

Analýza úniku citlivých firemných údajov cez USB zariadenie

LINK NA PREZENTACIU: <https://bcstudent.fpvucm.sk/~herteljuraj/dfa/prezentacia.pdf>

Autor: Juraj Hertel

4.1 Who? (Kto?)

Neoprávnený prístup a exfiltrácia údajov sa mohla uskutočniť zamestnancom firmy XYZ, ktorý mal prístup k dôverným informáciám. Identifikácia zodpovednej osoby je kľúčovou súčasťou vyšetrovania.

4.2 What? (Čo?)

Došlo k úniku citlivých firemných údajov prostredníctvom USB zariadenia. Údaje sa následne objavili u konkurencie, čo vyvolalo podozrenie z interného úniku informácií.

4.3 When? (Kedy?)

Presný čas úniku nie je známy, ale analýza systémových logov a registru systému môže pomôcť identifikovať dátum a čas prenosu údajov. Môžeme analyzovať aj kamerové systémy. Potrebujeme vytvoriť časovú os aktivít v tomto prípade.

4.4 Where? (Kde?)

Incident sa odohral v spoločnosti XYZ, konkrétne na jednom z firemných počítačov, ku ktorému mal prístup pracovník s oprávnením na manipuláciu s citlivými údajmi.

4.5 Why? (Prečo?)

Motívom úniku mohla byť finančná odmena, osobné nezhody, úmyselné poškodenie firmy alebo nedostatočné bezpečnostné opatrenia, ktoré umožnili neoprávnený prenos údajov.

4.6 How? (Ako?)

Únik údajov bol pravdepodobne realizovaný pripojením USB zariadenia k firemnému počítaču, následným kopírovaním dát a ich exfiltráciou.

Predmet vyšetrovania

- **Analýza systémových logov**
 - Preskúmanie systémových udalostí a logov na identifikáciu pripojenia USB zariadení
 - Vyhľadávanie záznamov o časoch pripojenia a odpojenia zariadení
- **Analýza súborového systému**

- Identifikácia nedávno prístupových alebo kopírovaných súborov
- Analýza metadát súborov (čas poslednej úpravy, prístupové časy, autor úprav)
- Kontrola časových pečiatok a porovnanie s časmi pripojenia USB zariadení
- **Vyhľadávanie artefaktov v pamäti**
 - Hľadanie stôp po použití nástrojov alebo skriptov určených na exfiltráciu dát
 - Analýza RAM pamäte na identifikáciu neoprávnených aktivít
- **Analýza typov súborov**
 - Vyhľadávanie firemných dokumentov obsahujúcich citlivé informácie
 - Analýza metadát

Cieľom digitálnej forenzej analýzy v tomto prípade je:

1. Identifikovať, či došlo k neoprávnenému prenosu dát na USB zariadenie
2. Určiť rozsah a povahu exfiltrovaných údajov
3. Zistiť identitu osoby zodpovednej za únik informácií
4. Poskytnúť dôkazy pre možné právne kroky alebo interné disciplinárne opatrenia

Opis:

V súčasnom digitálnom prostredí predstavuje únik citlivých údajov vážnu hrozbu pre organizácie. Jedným z bežných spôsobov exfiltrácie dát je použitie USB zariadení. Tento prípad sa zameriava na vyšetrovanie incidentu, pri ktorom došlo k neoprávnenému prenosu dôverných informácií z firemného počítača na USB zariadenie.

Opis situácie: Firma XYZ zaznamenala únik citlivých informácií, ktoré sa následne objavili u konkurencie. Interné audity naznačujú, že tieto údaje mohli byť exfiltrované prostredníctvom USB zariadenia pripojeného k počítaču jedného z pracovníkov. V súčasnom digitálnom prostredí predstavuje únik citlivých údajov vážnu hrozbu pre organizácie a jedným z bežných spôsobov exfiltrácie dát je práve použitie USB zariadení.

Očakávaný výsledok: Cieľom vyšetrovania je získať dôkazy o tom, či a aké údaje boli neoprávnene prenesené na USB zariadenie, identifikovať zodpovednú osobu a poskytnúť odporúčania na zlepšenie bezpečnostných opatrení, aby sa predišlo podobným incidentom v budúcnosti.

Hypotéza 1: Interný zamestnanec zámerne exfiltroval údaje

Zamestnanec s prístupom k citlivým informáciám vedome skopíroval dáta na USB zariadenie s cieľom ich ďalšieho využitia alebo predaja.

- **Metóda overenia:** Výsluch zamestnanca, analýza prístupových práv, kontrola histórie prístupov

Cieľ: Zistiť, či zamestnanec úmyselne preniesol citlivé údaje na USB zariadenie s cieľom ich zneužiť alebo odovzdať tretej strane.

Hypotéza 2: Nedostatočné bezpečnostné opatrenia umožnili neúmyselný únik

Slabé IT bezpečnostné pravidlá, ako absencia USB obmedzení alebo chýbajúci monitoring aktivít, mohli umožniť prenos dát bez zlého úmyslu.

