

Vniknutie do budovy firmy a možné odcudzenie dát a patentov

Saša Lukačovičová

Prezentacia

Prípado

Nová technologická spoločnosť, ktorá vyvíja prelomové patenty v oblasti technologických zariadení, sa stala obeťou možného úniku citlivých dát. Neznáme osoby pravdepodobne prenikli do budovy spoločnosti a mohli získať prístup k pracovným staniciam. Spoločnosť na incident prišla až po tom, ako zamestnanec prišiel ráno do kancelárie

Jediné dôkazy, ktoré boli nájdené a sú podozrivé:

- USB kľúč nájdený v blízkosti vchodových dverí do budovy
Pevný disk pripojený k vypnutému a čiastočne poškodenému počítaču

Použité nástroje:

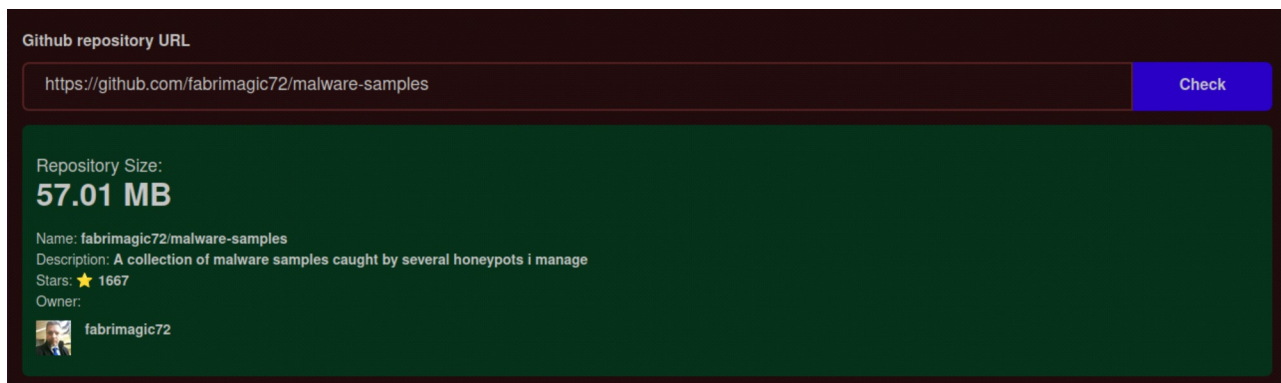
FTK Imager 3.1.1 - použitý na vytvorenie kópii diskov, ako aj vytvorenie obrazu RAM pamäte

Autopsy 4.23.1 – použitý na analyzovanie obrazu diskov

HxD 2.5.0.0 – použitý na analýzu obrazu RAM pamäte

Datasey sú použité z internetu,

USB: <https://github.com/fabrimagic72/malware-samples/>



Disk:

<https://patents.google.com>, <https://perchance.org/patent>, použitých 5 patentov, približne 8 MB

- patenty sú exkluzívne v PDF formáte

<https://corp.digitalcorpora.org/corpora/files/govdocs1/zipfiles/> prvých 5 zip súborov, dokopy 5933 suborov,

- mix súborov ako pdf, pptx, png, txt.....

Hypotézy

Hypotéza 1:

Útočník mal fyzický prístup k budove a použil USB kľúč na zahľadanie stôp po exfiltrácii dát alebo na prenos citlivých súborov mimo spoločnosti.

Hypotéza 2:

USB kľúč mohol slúžiť ako prenosné úložisko na dočasné uloženie odcudzených dát, ktoré boli následne prenesené na iné zariadenie mimo priestorov spoločnosti.

Hypotéza 3:

Externý pevný disk bol použitý na neautorizované kopírovanie dát, ktoré mali byť následne fyzicky odcudzené bez potreby online exfiltrácie.

5WH

- **Čo (What):**
- **Čo útočník spravil, prípadne čo sa mu podarilo odcudziť**
- Možné odpovede:
 - Je možné že útočník použil disk nechaný na mieste činu na kopírovanie citlivých údajov z pracovnej stanice, ale keďže bol disk na mieste činu ponechaný, môžeme logicky dedukovať že útočník bol v akte kradnutia údajov vyrušený.
- **Kto (Who):**
 - **Kto mal prístup k budove a zariadeniam spoločnosti?**
 - Možné odpovede:
 - Neznámy útočník, ktorý získal fyzický prístup.
 - Zamestnanci spoločnosti s administrátorskými právami.
 - Osoba s internými kontakty alebo niekto, kto mal prístup cez spoluprácu s firmou.
- **Kde (Where):**
 - **Kde bol nájdený USB kľúč a pevný disk?**
 - Možné odpovede:
 - USB kľúč bol nájdený v blízkosti vchodových dverí do budovy.
 - Pevný disk bol pripojený k poškodenej pracovnej stanici v kancelárii.
- **Prečo (Why):**
 - **Prečo bol externý disk zapojený do počítača ktorý bol poškodený?** Možné odpovede:
 - Útočník sa pokúsil exfiltrovať citlivé dáta, ale mohol byť vyrušený, čo by zodpovedalo ponechanému disku a vypadnutému usb kľúču.
 - Pevný disk mohol byť použitý na lokálne kopírovanie dát na neskoršie exfiltrácie.
- **Kedy (When):**
 - **Kedy sa incident odohral?**
 - Možné odpovede:
 - Pred niekoľkými hodinami, nakoľko incident bol objavený z pondelka na utorok mimo

pracovných hodín.

