

Kybernetický útok na firmu SoftCom Solutions s.r.o.

Vyšetrovatel: Šimon Schmidt

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

Prípad:

Bratislavská IT spoločnosť SoftCom Solutions s.r.o., ktorá sa špecializuje na vývoj softvérových riešení, zažila v stredu 12. februára nečakaný kolaps svojich IT systémov. Zamestnanci si po príchode do práce všimli, že nemajú prístup k interným databázam, e-mailom ani firemným súborom. Pri pokuse o otvorenie akéhokoľvek dokumentu sa na ich obrazovkách objavila správa s výkupným v angličtine:

"Vaše servery boli napadnuté a zašifrované. Ak ich chcete získať späť, musíte zaplatiť výkupné vo výške 500 000€ v kryptomene Bitcoin na adresu 1FfmbHfnpaZjKFvyi1okTjJusN455paPH. Ak nezaplatíte do 72 hodín, všetky údaje budú nenávratne stratené."

Pri kontrole kancelárií a IT vybavenia technici objavili USB kľúč v serverovni firmy. Nebolo jasné, komu patrí ani či má s prípadom niečo spoločné. Bol USB kľúč súčasťou útoku, alebo ho tam niekto zabudol?

Cieľ vyšetovania:

Identifikovať páchatel'a kybernetického útoku na SoftCom Solutions s.r.o., určiť spôsob prieniku ransomvéru do firemnej siete a zabezpečiť dôkazy na potvrdenie alebo vyvrátenie hypotéz o vinníkoch.

Postup vyšetovania:

Pri vyšetovaní prípadov týkajúcich sa digitálnej forenznej analýzy si vieme ako vyšetovatelia vybrať z viacerých starších alebo ideálne novších schém vyšetovania. V mojom vyšetovaní budem postupovať podľa schémy Arnes 2017. Vyzerá takto:



Vysvetlenie jednotlivých bodov schémy:

1. Identifikácia

V tejto fáze sa určí cieľ vyšetovania, dostupné zdroje a definujú sa potrebné postupy. Prvotne sa analyzuje miesto činu a vykonáva sa identifikácia potenciálnych digitálnych dôkazov. Každé identifikované zariadenie je riadne zdokumentované a označené.

Bezpečnostné opatrenia:

- Tvorba podrobnej dokumentácie o zariadeniach a prostredí.

- Použitie certifikovaných nástrojov na skenovanie a detekciu digitálnych stôp.
- Zachovanie integrity miesta incidentu a predchádzanie kontaminácii dôkazov.

2. Zaisťovanie a zber

V tejto fáze sa zabezpečia a zhromaždia digitálne stopy, ktoré budú potom prepravené do laboratória v ochranných puzdrách či vreckách. Následne sa vytvoria obrazy pamätí na zariadeniach a tie budú v ďalších fázach prešetrované.

Bezpečnostné opatrenia:

- Vytvorenie aspoň 3 kópií obrazov zariadení spojených s vyšetrovaním.
- Použitie certifikovaných forenzných nástrojov na tvorbu obrazov digitálnych dôkazov.
- Každý obraz je skontrolovaný hashmi na zabezpečenie integrity.
- Dôkazy sa ukladajú do zabezpečených prostredí s digitálnymi podpismi (napr. špeciálny šifrovaný prázdny HDD).

3. Vyťažovanie

Digitálne stopy sa podrobia detailnému spracovaniu a identifikácii relevantných artefaktov. Dáta sa filtrujú a analyzujú na prítomnosť podozrivých súborov, procesov a aktivít, ktoré možno ukázať na vinníka v prípade.

Bezpečnostné opatrenia:

- Použitie izolovaných testovacích prostredí na spustenie podozrivých súborov.
- Analýza spustených procesov v RAM a kontrola Prefetch logov na detekciu podozrivých aktivít.
- Forenzná analýza USB logov a sieťových artefaktov na sledovanie komunikácie ransomvéru.

4. Analýza

Vykonanie detailnej analýzy digitálnych stôp s cieľom rekonštruovať priebeh incidentu a identifikovať páchateľa.

5. Prezentácia

Na záver sa pripraví správa s detailným popisom zistení a forenzné dôkazy sa predložia orgánu činnému v trestnom konaní.

Opatrenia:

- Použitie vizuálnych nástrojov na prezentáciu časovej osi a korelácie dôkazov.
- Uchovanie originálnych dôkazov v zabezpečenom prostredí.

5WH

Who? - (Kto?)

Útok mohol byť zámerne vykonaný hackerskou skupinou, konkurenčnou firmou alebo kludne aj interným zamestnancom. Momentálne sa nedá vylúčiť ani možnosť, že sa firma stala náhodným terčom útoku nejakej skupiny.

