Hive Pro®

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

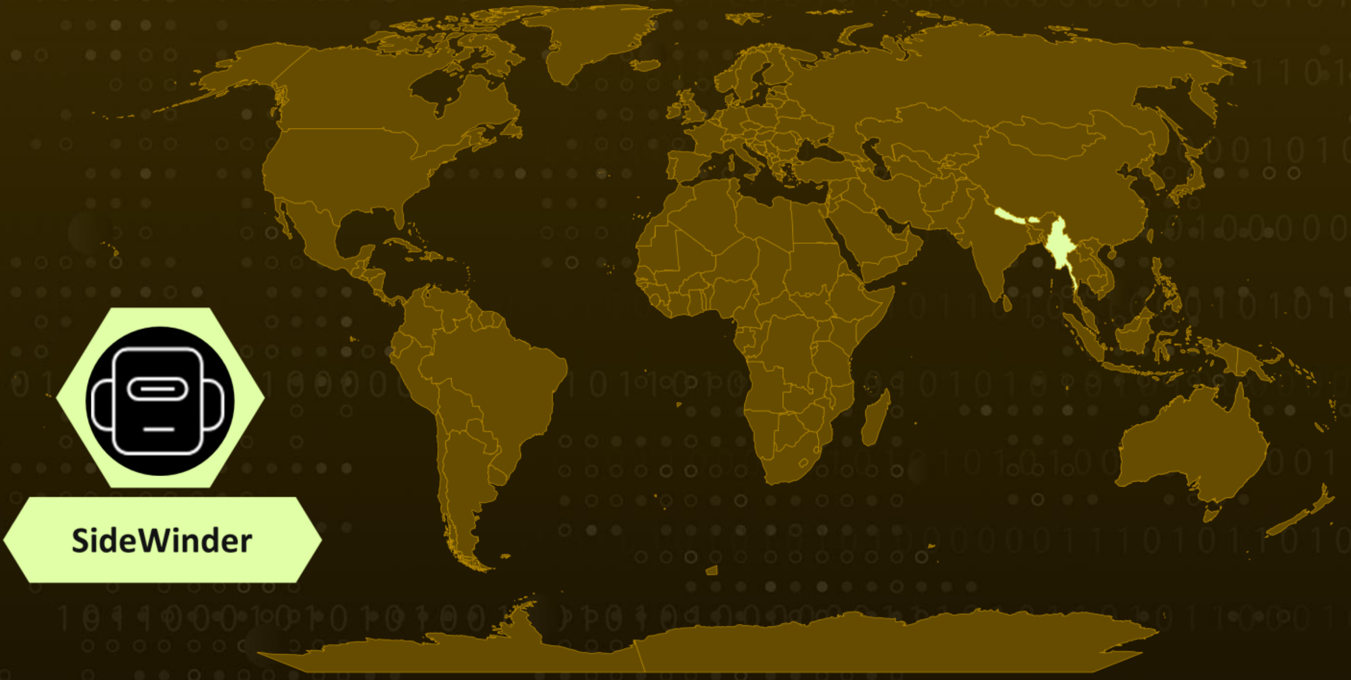
SideWinder's Nim Backdoor Spells Trouble for South Asian Nations

Date of Publication	Admiralty Code	TA Number
November 21, 2023	A1	TA2023470

Summary

Active Since: 2012
Malware: Nim backdoor
Threat Actor: SideWinder (aka Razor Tiger, Rattlesnake, T-APT-04, APT-C-17, Hardcore Nationalist, HN2, APT-Q-39, BabyElephant, GroupA21)
Attack Region: Bhutan, Nepal, and Myanmar.
Affected Platform: Government
Attack: SideWinder, also known as Razor Tiger, commenced its offensive operations in 2012 and has recently shifted its focus to targeting Bhutan. It employs deceptive content, ultimately executing the Nim Backdoor. The decoy content utilized in the sample is directly sourced from announcements published on the Bhutanese government website.

