

Forenzná analýza USB zariadenia v prípade manipulácie kamerového systému

[Prezentacia](#)

Prípád (opis prípadu a motivácia):

Autor: Martin Dobiaš

Táto práca sa zameriava na forenznú analýzu USB zariadenia. Na základe incidentu, ku ktorému došlo v serverovni spoločnosti X, sa začalo digitálne forenzné vyšetrovanie. V nočných hodinách bol zaznamenaný výpadok kamerového systému, pričom po jeho obnovení bolo zistené, že chýbajú videozáznamy v časovom intervale medzi 02:15 až 03:00. Tento výpadok vyvolal podozrenie z možného úmyselného zásahu do záznamov. Počas následnej kontroly IT oddelenie objavilo v serverovni USB zariadenie, ku ktorému sa žiaden zamestnanec nehlásil. Zariadenie bolo nájdené na podlahe miestnosti. Jeho prítomnosť nevedel nikto zo zamestnancov vysvetliť, a nevykazovalo žiadnu bežnú administrátorskú činnosť. Následná analýza NVR logov potvrdila, že v čase incidentu bolo toto zariadenie aktívne a zo súborov boli spustené podozrivé SQL príkazy. Cieľom vyšetrovania je zistiť, či USB zohralo úlohu pri neoprávnenej manipulácii s kamerovým systémom, a identifikovať možné stopy vedúce k páchateľovi. Zmena alebo vymazanie video dôkazov môže znemožniť vyšetrovanie incidentov a skryť stopy páchateľov. Jednou z možných metód takéhoto útoku je použitie USB zariadenia na spustenie škodlivého skriptu alebo manuálnu úpravu záznamov. USB zariadenie predstavuje potenciálne médium na spustenie škodlivého skriptu, ktorý mohol spôsobiť vymazanie, úpravu alebo presmerovanie video dôkazov. V prípade, že bol takýto skript na zariadení uložený, ide o priame ohrozenie bezpečnosti a integrity interných systémov spoločnosti.

Ciele digitálnej forenznej analýzy

1. Identifikovať, či USB zariadenie obsahuje dôkazy o manipulácii s kamerovým systémom.
2. Preskúmať súbory a metadáta na USB a zistiť, či obsahujú škodlivý kód alebo podozrivé logy.
3. Zrekonštruovať udalosti vedúce k vymazaniu záznamov a určiť spôsob ich odstránenia.

4. Identifikovať možného páchatel'a na základe zachytených digitálnych stôp.
5. Poskytnúť dôkazy pre právne kroky alebo interné bezpečnostné opatrenia.

Použitý dataset sú reálne dáta pozostávajúce z 2006 súborov, obrázky, textové súbory a Python script, ktoré boli nájdené na USB + výpis logov z NVR. Postup vyšetovania postupoval podľa schémy Arnes2017.

Identifikácia (5WH):

Identifikácia je prvotnou fázou digitálnej forenznej analýzy (vyšetrovania), v rámci ktorej boli Kiplingovou metódou zadané ciele vyšetrovania (**5WH**):

Who? (Kto?)

- Cieľom tejto časti je identifikovať osoby, ktorá spáchala trestný skutok X a taktiež sa dopustila pozmenenia kamerového záznamu (+ zabudla v serverovni USB). Neznámy útočník, ktorý mohol mať priamy alebo vzdialený prístup k NVR systému.

What? (Čo?)

- Hlavným predmetom vyšetrovania je hľadanie osoby, ktorá vymazala alebo inak pozmenila dôležitý kamerový záznam a taktiež zabudla USB zariadenie v serverovni po výpadku kamerového systému.

When? (Kedy?)

- Incident sa odohral v nočných hodinách podľa logov keď došlo k výpadku a strate kamerových záznamov, vymazal sa záznam medzi 02:15 a 03:00. USB bolo objavené počas neskoršej analýzy priestorov.

Where? (Kde?)

- V serverovni spoločnosti X, kde sa nachádzali NVR kamerový systém a neznáme USB zariadenie. Tento priestor je zvyčajne prístupný len oprávneným osobám ktorých osobné PC sú tiež predmetom vyšetrovania.

