Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

SideWinder's Growing Focus on Maritime and Nuclear Entities

Date of Publication

March 11, 2025

Admiralty Code

A1

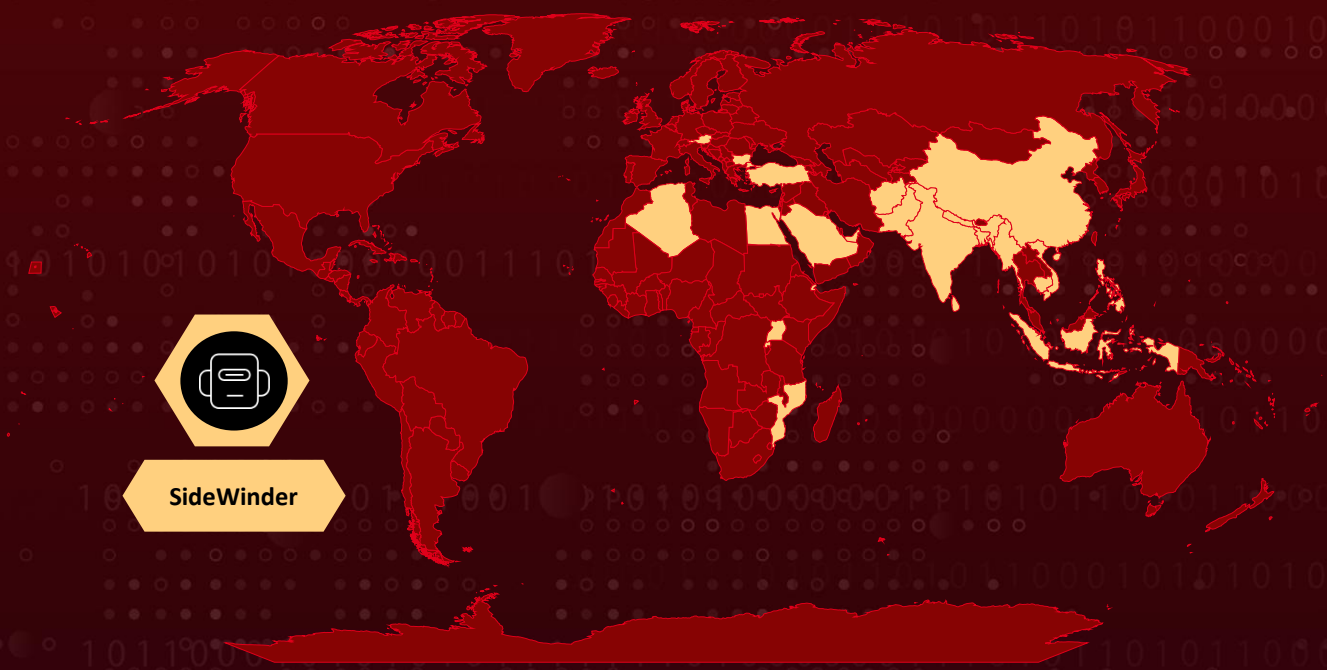
TA Number

TA2025073

Summary

Attack Commenced: 2024
Targeted Countries: Pakistan, Sri Lanka, India, Nepal, Bangladesh, Myanmar, Indonesia, Cambodia, Philippines, Vietnam, Egypt, Saudi Arabia, United Arab Emirates, Turkey, Algeria, Djibouti, Mozambique, Rwanda, Uganda, Austria, Bulgaria, Afghanistan, Maldives, and China
Malware: StealerBot
Threat Actor: SideWinder (aka Razor Tiger, Rattlesnake, T-APT-04, APT-C-17, Hardcore Nationalist, HN2, APT-Q-39, BabyElephant, GroupA21)
Targeted Industries: Government, Military, Defense, Logistics, Maritime, Nuclear, Energy, Telecommunications, Consulting Firms, IT Service, Real Estate, and Hospitality
Attack: SideWinder, a persistent APT group, continues targeting government, military, maritime, and nuclear sectors across Asia, the Middle East, and Africa. Their attack chain begins with spear-phishing emails exploiting CVE-2017-11882 to deploy StealerBot, enabling espionage via credential theft, keylogging, and file exfiltration. The group rapidly evolves its malware to evade detection, often modifying tools within hours. Strong security measures, including patch management and phishing awareness, are crucial to countering this threat.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓

Attack Details

#1

SideWinder, a highly active APT group, continues to target government, military, and logistics sectors, expanding its operations across South and Southeast Asia, the Middle East, and Africa. Their attacks in 2024 have intensified, particularly against maritime infrastructures and nuclear energy entities, with a notable focus on Djibouti and Egypt. The group has also expanded its efforts into Africa, demonstrating a persistent and evolving threat to high-profile organizations.