- **Ako (How):**
- **Ako útočník prenikol do systému a získal prístup k dátam?**
- Možné odpovede:
- Fyzický prístup k zariadeniam v budove a vloženie USB kľúča, ktorý spustil skript na exfiltráciu dát.
- Zneužitie nedostatočného zabezpečenia na pracovnej stanici.

Ciele vyšetrovania

Ciele vyšetrovania zahŕňajú identifikáciu spôsobu, akým mohlo dôjsť k exfiltrácii alebo kompromitácii citlivých dát technologickej spoločnosti. Hlavné úlohy vyšetrovania sú preverenie, či bol USB kľúč použitý na prenos dát alebo zavedenie škodlivého softvéru. Bezpečnostné opatrenia pri vyšetrovaní zahŕňajú dôkladné zaistenie zariadení a vytvorenie troch kópií forenzných obrazov úložných médií. Originálny dôkazový materiál sa uchováva v nezmenenej podobe, zatiaľ čo prvá kópia slúži na analýzu, druhá ako záložná verzia pre prípad poškodenia primárnej kópie a tretia na dlhodobú archiváciu. Forenzné snímky sa vytvárajú s overením kontrolných súčtov (MD5, SHA1) na zabezpečenie integrity údajov. Okrem toho sa izolujú kompromitované zariadenia od siete, aby sa zabránilo ďalšej kontaminácii alebo nežiaducim úpravám dát.

Bezpečnostné opatrenia

Po zistení incidentu sme okamžite fyzicky zabezpečili všetky relevantné zariadenia a miesto činu. Prvým krokom bolo uzavretie kancelárie, kde boli nájdené dôkazy, aby sa zabránilo neoprávnenému prístupu. Zariadenia sme ponechali v ich pôvodnom stave a nedotýkali sa ich, kým sme nemali pripravené forenzné postupy.

USB kľúč sme zaistili použitím antistatických rukavíc a okamžite sme ho umiestnili do forenzného obalu na ochranu pred akoukoľvek manipuláciou. Pevný disk, ktorý bol stále pripojený k zapnutému počítaču, sme najprv zdokumentovali fotografiami a až potom bezpečne odpojili. Dôležité bolo zabezpečiť, aby sme zariadenia neaktivovali a neprepojili k žiadnemu inému systému, čím by sa mohli zmeniť dáta.

Po presunu zaistených zariadení do laboratória sme vykonali vytvorenie štyroch identických forenzných kópií pomocou špecializovaného hardvérového zariadenia na klonovanie diskov. Originálne úložné médiá sme následne uzamkli do zabezpečeného archívu s prístupom iba pre poverené osoby. Počas celého procesu sme viedli presnú dokumentáciu o každom kroku, zaznamenali sme čas a podmienky zaistenia, aby bola zachovaná integrita dôkazového materiálu.

Zariadenia nájdené na mieste činu

Verbatim Externý SSD Disk

Parameter	Hodnota
Kapacita	240 GB
Rozhranie	USB 3.1
Technológia pripojenia	USB
Značka	Verbatim
Špeciálne vlastnosti	Odolný voči nárazom, robustný
Formát disku	2,5 palca
Typ disku	SSD (Solid State Drive)
Kompatibilné zariadenia	Stolný počítač
Typ inštalácie	Externý pevný disk
Farba	Strieborná
Rýchlosť čítania	až do 500 MB/s
Rýchlosť zápisu	až do 430 MB/s
Rozmery	92 mm × 29 mm × 9 mm
Hmotnosť	29 g
Výkon rozhrania	USB 3.2 Gen 2



SanDisk USB Kľúč

Parameter	Hodnota
Značka	SanDisk
Kapacita úložiska	64 GB
Rozhranie	USB 3.0
Špeciálna vlastnosť	Ľahký dizajn
Kompatibilné zariadenia	Laptop
Rýchlosť čítania	až do 130 MB/s
Spätná kompatibilita	USB 2.0
Bezpečnostné funkcie	Šifrovanie súborov, ochrana heslom



Informácie z FTK imageru:

USB KLUC:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 59680

Heads: 64

Sectors per Track: 32

Bytes per Sector: 512

Sector Count: 122224640

sudo ftkimager /dev/sdX test --case-number 1 --evidence-number 1 --examiner Lukacovicova --compress 0 --verify

AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)

Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042

All rights reserved.

