Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

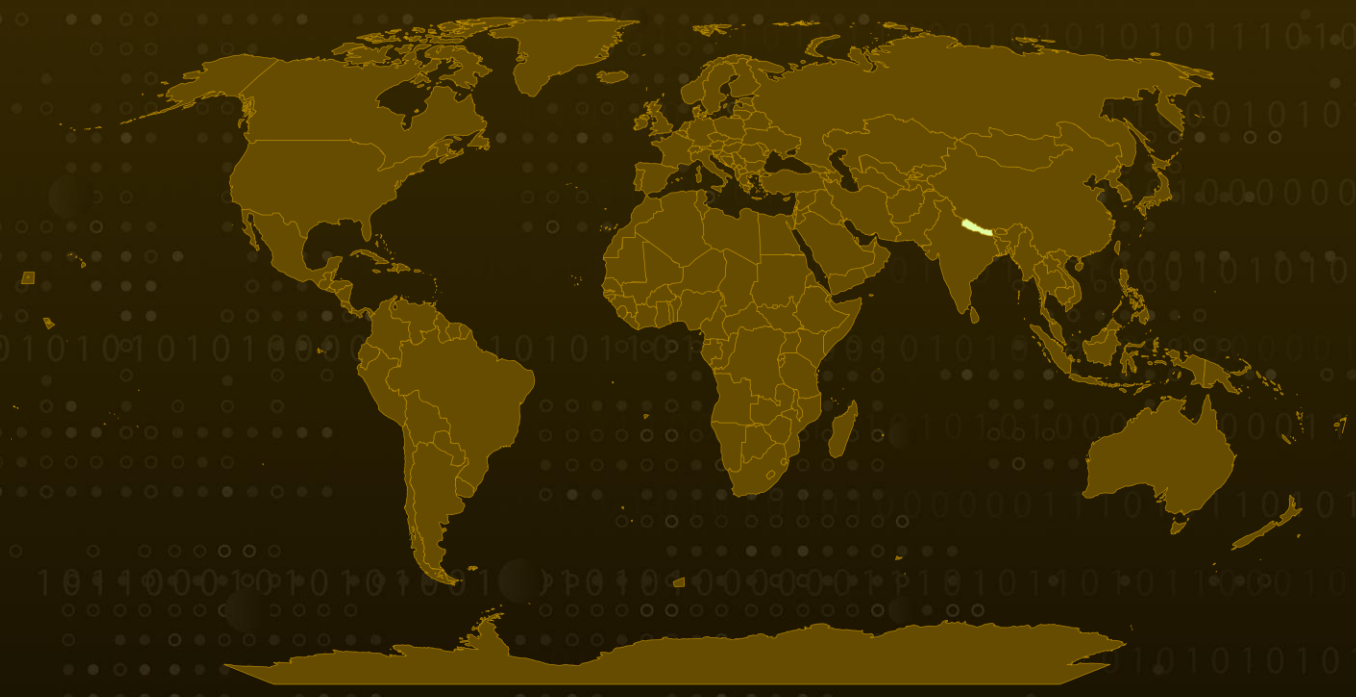
Nim Backdoor Masquerades as Nepal Government Security

Date of Publication	Admiralty Code	TA Number
January 3, 2024	A1	TA2024002

Summary

First appeared: December 2023
Attack Region: Nepal
Malware : Nim Backdoor
Attack: Attackers employed malicious Microsoft Word documents disguised as official communications from the Nepali government. These documents aimed to trick victims into downloading and executing a backdoor program written in the Nim programming language. As Nim is an uncommon language, it poses challenges for analysis and underscores the need for ongoing vigilance in the security community.

Attack Regions



Attack Details

#1 A malicious Word document, disguised as a Nepali government security communication, delivers the Nim backdoor. Despite security controls, the document exploits macros, initiating a complex sequence of VBScripts and batch files to obfuscate and deliver the Nim backdoor, under the guise of "conhost.exe." The attackers employ advanced evasion techniques, including password-protected VBA projects and obfuscated macros.

#2 The Nim backdoor, compiled in September 2023, operates at the user's privilege level and communicates with command and control (C&C) servers mimicking government domains. Anti-analysis measures include checks for known tools, and the Nim backdoor encrypts the machine's hostname before connecting to the C&C server. Persistence is achieved through a VBScript in the startup folder and scheduled tasks.

#3 The use of Nim, an uncommon programming language, adds complexity for researchers. Despite C2 server inaccessibility during analysis, this threat underscores the need for continual monitoring and adaptation within the security community to combat advanced threats utilizing less common programming languages. Recently SideWinder actors employed deceptive content, ultimately executing the Nim Backdoor to target South Asian nations.

Recommendations

Email Security: Deploy robust email filtering solutions to detect and block malicious attachments and phishing attempts. Implement email mechanisms (SPF, DKIM, DMARC) to prevent email spoofing and phishing.

Macro Policies: Disable macros in Microsoft Office files by default and enable them only for trusted sources through Group Policy or security settings.Consider implementing Application Control solutions to restrict the execution of macros in untrusted environments

Endpoint Protection: Utilize reputable antivirus and anti-malware solutions for early detection and removal of Nim backdoor and similar threats. Keep endpoint protection software up-to-date to recognize and mitigate the latest malware variants.