What? - (Čo?)

Firemné servery a pracovné stanice boli infikované špeciálnym typom PC vírusu - ransomvérom, ktorý zašifroval dôležité firemné údaje a znemožnil ich používanie. Za odstránenie vírusu žiadajú útočníci veľa peňazí.

When? - (Kedy?)

Verejne bol vírus oznámený firmou stredu 12. februára. Ďalšie informácie, ako kedy vírus infikoval firemné zariadenie a podobne zistia až forenzní analytici.

Where? - (Kde?)

Incident sa stal vo firemných priestoroch SoftCom Solutions s.r.o. v Bratislave. Napadnuté boli servery v dátovom centre a pracovné stanice zamestnancov pripojené do internej siete tejto bratislavskej firmy.

Why? - (Prečo?)

Motívom útoku je určite finančný zisk, keďže útočníci požadujú výkupné v Bitcoine výmenou za poskytnutie dešifrovacieho kľúča. Ďalším možným dôvodom mohla byť snaha o sabotáž alebo krádež firemných údajov, ak by išlo o konkurenciu či nespokojného zamestnanca.

How? - (Ako?)

Útok mohol byť vykonaný napr. cez phishingový e-mail obsahujúci škodlivý súbor alebo cez USB kľúč s vírusom, ktorý bol nejakým spôsobom pripojený k firemnej sieti.

Hypotézy - Kto môže byť páchatelom?

Hackerská skupina špecializujúca sa na ransomvérové útoky

Útok mohla vykonať organizovaná kybernetická skupina, ktorá zámerne infikovala firmu ransomvérom napríklad cez zraniteľnosti v softvéri. Ich cieľom je získať výkupné v kryptomene.

Overenie hypotézy: Podrobnou analýzou ransomvéru, porovnaním hashu s inými podobnými prípadmi, v ktorých figurovali organizované skupiny, prípadne zistenie, kam smeruje výkupné v kryptomene.

Interný zamestnanec alebo bývalý pracovník firmy

Niektro z vnútra spoločnosti, napríklad nespokojný zamestnanec alebo bývalý pracovník so znalosťou IT infraštruktúry, mohol úmyselne zaviesť vírus do firemnej siete. Mohol použiť USB kľúč alebo inú chybičku systému.

Overenie hypotézy: Skontrolujem prístupové logy počítačov v lokálnej sieti firmy, históriu USB zariadenia, aktivitu zamestnancov pred útokom a časové pečiatky súborov na USB. Následne spojím nejakého zamestnanca s USB zariadením pomocou získaných dôkazov.

Konkurenčná firma

Konkurencia mohla financovať alebo aj priamo uskutočniť útok s cieľom poškodiť reputáciu SoftCom Solutions s.r.o., narušiť jej činnosť alebo získať prístup k citlivým firemným údajom. V takom prípade by ransomvér mohol byť len zásterkou a hlavným cieľom by bola krádež obchodných informácií.

Overenie hypotézy: Zistím, či bol útok cielený iba na firmu SoftCom Solutions, preveríme únik firemných dát, sieťovú aktivitu a prípadné phishingové útoky.

Náhodný útok skupiny alebo jednotlivca

SoftCom Solutions s.r.o. sa mohla stať obeťou plošného kybernetického útoku, pri ktorom útočníci

automaticky skenujú internet na zraniteľné servery a pracovné stanice. Ak firma nemala dostatočne zabezpečené pripojenia, mohla byť infikovaná bez priameho cieľa.

Overenie hypotézy: Skontrolujem, či ransomvér využil zraniteľnosť systému, ktorú nemohol poznať nikto iný, ako interný zamestnanec. Či bol súčasťou plošného útoku, poprípade či spadá do nejakej známej rodiny malvérov využívaných na tieto účely.

Dáta využité v prípade:

V prípade sú využité data sety stiahnuté z voľne dostupných zdrojov na internete. V mojom prípade sú to stránky <https://datasets.fbreitinger.de/datasets/> a <https://www.digitalforensicsworkbook.com/data-sets>. Veľkosť data setov je dokopy cca 2GB.

Okrem týchto data setov vo vyšetrovaní využívam aj „reálne“ dáta. Tieto „reálne“ dáta sú nejaké súbory, ktoré nebolo jednoduché obdržať pomocou data setov (napr. ransomvér malej veľkosti setup.exe).