Creating image...

Image creation complete.

Verifying image...

Image verification complete.

[MD5]

Computed hash:

Report hash:

Verify result: Match

[SHA1]

Computed hash:

Report hash:

Verify result: Match

DISK:

AccessData FTK Imager v3.1.1 CLI (Aug 24 2012)

Copyright 2006-2012 AccessData Corp., 384 South 400 West, Lindon, UT 84042

All rights reserved.

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 29185

Heads: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 468862128

Verifying image...

Verify result: Match

Chain of Custody

Císlo:	01	Typ súboru:	raw	Obnovený súbor:		Veľkosť:	8500 MB
Popis prípadu:		Utok na startup					
Názov súboru:		ram-image					
Miesto ziskania digitálnej stopy:		Kancelaria startupu kde doslo ku vniknutí					
Poznámky:		RAM pamat					
Časové pečiatky							
Access:	25/03/10 11:35:03	Modify:	25/03/10 11:35:03	Change:			
Digitálny odlačok (heš)							
MD5	96041fb62e4b251bb1380fa5eac5026						
SHA1	595ec1d128d7d54d029fb6d66761da7ad9e2a0ee						
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
25/03/10 11:40:22		Zistenie MD5 Hashu					
25/03/10 11:40:50		Zistenie SHA1 Hashu					

Typy súborov na ktoré sa budeme zameriavať počas analýzy obrazov diskov

1. Dokumenty a textové súbory

- **.doc, .docx, .odt, .rtf** – textové dokumenty, ktoré môžu obsahovať firemné plány, patenty alebo iné citlivé informácie.
- **.pdf** – často používané na zdieľanie oficiálnych dokumentov a kontraktov.
- **.txt, .csv** – textové alebo tabuľkové súbory s databázovými údajmi alebo exportovanými informáciami.

2. Zdrojové kódy a skripty

- **.py, .js, .c, .cpp, .java, .cs** – programátorské súbory, ktoré môžu obsahovať zdrojový kód firemných aplikácií.
- **.sh, .bat, .ps1** – skripty, ktoré mohli byť použité na automatizáciu exfiltrácie dát alebo na spustenie škodlivého kódu.

3. Databázové súbory

- **.sql, .db, .mdb, .accdb** – databázové súbory, ktoré môžu obsahovať firemné dáta, zákaznicke informácie alebo obchodné tajomstvá.

4. Archívy a komprimované súbory

- **.zip, .rar, .7z, .tar.gz** – balíčky súborov, ktoré mohli byť vytvorené na rýchly prenos veľkého množstva dát.
- **.iso** – obrazy diskov, ktoré môžu obsahovať zálohy alebo skopírované údaje.

5. Multimediálne súbory

- **.jpg, .png, .bmp, .gif** – obrázky, ktoré môžu obsahovať snímky obrazovky alebo sfotené dokumenty.
- **.mp4, .avi, .mov** – video súbory, ktoré môžu obsahovať zaznamenané informácie z kamerového systému.
- **.wav, .mp3** – zvukové súbory, ktoré mohli byť použité na záznam hlasovej komunikácie.

6. Spustiteľné a škodlivé súbory

- **.exe, .dll, .sys** – spustiteľné súbory, ktoré mohli byť použité na vzdialený prístup alebo škodlivé aktivity.
- **.bin, .img** – binárne súbory, ktoré môžu obsahovať firmvérové alebo systémové dáta.
- **.vbs, .js, .wsf** – skripty v systéme Windows, ktoré mohli byť využité na automatizáciu exfiltrácie dát.

7. Logy a systémové súbory

- **.log** – systémové a aplikácie logy, ktoré môžu ukázať časovú os prístupu k súborom.
- **.evtx** – Windows Event Log, ktorý zaznamenáva dôležité udalosti v systéme.
- **.ini, .conf, .cfg, .json, .xml, .plist** – konfiguračné súbory, ktoré môžu obsahovať informácie o sieťových pripojeniach, prístupových právach alebo škodlivých konfiguráciách.

Tieto typy súborov budeme analyzovať na známky neoprávnenej manipulácie, prenosu citlivých dát alebo zavedenia škodlivého softvéru.

Hypotéza 1: Útočník použil USB na získanie prístupu k systému a exfiltráciu dát

Postup vyšetrovania:

- Forenzná analýza USB kľúča
- Skontrolujeme obsah USB, či obsahuje súbory s citlivými údajmi alebo exekučné skripty.
- Zistíme, či sú na USB prítomné skryté súbory, šifrované dáta alebo fragmenty neúplne vymazaných údajov.

