Unknown Title

Blogs

The latest cybersecurity trends, best practices, security vulnerabilities, and more

SideWinder's Shifting Sands: Click Once for Espionage

By Ernesto Fernández Provecho and Pham Duy Phuc · October 22, 2025

In September 2025, the Trellix Advanced Research Center (ARC) detected a campaign targeting a European embassy located in New Delhi, India. Further investigation led to the discovery of multiple targeted institutions from various countries, including Sri Lanka, Pakistan, and Bangladesh.

This report examines the tactics, techniques, and procedures (TTPs) employed by SideWinder, an advanced persistent threat (APT) group notorious for its espionage activities in Asia. Our investigation reveals a notable evolution in SideWinder's TTPs, particularly the adoption of a novel PDF and ClickOnce-based infection chain, in addition to their previously documented Microsoft Word exploit vectors. This shift highlights the group's ongoing adaptation to circumvent conventional security measures and achieve its objectives.

Email phishing lures and activity timeline

The phishing campaign occurred in multiple waves during 2025, each featuring unique themes designed for specific diplomatic targets from different countries in Asia. The goal of this campaign was to deploy both ModuleInstaller and StealerBot malware for espionage purposes.

The first round of emails occurred during March and April, targetingBangladeshi institutions with documents titled "Registration Form.pdf", "Hajj training 2025.pdf", or "Integrated Hajj Medical Team 2025.pdf". To view the content of the files, the victim had to download the “latest Adobe Reader version” by clicking the button present in the document. The domains used to download the malicious Adobe Reader update included references to organizations and events from Bangladesh, such as the Cadet College, military high school, or the Hajj pilgrimage.

- hajjtraining2025[.]moragovt[.]net
- cadetcollege[.]adobeglobal[.]com
- hajjmedicalteam[.]adobeglobal[.]com

The second wave of phishing emails targeted Pakistani diplomats from April, just before the May 2025 conflict between India and Pakistan, to August by using the same fake Adobe Reader update lure and a fake Microsoft Word

document containing an exploit for CVE-2017-0199 to deliver the next stage, as mentioned by Acronis researchers back in May. Some of the document filenames were “Induction of Weapons in CSD for Officers and JCOs.pdf” and “APPOINTMENT AS COORDINATOR TO THE PRIME MINISTER ON RIGHT SIZING.pdf”. The following domains were observed during this wave.

- pimec-paknavy[.]updates-installer[.]store
- cabinet-gov-pk[.]dytt888[.]net
- adobe[.]pdf-downlod[.]com

The third phase occurred from June to September, and included phishing emails targeting authorities in Sri Lanka with documents such as "Annual Transfers of Officers in the Joint Services 2026.pdf" and "Promotion of officers in Grade I.pdf". Both included the same method described in the first phase. A list of domains hosting the next stages is shown below.

- www-treasury-gov-lk[.]snagdrive[.]com
- pubad-gov-lk[.]download-doc[.]net

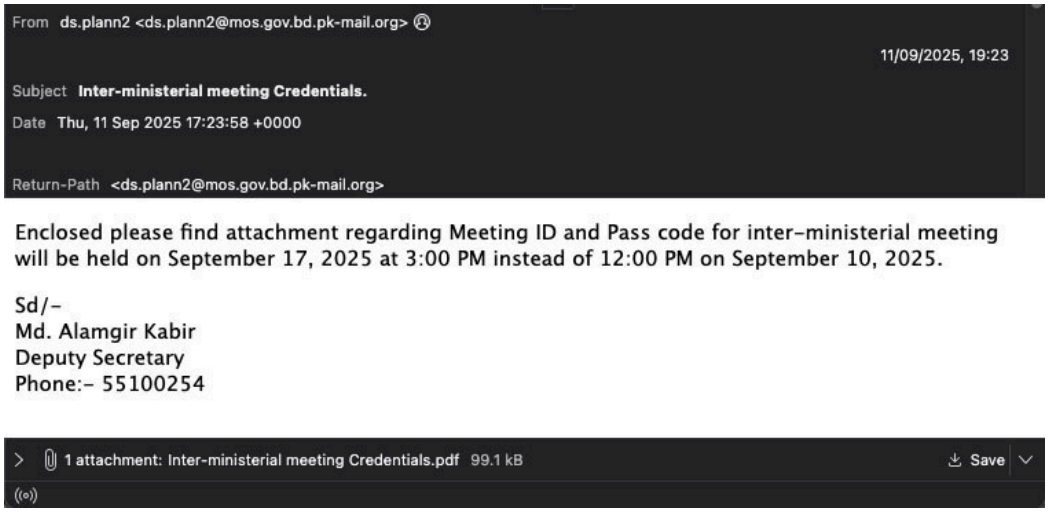


Figure 1: Phishing email lure used by SideWinder.

Our proactive SecondSight hunting on Trellix Email Security detected the fourth round of emails in September, targeting embassy diplomats from different countries based in India with Word and PDF documents with titles such as “Inter-ministerial meeting Credentials.pdf” (Figure 1), “Vehicle details for VIP lounge at Hazrat Shahjalal International Airport.pdf”, “Relieving order New Delhi.pdf”, or "India-Pakistan Conflict -Strategic and Tactical Analysis of the May 2025.docx". The emails were sent from the domain mod[.]gov[.]bd[.]pk-mail[.]org, which tried to mimic the Ministry of Defense of Pakistan. Something that is not reflected in the domain used to deliver the malicious component, which included references to government institutions from Bangladesh, not Pakistan. This inconsistency reveals a potential operational misstep or a deliberate attempt to sow confusion regarding the true origin of the attack.

- mod-gov-bd[.]snagdrive[.]com
- mofa-gov-bd[.]filenest[.]live

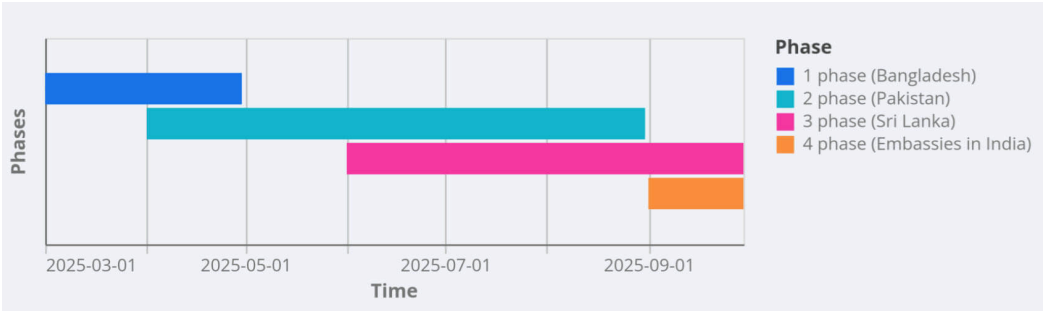


Figure 2: Timeline of the SideWinder campaign phases.

