

Neautorizovaný prenos dát

Link na prezentáciu: <https://bcstudent.fpvucm.sk/~mihalikjakub/dfa/prezentacia.pdf>

Motivácia

Táto forenzná analýza sa zaoberá vyšetrovaním prípadu podozrenia z neoprávneného prenosu citlivých dát zo systému spoločnosti DataSecure. Na mieste incidentu bolo objavené neznáme USB zariadenie, ktoré mohlo byť použité na exfiltráciu dát alebo vykonanie škodlivých operácií. Cieľom analýzy je preskúmať digitálne dôkazy a určiť, či došlo k úniku informácií alebo manipulácii s dátami.

Ciele digitálnej forenzej analýzy

1. Overiť, či USB zariadenie obsahuje dôkazy o neautorizovanom prenose dát.
2. Preskúmať obsah USB, jeho metadáta a históriu použitia.
3. Analyzovať sieťové logy a systémové záznamy na identifikáciu podozrivých aktivít.
4. Zrekonštruovať postup útoku a spôsob získania alebo odstránenia dát.
5. Identifikovať možného páchatel'a na základe digitálnych dôkazov.

Opis incidentu

Spoločnosť DataSecure zaznamenala anomáliu v prenose dát, ktorá naznačuje možný únik citlivých informácií. Interný bezpečnostný systém zaznamenal pripojenie neznámeho USB zariadenia k firemnému notebooku v čase, keď došlo k náhlemu zvýšeniu sieťovej aktivity. Po ďalšej analýze sa zistilo, že niektoré súbory boli buď skopírované, alebo vymazané.

Počas fyzickej kontroly miesta incidentu IT oddelenie objavilo USB kľúč, ktorý nepatrí žiadnemu zo zamestnancov. Toto zariadenie mohlo byť použité na exfiltráciu dát alebo na vykonanie neoprávnených operácií v systéme.

Zariadenia prítomné na mieste incidentu

1. Firemný notebook

- Používaný na prístup k interným databázam a spracovanie citlivých informácií.
- Zaznamenaná aktivita naznačuje pripojenie neznámeho USB zariadenia a možný prenos dát.
- Možná kompromitácia softvéru alebo zneužitie administrátorských práv.

2. USB kľúč (neidentifikované zariadenie)

- Objavený na mieste incidentu, pravdepodobne použitý na exfiltráciu dát.
- Môže obsahovať digitálne dôkazy, ako sú skopírované súbory alebo logy z prístupu.
- Potenciálne obsahuje škodlivý softvér určený na manipuláciu so systémom.

Hypotézy

1. USB zariadenie bolo použité na exfiltráciu dát.

- Útočník skopíroval citlivé súbory z firemného notebooku na USB kľúč.
- Dôkazy: metadáta skopírovaných súborov, záznamy v systéme, analýza obsahu USB.

2. USB obsahovalo škodlivý kód na manipuláciu s dátami.

- Útočník použil USB na spustenie škodlivého skriptu, ktorý modifikoval alebo vymazal súbory.
- Dôkazy: nájdené spustiteľné súbory alebo logy o neobvyklých operáciách.

3. Firemný notebook bol kompromitovaný fyzickým prístupom

- Útočník získal priamy prístup k notebooku, využil administrátorské práva alebo bezpečnostné slabiny.
- Dôkazy: záznamy o prihlásení, systémové udalosti, zmeny nastavení, stopy po použití USB

4. Externej osobe bolo umožnené vykonať analýzu a manipuláciu s dátami na firemnom zariadení

- Externý odborník mohol vykonať prístup k firemnému notebooku alebo iným zariadeniam s cieľom vykonať analýzu alebo zmeniť nastavenia systému.
- Dôkazy: Záznamy o prístupe od externých osôb, IP adresy, časové pečiatky, logy o prihlásení.