Zariadenia, ktoré budem vo vyšetrovaní skúmať

USB kľúč z miesta činu

- Obsahuje vírus?
- Aké súbory sú na ňom uložené a kedy boli naposledy modifikované?
- Aké metadáta sú spojené so súbormi

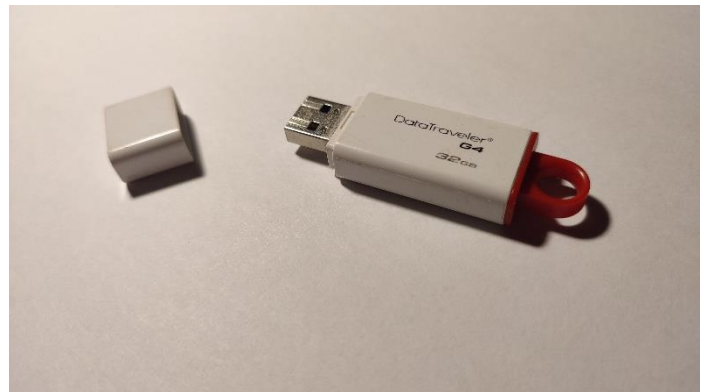
Firemný server - hlavný cieľ ransomvéru

- Logy prihlásení: kto a kedy mal prístup k systému?
- Sieťová aktivita: boli zaznamenané podozrivé pripojenia alebo veľké presuny dát?
- Stav šifrovaných súborov: existujú nešifrované kópie alebo zálohy?

Pracovné stanice zamestnancov

- Bol ransomvér spustený z pracovného PC niektorého zo zamestnancov?
- Aké aplikácie boli nedávno nainštalované alebo spustené?
- Existujú dôkazy o phishingovom útoku alebo víruse v e-mailoch?

Zariadenie USB nájdené na mieste činu



USB kľúč bol objavený v serverovni firmy, ležal pod stolom v miestnosti. Objavil ho administrátor pri kontrole serverov po útoku.

Bezpečnostné opatrenia vykonané s USB kľúčom:

- Kľúč bol pred akoukoľvek manipuláciou zdokumentovaný a odfotený.
- Kľúč bol vložený do špeciálneho obalu, aby sa zabránilo jeho poškodeniu.
- Každý krok bol zaznamenaný do vyšetrovacieho protokolu.
- Na prehliadku obsahu USB kľúča som využil bezpečné prostredie - Virtual Machine.
- Pred akýmkoľvek zásahom sme spravili aspoň 3 kópie obsahu USB s potvrdenou integritou jeho údajov pomocou vypočítaných hashov.
- Kópie obrazov USB kľúča som uložil do špeciálneho izolovaného prostredia - na úplne prázdny šifrovaný HDD.

Špecifikácia zariadenia:

- **Kapacita:** 32 GB
- **Súborový systém:** FAT32
- **Značka:** Kingston
- **Model:** DataTraveler G4
- **Sériové číslo:** 0B8E6B0166E7
- **Rozhranie:** USB 3.0 spätne kompatibilné s USB 2.0
- **Farba:** Biela s červenými prvkami
- **Rozmery:** 55 × 21 × 10,1 mm
- **Hmotnosť:** cca 10 g
- **Typ pamäte:** Flash NAND
- **Priemerná prístupová doba:** <1 ms
- **Životnosť:** cca 10 000 prepisovacích cyklov
- **Architektúra:** Používa radič Phison/EKMP a TLC NAND Flash

- **Systémové požiadavky:** Windows 8.1, Windows 8, Windows 7 (SP1), Windows Vista (SP2), Mac OS X v.10.8.x alebo novší, Linux v.2.6.x alebo novší, USB port
- **Rýchlosť čítania:** cca 100 MB/s (pri pripojení cez USB 3.0)
- **Rýchlosť zápisu:** cca 20 MB/s (pri pripojení cez USB 3.0)

Softvér použitý pri skúmaní USB zariadenia

Vytvorenie obrazu USB: FTK Imager

Analýza obrazu: Autopsy

Potvrdenie rýchlosti a prístupovej doby: CrystalDiskMark

Informácie získané pomocou programu FTK Imager:

Obraz USB zariadenia – pracovná kópia

Názov: USB_Image

Veľkosť: 28,8GB

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: USB image

Examiner: SS

Notes:

Information for C:\Users\simon\Desktop\USB_Image:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 3 765

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 60 489 728

[Physical Drive Information]

Drive Model: Kingston DataTraveler 3.0 USB Device

Drive Serial Number: 0B8E6B0166E7

Drive Interface Type: USB

Removable drive: True

Source data size: 29536 MB

Sector count: 60489728

[Computed Hashes]

MD5 checksum: bac900fd13f8147b996b84126ed9f61a

SHA1 checksum: bb5194fa3c1554a584222d0757cc887ebec56e91

Image Information:

Acquisition started: Sun Mar 16 15:23:00 2025

Acquisition finished: Sun Mar 16 15:27:10 2025

Segment list:

