Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

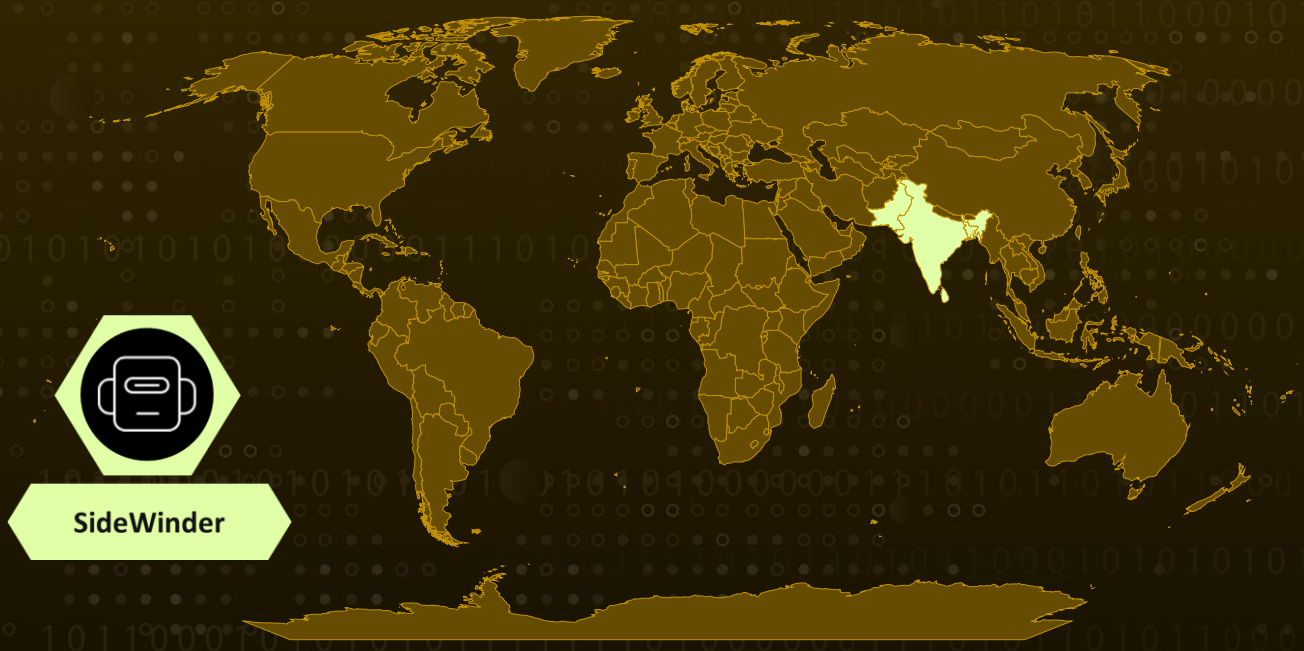
ClickOnce Deception: SideWinder's New Path to Diplomats

Date of Publication	Admiralty Code	TA Number
October 29, 2025	A1	TA2025330

Summary

Attack Discovered: March 2025
Targeted Countries: Sri Lanka, Pakistan, Bangladesh, India
Targeted Industry: Diplomats
Malware: ModuleInstaller, StealerBot
Actor: SideWinder (aka Rattlesnake, Razor Tiger, T-APT-04, APT-C-17, Hardcore Nationalist, HN2, APT-Q-39, BabyElephant, GroupA21, G0121)
Attack: SideWinder has launched a highly targeted espionage campaign across Asia, using realistic diplomatic and government-themed documents to trick officials into installing what looks like legitimate Adobe Reader updates, but which actually initiate a ClickOnce-based attack that silently downloads and runs a malicious application. That ClickOnce chain sideloads weaponized DLLs and unpacks a multi-stage loader that ultimately deploys modular spyware such as ModuleInstaller and StealerBot to harvest sensitive files and credentials. Combined with geofenced payload delivery, rapidly shifting domains, and social-engineering tailored to regional politics, this technique lets the group blend into trusted workflows and quietly exfiltrate data, underscoring how SideWinder has sharpened its operational tradecraft.