Why? (Prečo?)

- Cieľom útoku mohlo byť odstránenie dôkazov, získanie citlivých informácií, exfiltrácia videozáznamov alebo skrytie inej neoprávnenej aktivity. Útočník mohol manipulovať so systémom, aby zakryl svoju identitu a činnosť.

How? (Ako?)

- Útočník mohol použiť USB na vykonanie škodlivých skriptov, manipuláciu databáz, vymazanie logov alebo exfiltráciu dát. Alternatívne mohol mať vzdialený prístup k NVR systému, pričom USB mohlo byť len náhodne objavené v serverovni, čo je predmetom riešenia.

V rámci fázy identifikácie boli vytvorené prvotné **hypotézy** o tom, čo sa mohlo stať:

1. **Hypotéza :** Útočník použil USB zariadenie na exfiltráciu dát z NVR systému. Útočník mal prístup k USB zariadeniu a použil ho na kopírovanie alebo exportovanie citlivých kamerových záznamov z NVR systému. Po exportovaní záznamov, mohol útočník tieto dáta použiť na rôzne nelegálne účely (napr. predat' konkurencii).
2. **Hypotéza :** Útočník sa pokúsil zahľadiť stopy vymazaním prístupových logov. Útočník vedel, že záznamy o prístupoch a aktivitách na NVR systéme sú ukladané v logoch a pokúsil sa ich vymazať. Tento krok bol zamýšľaný ako pokrytie stôp a zabránil sledovaniu jeho aktivít. Následne sa pokúsil manipulovať s kamerovými záznamami tak, aby nebolo možné zistiť, čo sa naozaj stalo.
3. **Hypotéza :** Útočník vykonal fyzický prístup k zariadeniu s cieľom zmeniť / vymazať záznamy na NVR. Útočník mal fyzický prístup k NVR a mohol doň fyzicky pripojiť USB, aby manipuloval so záznamami. Tento prístup mohol zahŕňať vymazanie starších záznamov, kopírovanie alebo upravovanie údajov priamo na serveri, čo malo za následok stratu určitých videí alebo dôkazov.
4. **Hypotéza :** Útočník nevyužil USB zariadenie na exfiltráciu dát (USB tam niekto zabudol dávnejšie), ale záznamy boli vymazané z NVR systému bez prítomnosti externého média. Útočník mohol získať prístup k NVR systému na diaľku, prostredníctvom zraniteľnosti v sieti, bez nutnosti použitia USB zariadenia. Existuje aj možnosť, že dáta boli vymazané z NVR cez pripojenie v lokálnej sieti alebo vzdialené pripojenie, a USB zariadenie bolo iba použité na zálohovanie alebo manipuláciu s inými dátami, ale nie na exfiltráciu. – **Táto hypotéza sa nepotvrdila**



Zaist'ovanie a zber

Digitálny forenzný tím po identifikácii potenciálneho miesta činu – Serverovne firmy X, objavili zariadenia NVR, ktoré bolo síce zapnuté ale všetky potrebné údaje a logy ukladá NVR aj po odpojení napájania. Digitálny forenzný tím rozhodol pre vypnutie NVR a zaistenie metódou tzv. post mortem. Zariadenie bolo odpojené od napájania, označené a bezpečne prepravené do vyhradených priestorov firmy Y za účelom detailnej digitálnej forenznej analýzy.

Pri predbežnej vizuálnej kontrole priestorov forenzný analytik dostal od zamestnancov firmy X USB, ktoré bolo nájdené na podlahe serverovne. Vzhľadom na podozrenie, že mohlo dôjsť k manipulácii s videozáznamami prostredníctvom tohto USB (napr. spustením škodlivého skriptu alebo vymazaním záznamov), USB zariadenie bolo prioritne zaistené a prevezené do priestorov firmy Y, kde bolo následne pripojené k foreznému pracovisku s použitím writeblockeru, aby sa zabránilo akémukoľvek zápisu na médium. Forenzný analytik následne pomocou nástrojov ako FTK Imager a Autopsy vytvoril dve bitové kópie USB zariadenia a vygeneroval digitálny otláčok (hash) pre zabezpečenie integrity dát.

