

Zrada vo FastFoode

Vyšetrovanie vedie: Roman Slezák

[prezentácia](#)

Popis prípadu:

V spoločnosti McLoland, v monitorovacom centre zaregistrovali incident že sa niekto pokúsil skopírovať dáta tajného receptu na USB zariadenie, čo nemôže nastať nakoľko zamestnanci pracujú s receptami napriamo na ich pracovných staniciach. Na to zareagovalo centrum bezpečnosti a začalo vyšetrovanie či došlo k úniku citlivých informácii alebo sa jednalo o falošný poplach. INC-0003213324

Predmet vyšetrovania:

Preskúvanie systémových logov

- ✓ Preverenie systémových udalostí a záznamov s cieľom detekovať pripojenie externých zariadení, ako sú USB kľúče alebo externe harddisky.
- ✓ Hľadanie časových údajov o momentoch pripojenia a odpojenia týchto zariadení.

Analýza pamäťových artefaktov

- ✓ Hľadanie dôkazov o použití nástrojov alebo skriptov na nelegálny prenos dát z počítača.
- ✓ Preverenie RAM pamäte na identifikovanie neautorizovaných operácií.

Záznam z kamier a identifikácia osôb pri počítači

- ✓ Preverenie záznamov z kamier v okolí počítača, aby sa identifikovalo, kto bol v danom čase prítomný pri počítači.
- ✓ Porovnanie časov z kamier s časovými pečiatkami zo systémových logov a pripojení USB zariadení, aby sa určila osoba, ktorá vykonala dané aktivity.

5WH

Kto (Who): Zamestnanec McLoland pracujúci v oddelení vývoja nových produktov pravdepodobne stiahol tajný recept na usb zariadenie.

Čo (What): Krádež a prenos tajných receptov a obchodných stratégií McLoland na USB zariadenie. Podozrenie na predaj konkurencii.

Kedy (When): Presný čas úniku údajov môžeme určiť analýzou systémových logov, registru systému a kamerových záznamov, čím vytvoríme časovú os aktivít.

Kde (Where): V laboratóriu McLoland na oddelení „vývoj nových produktov“.

Prečo (Why): Motívom úniku údajov môže byť túžba po finančnej odmene, osobné konflikty, zámer poškodiť firmu alebo slabé bezpečnostné opatrenia, ktoré umožnili prístup k citlivým informáciám

Ako (How): Únik údajov pravdepodobne prebehol pripojením USB zariadenia k firemnému počítaču, kopírovaním dát a ich následným prenesením. Cieľom vyšetrovania je získať dôkazy o neoprávnenom

prenose údajov, identifikovať zodpovednú osobu a navrhnúť opatrenia na zlepšenie bezpečnosti, aby sa zabránilo podobným incidentom v budúcnosti.

Hypotézy

Hypotéza 1: Únik údajov zo strany interného zamestnanca

Zamestnanec, ktorý mal prístup k citlivým informáciám, mohol úmyselne preniesť dáta na USB zariadenie s cieľom ich zneužiť alebo predať.

Overovacia metóda: Rozhovor so zamestnancom, preverenie prístupových práv a analýza histórie prístupov.

Hypotéza 2: Neoprávnený prístup externou osobou

Externá osoba, ako napríklad návštevník alebo dodávateľ, mohla získať fyzický prístup k počítaču a skopírovať údaje bez vedomia zamestnanca.

Overovacia metóda: Skontrolovanie kamerových záznamov a prístupových logov budovy, aby sa potvrdil prístup neautorizovaných osôb.

Hypotéza 3: Malvér na USB zariadení

USB zariadenie mohlo obsahovať škodlivý softvér, ktorý bez vedomia používateľa automaticky kopíroval údaje na iné miesto.

Overovacia metóda: Skúmanie USB zariadenia na prítomnosť malvéru a kontrola prítomnosti autorun súborov.

Hypotéza 4: Neúmyselný prenos údajov

Zamestnanec mohol pri bežnej práci neúmyselne preniesť citlivé informácie na USB zariadenie, a ani si neuvedomil ich citlivosť.

Overovacia metóda: Preskúmanie pracovných postupov pri manipulácii s USB zariadeniami a rozhovory s príslušnými zamestnancami.