Attack Regions



Attack Details

#1 In September 2025, a new phishing campaign was discovered targeting a European embassy in New Delhi, and soon after, similar attacks were seen against government and diplomatic groups in Sri Lanka, Pakistan, and Bangladesh. The activity was linked to SideWinder, a long-running espionage group in Asia known for constantly changing its methods. This time, they shifted to using malicious PDFs and ClickOnce applications instead of relying only on Microsoft Word exploits as they did before. This technique first started appearing in March, but the attacks found in September show a new and more aggressive wave focusing on diplomatic targets.

#2 The attacks unfolded in multiple themed waves throughout 2025; each tailored to local geopolitical interests to boost credibility. Bangladeshi organizations received fraudulent Hajj training and registration files, while Pakistani diplomats were lured with defense procurement and political appointment documents embedded with malicious payloads. In these waves, SideWinder re-employed the well-known **CVE-2017-0199** vulnerability in Microsoft Word to deliver malware. Sri Lankan targets later received documents referencing defense personnel transfers and promotions, and a final wave struck embassy officials in India with documents related to bilateral conflicts and diplomatic meetings. Spoofed domains mimicking official government entities added another layer of deception to the operation.

#3 The most notable innovation appeared in the malicious PDF chain. Victims were encouraged to install a fake Adobe Reader update, which silently downloaded a signed ClickOnce application disguised with Adobe-style branding. Behind this legitimate appearance, altered internal components sideloaded a tampered DLL (DEVOBJ.dll), launching a multi-stage process that decrypted and executed additional payloads. This eventually deployed SideWinder's familiar espionage toolkit, including ModuleInstaller and the StealerBot malware, which can load further plugins based on operational needs.

#4 SideWinder demonstrated strong operational security throughout the campaign. Payloads were geofenced to specific countries, URLs changed dynamically for each session, and malicious files disappeared quickly after delivery, all tactics designed to hinder detection and forensic analysis. Additionally, the use of lookalike government domains blurred attribution and challenged defenders attempting to trace the activity back to its source.

#5 This campaign highlights SideWinder's steady escalation in sophistication, blending legitimate software with stealthy infection methods while exploiting trust in local government communications. With their apparent focus on sensitive regional politics and diplomatic intelligence, South Asian institutions remain high-priority targets. Strengthening email filtering, enhancing endpoint monitoring, and building awareness around socially engineered lures are crucial steps to mitigate the growing risk posed by this persistent threat actor.

Recommendations

- **Be cautious with email attachments:** Even if a message looks official or urgent, verify the sender before opening any PDF, Word file, or clicking Update buttons inside documents. When in doubt, contact the sender through a trusted channel.
- **Block fake software updates:** Disable automatic prompts from documents that ask users to install an "Adobe Reader update" or any app outside your organization's approved software list.
- **Keep systems and Office applications up to date:** Old vulnerabilities like CVE-2017-0199 are still being exploited. Regular patching closes those doors for attackers.
- **Use network-based controls:** Restrict or monitor outbound traffic to unknown domains, especially newly registered ones, to block malware from reaching its command servers.
- **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

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0004** Privilege Escalation
TA0005 Defense Evasion	**TA0007** Discovery	**TA0009** Collection	**TA0011** Command and Control
TA0010 Exfiltration	**T1566** Phishing	**T1566.001** Spearphishing Attachment	**T1204** User Execution
T1204.002 Malicious File	**T1547** Boot or Logon Autostart Execution	**T1547.001** Registry Run Keys / Startup Folder	**T1053** Scheduled Task/Job

