

Návrat strateného USB kľúča

<https://bcstudent.fpvucm.sk/~rezbarikmiroslav/dfa/prezentacia.pdf>

Vyšetrovateľ: Miroslav Rezbárik

Opis prípadu:

Daný prípad sa zaoberá USB kľúčom, ktorý bol zamestnancovi údajne odcudzený zo stola počas jeho obednej prestávky (3. máj 2025, 12:00-13:00). Tento USB kľúč bol chránený PIN kódom, ktorý mal zamestnanec zapísaný na papieriku pripevnenom na nástenke. Po návrate z obeda zistil jeho stratu a nahlásil incident. Ďalej zamestnanec tvrdí, že daný USB kľúč v ten deň nepoužil. Na druhý deň ráno (4. mája 2025 8:00), keď prišiel do práce, USB kľúč sa opäť objavil na jeho stole.

Predmet vyšetrovania:

- Zisťovanie, aké súbory boli uložené alebo odstránené z USB kľúča.
- Overenie, či došlo k neoprávnenému kopírovaniu firemných dokumentov.
- Analýza možnej prítomnosti škodlivého softvéru.

Očakávaný výsledok:

Cieľom tohto vyšetrovania je určiť čo sa dialo s USB kľúčom od času zmiznutia po čas nálezu. To znamená zistiť:

- či sa z neho kopírovali alebo inak manipulovali údaje (analýza metadát)
- či daný USB kľúč nebol infikovaný malwarom (napr. program USBFix alebo nejaký antivírusový softvér napr. Malwarebytes)
- a ak to bude možné tak určiť kto je páchatelom

5WH analýza:

- **Kto?** Neznáma osoba, ktorá mohla počas neprítomnosti zamestnanca získať prístup k jeho USB kľúču. Môže ísť o kolegu alebo cudzieho človeka, ktorý sa infiltroval do firmy.
- **Kde?** Incident sa odohral v kancelárii zamestnanca, kde bol USB kľúč údajne odcudzený zo stola. Následné použitie USB kľúča mohlo prebehnúť na inom mieste v rámci firmy alebo mimo nej.
- **Kedy?** USB kľúč zmizol počas obednej prestávky zamestnanca a vrátil sa na jeho stôl nasledujúce ráno. Presný čas neoprávneného použitia je neznámy, preto je potrebné analyzovať časové pečiatky súborov a záznamy o pripojení. (3.3. 2025 13:00 – 4.3. 2025 8:00)
- **Čo?** USB kľúč obsahoval citlivé firemné dokumenty chránené PIN kódom. Je potrebné zistiť, či došlo k neoprávnenému prístupu k týmto súborom, ich kopírovaniu, úprave alebo vymazaniu.
- **Prečo?** Motivácia páchatel'a môže byť rôzna: získanie citlivých informácií pre osobný prospech, predaj konkurencii, snaha poškodiť firmu alebo jednoducho zvedavosť.
- **Ako?** Páchatel' mohol využiť dostupnosť PIN kódu na nástenke na odomknutie USB kľúča. Následne mohol kľúč pripojiť k inému zariadeniu, skopírovať alebo upraviť súbory, prípadne infikovať kľúč škodlivým softvérom.

Stanovenie hypotéz:

1. **Neoprávnené kopírovanie alebo pozmenenie firemných dokumentov:**
 - **Popis:** Páchatel' získal prístup k USB kľúču pomocou PIN kódu a skopíroval citlivé firemné dokumenty na iné médium alebo zariadenie.
 - **Dôsledky:** Únik citlivých informácií môže viesť k finančným stratám, poškodeniu reputácie firmy alebo strate konkurenčnej výhody.
2. **Infikovanie USB kľúča škodlivým softvérom:**
 - **Popis:** Páchatel' mohol na USB kľúč nainštalovať škodlivý softvér s cieľom infikovať firemnú sieť po jeho opätovnom pripojení.
 - **Dôsledky:** Infekcia môže viesť k narušeniu integrity dát, neoprávnenému prístupu k systémom alebo krádeži ďalších informácií.
3. **Neoprávnené použitie USB kľúča bez zlého úmyslu:**
 - **Popis:** Niektorí z kolegov si mohli USB kľúč požičať bez vedomia vlastníka, napríklad na prenos vlastných dát, a následne ho vrátil bez zlého úmyslu.

