Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

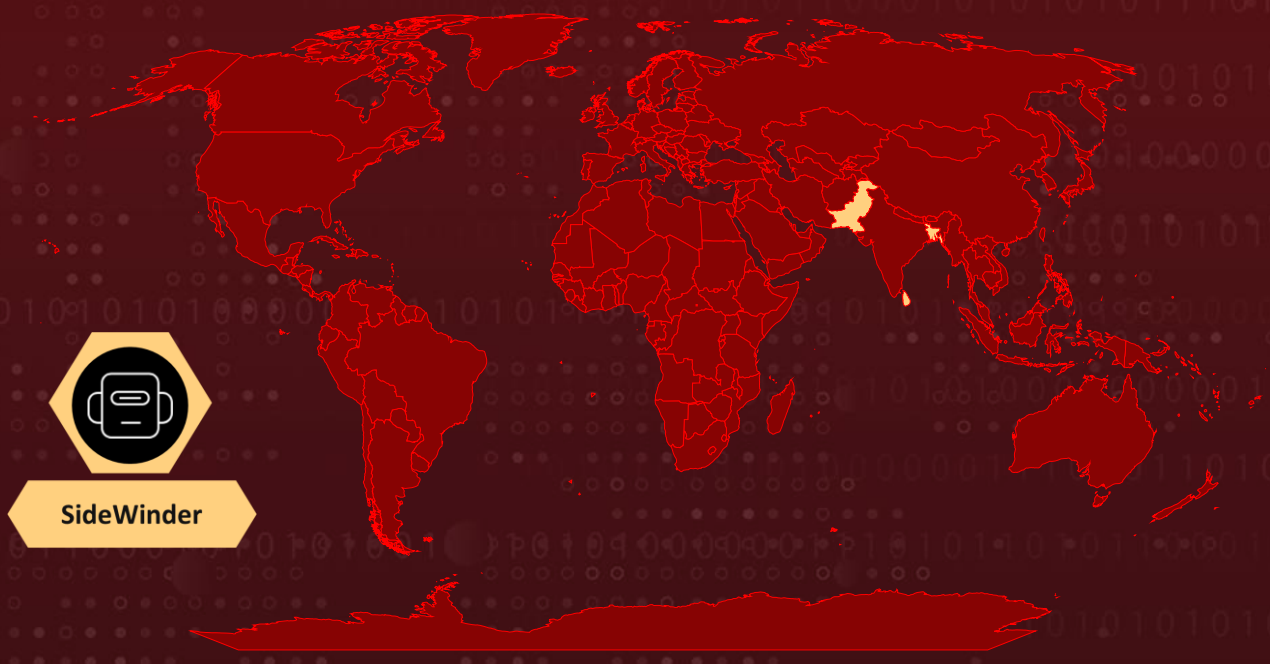
SideWinder's Silent War Using Old Exploits on New Targets

Date of Publication	Admiralty Code	TA Number
May 21, 2025	A1	TA2025157

Summary

Attack Discovered: 2025
Targeted Countries: Sri Lanka, Bangladesh and Pakistan
Affected Industries: Government Institutions, Military Institutions, Banking
Malware: StealerBot
Actor: SideWinder (aka Rattlesnake, Razor Tiger, T-APT-04, APT-C-17, Hardcore Nationalist, HN2, APT-Q-39, BabyElephant, GroupA21)
Attack: SideWinder is back with a highly targeted cyberattack campaign across South Asia, aiming at government and military institutions in countries like Sri Lanka, Bangladesh, and Pakistan. Using old but still dangerous Microsoft Office flaws, the attackers deliver stealthy, multi-stage malware that steals credentials and maintains access for long-term espionage. What makes this campaign stand out is how SideWinder mixes techniques like shellcode-based loaders, DLL sideloading, and fast-changing command-and-control domains to stay under the radar.

Attack Regions



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2017-0199	Microsoft Office and WordPad Remote Code Execution Vulnerability	Microsoft Office and WordPad	✓	✓	✓
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓

Attack Details

#1 SideWinder, a persistent threat actor with a history of cyber-espionage across South Asia, has once again launched a highly targeted campaign aimed at sensitive government and military sectors. This time, the group has been seen exploiting old but still dangerous Microsoft Office vulnerabilities (CVE-2017-0199 and CVE-2017-11882) to infiltrate systems in countries like Sri Lanka, Bangladesh, and Pakistan. These security flaws allow attackers to remotely run code on a victim's machine just by getting them to open a malicious Word document an approach that continues to work against organizations running outdated software.