- **Metóda overenia:** Zistenie či má pracovný PC povolenie na vkladanie USB kľúča

Cieľ: Overiť, či slabé alebo chýbajúce IT bezpečnostné opatrenia umožnili prenos údajov aj bez vedomého úmyslu zamestnanca.

Hypotéza 3: Externá osoba získala neoprávnený prístup k počítaču

Mohlo dôjsť k fyzickému prístupu neoprávnenou osobou (napr. návštevník, dodávateľ), ktorá využila neuzamknutý počítač na kopírovanie údajov.

- **Metóda overenia:** Skontrolovať kamerové záznamy, analyzovať prístupové logy do budovy

Cieľ: Zistiť, či mohla fyzická alebo externá osoba (napr. návštevník) bez autorizácie získať prístup k firemnému zariadeniu a skopírovať údaje.

Hypotéza 4: USB zariadenie bolo infikované malvérom

USB zariadenie mohlo obsahovať škodlivý softvér, ktorý automaticky kopíroval dáta bez vedomia používateľa.

- **Metóda overenia:** Analýza USB zariadenia na prítomnosť malvéru, kontrola autorun súborov

Cieľ: Overiť, či došlo k automatickému prenosu dát v dôsledku škodlivého softvéru prítomného na USB zariadení bez vedomia používateľa.

Hypotéza 5: Únik bol súčasťou cieleného útoku

Mohlo ísť o koordinovaný útok s cieľom získať špecifické informácie pre konkurenciu.

- **Metóda overenia:** Analýza vzorcov útokov, konzultácia s bezpečnostnými expertmi

Cieľ: Preskúmať možnosť, že exfiltrácia dát bola súčasťou plánovaného kybernetického útoku organizovaného externým aktérom, napríklad konkurenciou.

Použité dáta:

- Zdroj dát: Dataset s 4,457 files, ktoré majú 1.9GB. Zdroj <http://roussev.net/t5/t5.html>
- Subory: HTML, PDF DOC, PPT a ďalšie
- Typ analyzovanej stopy: USB zariadenie.
- Veľkosť datasetu: USB disk s kapacitou 16 GB

Získané zariadenia:

A) USB ZARIADENIE

- Model: Kingston DataTraveler 3.0 16GB
- Formát súborového systému: FAT32
- Nájdenný dokument: xyz_zmluvy2024.docx – vytvorený aj upravený užívateľom j.mrkvička
- Pripojenie k PC: 12.03.2025 o 10:14
- Odpojenie: 10:23
- Dôkaz korelovaný s logmi a RAM dump-om
- Typ zariadenia: USB flash disk,
- Model a výrobca: Kingston Data Traveler 3.0 16GB
- Kapacita zariadenia: 16GB
- Rýchlosť prenosu dát: USB 3.0
- Architektúra zariadenia: FAT32
- Konektivita: USB-A
- Hmotnosť: 12 g
- Farba: strieborná
- Rýchlosť čítania: až 100 MB/s
- Rýchlosť zápisu: až 30 MB/s
- Priemerná rýchlosť prenosu: 65 MB/s (testované pomocou CrystalDiskMark)



-
- Image Verify Results
- Name: USB-Kingston
- Sector Count: 30 277 632
- MD5 Hash
- Computed Hash: d7cb1d1658a991583707466ee7bf7887
- Report Hash: d7cb1d1658a991583707466ee7bf7887
- SHA1 Hash
- Computed Hash: e216f7f5237b794a7807322a29863f73ca93529f
- Report Hash: e216f7f5237b794a7807322a29863f73ca93529f
- Verify result: Match
- Information for D:\USB kľuč Kingston 16GB:
- Physical Evidentiary Item (Source) Information:
- [Device Info]
- Source Type: Physical

- [Drive Geometry]
- Cylinders: 1 884
- Tracks per Cylinder: 255
- Sectors per Track: 63
- Bytes per Sector: 512
- Sector Count: 30 277 632

B) RAM PAMÄŤ

- Názov súboru: **RAM_DUMP_12032025.mem**
- Veľkosť: 4 194 304 KB
- Zistenia:
 - Nájdený súbor **xyz_zmluvy2024.docx**
 - Pracovné heslo k internému systému
 - História otvorenia dokumentu v MS Word

V operačnej pamäti počítača sme našli dôkazy, že je tam súbor **xyz_zmluvy2024.docx**