Hypotéza 2: USB kľúč bol použitý ako prenosné médium na dočasné uloženie a presun odcudzených dát

Postup vyšetrovania:

- Analýza USB kľúča
- Skontrolujeme prítomnosť veľkých archívov, šifrovaných kontajnerov alebo komprimovaných súborov (.zip, .rar, .7z).
- Preskúmame názvy adresárov a štruktúru súborov, či korešpondujú s internými firemnými dátami alebo projektmi spoločnosti.

Hypotéza 3: Pevný disk bol použitý na neautorizované kopírovanie dát

Postup vyšetrovania:

- Forenzná analýza pevného disku
- Vytvoríme bitovú kópiu disku a vykonáme analýzu zmien.
- Skontrolujeme časové značky súborov (MAC – Modified, Accessed, Created), aby sme zistili, ktoré dáta boli nedávno presunuté alebo upravené.
- Použijeme softvér na obnovu súborov, aby sme preverili, či neboli niektoré dáta vymazané po kopírovaní.
- Identifikácia nedávnych operácií
- Skontrolujeme nedávne prístupy k veľkým súborom, ktoré môžu naznačovať kopírovanie citlivých údajov.
- Vyhľadáme stopy po použití externých médií, ak existujú dočasné logy o manipulácii s diskom.

Listing: /img_usb.001/Generic Trojan

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[parent folder]				2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	2026-05-12 07:58:23 PDT	2026-05-12 04:14:47 PDT	56	Allocated	Allocated	unknown	/img_usb.001/Generic
[parent folder]				2026-05-12 13:41:28 PDT	2026-05-12 13:41:28 PDT	2026-05-12 07:58:23 PDT	2026-05-12 04:00:16 PDT	56	Allocated	Allocated	unknown	/img_usb.001/Generic
1499792134116cac20f7c9c1a26e1521b00073aff05d4c0967046e9523b13a.zip	1	0	0	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	18942	Allocated	Allocated	unknown	/img_usb.001/Generic
5b2ae33001c084222ebf931b8235e0cc786c8e3e	1	0	0	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	68235	Allocated	Allocated	unknown	/img_usb.001/Generic
79ba6b16239f14616642ba438f78a9.zip	1	0	0	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	33295	Allocated	Allocated	unknown	/img_usb.001/Generic
1c7995d6116af9f0cc3c1ae69047e1cc0bfcac01464b2c	1	0	0	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	66240	Allocated	Allocated	unknown	/img_usb.001/Generic
smb-1b_cy5.7z	1	0	0	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	87962	Allocated	Allocated	unknown	/img_usb.001/Generic
smb-k_h777.zip	1	0	0	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	53648	Allocated	Allocated	unknown	/img_usb.001/Generic
smb-ufd87p.zip	1	0	0	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	2026-05-12 04:14:27 PDT	2026-05-12 04:14:47 PDT	12963	Allocated	Allocated	unknown	/img_usb.001/Generic

Item: 1499792134116cac20f7c9c1a26e1521b00073aff05d4c0967046e9523b13a.zip
Aggregate Score: Notable