Cieľ vyšetrovania:

Cieľom vyšetrovania je určiť, či bol daný USB kľúč použitý neoprávnenou osobou/osobami a teda či obsah na ňom bol manipulovaný. Vyšetrovanie sa zameria na:

- **Kontrolu metadát súborov** – skontrolovanie časov poslednej úpravy, prístupové časy, či počas absencie bol daný USB kľúč používaný
- **Kontrola samotných dát** – kontrola, či boli dáta pridané, zmazané alebo inak upravené
- **Kontrola prítomnosti malwaru** – kontrola, či daný USB kľúč nebol infikovaný škodlivým softvérom

Informácie, ktoré hľadáme:

Dôkazy o možnom zásahu do súborov, ich úprave alebo odstránení. Preskúmame obsah dokumentov a multimediálnych súborov, ktoré môžu obsahovať dôverné alebo citlivé informácie. Zameriame sa aj na metadáta, ktoré môžu prezradiť históriu prístupu, zmien a zdieľania týchto súborov.

Typ analyzovanej digitálnej stopy:

Budeme sa zameriavať na vyhľadávanie informácií uložených na USB kľúči, konkrétne v súboroch formátov ako HTML, PDF, TXT, DOC, PPT, JPG, XLS a GIF. Skúmame históriu úprav, časové pečiatky a možné digitálne stopy, ktoré môžu naznačiť, kto používal USB a aké dáta boli upravované. Naším cieľom je zistiť, či došlo k neoprávnenej manipulácii alebo prenosu citlivých informácií.

4,457 files, 1.9GB of data (1.2GB compressed)

Zdroj: <http://roussev.net/t5/t5.html>

Nájdené na: <https://datasets.fbreitinger.de/datasets/>

Digitálne zariadenie súvisiace s prípadom:

Dané zariadenie mohlo byť použité na neoprávnený prístup k citlivým informáciám.



Značka VERBATIM

Model Keypad Secure USB Drive USB 3.2 Gen 1 - 32GB

Sériové číslo 49427

Kapacita 32 GB

Pripojenie USB 3.2 Gen 1 (USB 3.0)

Konektor USB-A

Rýchlosť čítania 160 MB/s

Rýchlosť zápisu 130 MB/s

Spracovanie a funkcie

Šifrovanie AES-256

Zabezpečenie Hardvérové šifrovanie, HW klávesnica

Funkcie Automatické zálohovanie, Ochrana proti útokom hrubou silou

Vyhotovenie Zamknuteľný

Výbava Krytka, LED signalizácia

Farba Čierna

Rozmery a hmotnosť

Šírka 28 mm

Výška 12 mm

Dĺžka 93,5 mm

Hmotnosť 30 g

Bezpečnostné opatrenia:

1. Fyzická ochrana

- Zariadenie bolo umiestnené do antistatického obalu a bezpečnostného puzdra. o Zabezpečené pred nepriaznivými vplyvmi, ako sú teplota, vlhkosť a magnetické polia.

2. Digitálna ochrana

- Aby sa zabránilo nežiadúcim zmenám dát, USB kľúč nebol pripojený k bežnému počítaču.
- Na zabránenie zápisu bol použitý write-blocker.
- Forenzný obraz bol čo najrýchlejšie ako sa dalo vytvorený pomocou FTK Imager.

3. Dokumentácia a skladovanie

- Boli zaznamenané informácie o dátume, čase, mieste nálezu a všetkých manipuláciách so zariadením.
- USB kľúč bol uložený do trezoru a analyzovaný v kontrolovanom, izolovanom prostredí.

