Кирилл Шипулин

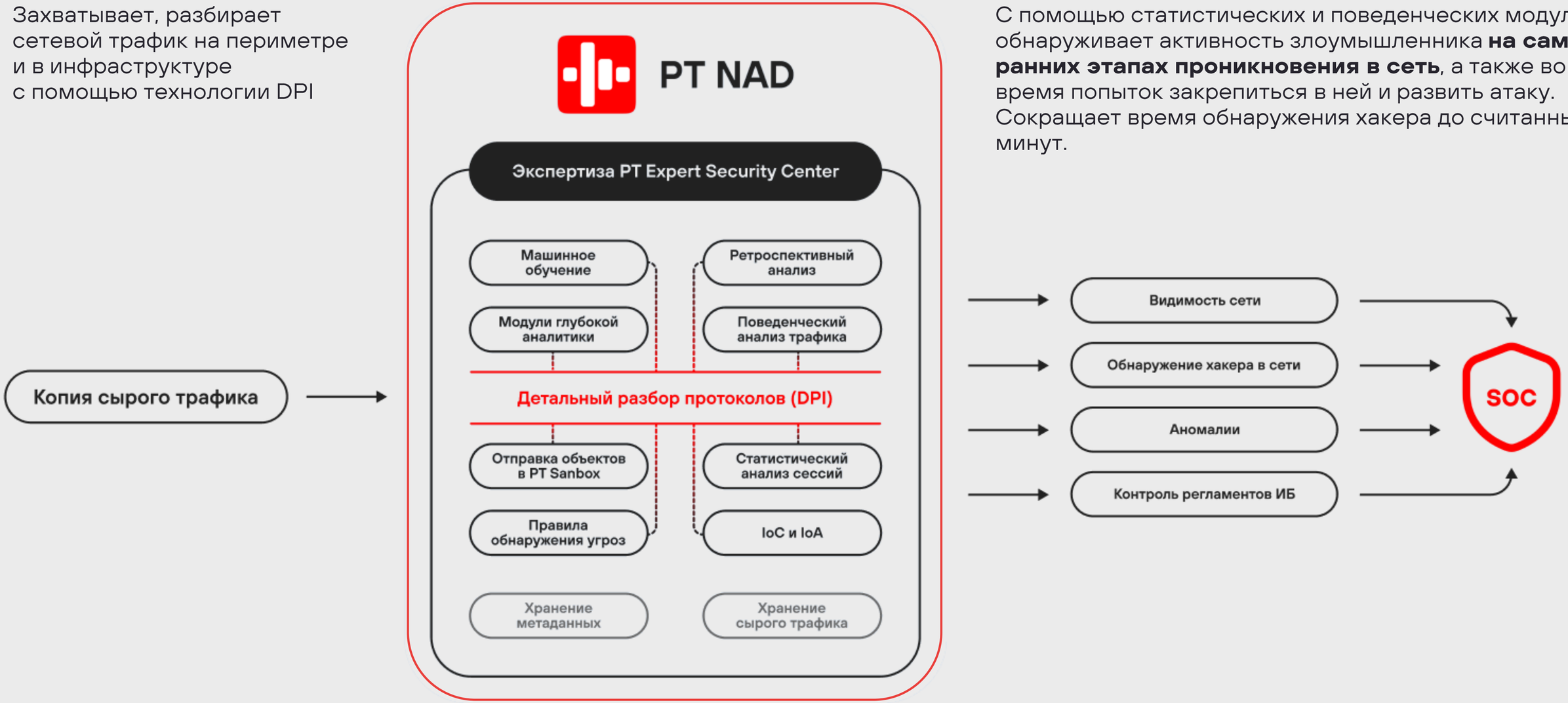
Старший специалист группы обнаружения
сетевых угроз экспертного центра ESC

PT NAD против Cobalt Strike и Brute Ratel C4

Как работает PT NAD

Захватывает, разбирает сетевой трафик на периметре и в инфраструктуре с помощью технологии DPI

С помощью статистических и поведенческих модулей обнаруживает активность злоумышленника **на самых ранних этапах проникновения в сеть**, а также во время попыток закрепиться в ней и развить атаку. Сокращает время обнаружения хакера до считанных минут.



Фреймворки для постэксплуатации зараженных систем

Самые известные:
Cobalt Strike и Brute Ratel C4

Созданы для специалистов по ИБ, но могут оказаться в руках злоумышленников

Количество инцидентов с ними большое и постоянно растет

GBHackers

Hackers Using Sliver Framework as an Alternative to Cobalt Strike & Metasploit

Sliver is an open-source command-and-control framework that is becoming increasingly popular among malicious actors at the current attacks.