Cieľ vyšetrovania:

Identifikovať zdroj a príčinu neoprávneného prenosu tajných receptov a obchodných stratégií z firemných počítačov McLoland na USB zariadenie, ktorý bol následne odovzdaný FFC.

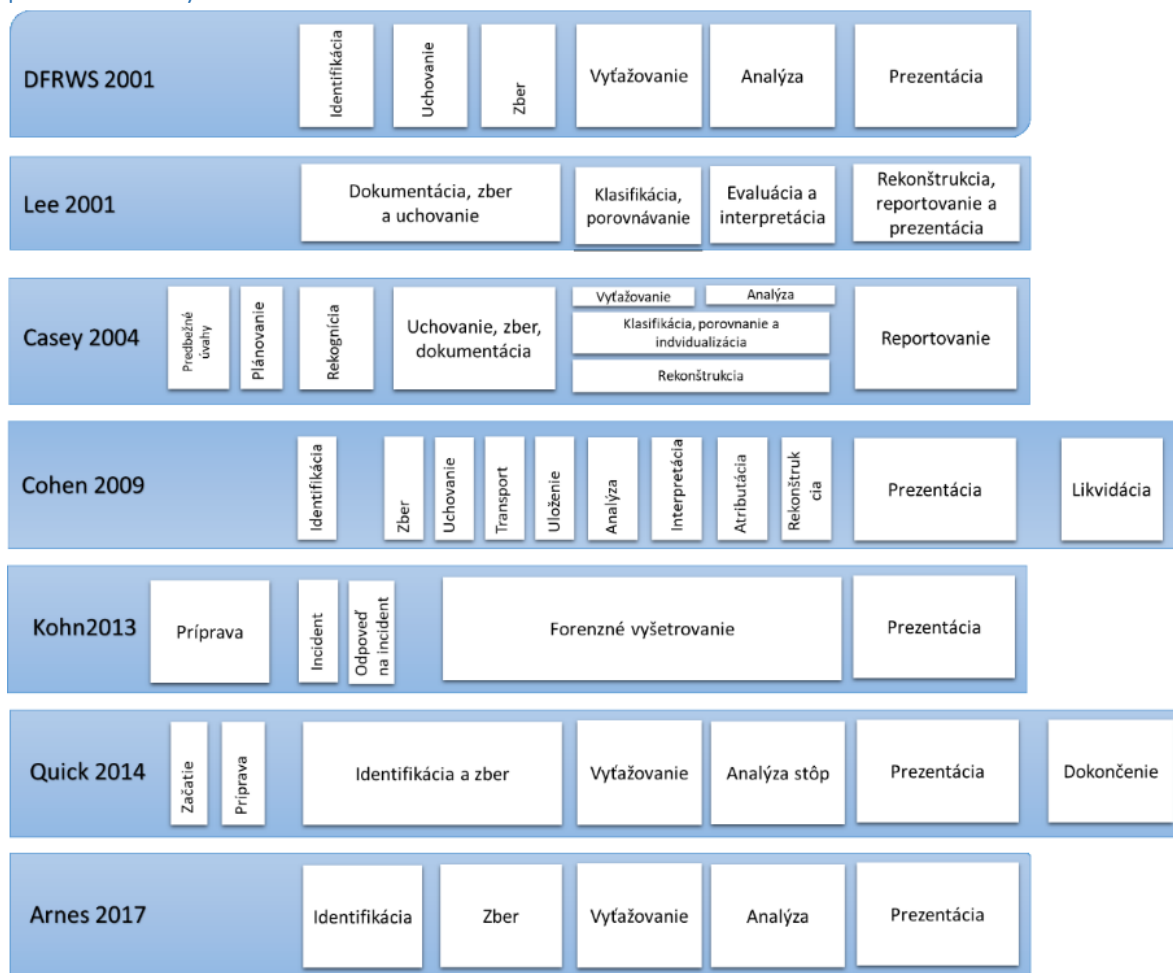
Identifikovať zamestnanca, ktorý je zodpovedný za prenos citlivých informácií z McLoland na USB kľúč a následné odovzдание týchto údajov konkurenčnej spoločnosti FFC.