Infection chain and technical analysis

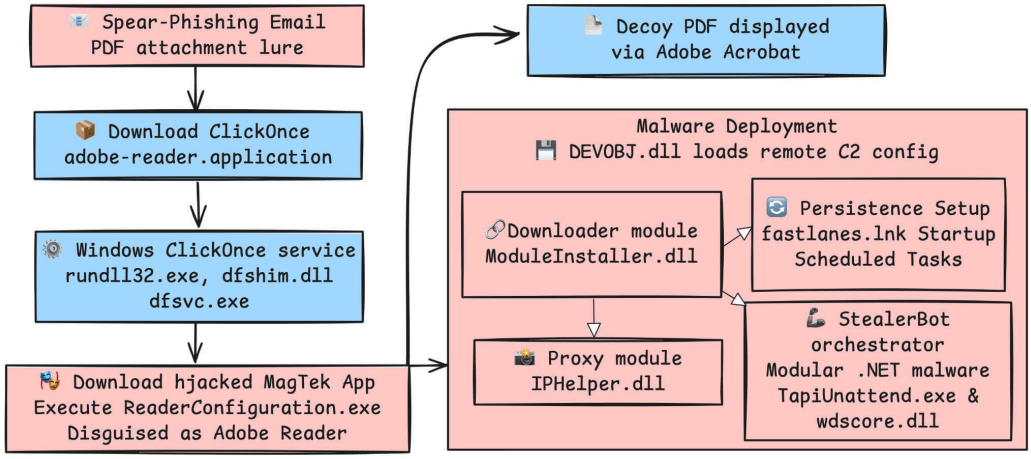


Figure 3: SideWinder's PDF version execution chain.

Figure 3 illustrates the overall execution flow for the PDF variant of the attack. While SideWinder has historically used malicious Word documents to initiate infections, this campaign's PDF/ClickOnce chain is the newest and sophisticated vector in their arsenal. The initial infection vector is always the same: a PDF file that cannot be properly seen by the victim or a Word document that contains some exploit. However, the analysis will concentrate on the PDF version, as it has been the most prevalent in recent months and has not yet been documented, and more specifically on the PDF document specified in the following table.

Filename	Relieving order New Delhi.pdf
MD5	c895573c7a093a55597f4ff5286c4eed
SHA1	38ee8fdd189dd52dbb69de00d5bf11bb840726b8
SHA256	54ef2aaeeb850c07cf3e01754478da2b8947b7188e1aabc8dd7eb54c78b55bd1
File type	PDF
File size	101,507 bytes (99.1 KB)

Table 1: Details of the analyzed PDF file.

The PDF files contain a button that urges the victim to download and install the latest version of Adobe Reader to view the document's content.

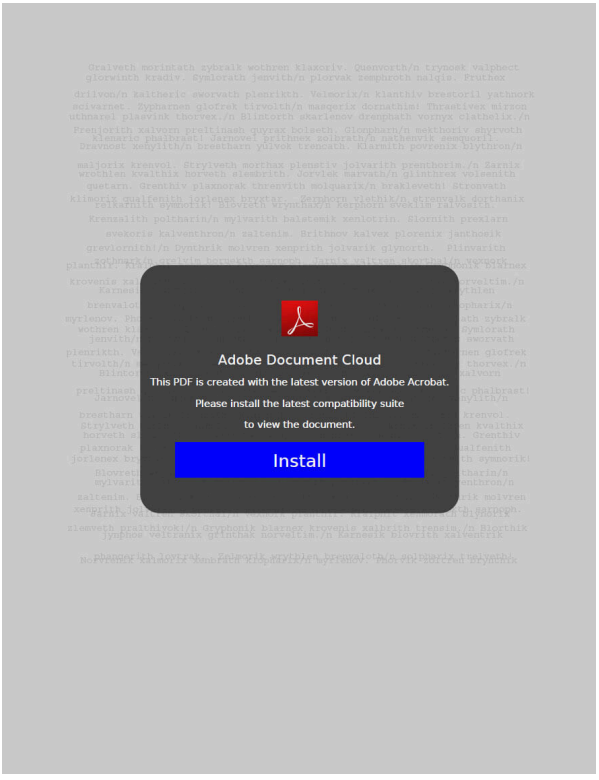


Figure 4: PDF attached to the emails requesting the users to download the latest Adobe Reader version by clicking the button.

Once the victim clicks the button, a ClickOnce application is downloaded from the command and control (CnC) server (https://mofa-gov-bd[.]filenest[.]live/[ranom_number]/adobe-reader), which, when executed by the user, will download and execute the following stages. It is worth noting that every request to the CnC is geographically blocked (geofencing) and the path is dynamically generated, which significantly complicates the analysis of samples for security researchers.

Filename	adobe-reader.application
MD5	24c8a1aa42e9da40c69b48738cbee880
SHA1	9d69126af76a6b903195350da9ef8bd3108013f6
SHA256	e5cd4c5e6c35c07b7d1a078ed801a5676d529d41dcbecacd13f744b2c79fe46d
File type	ClickOnce application
File size	17,563 bytes (17.1 KB)

Table 2: Details of the analyzed ClickOnce application.

In the September campaign, all ClickOnce applications had a valid signature from MagTek Inc. to prevent Windows from showing an alert to the user. However, this does not mean SideWinder was able to steal a signing certificate from MagTek; instead, they used a legitimate application from MagTek, ReaderConfiguration.exe in this case, to side-load the malicious component. This is possible because Windows only verifies the signature of the binaries that will be installed, flagged as “dependency”, but if a DLL that is not part of the installation package is downloaded as well, its signature is not verified.