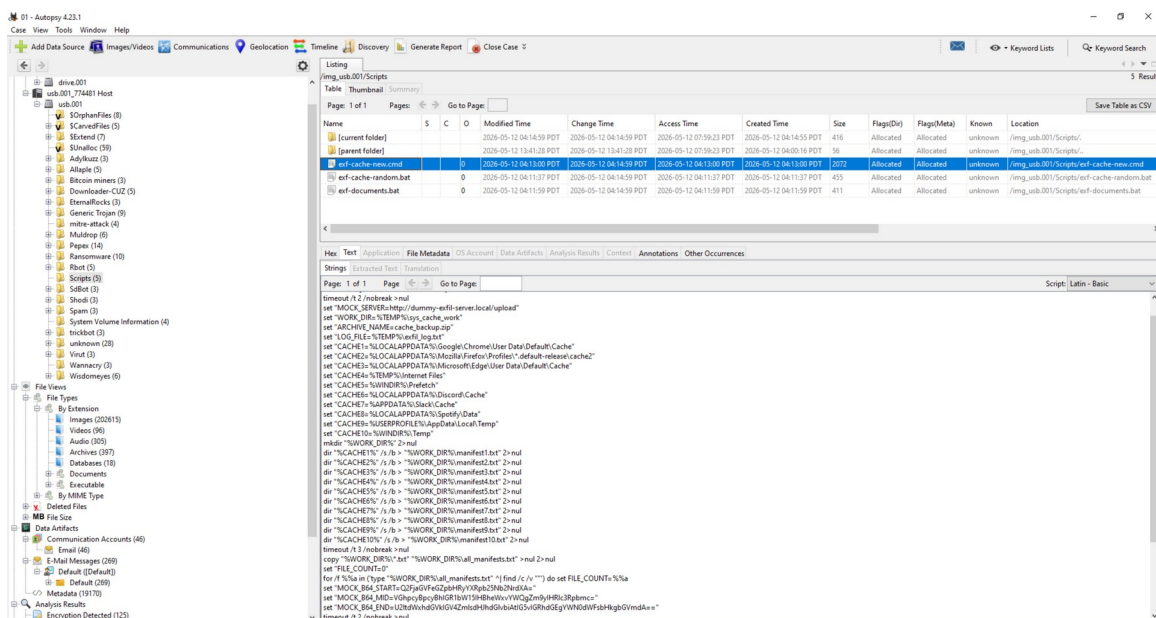
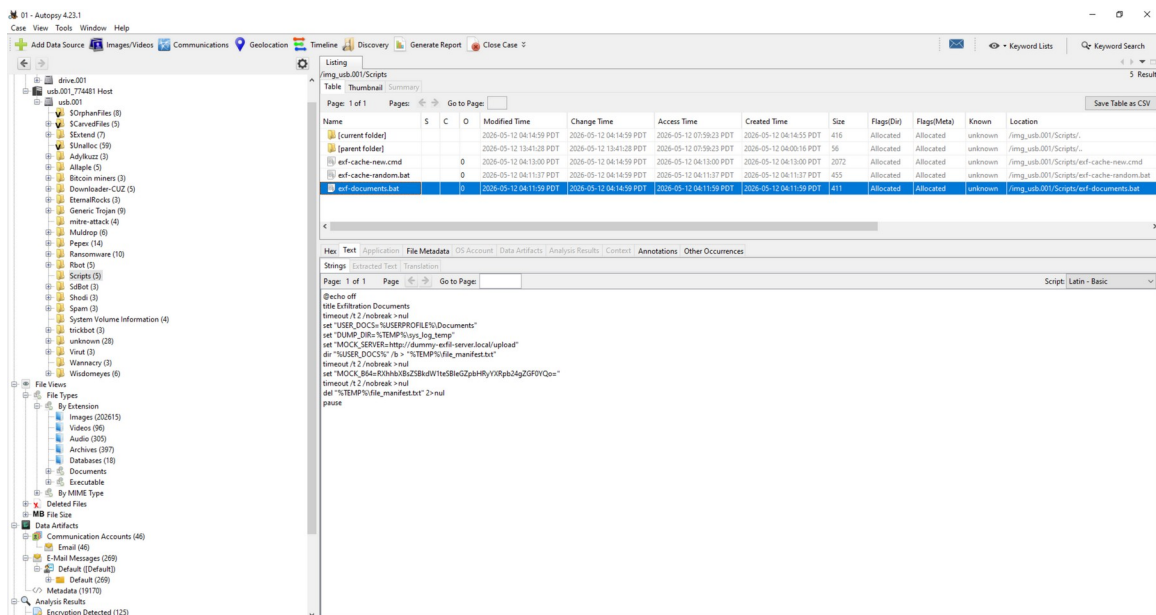
Analysis Result 1

Score: Notable
Type: Encryption Detected
Configuration:
Conclusion:
Justification: Password protection detected.
Comment: Password protection detected.

Pri analýze USB kľúča neboli nájdené žiadne súbory obsahujúce odcudžené firemné dáta, fotografie projektov ani archívy súvisiace s internými materiálmi spoločnosti. Rovnako sa na zariadení nenachádzali šifrované kontajnery, veľké komprimované súbory ani adresárová štruktúra, ktorá by korešpondovala s firemnými projektmi alebo dokumentáciou.