Zistiť obsah USB zariadenia, ktorý bol použitý na prenos tajných receptov a obchodných stratégií McLoland.

Identifikovať možné citlivé údaje nachádzajúce sa na USB zariadení ktoré sú kľúčové pre konkurencieschopnosť McLoland.

Postup vyšetrovania:

podľa schémy Arnes 2017



1. Identifikácia

Hľadáme cieľ vyšetrovania a určujeme, aké dôkazy sú dôležité.

Identifikujeme zariadenia a materiály, ktoré môžu obsahovať relevantné informácie.

2. Zaisťovanie a zber

Zabezpečíme a prenesieme dôkazy do laboratória.

Vytvoríme kópie dát zo zariadení na ďalšiu analýzu.

3. Vyťažovanie

Prehľadáme dáta a hľadáme podozrivé súbory alebo aktivity, ktoré nám pomôžu nájsť páchateľa.

4. Analýza

Dôkladne analyzujeme dôkazy, rekonštruujeme priebeh incidentu a identifikujeme páchateľa.

5. Prezentácia

Pripravíme správu a predložíme dôkazy.

Príprava dát

Dataset je ztiahnutý z internetu z viacerých zdrojov.

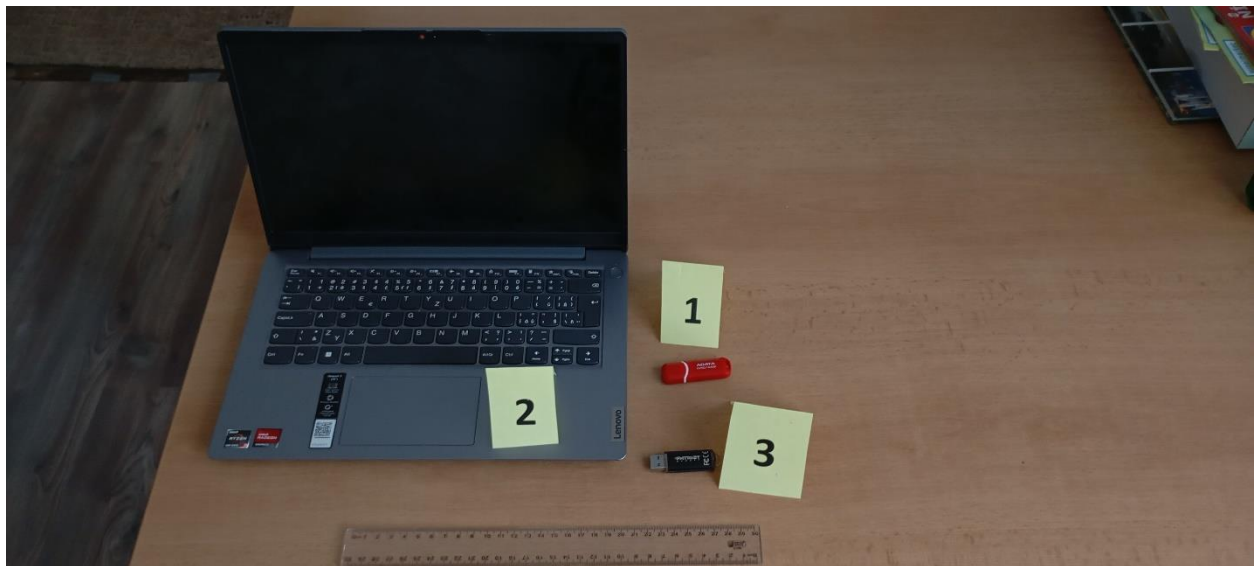
Cca 10tis suborov. Obrázky, emaily, dokumenty, **pridaný subor s receptami McLoland.**

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

emailové konverzácie

cca 150 email adresárov s tisíckami emailov

<https://www.cs.cmu.edu/~enron/>



Zaistenie dokazov:

USB zariadenie 1 aj USB zariadenie 2 bolo pripojené k čítačke USB ktorá len číta aby sa predišlo náhodnému prepisu údajov. Spravili sa 3 pracovné kópie pre analýzu. Z každého zariadenia je záznam o evidencii kde je zapísané kto s týmto zariadením pracoval. Z pracovnej stanice sa urobila kopia zapnutého PC. Manipulácia s dôkazmi je zdokumentovaná v case of custody pre každé zariadenie. História a kto čo robil s dôkazom.

