Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

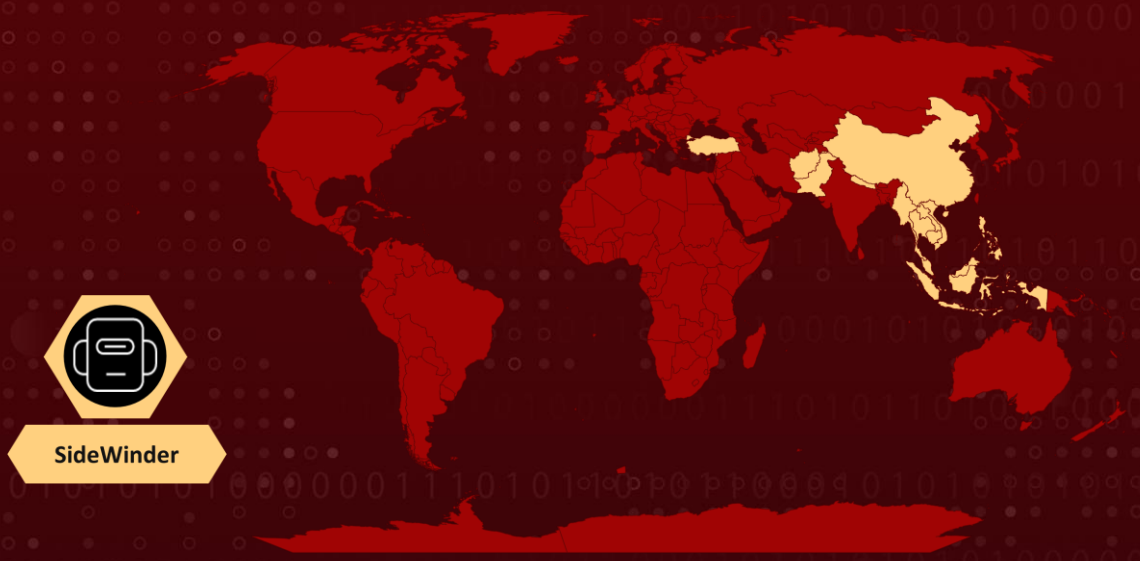
Uncovering the Latest Tactics of the SideWinder APT

Date of Publication	Admiralty Code	TA Number
May 11, 2023	A1	TA2023223

Summary

Attack began: November 2022
Actor: SideWinder (aka Rattlesnake, T-APT-04, APT-C-17, Razor Tiger, Baby Elephant, Operation Origami)
Attack Region: Pakistan, Turkey, Brunei, Cambodia, East Timor, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Vietnam, Afghanistan, China, and Nepal
Targeted Sector: Military, Government, and Business Entities
Attack: SideWinder APT group, originating from India, targets military, government & business entities in Asia. They use advanced tactics like spear-phishing, DLL side-loading & more. A new server-side polymorphism technique, highlighting the need for multi-layered security measures.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2017-0199	Microsoft Office/WordPad Remote Code Execution Vulnerability with Windows API	Microsoft Windows, Windows Server, Office	✓	✓	✓

Attack Details

#1 Since at least 2012, the SideWinder APT(aka Razor Tiger, Rattlesnake, and T-APT-04) group has been targeting various Pakistani government organizations. SideWinder is believed to have originated in India and is one of the earliest established threat actors. It has been observed attacking military, government, and business entities, with a particular focus on Pakistan, Afghanistan, China, and Nepal.

#2 The SideWinder group's primary mode of operation is to use sophisticated email spear-phishing techniques, document exploitation, and DLL side-loading to avoid detection and deliver targeted malicious implants. As part of their tactics, the group has implemented a server-side polymorphism technique.

#3 This technique enables the threat actors to potentially bypass conventional signature-based antivirus (AV) detection and deploy the subsequent stage payload with ease. What's notable about this campaign is that the group did not rely on embedding malicious macro code in the documents to deliver the subsequent stage payload. Instead, they exploited the CVE-2017-0199 vulnerability.

