SideWinder Uses Server-side Polymorphism to Attack Pakistan Government Officials — and Is Now Targeting Turkey

blogs.blackberry.com/en/2023/05/sidewinder-uses-server-side-polymorphism-to-target-pakistan

The BlackBerry Research & Intelligence Team

1. BlackBerry Blog
2. SideWinder Uses Server-side Polymorphism to Attack Pakistan Government Officials — and Is Now Targeting Turkey

Summary

The BlackBerry Threat Research and Intelligence team has been actively tracking and monitoring the SideWinder APT group, which has led to the discovery of their latest campaign targeting Pakistan government organizations.

In this campaign, the SideWinder advanced persistent threat (APT) group used a server-based polymorphism technique to deliver the next stage payload.

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	Obfuscated JavaScript, PE executable
Attack Vector	Weaponized document used for targeted attack
Network Infrastructure	DDNS
Targets	Pakistan Government organizations

Technical Analysis

Context

The SideWinder APT group, also known as Razor Tiger, Rattlesnake, and T-APT-04, has been actively targeting Pakistan government organizations since at least 2012.

One of the oldest nation-state threat actors, SideWinder is believed to originate from India. Active since at least 2012, the group has been observed targeting military, government, and business entities, with a particular focus on Pakistan, Afghanistan, China, and Nepal. SideWinder primarily makes use of email spear-phishing, document exploitation, and DLL side-loading techniques in an attempt to avoid detection and deliver targeted implants.

Through our threat hunting efforts, the BlackBerry Threat Research and Intelligence team discovered a new malware campaign by the SideWinder group. This campaign utilized a server-side polymorphism technique. The use of this technique allows the threat actor to

potentially bypass traditional signature-based antivirus (AV) detection to deliver the next stage payload.

Attack Vector

MD5	666b2b178ce52e30be9e69de93cc60a9
SHA256	cd09bf437f46210521ad5c21891414f236e29aa6869906820c7c9dc2b565d8be
File Name	GUIDELINES FOR JOURNAL - 2023 PAKISTAN NAVY WAR COLLEGE (PNWC).docx
File Size	12.81 KB (13115 bytes)
Created	2022-11-30 04:52:00 UTC
Author	Windows User
Last Modified	2022-11-30T05:44:00Z
Last Modified by	Windows User

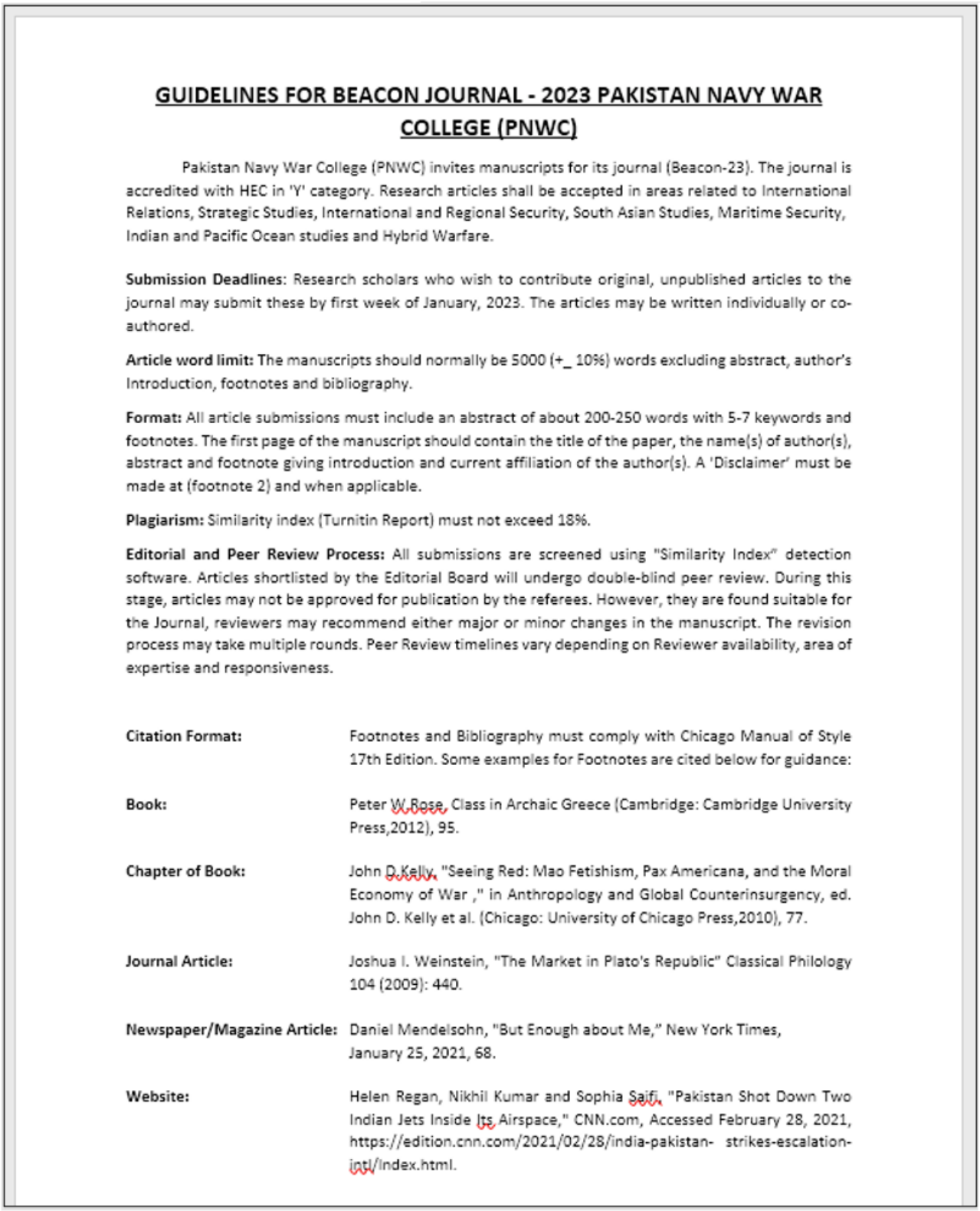
What is Server-Side Polymorphism?