5WH (Who, What, When, Where, Why, How)

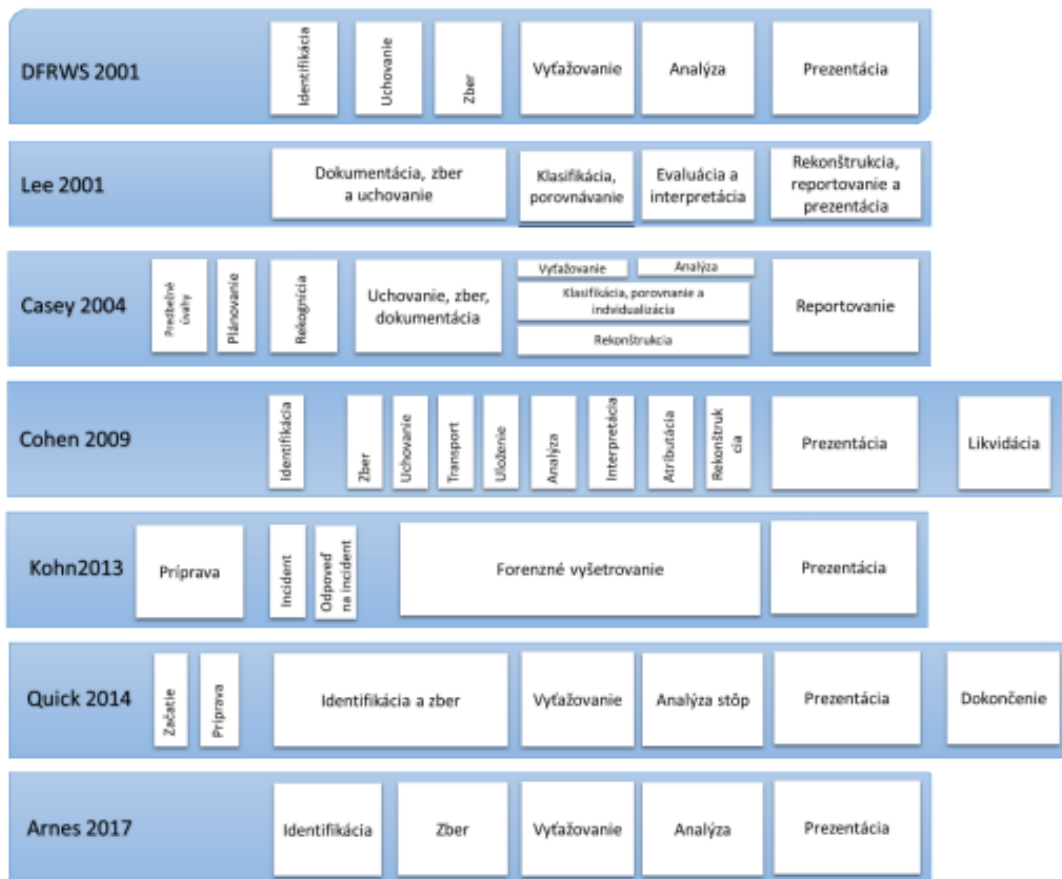
- **Who (Kto?)** — Neznámy útočník, interný alebo externý aktér so znalosťou firemného prostredia.
- **What (Čo?)** – USB zariadenie, notebook a mobilný telefón, ktoré mohli byť použité na získanie alebo manipuláciu s dátami.
- **When (Kedy?)** – Incident sa stal v nočných hodinách, v čase zvýšenej sieťovej aktivity a pripojenia neznámeho USB.
- **Where (Kde?)** — Na pracovisku v spoločnosti X, v kancelárii IT oddelenia, kde sa nachádzal notebook s prístupom k citlivým údajom.
- **Why (Prečo?)** — Cieľom mohlo byť získanie obchodne citlivých informácií alebo úmyselné poškodenie firemných systémov.
- **How (Ako?)** — Útočník použil USB na kopírovanie súborov alebo mobilný telefón na vzdialený prístup a exfiltráciu dát.

Cieľ vyšetrovania

Cieľom vyšetrovania je analyzovať USB zariadenie a notebook, aby sa zistilo, či došlo k neautorizovanému prenosu dát a kto je zaň zodpovedný. Forenzná analýza sa zameria na digitálne dôkazy, rekonštrukciu udalostí a identifikáciu bezpečnostných slabín. Výsledky poslúžia na určenie páchateľa, právne kroky a bezpečnostné odporúčania. Budú sa vyšetrovať reálne dáta o veľkosti 3000 súborov.