#2 The campaign shows SideWinder's shift from older delivery methods like mshta.exe to more sophisticated shellcode-based loaders. These loaders are delivered through fake but convincing documents, often tailored for each target, such as military units or central banking institutions. In one instance, specific targets included the Sri Lanka Army's 55th Division and the Central Bank of Sri Lanka. The attackers also craft fake domains that mimic legitimate government or military sites to lure their victims into opening malicious attachments.

#3 Once the victim opens the booby-trapped file, a decoy document is loaded while a hidden script quietly triggers the next stage. The embedded shellcode checks if it's in a virtual or sandbox environment a common tactic used to evade detection during analysis. If it's running in a real system, it reaches out to attacker-controlled servers to download an encoded payload. This malicious code is then injected into a legitimate system process, like explorer.exe, which helps it hide and avoid raising red flags.

#4 The payload includes a tool called StealerBot, which gathers system information, checks for antivirus software, and sends data back to the attackers. It uses sneaky tricks like base64 encoding, XOR encryption, and hiding in DLL files that are loaded by trusted Windows applications (like TapiUnattend.exe). One of the clever ways SideWinder ensures persistence is by placing shortcuts in the Windows Startup folder so the malware survives reboots and remains active on the system.

#5 What's especially concerning is SideWinder's ability to adapt and evolve. Even while relying on older exploits, the group keeps refining its delivery methods, payload obfuscation, and infrastructure. In January 2025 alone, they registered or repointed 34 domains for command-and-control operations, making it hard for defenders to block their activities. This campaign is a reminder that unpatched software is still a golden opportunity for advanced threat actors and that even legacy vulnerabilities can be used in very modern, targeted attacks.

Recommendations

- **Patch Immediately:** Ensure that Microsoft Office and all associated components are fully updated. Vulnerabilities like CVE-2017-0199 and CVE-2017-11882 are old but still dangerous attackers rely on outdated software to gain access. Regularly update all systems.
- **Disable Unused Office Features:** Disable support for legacy features like the Equation Editor and external OLE object loading in Microsoft Office. These components are often abused to run malicious code in phishing documents.
- **Strengthen Email Security:** Deploy advanced email filtering solutions that can detect and block weaponized attachments, malicious macros, or unusual file formats. Train staff to recognize suspicious emails, even those that look official or come from trusted names.
- **Implement Application Whitelisting:** Restrict which applications can run on endpoints, particularly preventing unsigned or unknown DLLs and executables from being executed, especially from temp or user directories.
- **Enhance Endpoint Protection:** Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0043 Reconnaissance	TA0001 Initial Access	TA0002 Execution
TA0003 Persistence	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery
TA0010 Exfiltration	TA0011 Command and Control	T1588 Obtain Capabilities	T1588.006 Vulnerabilities
T1190 Exploit Public-Facing Application	T1566 Phishing	T1566.001 Spearphishing Attachment	T1574 Hijack Execution Flow
T1574.001 DLL	T1059 Command and Scripting Interpreter	T1218 System Binary Proxy Execution	T1218.005 Mshta
T1036 Masquerading	T1656 Impersonation	T1590 Gather Victim Network Information	T1218.011 Rundll32
T1140 Deobfuscate/Decode Files or Information	T1082 System Information Discovery	T1132 Data Encoding	T1132.001 Standard Encoding
T1518 Software Discovery	T1518.001 Security Software Discovery	T1027 Obfuscated Files or Information	T1547 Boot or Logon Autostart Execution
T1547.001 Registry Run Keys / Startup Folder			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	725ded50e7f517addd12f029aeaf9a23f2b9ce6239b98820c8a12ea5cb79dbfa, 57b9744b30903c7741e9966882815e1467be1115cbd6798ad4bfb3d334d3523d, 558de2a01fbd76be171561c3c82fd6a8e2d4c913444850af99d44a4cfb41b680, f464ad5c6aba13b42aa903bda0add7c074d45388da379747c83f2c3756c9b658, 63f5445527c47e17b71e87eef4dd7a86883607a22830bcee5b1fabc5d03bab38, 65c9e15d9b916b193ce1d96bb99c1c1f3ade0273270b56cf6e476a21b31a3491, 7363887b6b0fe7cece3c21ad18515835922379c7d78c47cea745940a1061a6c4, 40712a087a8280425f1b317e34e265c0329ffb0057be298d519fc5e0af6cb58f, 69eee36642f274c724fadcfdf1f103ae0fd9b5f4bad7ac6a33b3c627d6114426, 2d92d24b3abed7acac165b002bd5922f8f17b6e4944e658938fe022902fe6a7e, 663a7b509db86ca498af57cc458139a76ee07c60d413d60a98921c7e901e0e3d, 5ec639facb2cb9503059d519790279f1b9f510d8d63a2a2c44637b1d1dd1e538, 0a7fce4e7456ecb12c95d28b6b4d263d9ca23a1de1e298234a904a319be6e708, 00877fcfb31fdc23ca6987e569090f761ed414bdee0546bdbd3ce3acc44cc293, 8d00c97d16e3733feee6b1bc6bd77b8423e0b79a812db55880f5b2d751a4bd47, dc7066d972367f15c9b6e2e36a5c643ab87deed958cc27ac0fbf0ff1f4535a99, 8dd189e390b168bff6caa82d5077f4eda8902c251fe0a0120aa42bd78e56f9bc, 46785f7e5cd2966d30167cbd496333a5dd871b19e6a2833ab1a4157fc35e8ee5, ac13697c19cf0b6767442fc001ca48d0d9e3c9340549d3e73539ea299e27015e, 32e2d29143f57335c6477dc764350fed13b7e3873fb06491d9863a95b8921e92, ffebc5f8fc3a0346f9767c64b5b040d7679e1d3726024e59fe134825e31c8b8c, 208c335a3cccbdba6b1ec0c76ad3b751c6409712e493c24e2532a389d887e0af,