Server-side polymorphism is a technique used by threat actors and other distributors of malware to attempt to evade detection by antivirus scanners. Polymorphic (literally “many shapes”) malware is malicious code that alters its appearance through encryption and obfuscation, making sure that no two samples look the same. It is hard for traditional or legacy AV software based on signatures to catch this type of malware, because the transformation code is not visible for security analysis. Although futuristic-sounding, it’s actually an older technique that has been used by threat actors since the early 1990s.

Campaign Analysis

The SideWinder APT group’s new campaign leveraging server-side polymorphism to deliver the next stage payload began in late November 2022. The malicious documents used in this campaign were created to target Pakistan government officials. The documents were designed to trick Pakistan officials by displaying convincing content relevant to their interests.

During the investigation, the BlackBerry Threat Research and Intelligence team analyzed the documents used by the threat group to identify various artefacts used in this campaign to potentially locate other files of interest. The first malicious lure we examined was a document titled “GUIDELINES FOR BEACON JOURNAL – 2023 PAKISTAN NAVY WAR COLLEGE (PNWC)”.



GUIDELINES FOR BEACON JOURNAL - 2023 PAKISTAN NAVY WAR COLLEGE (PNWC)

Pakistan Navy War College (PNWC) invites manuscripts for its journal (Beacon-23). The journal is accredited with HEC in 'Y' category. Research articles shall be accepted in areas related to International Relations, Strategic Studies, International and Regional Security, South Asian Studies, Maritime Security, Indian and Pacific Ocean studies and Hybrid Warfare.

Submission Deadlines: Research scholars who wish to contribute original, unpublished articles to the journal may submit these by first week of January, 2023. The articles may be written individually or co-authored.

Article word limit: The manuscripts should normally be 5000 (+_ 10%) words excluding abstract, author's Introduction, footnotes and bibliography.

Format: All article submissions must include an abstract of about 200-250 words with 5-7 keywords and footnotes. The first page of the manuscript should contain the title of the paper, the name(s) of author(s), abstract and footnote giving introduction and current affiliation of the author(s). A 'Disclaimer' must be made at (footnote 2) and when applicable.

Plagiarism: Similarity index (Turnitin Report) must not exceed 18%.

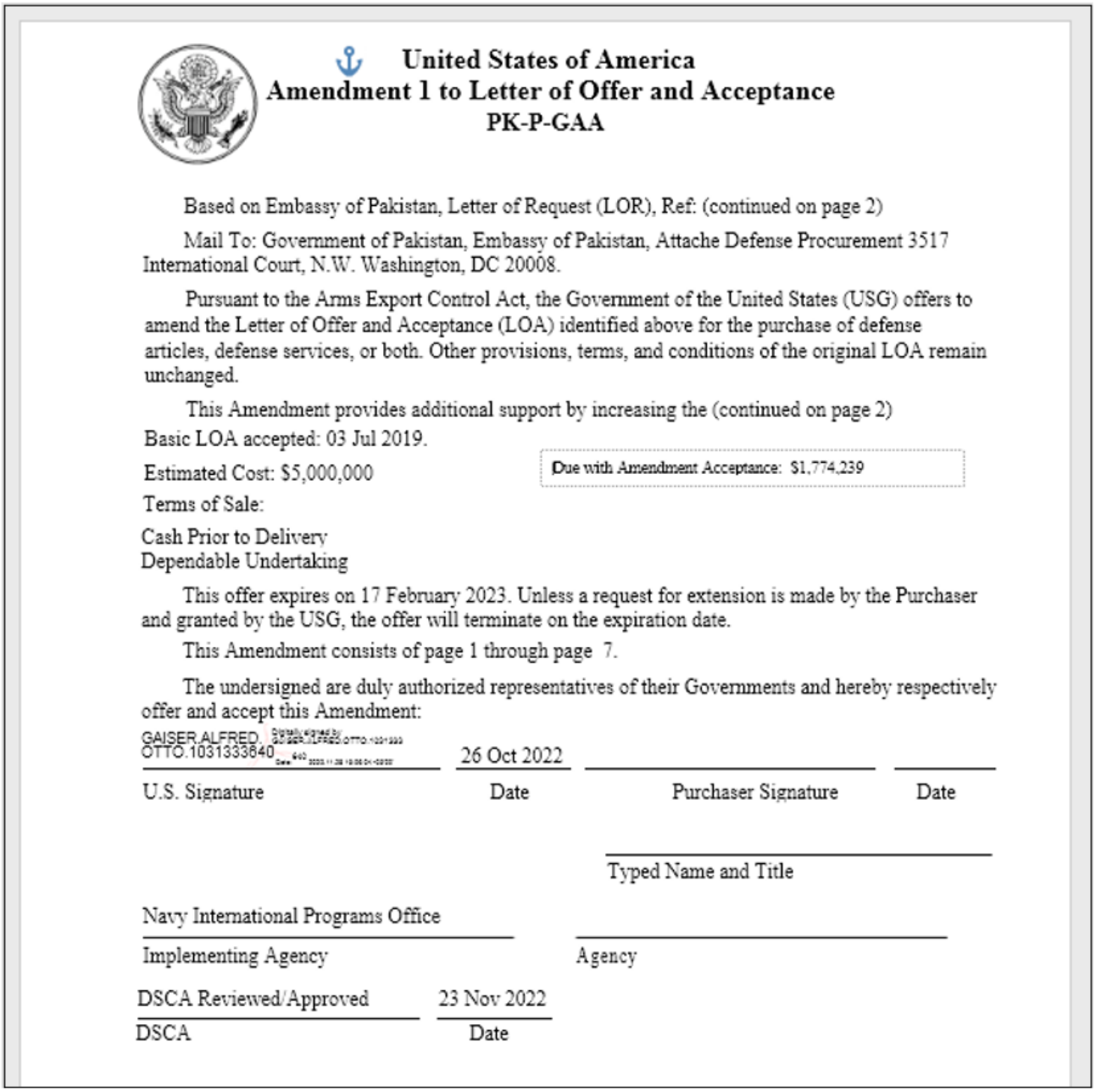
Editorial and Peer Review Process: All submissions are screened using "Similarity Index" detection software. Articles shortlisted by the Editorial Board will undergo double-blind peer review. During this stage, articles may not be approved for publication by the referees. However, they are found suitable for the Journal, reviewers may recommend either major or minor changes in the manuscript. The revision process may take multiple rounds. Peer Review timelines vary depending on Reviewer availability, area of expertise and responsiveness.