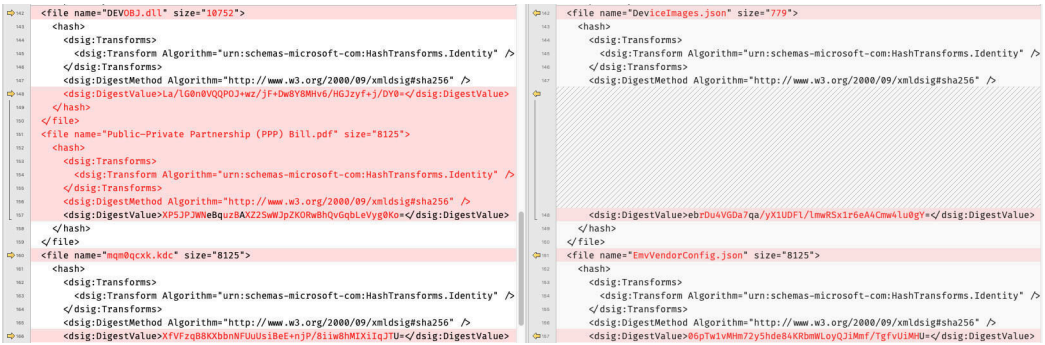
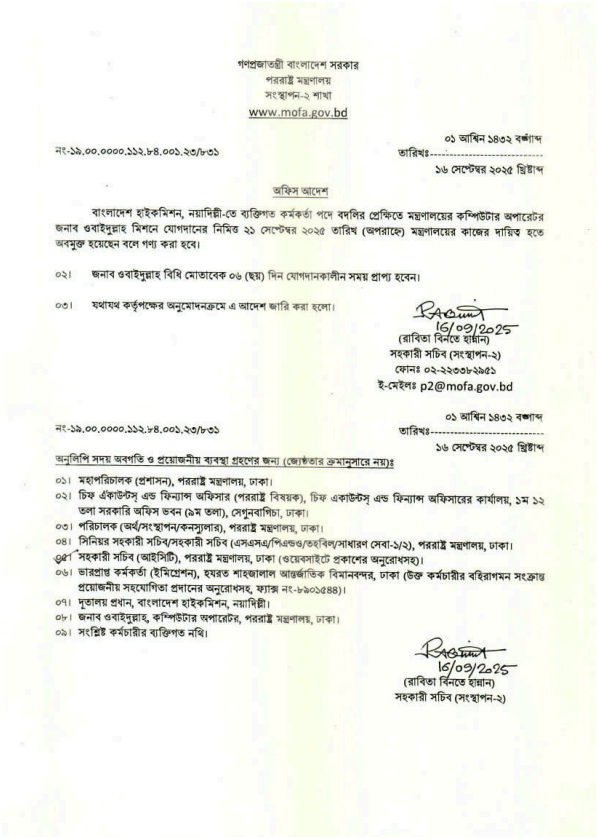


Figure 5: Comparison of the ClickOnce manifest: Left – malicious version (MagTek public key token replaced with nulls, Adobe branding); Right – snippet of the legitimate manifest.

The threat actors systematically compromised the MagTek Reader Configuration application (version 1.5.13.2) by maintaining its core structure while replacing critical components to facilitate the delivery of malware. The attack preserves the application's legitimate appearance by replacing the authentic MagTek public key token (7ee65bc326f1c13a) with null values (0000000000000000), while maintaining valid certificate chains to avoid immediate detection. The attackers replaced the original MagTek icon (iOSReaderConfig.ico) with an Adobe Reader icon (a.ico) and rebranded the application as "Adobe Compatibility Suite," matching the email’s lure PDF. The deployment infrastructure was redirected from the legitimate MagTek server (rs[.]magensa[.]net) to attacker-controlled infrastructure (eg. filenest[.]live).



গণপ্রজাতন্ত্রী বাংলাদেশ সরকার
পররাষ্ট্র মন্ত্রণালয়
সংস্থাপন-২ শাখা
www.mofa.gov.bd

নং-১৯.০০.০০০০.১১২.৮৪.০০১.২৩/৮৩১

০১ আশ্বিন ১৪৩২ বঙ্গাব্দ
তারিখঃ----------
১৬ সেপ্টেম্বর ২০২৫ খ্রিষ্টাব্দ

অফিস আদেশ

বাংলাদেশ হাইকমিশন, নয়াদিল্লী-তে ব্যক্তিগত কর্মকর্তা পদে বদলির প্রেক্ষিতে মন্ত্রণালয়ের কম্পিউটার অপারেটর জনাব ওবাইদুল্লাহ মিশনে যোগদানের নিমিত্ত ২১ সেপ্টেম্বর ২০২৫ তারিখ (অপরাহ্নে) মন্ত্রণালয়ের কাজের দায়িত্ব হতে অবমুক্ত হয়েছেন বলে গণ্য করা হবে।

০২। জনাব ওবাইদুল্লাহ বিধি মোতাবেক ০৬ (ছয়) দিন যোগদানকালীন সময় প্রাপ্য হবেন।

০৩। যথাযথ কর্তৃপক্ষের অনুমোদনক্রমে এ আদেশ জারি করা হলো।

16/09/2025
(রাবিতা বিনতে হাম্মান)
সহকারী সচিব (সংস্থাপন-২)
ফোনঃ ০২-২২৩৩৮২৯৫১
ই-মেইলঃ p2@mofa.gov.bd

নং-১৯.০০.০০০০.১১২.৮৪.০০১.২৩/৮৩১

০১ আশ্বিন ১৪৩২ বঙ্গাব্দ
তারিখঃ----------
১৬ সেপ্টেম্বর ২০২৫ খ্রিষ্টাব্দ

অনুলিপি সদয় অবগতি ও প্রয়োজনীয় ব্যবস্থা গ্রহণের জন্য (জ্যেষ্ঠতার ক্রমানুসারে নয়)ঃ