TYPE	VALUE
SHA256	a90fd0e3d3be14b92b3dc809ddea9a0cc377b130ebb4c48a8891e4832a85c412, fa5a3e215e4970b0c39b6bbfb9425aa6ee4a8bc1359d85f7052d99e663aee333, bb9acc2d23afee3265b81326ce65cfddde3fc04648d3ba2d2ea22ec0e3d8f90e, 5b5a1833d4daaf05699a009316a4d866851130b258f424f066b867a534ba944d, 9b76d98c2641512c66e8f2f99b2d0bda86ec1a4809420b74feadfb8f4f7dbf48, fb4695b45ac62e10f29e9a45c4190dce2fe6af71a96a2bd66e08c1a99416cc7e, 677b4d9efcfcae9cbbd39b2b2cdc0df69d4a55460814747f60f35ea2e81dad2e, 2be8ca1e2415b5ca1605977b2ff10ff9aef06e3be7eb39496bb18d3ba7772901, 1c68ca3ede75946568bb00c39b7054cb2ae4fcbe2805061e38ed15f4d526262c, 9700f9b614aa87c6137c4325951e59258cdb87f02df7a5ed4f4accea279ede26, 74111c9b0ed748fc6bfc025d13a2ed08663b988cb69c044f1c6f153f9020294c, a61335c10cf98064761806af6451b3cddd66641ccb35a6d8b915a02d6279f46a, 1527cf10f00c798262b3347c00af8028fee3bc88a450bc2df7766b1118c62cd5, 5891f4dfa47d5b268c5d82366c312ecda715da91e148afa6064f3058f3c5a69b, e33e74e3925bc3f287ef817a186807a38d411524984a5d0930939646022206b0, 1321fc1eefc3d3f5aae16a81ac139a31beaf2355935d94210abf69253d29b486, 96d429d67a2663ef2cf3f45ccd0619adf0cd030f7fe70f072af1ce1d67ec52a3, 22527dd1a62dc46dd4edd23a681657cf4c3477e9f90fb1ef63ef657608b9838c, fb50c60c237ea00f29e4876b326f5f8e872f5ad6d1ca7c9925d9b901e573f788, de54f8933ff81f93652ab824e8f9e60197135e1064f0ca4ca99df833a7a94e9d, 47d77499968244911d0179fb858578de00dbb98079e33f5ed5d229d03eb04d67, ffd26019b21da5833caf2b6974cbc9ce79d911653cdfbb6e59a8ac7d4cc80f51, 15cf5271c7b9b8ad22c4c96bc8674d9835e8d419fc1a6077f3b59fbd7e59d112,