C:\Users\simon\Desktop\USB_Image

COMPUTED HASH : bac900fd13f8147b996b84126ed9f61a

COMPUTED HASH : bb5194fa3c1554a584222d0757cc887ebec56e91

Image Verification Results:

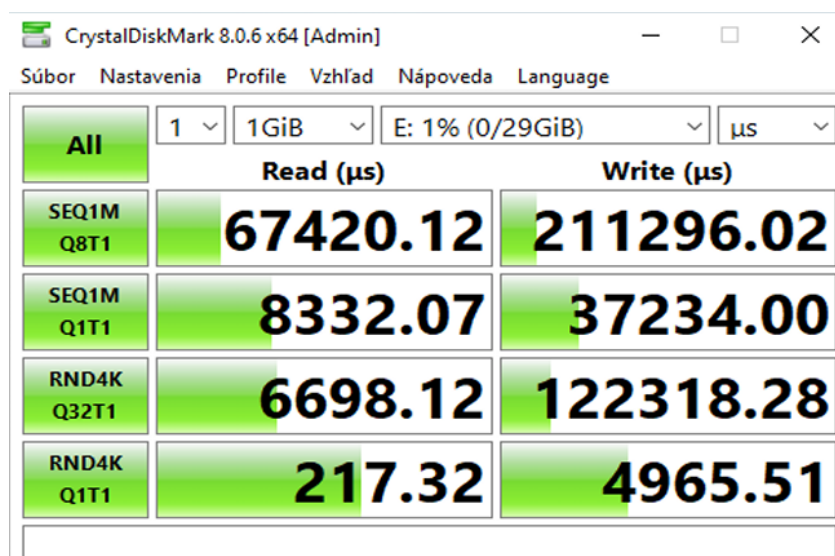
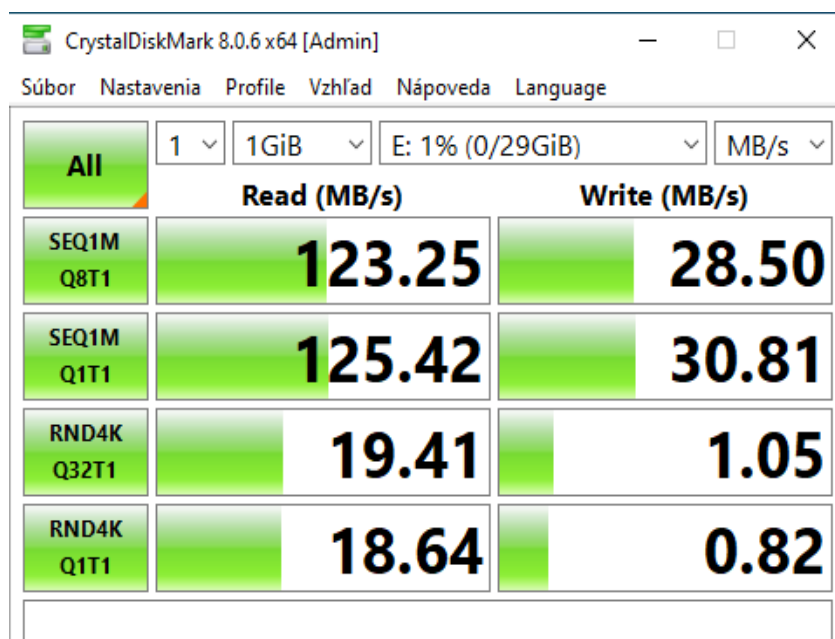
Verification started: Sun Mar 16 15:27:10 2025

Verification finished: Sun Mar 16 15:28:37 2025

MD5 checksum: bac900fd13f8147b996b84126ed9f61a : verified

SHA1 checksum: bb5194fa3c1554a584222d0757cc887ebec56e91 : verified

Údaje o USB zariadení potvrdené programom CrystalDiskMark:



Chain of custody USB zariadenia:

Číslo:	01	Typ súboru:	WinRAR archive	Obnovený súbor:	Nie	Veľkosť:	28,8GB
Popis prípadu:		Kybernetický útok na firmu SoftCom Solutions					
Názov súboru:		USB_Image					
Miesto získania digitálnej stopy:		Serverovňa firmy SoftCom Solutions					
Poznámky:		Kópia obrazu zariadenia USB Kingston DataTraveler G4 32GB spravená pomocou FTK® Imager 4.7.3.81					
Časové pečiatky							
Access:	23.2.2025 10:32:24		Modify:	23.2.2025 10:32:24		Change:	-
Digitálny odtlačok (heš)	MD5	bac900fd13f8147b996b84126ed9f61a					
	SHA1	bb5194fa3c1554a584222d0757cc887ebec56e91					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
23.2.2025 11:29:43		Zabezpečenie USB zariadenia a prevoz do laboratória					
25.2.2025 15:44:19		Vyťažovanie informácií z USB zariadenia					
25.2.2025 17:21:58		Koniec vyťažovania, overenie integrity USB zariadenia					
25.2.2025 17:11:17		Uloženie USB do trezoru k ostatným dôkazom					

Skúmané dáta - Analýza

Počet súborov: 200 352

Veľkosť: 30,97GB(z toho 2,32GB využitý dátový priestor)

Čo hľadám:

Spustiteľné súbory (exe, bat...)