Forenzný tím taktiež zaistil osobné počítače zamestnancov, ktorí boli za zozname pracovníkov s priamym prístupom do serverovne, z dôvodu preverenia či súbory na USB boli nahraté z ich počítača, prípadne ak išla vzdialená komunikácia na NVR, či bola z ich PC.

Zariadenia prítomné na mieste incidentu:

Na mieste, kde došlo k manipulácii kamerového systému, sa nachádzali nasledovné digitálne zariadenia + dve zariadenia osôb ktoré mali oprávnený prístup do tejto miestnosti.

1. NVR kamerového systému – uchováva záznamy z bezpečnostných kamier a spravuje prístup k nim. V tomto zariadení sa nachádza disk – HDD.
2. USB zariadenie (neidentifikované) – nájdené v serverovni, pravdepodobne použité pri útoku.
3. PC správcu siete a PC vedúceho pracovníka IT – len títo dvaja zamestnanci mali do serverovne oprávnený prístup, ak sa niekto dostal do serverovne oni o tom musia vedieť – serverovňa je zamknutá na čítačku otláčkov (RAM).

Prítomnosť neznámeho USB zariadenia naznačuje možnosť priamej manipulácie s kamerovým serverom. Preto je kľúčové analyzovať jeho obsah a určiť, či obsahuje digitálne dôkazy o útoku.

Údaje o zaistenom USB:

- **Model:** Kingston DataTraveler 2.0 USB Device
- **Sériové číslo:** CB806800040A
- **Typ rozhrania:** USB 2.0
- **Odnímateľné médium:** Áno
- **Veľkosť dátového zdroja:** 14 766 MB
- **Celkový počet sektorov:** 30 240 768
- **Súborový systém:** FAT32
- **Názov zväzku:** boot
- **Rýchlosť čítania/zápisu:** ~100 MB/s (čítanie), ~10 MB/s (zápis)



Obraz pamäte nájdeného USB

Created By AccessData® FTK® Imager 4.7.1.2

Case Information:

Acquired using: ADI4.7.1.2

Case Number: 01

Evidence Number: 001

Unique description: Kingstone

Examiner: Autor

Notes: 32GB moj prípad

Information for C:\Users\student\Downloads\ram-capturer\RamCapturer\x64\usb-key-kingstone-externe:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 1 882

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 30 240 768

[Physical Drive Information]

Drive Model: Kingston DataTraveler 2.0 USB Device

Drive Serial Number: CB806800040A

Drive Interface Type: USB

Removable drive: True

Source data size: 14766 MB

Sector count: 30240768

[Computed Hashes]

MD5 checksum: 2074394f08ade3501392f4b9ea8bb873

SHA1 checksum: 562d0bec89e45576592a77c3b92ac2fad3121335

Image Information:

Acquisition started: Sat Mar 28 10:24:54 2025

Acquisition finished: Sat Mar 28 10:34:57 2025

Segment list:

C:\Users\student\Downloads\ram-capturer\RamCapturer\x64\usb-key-kingstone-externe.001

Image Verification Results:

Verification started: Sat Mar 22 10:34:57 2025

Verification finished: Sat Mar 22 10:35:29 2025

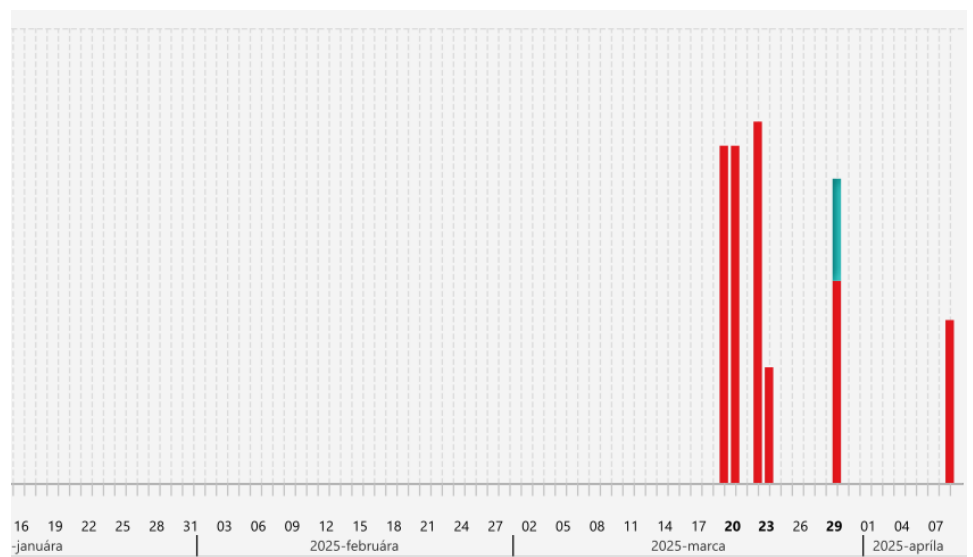
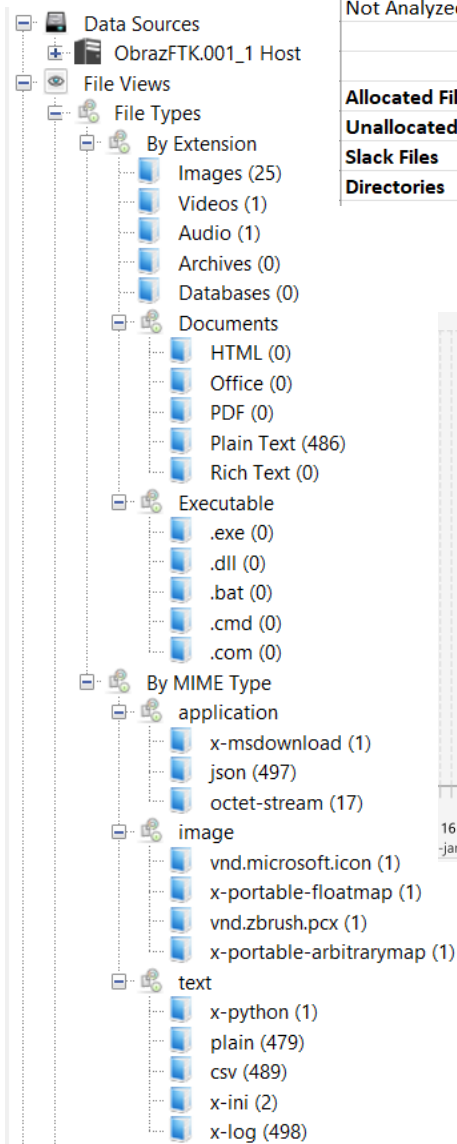
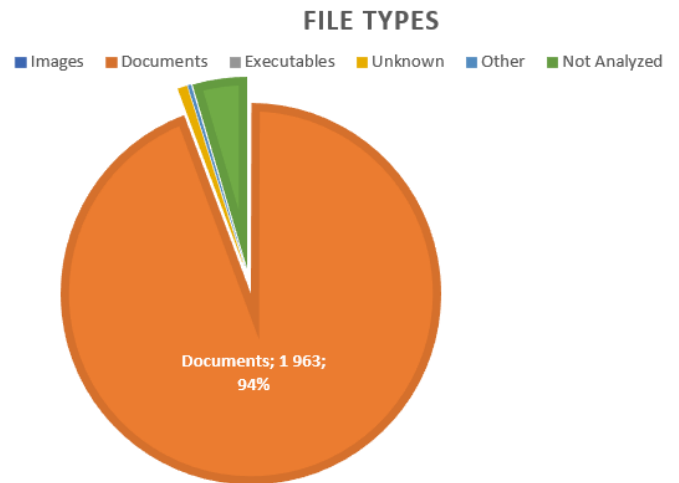
MD5 checksum: 2074394f08ade3501392f4b9ea8bb873 : verified