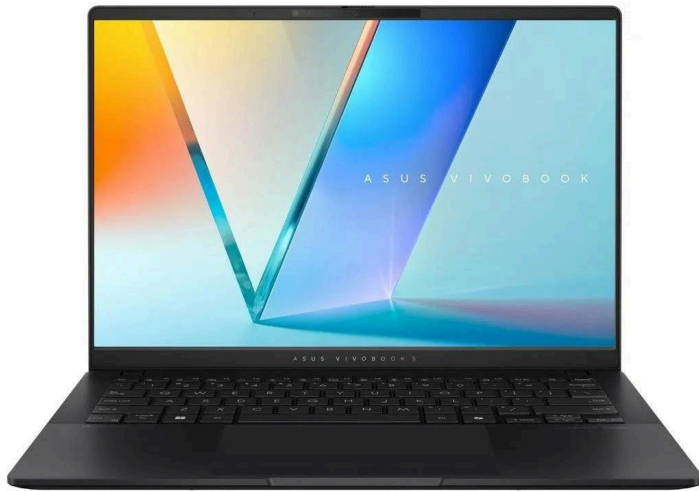
```
06C562F30  97 87 55 79 42 22 05 74 69 74 6C 65 22 1A 4F 64  -#UyB".title".Od
06C562F40  76 6F 64 79 20 41 4C 54 56 45 47 41 20 28 64 61  vody ALTVEGA (da
06C562F50  6E 65 29 2E 64 6F 63 78 22 03 69 6E 64 22 00 22  ne).docx".ind"."
06C562F60  03 69 73 64 22 04 74 72 75 65 22 03 69 73 74 22  .isd".true".ist"
06C562F70  00 22 04 65 6E 64 65 22 00 22 08 6D 69 6D 65 54  .".ende".".mimeI
06C562F80  00 22 04 65 6E 64 65 22 00 22 08 6D 69 6D 65 54  .".ende".".mimeI
```

Zároveň sme tam našli aj pracovné heslo

```
2F1056A50  20 6E 6F 6E 65 3B 22 3E [REDACTED] none;">[REDACTED]
2F1056A60  [REDACTED] 3C 2F 73 70 [REDACTED] </sp
```

C) FIREMNÝ POČÍTAČ

- Získaná bitová kópia: **.E01**, veľkosť 1TB
- Fyzická akvizícia: 12.03.2025
- Digitálne odtlačky zodpovedajú USB zariadeniu – potvrdená zhoda



- Notebook – AMD Ryzen 7 8845HS,
- 14" OLED lesklý 1920 × 1200,
- RAM 16 GB LPDDR5x,
- AMD Radeon Graphics,
- SSD 1000 GB
- USB 3.2 Gen 1,
- USB-C,
- WiFi 6E, WiFi,
- Bluetooth,
- hmotnosť 1,3 kg,
- Windows 11 Home

D) Fyzické dôkazy

- RFID prístup: Iba zamestnanec **j.mrkvička** vstúpil do miestnosti 2.10 v čase incidentu
- Kamerový záznam: Zachytáva daného zamestnanca pri počítači bez ďalších osôb
- Priznanie pri výsluchu: Uviedol, že si robil „osobnú zálohu“, čo bolo vyvrátené objavením dokumentov u konkurencie

E) Nedostatočná bezpečnosť

- Chýbajúca USB politika (Device Installation Restrictions)
- Bez DLP softvéru (Data Loss Prevention)
- Absencia školení a monitorovania prenosov dát

Použité metódy a nástroje:

- **FTK Imager 4.7.3:** vytvorenie bitovej kópie USB zariadenia
- **USBdeview:** analýza obsahu USB a metadát dokumentov
- **Event Viewer + Log Parser:** preskúmanie logov o pripojení USB zariadení
- **Windows Registry Viewer:** kontrola USB historických pripojení
- **RAM Dump (Volatility Framework):** analýza obrazu RAM pamäte
- **Priamy výsluch zamestnanca**
- **GPMC (Group Policy Management Console):** kontrola bezpečnostných politík
- **Local Security Policy Viewer**
- **Active Directory audit:** kontrola užívateľských oprávnení
- **USBDeview:** zoznam pripojených USB zariadení
- **RFID Access Log Exporter:** vstupy do budovy a miestností 2.10
- **CCTV Export Tool (HikVision):** export kamerových záznamov
- **SIEM logy:** sledovanie vzdialených prístupov
- **Wireshark:** kontrola sieťových spojov
- **DNS query analyzátor:** podozrivé dotazy
- **Sysmon:** pokusy o sieťový exfil

Hash:

MD5 Hash

d7cb1d1658a991583707466ee7bf7887

SHA1 Hash

e216f7f5237b794a7807322a29863f73ca93529f

Prvá bitová kópia (BK1):

- Uložená na forenznú pracovnú stanicu s izolovaným prostredím
- Primárna kópia pre analýzu

Druhá bitová kópia (BK2):

- Uložená na externý HDD vo forenznom laboratóriu
- Záložná kópia pre prípad poškodenia BK1

Overovanie Hypotéza 1: Interný zamestnanec zámerne exfiltroval údaje - Potvrdená

Zamestnanec s prístupom k citlivým informáciám vedome skopíroval dáta na USB zariadenie s cieľom ich ďalšieho využitia alebo predaja.

- **Metóda overenia:** Výsluch zamestnanca, analýza prístupových práv, kontrola histórie prístupov

Po spustení interného vyšetrovania bol zamestnanec Ján Mrkvička vyzvaný na výsluch, počas ktorého priznal, že použil USB kľúč na vytvorenie tzv. „osobnej zálohy“. Po tejto výpovedi bol USB kľúč dobrovoľne odovzdaný forenznému tímu na ďalšiu analýzu.