#2

The attack chain begins with a spear-phishing email containing a malicious DOCX file that exploits the CVE-2017-11882 vulnerability via remote template injection. Upon opening, the document downloads an RTF exploit, which executes malicious shellcode using mshta.exe to fetch and execute a JavaScript-based dropper. This dropper then downloads additional malware components, initiating a multi-stage infection process.

#3

To establish persistence, the malware deploys a Backdoor Loader, which is sideloaded by legitimate signed applications. This loader drops an encrypted file while also modifying system settings, such as registry values and scheduled tasks, to maintain access. The encrypted file loads StealerBot, an advanced orchestrator that communicates with a command-and-control (C2) server, enabling remote control over infected systems.

#4

Once installed, StealerBot activates additional plugins that provide extensive espionage capabilities, including credential theft, keylogging, file exfiltration, screenshot capturing, RDP credential stealing, and UAC bypass techniques. These tools allow SideWinder to maintain persistence while continuously improving its malware to evade detection, often modifying its toolset within hours in response to security countermeasures. Given SideWinder's ability to quickly adapt and maintain long-term access to critical infrastructures, organizations must implement robust security measures.

Recommendations

Patch Management: Regularly update and patch all software, especially addressing known vulnerabilities like CVE-2017-11882, which SideWinder exploits.

Email Security and User Training: Deploy advanced email filtering solutions to detect and block spear-phishing attempts. Conduct regular cybersecurity training to educate employees on recognizing and avoiding phishing emails and malicious attachments.

Endpoint Protection: Utilize robust endpoint security solutions capable of detecting and preventing malware infections, including advanced persistent threats. Ensure these solutions are regularly updated to recognize the latest threats.

Network Security Measures: Implement network security tools, such as firewalls and intrusion detection/prevention systems, to monitor and control network traffic. For example, configuring devices that has explicit forward proxies can help inspect outgoing HTTP traffic and block communications with known malicious domains and IP addresses associated with SideWinder's operations.

Potential MITRE ATT&CK TTPs

TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command and Control
TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access
TA0001 Initial Access	TA0002 Execution	TA0040 Impact	T1584 Compromise Infrastructure
T1566.001 Spearphishing Attachment	T1566 Phishing	T1204 User Execution	T1547.001 Registry Run Keys / Startup Folder

T1547 Boot or Logon Autostart Execution	T1053.005 Scheduled Task	T1204.002 Malicious File	T1053 Scheduled Task/Job
T1027 Obfuscated Files or Information	T1218.005 Mshta	T1218 System Binary Proxy Execution	T1574.002 DLL Side-Loading
T1548 Abuse Elevation Control Mechanism	T1003 OS Credential Dumping	T1574 Hijack Execution Flow	T1059 Command and Scripting Interpreter
T1548.002 Bypass User Account Control	T1056.001 Keylogging	T1056 Input Capture	T1047 Windows Management Instrumentation
T1555 Credentials from Password Stores	T1012 Query Registry	T1113 Screen Capture	T1059.007 JavaScript
T1059.003 Windows Command Shel l			

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	e9726519487ba9e4e5589a8a5ec2f933, d36a67468d01c4cb789cd6794fb8bc70, 313f9bbe6dac3edc09fe9ac081950673, bd8043127abe3f5cfa61bd2174f54c60, e0bce049c71bc81afe172cd30be4d2b7, 872c2ddf6467b1220ee83dca0e118214, 3d9961991e7ae6ad2bae09c475a1bce8, a694ccdb82b061c26c35f612d68ed1c2, f42ba43f7328cbc9ce85b2482809ff1c, 0216ffc6fb679bdf4ea6ee7051213c1e, 433480f7d8642076a8b3793948da5efe

