

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

[blogs.blackberry.com/en/2024/07/sidewinder-targets-ports-and-maritime-facilities-in-the-mediterranean-sea](https://blogs.blackberry.com/en/2024/07/sidewinder-targets-ports-and-maritime-facilities-in-the-mediterranean-sea)

The BlackBerry Research and Intelligence Team



## 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

---

<b>Weapons</b>	Malicious documents, Obfuscated JavaScript
<b>Attack Vector</b>	Weaponized document used for targeted attack
<b>Network Infrastructure</b>	Phishing domains
<b>Targets</b>	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.

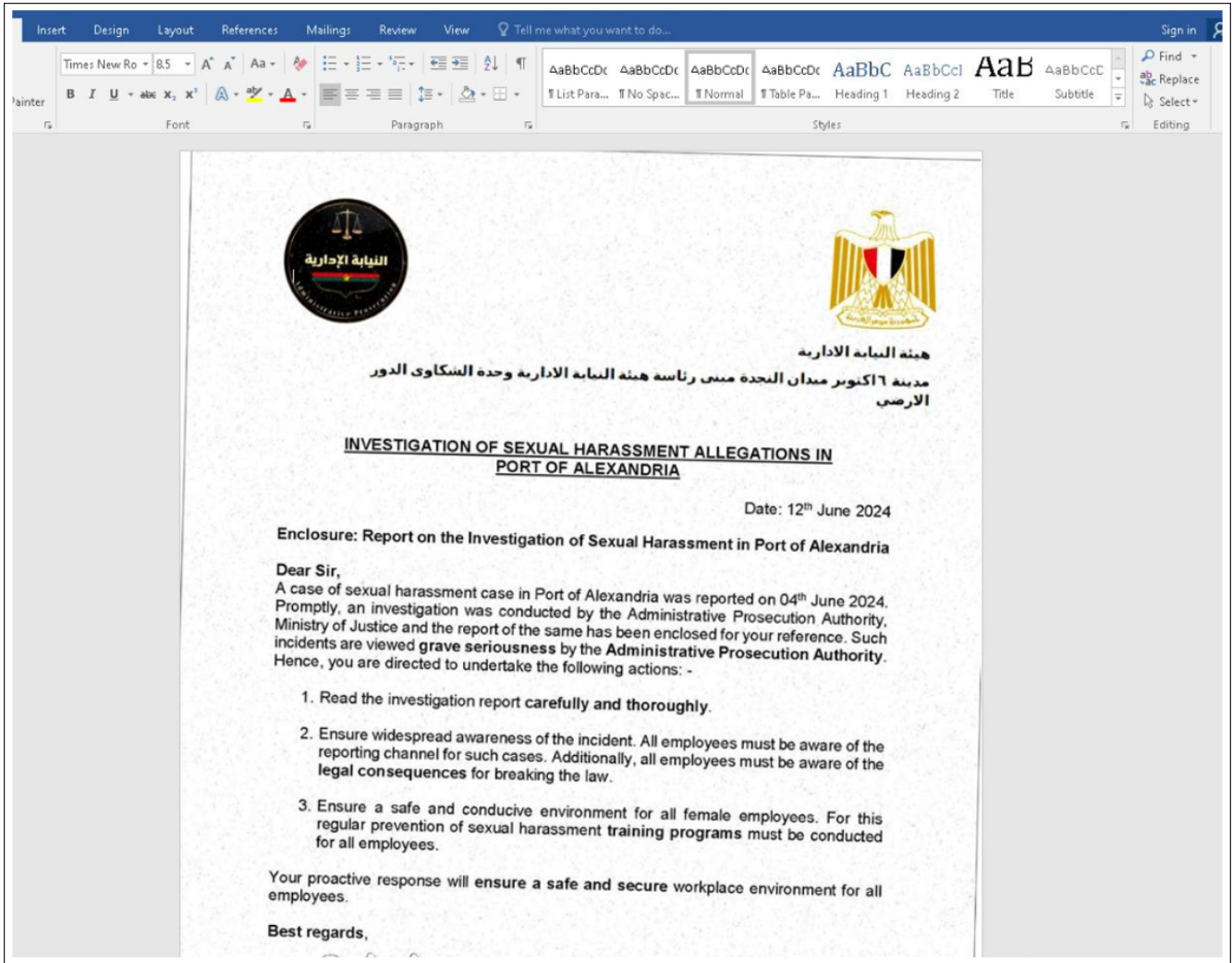


Figure 1: A visual lure contained in one of the malicious documents.