Attack Regions



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

Attack Details

#1 The earliest instances of offensive operations by **SideWinder**, also identified as Razor Tiger, date back to 2012. In more recent times, its focus has shifted to targeting Bhutan. The misleading content within the document undergoes a series of VBS and BAT scripts before ultimately executing the backdoor devised by Nim Backdoor.

#2 The macro code is solely responsible for releasing files. The malicious sample orchestrates the initiation of scripts by utilizing the startup file in the Startup directory, thereby intensifying the covert nature of the attack. Upon the execution of Nim Backdoor, an initial check is conducted on the operating environment.

#3 Following this, several alternative C&C server URLs are copied, and the command from the C&C server is obtained through an HTTP GET request. The encrypted result of the hostname is then encoded in base64. Certain Nim backdoors also include code designed to assess the operating environment based on mouse movement distance.

#4 The functionality of the Nim backdoor, disseminated through malicious documents, is relatively straightforward and likely represents just one facet of a prolonged and intricate attack campaign.

Recommendations

Behavior-Based Monitoring: Deploy behavior-based monitoring to detect unusual activity patterns, including suspicious processes attempting unauthorized network connections, which is a common behavior of Backdoors.

Phishing Awareness Training: Conduct regular training sessions to educate employees about phishing threats, including recognizing suspicious emails, links, and attachments. Create a culture of skepticism towards unexpected or unusual email requests.

Network Segmentation: Segment your network into isolated zones to limit lateral movement for attackers and reduce the impact of a breach. Deploy network traffic analysis tools to monitor and analyze patterns of communication between endpoints and potential command and control servers

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
TA0010 Exfiltration	T1598 Phishing for Information	T1566.001 Spearphishing Attachment	T1059 Command and Scripting Interpreter
T1083 File and Directory Discovery	T1057 Process Discovery	T1056 Input Capture	T1053 Scheduled Task/Job
T1204 User Execution	T1547 Boot or Logon Autostart Execution	T1543 Create or Modify System Process	T1211 Exploitation for Defense Evasion
T1132 Data Encoding	T1041 Exfiltration Over C2 Channel		

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	c2184d8fd3dd3df9fd6cf7ff8e32a3a4, b2ab01d392d7d20a9261870e709b18d7, 30ddd9ebe00f34f131efcd8124462fe3, 92612dc223e8f0656512cd882d66f78b, 7bea8ea83d5b4fe5985172dbb4fa1468, 04e9ce276b3cd75fc2b20b9b33080f7e
C2	dns-mofgovbt[.]ddns[.]net, mail-mofgovbt[.]hopto[.]org, microsoftupdte[.]redirectme[.]net, updatemanager[.]ddns[.]net, mx2[.]nepal[.]gavnp[.]org, cloud[.]nitc[.]gavnp[.]org, dns[.]nepal[.]gavnp[.]org,

TYPE	VALUE
C2	mx1[.]nepal[.]gavnp[.]org, asean-ajp[.]myftp[.]org, dof-govmm[.]sytes[.]net, mail-mohs[.]servehttp[.]com, drsasa[.]hopto[.]org, pdf-shanstate[.]serveftp[.]com, myanmar-apn[.]serveftp[.]com, mytel-mm[.]servehttp[.]com, pdf-shanstate[.]redirectme[.]net
File Paths	%AppData%\Microsoft\Windows\Start Menu\Programs\Startup, %LocalAppData%\skriven.vbs, %LocalAppData%\Microsoft\svchost.zip, %LocalAppData%\8lGghf8kIPIuu3cM.bat, E:\\Store\\MACRO\\BT\\bt_apache.nim, E:\\Store\\MACRO\\NP\\np_apache.nim, E:\\Store\\macro\\mm\\mm_apache.nim, C:\\Users\\ProCoder\\Desktop\\Store\\MACRO\\MM\\mm_apache.nim
File Names	OCu3HBg7gyI9aUaB.vbs, 8lGghf8kIPIuu3cM.bat
URLs	hxxp://dns-mofgovbt.ddns.net/update/, hxxp://mail-mofgovbt.hopto.org/update/, hxxp://microsoftupdte.redirectme.net/update/, hxxp://updatemanager.ddns.net/update/, hxxp://mx2.nepal.gavnp.org/mail/AFA/, hxxp://cloud.nitc.gavnp.org/mail/AFA/, hxxp://dns.nepal.gavnp.org/mail/AFA/, hxxp://mx1.nepal.gavnp.org/mail/AFA/, hxxp://asean-ajp.myftp.org/MOFA/, hxxp://dof-govmm.sytes.net/MOFA/, hxxp://mail-mohs.servehttp.com/MOFA/, hxxp://drsasa.hopto.org/MOFA/, hxxp://pdf-shanstate.serveftp.com/MOFA/