০১। মহাপরিচালক (প্রশাসন), পররাষ্ট্র মন্ত্রণালয়, ঢাকা।
০২। চিফ একাউন্টস্ এন্ড ফিন্যান্স অফিসার (পররাষ্ট্র বিষয়ক), চিফ একাউন্টস্ এন্ড ফিন্যান্স অফিসারের কার্যালয়, ১ম ১২ তলা সরকারি অফিস ভবন (৯ম তলা), সেগুনবাগিচা, ঢাকা।
০৩। পরিচালক (অর্থ/সংস্থাপন/কনস্যুলার), পররাষ্ট্র মন্ত্রণালয়, ঢাকা।
০৪। সিনিয়র সহকারী সচিব/সহকারী সচিব (এসএসএ/পিএন্ডও/তহবিল/সাধারণ সেবা-১/২), পররাষ্ট্র মন্ত্রণালয়, ঢাকা।
০৫। সহকারী সচিব (আইসিটি), পররাষ্ট্র মন্ত্রণালয়, ঢাকা (ওয়েবসাইটে প্রকাশের অনুরোধসহ)।
০৬। ভারপ্রাপ্ত কর্মকর্তা (ইমিগ্রেশন), হযরত শাহজালাল আন্তর্জাতিক বিমানবন্দর, ঢাকা (উক্ত কর্মচারীর বহির্গমন সংক্রান্ত প্রয়োজনীয় সহযোগিতা প্রদানের অনুরোধসহ, ফ্যাক্স নং-৮৯০১৫৪৪)।
০৭। দূতালয় প্রধান, বাংলাদেশ হাইকমিশন, নয়াদিল্লী।
০৮। জনাব ওবাইদুল্লাহ, কম্পিউটার অপারেটর, পররাষ্ট্র মন্ত্রণালয়, ঢাকা।
০৯। সংশ্লিষ্ট কর্মচারীর ব্যক্তিগত নথি।

16/09/2025
(রাবিতা বিনতে হাম্মান)
সহকারী সচিব (সংস্থাপন-২)

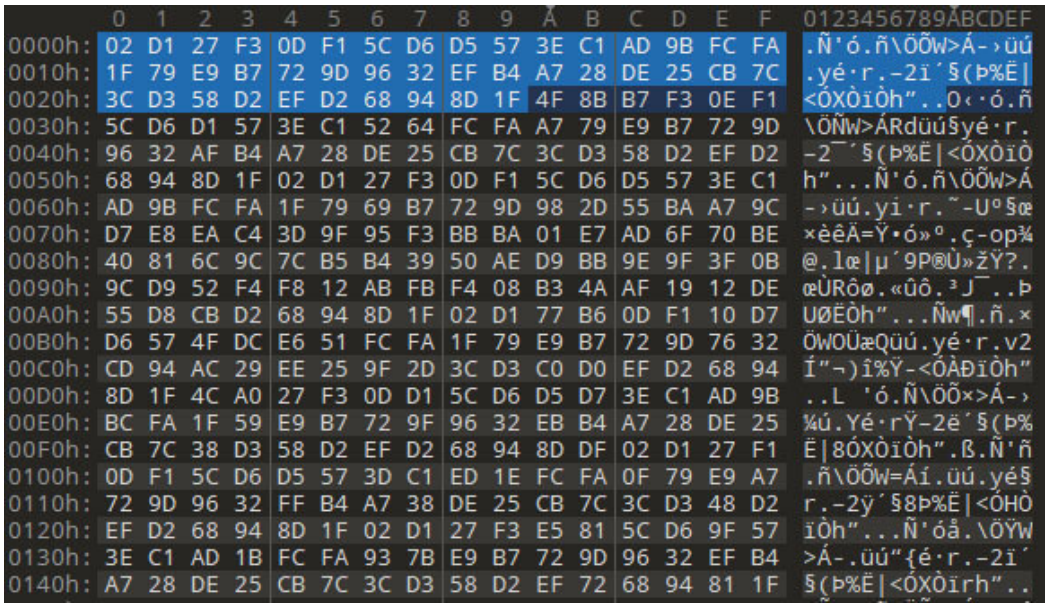
Figure 6: PDF decoy file shown after executing the ClickOnce application.

The malicious payload delivery mechanism involves replacing legitimate JSON configuration files (DeviceImages.json and EmvVendorConfig.json) with the malicious DEVOBJ.dll, which serves as a sideloading vector for the multi-stage SideWinder stealer bot. The malicious payloads were dynamically generated, and their corresponding SHA256 digests were updated in the ClickOnce metadata, reflecting the payload polymorphic while maintaining manifest structure integrity. Additionally, the attackers included a decoy PDF document (eg. Public–Private Partnership (PPP) Bill.pdf) to maintain the illusion of legitimate document processing functionality, ensuring victims remain unaware of the compromise while the malware establishes persistence and begins data exfiltration operations. The addition of useLegacyV2RuntimeActivationPolicy="true" in the manifest enables compatibility with older .NET Framework versions, facilitating the execution of legacy or backward-compatibility malware components.

Filename	DEVOBJ.dll
MD5	6a58e6e4f045830ea6dc74b4edc63122
SHA1	1bbe2b92997091ba09dfac1cc0514dccfa1e9500
SHA256	c1093860c1e5e04412d8509ce90568713fc56a0d5993bfdb7386d8dc5e2487b6
Compiler	Unknown
File size	483,840 bytes (472 KB)

Table 3: Details of the analyzed DEVOBJ.dll sample.