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.

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

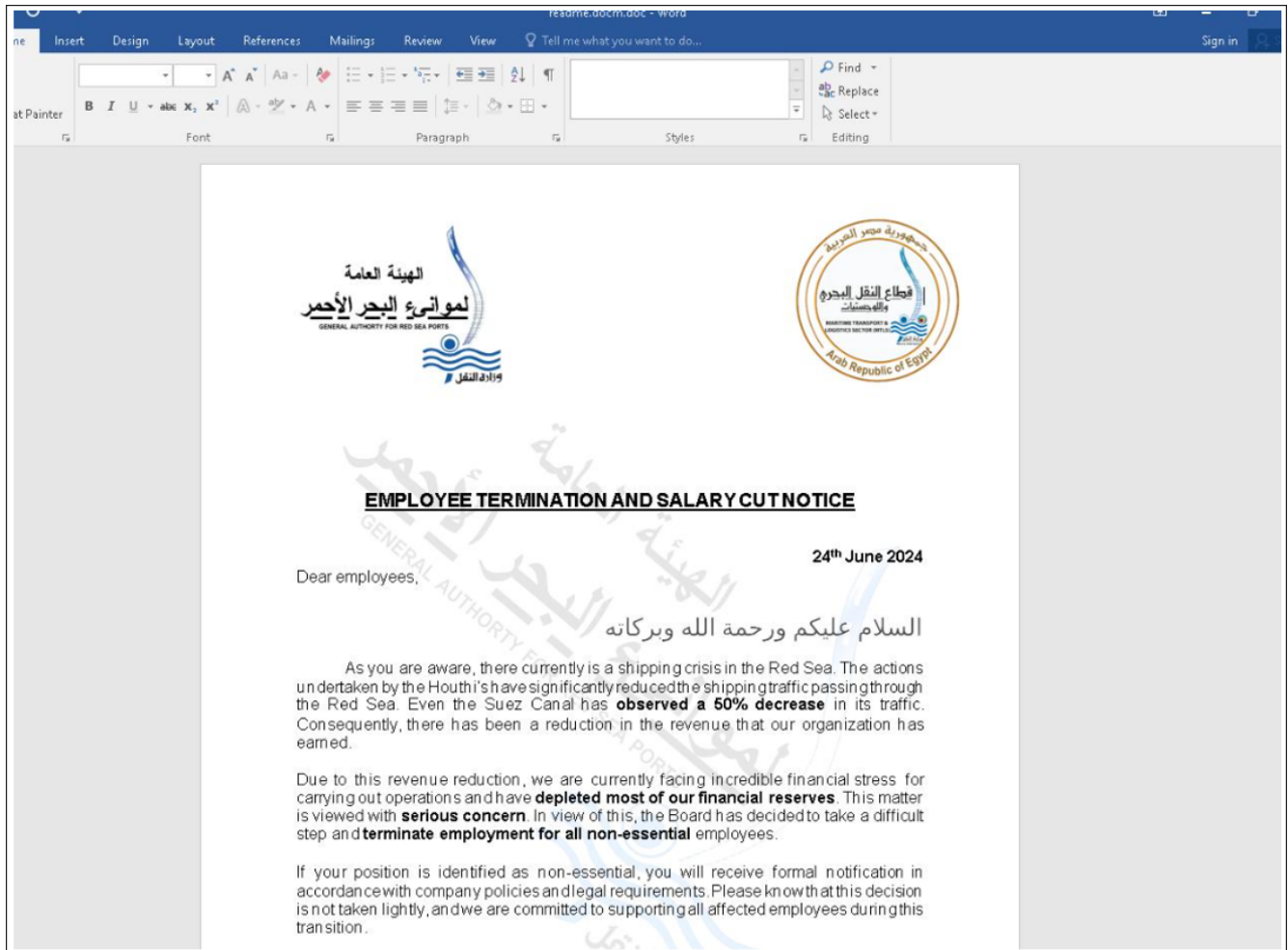


Figure 2: Another visual lure that abuses the logo of the (legitimate) Red Sea Port Authority in Egypt.

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.