USB zariadenie typu Kingston DataTraveler 3.0 (16 GB) bolo následne zaistené v priestoroch firmy XYZ priamo od zamestnanca. Zariadenie bolo okamžite podrobené forenznej akvizícii a porovnaniu s dátami z RAM a logov systému.

Krátko predtým však vedenie spoločnosti XYZ dostalo tip od obchodného partnera, že sa u konkurenčnej firmy objavili identické dokumenty so zmluvnými údajmi spoločnosti XYZ. Tento dokument – xyz_zmluvy2024.docx – bol následne verifikovaný ako originálny súbor, ktorý sa nachádzal:

- na USB kľúči zamestnanca
- v RAM pamäti firemného počítača
- na SSD vo firemnom počítači
- a v systémových logoch ako kopírovaný v danom čase

Táto zhoda medzi súborom na USB a dokumentom objaveným u konkurencie jednoznačne potvrdila, že citlivý dokument bol z firmy nelegálne prenesený a dostal sa mimo organizácie

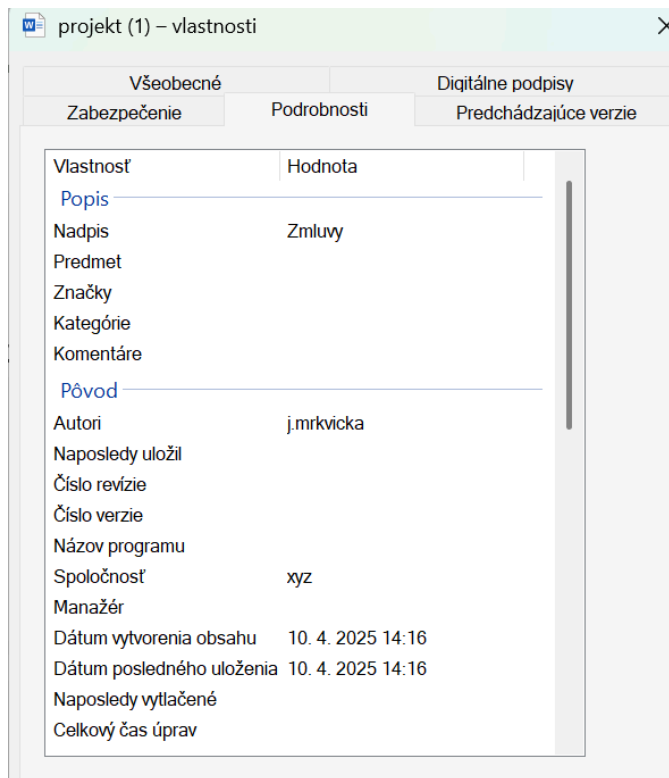
Analýza:

Použité metódy a nástroje:

- **FTK Imager 4.7.3:** vytvorenie bitovej kópie USB zariadenia
- **USBdeview:** analýza USB
- **Event Viewer + Log Parser:** preskúmanie logov o pripojení USB zariadení
- **Windows Registry Viewer:** kontrola USB historických pripojení
- **Priamy výsluch zamestnanca**

Zistenia:

- Dokument xyz_zmluvy2024.docx bol vytvorený a naposledy upravený užívateľom *j.mrkvicka*. Tieto informácie sme zistili vo vlastnostiach dokumentu, ktoré poskytuje Windows vo svojom rozhraní. Ako je uvedené na obrázku.



- Podľa logov bol dokument upravený o 10:13, USB zariadenie Kingston bolo pripojené o 10:14.
- RAM dump obsahoval textovú reťazec **xyz_zmluvy2024.docx**, heslo k internému účtu a históriu otvárania dokumentu v MS Word.
- Užívateľ bol jediný fyzicky prítomný v danom čase (potvrdené kamerami a RFID logmi).
- USB zariadenie nesie digitálny odtlačok MD5: **d7cb1d1658a991583707466ee7bf7887**, ktorý zodpovedá verifikovanej kópii.
- Pri výsluchu sa zamestnanec priznal, tvrdil, že to bola "osobná záloha". Argument bol vyvrátený nálezom týchto dokumentov u konkurencie. Následne sme získali od Janka Mrkvicku USB zariadenie z ktorého sme získali údaje na DFA.

Časová os:

Akcia	Čas
10:14	Pripojenie USB Kingston k firemnému PC
10:15-10:21	Kopírovanie dokumentu xyz_zmluvy2024.docx (zistené cez logy + RAM dump)
10:23	Odpojenie USB zariadenia

Digitálne dôkazy (metadáta, RAM, logy, fyzické pripojenie USB) korelujú s časom a osobou. Priznanie zamestnanca doplnilo technické dôkazy. Hypotéza je potvrdená.