SHA1 checksum: 562d0bec89e45576592a77c3b92ac2fad3121335 : verified

Vyt'ažovanie

Vyššie uvedenú kópiu obnovených súborov analytik FF použil ako vstup pre program Autopsy 4.21.0, pomocou ktorého zistil nasledujúce informácie:

Usage	
OS	
Size	15,48 GB
File Types	Count
Images	1
Documents	1 963
Executables	1
Unknown	17
Other	6
Not Analyzed	95
Allocated Files	2 059
Unallocated Files	24
Slack Files	13
Directories	35



Analýza

Chain of custody

Číslo:	01	Typ súboru:	.py	Obnovený súbor:	nie	Veľkosť:	1kB
Popis prípadu:		Forenzná analýza USB zariadenia v prípade manipulácie kamerového systému					
Názov súboru:		backup_script.py					
Miesto získania digitálnej stopy:		USB zariadenie					
Poznámky:		USB nájdené na podlahe serverovne, nikto sa k USB nehlásil					
Časové pečiatky							
Access:	[2025-03-25 1:03:58]	Modify:	[2025-03-25 1:58:00]			Change:	
Digitálny odtlačok (heš)	MD5	2074394f08ade3501392f4b9ea8bb873					
	SHA1	562d0bec89e45576592a77c3b92ac2fad3121335					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
28.03.2025 10:24		Kontrola zhody digitálneho odtlačku					
28.03.2025 10:36		Skúmanie obsahu pomocou digitálneho nástroja AutoPsy					

Chain of Custody pre USB

Číslo:	02	Typ súboru:	.txt	Obnovený súbor:	nie	Veľkosť:	9kB
Popis prípadu:		Forenzná analýza USB zariadenia v prípade manipulácie kamerového systému					
Názov súboru:		20250410140051logBack.txt					
Miesto získania digitálnej stopy:		NVR Hikvision					
Poznámky:		NVR značky Hikvision, nájdené v serverovni z ktorého bol pravdepodobne vymazaný record					
Časové pečiatky							
Access:	[2025-04-10 9:00:00]	Modify:	[2025-04-10 9:00:00]			Change:	
Digitálny	MD5	2074394f08ade3512592f4b9eb8ab122					
	SHA1	2074394f08ade3512592f4b9eb8abd3121335					

odtlačok (heš)		
Časová pečiatka	Akcia vykonaná s digitálnou stopou	
28.03.2025 11:24	Export logov z NVR	

Chain of Custody pre NVR

Číslo:	03	Typ súboru:		Obnovený súbor:	nie	Veľkosť:	8GB
Popis prípadu:		Forenzná analýza USB zariadenia v prípade manipulácie kamerového systému					
Názov súboru:		sys					
Miesto získania digitálnej stopy:		PC v kancelárii X					
Poznámky:		PC podozrivého zamestnanca firmy , PC zapnutý – urobený image RAM					
Časové pečiatky							
Access:			Modify:			Change:	
Digitálny odtlačok (heš)	MD5	f5d2b3a0ac467f7fa1ff3b428d8d7f4b					
	SHA1	ce2e4d97fd76efed6fcb8275e8f8f24f3c9f7c9a					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
26.03.2025 8:24		Vytvorenie image pamäte RAM z PC					
28.03.2025 15:36		Analýza image v AutoPsy					

Chain of Custody pre PC

Nájdený PC bol:

AMD Ryzen 5 2500U, 14" TN antireflexný 1920 × 1080, RAM 8 GB DDR4, AMD Radeon Graphics, SSD 500 GB, webkamera, USB 3.2 Gen 1, USB-C, WiFi 5, Bluetooth, hmotnosť 1,41 kg, Windows 10 Home.