T1053.005 Scheduled Task	T1134 Access Token Manipulation	T1134.001 Token Impersonation/Theft	T1087 Account Discovery
T1574 Hijack Execution Flow	T1574.001 DLL	T1140 Deobfuscate/Decode Files or Information	T1027 Obfuscated Files or Information
T1027.008 Stripped Payloads	T1027.009 Embedded Payloads	T1027.013 Encrypted/Encoded File	T1027.016 Junk Code Insertion
T1218 System Binary Proxy Execution	T1082 System Information Discovery	T1016 System Network Configuration Discovery	T1518 Software Discovery
T1518.001 Security Software Discovery	T1083 File and Directory Discovery	T1012 Query Registry	T1652 Device Driver Discovery
T1005 Data from Local System	T1119 Automated Collection	T1560 Archive Collected Data	T1560.002 Archive via Library
T1071 Application Layer Protocol	T1071.001 Web Protocols	T1573 Encrypted Channel	T1573.002 Asymmetric Cryptography
T1105 Ingress Tool Transfer	T1090 Proxy	T1041 Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	06da4a5755a81785f68caf75cca2b7a41c3aa9b4af24d2bb93964abf87343869, 09b96a2426f8ddcc20aa58a72ad147d410525f1a4a42835b7ece126211537b3b, 0f407b9b1cffa88edfe5a439f316dd41eea2fc47ba24a8dd986a6ffe520cb66b, 32febd24765e996c8f01f77f02b02af3e35914ea215f98fcf2054a15a5bb0262, 341a21538b90c87b40e150967519a695f2c339befde232e2f3cd85caf6885803, 4e984a01dee63ca0a7fb1efa42a483d2e378e8f87896c76788f11abe8ddeec3c,

TYPE	VALUE
SHA256	5f8cdb9a5000a4d4ab08255efb3bd0c074551df94ebff820510078b45ad0b9f1, 7d51aba5a9bbad297c05a0a3b99aa32af354b45ad2e99191fe0e611c9f44dfa4, 8183a28cc1d962c173d5a63d1b61acafd995e6f0c4f595d6f0e43988b88c480b, 81dda6e8d6835980aaa3fa26b1ee4a8d7931fea7c33caf5f639a1057ad39add1, 84ddd27b18b7401fd46149c60b0fff4ea0f01ba8668649dc246769784bc7a00d, aaf08583c38289e617cfaae8bd42aa4ce48a0d7c9e401e9cb4cbfa6fb65e4935, f6e54fd80aa4f8b779f2fb85466c7e6d4f9c2dbd0a79d0d8e9d1f275654e51c5, 36f7db22dbd834d0bbffbd1c7647101604054a2d1595ea0baf106a4da7d5fefb, 54ef2aaeeb850c07cf3e01754478da2b8947b7188e1aabc8dd7eb54c78b55bd1, 632d1e049e74e3cc34f01fa7d4b4e18e8679636eb58e38756b8ed0314a861a02, aa7c242c325528bbb6184a603b4b0ae2b67711b774e2400f1fe086e0d5eb66bc, 65125a51edf9e2ab776bc041b77267dc04045bf4f6df03138494966cee9f5a54, c67ee29964506676bde38e7732e720078abdb0adebc743a367a5d9a1215f5020, be4916940676befe86749c8a9b156346fa80ce6c0a341ab59dfd49344ef8162b, 71409564792f503c4ec6c5000d98ac4a97a153d4c16cc6f6528c136271bc8ed8, dd30478a1f2e822d3e9be536ca249e1c677ccaf1106fb9a9f41003e2bb609d09, 39eba7eeadab00b4552cc42550dd285f7b3c5fbf451634ce0f6458d61d0b1aed, e4d494948ce5c81e600ca36d3c35007f371cceef7e2c16addf2668bed1533efb, f022b5b6ef036bed3c4e4fef2dc8a703cd51146cf449c0be48fa963a62eba752, a28135ad1294328cbf0b200f7fa4ad7a0691bd80fb87e88b348c396fa652aa10, d2c8d33ea2d855bc9cd52d3a4d312c81f848c4f5afb9414ee90b036f3f27a4a4, 6226704e0cbe5b17c50bfbdb79912028137abf1f0f918fd455d9a71ed4478fcf, f4f851ed2a972e2c90ea20a1d8a2421111264022700caab82e42b89e80bc321a,