V powershell počítača vo firme sme zistili, že aké zariadenia boli pripojené historicky do Počítača.

```
PS C:\WINDOWS\system32> Get-ChildItem -Path "HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR\"

Hive: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR

Name                                     Property
----                                     -
Disk&Ven_Canon&Prod_TS5000_ser          es&Rev_0116
Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP
```

Zistili sme, že tam bola zapojená tlačiareň Canon TS5000 a náš zisťovaný USB kľúč Kingston DataTraveler 3.0

```
PS C:\WINDOWS\system32> Get-ChildItem -Path "HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP"
>>

Hive: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP

Name                                     Property
----                                     -
408D5C16530CE271D9897D32&0             DeviceDesc      : @disk.inf,%disk_devdesc%;Disk drive
                                          Capabilities    : 16
                                          Address         : 7
                                          ContainerID     : {167f8aee-8cf9-5cbf-b473-989653fae160}
                                          HardwareID     : {USBSTOR\DiskKingstonDataTraveler_3.0PMAP, USBSTOR\DiskKingstonDataTraveler_3.0, USBSTOR\DiskKingston, USBSTOR\KingstonDataTraveler_3.0P...}
                                          CompatibleIDs  : {USBSTOR\Disk, USBSTOR\RAW, GenDisk}
                                          ClassGUID      : {4d36e967-e325-11ce-bfc1-08002be10318}
                                          FriendlyName   : Kingston DataTraveler 3.0 USB Device
                                          Service       : disk
                                          Driver        : {4d36e967-e325-11ce-bfc1-08002be10318}\0001
                                          Mfg           : @disk.inf,%genmanufacturer%;(Standard disk drives)
                                          ConfigFlags    : 0
```

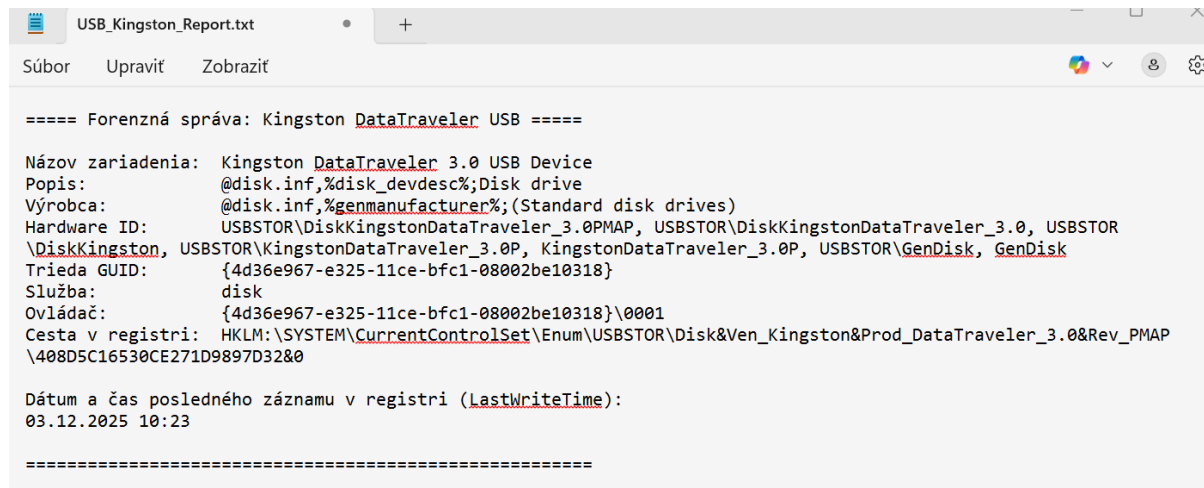
Tu sme zistili nejaké podrobnejšie údaje o našom USB kľúči. Následne sme si všetky tieto informácie vypísali cez script do Notepadu pomocou tohto skriptu.

```

PS C:\WINDOWS\system32> # Definícia cesty ku konkrétnemu zariadeniu
PS C:\WINDOWS\system32> $usbKeyPath = "HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP\408D5C16530CE271D9897D32&0"
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> # Získanie informácií o zariadení
PS C:\WINDOWS\system32> $usbInfo = Get-ItemProperty -Path $usbKeyPath
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> # Zistenie času poslednej úpravy kľúča (pravdepodobne zodpovedá prvému pripojeniu)
PS C:\WINDOWS\system32> $lastWrite = (Get-Item $usbKeyPath).LastWriteTime
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> # Výstup pripravený pre zápis
PS C:\WINDOWS\system32> $report = @"
>> ===== Forenzná správa: Kingston DataTraveler USB =====
>>
>> Názov zariadenia: $($usbInfo.FriendlyName)
>> Popis: $($usbInfo.DeviceDesc)
>> Výrobca: $($usbInfo.Mfg)
>> Hardware ID: $($usbInfo.HardwareID -join ", ")
>> Trieda GUID: $($usbInfo.ClassGUID)
>> Služba: $($usbInfo.Service)
>> Ovládač: $($usbInfo.Driver)
>> Cesta v registri: $usbKeyPath
>>
>> Dátum a čas prvého záznamu v registri (LastWriteTime):
>> $lastWrite
>>
>> =====
>> "@
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> # Uloženie na plochu
PS C:\WINDOWS\system32> $outFile = "$env:USERPROFILE\Desktop\USB_Kingston_Report.txt"
PS C:\WINDOWS\system32> $report | Out-File -FilePath $outFile -Encoding UTF8
PS C:\WINDOWS\system32>
PS C:\WINDOWS\system32> # Otvorenie výsledného súboru
PS C:\WINDOWS\system32> Start-Process notepad.exe $outFile