Software and System Updates: Regularly update operating systems, software, and applications to patch vulnerabilities. Implement automatic updates to ensure timely patching and security improvements.

User Privileges and Access Controls: Follow the principle of least privilege, granting users the minimum necessary access. Implement strong authentication mechanisms and enforce complex password policies.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0001 Initial Access	TA0005 Defense Evasion	TA0004 Privilege Escalation
TA0010 Exfiltration	TA0003 Persistence	TA0011 Command and Control	T1140 Deobfuscate/Decode Files or Information
T1059 Command and Scripting Interpreter	T1057 Process Discovery	T1053.005 Scheduled Task	T1053 Scheduled Task/Job
T1566.001 Spearphishing Attachment	T1566 Phishing	T1204.002 Malicious File	T1204 User Execution
T1547 Boot or Logon Autostart Execution	T1137 Office Application Startup	T1048 Exfiltration Over Alternative Protocol	T1071 Application Layer Protocol
T1027 Obfuscated Files or Information			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	e2a3edc708016316477228de885f0c39, 777fcc34fef4a16b2276e420c5fb3a73, EF834A7C726294CE8B0416826E659BAA, 32C5141B0704609B9404EFF6C18B47BF
SHA1	3aa803baf5027c57ec65eb9b47daad595ba80bac, 5D2E2336BB8F268606C9C8961BED03270150CF65, 4CAE7160386782C02A3B68E7A9BA78CC5FFB0236, 0599969CA8B35BB258797AEE45FBD9013E57C133
Hostname	mail[.]mofa[.]govnp[.]org, nitc[.]govnp[.]org, mx1[.]nepal[.]govnp[.]org, dns[.]govnp[.]org
SHA256	b5c001cbcd72b919e9b05e3281cc4e4914fee0748b3d81954772975630233a6e, 696f57d0987b2edefcadecd0eca524cca3be9ce64a54994be13eab7bc71b1a83, 88FA16EC5420883A9C9E4F952634494D95F06F426E0A600A8114F69A6127347F, 1246356D78D47CE73E22CC253C47F739C4F766FF1E7B473D5E658BA1F0FDD662

References

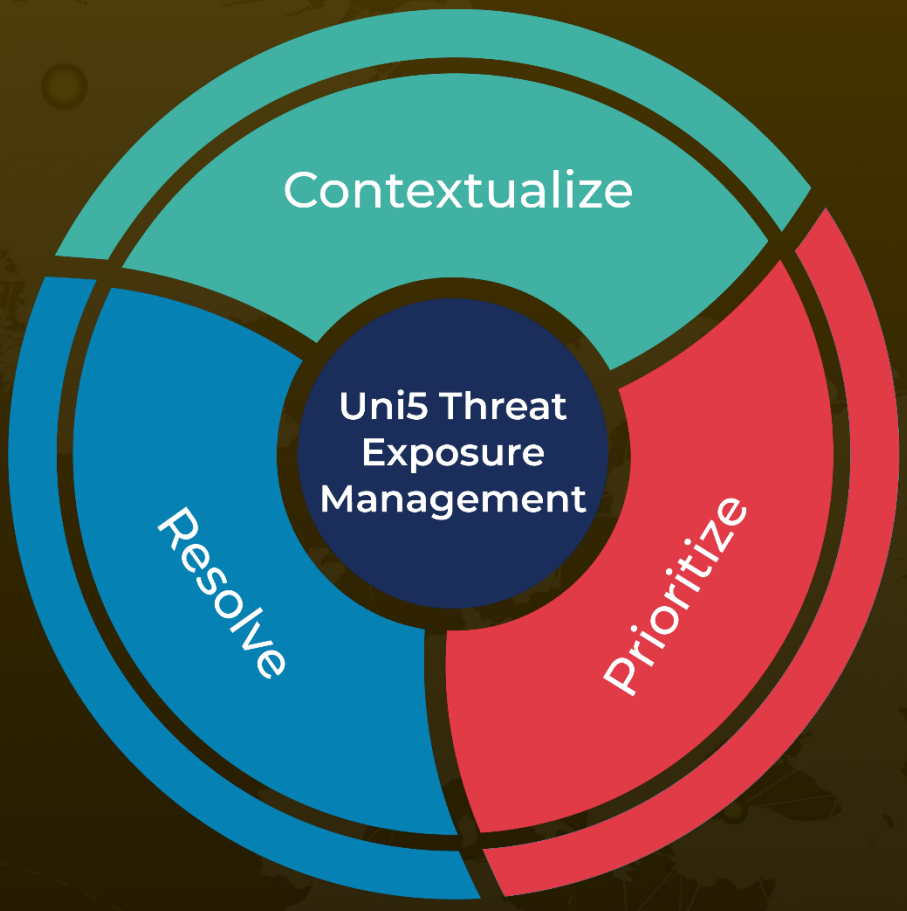
https://www.netskope.com/blog/a-look-at-the-nim-based-campaign-using-microsoft-word-docs-to-impersonate-the-nepali-government

https://www.hivepro.com/threat-advisory/sidewinders-nim-backdoor-spells-trouble-for-south-asian-nations/

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

January 3, 2023 • 5:00 AM

More at www.hivepro.com