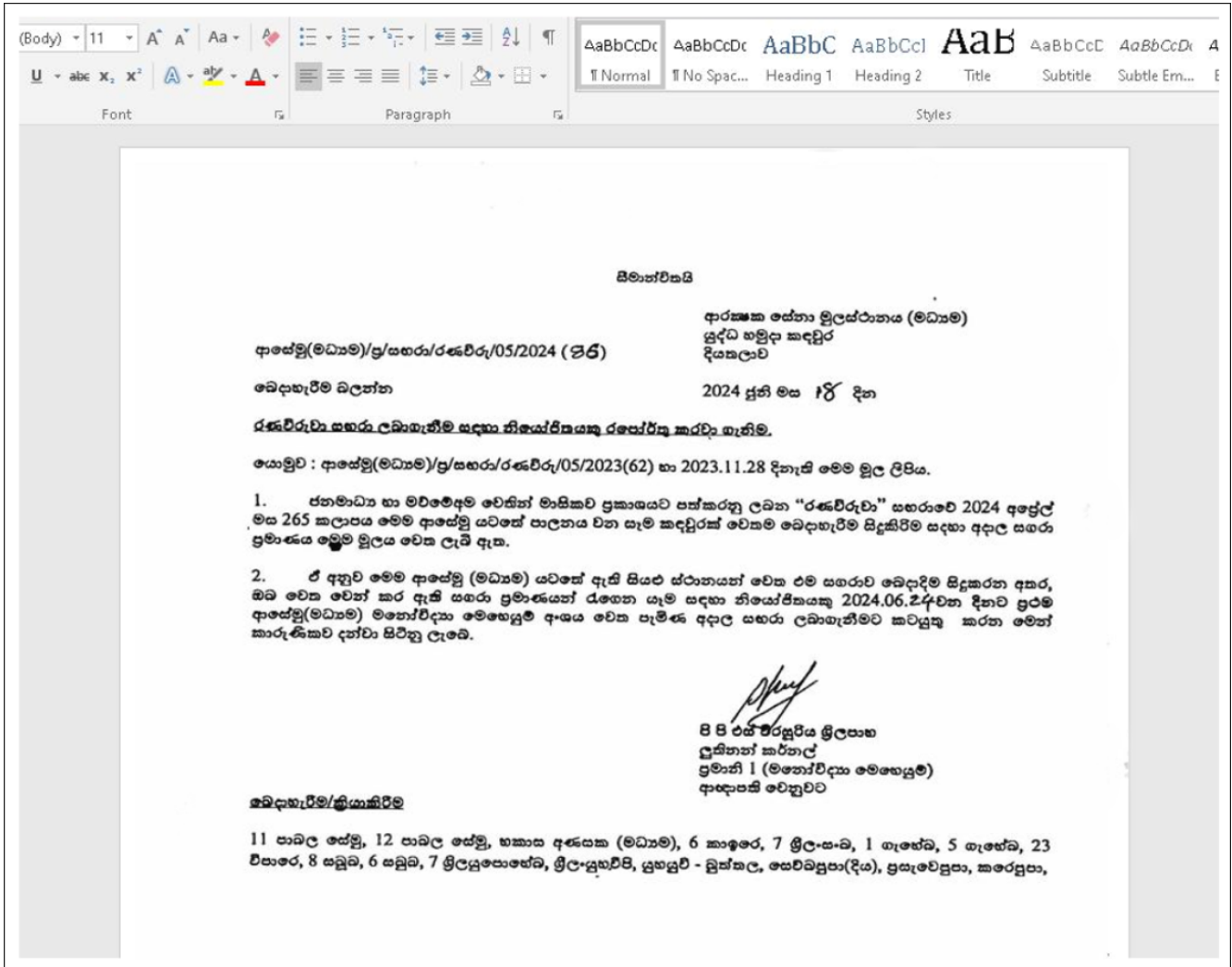


Figure 3: Another visual lure. The text is written in the Sinhala language used in Sri Lanka.