USB klíč s datami:

Prečo: USB kľúč bol nosičom dát, ktorý umožnil prenos citlivých informácií mimo bezpečnostného prostredia firmy. Tieto dáta boli následne poskytnuté konkurenčnej firme FFC, čo predstavuje vážnu hrozbu pre bezpečnosť a konkurencieschopnosť McLoland.

Číslo:	001	Typ:	USB kluc				
Popis prípadu:	hamburger						
Názov súboru:							
Miesto získania digitálnej stopy:	Pracovisko McLoland						
Poznámky:	Červený usb kluc, sn: 575833314133343231313937, ADATA USB Flash Drive USB Device						
Časové pečiatky							
Access:		Modify:		Change:			
1.2.2025 11:32	Robert Kalinak	Zaistenie dokazu					
1.2.2025 13:15	Kurier UPC 15	Prevzatie na prenos					
22.3.2025 10:25	Roman Slezak	Analýza dokazu					
8.4.2025 11:15	Viera Zelienkova	Uloženie do archivu					
Digitálny odtlačok hash	MD5: 6a882e861c18ede426ccf651fcf21a2						
	SHA1: 183baafeb8decd96a6a678ea19951c4ed4de903c						
Časová pečiatka	Akcia vykonaná s digitálnou stopou						
22.3.2025 10:25	Vytvorena kopia usb disku	Roman Slezak					
22.3.2025 12:11	USB zariadenie vrátené do skladu	Roman Slezak					
22.3.2025 15:41	Analýza image USB zariadenia	Roman Slezak					

Pracovní počítač:

Popis: Pracovný počítač, ktorý bol používaný v laboratóriu McLoland. Tento počítač obsahoval prístup k interným serverom a dôverným dokumentom firmy.

Prečo: Pracovný počítač mal priamy prístup k citlivým údajom, ktoré boli neskôr použité na nelegálny prenos informácií. Identifikovanie tohto zariadenia umožňuje vysledovať konkrétne akcie vykonávané na počítači, ako aj určiť čas a dátum prenosu dát.

Číslo:	002	Typ:	Počítač				
Popis prípadu:	hamburger						
Názov súboru:	recept_mclonald2.txt						
Miesto získania digitálnej stopy:	Pracovisko McLoland						
Poznámky:	Počítač zapnutý, urobený image RAM						
Časové pečiatky							
Access:		Modify:	1.1.2025	Change:			
1.2.2025 11:32	Robert Kalinak	Zaistenie dokazu					
1.2.2025 13:15	Kurier UPC 15	Prevzatie na prenos					
22.3.2025 11:25	Roman Slezak	Analýza dokazu					
8.4.2025 14:15	Viera Zelienkova	Uloženie do archivu					
Digitálny odtlačok hash	MD5: f5d2b3a0ac467f7fa1ff3b428d8d7f4b						
	SHA1: ce2e4d97fd76efed6fcb8275e8f8f24f3c9f7c9a						
Časová pečiatka	Akcia vykonaná s digitálnou stopou						
1.2.2025 11:32	Robert Kalinak	Vytvorenie image pamate RAM PC					
22.3.2025 15:41	Analyza image PC	Roman Slezak					

Popis: Kamerový server je kľúčový nástroj pri vyšetrovaní úniku dát, pretože umožňuje identifikovať osoby, ktoré mali prístup k citlivým informáciám v danom čase a prostredí.

Prečo: Spolu s informáciami o USB kľúči a pracovnom počítači môže kamerový server pomôcť vytvoriť celkový obraz o tom, ako a kedy došlo k úniku dát, a aké zariadenia a osoby sú zapojené.