Recommendations

Keep software and systems up-to-date: The SideWinder group exploited a known vulnerability (CVE-2017-0199) to deliver its malicious implants. To prevent this type of attack, it is crucial to regularly apply security patches and updates to software and systems. This will ensure that known vulnerabilities are fixed and cannot be exploited by threat actors.

Deploy a layered defense approach: To counter SideWinder's evolving tactics, employ a comprehensive security solution incorporating endpoint, network & email security to detect & block their diverse attack vectors, including email spear-phishing & DLL side-loading.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion
TA0007 Discovery	TA0011 Command and Control	T1518 Software Discovery	T1480 Execution Guardrails
T1574 Hijack Execution Flow	T1559 Inter-Process Communication	T1027 Obfuscated Files or Information	T1047 Windows Management Instrumentation
T1059 Command and Scripting Interpreter	T1071 Application Layer Protocol	T1105 Ingress Tool Transfer	T1140 Deobfuscate/Decode Files or Information
T1203 Exploitation for Client Execution	T1204 User Execution	T1221 Template Injection	T1204.002 Malicious File

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	b7e63b7247be18cdfb36c1f3200c1dba 5efddbdcf40ba01f1571140bad72dccb 3b853ae547346befe5f3d06290635cf6 666b2b178ce52e30be9e69de93cc60a9 ef00004a1ebc262ffe0fb89aa5524d42 6c7d24b90f3c6b4383bd7d08374a0c6f 73750f08265bbe80c3f235318bcef6fe 16341fcff1bc7388387fd17b4b3a7a50 1c62441de076eb5a5b2e1f8146767777 dacdb33b6e9de4c1fe8591bb5a65c55c 709e6a64735432c25cafb89951cc149c
SHA256	cf1f4ec1d7db6cf1fe8e15687b348a279889689fa9c387de4a2c310c34336f9f 8af93bed967925b3e5a70d0ad90eae1f13bc6e362ae3dac705e984f8697aaaad a45258389a3c0d4615f3414472c390a0aabe77315663398ebdea270b59b82a5c

TYPE	VALUE
SHA256	bc9d4eb09711f92e4e260efcf7e48906dca6bf239841e976972fd74dac412e2f cd09bf437f46210521ad5c21891414f236e29aa6869906820c7c9dc2b565d8be a3283520e04d7343ce9884948c5d23423499fa61cee332a006db73e2b98d08c3 4db0a2d4d011f43952615ece8734ca4fc889e7ec958acd803a6c68b3e0f94eea bc3c6f9d51e2bdb37e03b01e2949f72836ecee4230e2320c5dc33a83b55b062f 75079e408ca9517825ffac396680a2d2169d691be3f1adbbd797e05e665c6fde cde768a4cf95e58f0e98e2bcca0663fd2c1a36510f6010065b4f54169a92e207 a2a9fd1db7f1dc196fa8af0669ea72d1f8ae48bf4775108ee746e0f83c5a7498
Domains	slpa.mod-gov[.]org mailrta.mfagov[.]org promotionlist.comsats-net[.]com mailnavybd.govpk[.]net mailnavymilbd.govpk[.]net
IPV4	185.205.187[.]234 5.230.73[.]106 62.113.255[.]80 194.61.121[.]216 5.255.104[.]32 5.255.112[.]194
URLs	hxxts[:]//forecast[.]comsats-net[.]com/5760/1/5035/2/0/0/0/m/files-4a0480ae/file[.]rtf hxxts[:]//moma[.]comsats-net[.]com/5753/1/4375/2/0/0/0/m/files-8062311a/file[.]rtf hxxts[:]//forecast[.]comsats-net[.]com/5760/1/5040/2/0/0/0/m/files-f3b20b30/file[.]rtf hxxts[:]//forecast[.]comsats-net[.]com/5760/1/5036/2/0/0/0/m/files-2ad09cbd/file[.]rtf hxxts[:]//moma[.]comsats-net[.]com/5753/1/4371/2/0/0/0/m/files-b62d382f/file[.]rtf hxxts[:]//srilanka-navy[.]lforvk[.]com/135/1/334/2/0/0/0/m/files-4fdaf6c7/file[.]rtf hxxts[:]//promotionlist[.]comsats-net[.]com/5756/1/8887/2/0/0/0/m/files-3d1dff0f/file[.]rtf hxxts[:]//dgms[.]paknavy-gov[.]com/5733/1/5051/2/0/0/0/m/files-73bdca4d/file[.]rtf