- **.exe** – Štandardný spustiteľný súbor pre OS Windows, často používaný na spustenie škodlivých programov.
- **.bat** – Možnosť vykonávať príkazy v systéme Windows.
- **.cmd** – Podobné ako .bat, používané pre skripty v príkazovom okne.
- **.com** – Ďalší typ spustiteľného súboru, často používaný v starších DOS programoch.
- **.scr** – Súbory šetriča obrazovky, ktoré môžu vykonávať kód podobne ako .exe.
- **.pf** – Programové informačné súbory, ktoré môžu byť použité na spustenie malvéru.

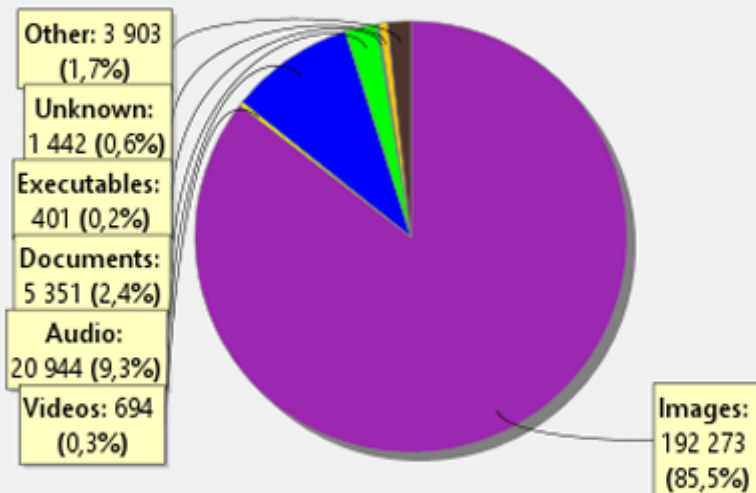
Graf z vyšetrovania obrazu dát USB Kingston DataTraveler G4:

Usage: Flash Drive

OS:

Size: 31 GB

File Types



Allocated Files: 200 352

Unallocated Files: 24 656

Slack Files: 6 144

Directories: 372

Zaujímavé súbory nájdené na USB:

Listing

File Search Results 1

File Search Results 2

File Search Results 3

Bookmark File Tags

8 Results

Table

Thumbnail

Summary

Page:

Pages:

Go to Page:

Save Table as CSV

File	File Path	Comment	Modified Time	Changed Time	Accessed Time	Created Time	Size
 setup.exe	/img_E/\$CarvedFiles/1/f1466496_ARCHPR.zip/ARCHP...		2002-07-17 18:48:24 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	848706
 setup.exe	/img_E/setup.exe		2025-03-11 19:36:56 SEČ	0000-00-00 00:00:00	2025-03-16 00:00:00 SEČ	2025-03-11 19:39:36 SEČ	1818826
 Setup.exe	/img_E/\$CarvedFiles/1/f0567488.rar/Duke Nukem 3D ...		2013-09-28 00:10:55 SELČ	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	645329
 1111.bat	/img_E/1111.bat		2025-03-16 15:02:02 SEČ	0000-00-00 00:00:00	2025-03-16 00:00:00 SEČ	2025-03-16 15:02:09 SEČ	14
 f4d3.bat	/img_E/f4d3.bat		2025-03-16 15:12:26 SEČ	0000-00-00 00:00:00	2025-03-16 00:00:00 SEČ	2025-03-16 15:12:31 SEČ	12
 f1468160_brutus.zip	/img_E/\$CarvedFiles/1/f1468160_brutus.zip		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	334124
 f1808000_wwwhack.zip	/img_E/\$CarvedFiles/1/f1808000_wwwhack.zip		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	490814
 f1807936_nc.zip	/img_E/\$CarvedFiles/1/f1807936_nc.zip		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	28614

V ďalšom kroku som odobral vzorku vírusu z infikovanej siete. Hash tejto kópie som následne porovnal s podozrivými súbormi na USB nájdenými s nástrojom Autopsy.