Číslo:	003	Typ súboru:	bvr	Obnovený súbor:	nie	Veľkosť:	1,41 MB (1 486 848 bytes)
Popis prípadu:	hamburger						
Názov súboru:	Ofiice22.01012025_194947.bvr						
Miesto získania digitálnej stopy:	Serverovna McLoland						
Poznámky:	Prijate od SBS pracovníkov na usb kluci						
Časové pečiatky							
Access:		Modify:		Change:			
1.2.2025 11:32	Robert Kalinak	prijatie dokazu					
Digitálny odtlačok hash	MD5:f5d2b3a0ac467f7fa1ff3b428d8d7f4b						
	SHA1: ce2e4d97fd76efed6fsb8275ess8f2413c9f739a						
Časová pečiatka	Akcia vykonaná s digitálnou stopou						
22.3.2025 15:41	Analyza video zaznamu	Roman Slezak					

Dokaz 001 (usb disk) - analýza

Výrobca: ADATA UV150 64GB

Sériové číslo: 575833314133343231313937

Kapacita úložiska: 64 GB

Rozhranie: USB 3.2 Gen 1 (USB 3.0)

Konektor: USB-A

Rýchlosť čítania: 90 MB/s

Materiál: Plast

Farba: Červená



Test rýchlosti zápisu a čítania USB programom CrystalDiskMark 8

CrystalDiskMark 8.0.6 x64 [Admin]					
Súbor Nastavenia Profile Vzhľad Nápoveda Language					
All	1	16MiB	D: 6% (4/59GiB)	MB/s	
	Read (MB/s)		Write (MB/s)		
SEQ1M Q8T1		28.91		28.10	
SEQ1M Q1T1		29.11		28.72	
RND4K Q32T1		10.77		2.04	
RND4K Q1T1		9.95		1.70	

Screenshot usb vysledku kopie kluca cez Magnet forensics

Drive/Image Verify Results	
Name	usb-kluc-cerveny.001
Sector count	123699200
MD5 Hash	
Computed hash	86a882e861c18ede426ccf651fcf21a2
Report Hash	86a882e861c18ede426ccf651fcf21a2
Verify result	Match
SHA1 Hash	
Computed hash	183baafeb8decd96a6a678ea19951c4ed4de903c
Report Hash	183baafeb8decd96a6a678ea19951c4ed4de903c
Verify result	Match
Bad Blocks List	
Bad block(s) in image	No bad blocks found in image

Unique description: cerveny usb kluc adata

Examiner: Roman Slezak

Notes: 64gb usb kluc

Information for C:\temp\usb kluc dump\usb-kluc-cerveny:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 7 699

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 123 699 200

[Physical Drive Information]

Drive Model: ADATA USB Flash Drive USB Device

Drive Serial Number: 0000000005

Drive Interface Type: USB

Removable drive: True

Source data size: 60400 MB

Sector count: 123699200

[Computed Hashes]

MD5 checksum: 86a882e861c18ede426ccf651fcf21a2

SHA1 checksum: 183baafeb8decd96a6a678ea19951c4ed4de903c

Image Information:

Acquisition started: Sat Mar 22 10:25:00 2025

Acquisition finished: Sat Mar 22 10:32:25 2025

Segment list:

C:\temp\usb kluc dump\usb-kluc-cerveny.001

Image Verification Results:

Verification started: Sat Mar 22 10:32:26 2025

Verification finished: Sat Mar 22 10:34:59 2025

MD5 checksum: 86a882e861c18ede426ccf651fcf21a2 : verified

SHA1 checksum: 183baafeb8dec96a6a678ea19951c4ed4de903c : verified

Záver: Image bol analyzovaný programom autopsy. Bol nájdený súbor ktorý obsahoval súbor s receptami. Súbor má názov recept_mclonald2.txt

The screenshot shows the Autopsy 4.22.0 interface. The left sidebar contains a tree view with categories like Data Sources, File Views, File Types, Deleted Files, MB File Size, Data Artifacts, Analysis Results, Extension Mismatch Detected, Keyword Hits, OS Accounts, Tags, Score, and Reports. The main window displays a 'Keyword search' table with columns: Name, Keyword Preview, Location, Modified Time, Change Time, Access Time, Created Time, Size, Flags(Dir), and Flags(Meta). A single result is shown for '001830.txt' with the keyword '200203011800200203011700big mac' and location '/img_data-usb-cerveny.001/vol_002/001830.txt'. Below the table, the 'Strings' tab is active, showing a list of extracted text strings. A search bar at the top right of the strings list shows the query '200203011800200203011700big MAC' with 1 match. The search results list includes various hex and text strings, with the first match being '200203011800200203011700big MAC'.