Citation Format:	Footnotes and Bibliography must comply with Chicago Manual of Style 17th Edition. Some examples for Footnotes are cited below for guidance:
Book:	Peter W Rose, Class in Archaic Greece (Cambridge: Cambridge University Press,2012), 95.
Chapter of Book:	John D Kelly, "Seeing Red: Mao Fetishism, Pax Americana, and the Moral Economy of War ," in Anthropology and Global Counterinsurgency, ed. John D. Kelly et al. (Chicago: University of Chicago Press,2010), 77.
Journal Article:	Joshua I. Weinstein, "The Market in Plato's Republic" Classical Philology 104 (2009): 440.
Newspaper/Magazine Article:	Daniel Mendelsohn, "But Enough about Me," New York Times, January 25, 2021, 68.
Website:	Helen Regan, Nikhil Kumar and Sophia Saifi, "Pakistan Shot Down Two Indian Jets Inside Its Airspace," CNN.com, Accessed February 28, 2021, https://edition.cnn.com/2021/02/28/india-pakistan- strikes-escalation-intl/index.html.

Figure 1: Malicious lure document targeting Pakistan officials

MD5	3b853ae547346befe5f3d06290635cf6
SHA256	bc9d4eb09711f92e4e260efcf7e48906dca6bf239841e976972fd74dac412e2f
File Name	PK_P_GAA_A1_Offerred.docx
File Size	36.35 KB (37220 bytes)
Created	2022-12-06 05:24:37 UTC
Author	Windows User
Last Modified	2022-12-06T05:24:37Z
Last Modified by	Windows User

Another malicious document that was used in early December 2022 was titled “PK_P_GAA_A1_Offerred.docx”. In this instance, the document was eight pages in length and pretended to be a letter of offer and acceptance “for the purchase of defense articles, defense services, or both.”



United States of America
Amendment 1 to Letter of Offer and Acceptance
PK-P-GAA

Based on Embassy of Pakistan, Letter of Request (LOR), Ref: (continued on page 2)

Mail To: Government of Pakistan, Embassy of Pakistan, Attache Defense Procurement 3517 International Court, N.W. Washington, DC 20008.

Pursuant to the Arms Export Control Act, the Government of the United States (USG) offers to amend the Letter of Offer and Acceptance (LOA) identified above for the purchase of defense articles, defense services, or both. Other provisions, terms, and conditions of the original LOA remain unchanged.

This Amendment provides additional support by increasing the (continued on page 2)

Basic LOA accepted: 03 Jul 2019.

Estimated Cost: $5,000,000

Due with Amendment Acceptance: $1,774,239

Terms of Sale:

Cash Prior to Delivery
Dependable Undertaking

This offer expires on 17 February 2023. Unless a request for extension is made by the Purchaser and granted by the USG, the offer will terminate on the expiration date.

This Amendment consists of page 1 through page 7.

The undersigned are duly authorized representatives of their Governments and hereby respectively offer and accept this Amendment:

GAISER.ALFRED.OTTO.1031333640 — 26 Oct 2022

U.S. Signature | Date | Purchaser Signature | Date

Typed Name and Title

Navy International Programs Office

Implementing Agency | Agency

DSCA Reviewed/Approved — 23 Nov 2022

DSCA | Date

Figure 2: First malicious lure sent by the SideWinder APT group

Notably, none of the documents used an embedded malicious macro code to deliver the next stage payload; instead, the threat group exploited the CVE-2017-0199 vulnerability (remote template injection).

The “GUIDELINES FOR JOURNAL - 2023 PAKISTAN NAVY WAR COLLEGE (PNWC).doc“ malicious lure template was instructed to reach out to the remote address of “hxxps[:]//pnwc[.]bol-north[.]com/5808/1/3686/2/0/0/0/m/files-a2e589d2/**file[.]rtf**”. The “pnwc[.]bol-north[.]com” domain in this instance resolves to the IP address 5.230.73[.]106.

Figure 3: The URL for the next stage download

The “PK_P_GAA_A1_Offerred.docx” malicious lure template was instructed to reach out to the remote address of “hxxps[:]//paknavy-gov-pkp[.]downld[.]net/14578/1/6277/2/0/0/0/m/files-75dc2b1e/**file[.]rtf**” to download the next stage. The “paknavy-gov-pk[.]downld[.]net” domain resolves to the IP address 185.205.187[.]234.

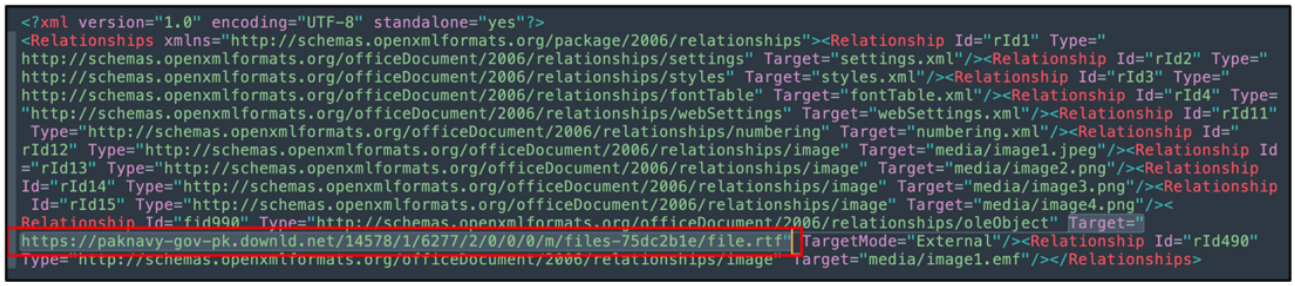


Figure 4: URL for next stage download

During the time when the malicious server was active, this threat group had set their servers in a way that if the user/victim enters part of the malicious URL into their browser, they will be redirected to the *legitimate* Pakistan Navy home page, which is hxxps[:]//www[.]paknavy[.]gov[.]pk. It is important to note that the malicious server is no longer active.

Figure 5: Legitimate Pakistan Navy website. The victim is redirected to this site from a malicious page.

In early March, we discovered a new document that was also spread through phishing emails. The peculiarity of this OLE document was that it contained the address of the connection to the malicious server, which was also configured to connect to victims from Turkey.