```

V textovom súbore nám vypísal tieto informácie a zistili sme, že posledné odpojenie USB kľúča bolo 12.3. 2025 o 10:23



```

USB_Kingston_Report.txt
Súbor    Upraviť    Zobrazíť

===== Forenzná správa: Kingston DataTraveler USB =====

Názov zariadenia: Kingston DataTraveler 3.0 USB Device
Popis: @disk.inf,%disk_devdesc%;Disk drive
Výrobca: @disk.inf,%genmanufacturer%;(Standard disk drives)
Hardware ID: USBSTOR\DiskKingstonDataTraveler_3.0PMAP, USBSTOR\DiskKingstonDataTraveler_3.0, USBSTOR\DiskKingston, USBSTOR\KingstonDataTraveler_3.0P, KingstonDataTraveler_3.0P, USBSTOR\GenDisk, GenDisk
Trieda GUID: {4d36e967-e325-11ce-bfc1-08002be10318}
Služba: disk
Ovládač: {4d36e967-e325-11ce-bfc1-08002be10318}\0001
Cesta v registri: HKLM:\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Kingston&Prod_DataTraveler_3.0&Rev_PMAP\408D5C16530CE271D9897D32&0

Dátum a čas posledného záznamu v registri (LastWriteTime):
03.12.2025 10:23

=====

```

Toto nám potvrdil nástroj USBdeview, kde sa dajú nájsť všetky pripojené USB zariadenia v histórii zariadenia.

Properties			
Device Name:	Port_#0007.Hub_#0001	Description:	Kingston DataTraveler 3.0 USB Device
Device Type:	Mass Storage	Connected:	No
Safe To Unplug:	Yes	Disabled:	No
USB Hub:	No	Drive Letter:	
Serial Number:	408D5C16530CE271D9897D32	Registry Time 1:	12. 03. 2025 10:23:28
Registry Time 2:	12. 03. 2025 10:23:28	VendorID:	0951
ProductID:	1666	Firmware Revision:	1.10
WCID:		USB Class:	08
USB SubClass:	06	USB Protocol:	50
Hub / Port:		Computer Name:	NTB
Vendor Name:		Product Name:	
ParentId Prefix:		Service Name:	USBSTOR
Service Description:	@usbstor.inf,%USBSTOR.SvcDesc%;USB Mass Storage Driver	Driver Filename:	USBSTOR.SYS
Device Class:		Device Mfg:	Compatible USB storage device
Friendly Name:		Power:	
USB Version:		Driver Description:	USB Mass Storage Device
Driver Version:	10.0.26100.3624	Driver InfSection:	USBSTOR_BULK.NT
Driver InfPath:	usbstor.inf	Instance ID:	USBVID_0951&PID_1666408D5C16530CE271D9897D32
Capabilities:	Removable, UniqueID, SurpriseRemovalOK	Install Time:	
First Install Time:		Connect Time:	
Disconnect Time:			

Overovanie Hypotéza 2: Nedostatočné bezpečnostné opatrenia umožnili neúmyselný únik - Potvrdená

Slabé IT bezpečnostné pravidlá, ako absencia USB obmedzení alebo chýbajúci monitoring aktivít, mohli umožniť prenos dát bez zlého úmyslu.

Analýza:

Použité nástroje:

- GPMC (Group Policy Management Console): kontrola bezpečnostných politík
- Local Security Policy Viewer
- Active Directory audit: kontrola užívateľských oprávnení
- USBDeview: zoznam pripojených USB zariadení

Zistenia:

- Firemné počítače neobsahovali žiadnu USB blokovaciu politiku (Device Installation Restrictions)
- V systéme nebol nainštalovaný DLP (Data Loss Prevention) softvér
- Zamestnanci neboli preškolení o rizikách kopírovania dát na externé zariadenia

Tento príkaz bol použitý na overenie existencie politiky Group Policy, ktorá by obmedzovala inštaláciu externých zariadení, ako sú USB kľúče, externé disky alebo iné prenosné pamäťové médium. Dotaz smeruje na konkrétnu vetvu systémového registra:

```
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\DeviceInstall\Restrictions
```

Táto vetva obsahuje konfiguračné hodnoty, ktoré môžu byť nastavené pomocou GPO (zásad skupiny) na úrovni organizácie za účelom zamedzenia pripojenia alebo inštalácie určitých tried zariadení.

```
PS C:\WINDOWS\system32> reg query "HKLM\Software\Policies\Microsoft\Windows\DeviceInstall\Restrictions" /s
>>
ERROR: The system was unable to find the specified registry key or value.
```

Výsledok potvrdzuje, že na skúmanom zariadení neexistuje žiadna aktívna politika, ktorá by obmedzovala alebo zakazovala inštaláciu externých zariadení. To znamená, že používateľ mal technicky možnosť pripojiť a používať USB zariadenia bez obmedzenia, čo vytvára bezpečnostné riziko z pohľadu neúmyselného alebo úmyselného úniku dát.