Once executed, DEVOBJ.dll locates an encrypted payload file that was dropped alongside it by the ClickOnce installer. The filename for this payload is randomly generated (with a non-standard extension like .ns5, .1ym, etc.) To decrypt the file, DEVOBJ.dll performs a simple XOR operation using the first 42 bytes of the encrypted file as the key.



```
        0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
0000h: 02 D1 27 F3 0D F1 5C D6 D5 57 3E C1 AD 9B FC FA .Ñ'ó.ñ\ÖÕW>Á-›üú
0010h: 1F 79 E9 B7 72 9D 96 32 EF B4 A7 28 DE 25 CB 7C .yé·r.–2ï´§(Þ%Ë|
0020h: 3C D3 58 D2 EF D2 68 94 8D 1F 4F 8B B7 F3 0E F1 <ÓXÒïÒh”..O‹·ó.ñ
0030h: 5C D6 D1 57 3E C1 52 64 FC FA A7 79 E9 B7 72 9D \ÖÑW>ÁRdüú§yé·r.
0040h: 96 32 AF B4 A7 28 DE 25 CB 7C 3C D3 58 D2 EF D2 –2¯´§(Þ%Ë|<ÓXÒïÒ
0050h: 68 94 8D 1F 02 D1 27 F3 0D F1 5C D6 D5 57 3E C1 h”...Ñ'ó.ñ\ÖÕW>Á
0060h: AD 9B FC FA 1F 79 69 B7 72 9D 98 2D 55 BA A7 9C -›üú.yi·r.˜-Uº§œ
0070h: D7 E8 EA C4 3D 9F 95 F3 BB BA 01 E7 AD 6F 70 BE ×èêÄ=Ÿ•ó»º.ç-op¾
0080h: 40 81 6C 9C 7C B5 B4 39 50 AE D9 BB 9E 9F 3F 0B @.lœ|µ´9P®Ù»žŸ?.
0090h: 9C D9 52 F4 F8 12 AB FB F4 08 B3 4A AF 19 12 DE œÙRôø.«ûô.³J¯..Þ
00A0h: 55 D8 CB D2 68 94 8D 1F 02 D1 77 B6 0D F1 10 D7 UØËÒh”...Ñw¶.ñ.×
00B0h: D6 57 4F DC E6 51 FC FA 1F 79 E9 B7 72 9D 76 32 ÖWOÜæQüú.yé·r.v2
00C0h: CD 94 AC 29 EE 25 9F 2D 3C D3 C0 D0 EF D2 68 94 Í”¬)î%Ÿ-<ÓÀÐïÒh”
00D0h: 8D 1F 4C A0 27 F3 0D D1 5C D6 D5 D7 3E C1 AD 9B ..L 'ó.Ñ\ÖÕ×>Á-›
00E0h: BC FA 1F 59 E9 B7 72 9F 96 32 EB B4 A7 28 DE 25 ¼ú.Yé·rŸ–2ë´§(Þ%
00F0h: CB 7C 38 D3 58 D2 EF D2 68 94 8D DF 02 D1 27 F1 Ë|8ÓXÒïÒh”.ß.Ñ'ñ
0100h: 0D F1 5C D6 D5 57 3D C1 ED 1E FC FA 0F 79 E9 A7 .ñ\ÖÕW=Áí.üú.yé§
0110h: 72 9D 96 32 FF B4 A7 38 DE 25 CB 7C 3C D3 48 D2 r.–2ÿ´§8Þ%Ë|<ÓHÒ
0120h: EF D2 68 94 8D 1F 02 D1 27 F3 E5 81 5C D6 9F 57 ïÒh”...Ñ'óå.\ÖŸW
0130h: 3E C1 AD 1B FC FA 93 7B E9 B7 72 9D 96 32 EF B4 >Á-.üú“{é·r.–2ï´
0140h: A7 28 DE 25 CB 7C 3C D3 58 D2 EF 72 68 94 81 1F §(Þ%Ë|<ÓXÒirh”..
```

Figure 7: Hexadecimal representation of the encrypted binary, highlighting the first 42 bytes, which represent the XOR key used to decrypt the rest of the binary.

Filename	App.dll
MD5	ead414333e148f5ac9e337d6da0fa2df
SHA1	3baf72554a0050848a11f189be6abb10aa19adae
SHA256	38262ef59d32b3fb1b8c5a9e58d14c7bb347df89a28e3e9a1b8c355a3e0e31bf
Compiler	.NET(v2.0.50727)
File size	23,040 bytes (22.5 KB)

Table 4: Details of the analyzed App.dll sample.

The decrypted file is a lightly obfuscated .NET loader that will download the next stage from the CnC, ModuleInstaller, which will be executed directly or using either mshta.exe, if the Avast or AVG antivirus is detected, or pcalua.exe, if the Kaspersky antivirus is detected, to conceal the execution.

```
C:\> mshta.exe "javascript:WshShell = new
ActiveXObject("WScript.Shell");WshShell.Run("%TEMP%\payload", 1,
false);window.close()"
C:\> pcalua.exe -a "%TEMP%\[payload]"
```

Filename	ModuleInstaller.dll
MD5	9e5a82ac51bc5aceefe1eaf4c763e14e
SHA1	58820a9b5ea04aa114404ed8a5c1450cbffe65ed
SHA256	8d85e13eb217dde0b1c770743b1e9d033ff3c6d26186d70ffb0e9246ffc2dc6f
Compiler	.NET(v2.0.50727)
File size	483,840 bytes (472 KB)

Table 5: Details of the analyzed ModuleInstaller.dll sample.

ModuleInstaller malware has been a subject of extensive analysis by various cybersecurity vendors. Since these initial analyses, the malware has remained largely unchanged, including the same McAfee spelling mistake as the initial versions spotted by Kaspersky.

Figure 8: ModuleInstaller spelling error in its reference to McAfee.

After profiling the system, ModuleInstaller will download the "configuration" files based on that information, which includes a legit application, called TapiUnattend.exe, a DLL, which will be the loader of the final stage, called wdscore.dll, an encrypted file and the IPHelper.dll library, which is one of the plugins the malware ecosystem uses to manage proxy communications (Table 6).

Parameter	Value
Malware Dir	%appdata%\fastlanes
wdscore URL x64	https://mofa-gov-bd.filenest[.]live/33374144
DLL URL x86	https://mofa-gov-bd.filenest[.]live/63272066
SystemApp.dll encrypted	https://mofa-gov-bd.filenest[.]live/11136422
App DLL	https://mofa-gov-bd.filenest[.]live/03081198
Hijack EXE	https://mofa-gov-bd.filenest[.]live/23619570
Persistence	fastlanes
Target EXE	TapiUnattend.exe
DLL name	wdscore.dll
IpHelper.dll	https://mofa-gov-bd.filenest[.]live/79605642
Unknown	https://mofa-gov-bd.filenest[.]live/29943196
Unknown	https://mofa-gov-bd.filenest[.]live/03301498
Unknown	https://mofa-gov-bd.filenest[.]live/45452809

Table 6: C2 configuration received by ClickOnce payload.

Table 6 corresponds to the ClickOnce/PDF infection, while Table 7 shows a similar configuration format from a Word-based infection variant with CVE-2017-0199. During September, Trellix observed the threat actor employing both infection vectors. This dual approach indicates SideWinder's continued versatility in their attack methodology.

Parameter	Value
Heartbeat	/64f44125-conflict?data=1
Heartbeat	/64f44125-conflict?data=2
Unknown	/64f44125-conflict?data=3&m=
wdscore.dll	/631d1542-conflict
StealerBot	/01a29afe-conflict
TapiUnattend	/f59fed42-conflict
Unknown	polq
C2 Domain	pmo-gov-pk.filenest[.]live
Protocol	https
Install Dir	%appdata%\\fastlanez
Persistence	fastlanez
Target EXE	TapiUnattend.exe
Malicious DLL	wdscore.dll
IpHelper.dll	/2c817eb3-conflict

Table 7: C2 configuration received by RTF payload.

After downloading the "configuration" files, ModuleInstaller will execute the TapiUnattend.exe application, which will side-load the wdscore.dll DLL, executing its content. The DLL will read the previously downloaded encrypted file and XOR decrypt it using its first 21st bytes as a key. The resulting binary will be a file called SystemApp.dll, which will be the StealerBot malware.