TYPE	VALUE
SHA256	ce72830bc037680d9ef50d328f3776d2bddf5aaffd077d2d884efafa3e30ee70, 3ffc09dda86b9c78028f20d5447616c4e60f7c70e2f3cabcc05c77ee8a92f7ce, e091d16488b1b638a2c0013e761d341a04728de4de4388827e62f8c039f77fbc, e5cd4c5e6c35c07b7d1a078ed801a5676d529d41dcbecacd13f744b2c79fe46d, 52602351cf896d44156016e44e2342d4eb75140b7415eaab3f629636d315fb1a, 8435f374161bcf63175e34fc331957c2661d2e83bbd55675b3a103a5cc2ed7c5, d4c746c27873a016c7d3d6d00400c60824afd1cd69840a76873096cbadb23a48, 2d988506cf300236b57744d16adea07525d7b709a0fbf181810143d89aa55017, 635e8abd8ce13a985229e5a0269096a272beef15307333f63cbc95cd13a71e88, 65bc2a15dd4201ddcec44cd02cfeea16c7734a0bd009c977ca5a3c6738c57ae6, c5c07c258ceb91ccba50428dc81c87f5eb0bb13dd6abde82811baa56d1be60fc, cf739fe6621968e2fd7d1ce4a7c513bf4b994a66f33bbc9b53b26672046aa77e, a8b4fcfed3dc3b25e5b9ad34c9f6909f4cc4bedb4606416a672d1a39976e1c5d, 8d85e13eb217dde0b1c770743b1e9d033ff3c6d26186d70ffb0e9246ffc2dc6f, c1093860c1e5e04412d8509ce90568713fc56a0d5993bfdb7386d8dc5e2487b6, 09cfec5b9cc3ef5939287fdb8b1bcb9a8a7185e45ef587a96f35744c02c0f03c, b06aa054491e7b07f54edced19ff648322427b8f5cfa6b46656667c9b40b7215, 31c7381c90b852b4cb858a4fb0a548f7c38ea134eb49a679a83ae2de9f8d98e2, 922bb79cbb76f2b51d5709500d87a55142a38368b4289fb5b45c1318c6a31cf6, 56220142f616d5fffacad4e83b3262e0499e96dcdf99fbb6b81cd9178ef97ced, 4d394319bf9952217aab6d5fc5603abeb3a6e06f6026ff80ec5fa5d02b08cd66, b97c5ed08e5072bf7fdf44864c942657dfcaa8c3f4627698e0b87f773d04cd15, 892089dc7e4af5ee4a89a2fd3083e6843ce7bffc94003d233063ba23d779a314, 2ff1eb3d23b32169d5f07b5c4df6ec9a20b543255a3af4c92de2c322455746a9