Popis vyšetrovania:

podľa schémy Arnes 2017



1. Identifikácia

Cieľom je overiť, či USB kľúč slúžil na neautorizovaný prenos firemných dát. Identifikovaným dôkazom je USB zariadenie obsahujúce podozrivé súbory, ktoré mohli byť skopírované z interného notebooku.

2. Zaisťovanie a zber

USB bolo zaistené, vytvorená bola forenzná kópia na analýzu. Zaznamenali sa technické údaje (kapacita, systém súborov). Originálne zariadenie nebolo ďalej používané.

3. Vyťažovanie

Prebehlo vyhľadávanie kľúčových slov, súborov a skriptov pomocou hex editora a forenzných nástrojov. Boli identifikované podozrivé súbory, dátumy úprav a možné prepojenie na firemné dáta.

4. Analýza

Súbory sa analyzovali podľa metadát a časových značiek. Overovalo sa, či mohli pochádzať z firemného systému a aký bol ich účel. Hľadali sa stopy po škodlivých skriptoch alebo nástrojoch na export dát.

5. Prezentácia

Výsledky boli spísané do správy s dôkazmi, časovou osou a závermi. Obsahuje návrhy na zlepšenie bezpečnosti a prevenciu podobných incidentov.

HW zariadenia, odobrané počas vyšetrovania:
USB kľúč s dátami:

Popis: USB kľúč Maxell Speedboat 64GB 3.1, čiernej farby, bol zaistený ako potenciálny dôkaz v prípade neautorizovaného prenosu dát z interných systémov spoločnosti. Kľúč obsahuje množstvo súborov, ktoré mohli byť skopírované z firemných zariadení bez povolenia, vrátane potenciálne citlivých alebo upravených dát.

Prečo sa vykonáva vyšetovanie: USB kľúč je podozrivý z toho, že bol použitý na prenos dát mimo bezpečnostného prostredia spoločnosti, čo môže znamenať porušenie interných bezpečnostných pravidiel a potenciálne úmyselné odstránenie alebo exfiltráciu dát. Cieľom vyšetovania je zistiť, aké dáta boli prenesené, či boli zmenené alebo poškodené, a identifikovať osobu, ktorá mohla tento prenos vykonať.

Číslo: 001

Popis prípadu: Neautorizovaný prenos dát

Názov súboru: prenos_dat_usb001

Miesto získania digitálnej stopy: Pracovisko spoločnosti X – serverovňa

Poznámky: Čierny USB kľúč, Maxell Speedboat 64GB USB 3.1, sériové číslo: 8756238392153193

Typ: USB kľúč

Access | Modify | Change

Časová pečiatka

1.4.2025 13:21

2.4.2025 10:00

3.4.2025 09:45

4.4.2025 14:20

Osoba

Samuel Horák

Kurier DPD 24

Jakub Mihálik

Jana Bieliková

Popis úkonu

Zaistenie dôkazu

Prebratie na prenos

Forenzná analýza dôkazu

Uloženie do archívu

Digitálny odtlačok (hash)

MD5: 7a5e820c8a1f3c7b2ff9056e3b1d2250

SHA1: cc3292fd1e0c4a13a23a465d1fd7e64f27359d7e

Časová pečiatka – Akcia vykonaná s digitálnou stopou

Dátum a čas

3.4.2025 09:45

3.4.2025 10:20

3.4.2025 11:10

Popis akcie

Vytvorená forenzná kópia USB

USB zariadenie vrátené do skladu

Analýza obsahu bitovej kópie

Zodpovedná osoba

Jakub Mihálik

Jakub Mihálik

Jakub Mihálik

Notebook (Pracovný počítač):

Popis: Notebook, ktorý bol používaný ako pracovná stanica na správu interných systémov spoločnosti. Zariadenie malo priamy prístup k databázam, sieťovým úložiskám a administrátorským nástrojom.

Prečo sa vykonáva vyšetrovanie: Tento počítač mohol zohrávať kľúčovú úlohu pri prenose dát na externé médium (USB). Analýza jeho operačnej pamäte (RAM), systémových logov a používateľskej aktivity môže pomôcť rekonštruovať udalosti spojené s neautorizovaným prenosom, identifikovať použitý softvér či skripty, a tiež časové pečiatky, ktoré potvrdzujú manipuláciu s dôvernými súbormi.