MD5	b7e63b7247be18cdfb36c1f3200c1dba
SHA256	8af93bed967925b3e5a70d0ad90eae1f13bc6e362ae3dac705e984f8697aaaad
File Name	Product.docx
File Size	579.69 KB (593604 bytes)
Created	2023-03-07 13:54:00 UTC
Author	user
Last Modified	2023-03-07T13:56:00Z
Last Modified by	user

Weaponization

The next stage payload “file.rtf”, a rich text document file, can only be downloaded by users in the Pakistani IP range. It is important to note that in both instances, only the name of the file “file.rtf” and the file type are the same; however, the contents, file size and the file hash are different. This is an example of server-based polymorphism, where each time the server responds with a different version of file, so bypassing the victim’s antivirus scanner (presuming the antivirus uses signature-based detection).

If the user is not in the Pakistani IP range, the server returns an 8-byte RTF file (**file.rtf**) that contains a single string: {\rtf1 }. However, if the user is within the Pakistani IP range, the server then returns the RTF payload, which varies between 406KB – 414KB in size.

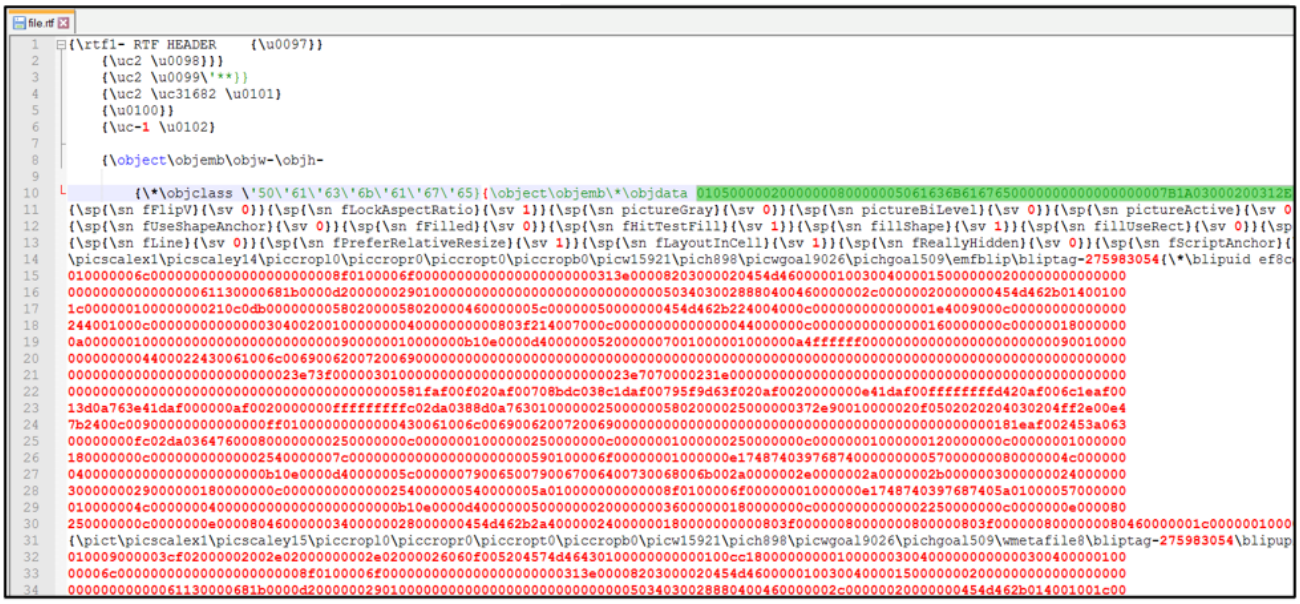


Figure 6: "file.rtf" malicious payload

Loader

Having listed the existing objects in the “file.rtf” file that was obtained from “paknavy-gov-pk[.]downld[.]net” domain, the “1.a” object was extracted for further analysis.

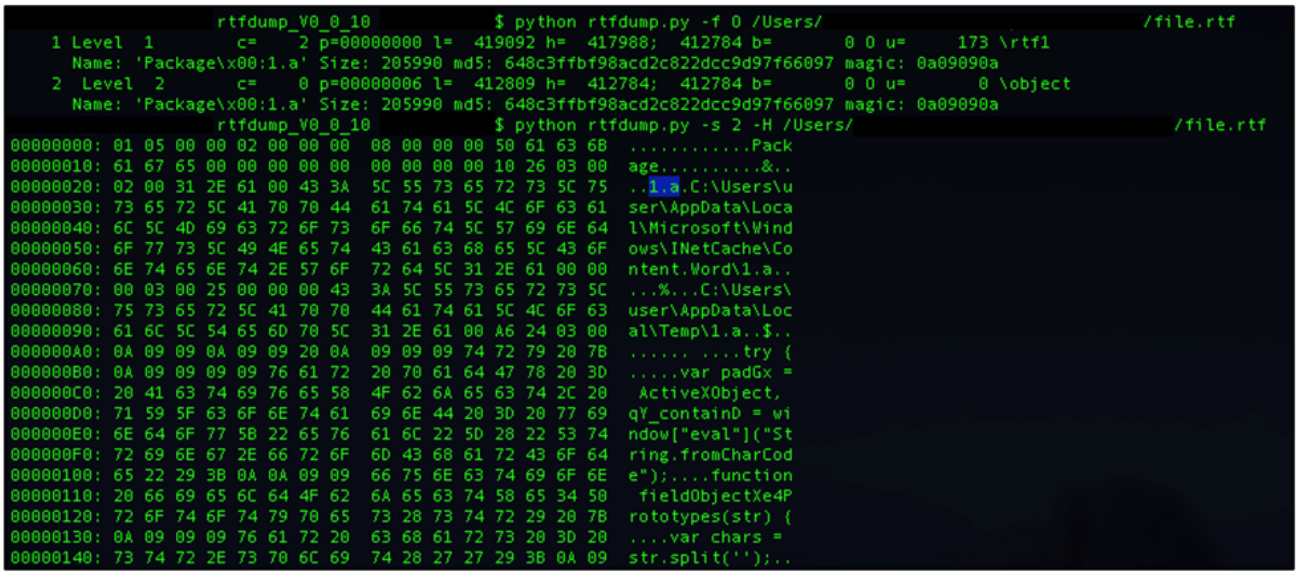


Figure 7: "1.a" object overview

During the malware execution chain, this object is saved under the “C:\Users\user\AppData\Local\Temp\1.a” location on the victim’s machine. The “1.a” file is an obfuscated JavaScript.