TYPE	VALUE
URLs	hxxts[:]//mofadividion[.]ptcl-gov[.]com/5724/1/3268/2/0/0/0/m/files-11e30891/file[.]rtf hxxts[:]//ksew[.]kpt-gov[.]org/5663/1/3275/2/0/0/0/m/files-937950ad/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5785/2/0/0/0/m/files-76f11745/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5788/2/0/0/0/m/files-3acec3be/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5782/2/0/0/0/m/files-78d7e141/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5796/2/0/0/0/m/files-97e02960/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5795/2/0/0/0/m/files-c9dddc54/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5790/2/0/0/0/m/files-a3d0041a/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5773/2/0/0/0/m/files-5a31d681/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5799/2/0/0/0/m/files-03dd18bd/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5781/2/0/0/0/m/files-62caea91/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5804/2/0/0/0/m/files-c43dece3/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5794/2/0/0/0/m/files-60cb1621/file[.]rtf hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5775/2/0/0/0/m/files-fca3cc50/file[.]rtf

Patch Links

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2017-0199

References

https://blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pakistan

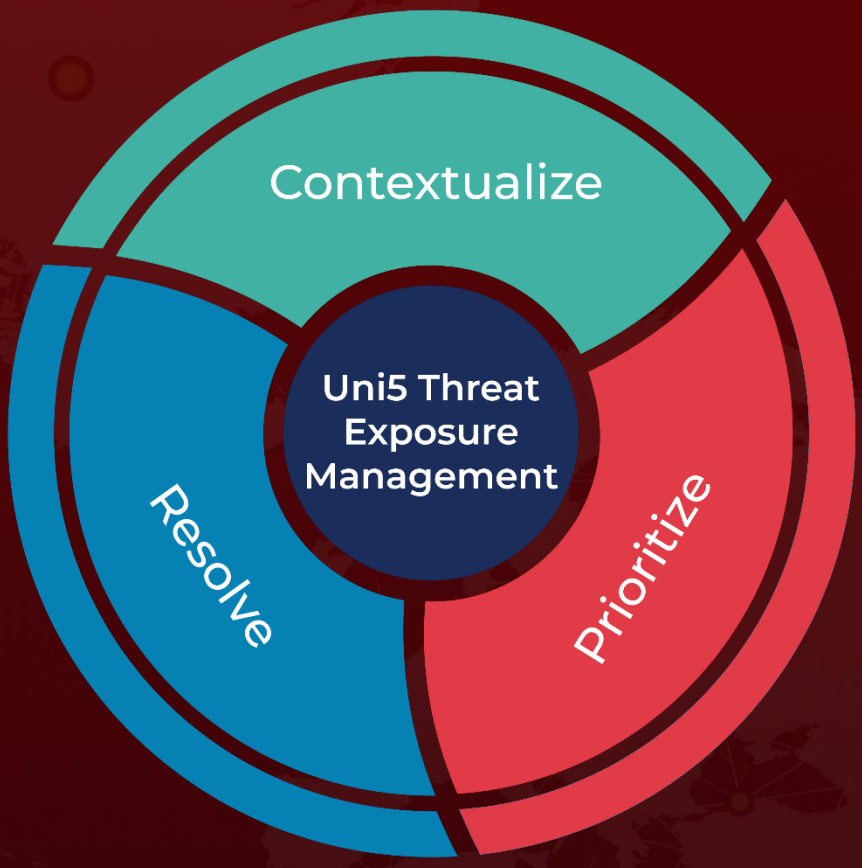
https://attack.mitre.org/groups/G0121/

https://www.hivepro.com/sidewinder-apt-groups-new-arsenal-named-warhawk/

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

May 11, 2023 • 4:21 AM

More at www.hivepro.com