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.



```

5 Relationships xmlns = "http://schemas.openxmlformats.org/package/2006/relationships" > < Relationship Id = "rid460"
6 Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/footer"
7 Target = "footnotes344.xml" / > < Relationship Id = "rid457"
8 Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/footer"
9 Target = "endnotes136.xml" / > < Relationship Id = "fid872"
10 Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
11 Target = "https://reports.dgps-govtpk.com/63645534-case/doc.rtf"
12 TargetMode = "External" / > < Relationship Id = "rId150"
13 Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
14 Target = "media/image2.jpg" / > < Relationship Id = "rId1"
15 Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles"
16 Target = "styles.xml" / > < Relationship Id = "rId2"
17 Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable"
18 Target = "FontTable.xml" / > < Relationship Id = "rId3"
19 Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme"
20 Target = "theme/theme1.xml" / > < Relationship Id = "rId4"

```

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

<b>md5</b>	2462db3be57df824f003f74d7a16cacb
<b>sha-256</b>	142c6a4c7e9efbf6f3176df3ff218449bb4f7b2a69d60060e6339f1c3cc95d93
<b>File Name</b>	File.rtf
<b>File Size</b>	17.72 KB (18141 bytes)
<b>Creation Time</b>	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.

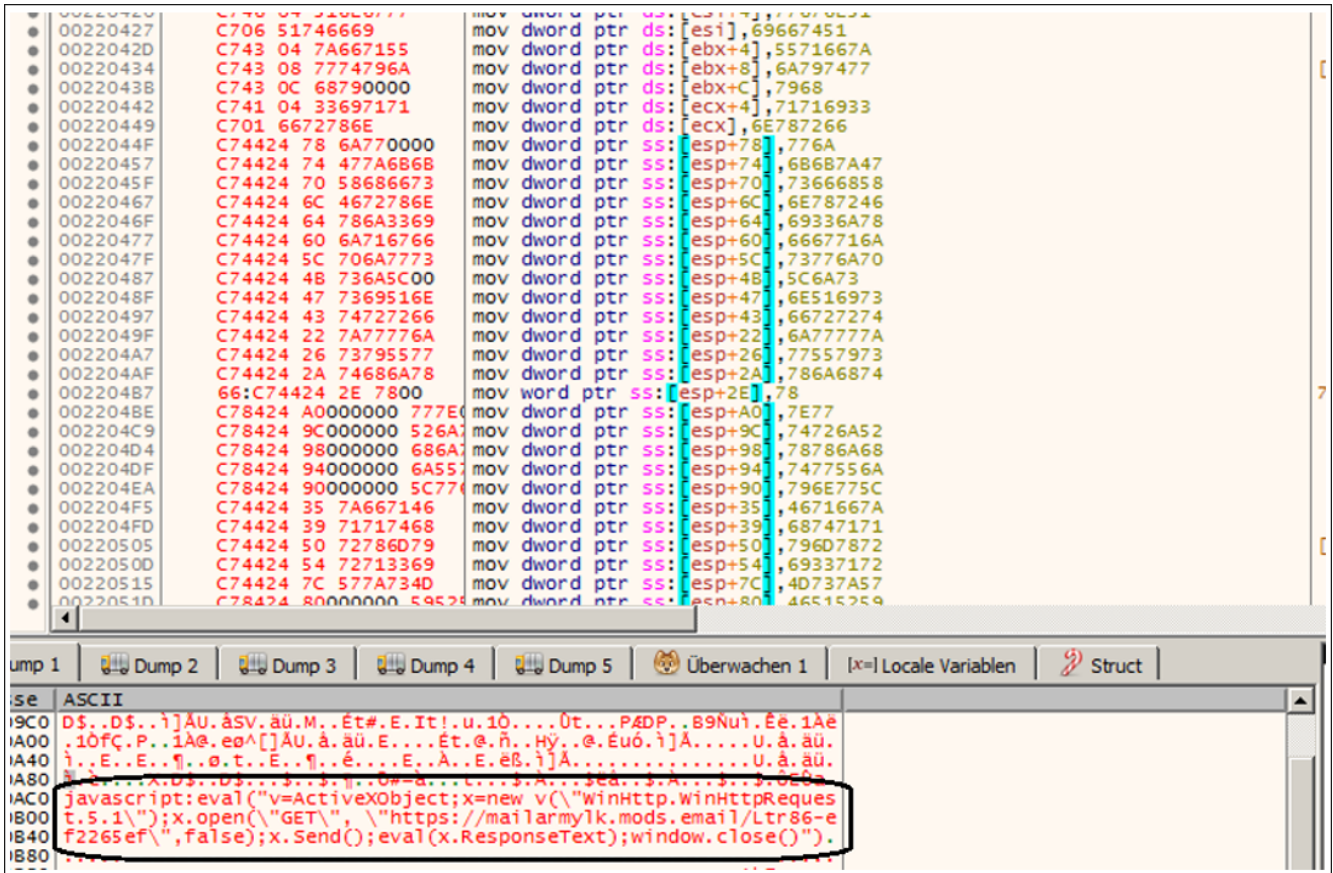


Figure 5. Shellcode decodes a small JavaScript at runtime.