Zhodu sme našli pri súbore setup.exe

Hashe súboru setup.exe získané z priamo z nájdeného USB:

Algorithm	Hash	Path
-----	----	----
SHA1	5019E2F7BE64755383C8B3D5B7947C556E1D77A0	E:\setup.exe

Algorithm	Hash	Path
-----	----	----
MD5	D3B9F0FF9520BA54D272513838D1CE14	E:\setup.exe

Hashe vírusu odobraného z infikovanej siete:

Algorithm	Hash	Path
-----	----	----
SHA1	5019E2F7BE64755383C8B3D5B7947C556E1D77A0	C:\ransomver_vzorka.exe

Algorithm	Hash	Path
-----	----	----
MD5	D3B9F0FF9520BA54D272513838D1CE14	C:\ransomver_vzorka.exe

Zhodujú sa nám 2 hashe. Vírus teda pochádza z tohto USB zariadenia.

Kľúčový bod prípadu

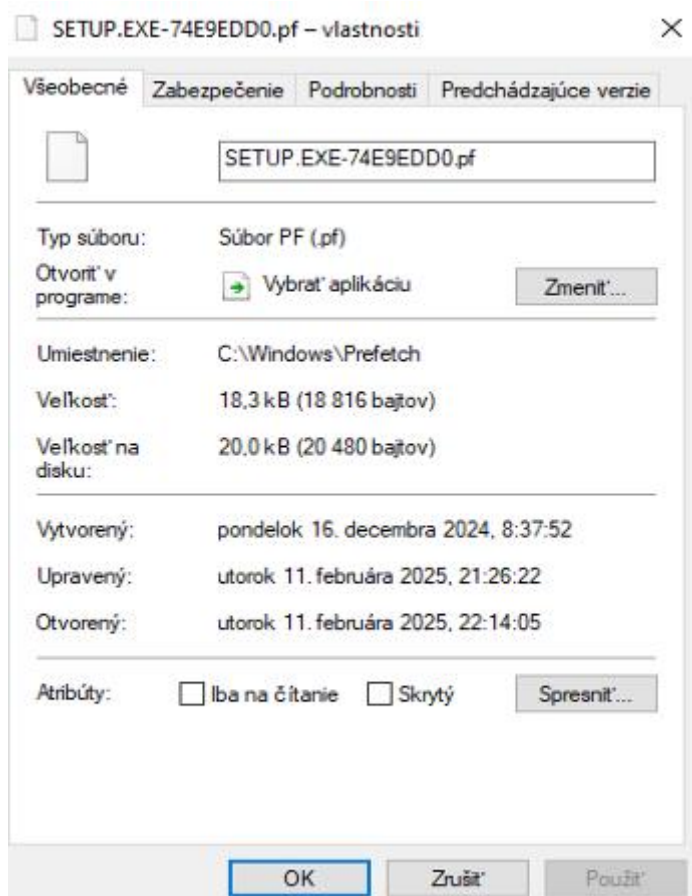
Vírus pochádza z USB zariadenia nájdeného v serverovni firmy. Dá sa teda skoro s plnou istotou konštatovať, že vinník je interným zamestnancom, ktorý dobre pozná štruktúru firmy. V ďalšej fáze prípadu sa budem sústrediť na vyšetrovanie obrazov operačnej pamäte firemných počítačov. Je veľká šanca že na jednom z nich sa nájde ransomvér s totožným hashom, ako má súbor setup.exe...

Vyšetrovanie Martinovho PC:

Pri vyšetrovaní priestorov firmy som našiel podozrivé súbory na PC Martina Molnára. Pátranie som u neho začal v zložke C:\Windows\Prefetch, kde o

peračný systém Windows ukladá záznamy aplikácií po spustení v systéme. Onedlho som našiel prvý reálny dôkaz proti Martinovi - .pf súbor setup.exe.