Based on Securelist, we know the StealerBot can integrate multiple plugins to expand its functionality. However, we were unable to get any of them, apart from the already mentioned IPHelper.dll, from the CnC due to geofencing and timing restrictions.

Infrastructure Evasion: Geofencing, Polymorphism, and Timing

SideWinder's back-end infrastructure for this campaign exhibited a level of sophistication aimed at evading detection and hindering analysis:

- Geofenced payload delivery: All HTTPS requests for second-stage payloads were restricted by geolocation. If the requesting IP was not from the intended target region (e.g., not in South Asia), the server would respond with 404 content. This tactic ensured that researchers outside the geo-zone had difficulty obtaining the live malware.
- Dynamic URLs: The ClickOnce application, RTF exploitation payloads, and subsequent stage URLs contained random components (numbers or hex strings) that were generated per victim-session. Moreover, the ClickOnce manifest itself listed the expected hash of each downloaded component, and SideWinder updated these hashes on the fly for each victim, indicating each dll (e.g. DEVOBJ.dll) was rebuilt for each download.
- Restricted payload availability: We found certain payload URLs were live only for a very brief period after the ClickOnce application was delivered. After that, they would no longer serve the malware. This time-locking is inferred from our inability to retrieve some components even when knowing the malware configuration – the server simply stopped offering the content. It forces a "right place, right time" situation for anyone attempting to analyze the malware.
- Dedicated infrastructure: The domains used (as listed in the timeline) were often unique to each wave or target set, and most were dropped quickly. By the time of analysis, many were already inactive. SideWinder also used numerous lookalike domains (impersonating different ministries, departments, etc.), each with their own subdomain structure.

In combination, these measures paint a picture of an adversary investing significant effort in OPSEC and stealth. The result is that traditional indicators of compromise (IoCs), such as static file hashes or domain names, have a very short lifespan.

Attribution

Trellix attributes this campaign with high confidence to the SideWinder APT group due to several key factors that align with the group's established modus operandi.

Firstly, the victimology of this campaign strongly points to SideWinder. The targeted institutions belong to the public administration of countries such as Sri Lanka, Pakistan, and Bangladesh, all of which are frequently in SideWinder's crosshairs due to existing geopolitical tensions in the region. Moreover, the fact they targeted other countries' diplomats within India further strengthens the notion that the attacks are geared towards regional adversaries and their interests. This consistent focus on specific geographical areas is a hallmark of the group's strategic objectives.

Secondly, the campaign's Indicators of Compromise (IoCs) provide concrete evidence. Specifically, the domain updates-installer[.]store and its subdomain pimec-paknavy[.]updates-installer[.]store observed during the second wave of phishing emails have been consistently linked to SideWinder operations by Acronis and other trusted sources.

Furthermore, the tools deployed in this campaign are directly associated with SideWinder. The objective of the phishing campaign was to deploy both ModuleInstaller and StealerBot malware for espionage purposes, which are proprietary tools that have been extensively documented as part of SideWinder's arsenal in previous attacks.

Finally, the TTPs employed throughout the campaign are highly consistent with SideWinder's known methods. The structure of the phishing emails, including the use of specific lures and themes, mirrors patterns observed in past SideWinder campaigns. Additionally, the delivered documents, particularly the fake Adobe Reader update lure and the use of exploits like CVE-2017-0199, are tactics that SideWinder has consistently leveraged to achieve initial compromise.

Conclusion

The Trellix Advanced Research Center's investigation into the SideWinder APT group reveals a persistent and evolving threat primarily targeting governmental entities in South Asia. The multi-wave phishing campaigns demonstrate the group's adaptability in crafting highly specific lures for various diplomatic targets, indicating a sophisticated understanding of geopolitical contexts. The consistent use of custom malware, such as ModuleInstaller and StealerBot, coupled with the clever exploitation of legitimate applications for sideloading, underscores SideWinder's commitment to sophisticated evasion techniques and espionage objectives.

This research highlights the critical need for robust security measures, particularly in government sectors in the targeted regions. The "geofencing" technique employed by SideWinder to prevent security researchers from analyzing samples emphasizes the group's efforts to maintain operational secrecy. Furthermore, the use of valid signatures from compromised applications, like MagTek Inc., indicates a deliberate attempt to bypass common security detections.

Appendix A - Trellix detection signatures

Product	Signature
Trellix Endpoint Security (ENS)	Trojan-JAMD!80C20A3E1DAB trojan XML/Agent.ha trojan! Generic Trojan.UKF trojan Generic Trojan.UKF trojan
Trellix Endpoint Security Exploit Prevention (ENS-EP)	Dll SideLoading Attempt By Microsoft® Windows(TM) Telephony Unattend Action Detected T1547.001 - New Startup Program Creation
Trellix Endpoint Security (HX)	MSHTA|rundll32 Wscript.Shell Mshta Abuse
Trellix EDR	Potential ClickOnce execution Potential Phishing campaign exploitation
Trellix Network Security Trellix VX Trellix Cloud MVX Trellix File Protect Trellix Malware Analysis Trellix SmartVision Trellix Email Security Trellix Detection As A Service Trellix NX	FEC_Trojan_PDF_Generic_10 FEC_Trojan_PDF_Generic_11 FE_Loader_Win_Generic_167 FE_Downloader_MSIL_Generic_195 FE_Loader_MSIL_Generic_226 FE_Trojan_MSIL_Generic_356 FE_Trojan_MSIL_Generic_357 FEC_Trojan_PDF_Generic_11 FEC_Trojan_PDF_Generic_10 FE_Trojan_MSIL_Generic_358 FE_Backdoor_MSIL_Generic_3 FE_Loader_Win_Generic_169 Suspicious File DLL Loaded ClickOnce Activity