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 Infrastructure for Stage 2 of the 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[.]169.189[.]137 - Hetzner Online GmbH	Namesilo.com Dnsowl.com Privacyguard.org Created 2024-06-13	
session-out[.]com	89[.]150.40[.]143 - HZ Hosting Ltd	Hostinger.com Privacyprotect.org Publicdomainregistry.com Created 2024-05-30	Delivery Infrastructure for Stage 2 of the attack chain.
mora.pdfadobe[.]com	5[.]255.113[.]149 - The Infrastructure Group B.V.	NetEarth One, Inc. Created 2024-02-13	Delivery Infrastructure for Stage 2
ftp[.]mods[.]email gta5[.]mods[.]email mailafdgovbd[.]mods[.]email mailarmylk[.]mods[.]email mailarmymilbd[.]mods[.]email mailforenggovmv[.]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
  - mailforengovmv[.]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)

<b>Sha-256 MD5</b>	b72ac58d599e6e1080251b1ac45a521b33c08d7d129828a4e82a7095e9f93e539345d52abd5bab4320c1273eb2c90161
<b>Sha-256 MD5</b>	9572312a12605c6a6ea6447af6fc063f4196aeba523ed38ce2c5ff51c33d48319a1c49322a9d950c047c2edfc781b778
<b>Sha-256 MD5</b>	ceb93ee3093dbf1a49918ede81055018d9c0f0945a97f904a16951010cfbce61c60b41f0981f617fa83a73704a10e147
<b>Sha-256 MD5</b>	512a83f1a6c404cb0ba679c7a2f3aa782bb5e17840d31a034de233f7500a6cb9e0bce049c71bc81afe172cd30be4d2b7
<b>Sha-256 MD5</b>	006e5fe0c01712391c54319a9d1579d7208f3cfa9f49fe56a14d93f0d0e8928b379edeaa9ed92ebe6091177417b2c751
<b>Sha-256 MD5</b>	613068422c214b944c7b2e3fb60412ed99d35c9e18d53d45b16965c5a36f734a3233db78e37302b47436b550a21cda9
<b>Sha-256 MD5</b>	9ce32ce5e2b70fec7f749e7868d89a4e3e739fed9c75cd6c4ec6eafde4c3711ad0d1fba6bb7be933889ace0d6955a1d7
<b>Sha-256 MD5</b>	142c6a4c7e9efbf6f3176df3ff218449bb4f7b2a69d60060e6339f1c3cc95d932462db3be57df824f003f74d7a16cacb
<b>Sha-256 MD5</b>	e21396bf5f9936310b4f53273db330a9620d78c1c744277b0e9126f0afdbc29d8d7c43913eba26f96cd656966c1e26d5
<b>Network Indicators</b>	<p>hxxp://investigation04[.]session-out[.]com/fbd901_harassment/doc[.]rtf</p> <p>hxxps://reports[.]dgps-govtpk[.]com/63645534-case/doc[.]rtf</p> <p>hxxps://salary-cutting[.]session-out[.]com/37656199_notice/doc[.]rtf</p> <p>hxxps://mailarmylk[.]mods[.]email/Ltr86-ef2265ef</p> <p>hxxps://moitt-gov-pk[.]fia-gov[.]net/643705null</p> <p>hxxps://mofa-gov-sa[.]direct888[.]net/015094_consulategz</p> <p>hxxps://moitt-gov-pk[.]fia-gov[.]net/720705null</p> <p>hxxps://heatwave[.]paknavy[.]store/pn/510426/doc.rtf</p> <p>hxxps://mora[.]pdfadobe[.]com/d8149d32/mora/doc.rtf</p>

## 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



## About The BlackBerry Research and Intelligence Team

---

The BlackBerry Research and Intelligence team is a highly experienced threat research group specializing in a wide range of cybersecurity disciplines, conducting continuous threat hunting to provide comprehensive insights into emerging threats. We analyze and address various attack vectors, leveraging our deep expertise in the cyberthreat landscape to develop proactive strategies that safeguard against adversaries.

Whether it's identifying new vulnerabilities or staying ahead of sophisticated attack tactics, we are dedicated to securing your digital assets with cutting-edge research and innovative solutions.

---

[Back](#)