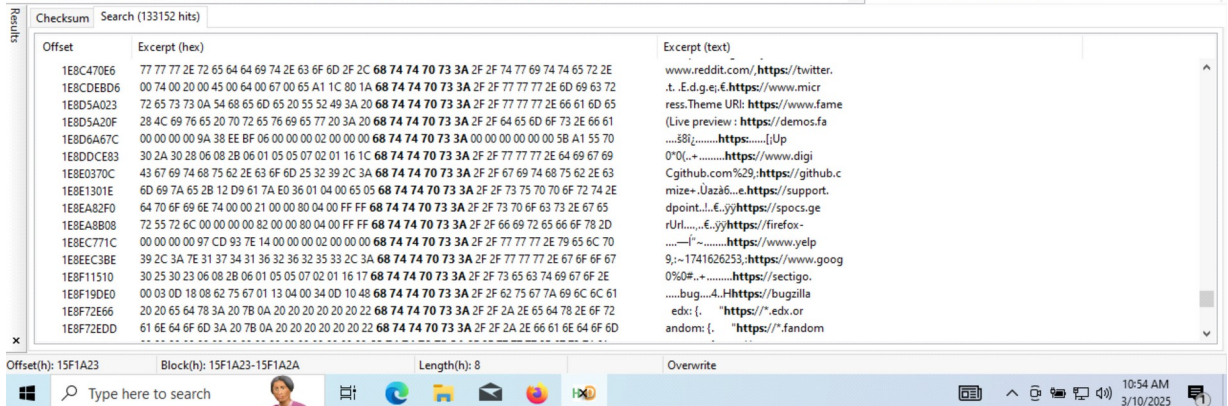
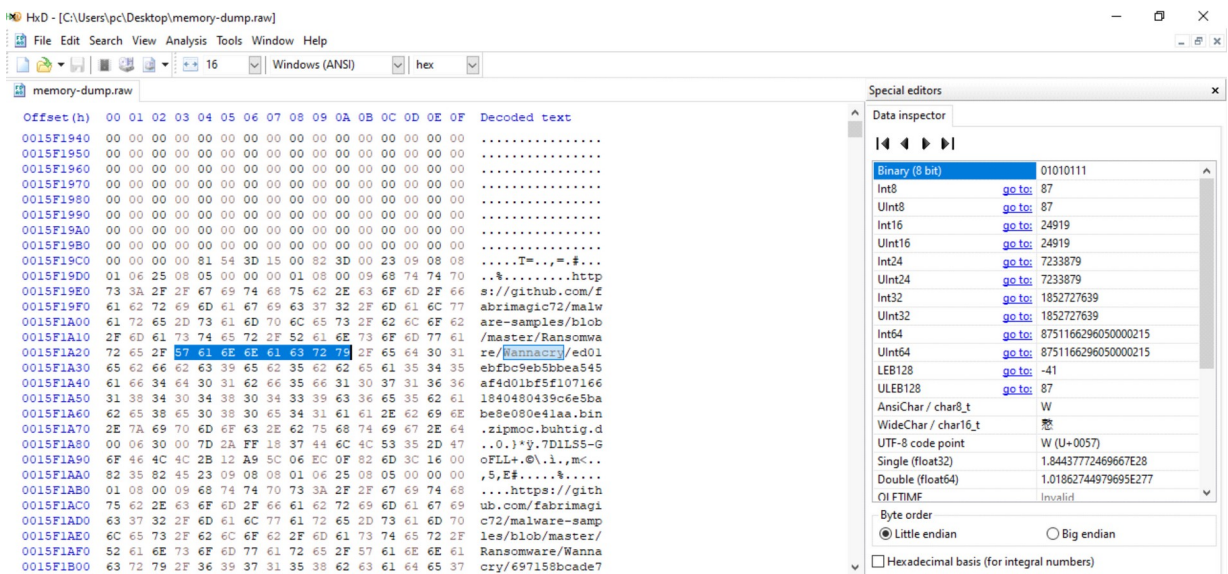
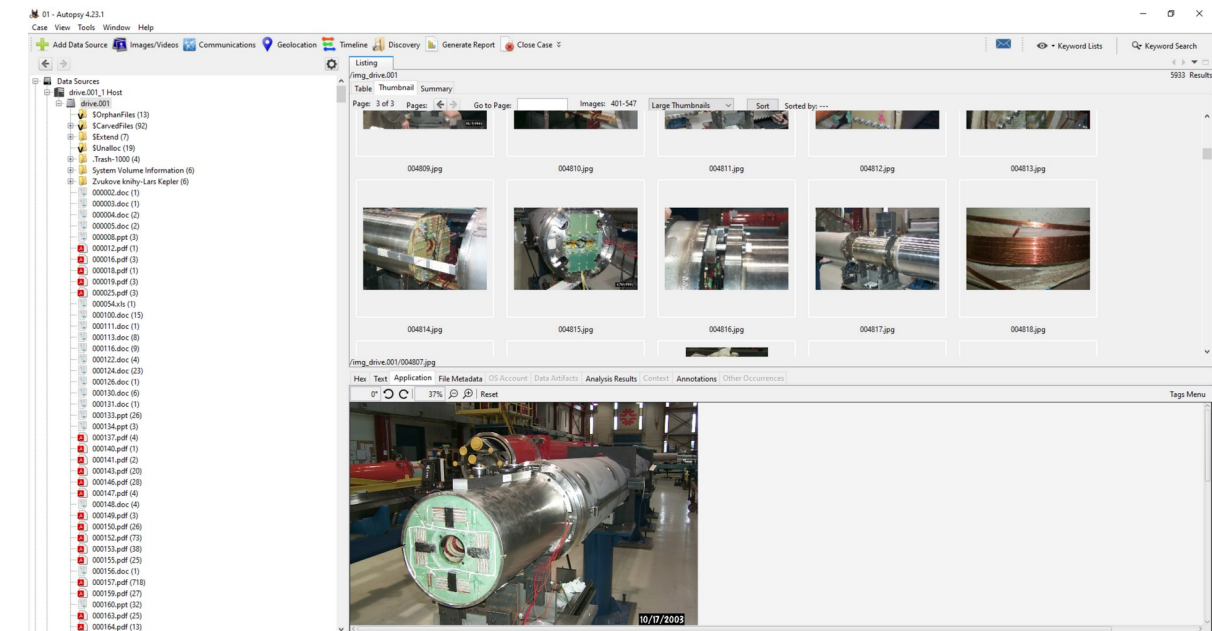
Na základe týchto zistení sa hypotéza, že USB kľúč bol použitý ako prenosné médium na dočasné uloženie a presun odcudzených dát, nepotvrdila. Dostupné dôkazy nenasvedčujú tomu, že by bolo USB použité na fyzický prenos alebo exfiltráciu citlivých údajov mimo spoločnosti.