25 янв. 2023 г.

The Stack

Hackers eye “Havoc” for C2 diversity, as Cobalt Strike detections improve

Hackers appear to be increasingly adopting the open source Havoc C2 framework as Cobalt Strike detections improve say researchers.

1 месяц назад

The Hacker News

Google Identifies 34 Cracked Versions of Popular Cobalt Strike Hacking Toolkit in the Wild

Google Cloud last week disclosed that it identified 34 different hacked release ver of the Cobalt Strike tool in the wild, the earliest...

Ведомости

Хакеры из группы Cobalt нанесли ущерб банкам на 1 млрд рублей

ЦБ в 2017 г. зафиксировал 21 волну атак преступной группы Cobalt более чем 240 банков, рассказал на X Уральском форуме «Информационная...

В компании подчеркивают, что тщательно проверяют всех покупателей лицензий Nighthawk, продают свой продукт только в определенные страны (ЕС, Австралия, Канада, Япония, Новая Зеландия, Норвегия, Швейцария и США), а также не распространяют пробные версии Nighthawk, так как это не раз приводило к злоупотреблению другими похожими продуктами в прошлом.

Как обнаруживают использование фреймворков

Большинство публичных способов обнаружения угроз используется **на узлах**: поиск аномалий, использование антивирусных сигнатур, анализ журналов, использование YARA-правил

В сети обнаружение угроз чаще всего происходит с помощью сигнатур для IDS и индикаторов компрометации

Некоторые исследователи ищут в интернете TLS-сертификаты, которые можно использовать по умолчанию, или хеши иконок, для поиска неизвестных управляющих серверов

Средства сетевой защиты часто выступают в роли догоняющих:

- IDS-сигнатуры пишутся для известных вредоносных семплов
- В индикаторы компрометации адреса попадают после инцидентов