USB – je analyzovaný vyššie

NVR – Značka Hikvision DS-7104HQHI-K1(S)

Zaujímavé dáta nájdené v obraze nájdeného USB:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
commands_backup.txt			0	2025-03-22 08:26:42 SEČ	2025-03-22 08:26:42 SEČ	2025-03-22 08:26:42 SEČ	2025-03-22 06:09:05 SEČ	227	Allocated	Allocated	unknown
file_1015.txt			0	2025-03-19 20:38:46 SEČ	2025-03-20 20:56:56 SEČ	2025-03-22 06:09:06 SEČ	2025-03-22 06:09:06 SEČ	405	Allocated	Allocated	unknown
file_1018.txt			0	2025-03-19 20:38:46 SEČ	2025-03-20 20:57:00 SEČ	2025-03-22 06:09:06 SEČ	2025-03-22 06:09:06 SEČ	410	Allocated	Allocated	unknown
file_102.txt			0	2025-03-19 20:38:46 SEČ	2025-03-20 20:57:19 SEČ	2025-03-22 06:09:06 SEČ	2025-03-22 06:09:06 SEČ	176	Allocated	Allocated	unknown
file_1026.txt			0	2025-03-19 20:38:46 SEČ	2025-03-20 20:56:42 SEČ	2025-03-22 06:09:06 SEČ	2025-03-22 06:09:06 SEČ	410	Allocated	Allocated	unknown

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 1 of 1 Page

Matches on page: - of - Match

100%

Reset

Text Source: File Text

-- Export všetkých záznamov pred vymazaním
SELECT * FROM recordings INTO OUTFILE '/tmp/extracted_data.csv';

-- Vymazanie logov o prístupe
DELETE FROM access_logs WHERE user='unknown' AND timestamp > '2025-03-18 02:00:00';

-----METADATA-----

V USB súboroch sme našli súbor s príponou txt v ktorom boli uložené SQL príkazy na stiahnutie všetkých „zvolených„ záznamov na USB

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
backup_script.py			0	2025-03-19 20:38:46 SEČ	2025-03-22 08:37:49 SEČ	2025-03-22 08:37:51 SEČ	2025-03-22 06:09:05 SEČ	229	Allocated	Allocated	unknown

Hex

Text

Application

File Metadata

OS Account

Data Artifacts

Analysis Results

Context

Annotations

Other Occurrences

Strings

Extracted Text

Translation

Page: 1 of 1 Page

Matches on page: - of - Match

100%

Reset

Text Source: File Text

import sqlite3
conn = sqlite3.connect('/var/security/camera.db')
cursor = conn.cursor()
cursor.execute("DELETE FROM recordings WHERE timestamp BETWEEN '2025-03-18 02:15:00' AND '2025-03-18 03:00:00';")
conn.commit()
conn.close()

Taktiež sa našiel súbor s príponou .py – takže ide o spustiteľný súbor napísaný v pythone a podľa bližšej analýzy kódu, súbor slúžil na vymazanie záznamu v danom čase kedy chýba video záznam, ktorý mal slúžiť na dokázanie trestnej činnosti

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known
camera_video_1.mp4				2025-03-19 20:48:46 SEČ	2025-03-20 20:56:30 SEČ	2025-03-22 06:10:12 SEČ	2025-03-22 06:10:12 SEČ	54	Allocated	Allocated	unknown

Vyššie vidíme taktiež, že sa na USB nachádza export z kamery, ktorý bol vykonaný pomocou príkazov vyššie (v .txt súbore) a následne vymazaný spustiteľným súborom .py. Ďalšou analýzou daného USB sa objavili aj nahrávky stiahnuté z NVR pred ich vymazaním, kde je zamestnanec vidieť.