Použité nástroje:

Exterro FTK imager – softvér na tvorbu obrazov zariadení

HxD – hexadecimálny editor umožňujúci analýzu binárnych súborov

Autopsy – softvér na analýzu obrazu zariadenia

MRCv120 (ram capturer)– softvér na extrakciu dát z operačnej pamäte

Malwarebytes – antivírusový softvér na kontrolu malvéru

Výstup z Exterro FTK Imager:

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 1

Evidence Number: 1

Unique description: Obraz USB kluca

Examiner: Miroslav Rezbárik

Notes: Obraz nájdeného USB kľúča

Information for C:\Users\Admin\Desktop\Nový priečinok (3)\obraz_usb:

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

[Physical Drive Information]

Drive Model: Kingston DataTraveler 3.0 USB Device

Drive Serial Number: 0E83670069E7

Drive Interface Type: USB

Removable drive: True

Source data size: 14784 MB

Sector count: 30277632

[Computed Hashes]

MD5 checksum: 148d81640e81764976f179c4d5b35445

SHA1 checksum: 522e553172c4ee372537ca832835b0c51504c356

Image Information:

Acquisition started: Mon Mar 10 15:38:52 2025

Acquisition finished: Mon Mar 10 15:45:17 2025

Segment list:

C:\Users\Admin\Desktop\Nový priečinok (3)\obraz_usb.001

COMPUTED HASH : 148d81640e81764976f179c4d5b35445

COMPUTED HASH : 522e553172c4ee372537ca832835b0c51504c356

Image Verification Results:

Verification started: Mon Mar 10 15:45:17 2025

Verification finished: Mon Mar 10 15:45:58 2025

MD5 checksum: 148d81640e81764976f179c4d5b35445 : verified

SHA1 checksum: 522e553172c4ee372537ca832835b0c51504c356 : verified

Výsledky overenia obrazu:

Drive/Image Verify Results

Name	obraz_usb.001
Sector count	30277632
MD5 Hash	
Computed hash	148d81640e81764976f179c4d5b35445
Report Hash	148d81640e81764976f179c4d5b35445
Verify result	Match
SHA1 Hash	
Computed hash	522e553172c4ee372537ca832835b0c51504c356
Report Hash	522e553172c4ee372537ca832835b0c51504c356
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Close

Zaujímavé dáta nájdené v obraze RAM:

```
3C3855750 69 74 00 00 56 79 6D 61 7A 61 74 20 6F 62 6A 65 it..Vymazať obje  
3C3855760 6B 74 79 20 70 6F 6D 6F 63 C3 AD 20 46 6F 74 6F kty pomocĎ. Foto
```

Získané z obrazu pamäte RAM pomocou ram capturer a zobrazené pomocou editora HxD, možný pokus vymazania dát (neskôr označené za nerelevantné k prípadu)

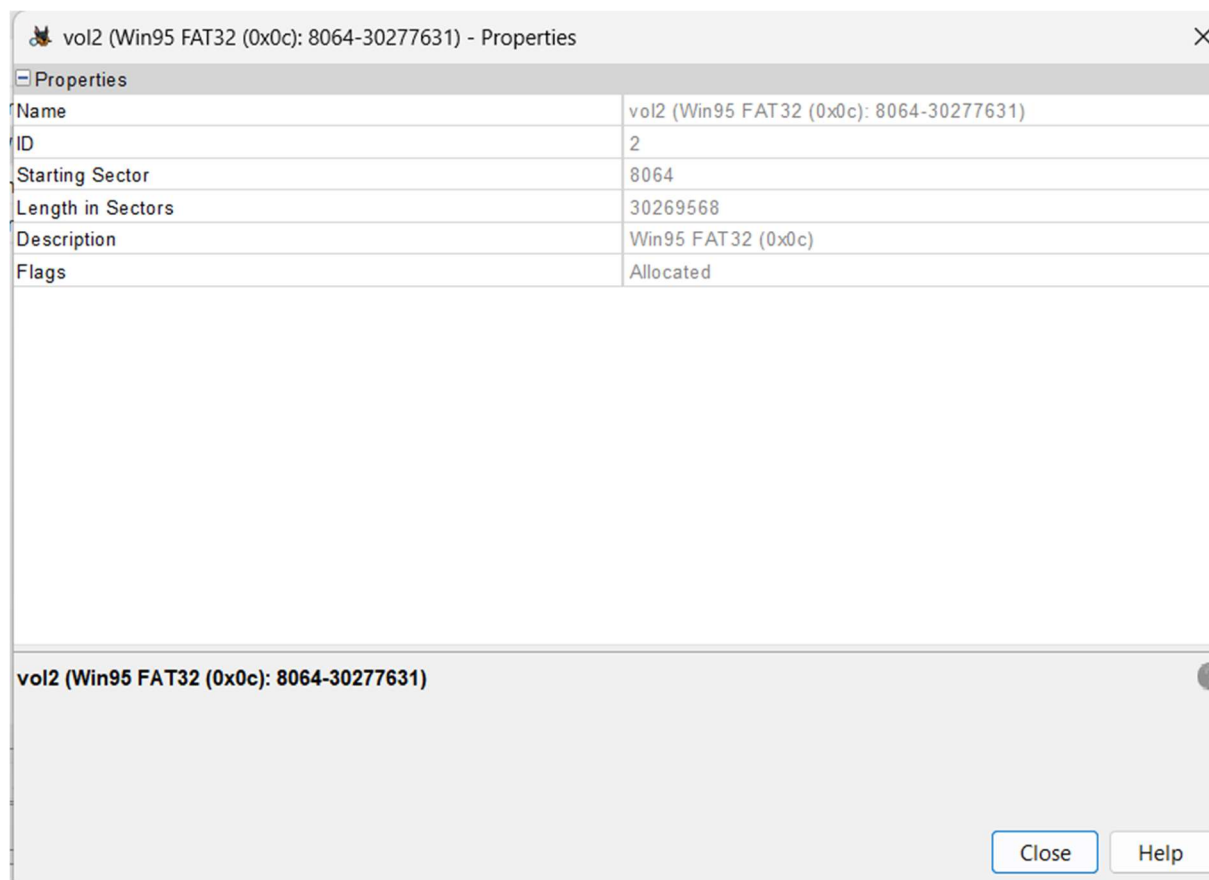
Bitové kópie:

1. **Bitová kópia** – uložená na pracovnom notebooku (OS Windows 10), ktorý slúži ako pracovná stanica
2. **Bitová kópia** – uložená na HDD, ktorý je zabezpečený a uzamknutý v špecializovanom laboratóriu

Chain of custody

Číslo:	1	Typ súboru:	raw	Obnovený súbor:	nie	Veľkosť:	14784 MB
Popis prípadu:		Návrat strateného USB kľúča					
Názov súboru:		obraz_usb.001					
Miesto získania digitálnej stopy:		USB kľúč zamestnanca					
Poznámky:		Vytvorenie obrazu USB kľúča					
Časové pečiatky							
Access:	ano		Modify:	nie		Change:	nie
Digitálny odtlačok (heš)	MD5	148d81640e81764976f179c4d5b35445					
	SHA1	522e553172c4ee372537ca832835b0c51504c356					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
Mon Mar 10 15:38:52 2025		Acquisition started					
Mon Mar 10 15:45:17 2025		Acquisition finished					
Mon Mar 10 15:45:17 2025		Verification started					
Mon Mar 10 15:45:58 2025		Verification finished					

Umiestnenie súborov v súborovom systéme a súborový systém



Zariadenie obsahuje partíciu vo formáte FAT32 (Win95 FAT32 LBA – 0x0c), ktorý umožňuje len obmedzené uchovávanie metadát.

Infikovanie USB kľúča škodlivým softvérom (vyvrátená)

Pomocou nástroja Autopsy bola vykonaná forenzná analýza obrazu USB zariadenia vrátane aktívnych, skrytých a zmazaných súborov. Zamerali sme sa najmä na výskyt spustiteľných súborov typických pre malvér, ako sú prípony .exe, .dll, .bat, .cmd, .com, prípadne skriptové a autorun súbory. Počas tejto analýzy neboli nájdené žiadne podozrivé súbory ani stopy po automatickom spúšťaní kódu.

Následne bol obraz USB zariadenia skontrolovaný aj pomocou antivírusového softvéru Malwarebytes, ktorý neidentifikoval žiadne škodlivé objekty ani súbory známe z databázy malvéru.

Na základe uvedených zistení možno konštatovať, že v čase analýzy nebol na USB kľúči prítomný žiadny malvér a nič nenasvedčuje tomu, že by bol do zariadenia počas jeho absencie zavedený škodlivý softvér.

The screenshot displays the Autopsy forensic tool interface. On the left is a sidebar with a tree view of data sources and analysis results. The main window is titled 'Scanner' and shows a 'Custom Scan summary' for a scan completed on 4. 4. 2025 at 18:05:14. The summary indicates that 3 items were scanned in 1m 2s, with no threats, PUPs, or PUMs detected. Below the summary is a 'Scan report' section with a 'Summary' tab showing 'No items detected' and a 'Date' of 4. 4. 2025 18:05:14. The 'Scan result' is 'Completed'. At the bottom right, there is a 'Close' button.