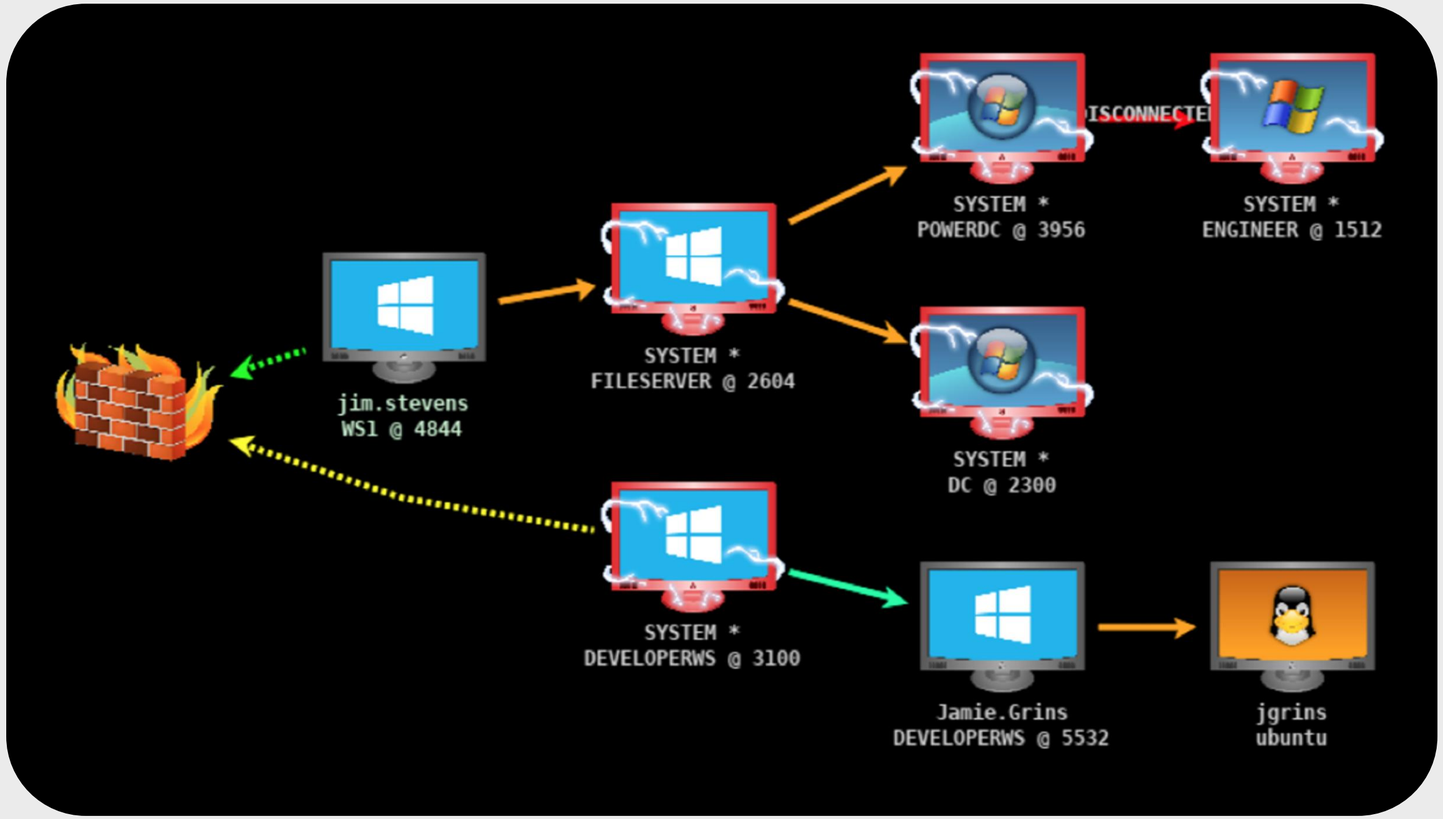
Cobalt Strike

Протоколы для связи
с управляющим сервером

- → **HTTP**
- → **HTTPS**
- → **DNS**

Протоколы для связи
между биконами

- → **SMB**
- → **TCP**



Cobalt Strike

Cobalt Strike **с каждым обращением к управляющему серверу** передает 128 байт шифрованных метаданных, которые могут рекурсивно кодироваться в разные формы: base64, netbios, xor.

Обращения обычно передаются с промежутком от 30 секунд до 5 минут со случайным отклонением

```
GET /jquery-3.3.1.min.js HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9
Referer: http://code.jquery.com/
Accept-Encoding: gzip, deflate
Cookie: __cfduid=Yszx4eTOvlZrAekhgC9J8jwK7KxfQQ44e9ocC
mDWkJhRv2fAGwfNPMxDyJviSqBD2lDunPh2GlWudQHg8zeR
dlEqMaKMQgFjXyorgtcc6laMiUxbHWhgcJ6G-Ip9BGz1h6AfRHR
Fed0cGKxyLJafmP1sUZalEcKk7ilMT4BTzk4
User-Agent: Mozilla/5.0 (Windows NT 6.3; Trident/7.0; rv:11.0
```

Malleable Config

Метаданные могут прятаться
в любом месте HTTP-запроса
и способны **мимикрировать**
под легитимные данные, например,
куки или JWT в теле запроса.

Мусорные данные можно добавлять
как к запросам, так и к ответам.
Например, полностью повторять
содержимое известных библиотек
JavaScript.

```
http-get {
    set uri "/jquery-3.3.1.min.js";
    set verb "GET";
    client {
        header "Accept"
"text/html,application/xhtml+xml,application/xml;q=0.9";
        header "Host" "code.jquery.com";
        header "Referer" "http://code.jquery.com/";
        header "Accept-Encoding" "gzip, deflate";
        metadata {
            base64url;
            prepend "__cfduid=";
            header "Cookie";
        }
    }
```

Cobalt Strike

```
GET /image/ v29f1tcLDDK80Qw...XSDDa51wg4sdOrU-.jpg
GET /image/ vdZiAoa9X8az468fY...nM1f_ndxNb465cA-.jpg
GET /image/ pXPHv80XrNvAEKr...K7QzRSg2M4Rotw-.jpg
```

Несмотря на то, что сами метаданные не меняются от запроса к запросу, Cobalt Strike имеет в арсенале xor-шифрование со случайным ключом.
Передаваться такие данные могут в URL-адресе.

```
http-get {
    set uri "/image/";
    set verb "GET";
    client {
        output {
            mask;
            base64url;
            append “-.jpg”
            uri-append;
        }
    }
```

Cobalt Strike

Метаданные

- Передаются с каждым обращением к управляющему серверу
- Хранятся в одном и том же месте
- Кодируются одинаково
- Имеют одинаковый размер
- Время между обращениями почти неизменно

Cobalt Strike

Метаданные

- Передаются с каждым обращением к управляющему серверу
- Хранятся в одном и том же месте
- Кодируются одинаково
- Имеют одинаковый размер
- Время между обращениями почти неизменно

