

Кирилл Шипулин

Старший специалист группы обнаружения
сетевых угроз экспертного центра ESC

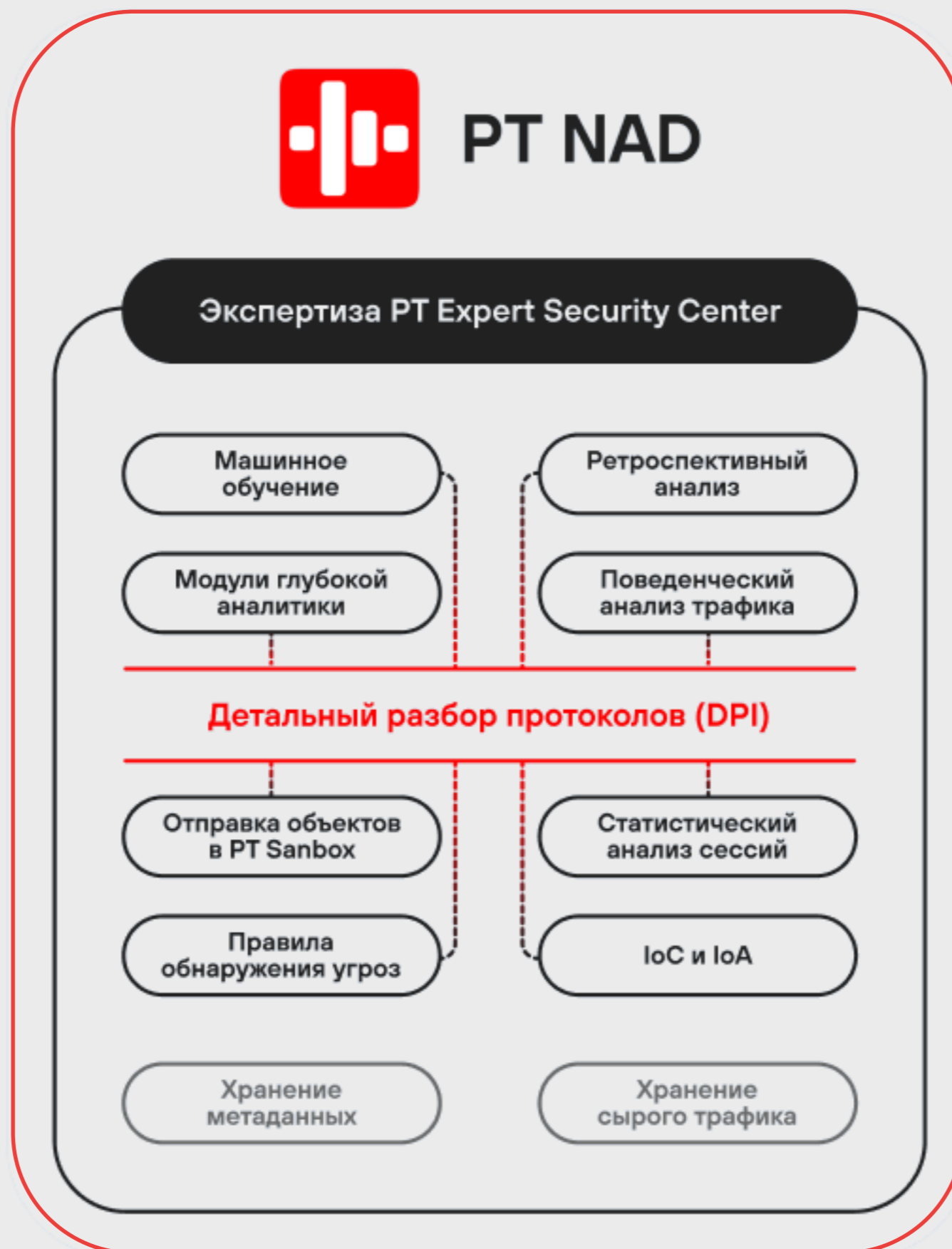


**PT NAD против
Cobalt Strike
и Brute Ratel C4**

Как работает PT NAD



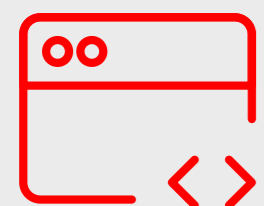
Захватывает, разбирает сетевой трафик на периметре и в инфраструктуре с помощью технологии DPI



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 versions of the Cobalt Strike tool in the wild, the earliest...