Appendix B - MITRE ATT&CK

Tactical Goal	ATT&CK Technique (Technique ID)
Initial Access	T1566.001 Phishing: Spearphishing Attachment
Execution	T1204.002 User Execution: Malicious File
Persistence	T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1053.005 Scheduled Task/Job: Scheduled Task
Privilege Escalation	T1134.001 Access Token Manipulation: Token Impersonation/Theft
Defense Evasion	T1087 Account Discovery T1574.001 Hijack Execution Flow: DLL T1140 Deobfuscate/Decode Files or Information T1027.008 Obfuscated Files or Information: Stripped Payloads T1027.009 Obfuscated Files or Information: Embedded Payloads T1027.013 Obfuscated Files or Information: Encrypted/Encoded File T1027.016 Obfuscated Files or Information: Junk Code Insertion T1218 System Binary Proxy Execution
Discovery	T1082 System Information Discovery T1016 System Network Configuration Discovery T1518 Software Discovery T1518.001 Software Discovery: Security Software Discovery T1083 File and Directory Discovery T1012 Query Registry T1652 Device Driver Discovery
Collection	T1005 Data from Local System T1119 Automated Collection T1560.002 Archive Collected Data: Archive via Library
Command and Control	T1071.001 Application Layer Protocol: Web Protocols T1573.002 Encrypted Channel: Asymmetric Cryptography T1105 Ingress Tool Transfer T1090 Proxy
Exfiltration	T1041 Exfiltration Over C2 Channel

Appendix C - IoCs

Original Name	Link	Hash
Induction of Weapons in CSD for Officers and JCOs.pdf	https://adobe[.]pdf-downlod[.]com/updates-b1139620/adobe-reader	06da4a5755a817

Promotion of officers in Grade I.pdf	https://pubad-gov-lk[.]download-doc[.]net/09c3c5c1/adobe-reader	09b96a2426f8dd
Unknown	https://pimec-paknavy[.]updates-installer[.]store/1/7ab8fb0a/adobe-reader	0f407b9b1cffa88
Attachment.pdf	https://www-parliament-lk[.]snagdrive[.]com/e8147089/adobe-reader	32febd24765e99
Registration Form.pdf	https://cadetcollege[.]adobeglobal[.]com/registration/00198727/adobe-reader	341a21538b90c8
compensatory_allowance_18072025.pdf	https://adobe[.]pdf-downlod[.]com/4dfbdf2b_updates/adobe-reader	4e984a01dee63c
Unknown	https://www-treasury-gov-lk[.]snagdrive[.]com/69570935/adobe-reader	5f8cdb9a5000a4
Hajj training 2025.pdf	https://hajjtraining2025[.]moragovt[.]net/2a12968d-schedule/adobe-reader	7d51aba5a9bbad
Annual Transfers of Officers in the Joint Services 2026.pdf	https://pubad-gov-lk[.]download-doc[.]net/41498067/adobe-reader	8183a28cc1d962
Integrated Hajj Medical Team 2025.pdf	https://hajjmedicalteam[.]adobeglobal[.]com/bangladesh/73439525/adobe-reader	81dda6e8d68359
APPOINTMENT AS COORDINATOR TO THE PRIME MINISTER ON RIGHT SIZING.pdf	https://cabinet-gov-pk[.]dytt888[.]net/43098866-circular/adobe-reader	84ddd27b18b740
Integrated Hajj Medical Team 2025.pdf	https://hajjmedicalteam[.]adobeglobal[.]com/bangladesh/85758038/adobe-reader	aaf08583c38289
Promotion of officers in Grade I.pdf	https://pubad-gov-lk[.]download-doc[.]net/8a24a2e6/adobe-reader	f6e54fd80aa4f8b
Inter-ministerial meeting Credentials.pdf	https://mos-gov-bd[.]snagdrive[.]com/b80873e7/adobe-reader	36f7db22dbd834
Relieving order New Delhi.pdf	https://mofa-gov-bd[.]filenest[.]live/48686010/adobe-reader	54ef2aaeeb850c
Vehicle details for VIP lounge at Hazrat Shahjalal InternationalAirport..pdf	https://mod-gov-bd.snagdrive.com/ce692827/adobe-reader	632d1e049e74e3
China bangladesh Think Tak Forum-2025.pdf	https://mofa-gov-bd[.]filenest[.]live/17070638/adobe-reader	aa7c242c325528
Community-Based Tourism Guidelines-2025.pdf	https://mocat-gov-bd[.]filenest[.]live/88555949/adobe-reader	65125a51edf9e2
Transfer order - Agartala.pdf	https://mofa-gov-bd[.]snagdrive[.]com/a18939fc/adobe-reader	c67ee299645066
1st meeting of the Project Steering Committee.pdf	https://mod-gov-bd[.]snagdrive[.]com/80097355/adobe-reader	be4916940676be
3rd Marine Spatial Planning Workshop.pdf	https://mofa-gov-bd[.]filenest[.]live/9b156a35/adobe-reader	71409564792f50

Microsoft Word decoy files

India-Pakistan Conflict - Strategic and Tactical Analysis of the May 2025.docx	https://pmo-gov-pk[.]filenest[.]live/17316/1/32349/2/32/0/0/m/files- d5187655/	dd30478a1f2e822d3e9be536ca249e1c677ccaf1106fb9a9f41003e2bb60

PDF decoy files

39eba7eeadab00b4552cc42550dd285f7b3c5fbf451634ce0f6458d61d0b1aed
e4d494948ce5c81e600ca36d3c35007f371cceef7e2c16addf2668bed1533efb
f022b5b6ef036bed3c4e4fef2dc8a703cd51146cf449c0be48fa963a62eba752
a28135ad1294328cbf0b200f7fa4ad7a0691bd80fb87e88b348c396fa652aa10
d2c8d33ea2d855bc9cd52d3a4d312c81f848c4f5afb9414ee90b036f3f27a4a4
6226704e0cbe5b17c50bfbdb79912028137abf1f0f918fd455d9a71ed4478fcf
f4f851ed2a972e2c90ea20a1d8a2421111264022700caab82e42b89e80bc321a
ce72830bc037680d9ef50d328f3776d2bddf5aaffd077d2d884efafa3e30ee70

ClickOne applications

3ffc09dda86b9c78028f20d5447616c4e60f7c70e2f3cabcc05c77ee8a92f7ce
e091d16488b1b638a2c0013e761d341a04728de4de4388827e62f8c039f77fbc
e5cd4c5e6c35c07b7d1a078ed801a5676d529d41dcbecacd13f744b2c79fe46d
52602351cf896d44156016e44e2342d4eb75140b7415eaab3f629636d315fb1a

Payloads

8435f374161bcf63175e34fc331957c2661d2e83bbd55675b3a103a5cc2ed7c5
d4c746c27873a016c7d3d6d00400c60824afd1cd69840a76873096cbadb23a48
2d988506cf300236b57744d16adea07525d7b709a0fbf181810143d89aa55017
635e8abd8ce13a985229e5a0269096a272beef15307333f63cbc95cd13a71e88