Číslo: 002

Popis prípadu: Neautorizovaný prenos dát

Názov súboru: prenos_dat_notebook002

Miesto získania digitálnej stopy: Pracovisko spoločnosti DataSecure – kancelária IT oddelenia

Poznámky: Firemný notebook, značky Lenovo ThinkPad T14s, SN: PF2R3X1T

Typ: Notebook

Access | Modify | Change

Časová pečiatka

1.4.2025 13:30

2.4.2025 10:15

3.4.2025 09:00

4.4.2025 14:45

Osoba

Samuel Horák

Kurier DPD 24

Jakub Mihálik

Jana Bieliková

Popis úkonu

Zaistenie dôkazu

Prebratie na prenos

Forenzná analýza

Uloženie do archívu

Digitálny odtlačok (hash)

MD5: e1a4d5a3b2c7d0f6a0be2f15d72cf891

SHA1: 9f6b1c2f4eaf2c70f30a4bc1c50e1672d4b7ea25

Časová pečiatka – Akcia vykonaná s digitálnou stopou

Dátum a čas

3.4.2025 09:45

Popis akcie

Vytvorenie bitovej kópie
systémového disku

Systémová analýza logov a
procesov

Zodpovedná osoba

Jakub Mihálik

Jakub Mihálik

Kamery:

Popis: Kamerový server slúži ako kľúčový zdroj vizuálnych dôkazov pri vyšetrovaní incidentu úniku dát. Umožňuje spätne overiť fyzickú prítomnosť osôb v konkrétnom čase a priestore, a tým identifikovať potenciálnych páchatel'ov alebo osoby s prístupom k postihnutým zariadeniam.

Prečo sa vykonáva vyšetrovanie: V kombinácii s údajmi získanými z USB kľúča a firemného notebooku poskytuje kamerový server dôležité súvislosti. Pomáha rekonštruovať udalosti, časové rámce a identifikovať osoby, ktoré mohli manipulovať so zariadeniami alebo sa nachádzali na mieste incidentu v rozhodujúcom čase.

Číslo: 003

Popis prípadu: Neautorizovaný prenos dát

Názov súboru: prenos_dat_camserver003

Miesto získania digitálnej stopy: Serverovňa – kamerový záznamový systém spoločnosti DataSecure

Poznámky: Kamerový server Hikvision DS-7732NI-I4, SN: HVK-7743X1289

Typ: Záznamové zariadenie

Access | Modify | Change

Časová pečiatka

1.4.2025 13:30

Osoba

Samuel Horák

Popis úkonu

Prijatie dokazu

Digitálny odtlačok (hash)

MD5: 9c1a22d3e9f4a1b7adbe43f7de908a3c

SHA1: d7b71c0a6e10d431f672b49e84c54d3279d1e3ad

Časová pečiatka – Akcia vykonaná s digitálnou stopou

Dátum a čas

3.4.2025 09:45

Popis akcie

Analýza záznamu

Zodpovedná osoba

Jakub Mihálik

Dokaz001 (USB kľúč) – analýza

Výrobca: Maxell Speedboat 64G

Sériové číslo: 8756238392153193

Kapacita: 64GB

Rozhranie: USB 3.2 Gen 2 (USB 3.1)

Konektor: USB-A

Materiál: Plast

Farba: Čierna

Created By AccessData® FTK® Imager 4.7.1.2

Case Information:

Acquired using: ADI4.7.1.2

Case Number: 12345

Evidence Number: 001

Unique description: USB DISK 3.0

Examiner: Autor

Notes: Moj kluc

Information for C:\Users\student\Downloads\ram-capturer\RamCapturer\x64\jm-USB:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 7 540

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 121 145 344

[Physical Drive Information]

Drive Model: USB DISK 3.0 USB Device

Drive Serial Number: 0477211720B0

Drive Interface Type: USB

Removable drive: True

Source data size: 59153 MB

Sector count: 121145344

[Computed Hashes]

MD5 checksum: dc7fd93eb3384745db6aa339607fcc42

SHA1 checksum: d596d8ec5efd59e0c59cf975333881f9e0f2ca33

Image Information:

Acquisition started: Sat Mar 22 10:24:55 2025

Acquisition finished: Sat Mar 22 10:36:06 2025

Segment list:

C:\Users\student\Downloads\ram-capturer\RamCapturer\x64\jm-USB.001

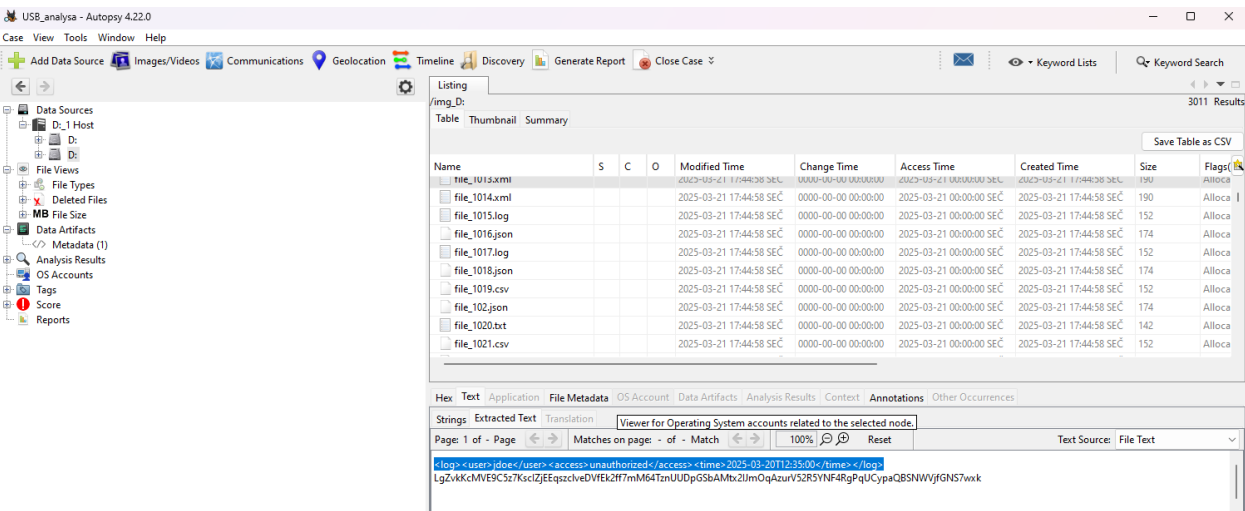
Image Verification Results:

Verification started: Sat Mar 22 10:36:06 2025

Verification finished: Sat Mar 22 10:38:22 2025

MD5 checksum: dc7fd93eb3384745db6aa339607fcc42 : verified

SHA1 checksum: d596d8ec5efd59e0c59cf975333881f9e0f2ca33 : verified



Bola vykonaná analýza programom Autopsy. Kde boli nájdené viaceré súbory a skripty, ktoré obsahovali neautorizovaný prístup. Ako napríklad: Confidential document. Access restricted, 2025-03-20 12:34:56 - Unauthorized access detected.,

Dôkaz 002 (notebook) – analýza

Lenovo ThinkPad T14 Gen 4 Black

Intel Core i5 1335U Raptor Lake, 14" IPS antireflexný 1920 × 1200, RAM 16 GB DDR5, Intel Iris Xe Graphics, SSD 512 GB, podsvietená klávesnica, webkamera, USB 3.2 Gen 1, čítačka odtlačkov prstov, WiFi 6E, hmotnosť 1,36 kg, Windows 10