Zhoda nájdená v obraze RAM (PC zamestnanca ktorý mal prístup do serverovne)

```
249E59000 01 00 00 00 F8 03 00 00 68 74 74 70 73 3A 2F 2F ...Ĥ...https://
249E59010 77 77 77 2E 67 6F 6F 67 6C 65 2E 63 6F 6D 2F 73 www.google.com/s
249E59020 65 61 72 63 68 3F 71 3D 75 73 62 2B 73 63 72 69 earch?q=usb+scri
249E59030 70 74 2B 74 6F 2B 64 65 6C 65 74 65 2B 72 65 63 pt+to+delete+rec
249E59040 6F 72 64 2B 66 72 6F 6D 2B 68 69 6B 76 69 73 65 ord+from+hikvisi
249E59050 6F 6E 2B 6E 76 72 26 63 6C 69 65 6E 74 3D 66 69 on+nvr&client=fi
249E59060 72 65 66 6F 78 2D 62 2D 64 26 73 63 61 5F 65 73 refox-b+disca_es
249E59070 76 3D 36 33 66 34 30 31 61 36 65 62 34 35 62 38 v=63f401a6eb45b8
249E59080 32 31 26 65 69 3D 4F 33 58 65 5A 5F 57 61 4E 37 21&ei=03XeZ_WaN7
249E59090 4B 72 39 75 38 50 38 49 4F 69 6B 41 67 26 76 65 Kr9u8P8IOiKAg&ve
249E590A0 64 3D 30 61 68 55 4B 45 77 69 31 70 4F 57 43 6F d=0ahUKEwilpOWCo
249E590B0 35 32 4D 41 78 57 79 6C 66 30 48 48 66 43 42 43 52MaxWylf0HHfCBC
249E590C0 49 49 51 34 64 55 44 43 42 41 26 75 61 63 74 3D IIQ4dUDCBA&uact=
249E590D0 35 26 6F 71 3D 75 73 62 2B 73 63 72 69 70 74 2B 5&oq=usb+script+
249E590E0 74 6F 2B 64 65 6C 65 74 65 2B 72 65 63 6F 72 64 to+delete+record
249E590F0 2B 66 72 6F 6D 2B 68 69 6B 76 69 73 69 6F 6E 2B +from+hikvision+
249E59100 6E 76 72 26 67 73 5F 6C 70 3D 45 67 78 6E 64 33 nvr&gs_lp=Egxnnd3
249E59110 4D 74 64 32 6C 36 4C 58 4E 6C 63 6E 41 69 4C 6E Mtd216LXN1cnAiLn
```

Obráz RAM pamäte administrátorského PC potvrdil vyhľadanie webov: „usb script to delete record from hikvision nvr“, vďaka tomuto môžeme predpokladať, že majiteľ tohto PC využil nájdené USB na vymazanie záznamu

Properties		X	
Device Name:	DataTraveler 2.0	Description:	Kingston DataTraveler 2.0 USB Device
Device Type:	Mass Storage	Connected:	Yes
Safe To Unplug:	Yes	Disabled:	No
USB Hub:	No	Drive Letter:	M:
Serial Number:	C860008863CFB0804A16A977	Registry Time 1:	12. 4. 2025 15:59:16
Registry Time 2:	12. 2. 2025 16:59:36	VendorID:	0930
ProductID:	6545	Firmware Revision:	1.10
WCID:		USB Class:	08
USB Sub-Class:	06	USB Protocol:	50
Hub / Port:		Computer Name:	LAPTOP-HJL3NFSO
Vendor Name:		Product Name:	
ParentID Prefix:		Service Name:	USBSTOR
Service Description:	@usbstor.inf;%USBSTOR.SvcDesc%;USB Mass	Driver Filename:	USBSTOR.SYS
Device Class:		Device Mfg:	Compatible USB storage device
Friendly Name:		Power:	300 mA
USB Version:	2.00	Driver Description:	USB Mass Storage Device
Driver Version:	10.0.19041.4355	Driver InfSection:	USBSTOR_BULK.NT
Driver InfPath:	usbstor.inf	Instance ID:	USBVID_0930&PID_6545\C860008863CFB0804A
Capabilities:	Removable, UniqueID, SurpriseRemovalOK	Install Time:	
First Install Time:		Connect Time:	
Disconnect Time:			
OK			