Name	Keyword Preview	Location	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)
001830.txt	200203011800200203011700big mac	374183 /img_data-usb-cerveny.001/vol_002/001830.txt	2009-03-05 18:29:06 SEC	0000-00-00 00:00:00	2025-03-21 05:00:00 SEC	2025-03-21 12:18:59 SEC	1341360	Allocated	Allocated

Strings: Extracted Text

Page: 41 of 45 Page 100% Reset

Matches on page: 1 of 1 Match

Text Source: Search Results

200203011800200203011700big MAC

Dokaz 002 (laptop) – analýza

IdeaPad 3 14ALC6 Arctic Grey

AMD Ryzen 3 5300U, 14" TN antireflexný 1920 × 1080, RAM 4 GB DDR4, AMD Radeon Graphics, SSD 128 GB, webkamera, USB 3.2 Gen 1, USB-C, WiFi 5, Bluetooth, hmotnosť 1,41 kg, Windows 10 S

Analýza pomocou software HxD nasla v pamati ze sa v osobe pravdepodobne pohlo svedomie

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F Decoded text

00E2D6D30 10 DC C6 9F 30 02 00 00 E5 E5 E5 E5 E5 E5 E5 E5 .0c20...iiiiiii

00E2D6D40 01 00 00 00 0E 00 00 00 6F 00 70 00 74 00 69 00o.p.t.i.

00E2D6D50 6F 00 6E 00 00 00 E5 E5 E5 E5 E5 E5 E5 E5 o.n...iiiiiii

00E2D6D60 01 00 00 00 0E 00 00 00 6F 00 70 00 74 00 69 00o.p.t.i.

00E2D6D70 6F 00 6E 00 00 00 E5 E5 E5 E5 E5 E5 E5 E5 o.n...iiiiiii

00E2D6D80 01 00 00 00 0E 00 00 00 6F 00 70 00 74 00 69 00o.p.t.i.

00E2D6D90 6F 00 6E 00 00 00 E5 E5 E5 E5 E5 E5 E5 E5 o.n...iiiiiii

00E2D6DA0 01 00 00 00 0E 00 00 00 62 00 75 00 74 00 74 00b.u.t.t.

00E2D6DB0 6F 00 6E 00 00 00 E5 E5 E5 E5 E5 E5 E5 E5 o.n...iiiiiii

00E2D6DC0 01 00 00 00 0A 00 00 00 6D 00 65 00 6E 00 75 00m.e.n.u.

00E2D6DD0 00 00 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 .iiiiiiiiiiiiiiii

00E2D6DE0 01 00 00 00 0E 00 00 00 73 00 65 00 61 00 72 00s.e.a.r.

00E2D6DF0 63 00 68 00 00 00 E5 E5 E5 E5 E5 E5 E5 E5 c.h...iiiiiii

00E2D6E00 19 00 00 00 D1 DB 35 79 02 00 00 00 00 00 00 00 ...NÜsy.....

00E2D6E10 40 36 01 AC 30 02 00 00 E5 E5 E5 E5 E5 E5 E5 E5 @e-0...iiiiiii

00E2D6E20 63 6F 20 68 72 6F 7A 69 20 7A 61 20 75 6E 69 6B co hrozi za unik

00E2D6E30 20 64 61 74 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 detiiiiiiiiiiii

00E2D6E40 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 .iiiiiiiiiiiiiiii

00E2D6E50 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 .iiiiiiiiiiiiiiii

00E2D6E60 01 00 00 00 12 00 00 00 74 00 6F 00 70 00 5F 00t.o.p..

00E2D6E70 73 00 69 00 74 00 65 00 00 00 E5 E5 E5 E5 E5 E5 E5 E5 s.i.t.e...iiiiiii

00E2D6E80 1F 00 00 00 EB B6 9D C3 02 00 00 00 00 00 00 00 ...e.t.a.....