TYPE	VALUE
URLs	hxxps[:]//adobe[.]pdf-downlod[.]com/updates-b1139620/adobe-reader, hxxps[:]//pubad-gov-lk[.]download-doc[.]net/09c3c5c1/adobe-reader, hxxps[:]//pimec-paknavy[.]updates-installer[.]store/1/7ab8fb0a/adobe-reader, hxxps[:]//www-parliament-lk[.]snagdrive[.]com/e8147089/adobe-reader, hxxps[:]//cadetcollege[.]adobeglobal[.]com/registration/00198727/adobe-reader, hxxps[:]//adobe[.]pdf-downlod[.]com/4dfbdf2b_updates/adobe-reader, hxxps[:]//www-treasury-gov-lk[.]snagdrive[.]com/69570935/adobe-reader, hxxps[:]//hajjtraining2025[.]moragovt[.]net/2a12968d-schedule/adobe-reader, hxxps[:]//pubad-gov-lk[.]download-doc[.]net/41498067/adobe-reader, hxxps[:]//hajjmedicalteam[.]adobeglobal[.]com/bangladesh/73439525/adobe-reader, hxxps[:]//cabinet-gov-pk[.]dytt888[.]net/43098866-circular/adobe-reader, hxxps[:]//hajjmedicalteam[.]adobeglobal[.]com/bangladesh/85758038/adobe-reader, hxxps[:]//pubad-gov-lk[.]download-doc[.]net/8a24a2e6/adobe-reader, hxxps[:]//mos-gov-bd[.]snagdrive[.]com/b80873e7/adobe-reader, hxxps[:]//mofa-gov-bd[.]filenest[.]live/48686010/adobe-reader, hxxps[:]//mod-gov-bd.snagdrive.com/ce692827/adobe-reader, hxxps[:]//mofa-gov-bd[.]filenest[.]live/17070638/adobe-reader, hxxps[:]//mocat-gov-bd[.]filenest[.]live/88555949/adobe-reader, hxxps[:]//mofa-gov-bd[.]snagdrive[.]com/a18939fc/adobe-reader, hxxps[:]//mod-gov-bd[.]snagdrive[.]com/80097355/adobe-reader, hxxps[:]//mofa-gov-bd[.]filenest[.]live/9b156a35/adobe-reader, hxxps[:]//pmo-gov-pk[.]filenest[.]live/17316/1/32349/2/32/0/0/m/files-d5187655/, hxxps[:]//mod-gov-bd[.]snagdrive[.]com/[8_random_hex_values]/adobe-reader, hxxps[:]//mos-gov-bd[.]snagdrive[.]com/[32_random_hex_values]/co/adobe-reader, hxxps[:]//mofa-gov-bd[.]filenest[.]live/[8_random_numeric_values]/adobe-reader, hxxps[:]//www-treasury-gov-lk[.]snagdrive[.]com/[8_random_numeric_values]/adobe-reader, hxxps[:]//www-parliament-lk[.]snagdrive[.]com/[8_random_hex_values]/adobe-reader, hxxps[:]//pubad-gov-lk[.]download-doc[.]net/[8_random_hex_values]/adobe-reader, hxxps[:]//pimec-paknavy[.]updates-installer[.]store/[8_random_hex_values]_1/Microsoft_License[.]rtf, hxxps[:]//pimec-paknavy[.]updates-installer[.]store/1/[8_random_hex_values]/adobe-reader, hxxps[:]//hajjmedicalteam[.]adobeglobal[.]com/bangladesh/[8_random_numeric_values]/adobe-reader, hxxps[:]//cadetcollege[.]adobeglobal[.]com/registration/[8_random_numeric_values]/adobe-reader,

TYPE	VALUE
URLs	hxxps[:]//hajjtraining2025[.]moragovt[.]net/[8_random_hex_values]-schedule/adobe-reader, hxxps[:]//cabinet-gov-pk[.]dytt888[.]net/[8_random_numeric_values]-circular/adobe-reader, hxxps[:]//adobe[.]pdf-downlod[.]com/[8_random_hex_values]_updates/adobe-reader, hxxps[:]//adobe[.]pdf-downlod[.]com/updates-[8_random_hex_values]/adobe-reader, hxxps[:]//pmo-gov-pk[.]filenest[.]live/17316/1/32349/2/32/0/0/m/files-[8_random_hex_values]/, hxxps[:]//pmo-gov-pk[.]filenest[.]live/[8_random_hex_values]-conflict, hxxps[:]//mos-gov-bd[.]snagdrive[.]com/[8_random_hex_values], hxxps[:]//mofa-gov-bd[.]filenest[.]live/[8_random_numeric_values], hxxps[:]//exosel[.]info/202/gYvXAIX6GGFkjJpAVSC5ls2CfMe66s8uwB1X5QZC/32349/17276/59fc0fdf, hxxps[:]//ostcone[.]site/202/q2cBahBKeA3vl6AijbYx1Mz9yAt5a1OvNHPv8api/32349/17303/88efad0d
Domains	mos-gov-bd[.]snagdrive[.]com, mofa-gov-bd[.]filenest[.]live, www-treasury-gov-lk[.]snagdrive[.]com, www-parliament-lk[.]snagdrive[.]com, pubad-gov-lk[.]download-doc[.]net, pimec-paknavy[.]updates-installer[.]store, hajjmedicalteam[.]adobeglobal[.]com, cadetcollege[.]adobeglobal[.]com, hajjtraining2025[.]moragovt[.]net, cabinet-gov-pk[.]dytt888[.]net, adobe[.]pdf-downlod[.]com, exosel[.]info, ostcone[.]site, pmo-gov-pk[.]filenest[.]live
Emails	ds.plann2@mos[.]gov[.]bd[.]pk-mail[.]org, d17@mod[.]gov[.]bd[.]pk-mail[.]org, p2@mofa[.]gov[.]bd[.]pk-mail[.]org, asresearch@mofa[.]gov[.]bd[.]pk-mail[.]org, js.admn@pmo[.]gov[.]pk-mail[.]org, mau@mofa[.]gov[.]bd[.]pk-mail[.]org, secretary@mocat[.]gov[.]bd[.]pk-mail[.]org, pc2@mod[.]gov[.]bd[.]pk-mail[.]org, d11@mod[.]gov[.]bd[.]pk-mail[.]org