Avšak, na základe analýzy obsahu USB kľúča boli identifikované viaceré podozrivé a škodlivé súbory. Medzi nimi sa nachádzali známe typy malvéru, ako napríklad WannaCry, Generic Trojan a EternalRocks, ktoré sú spojené s neoprávneným prístupom do systémov, šifrovaním dát a šírením škodlivého kódu. Okrem toho boli na USB nájdené aj .bat skripty určené na automatizované spúšťanie príkazov, pričom ich obsah naznačoval možné použitie na exfiltráciu dát alebo manipuláciu so súbormi.



Pri analýze zaisteného externého disku boli nájdené fotografie prototypu technologického zariadenia, na ktorom spoločnosť interne pracovala. Obsah fotografií naznačuje, že ide o materiály súvisiace s vývojom pripravovaného produktu alebo patentovaného riešenia. Súbory predstavujú citlivé firemné dáta s vysokou hodnotou z pohľadu vlastníctva spoločnosti.

Nález týchto fotografií potvrdzuje podozrenie, že mohlo dôjsť k neoprávnenému kopírovaniu interných materiálov za účelom ich odcudzenia alebo ďalšieho šírenia. Zároveň ide o významný dôkaz, ktorý môže súvisieť s pokusom o exfiltráciu dát a únikom dôverných informácií mimo spoločnosti.



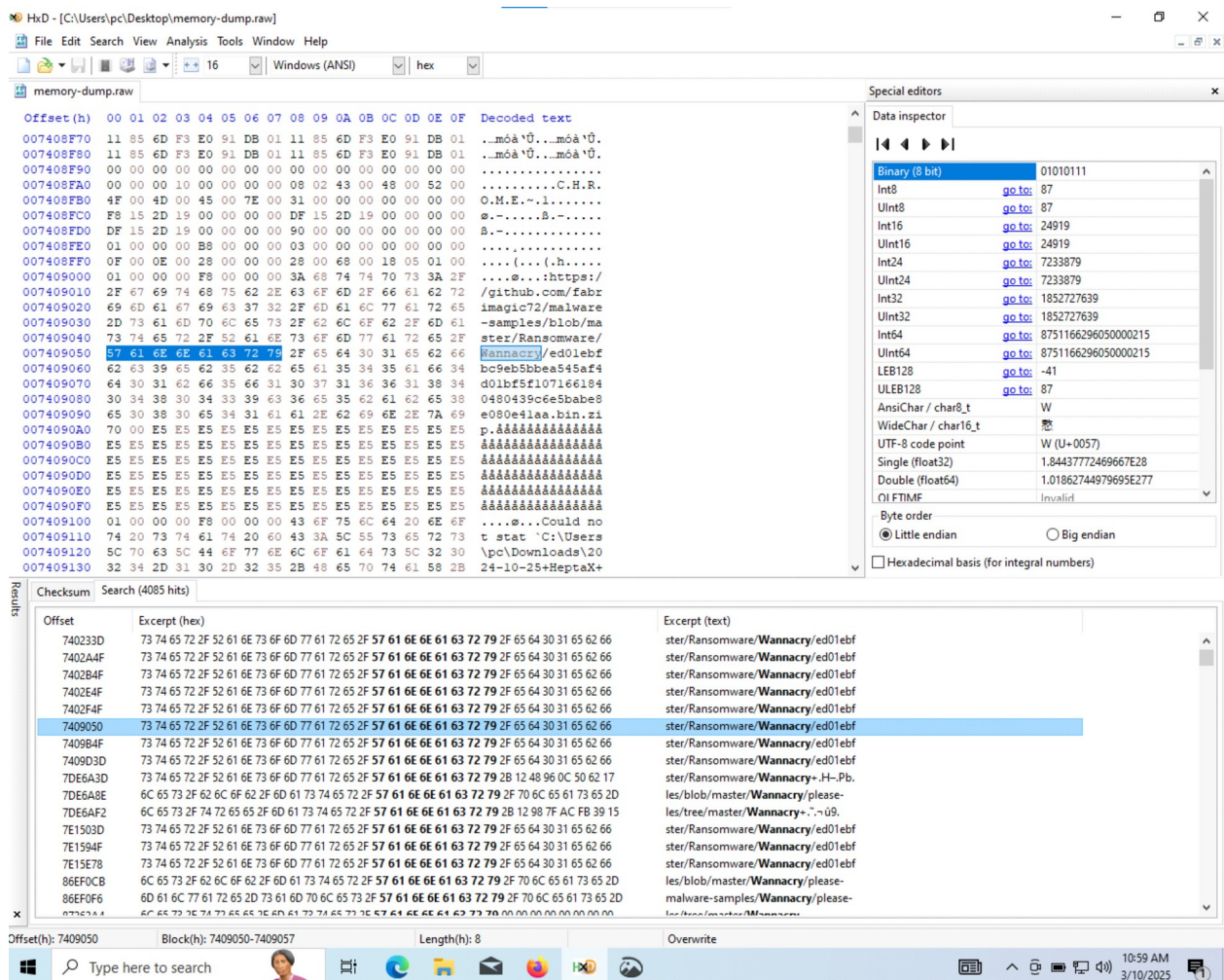
Analýza RAM pamäte – Identifikácia škodlivého softvéru

