

Únik citlivých firemných dát

Prezentácia

Motivácia:

Pred dvoma týždňami dostalo niekoľko manažérov spoločnosti zaoberajúcej sa dodávaním softvérových riešení e-mail s predmetom „Ste si istí, že vaše tajomstvá zostanú v bezpečí?“. Príloha obsahovala výpis niektorých dôverných údajov, ktoré mali byť prístupné len na firemnom serveri.

Interná IT bezpečnosť analyzovala uniknuté dáta a potvrdila, že ide o dokumenty uložené v zabezpečenom firemnom úložisku. K týmto súborom mali prístup len vybraní zamestnanci vyššieho manažmentu.

Pri kontrole záznamov sa zistilo, že pred tromi týždňami došlo k neautorizovanému presunu veľkého množstva dát na externé zariadenie – USB kľúč. Túto operáciu vykonal užívateľský účet, ktorý patrilo Davidovi R., senior analytikovi v oddelení finančných stratégií.

David tvrdí, že v daný deň nebol v práci, pretože bol na služobnej ceste. Avšak, bezpečnostné kamery zachytili neznámu osobu vojsť do jeho kancelárie pred tým ako odišiel na letisko.

V koši v priestoroch firmy sa našiel USB kľúč značky SanDisc, ktorý by mohol obsahovať uniknuté dáta.

Typ analyzovanej digitálnej stopy:

Informácie, ktoré hľadáme:

- Identifikácia spôsobu, akým dôverné údaje unikli z firemného úložiska.
- Overenie, či bol na prenos údajov použitý nájdený USB kľúč.
- Identifikácia osoby, ktorá vykonala neautorizovaný presun dát.
- Overenie tvrdenia Davida R., že v daný deň nebol v práci.
- Skúmanie záznamov o fyzickom prístupe (napr. elektronické karty na vstup).
- Forenzná analýza nájdeného USB kľúča SanDisc
- Skúmanie možných motívov Davida R. alebo iných zamestnancov na vykonanie úniku dát.

Digitálne zariadenie súvisiace s prípadom:

- Nájdené USB pamäťové zariadenie
- Bezpečnostný kamerový systém
- Dochádzkový systém
- PC Davida R.
- Firemný server

5WH - Predmet a ciele vyšetovania:

Kto? Neznámy páchateľ využil účet Davida R., senior analytika, na neautorizovaný presun dát.

Čo? Došlo k úniku dôverných firemných informácií cez USB kľúč.

Kedy? Pred tromi týždňami sa uskutočnil prenos dát, incident bol zistený pred dvoma týždňami.

Kde? Únik dát sa odohral na firemnom serveri a kancelárii Davida R.

Prečo? Motivácia páchateľa zatiaľ nie je známa – môže ísť o priemyselnú špionáž, osobnú odplatu alebo finančný zisk.

Ako? Použitím USB zariadenia na skopírovanie dát, útočník mohol získať prístup k účtu Davida R.

Ciele vyšetovania:

- Analyzovať digitálne zariadenia spojené s prípadom
- Určiť, či bol uniknutý USB kľúč skutočne použitý na kopírovanie dát.
- Identifikovať páchateľa.
- Identifikovať motív páchateľa.
- Identifikovať škody spôsobené páchateľom

Hypotézy:

1. Únik dát vykonal samotný David R.

- Overenie: Preskúmame jeho pohyb cez záznamy bezpečnostných kamier a elektronických dochádzkových systémov. Skontrolujeme históriu jeho pripojenia a použitia USB zariadení.
- Výsledok: Ak záznamy preukážu, že v daný deň nebol v práci a nemohol vykonať prenos, hypotéza bude zamietnutá.

2. Útočník získal prístup k účtu Davida R. bez jeho vedomia.

- Overenie: Skontrolujeme, či došlo k neautorizovanému prihláseniu alebo kompromitácii hesla. Zistíme, či boli v systéme zistené neobvyklé aktivity.
- Výsledok: Ak nájdeme dôkazy o podvodnom prihlásení alebo narušení bezpečnosti, hypotéza bude potvrdená.

3. Neznáma osoba fyzicky použila počítač Davida R. na stiahnutie dát.

- Overenie: Analyzujeme záznamy bezpečnostných kamier a preskúmame počítač Davida R., aby sme zistili, kto a kedy s ním manipuloval.
- Výsledok: Ak sa potvrdí prístup inej osoby do kancelárie a interakcia s počítačom, hypotéza bude potvrdená.