00E2D6E90 40 52 4A A8 30 02 00 00 E5 E5 E5 E5 E5 E5 E5 E5 BRJ 0...iiiiiii

00E2D6EA0 19 00 00 00 51 B6 45 78 02 00 00 00 00 00 00 00 ...QEX.....

00E2D6EB0 C0 31 01 AC 30 02 00 00 E5 E5 E5 E5 E5 E5 E5 E5 R1.-0...iiiiiii

00E2D6EC0 E0 5E BC D2 FC 7F 00 00 20 BB 07 A1 30 02 00 00 ...t.Ng...»..0...

00E2D6ED0 01 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 E5 .iiiiiiiiiiiiiiii

00E2D6EE0 1F 00 00 00 D8 1A E3 0C 02 00 00 00 00 00 00 00 ...R.a.....

00E2D6EF0 D0 2D 0B AA 30 02 00 00 E5 E5 E5 E5 E5 E5 E5 E5 B--g0...iiiiiii

00E2D6F00 61 6B 6F 20 75 6B 72 61 64 6E 75 74 20 7A 65 6C ako ukradnut zel

00E2D6F10 65 6E 75 20 6F 63 74 61 76 69 75 20 33 E5 E5 E5 enu octavia 3iii

00E2D6F20 E0 FB BD D2 FC 7F 00 00 00 E5 E5 E5 E5 E5 E5 E5 E5 zü"Nu.....

00E2D6F30 03 00 00 00 00 00 00 00 E5 E5 E5 E5 E5 E5 E5 E5iiiiiii

00E2D6F40 01 00 00 00 00 00 00 00 E5 E5 E5 E5 E5 E5 E5 E5iiiiiii

Results

Checksum Search (0 hits)

Offset Excerpt (hex) Excerpt (text)

Offset(h): E2D6E20 Block(h): E2D6E20-E2D6E33 Length(h): 14 Overwrite

Pomocou software USBDeview analyzujeme logy pripojených zariadení

Device Name	Description	Device Type	Connected	Safe To Unplug	Disabled	USB Hub	Drive Letter	Serial Number	Registry Time 1
ADATA USB Flash Drive	ADATA USB Flash Drive USB Device	Mass Storage	Yes	Yes	No	No	D:	29724506	1.1.2025 18:19

Záver: v pracovnom počítači je nájdený záznam o pripojení USB zariadenia

Dokaz 003 (USB disk dodaný SBS teamom) - analýza



Záver: Zo záznamu kamery vidno kto sedel pri PC v čase incidentu

Hypotézy- POTVRDENIE

Hypotéza 1: Únik údajov zo strany interného zamestnanca (POTVRDENE)

Zamestnanec skopíroval súbor s receptami na USB zariadenie. Incident potvrdzujú logy so serveru, logy z pracovnej stanice a záznam z kamery. Všetky dôkazy sa posúvajú polícii na došetrenie.

Hypotéza 2: Neoprávnený prístup externou osobou - NEPOTVRDENE

Hypotéza 3: Malvér na USB zariadení - NEPOTVRDENE

Hypotéza 4: Neúmyselný prenos údajov - NEPOTVRDENE

Literatúra - odborné príspevky k prípadu

Miesto činu 2019

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

Stručný popis: V poradí už siedmy ročník odbornej policajnej súťaže Miesto činu 2019 sa uskutočnil 5. a 6. septembra 2019 v priestoroch Centra výcviku Lešť. *„Organizátori pripravili pre trinásť súťažných trojčlenných tímov identické súťažné stanovišťa, kde si jednotlivé tímy zmerali sily vo vysoko odbornej činnosti pri dokumentovaní namodelovaného trestného činu.*

Digitálna forenzná analýza

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

Stručný popis: Dokument poskytuje prehľad o digitálnej forenznej analýze, vrátane rozdielov medzi riešením kybernetických bezpečnostných incidentov a vyšetrovaním počítačovej kriminality.

Trestno-právne aspekty počítačovej bezpečnosti

Odkaz: https://www.researchgate.net/publication/281550242_Trestno-pravne_aspekty_pocitacovej_bezpecnosti

Stručný popis: Tento článok sa zameriava na trestno-právne aspekty počítačovej bezpečnosti, vrátane rozdielov medzi počítačovou kriminalitou a tradičnou kriminalitou.