V rámci forenzejnej analýzy získanej RAM pamäte boli objavené indície naznačujúce prítomnosť škodlivého softvéru. Hexadecimálna analýza dumpu pamäte odhalila viacero referencií na zložku obsahujúcu ransomware **WannaCry**. Táto skutočnosť naznačuje, že v čase získania pamät'ového obrazu mohol byť škodlivý softvér aktívny alebo sa vyskytoval v procese systému.

Na základe identifikovaných textových reťazcov a analýzy štruktúry dát:

- **Obrázok 1:** Nachádza sa odkaz na adresár obsahujúci súbory ransomvéru **WannaCry**, pričom v pamäti sa nachádzajú aj možné hash hodnoty alebo identifikátory spojené s konkrétnou variantou malvéru.
- **Obrázok 2:** Vidíme ďalšie výskyty názvu **WannaCry**, spolu s viacerými URL adresami, ktoré môžu súvisieť s komunikáciou ransomvéru so servermi alebo s jeho šírením cez internet.

Táto analýza naznačuje, že skúmané zariadenie mohlo byť kompromitované ransomvérom, alebo v ňom ostali stopy po jeho predchádzajúcej aktivite. Ďalšie kroky zahŕňajú detailnejšiu analýzu aktívnych procesov, vyhľadanie škodlivých knižníc v pamäti a preverenie sieťovej komunikácie s cieľom potvrdiť alebo vyvrátiť prítomnosť aktívnej infekcie.



Образок 2.

Záver

Na základe vykonanej analýzy možno konštatovať, že neboli nájdené priame dôkazy potvrdzujúce úspešnú exfiltráciu dát mimo spoločnosti. Externý pevný disk, ako aj stratený USB kľúč, boli ponechané na mieste incidentu, čo výrazne znižuje pravdepodobnosť, že boli použité na finálne odcudzenie a prenesenie citlivých údajov mimo priestorov firmy.

Zároveň sa pri forenznnej analýze USB kľúča nenašli žiadne skripty ani nástroje, ktoré by sa pokúšali o prenos dát prostredníctvom siete alebo o komunikáciu so vzdialenými servermi. Hoci boli identifikované škodlivé súbory a podozrivé .bat skripty, ich funkcionality nesmerovala k automatizovanej online exfiltrácii dát.

Na základe dostupných dôkazov preto existuje vysoká pravdepodobnosť, že k úplnému úniku citlivých údajov mimo spoločnosti nedošlo, prípadne bol pokus o exfiltráciu prerušený alebo .

Keďže kamerový dohľad v budove bol v čase incidentu nefunkčný, nebolo možné získať žiadne vizuálne záznamy pohybu osôb v kritickom období. Táto skutočnosť výrazne obmedzila možnosti identifikácie páchateľa a rekonštrukcie jeho pohybu v priestoroch spoločnosti.

V dôsledku absencie kamerových záznamov sa nepodarilo jednoznačne určiť, kto manipuloval s nájdenými zariadeniami ani kto mohol mať prístup k citlivým oblastiam firmy. Identita páchateľa tak ostáva neznáma a vyšetrovanie sa musí opierať výhradne o digitálne forenzné stopy a analýzu zaistených zariadení.

Použitá literatúra

- **"Digital Forensics: Artifact Profile – USB Devices"**: Článok sa zameriava na význam histórie USB zariadení v digitálnej forenznnej analýze, vrátane umiestnenia relevantných artefaktov v systéme Windows a ich využitia pri vyšetrovaní.
<https://www.magnetforensics.com/blog/artifact-profile-usb-devices/>
- **"Ako sa obnova dát používa v počítačovej forenznnej oblasti"**: Tento článok vysvetľuje, ako digitálni forenzní vyšetrovatelia používajú softvér na obnovu dát na získavanie skrytých alebo odstránených údajov z digitálnych zariadení.
<https://www.datanumen.com/sk/blogy/ako-sa-obnova-d%C3%A1t-pou%C5%BE%C3%ADva-v-po%C4%8D%C3%ADta%C4%8Dovej-forenznnej-praxi/>