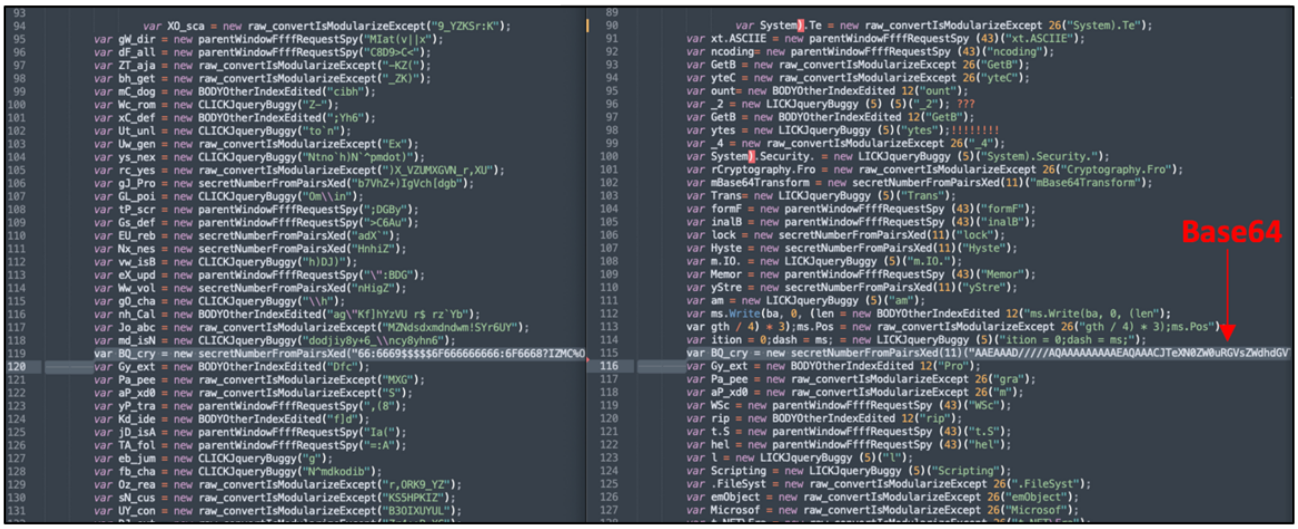


Figure 8: De-obfuscated strings

There are two things that stand out from our analysis – the base64 encoded data blob, and two URLs. The base64 data blob decodes to Win32 DLL(App.dll), and the two URLs are used for further communications with the threat actor.

Figure 9: URLs used for further communications with SideWinder

Agent

The previously mentioned base64 encoded data blob is a .NET compiled Win32 DLL called “App.dll”.

Hashes (md5, sha-256)	8934f22ed2d4390f2e6170e4cfdbd483 8b718a15f76768ba29849a5f4a6ca0ff1d9c8ba7bcdc9d89efc792fe20e9fdb5
ITW File Name	App.dll

Compilation Stamp	Fri Nov 16 02:26:21 2074
File Type/Signature	DLL
File Size	139339 (bytes)
Compiler Name/Version	Microsoft Visual C# / Basic .NET

To further avoid static signature-based detection, the “App.dll” file is obfuscated in the same way as the majority of other files and scripts uncovered in this campaign.

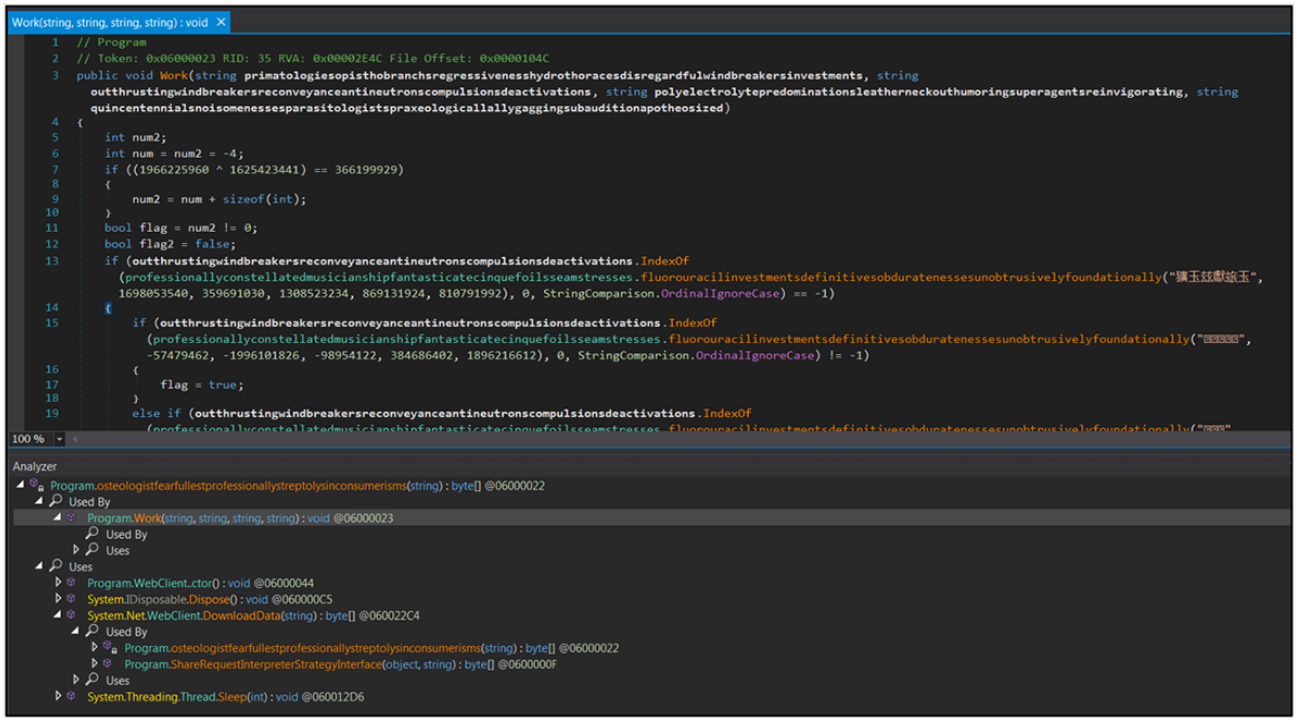


Figure 10: "App.dll" file

The “App.dll” file is launched by earlier stage JavaScript code. The JavaScript deserializes the .NET binary and passes a URL to the executable's “Work()” function. This function makes a request to the URL and attempts to decrypt and then execute the response. In other words, the .NET executable can retrieve the next stage code and execute it.