Scanner

Scan Scheduler Reports

Custom Scan summary
4. 4. 2025 18:05:14

Scan time	1m 2s
Items scanned	3
Threats detected	0
PUPs detected	0
PUMs detected	0
Detections ignored	0
Detections quarantined	0

[View report](#) [Done](#)

Scan report

Summary Advanced

Scan summary
No items detected

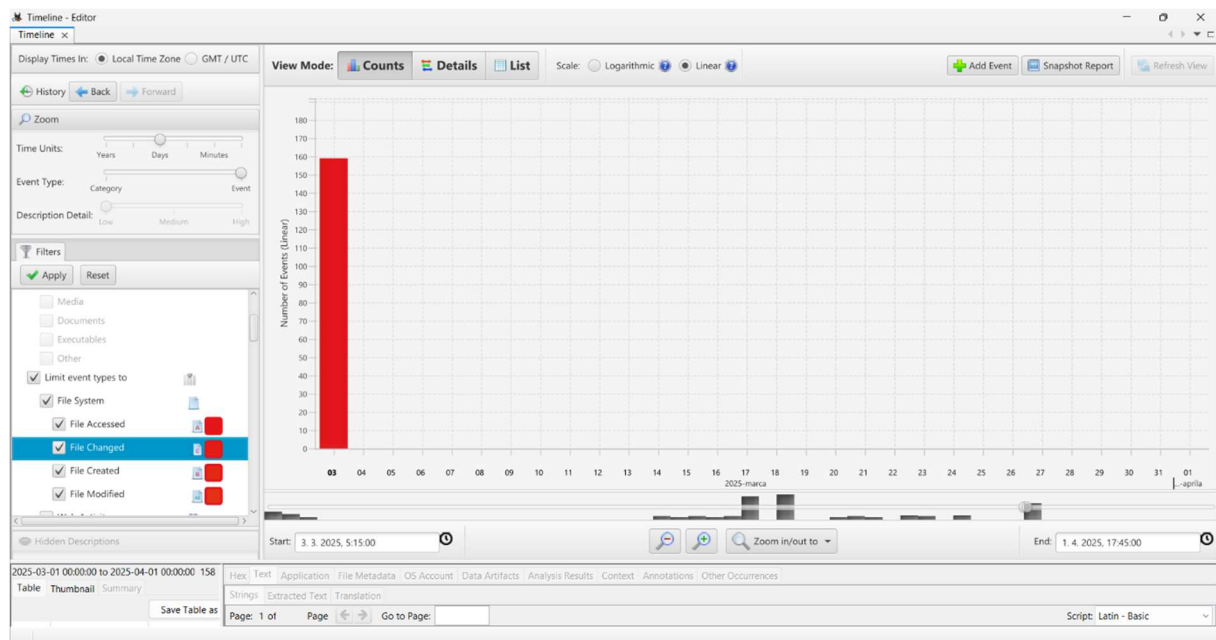
Date
4. 4. 2025 18:05:14

Scan result
Completed

[Export](#) [Close](#)

Neoprávnené kopírovanie alebo pozmenenie firemných dokumentov (potvrdená)

Zamestnanec, ktorý mal na starosti daný USB kľúč vo svedeckej výpovedi uviedol, že ho v deň odcudzenia nepoužil. Pomocou nástroja Autopsy sme došli k záveru, že bol určite použitý v deň incidentu.



Kontrolovali sme metadáta všetkých súborov. Pri tejto kontrole sme sa zameriavali na metadáta Modified Time, Access Time, Change Time a Created Time. Objavili sme jeden súbor, s ktorým sa manipulovalo v čase absencie. Bol vymazaný v čase odcudzenia USB kľúča. Jednalo sa o súbor s názvom _00043.xls, čo je formát tabuľkového súboru Microsoft Excel.