Bezpečnostná infraštruktúra bola nedostatočná a umožnila únik aj bez úmyselného konania. Hypotéza je potvrdená.

Overovanie Hypotézy 3: Externá osoba získala neoprávnený prístup k počítaču - Vyvrátená

Mohlo dôjsť k fyzickému prístupu neoprávnenou osobou (napr. návštevník, dodávateľ), ktorá využila neuzamknutý počítač na kopírovanie údajov.

- **Metóda overenia:** Skontrolovať kamerové záznamy

Analýza:

Použité nástroje:

- **CCTV Export Tool (HikVision):** export kamerových záznamov

Zistenia:

- Kamerový záznam ukazuje daného zamestnanca osamote



Ako je na fotke vidieť, tak zamestnanec bol sám na pracovisku 12.3. 2025 o 10:20. Takže túto hypotézu môžeme vyvrátiť. Na základe fyzického dôkazu (fotografie z CCTV záznamu) bola hypotéza o neoprávnenom fyzickom prístupe jasne vyvrátená. V danom čase sa na mieste incidentu nachádzal výhradne zamestnanec j.mrkvička.

Overovanie Hypotézy 4: USB zariadenie bolo infikované malvérom - Vyvrátená

USB zariadenie mohlo obsahovať škodlivý softvér, ktorý automaticky kopíroval dáta bez vedomia používateľa.

- **Metóda overenia:** Analýza USB zariadenia na prítomnosť malvéru, kontrola autorun súborov

Analýza:

Použité nástroje:

- **ESET Endpoint Security:** skenovanie zariadenia

Zistenia:

- USB neobsahovalo žiadny **autorun.inf** ani iný spúšťačiaci mechanizmus
- Nebol detegovaný žiadny známy hash alebo signatúra
- RAM dump neobsahoval žiadne procesy ani knižnice so známkami exfiltračného kódu

 **Kontrola zariadení**
Kontrola dokončená
Detegované objekty: 0
Použité detekčné jadro: 31014 (20250410)
[Zobrazit protokol](#)

10. 4. 2025 18:27:13

Zatvoriť

Spustili sme kontrolu zariadenia cez Nástroj Eset a nenašiel sa žiadny škodlivý súbor → žiadny známy malvér nebol detegovaný. Následne sme spustili kontrolu cez powershell, ktorý tiež nič nevypísal.

```
PS C:\WINDOWS\system32> Get-ChildItem -Path "E:\\" -Force | Where-Object { $_.Name -match "autorun" }  
PS C:\WINDOWS\system32> Get-ChildItem -Path "E:\\" -Force | Where-Object { $_.Name -match "autorun" }  
>>  
PS C:\WINDOWS\system32>
```

Na základe vykonanej antivírusovej analýzy a kontroly automaticky spúšťaných súborov bolo zistené, že USB zariadenie neobsahovalo žiadny súbor **autorun.inf** ani iné automaticky vykonávané komponenty.

Antivírusový softvér ESET Endpoint Security neidentifikoval prítomnosť známeho škodlivého softvéru alebo rizikových súborov na zariadení.

Neexistujú žiadne technické dôkazy, ktoré by potvrdzovali prítomnosť malvéru na USB zariadení. Hypotéza 4 je vyvrátená.

Overovanie Hypotézy 5: Únik bol súčasťou cieleného útoku - Vyvrátená

Mohlo ísť o koordinovaný útok s cieľom získať špecifické informácie pre konkurenciu.

- **Metóda overenia:** Analýza vzorcov útokov, konzultácia s bezpečnostnými expertmi

Analýza:

Použité nástroje:

- **Wireshark:** kontrola sieťových spojov
- **DNS query analyzátor:** podozrivé dotazy
- **Sysmon:** pokusy o sieťový exfil

Zistenia:

- Žiadna komunikácia mimo lokálnej siete
- Vylúčené C2 spojenia
- Všetky aktivity prebehli **manuálne v lokálnom prostredí**

Cieľom tohto kroku bolo overiť, či operačný systém evidoval prichádzajúce alebo odchádzajúce spojenia, najmä DNS dotazy (port 53), ktoré by mohli indikovať komunikáciu s externými servermi – potenciálne spojenia typu C2 (Command and Control).

```
PS C:\WINDOWS\system32> Get-Content "C:\Windows\System32\LogFiles\Firewall\pfirewall.log" | Select-String "53"  
Get-Content : Cannot find path 'C:\Windows\System32\LogFiles\Firewall\pfirewall.log' because it does not exist.
```

Záznamový súbor pre Windows Firewall neexistuje, čo znamená, že logovanie sieťových udalostí (vrátane DNS dotazov) nebolo na systéme aktivované. Nie je teda možné späťne analyzovať, či z tohto počítača smerovala podozrivá sieťová aktivita mimo organizácie.