Network Infrastructure

SideWinder's campaign command-and-control (C2) infrastructure is only live for short periods of time. Non-Pakistani IP responses from the systems hosting RTF files have been identical since at least January 2021, with an 8-byte file with {\rtf1 } as the content. Following the relationships in VirusTotal shows the distribution infrastructure and the longevity of similar campaigns. 28 domains have been seen in the wild hosting this empty RTF file, all with similar URLs used for hosting.

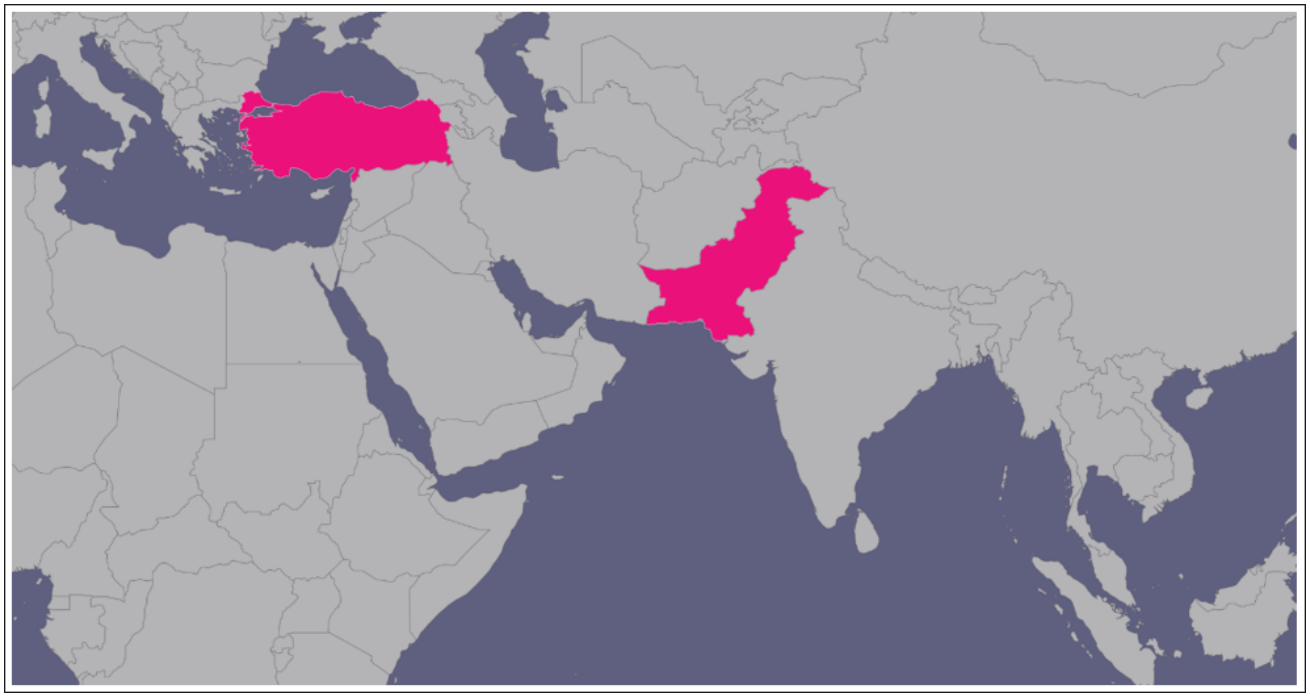
For these campaigns, SideWinder also uses predictable URL structures when hosting their malicious files:

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

The longevity of these tactics, techniques, and procedures (TTPs) – nearly 2 years – gives us confidence that they can be utilized for the detection of future campaigns.

In mid-March 2023, we discovered a new configured server delivering the payload. This server was different in that it was configured so that a victim in Turkey could receive a second-stage payload. This shows that this threat actor is also now targeting organizations in Turkey.

Targets



The SideWinder group's main target remains Pakistan government organizations. The campaign investigated by BlackBerry in early March 2023 identified Turkey as a new target.

Attribution

The SideWinder APT group's primary targets are in Southeast Asia regions such as Pakistan and Sri Lanka; however, government institutions in Pakistan still remain their main target of interest.

Conclusions

This report discussed the SideWinder group's targeted attack carried out in early December 2022. The latest SideWinder campaign targeting Turkey overlaps with the most recent developments in geopolitics; specifically, in Turkey's support of Pakistan and the ensuing reaction from India.

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. We hope this data will help provide protection and prevention measures going forward.

APPENDIX 1 – Indicators of Compromise (IoCs)

Indicator Type	Indicator
MD5	b7e63b7247be18cdfb36c1f3200c1dba
SHA256	8af93bed967925b3e5a70d0ad90eae1f13bc6e362ae3dac705e984f8697aaaad
MD5	5efddbdcf40ba01f1571140bad72dccb
SHA256	a45258389a3c0d4615f3414472c390a0aabe77315663398ebdea270b59b82a5c
MD5	3b853ae547346befe5f3d06290635cf6
SHA256	bc9d4eb09711f92e4e260efcf7e48906dca6bf239841e976972fd74dac412e2f
MD5	666b2b178ce52e30be9e69de93cc60a9
SHA256	cd09bf437f46210521ad5c21891414f236e29aa6869906820c7c9dc2b565d8be

MD5	ef00004a1ebc262ffe0fb89aa5524d42
SHA256	a3283520e04d7343ce9884948c5d23423499fa61cee332a006db73e2b98d08c3
MD5	6c7d24b90f3c6b4383bd7d08374a0c6f
SHA256	4db0a2d4d011f43952615ece8734ca4fc889e7ec958acd803a6c68b3e0f94eea
MD5	73750f08265bbe80c3f235318bcef6fe
SHA256	bc3c6f9d51e2bdb37e03b01e2949f72836ecee4230e2320c5dc33a83b55b062f
MD5	16341fcff1bc7388387fd17b4b3a7a50
	cf1f4ec1d7db6cf1fe8e15687b348a279889689fa9c387de4a2c310c34336f9f
MD5	1c62441de076eb5a5b2e1f8146767777
SHA256	75079e408ca9517825ffac396680a2d2169d691be3f1adbbd797e05e665c6fde
MD5	dacdb33b6e9de4c1fe8591bb5a65c55c
SHA256	cde768a4cf95e58f0e98e2bcca0663fd2c1a36510f6010065b4f54169a92e207
MD5	709e6a64735432c25cafb89951cc149c
SHA256	a2a9fd1db7f1dc196fa8af0669ea72d1f8ae48bf4775108ee746e0f83c5a7498
URL	hxxps[:]//paknavy-gov-pkp[.]downld[.]net/14578/1/6277/2/0/0/0/m/files-75dc2b1e/file[.]rtf
URL	hxxps[:]//pnwc[.]bol-north[.]com/5808/1/3686/2/0/0/0/m/files-a2e589d2/file[.]rtf
IP	185.205.187[.]234
IP	5.230.73[.]106