TYPE	VALUE
SHA256	54c4641f709e51622531dc3d04fd2f4a3bad2a42dca287e2777c04d59cbca789, d3fb61c0211bd379bf80f15cf072fdbc1187fe95546fdfcfcbdf8918004f05e2, 35cc327806ae0d760b94a5b3daedea9cdcb2ed0854a484c8ec3cded195e75037, 896ddb35cde29b51ec5cf0da0197605d5fd754c1f9f45e97d40cd287fb5a2d25
Domains	army-govbd[.]info, updates-installer[.]store, dwnlld[.]com, bismi[.]pro, viewdoc[.]online, dwnlld[.]info, net-co[.]info, milqq[.]info, vpdf[.]online, org-co[.]net, nic-svc[.]net, live-co[.]org, org-liv[.]net, net-src[.]info, info-lanka[.]org, onlinestatus[.]live, modpak[.]live, mail163[.]info
URLs	advisory[.]army-govbd[.]info, geninstr[.]army-govbd[.]info, advisary[.]army-govbd[.]info, amended[.]army-govbd[.]info, mail[.]army-govbd[.]info, emv1[.]army-govbd[.]info, www[.]army-govbd[.]info, pimec-paknavy[.]updates-installer[.]store, hisidewinderSideWinder[.]pimec-paknavy[.]updates-installer[.]store, imec-paknavy[.]updates-installer[.]store, www-presidentsoffice-gov-lk[.]dwnlld[.]com, www-cbsl-gov-lk[.]dwnlld[.]com, email[.]sco[.]gov[.]pk[.]viewdoc[.]online, mod-gov-bd[.]dwnlld[.]info, moitt-gov-pk[.]dwnlld[.]info, mfa-gov-lk[.]dwnlld[.]info, www-cbsl-gov-lk[.]dwnlld[.]info, prison-gov-bd[.]dwnlld[.]info, bscic-gov-bd[.]dwnlld[.]info, cabinet-gov-bd[.]dwnlld[.]info,

TYPE	VALUE
URLs	fa-gov-lk[.]dwnlld[.]info, infomfa-gov-lk[.]dwnlld[.]info, mofa-gov-bd[.]dwnlld[.]info, www-cbsl-gov-lk[.]dwnlld[.]infomfa-gov-lk[.]dwnlld[.]info, www-erd-gov-lk[.]dwnlld[.]info, xcfhg[.]dwnlld[.]info, mof-gov-np[.]dwnlld[.]info, 6441056b613c32a9[.]dwnlld[.]info, www[.]dwnlld[.]info, dwnlld[.]infomfa-gov-lk[.]dwnlld[.]info, customs-gov-lk[.]net-co[.]info, postmaster[.]net-co[.]info, www[.]customs-gov-lk[.]net-co[.]info, jtops[.]milqq[.]info, dirsports[.]milqq[.]info, mail[.]ntc[.]net[.]pk[.]vpdf[.]online, pubad-gov-lk[.]org-co[.]net, a5936441-e402-41e3-b02b-75af112074b5[.]org-co[.]net, esxipubad-gov-lk[.]org-co[.]net, mof-gov-bd[.]nic-svc[.]net, lolsidewinderSideWinder[.]nic-svc[.]net, wwww[.]nic-svc[.]net, www-erd-gov-lk[.]nic-svc[.]net, www[.]treasury-gov-lk[.]nic-svc[.]net, treasury-gov-lk[.]nic-svc[.]net, mail-mofa-gov[.]org-liv[.]net, pubad-gov-lk[.]org-liv[.]net, cabinet-gov-bd[.]org-liv[.]net, cirt-gov-bd[.]org-liv[.]net, gov-lk[.]org-liv[.]net, mod-gov-bd[.]org-liv[.]net, www-treasury-gov-lk[.]org-liv[.]net, pubad-gov-lk[.]live-co[.]org, mofa-gov-bd[.]live-co[.]org, mod-gov-bd[.]live-co[.]org, data-sob-gov-bd[.]live-co[.]org, 7ef1996f-c463-4540-936a-70d0fd477f98[.]live-co[.]org, mofa-gov-np[.]live-co[.]org, mofa-gov-np[.]org-liv[.]net, pubad-gov-lk[.]net-src[.]info, probashi-gov-bd[.]net-src[.]info, mofa-gov-np[.]net-src[.]info, modltr[.]info-lanka[.]org, www[.]info-lanka[.]org, mail[.]nepla[.]gov[.]np[.]onlinestatus[.]live, mail[.]ntc[.]net[.]pk[.]onlinestatus[.]live, mail[.]paf[.]gov[.]pk[.]onlinestatus[.]live,

TYPE	VALUE
URLs	mail[.]pof[.]gov[.]pk[.]onlinestatus[.]live, paknavy[.]modpak[.]live, interior-gov-pk[.]mail-govt[.]org, www-cabinetoffice-gov-lk[.]mail-govt[.]org, probashi-gov-bd[.]mail-govt[.]org, gso2[.]mail163[.]info

Patch Links

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

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

References

https://www.acronis.com/en-us/cyber-protection-center/posts/from-banks-to-battalions-sidewinders-attacks-on-south-asias-public-sector/

https://hivepro.com/threat-advisory/sidewinders-growing-focus-on-maritime-and-nuclear-entities/

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 21, 2025 • 5:30 AM

More at www.hivepro.com