 Ведомости

Хакеры из группы Cobalt нанесли ущерб банкам на 1 млрд рублей

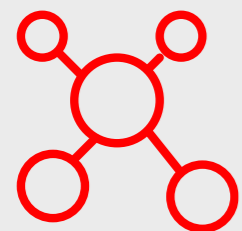
ЦБ в 2017 г. зафиксировал 21 волну атак преступной группы Cobalt более чем 240 банков, рассказал на X Уральском форуме «Информационная...

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:

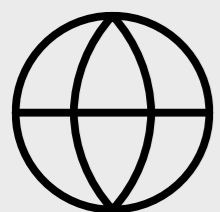
- IDS-сигнатуры пишутся для известных вредоносных семплов
- В индикаторы компрометации адреса попадают после инцидентов

Cobalt Strike



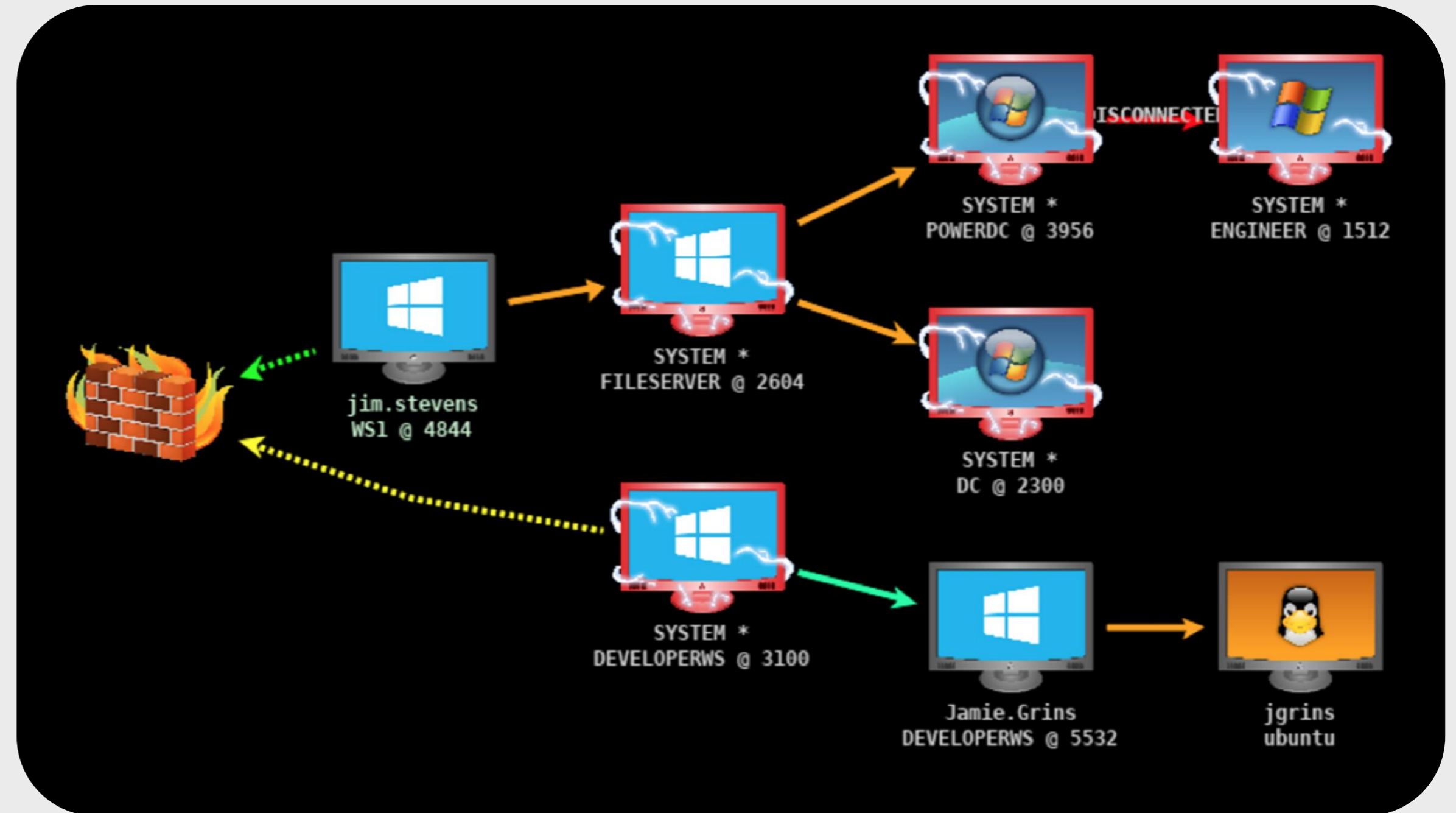
Протоколы для связи
с управляющим сервером