Odborné príspevky:

https://dfrws.org/wp-content/uploads/2019/06/pres_deleted_file_persistence_on_digital_media.pdf

Tento príspevok sa zaoberá pretrváváním vymazaných súborov na digitálnych médiách a faktormi, ktoré ovplyvňujú ich obnoviteľnosť.

https://dfrws.org/sites/default/files/session-files/2007_USA_pres-10_good_reasons_why_you_should_shift_focus_to_small_scale_digital_device_forensics.pdf

Tento príspevok zdôrazňuje význam forenzného skúmania malých digitálnych zariadení (Small Scale Digital Devices – SSDD), ako sú mobilné telefóny, PDA, herné konzoly či flash pamäte, vzhľadom na ich rastúcu úlohu v kybernetických incidentoch a kriminalite.

Foto nájdeneho USB kľúča:



Vlastnosti:

- Značka: SanDisk
- Model: Ultra Dual Luxe
- SN: BM2210006318Z
- Rozmery: 12,1 x 8,6 x 44,41 mm
- Hmotnosť: 12,6g
- Kapacita: 32 GB
- Rozhranie: USB 3.2 Gen 1
- Podporované operačné systémy: Windows 10/8/7, Mac OS X v10.9+
- Rýchlosť Čítania: 150 MB/s

- Rýchlosť Zápisu: 25 MB/s
- Šifrovanie: AES-128
- Farba: Strieborná
- Materiál: Kov

Foto laptopu:



Vlastnosti:

- Lenovo ThinkPad T460
- Procesor: Intel Core i5-6200U (2.30 GHz, 6. generácia)
- Pamäť RAM: 8 GB DDR4
- Úložisko: 256GB SSD
- Displej: 14" Full HD (1920x1080)
- Operačný systém: Windows 10 Pro
- Typ systému: 64-bitový

Bezpečnostné opatrenia:

- Vytvorenie forenzej image - bitovej kópie disku bez modifikácie originálu (dve kópie)
- Fyzická izolácia a zabezpečenie zariadení - uloženie do antistatického vrečka s pečatou, zaznamenanie fyzického stavu (značka, sériové číslo, poškodenia)
- Výpočet kryptografických hashov pre originál a image - porovnanie hashov pred a po analýze na detekciu manipulácie
- Reťazec starostlivosti (Chain of Custody) - dátum a čas zabavenia, mená osôb ktoré zariadenia prevzali, popis opatrení na ochranu dôkazov

- Bezpečné uloženie - USB a laptop uložený v klimatizovanom trezore s kontrolou prístupu, zabezpečenie proti elektromagnetickému žiareniu, vlhku a extrémnym teplotám
- Pre digitálne kópie použité šifrovanie AES-256

Použité nástroje digitálnej forenzej analýzy:

- **FTK Imager** – nástroj na rýchle vytváranie bitových kópií diskov a USB zariadení a ich následné prehliadanie bez narušenia originálnych dát.
- **Autopsy** – open-source digitálna forenzná platforma na analýzu súborov, logov, e-mailov a obnovu zmazaných dát.
- **OSForensics** – softvér určený na podrobnú forenznú analýzu počítačových systémov vrátane vyhľadávania súborov, hesiel a emailov.
- **Belkasoft X Forensic** – komplexný nástroj pre analýzu počítačov, mobilných zariadení a cloudových dát s podporou artefaktov z mnohých aplikácií.
- **Magnet RAM Capture** – špecializovaný nástroj na získavanie obsahu operačnej pamäte (RAM) zo živých systémov na účely forenznej analýzy.

Chain of custody:

Číslo:	01	Typ súboru:	raw	Obnovený súbor:	Nie	Veľkosť:	30 765 222 477 B
Popis prípadu:		Únik citlivých firemných dát					
Názov súboru:		USB_image					
Miesto získania digitálnej stopy:		Nájdenny USB kľúč					
Poznámky:		Bitová kópia nájdenného USB kľúča					
Časové pečiatky							
Access:	Sun Apr 13 16:32:23 2025	Modify:	Sun Apr 13 16:32:23 2025	Change:	Sun Apr 13 16:32:23 2025		
Digitálny odtlačok (heš)							
MD5		38d9fe233fd4e825cbbd6fb55750fd43					
SHA1		496e06d8299edb750635948b96175174e6865b72					
Časová pečiatka							
Akcia vykonaná s digitálnou stopou							

Metadáta USB kľúča získané pomocou FTK Imager:

Created By Exterro® FTK® Imager 4.7.3.81

Case Information:

Acquired using: ADI4.7.3.81

Case Number: 01

Evidence Number: 001

Unique description: USB_kluc

Examiner: Jozef

Notes: USB kluc najdeny v kosi v kancelarii

Information for C:\Users\User\Desktop\Digitalna forenzna analyza\USB_Image\USB_image:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 3 740

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 60 088 320

[Physical Drive Information]