URL	https[:]//cstc-spares-vip-163.dowmload[.]net/14668/1/1228/2/0/0/0/m/files-403a1120/file[.]rtf
URL	https[:]//mtss.bol-south[.]org/5974/1/8682/2/0/0/0/m/files-b2dff0ca/file[.]rtf
URL	https[:]//paknavy-gov-pk[.]downld[.]net/14578/1/6277/2/0/0/0/m/files-75dc2b1e/file[.]rtf
URL	hxxts[:]//paknavy-gov-pk[.]downld[.]net/14578/1/6277/2/0/0/0/m/files-75dc2b1e/file[.]rtf
URL	hxxts[:]//pnwc[.]bol-north[.]com/5808/1/3686/2/0/0/0/m/files-a2e589d2/file[.]rtf
URL	hxxts[:]//sl-navy[.]office-drive[.]live/45/1/334/2/0/0/0/m/files-fe9dade2/file[.]rtf
URL	hxxts[:]//forecast[.]comsats-net[.]com/5760/1/5041/2/0/0/0/m/files-dd96433f/file[.]rtf
URL	https[:]//forecast[.]comsats-net[.]com/5760/1/5039/2/0/0/0/m/files-d7c7dda1/file[.]rtf
URL	hxxts[:]//forecast[.]comsats-net[.]com/5760/1/5035/2/0/0/0/m/files-4a0480ae/file[.]rtf
URL	hxxts[:]//moma[.]comsats-net[.]com/5753/1/4375/2/0/0/0/m/files-8062311a/file[.]rtf
URL	hxxts[:]//forecast[.]comsats-net[.]com/5760/1/5040/2/0/0/0/m/files-f3b20b30/file[.]rtf
URL	hxxts[:]//forecast[.]comsats-net[.]com/5760/1/5036/2/0/0/0/m/files-2ad09cbd/file[.]rtf
URL	hxxts[:]//moma[.]comsats-net[.]com/5753/1/4371/2/0/0/0/m/files-b62d382f/file[.]rtf
URL	hxxts[:]//srilanka-navy[.]lforvk[.]com/135/1/334/2/0/0/0/m/files-4fdaf6c7/file[.]rtf

URL	hxxts[:]//promotionlist[.]comsats-net[.]com/5756/1/8887/2/0/0/0/m/files-3d1dff0f/file[.]rtf
URL	hxxts[:]//dgms[.]paknavy-gov[.]com/5733/1/5051/2/0/0/0/m/files-73bdca4d/file[.]rtf
URL	hxxts[:]//mofadividion[.]ptcl-gov[.]com/5724/1/3268/2/0/0/0/m/files-11e30891/file[.]rtf
URL	hxxts[:]//ksew[.]kpt-gov[.]org/5663/1/3275/2/0/0/0/m/files-937950ad/file[.]rtf
URL	hxxts[:]//ministryofforeignaffairs-mofa-gov-pk[.]dytt88[.]org/14444/1/2454/2/0/0/0/m/files-9ba90b7f/file[.]rtf
URL	hxxt[:]//bdmil[.]alit[.]live/3398/1/50073/2/0/0/0/m/files-ac995f17/file[.]rtf
URL	hxxt[:]//navy-mil-bd[.]jmicc[.]xyz/5625/1/8145/2/0/0/0/m/files-b11074b7/file[.]rtf
URL	hxxts[:]//navy-mil-bd[.]jmicc[.]xyz/5625/1/8145/2/0/0/0/m/files-b11074b7/file[.]rtf
URL	hxxts[:]//paknavy[.]jmicc[.]xyz/5627/1/4367/2/0/0/0/m/files-9e0912cc/file[.]rtf
URL	hxxt[:]//bdmil[.]alit[.]live/3398/1/54346/2/0/0/0/m/files-491dc489/file[.]rtf
URL	hxxts[:]//paknavy[.]comsats[.]xyz/5552/1/5037/2/0/0/0/m/files-1b5c7556/file[.]rtf
URL	hxxts[:]//mofa-gov[.]interior-pk[.]org/14419/1/6/2/0/0/0/m/files-07b01f9b/file[.]rtf
URL	hxxt[:]//mofa-gov[.]interior-pk[.]org/14419/1/6/2/0/0/0/m/files-07b01f9b/file[.]rtf
URL	hxxts[:]//paknavy[.]paknavy[.]live/5516/1/4367/2/0/0/0/m/files-db71f6b3/file[.]rtf
URL	hxxts[:]//mofabn[.]ksewpk[.]com/5511/1/4993/2/0/0/0/m/files-18e5db65/file[.]rtf
URL	hxxt[:]//srilankanavy[.]ksew[.]org/5471/1/1101/2/0/0/0/m/files-cd6e6dbd/file[.]rtf
URL	hxxts[:]//srilankanavy[.]ksew[.]org/5471/1/1101/2/0/0/0/m/files-cd6e6dbd/file[.]rtf