Tento počítač > Lokálny disk (C:) > Windows > Prefetch					Hľadať v: Prefetch
	Názov	Dátum úpravy	Typ	Veľkosť	
ck	KUNTIMEBROKER.EXE-DA83EUA1.pt	18. 3. 2025 1:38	Súbor PF	7 kB	
.ocker	RUNTIMEBROKER.EXE-E66EAD8.pf	18. 3. 2025 1:52	Súbor PF	10 kB	
aded	S2_SP64_SHIP.EXE-AF746837.pf	14. 12. 2024 2:44	Súbor PF	28 kB	
	SCREENCLIPPINGHOST.EXE-A742536A.pf	18. 3. 2025 1:45	Súbor PF	35 kB	
	SCREENCLIPPINGHOST.EXE-DB4CD255.pf	15. 2. 2025 16:53	Súbor PF	37 kB	
arPres	SCREENSKETCH.EXE-1CDB6283.pf	11. 3. 2025 20:38	Súbor PF	61 kB	
zation	SDXHELPER.EXE-832215EB.pf	18. 3. 2025 0:45	Súbor PF	12 kB	
	SEARCHAPP.EXE-03FE5603.pf	12. 10. 2024 12:42	Súbor PF	98 kB	
RL	SEARCHAPP.EXE-1525110D.pf	13. 3. 2025 18:05	Súbor PF	116 kB	
	SEARCHFILTERHOST.EXE-44162447.pf	18. 3. 2025 1:48	Súbor PF	4 kB	
iveCo	SEARCHPROTOCOLHOST.EXE-69C456C3.pf	18. 3. 2025 1:48	Súbor PF	4 kB	
pps	SECHEALTHUI.EXE-6ACE3B2E.pf	27. 1. 2025 16:03	Súbor PF	49 kB	
	SETUP.EXE-74E9EDD0.pf	17. 3. 2025 21:10	Súbor PF	19 kB	
	SETUP.TMP-2BF926CB.pf	11. 3. 2025 19:37	Súbor PF	9 kB	
ethod	SETUP.TMP-3D81080F.pf	11. 3. 2025 19:39	Súbor PF	14 kB	
mas	SHELLEXPERIENCEHOST.EXE-28A44C7B.pf	17. 3. 2025 20:36	Súbor PF	45 kB	
nelReq	SHELLEXPERIENCEHOST.EXE-35108DDA.pf	13. 11. 2024 17:45	Súbor PF	42 kB	
	SHELLEXPERIENCEHOST.EXE-AA63A567.pf	17. 10. 2024 3:26	Súbor PF	41 kB	
	SHJ2MSM.EXE-C05FEFBE.pf	2. 3. 2025 16:11	Súbor PF	12 kB	
	SIHOST.EXE-115B507F.pf	16. 3. 2025 18:26	Súbor PF	18 kB	
oft.NE	SMARTSCREEN.EXE-EACC1250.pf	18. 3. 2025 1:49	Súbor PF	14 kB	
on	SNDVOL.EXE-425BC49B.pf	18. 3. 2025 1:46	Súbor PF	15 kB	
Logs	SOUNDREC.EXE-26D9FE0C.pf	12. 3. 2025 16:18	Súbor PF	59 kB	
	SPLWOW64.EXE-57576C25.pf	5. 3. 2025 20:44	Súbor PF	9 kB	
Web F	SPOTIFY.EXE-1736D2AC.pf	18. 3. 2025 0:43	Súbor PF	90 kB	
r	SPOTIFY.EXE-1736D2AD.pf	18. 3. 2025 0:43	Súbor PF	37 kB	
nance	SPOTIFY.EXE-1736D2AE.pf	18. 3. 2025 0:43	Súbor PF	28 kB	
	SPOTIFY.EXE-1736D2AF.pf	18. 3. 2025 0:43	Súbor PF	21 kB	
	SPOTIFY.EXE-1736D2B0.pf	18. 3. 2025 0:43	Súbor PF	8 kB	
efiniti	SPOTIFY.EXE-1736D2B4.pf	18. 3. 2025 0:45	Súbor PF	29 kB	
	SDBSVIC.EXE-96070FE0.pf	17. 3. 2025 23:07	Súbor PF	7 kB	



Meta údaje o súbore tiež svedčia proti Martinovi. Časy, v ktorých sa so súborom manipulovalo sú podozrivo blízke k dátumu útoku.

Obraz operačnej pamäte Martinovho PC:

Ďalším krokom bolo odobranie obrazu RAM pamäte z PC Martina Molnára.

Obraz som vyhotovil, pred viacerými svedkami overil jeho integritu a bezpečne ho uskladnil na pracovnom šifrovanom HDD.

