845, d29f25c4b162f6a19d4c6b96a540648c, 8b7a358005eff6c44d66e44f5b266d33, d5ea5ad8678f362bac86875cad47ba21

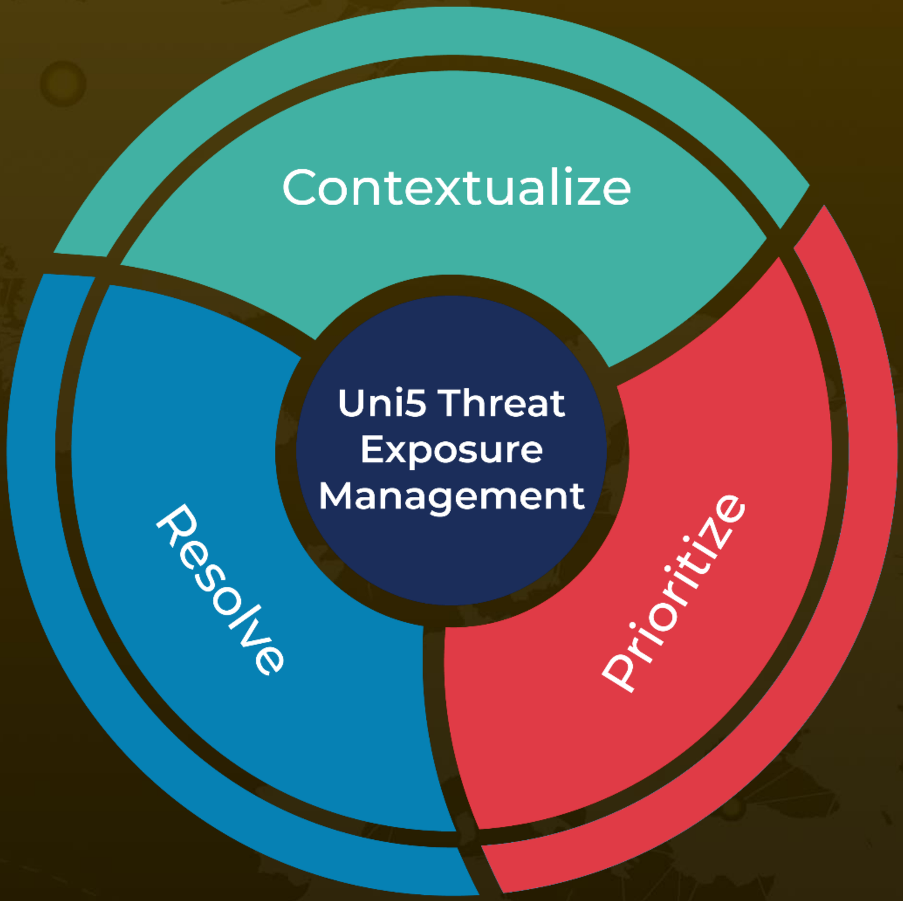
References

https://asec.ahnlab.com/ko/63738/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 9, 2024 • 6:50 AM

More at www.hivepro.com