URL	hxxt[:]//maritimepakistan[.]kpt-pk[.]net/5434/1/3694/2/0/0/0/m/files-ce32ed85/file[.]rtf
URL	hxxts[:]//maritimepakistan[.]kpt-pk[.]net/5434/1/3694/2/0/0/0/m/files-ce32ed85/file[.]rtf
URL	hxxt[:]//dgmp-paknavy[.]mod-pk[.]com/14325/1/10/2/0/0/0/m/files-5291bef6/file[.]rtf
URL	hxxts[:]//dgmp-paknavy[.]mod-pk[.]com/14325/1/10/2/0/0/0/m/files-5291bef6/file[.]rtf
URL	hxxt[:]//dgpr[.]paknvay-pk[.]net/5330/1/1330/2/0/0/0/m/files-4d9d0395/file[.]rtf
URL	hxxts[:]//cabinet-gov-pk[.]ministry-pk[.]net/14300/1/1273/2/0/0/0/m/files-68ebf815/file[.]rtf
URL	hxxts[:]//dgpr[.]paknvay-pk[.]net/5330/1/1330/2/0/0/0/m/files-4d9d0395/file[.]rtf
URL	hxxts[:]//careitservices[.]paknvay-pk[.]net/5359/1/4586/2/0/0/0/m/files-266ad911/file[.]rtf
URL	hxxts[:]//defencelk[.]cvix[.]live/3023/1/54082/2/0/0/0/m/files-0c31ed2d/file[.]rtf
URL	hxxt[:]//mohgovsg[.]bahariafoundation[.]live/5320/1/13/2/0/0/0/m/files-1ddf5195/file[.]rtf
URL	hxxts[:]//mohgovsg[.]bahariafoundation[.]live/5320/1/13/2/0/0/0/m/files-1ddf5195/file[.]rtf
URL	hxxts[:]//sppc[.]moma-pk[.]org/5281/1/4265/2/0/0/0/m/files-d2608a99/file[.]rtf
URL	hxxps[:]//mailrta.mfagov[.]org/3818/1/53382/2/0/0/0/m/files-c78a6966/file[.]rtf
URL	http[:]//mailnavybd.govpk[.]net/5845/1/12/2/0/0/0/m/files-ca78574e/file[.]rtf
URL	hxxts[:]//mailaplf[.]cvix[.]live/2968/1/50390/2/0/0/0/m/files-7630e91a/file[.]rtf

URL	hxxt[:]//slpa[.]mod-gov[.]org/5946/1/5775/2/0/0/0/m/files-fca3cc50/file[.]rtf
URL	hxxt[:]//slpa[.]mod-gov[.]org/5946/1/5780/2/0/0/0/m/files-20bba5af/file[.]rtf
URL	hxxt[:]//slpa[.]mod-gov[.]org/5946/1/5795/2/0/0/0/m/files-c9dddc54/file[.]rtf
URL	hxxt[:]//slpa[.]mod-gov[.]org/5946/1/5797/2/0/0/0/m/files-875e140b/file[.]rtf
URL	hxxt[:]//slpa[.]mod-gov[.]org/5946/1/5771/2/0/0/0/m/files-5995311a/file[.]rtf
URL	hxxt[:]//slpa[.]mod-gov[.]org/5946/1/5784/2/0/0/0/m/files-94153639/file[.]rtf
URL	hxxt[:]//slpa[.]mod-gov[.]org/5946/1/5770/2/0/0/0/m/files-2d21c32e/file[.]rtf
URL	hxxt[:]//slpa[.]mod-gov[.]org/5946/1/5778/2/0/0/0/m/files-27d5c7d3/file[.]rtf
URL	hxxt[:]//mailnavymilbd[.]govpk[.]net/5848/1/13/2/0/0/0/m/files-57d837e4/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5792/2/0/0/0/m/files-da7756e4/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5776/2/0/0/0/m/files-175c56e7/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5783/2/0/0/0/m/files-a26663eb/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5780/2/0/0/0/m/files-20bba5af/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5785/2/0/0/0/m/files-76f11745/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5788/2/0/0/0/m/files-3acec3be/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5782/2/0/0/0/m/files-78d7e141/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5796/2/0/0/0/m/files-97e02960/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5795/2/0/0/0/m/files-c9dddc54/file[.]rtf

URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5790/2/0/0/0/m/files-a3d0041a/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5773/2/0/0/0/m/files-5a31d681/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5799/2/0/0/0/m/files-03dd18bd/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5781/2/0/0/0/m/files-62caea91/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5804/2/0/0/0/m/files-c43dece3/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5794/2/0/0/0/m/files-60cb1621/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5775/2/0/0/0/m/files-fca3cc50/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5778/2/0/0/0/m/files-27d5c7d3/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5787/2/0/0/0/m/files-fb528413/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5786/2/0/0/0/m/files-5def1d52/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5798/2/0/0/0/m/files-c3178f3d/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5779/2/0/0/0/m/files-2f2e186d/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5789/2/0/0/0/m/files-8822f8ff/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5777/2/0/0/0/m/files-7f2e758b/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5791/2/0/0/0/m/files-bda6f896/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5769/2/0/0/0/m/files-2f6b9c9a/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5774/2/0/0/0/m/files-12eca223/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5772/2/0/0/0/m/files-84c4942a/file[.]rtf

URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5771/2/0/0/0/m/files-5995311a/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5797/2/0/0/0/m/files-875e140b/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5784/2/0/0/0/m/files-94153639/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5770/2/0/0/0/m/files-2d21c32e/file[.]rtf
URL	hxxts[:]//slpa[.]mod-gov[.]org/5946/1/5793/2/0/0/0/m/files-f2d0617e/file[.]rtf
URL	hxxts[:]//mailrta[.]mfagov[.]org/3818/1/53382/2/0/0/0/m/files-c78a6966/file[.]rtf
URL	hxxt[:]//promotionlist[.]comsats-net[.]com/5756/1/8887/2/0/0/0/m/files-3d1dff0f/file[.]rtf
URL	hxxts[:]//mailnavymilbd[.]govpk[.]net/5848/1/13/2/0/0/0/m/files-57d837e4/file[.]rtf
URL	hxxt[:]//mailnavybd[.]govpk[.]net/5845/1/12/2/0/0/0/m/files-ca78574e/file[.]rtf
Domain	slpa.mod-gov[.]org
IP	62.113.255[.]80
Domain	mailrta.mfagov[.]org
IP	194.61.121[.]216
Domain	promotionlist.comsats-net[.]com
IP	5.255.104[.]32
Domain	mailnavybd.govpk[.]net
IP	5.255.112[.]194
Domain	mailnavymilbd.govpk[.]net

APPENDIX 2 – Applied Countermeasures

YARA Rules

Available upon request (see below).

Suricata Rules

Available upon request (see below).

Disclaimer: *The private version of this report is available upon request. It includes but is not limited to the complete and contextual MITRE ATT&CK® mapping, MITRE D3FEND™ countermeasures, Attack Flow by MITRE, and other threat detection content for tooling, network traffic, complete IOCs list, and system behavior. Please email us at cti@blackberry.com for more information.*

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back