ext-jm-ram.raw																	
Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00804AA0	64	65	76	69	63	65	20	6F	72	20	61	64	64	72	65	73	device or address
00804AB0	73	00	00	00	00	00	00	00	6E	6F	20	73	75	63	68	20	s.....no such
00804AC0	64	65	76	69	63	65	00	00	6E	6F	20	73	75	63	68	20	device..no such
00804AD0	66	69	6C	65	20	6F	72	20	64	69	72	65	63	74	6F	72	file or director
00804AE0	79	00	00	00	00	00	00	00	6E	6F	20	73	75	63	68	20	y.....no such
00804AF0	70	72	6F	63	65	73	73	00	6E	6F	74	20	61	20	64	69	process.not a di
00804B00	72	65	63	74	6F	72	79	00	6E	6F	74	20	61	20	73	6F	rectory.not a so
00804B10	63	6B	65	74	00	00	00	00	6E	6F	74	20	61	20	73	74	cket.....not a st
00804B20	72	65	61	6D	00	00	00	00	6E	6F	74	20	63	6F	6E	6E	ream.....not conn
00804B30	65	63	74	65	64	00	00	00	6E	6F	74	20	65	6E	6F	75	ected...not enou
00804B40	67	68	20	6D	65	6D	6F	72	79	00	00	00	00	00	00	00	gh memory.....
00804B50	6E	6F	74	20	73	75	70	70	6F	72	74	65	64	00	00	00	not supported...
00804B60	6F	70	65	72	61	74	69	6F	6E	20	63	61	6E	63	65	6C	operation cancel
00804B70	65	64	00	00	00	00	00	00	6F	70	65	72	61	74	69	6F	ed.....operatio
00804B80	6E	20	69	6E	20	70	72	6F	67	72	65	73	73	00	00	00	n in progress...
00804B90	6F	70	65	72	61	74	69	6F	6E	20	6E	6F	74	20	70	65	operation not pe
00804BA0	72	6D	69	74	74	65	64	00	6F	70	65	72	61	74	69	6F	rmitted.operatio
00804BB0	6E	20	6E	6F	74	20	73	75	70	70	6F	72	74	65	64	00	n not supported.
00804BC0	6F	70	65	72	61	74	69	6F	6E	20	77	6F	75	6C	64	20	operation would
00804BD0	62	6C	6F	63	6B	00	00	00	6F	77	6E	65	72	20	64	65	block...owner de
00804BE0	61	64	00	00	00	00	00	00	70	65	72	6D	69	73	73	69	ad.....permissi
00804BF0	6F	6E	20	64	65	6E	69	65	64	00	00	00	00	00	00	00	on denied.....
00804C00	70	72	6F	74	6F	63	6F	6C	20	65	72	72	6F	72	00	00	protocol error..
00804C10	70	72	6F	74	6F	63	6F	6C	20	6E	6F	74	20	73	75	70	protocol not sup
00804C20	70	6F	72	74	65	64	00	00	72	65	61	64	20	6F	6E	6C	ported...read onl
00804C30	79	20	66	69	6C	65	20	73	79	73	74	65	6D	00	00	00	y file system...
00804C40	72	65	73	6F	75	72	63	65	20	64	65	61	64	6C	6F	63	resource deadloc
00804C50	6B	20	77	6F	75	6C	64	20	6F	63	63	75	72	00	00	00	k would occur...
00804C60	72	65	73	6F	75	72	63	65	20	75	6E	61	76	61	69	6C	resource unavail
00804C70	61	62	6C	65	20	74	72	79	20	61	67	61	69	6E	00	00	able try again..
00804C80	72	65	73	75	6C	74	20	6F	75	74	20	6F	66	20	72	61	result out of ra
00804C90	6E	67	65	00	00	00	00	00	73	74	61	74	65	20	6E	6F	range.....state no
00804CA0	74	20	72	65	63	6F	76	65	72	61	62	6C	65	00	00	00	t recoverable...
00804CB0	73	74	72	65	61	6D	20	74	69	6D	65	6F	75	74	00	00	stream timeout..
00804CC0	74	65	78	74	20	66	69	6C	65	20	62	75	73	79	00	00	text file busy..
00804CD0	74	69	6D	65	64	20	6F	75	74	00	00	00	00	00	00	00	timed out.....
00804CE0	74	6F	6F	20	6D	61	6E	79	20	66	69	6C	65	73	20	6F	too many files o
00804CF0	70	65	6E	20	69	6E	20	73	79	73	74	65	6D	00	00	00	pen in system...
00804D00	74	6F	6F	20	6D	61	6E	79	20	66	69	6C	65	73	20	6F	too many files o
00804D10	70	65	6E	00	00	00	00	00	74	6F	6F	20	6D	61	6E	79	pen.....too many
00804D20	20	6C	69	6E	6B	73	00	00	74	6F	6F	20	6D	61	6E	79	links...too many
00804D30	20	73	79	6D	62	6F	6C	69	63	20	6C	69	6E	6B	20	6C	symbolic link l
00804D40	65	76	65	6C	73	00	00	00	76	61	6C	75	65	20	74	6F	evels...value to
00804D50	6F	20	6C	61	72	67	65	00	77	72	6F	6E	67	20	70	72	o large.wrong pr