Алгоритм обнаружения

- Собрать побольше HTTP-запросов
- Найти, где хранятся метаданные
- Убедиться в неизменности HTTP-хедеров
- Декодировать и проверить энтропию
- Проверить временные интервалы
- Учесть похожий легитимный трафик

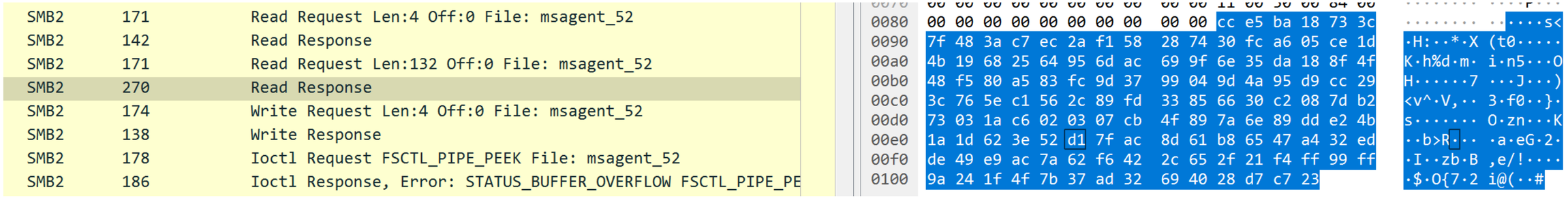
Cobalt Strike

SMB

- 132 байта метаданных в начале
- 4 байта длины перед каждым отстуком
- Мусорные данные перед полем длины
- Настраиваемое имя файла

TCP

- 132 байта метаданных в начале
- 4 байта длины перед каждым обращением к управляющему серверу
- Мусорные данные перед полем длины
- Настраиваемый порт