References

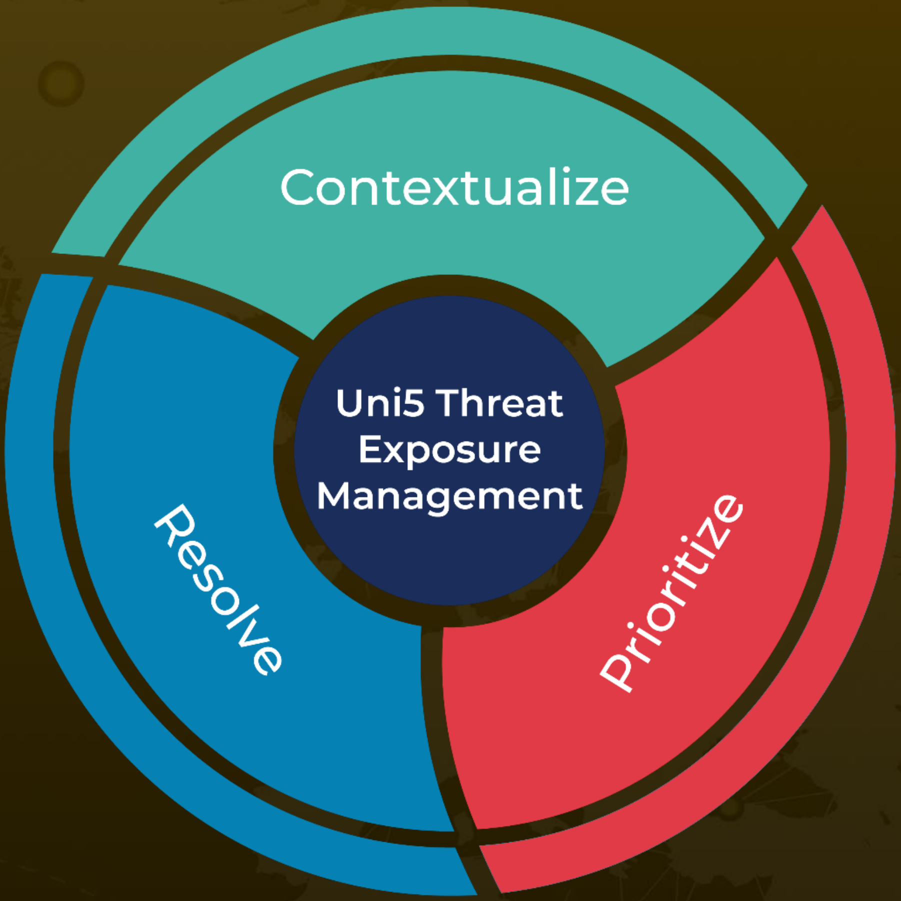
https://mp.weixin.qq.com/s?__biz=MzI2MDc2MDA4OA==&mid=2247508655&idx=1&sn=b808c9a435b473e5dc957d1b34a79432

https://www.hivepro.com/threat-advisory/uncovering-the-latest-tactics-of-the-sidewinder-apt/

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

November 21, 2023 • 5:00 AM

More at www.hivepro.com