TYPE	VALUE
Domains	pmd-office[.]info, modpak[.]info, dirctt888[.]info, modpak-info[.]services, pmd-offc[.]info, dowmloade[.]org, dirctt888[.]com, portdedjibouti[.]live, mods[.]email, dowmload[.]co, downl0ad[.]org, d0wnlaod[.]com, d0wnlaod[.]org, dirctt88[.]info, directt88[.]com, file-dwnld[.]org, defencearmy[.]pro, document-viewer[.]info, aliyum[.]email, d0cumentview[.]info, debcon[.]live, document-viewer[.]live, documentviewer[.]info, ms-office[.]app, ms-office[.]pro, pncert[.]info, session-out[.]com, zeltech[.]live, ziptec[.]info, depo-govpk[.]com, crontec[.]site, mteron[.]info, mevron[.]tech, veorey[.]live, mod-kh[.]info
SHA256	d9e373aeea5fe0c744f0de94fdd366b5b6da816209ac394cbbda1c64c03b50b1, 865f5b3b1ee94d89ad9a9840f49a17d477cddfc3742c5ef78d77a6027ad1caa5, fa95fadc73e5617305a6b71f77e9d255d14402650075107f2272f131d3cf7b00,

TYPE	VALUE
SHA256	aacaf712cf67176f159657be2fbd0fce018aa03b890cb1616b146eddb1de73be, 512a83f1a6c404cb0ba679c7a2f3aa782bb5e17840d31a034de233f7500a6cb9, 57d761453bbc6ba9ace467f4491d7a19b9c7e097f81d9772efbcd2f43ada4dce, a84b3dd5f7d29d8d257fdef0ede512ae09e6cd5be7681b9466a5c60f6f877c2b

Patch Link

https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2017-11882

References

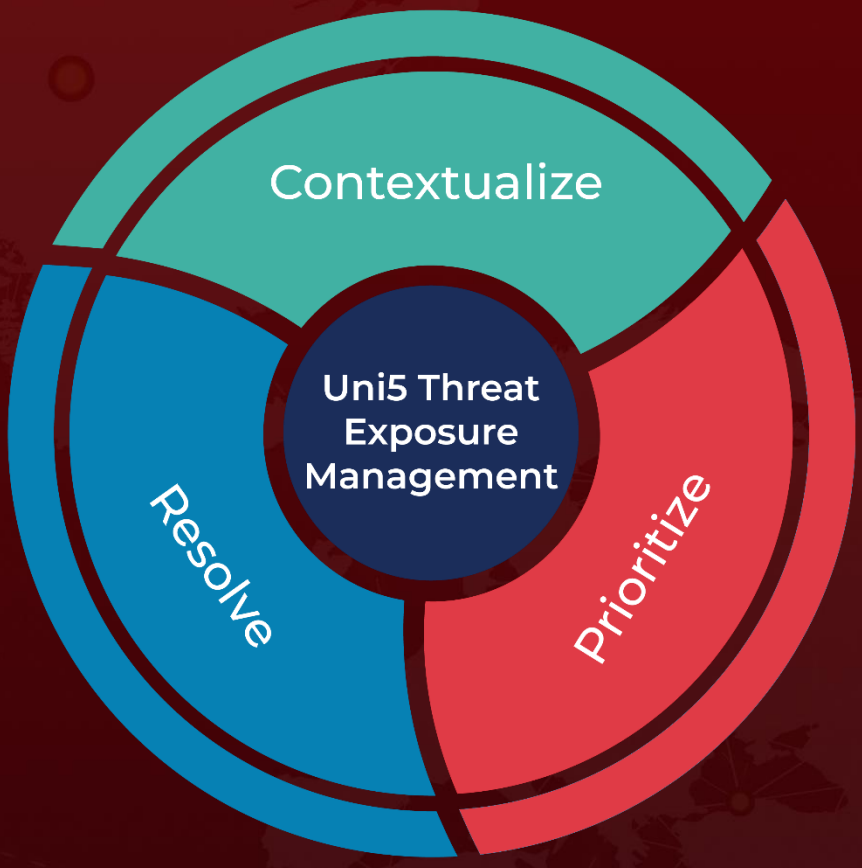
https://securelist.com/sidewinder-apt-updates-its-toolset-and-targets-nuclear-sector/115847/

https://www.hivepro.com/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

March 11, 2025 • 9:30 PM

More at www.hivepro.com