Chain of custody USB

Číslo:	1	Typ súboru:	.mem	Obnovený súbor:	Nie	Veľkosť:	4 194 304 KB
Popis prípadu:		Zachytenie obsahu operačnej pamäte podozrivého zariadenia na účely digitálnej forenzej analýzy v prípade úniku citlivých firemných údajov prostredníctvom USB zariadenia.					
Názov súboru:		RAM_DUMP_12032025.mem					
Miesto získania digitálnej stopy:		Forenzná pracovná stanica firmy XYZ – laboratórium, miestnosť 2.10					
Poznámky:		Obraz bol vytvorený v izolovanom offline prostredí. Použitá USB verzia nástroja s jednorazovým spustením					
Časové pečiatky							
Access:	12.03.2025 10:21	Modify:	12.03.2025 10:22	Change:	12.03.2025 10:23		
Digitálna odtlačok (heš)	MD5	bf7e29cdb087f2d58f7f3e7ef1f52f11					
	SHA1	49c8db207d6d49c8a50488e8f8e6a65b235c71dc					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
12.03.2025 10:21		Spustenie snímania operačnej pamäte					
12.03.2025 10:22		Dokončenie vytvárania bitovej kópie RAM					
12.03.2025 10:23		Overenie hashov, bezpečné odpojenie USB					
12.03.2025 10:25		Prenos súboru na izolovanú forenznú pracovnú stanicu					
12.03.2025 10:30		Vytvorenie záložnej kópie na externý HDD (BK2)					

Chain of Custody PC

Číslo:	2	Typ súboru:	.E01	Obnovený súbor:	Ni e	Veľkosť:	1TB
Popis prípadu:		Získanie bitovej kópie PC zariadenia, ktoré bolo použité pri exfiltrácii citlivých firemných dát v rámci incidentu spoločnosti XYZ.					
Názov súboru:		Firemný PC					

Miesto získania digitálnej stopy:		Forenzná pracovná stanica firmy XYZ – laboratórium, miestnosť 2.10			
Poznámky:		Zariadenie bolo zaistené fyzicky			
Časové pečiatky					
Access:	12.03.2025 11:08	Modify:	12.03.2025 11:09	Change:	12.03.2025 11:10
Digitálna odtlačok (heš)	MD5	d7cb1d1658a991583707466ee7bf7887			
	SHA1	e216f7f5237b794a7807322a29863f73ca93529f			
Časová pečiatka		Akcia vykonaná s digitálnou stopou			
12.03.2025 11:21		Akvizícia sa začala			
12.03.2025 11:25		Akvizícia ukončená			

Záver:

Digitálna forenzná analýza jednoznačne preukázala, že k úniku citlivých firemných údajov v spoločnosti XYZ došlo zámerným konaním interného zamestnanca. Kombináciou technických dôkazov – ako sú systémové logy, metadáta dokumentov, obsah RAM pamäte, hash odtlačky, výsledky z USB analýz – a fyzických dôkazov – vrátane kamerových záznamov a RFID logov – bola hypotéza o úmyselnej exfiltrácii dát potvrdená.

Vyšetrovanie poukázalo aj na závažné nedostatky v oblasti bezpečnostných opatrení. Absencia politiky obmedzujúcej používanie USB zariadení, chýbajúci DLP softvér, nedostatočný monitoring a školenia zamestnancov predstavujú významné riziko pre firemnú informačnú bezpečnosť.

Na základe získaných zistení odporúčame implementovať prísnejšiu bezpečnostnú politiku, pravidelne vzdelávať zamestnancov v oblasti ochrany dát a zaviesť technické riešenia na monitoring a prevenciu exfiltrácie citlivých údajov.

Prípadové štúdie:

1. Ochrana hostiteľov pred škodlivými USB perifériami

Štúdia o útok založených na USB.

<https://arxiv.org/pdf/2409.12850>

2. Injekčné útoky mimo cesty na USB komunikáciu

Štúdia o tom ako niekto môže odpočúvať USB komunikáciu.

<https://arxiv.org/pdf/2211.01109>

Odborné články:

1. "Duck Hunt: Memory Forensics of USB Attack Platforms" – Táto štúdia sa zaoberá analýzou forenzných artefaktov v pamäti generovaných USB útokmi a poskytuje cenné poznatky pre identifikáciu škodlivých USB zariadení.

2. "Detecting Data Theft Using Stochastic Forensics" – Tento príspevok predstavuje metódy na detekciu krádeže dát prostredníctvom analýzy prístupových vzorcov k súborom, čo je relevantné pre identifikáciu neoprávneného kopírovania údajov.