Name	S	C	O	Modified Time	Access Time	Change Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
_00043.xls				2025-03-03 16:37:04 SEČ	2025-03-03 16:00:00 SEČ	0000-00-00 00:00:00	12656640	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
NORTHBRIDGE				2022-02-18 10:58:28 SEČ	1988-01-20 01:00:00 SEČ	0000-00-00 00:00:00	1330598466	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
LCOTTSVILLE				2021-10-14 09:42:16 SELČ	1985-09-24 01:00:00 SELČ	0000-00-00 00:00:00	1280067926	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
TIPTONVILLE				2021-02-09 11:32:00 SEČ	2020-02-15 01:00:00 SEČ	0000-00-00 00:00:00	1280067912	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
SPEARVILLE				2021-02-01 11:34:38 SEČ	1982-09-23 01:00:00 SELČ	0000-00-00 00:00:00	825688064	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
OUTIERVILLE				2019-10-12 09:24:00 SELČ	2021-02-05 01:00:00 SEČ	0000-00-00 00:00:00	1329733714	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
ASSOCIATION				2018-10-01 09:24:00 SELČ	2019-02-09 01:00:00 SEČ	0000-00-00 00:00:00	541871173	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
ARGENTVILLE				2018-02-01 09:42:38 SEČ	1984-09-19 01:00:00 SELČ	0000-00-00 00:00:00	88430159	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
ALVERTVILLE				2018-02-01 09:24:00 SEČ	2019-02-09 01:00:00 SEČ	0000-00-00 00:00:00	1124073479	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
BLOUNTSTOWN				2016-10-14 10:58:04 SELČ	1983-09-20 01:00:00 SELČ	0000-00-00 00:00:00	1369	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
SENECAVILLE				2016-10-14 09:42:38 SELČ	1982-10-25 00:00:00 SEČ	0000-00-00 00:00:00	1163067392	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
VEEDERSBURG				2015-10-05 11:48:00 SELČ	2018-10-21 01:00:00 SELČ	0000-00-00 00:00:00	1163264000	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
RAGLESVILLE				2015-10-01 11:16:00 SELČ	2024-10-05 01:00:00 SELČ	0000-00-00 00:00:00	1095892992	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
CRADLEBAUGH				2015-02-01 11:18:06 SEČ	1983-10-20 00:00:00 SEČ	0000-00-00 00:00:00	1870	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
LARENDON				2014-10-12 09:10:44 SELČ	1989-09-18 01:00:00 SELČ	0000-00-00 00:00:00	1142959183	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi
AYETTEVILLE				2014-10-05 11:18:12 SELČ	1984-09-22 01:00:00 SELČ	0000-00-00 00:00:00	88427596	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi

Name	S	C	O	Modified Time	Access Time	Change Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
_00043.xls				2025-03-03 16:37:04 SEČ	2025-03-03 16:00:00 SEČ	0000-00-00 00:00:00	12656640	Unallocated	Unallocated	unknown	/img_obraz.001/vol_voi2/

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
	Name:		/img_obraz.001/vol_vol2/\$OrphanFiles/_00043.xls						
	Type:		File System						
	MIME Type:		application/octet-stream						
	Size:		12656640						
	File Name Allocation:		Unallocated						
	Metadata Allocation:		Unallocated						
	Modified:		2025-03-03 16:37:04 SEČ						
	Accessed:		2025-03-03 16:00:00 SEČ						

K vymazaniu tohto súboru došlo pravdepodobne v čase okolo 16:37 v deň odcudzenia.

Neoprávnené použitie USB kľúča bez zlého úmyslu(vyvrátená)

Do okruhu možných osôb, ktoré mohli použiť USB kľúč, patrili kolega zdieľajúci kanceláriu s dotknutým zamestnancom a upratovačka, ktorá zabezpečuje upratovanie celého objektu. Len tieto dve osoby mali prístup do danej kancelárie, keďže sa pri neprítomnosti daných zamestnancov zamyká.

Obaja podozriví však majú alibi. Kolega bol v čase medzi 12:00 a 13:00 na obede (išiel o pár minút skôr a vrátil sa neskôr ako dotknutý zamestnanec), čo potvrdilo viacero očitých svedkov. Upratovačka v tom čase čerpala dovolenku, čo potvrdila aj jej rodina.

Navyše je táto hypotéza vyvrátená, lebo sa jednalo o neoprávnené použitie so zlým úmyslom.