References

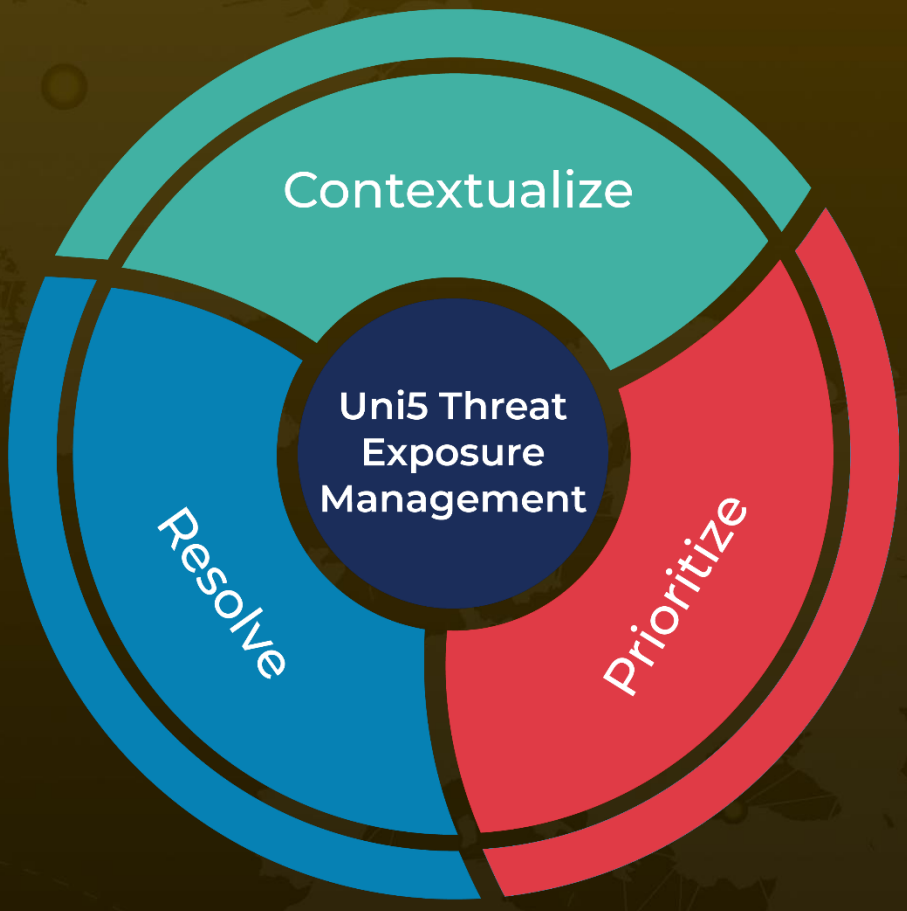
https://www.trellix.com/blogs/research/sidewinders-shifting-sands-click-once-for-espionage/

https://hivepro.com/threat-advisory/sidewinders-silent-war-using-old-exploits-on-new-targets/

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

October 29, 2025 • 8:00 AM

More at www.hivepro.com