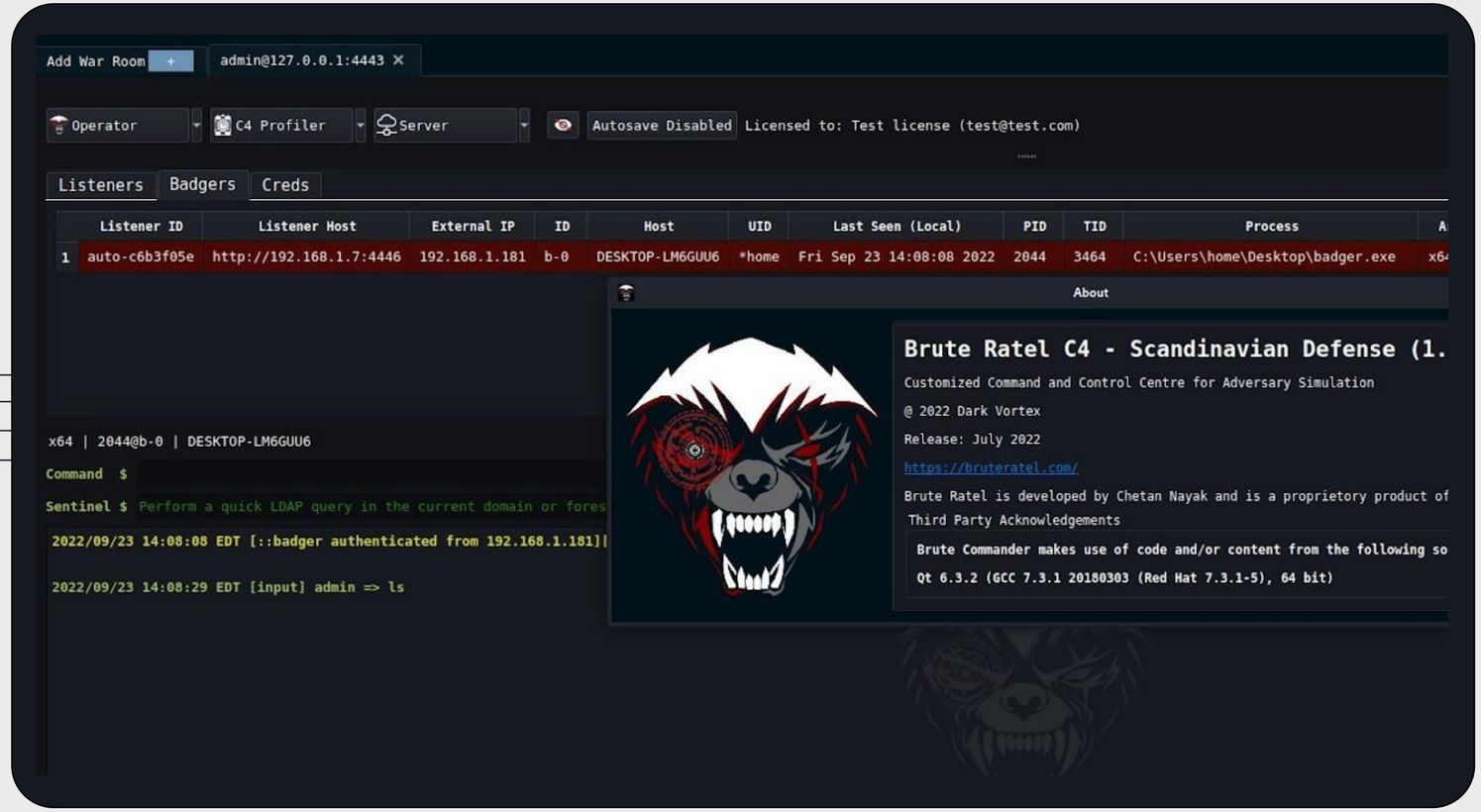
Brute Ratel C4

Упор сделан на обход узловых СЗИ

Первые релизы в 2021 году

Публичный слив в декабре 2022 года

Badger doesn't care. It takes what it wants!



Brute Ratel C4

Отличия
от Cobalt Strike

```
POST /example.php HTTP/1.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64
Host: 10.0.180.142:8080
Content-Length: 108
Cache-Control: no-cache

y4lldKvro7CMW0Zxil2U1pVmYvFKsndTJ622SET/Dnnc0xJ2/ve8b
f8H2GeQ8aupwT9rdOW9yKRhjpOJDhzJSCAKvp4r/IT64QYVHd
0qT5l=
```

- 80 байт метаданных
- Передаются только в теле POST-запроса
- Кодируются только в Base64
- Ротация URL-адреса

Демо

Другие фреймворки

- Sliver
- Havoc
- Meterpreter
- Covenant
- C3

```
POST /oauth2callback/database/oauth2callback/authenticate/rpc.html?
ij=z22219621&p=781310z05 HTTP/1.1
Host: 10.211.55.22
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/100.0.9070.541 Safari/537.36
Content-Length: 1047
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip

WEEDLIKE BEAMLESS ZOMBIES UNWARRANTABLE MEDIATIONS STONECROP DACTYLOLOGY GENTAMICIN
APHTHAE MUCLUCS UMBERS SKIVVY MESHUGGAH PITCHFORKING BEARDEDNESSES REANOINTS BUCKSHOT
COSTUMERY PENTACLE SOURPUSS COPOLYMERS DREARY DECLIVITIES QUADRICEPSES POOLHALL
GEOMAGNETISM JARLS BLUECAPS THICKHEADED PITCHFORKING VASSAL ASSIGNERS KECKING WOORALI
NONLIBRARIAN SULLENLY HYDROSERES VACATIONED INCUR SITUATING FAIRLEAD MUCLUCS EXPLICABLE
SPECIFICITIES REPLETION TREWS ORRIS DEVIANCY TEABOARD POOLHALL OUTCOACHED THICKHEADED
BANTERS OUTBOAST RUNDOWN GRIPPIEST KEYSTONE SALUTARY WHIRLWINDS ALLEGRETTOS SANDBARS
LECTOR UNWARRANTABLE OCTOSYLLABICS ABNEGATOR PINEAL ANTICLING NEIGHED CASE COHOLDERS
COUNTERTENDENCY CROAK ANTITUSSIVE INNOVATIONAL MESHUGGENER GEOMAGNETISM CONSERVATORSHIP
NEIGHED COHOLDERS POIKILOTHERMIC UMPIRING OCTAVES MANDAMUS BIOGAS SKIVVY GABFESTS
OVERDRIVE NAZI UNRESOLVABLE GROUNDINGS SQUATLY MUCKRAKING EMBRASURE PREPROCESSING
OVERORGANIZE OVERDRIVE FOZY TALLAGES TETRAHEDRA EMETIN CARAMELIZE SLOBBERERS OEDEMATA
SWOTTED WATERFLOODED REUTTERS
```

https://github.com/tcostam/awesome-command-control

Скоро увидимся! →

Телеграм-чат
о PT NAD
t.me/PTNADChat

Дополнительные
материалы о PT NAD
clck.ru/33f7PP

pt@ptsecurity.com

ptsecurity.com