Záver

Na základe vykonanej digitálnej forenzej analýzy, svedeckých výpovedí a technických zistení bolo možné potvrdiť, že v danom prípade došlo k neoprávnenému zásahu do firemných dát, konkrétne ku kopírovaniu a vymazaniu citlivého súboru z USB zariadenia.

Analyzované dôkazy nasvedčujú tomu, že išlo o úmyselný čin neautorizovanej osoby, čo napĺňa znaky priemyselnej špionáže a sabotáže. Prípadná snaha zahladať stopy zmazaním súboru len potvrdzuje zámer útočníka.

Hypotéza o neoprávnenom pozmenení alebo kopírovaní firemných dokumentov bola jasne potvrdená. Digitálne metadáta súboru _00043.xls preukázali manipuláciu počas obdobia, keď mal byť USB kľúč fyzicky neprístupný a zamestnanec, ktorý bol zaň zodpovedný, v danom čase tvrdil, že ho nepoužil.

Tvrdenia tohto zamestnanca sa pritom nejavia ako klamstvo. Jeho prístup k PC bol zabezpečený pomocou fyzického bezpečnostného kľúča YubiKey, a preto neexistovali dôvody analyzovať jeho pracovný počítač ani systémové logy. Navyše, manipulácia so súborom sa odohrala v čase jeho preukázateľnej neprítomnosti.

Rovnako bol vylúčený kolega zdieľajúci kanceláriu. Ten odišiel na obed o pár minút skôr a vrátil sa neskôr ako dotknutý zamestnanec, než bol USB kľúč odcudzený a jeho alibi bolo potvrdené viacerými osobami.

Z analýzy vyplynulo, že USB zariadenie bolo manipulované neoprávnenou osobou, ktorej identitu sa doposiaľ nepodarilo zistiť. Všetky dostupné technické a personálne dôkazy však smerujú k tomu, že páchatel' nemal oficiálny prístup k systému ani k USB kľúču, čo značí, že išlo o externý alebo účelovo utajený zásah do infraštruktúry spoločnosti.

Na základe uvedeného možno konštatovať, že:

- Došlo k neoprávnenému použitiu USB zariadenia a manipulácii s citlivým súborom.
- Incident vykazuje znaky priemyselnej špionáže a sabotáže.
- Páchatel' zostáva neznámy, avšak s vysokou pravdepodobnosťou ide o osobu mimo okruhu oprávnených zamestnancov.

Odborné články z DFRWS:

In Search of Lost Data: A Study of Flash Sanitization Practices: Tento článok sa zaoberá problémom nedostatočného mazania dát na USB kľúčoch predávaných ako nové. Výskum ukazuje, že viac ako 12 % testovaných zariadení obsahovalo obnoviteľné údaje, čo predstavuje bezpečnostné riziko. Štúdia sa zameriava na trh s lacnými USB kľúčmi v Číne a poukazuje na dôsledky tohto problému pre forenzné vyšetovanie.

<https://dfrws.org/presentation/in-search-of-lost-data-a-study-of-flash-sanitization-practices/>

Secure USB Bypassing Tool: Tento text je o raste používania USB pamätí v dôsledku zvyšujúcej sa kapacity úložného priestoru a vývoja flash pamäte. S nárastom používania týchto zariadení sa častejšie vyskytujú porušenia súkromia a úniku technických informácií. Text sa zaoberá bezpečnostnými funkciami USB pamätí a popisuje návrh a implementáciu nástroja na obídenie týchto bezpečnostných funkcií, ktorý využíva príkazy USB ovládača.

<https://dfrws.org/presentation/secure-usb-bypassing-tool/>

Literatúra a prípadové štúdie:

<https://www.mailxaminer.com/blog/usb-forensics/>

Tento článok sa zameriava na analýzu USB zariadení. Popisuje proces identifikácie zariadení, extrakcie dát a forenzného snímania. Popisuje aj výzvy ako šifrovanie a techniky zamerané proti forenznej analýze.

<https://hawkeyeforensic.com/2024/02/05/usb-forensics-understanding-the-basics-of-digital-investigation>

Tento článok sa zameriava na metodológie USB forenznej analýzy, vrátane identifikácie zariadení a analýzy časových línií. Rieši aj výzvy ako šifrovanie a útoky na firmvér.