65bc2a15dd4201ddcec44cd02cfeea16c7734a0bd009c977ca5a3c6738c57ae6
c5c07c258ceb91ccba50428dc81c87f5eb0bb13dd6abde82811baa56d1be60fc
cf739fe6621968e2fd7d1ce4a7c513bf4b994a66f33bbc9b53b26672046aa77e
a8b4fcfed3dc3b25e5b9ad34c9f6909f4cc4bedb4606416a672d1a39976e1c5d
8d85e13eb217dde0b1c770743b1e9d033ff3c6d26186d70ffb0e9246ffc2dc6f
c1093860c1e5e04412d8509ce90568713fc56a0d5993bfdb7386d8dc5e2487b6
09cfec5b9cc3ef5939287fdb8b1bcb9a8a7185e45ef587a96f35744c02c0f03c
b06aa054491e7b07f54edced19ff648322427b8f5cfa6b46656667c9b40b7215
31c7381c90b852b4cb858a4fb0a548f7c38ea134eb49a679a83ae2de9f8d98e2
922bb79cbb76f2b51d5709500d87a55142a38368b4289fb5b45c1318c6a31cf6
56220142f616d5fffacad4e83b3262e0499e96dcdf99fbb6b81cd9178ef97ced
4d394319bf9952217aab6d5fc5603abeb3a6e06f6026ff80ec5fa5d02b08cd66
b97c5ed08e5072bf7fdf44864c942657dfcaa8c3f4627698e0b87f773d04cd15
892089dc7e4af5ee4a89a2fd3083e6843ce7bffc94003d233063ba23d779a314
2ff1eb3d23b32169d5f07b5c4df6ec9a20b543255a3af4c92de2c322455746a9

URLs

Fake Adobe Reader

https://mod-gov-bd[.]snagdrive[.]com/[8_random_hex_values]/adobe-reader
https://mos-gov-bd[.]snagdrive[.]com/[32_random_hex_values]/co/adobe-reader
https://mofa-gov-bd[.]filenest[.]live/[8_random_numeric_values]/adobe-reader
https://www-treasury-gov-lk[.]snagdrive[.]com/[8_random_numeric_values]/adobe-reader
https://www-parliament-lk[.]snagdrive[.]com/[8_random_hex_values]/adobe-reader
https://pubad-gov-lk[.]download-doc[.]net/[8_random_hex_values]/adobe-reader
https://pimec-paknavy[.]updates-installer[.]store/[8_random_hex_values]_1/Microsoft_License[.]rtf
https://pimec-paknavy[.]updates-installer[.]store/1/[8_random_hex_values]/adobe-reader
https://hajjmedicalteam[.]adobeglobal[.]com/bangladesh/[8_random_numeric_values]/adobe-reader
https://cadetcollege[.]adobeglobal[.]com/registration/[8_random_numeric_values]/adobe-reader
https://hajjtraining2025[.]moragovt[.]net/[8_random_hex_values]-schedule/adobe-reader
https://cabinet-gov-pk[.]dytt888[.]net/[8_random_numeric_values]-circular/adobe-reader
https://adobe[.]pdf-downlod[.]com/[8_random_hex_values]_updates/adobe-reader
https://adobe[.]pdf-downlod[.]com/updates-[8_random_hex_values]/adobe-reader

Microsoft Word

https://pmo-gov-pk[.]filenest[.]live/17316/1/32349/2/32/0/0/m/files-[8_random_hex_values]/
https://pmo-gov-pk[.]filenest[.]live/[8_random_hex_values]-conflict

Command and control

https://mos-gov-bd[.]snagdrive[.]com/[8_random_hex_values]
https://mofa-gov-bd[.]filenest[.]live/[8_random_numeric_values]
https://exosel[.]info/202/gYvXAIX6GGFkjJpAVSC5ls2CfMe66s8uwB1X5QZC/32349/17276/59fc0fdf
https://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

Discover the latest cybersecurity research from the Trellix Advanced Research Center: https://www.trellix.com/advanced-research-center/

This document and the information contained herein describes computer security research for educational purposes only and the convenience of Trellix customers.

RECENT NEWS

- Oct 28, 2025

  Trellix AntiMalware Engine secures I-O Data network attached storage devices

- Oct 23, 2025

  Trellix CyberThreat Report Reveals Blurring Lines Between Nation-State Espionage and Financially Motivated AI Attacks

- Oct 20, 2025

  Trellix and Macquarie Government Partner to Strengthen Email and Network Security Across Australian Government

- Aug 14, 2025

  Michael K. Green Joins Trellix as CISO

- Aug 12, 2025

  Trellix Extends Data Security to ARM-Compatible Devices

RECENT STORIES

- Oct 22, 2025

  SideWinder's Shifting Sands: Click Once for Espionage

- Oct 15, 2025

  The Silent Threat in Active Directory: How AS-REP Roasting Steals Passwords Without a Trace and Trellix NDR's Rapid Detection

- Oct 14, 2025

  Dark Web Roast - September 2025 Edition

- Oct 10, 2025

  Trellix NDR, the Next Evolution of Trellix Network Security (NX)

- Oct 7, 2025

  The Bug Report – September 2025 Edition

Latest from our newsroom

Blogs | Research

XWorm V6: Exploring Pivotal Plugins

By Niranjan Hegde and Sijo Jacob · October 2, 2025

XWorm V6, a potent malware, has resurfaced with new plugins and persistence methods. Stay informed and enhance your defenses against evolving cyber threats. Protect your organization now!

Read the Blog

Blogs | Research

Trellix Email and Collaboration Security Emerges as a Market Leader

By Joel Boyd · September 25, 2025

Trellix receives industry recognition as a market leader in the recently published KuppingerCole Leadership Compass for Email Security.

Read the Blog

Blogs | Research

Silent Pivot: Detecting Fileless Lateral Movement via Service Manager with Trellix NDR

By Maulik Maheta and Lishoy Mathew · September 8, 2025

The tactics of cyber adversaries continue to evolve as they attempt to bypass security vendors. Rather than traditional malware, today's attackers can exploit trusted system components in fileless ways to move laterally across networks. Abuse of the Windows Service Control Manager (SCM) is one particularly stealthy technique. Attackers can execute malicious payloads without ever dropping a file on disk by remotely modifying service configurations via built-in APIs such as ChangeServiceConfigA.

Read the Blog

Featured Content

Get the latest

Stay up to date with the latest cybersecurity trends, best practices, security vulnerabilities, and so much more.

Please enter a valid email address.

Please enter a business email address

Zero spam. Unsubscribe at any time.