- HTTP
- HTTPS
- DNS



Протоколы для связи
между биконами

- SMB
- TCP



Cobalt Strike



Cobalt Strike **с каждым обращением к управляющему серверу** передает 128 байт зашифрованных 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  
mDWkJhRv2fAGwfNPMxDyJviSqBD2IDunPh2GIWudQHg8zeR  
dIEqMaKMQgFjXyorgtcc6laMiUxbHWhgCJ6G-lp9BGz1h6AfRHR  
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 хог-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;
        }
    }
}
```


Метаданные

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



Метаданные

- Передаются с каждым обращением к управляющему серверу
- Хранятся в одном и том же месте
- Кодироваться 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 отступом
- 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

SMB2	171	Read Request Len:4 Off:0 File: msagent_52	0070	00 00 00 00 00 00 00 00 00 00 11 00 30 00 04 00P....
SMB2	142	Read Response	0080	00 00 00 00 00 00 00 00 00 00 cc e5 ba 18 73 3cs<
SMB2	171	Read Request Len:132 Off:0 File: msagent_52	0090	7f 48 3a c7 ec 2a f1 58 28 74 30 fc a6 05 ce 1d	·H:··*·X (t0····
SMB2	270	Read Response	00a0	4b 19 68 25 64 95 6d ac 69 9f 6e 35 da 18 8f 4f	K·h%d·m· i·n5···0
SMB2	174	Write Request Len:4 Off:0 File: msagent_52	00b0	48 f5 80 a5 83 fc 9d 37 99 04 9d 4a 95 d9 cc 29	H·····7 ··J···)
SMB2	138	Write Response	00c0	3c 76 5e c1 56 2c 89 fd 33 85 66 30 c2 08 7d b2	<v^·V,·· 3·f0··}
SMB2	178	Ioctl Request FSCTL_PIPE_PEEK File: msagent_52	00d0	73 03 1a c6 02 03 07 cb 4f 89 7a 6e 89 dd e2 4b	s······ 0·zn···K
SMB2	186	Ioctl Response, Error: STATUS_BUFFER_OVERFLOW FSCTL_PIPE_PEEK	00e0	1a 1d 62 3e 52 d1 7f ac 8d 61 b8 65 47 a4 32 ed	··b>R· ·· ·a·eG·2·
			00f0	de 49 e9 ac 7a 62 f6 42 2c 65 2f 21 f4 ff 99 ff	·I··zb·B ,e/!····
			0100	9a 24 1f 4f 7b 37 ad 32 69 40 28 d7 c7 23	·\$.0{7·2 i@(..#

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!

The screenshot displays the Brute Ratel C4 interface. At the top, there's a window title 'admin@127.0.0.1:4443'. Below it are several tabs: 'Operator', 'C4 Profiler', 'Server', 'Autosave Disabled', and 'Licensed to: Test license (test@test.com)'. There are three main sections: 'Listeners', 'Badgers', and 'Creds'. The 'Listeners' section contains a table with the following data:

Listener ID	Listener Host	External IP	ID	Host	UID	Last Seen (Local)	PID	TID	Process	A	
1	auto-c6b3f05e	http://192.168.1.7:4446	192.168.1.181	b-0	DESKTOP-LM6GUU6	*home	Fri Sep 23 14:08:08 2022	2044	3464	C:\Users\home\Desktop\badger.exe	x64

Below the table, there's a terminal window showing the following output:

```
x64 | 2044@b-0 | DESKTOP-LM6GUU6
Command $
Sentinel $ Perform a quick LDAP query in the current domain or fores
2022/09/23 14:08:08 EDT [::badger authenticated from 192.168.1.181]
2022/09/23 14:08:29 EDT [input] admin => ls
```

On the right side, there's an 'About' section with a logo of a badger and the following text:

Brute Ratel C4 - Scandinavian Defense (1.
Customized Command and Control Centre for Adversary Simulation
@ 2022 Dark Vortex
Release: July 2022
<https://bruteratel.com/>
Brute Ratel is developed by Chetan Nayak and is a proprietary product of
Third Party Acknowledgements
Brute Commander makes use of code and/or content from the following so
Qt 6.3.2 (GCC 7.3.1 20180303 (Red Hat 7.3.1-5), 64 bit)

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
- Кодироваться 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 CAMELIZE SLOBBERERS OEDEMATA  
SWOTTED WATERFLOODED REUTTERS
```

Скоро увидимся! →



Telegram-чат
о PT NAD
t.me/PTNADChat



Дополнительные
материалы о PT NAD
clck.ru/33f7PP





pt@ptsecurity.com



ptsecurity.com