V notebooku je nájdený záznam o pripojení neznámeho USB zariadenia. V tomto obrázku je zobrazená analýza operačnej pamäte (RAM) v hexadecimálnom editore HxD. Cieľom bolo vyhľadať kľúčové slová súvisiace s vyšetrovaným prípadom.

Dôkaz 003 (Video záznam dodaný bezpečnostným tímom) – analýza

Záznam z interného kamerového systému spoločnosti DataSecure zachytáva osobu vstupujúcu do kancelárie v nočných hodinách. Miestnosť je slabo osvetlená, no kamera jasne zaznamenáva tvár osoby v momente, keď sa otáča smerom ku dverám. Postava nemá prekrytú tvár a na zázname je možné jednoznačne identifikovať jej fyzické črty. Video zaznamenáva, ako dotyčný otvára dvere a vstupuje do kancelárie, kde neskôr došlo k pripojeniu neautorizovaného USB zariadenia.

Video poskytuje presný čas a vizuálny dôkaz o prítomnosti konkrétnej osoby v čase a na mieste incidentu. Jasná identifikácia tváre umožnila overiť totožnosť páchateľa a spojiť fyzickú prítomnosť s digitálnymi dôkazmi z USB zariadenia a notebooku

Záver forenznnej analýzy

Digitálna forenzná analýza v prípade podozrenia z neautorizovaného prenosu dát v spoločnosti DataSecure potvrdila, že k úniku citlivých informácií skutočne došlo. Na základe dôkazov z USB zariadenia, firemného notebooku a záznamu z kamerového systému sa podarilo jednoznačne identifikovať páchatel'a – zamestnanca spoločnosti **Marek Varga**, ktorý v čase incidentu neoprávnene manipuloval so systémom.

Vyhodnotenie hypotéz:

1. **USB zariadenie bolo použité na exfiltráciu dát – POTVRDENÉ**
→ Forenzná analýza odhalila skopírované súbory z firemného notebooku, vrátane metadát a záznamov o ich prenose.
2. **USB obsahovalo škodlivý kód na manipuláciu s dátami – POTVRDENÉ**
→ Na zariadení boli identifikované spustiteľné skripty, ktoré vymazávali súbory a narúšali systémové záznamy, čím mali zakryť stopy po činnosti páchatel'a.
3. **Firemný notebook bol kompromitovaný fyzickým prístupom – POTVRDENÉ**
→ Záznamy o prihlásení a fyzický prístup k zariadeniu v kombinácii s kamerovým záznamom dokazujú, že Marek Varga mal v daný čas prístup k notebooku, pričom využil administrátorské oprávnenia.
4. **Externejši osobe bolo umožnené vykonať analýzu a manipuláciu s dátami na firemnom zariadení - NEPOTVRDENÉ**

Zhrnutie:

Na videozázname z kamerového systému je jasne viditeľný Marek Varga vchádzajúci do kancelárie v nočných hodinách. Jeho totožnosť bola potvrdená podľa tvárových črt a časovej zhody s digitálnymi záznamami. Spolu s dôkazmi zo zaisteného USB kľúča a systémového logovania notebooku možno s istotou potvrdiť jeho zodpovednosť za incident.

Zistenia tejto analýzy poskytujú komplexný pohľad na spôsob útoku, použité nástroje aj slabiny v zabezpečení systému. Výsledky sú dostatočne presvedčivé pre ďalšie právne alebo interné kroky a zároveň slúžia ako podklad pre návrh preventívnych opatrení na zamedzenie podobných incidentov v budúcnosti.

Odborné články:

Miesto činu 2019

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

Digitálna forenzná analýza

Odkaz: <https://unibook.upjs.sk/img/cms/2020/pf/digitalna-forenzna-analyza-1.pdf>