Pripojenie USB k PC technikov DFA pre zistenie správneho formátu sériového čísla

Properties		X	
Device Name:	Port_#0002.Hub_#0002	Description:	Kingston DataTraveler 2.0 USB Device
Device Type:	Mass Storage	Connected:	No
Safe To Unplug:	Yes	Disabled:	No
USB Hub:	No	Drive Letter:	M:
Serial Number:	C860008863CFB0804A16A977	Registry Time 1:	25. 3. 2025 1:58:00
Registry Time 2:	12. 2. 2025 16:59:36	VendorID:	0930
ProductID:	6545	Firmware Revision:	1.10
WCID:		USB Class:	08
USB Sub-Class:	06	USB Protocol:	50
Hub / Port:		Computer Name:	LAPTOP-16A977
Vendor Name:		Product Name:	
ParentID Prefix:		Service Name:	USBSTOR
Service Description:	@usbstor.inf;%USBSTOR.SvcDesc%;USB Mass	Driver Filename:	USBSTOR.SYS
Device Class:		Device Mfg:	Compatible USB storage device
Friendly Name:		Power:	
USB Version:	2.00	Driver Description:	USB Mass Storage Device
Driver Version:	10.0.19041.4355	Driver InfSection:	USBSTOR_BULK.NT
Driver InfPath:	usbstor.inf	Instance ID:	USBVID_0930&PID_6545\C860008863CFB0804A
Capabilities:	Removable, UniqueID, SurpriseRemovalOK	Install Time:	
First Install Time:		Connect Time:	
Disconnect Time:			
OK			

Po spustení softvéru na PC podozrivého zamestnanca sme našli údaj o zapojení nájdeného USB na jeho PC – momentálne nie je pripojený k nemu, sériové číslo sa zhoduje so sériovým číslom nájdeného USB a posledné pripojenie k tomuto PC bolo 25.3.2025 o 1:58 – cca 20 minút pred vymazaním kamerového záznamu (dokaz o tom že USB kľúč patrí danému technikovi).

Vyššie je nájdená zhoda o zapojení nájdeného USB do PC pracovníka podozrivého z trestnej činnosti, pomocou softvéru USBDeview (od NirSoft), sériové číslo USB sa zhoduje s tým nájdeným (prehľadnejšia alternatíva k systémovým logom).

NVR Logy

```
-----  
1          2025-3-25 2:15:00  
-----  
Hlavný typ: Informácie  
Vedľajší typ: USB zariadenie pripojené  
Lokálne prihlásenie užívateľa: admin  
IP adresa hosta: N/A  
Parameter: USB_DISK_1  
Port: USB-Front  
  
-----  
2          2025-3-25 2:15:35  
-----  
Hlavný typ: Operácia  
Vedľajší typ: Export záznamu  
Lokálne prihlásenie užívateľa: admin  
IP adresa hosta: N/A  
Parameter: 2025-03-25 02:15:00 - 2025-03-25 03:00:00  
Kanál č.: A1  
  
-----  
3          2025-3-25 2:16:00  
-----  
Hlavný typ: Informácie  
Vedľajší typ: USB zariadenie odpojené  
Lokálne prihlásenie užívateľa: admin  
IP adresa hosta: N/A  
Parameter: USB_DISK_1  
Port: USB-Front
```

Vyššie vidíme výpis logov z NVR ktoré taktiež dokazujú manipuláciu s kamerovým záznamom na danej kamere a taktiež vidíme že bolo zapojené USB, export záznamu a následné vymazanie záznamu + odpojenie

Záver

Na základe výpisu z NVR vieme dokázať, že naozaj bola manipulácia zo záznamom a taktiež že nájdené USB bolo naozaj pripojené a využité na tento útok. Na PC ktorého RAM pamäť prešla analýzou sa taktiež vyhl'adával podozrivý obsah (po otvorení webovej adresy sme našli použité príkazy, ktoré sa zhodovali s tými na USB). Taktiež po analýze PC dvoch zamestnancov firmy sa potvrdilo že v jednom z ich PC bolo dané USB zapojené cca 15 minút pred incidentom. Po pokročilom preskúmaní sa na USB objavili aj stiahnuté záznamy na ktorých sa majiteľ PC taktiež nachádza. Potvrdili sa hypotézy 1-3, 4 hypotéza že išlo o sieťový útok sa vyvrátila.

Prezentácia

Odborné články

Miesto činu 2019

Odkaz: <https://www.mosr.sk/45257-sk/miesto-cinu-2019/>

Čítanie logov v NVR zariadení značky Hikvision

Odkaz: https://enpinfo.hikvision.com/unzip/20200731103027_05278_doc/GUID-F3D0A4E1-0ED0-4BA9-A4EF-7809F512C995.html