Drive Model: USB SanDisk 3.2Gen1 USB Device

Drive Serial Number: 01018adfb55b9c145b18

Drive Interface Type: USB

Removable drive: True

Source data size: 29340 MB

Sector count: 60088320

[Computed Hashes]

MD5 checksum: 38d9fe233fd4e825cbbd6fb55750fd43

SHA1 checksum: 496e06d8299edb750635948b96175174e6865b72

Image Information:

Acquisition started: Sun Apr 13 16:32:23 2025

Acquisition finished: Sun Apr 13 16:36:45 2025

Segment list:

C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.001
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.002
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.003
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.004
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.005
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.006
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.007
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.008
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.009
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.010
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.011
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.012
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.013
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.014
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.015
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.016
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.017
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.018
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.019
C:\Users\User\Desktop\Digitalna forenzna analiza\USB_Image\USB_image.020

Podozrivé údaje obrazu RAM získané pomocou FTK Imager:

Podozrivý David R. má v pamäti RAM svojho firemného PC záznamy o kopírovaní dokumentu s názvom „Confidential Exec Budget“.

014b698b0	75 00 20 00 6E 00 61 00-20 00 55 00 53 00 42 00	u · n · a · U · S · B ·
014b698c0	2C 00 22 00 63 00 6F 00-70 00 79 00 20 00 22 00	, · " · c · o · p · y · " ·
014b698d0	22 00 43 00 3A 00 5C 00-55 00 73 00 65 00 72 00	" · C · : · \ · U · s · e · r ·
014b698e0	73 00 5C 00 44 00 61 00-76 00 69 00 64 00 52 00	s · \ · D · a · v · i · d · R ·
014b698f0	5C 00 44 00 6F 00 63 00-75 00 6D 00 65 00 6E 00	\ · D · o · c · u · m · e · n ·
014b69900	74 00 73 00 5C 00 45 00-78 00 65 00 63 00 5C 00	t · s · \ · E · x · e · c · \ ·
014b69910	43 00 6F 00 6E 00 66 00-69 00 64 00 65 00 6E 00	C · o · n · f · i · d · e · n ·
014b69920	74 00 69 00 61 00 6C 00-5F 00 45 00 78 00 65 00	t · i · a · l · _ · E · x · e ·
014b69930	63 00 5F 00 42 00 75 00-64 00 67 00 65 00 74 00	c · _ · B · u · d · g · e · t ·
014b69940	2E 00 78 00 6C 00 73 00-78 00 22 00 22 00 20 00	· x · l · s · x · " · " · ·

Podozrivý David R. má v pamäti RAM svojho firemného PC záznamy o návšteve webovej stránky anonymného uploadera.

014b699ab0	64 00 65 00 72 00 61 00-2C 00 68 00 74 00 74 00	d · e · r · a · , · h · t · t ·
014b699ac0	70 00 73 00 3A 00 2F 00-2F 00 61 00 6E 00 6F 00	p · s · : · / · / · a · n · o ·
014b699ad0	6E 00 79 00 6D 00 66 00-69 00 6C 00 65 00 2E 00	n · y · m · f · i · l · e · . ·
014b699ae0	69 00 6F 00 2F 00 75 00-70 00 6C 00 6F 00 61 00	i · o · / · u · p · l · o · a ·
014b699af0	64 00 0D 00 00 00 00 00-04 00 00 00 00 00 00	d · . · . · . · . · . · . · .

Časy týchto záznamov v RAM sedia s časom incidentu.

014b699a20	0D 00 32 00 30 00 32 00-35 00 2D 00 30 00 33 00	· 2 · 0 · 2 · 5 · - · 0 · 3 ·
014b699a30	2D 00 31 00 35 00 20 00-30 00 39 00 3A 00 33 00	- · 1 · 5 · - · 0 · 9 · : · 3 ·
014b699a40	35 00 3A 00 34 00 35 00-2C 00 63 00 68 00 72 00	5 · : · 4 · 5 · , · c · h · r ·

Podozrivé údaje z dochádzkového systému budovy:

Dátum	Zariadenie	Typ záznamu	Užívateľ	ID karty	Oddelenie	Prístup povolený	Čas vstupu	Dverný senzor	kancelária
2025-03-15	Prístupový terminál č. 2	(hlavný vstup - 1. poschodie)	Prístup do objektu	Lenka B.	9001732LB	Marketing	Áno	07:10:49 CET	07:11:06 CET
2025-03-15	Prístupový terminál č. 2	(hlavný vstup - 1. poschodie)	Prístup do objektu	Roman V.	0019342RV	Logistika	Áno	07:53:32 CET	07:54:09 CET
2025-03-15	Prístupový terminál č. 2	(hlavný vstup - 1. poschodie)	Prístup do objektu	Tibor S.	2231109TS	Bezpečnosť	Áno	08:15:34 CET	08:16:39 CET
2025-03-15	Prístupový terminál č. 2	(hlavný vstup - 1. poschodie)	Prístup do objektu	Martin K.	5820132MK	IT	Áno	08:56:41 CET	08:57:05 CET
2025-03-15	Prístupový terminál č. 2	(hlavný vstup - 1. poschodie)	Prístup do objektu	Petra H.	1183920PH	HR	Áno	09:08:14 CET	09:08:20 CET
2025-03-15	Prístupový terminál č. 2	(hlavný vstup - 1. poschodie)	Prístup do objektu	David R.	0293874DR	Finančné stratégie	Áno	09:25:37 CET	09:26:02 CET
2025-03-15	Prístupový terminál č. 2	(hlavný vstup - 1. poschodie)	Prístup do objektu	Ivana J.	3838473IJ	Právne oddelenie	Áno	09:52:12 CET	09:53:05 CET
2025-03-15	Prístupový terminál č. 2	(hlavný vstup - 1. poschodie)	Prístup do objektu	Marek F.	8381113MF	Údržba	Áno	09:58:39 CET	09:59:16 CET

Podozrivé údaje z firemnej databázy:

2025-03-15	Roman V.	Legal_Contracts_Archive.zip	viewed	09:15:00 CET
2025-03-15	Roman V.	HR_Policy_2024.pdf	viewed	10:37:00 CET
2025-03-15	Marek F.	Fin_Report_Q1_2025.xlsx	viewed	09:28:00 CET
2025-03-15	Tibor S.	Legal_Contracts_Archive.zip	downloaded	09:14:00 CET
2025-03-15	Ivana J.	Marketing_Strategy_2025.docx	viewed	09:38:00 CET
2025-03-15	Martin K.	Fin_Report_Q1_2025.xlsx	downloaded	08:16:00 CET
2025-03-15	Petra H.	Confidential_Exec_Budget.xlsx	edited	08:11:00 CET
2025-03-15	David R.	Confidential_Exec_Budget.xlsx	downloaded	09:34:10 CET
2025-03-15	Roman V.	Confidential_Exec_Budget.xlsx	viewed	08:25:00 CET
2025-03-15	Petra H.	Warehouse_Log_March.csv	edited	11:56:00 CET
2025-03-15	Lenka B.	HR_Policy_2024.pdf	edited	08:26:00 CET

Snímka z bezpečnostnej kamery:



Záver:

Na základe komplexnej digitálnej forenznej analýzy uskutočnenej v rámci incidentu úniku dôverných údajov zo zabezpečeného firemného úložiska bolo možné dôveryhodne rekonštruovať sled udalostí a identifikovať pravdepodobného páchatela.

Spočiatku sa ako kľúčová stopa javil USB kľúč značky SanDisk, nájdený v odpadkovom koši v priestoroch firmy. Po detailnej forenznej analýze obsahu tohto zariadenia sa však ukázalo, že nejde o relevantný dôkaz – na USB kľúči sa nenachádzali žiadne dáta, ktoré by súviseli s únikom dôverných dokumentov. Táto stopa bola preto vyhodnotená ako falošná alebo prípadne ako pokus páchatela o odvedenie pozornosti vyšetrovateľov.

Forezná pozornosť sa následne zamerala na notebook podozrivého – Davida R., firemnú databázu logov, záznamy z dochádzkového systému a bezpečnostné kamery.

Analýza poskytla súbor jednoznačných digitálnych dôkazov, ktoré zahŕňajú:

Záznam bezpečnostnej kamery zachytávajúci neznámu osobu vstupujúcu do kancelárie Davida R. krátko pred jeho deklarovaným odchodom na služobnú cestu

Dochádzkový záznam potvrdzujúci fyzickú prítomnosť Davida R. v budove v čase incidentu,

Záznam z firemnej databázy prístupov, ktorý preukázal, že z jeho používateľského účtu boli stiahnuté dôverné dokumenty v konkrétnom čase,

Forezná analýza RAM pamäte, ktorá odhalila spustené aplikácie, manipuláciu so súbormi, pripojené USB zariadenie a dokonca pokus o ich odoslanie prostredníctvom anonymnej webovej služby,

Komunikačné artefakty, ktoré poukazujú na potenciálny úmysel vydierať firmu výmenou za nezverejnenie citlivých údajov.

Na základe týchto zistení možno s vysokou mierou pravdepodobnosti potvrdiť platnosť prvej hypotéz že páchatelom je interný zamestnanec David R., ktorý vedome a cielene manipuloval s dôvernými firemnými údajmi s úmyslom osobného obohatenia.