Nástroj pre vytváranie záznamov RAM pamäte: FTK Imager

Nástroj pre otváranie a analýzu záznamov RAM pamäte: HxD

Názov: ram_dump.mem

Veľkosť obrazu: 32,9 GB

Vytvorenie obrazu RAM pamäte: 16.3.2025 15:27:10

MD5 HASH : 162C75B966A4995C01126C74FD9429C0

SHA1 HASH : 579921EA78863BAED9AAB537CCF5BEBE50D9E3B3

MD5 checksum: 162C75B966A4995C01126C74FD9429C0

SHA1 checksum: 579921EA78863BAED9AAB537CCF5BEBE50D9E3B3

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
152B9AC50	45	07	00	00	05	50	B3	05	01	4B	12	00	08	00	00	00	E....P1..K.....
152B9AC60	49	99	B8	00	ED	4F	B3	05	D5	1F	10	00	D1	B2	E5	0A	I™,.iO1.Ö...N.í.
152B9AC70	65	05	00	00	04	00	00	00	F1	B2	E5	0A	DD	4F	B3	05	e.....ń.í.YO1.
152B9AC80	61	CA	65	01	45	07	00	00	45	07	00	00	CD	83	F8	00	aEe.E...E...í.ř.
152B9AC90	61	CA	65	01	45	07	00	00	45	07	00	00	11	00	00	00	aEe.E...E.....
152B9ACA0	61	CA	65	01	45	07	00	00	45	07	00	00	C1	4F	B3	05	aEe.E...E...ÄO1.
152B9ACB0	D1	82	CE	0A	45	07	00	00	45	07	00	00	71	00	00	00	N,í.E...E...q...
152B9ACC0	55	00	00	00	55	99	7D	05	45	07	00	00	45	07	00	00	U...U™}.E...E...
152B9ACD0	0A	00	00	00	99	86	B3	05	31	21	61	00	31	21	61	00	™+1.1!a.1!a.
152B9ACE0	61	F4	E5	08	DD	8B	B3	05	55	42	B3	05	BD	42	B3	05	aó1.Y<1.UB1.~B1.
152B9ACF0	0A	00	00	00	2D	00	00	00	2D	00	00	00	A9	86	B3	05	-...-...@+1.
152B9AD00	A9	86	B3	05	2D	00	00	00	2D	00	00	00	2D	00	00	00	@+1.-...-...-...
152B9AD10	32	00	00	00	00	00	20	00	00	00	20	00	2D	00	00	00	2.....-...-...
152B9AD20	00	00	00	00	00	00	00	00	2D	00	00	00	55	99	7D	05	-...U™}.
152B9AD30	45	07	00	00	45	07	00	00	0A	00	00	00	89	45	B3	05	E...E.....%E1.
152B9AD40	E1	C2	61	00	E1	C2	61	00	F1	F3	E5	08	65	83	B3	05	áÄa.áÄa.ńó1.e.1.
152B9AD50	2D	00	00	00	9D	45	B3	05	02	00	00	00	2D	00	00	00	-...tE1.....-...
152B9AD60	2D	00	00	00	05	46	B3	05	05	46	B3	05	2D	00	00	00	-....F1..F1.-...
152B9AD70	2D	00	00	00	2D	00	00	00	32	00	00	00	00	00	20	00	-...-...2.....
152B9AD80	00	00	00	00	2D	00	00	00	00	00	00	00	00	00	00	00	-.....
152B9AD90	2D	00	00	00	AD	03	00	00	03	00	00	00	1C	00	00	00	-.....
152B9ADA0	51	75	E7	0A	6A	02	00	00	B5	00	00	00	03	00	00	00	Quç.j...u.....
152B9ADB0	09	00	00	00	73	65	74	75	70	2E	65	78	65	00	00	00	setup.exe....
152B9ADC0	65	05	00	00	22	00	00	00	55	45	B3	05	75	45	B3	05	e..."....UE1.uE1.
152B9ADD0	61	07	00	00	61	07	00	00	61	07	00	00	61	07	00	00	a...a...a...a...
152B9ADE0	61	07	00	00	61	07	00	00	61	07	00	00	61	07	00	00	a...a...a...a...
152B9ADF0	61	07	00	00	61	07	00	00	61	07	00	00	61	07	00	00	a...a...a...a...
152B9AE00	61	07	00	00	61	07	00	00	61	07	00	00	65	05	00	00	a...a...a...e...
152B9AE10	22	00	00	00	21	45	B3	05	41	45	B3	05	61	07	00	00	"...!E1.AE1.a...
152B9AE20	61	07	00	00	61	07	00	00	61	07	00	00	61	07	00	00	a...a...a...a...
152B9AE30	61	07	00	00	61	07	00	00	61	07	00	00	61	07	00	00	a...a...a...a...
152B9AE40	61	07	00	00	61	07	00	00	61	07	00	00	61	07	00	00	a...a...a...a...
152B9AE50	61	07	00	00	61	07	00	00	65	05	00	00	22	00	00	00	a...a...e..."...
152B9AE60	ED	44	B3	05	0D	45	B3	05	61	07	00	00	61	07	00	00	iD1..E1.a...a...
152B9AE70	61	07	00	00	61	07	00	00	61	07	00	00	61	07	00	00	a...a...a...a...
152B9AE80	61	07	00	00	61	07	00	00	61	07	00	00	61	07	00	00	a...a...a...a...
152B9AE90	61	07	00	00	61	07	00	00	61	07	00	00	61	07	00	00	a...a...a...a...
152B9AEA0	61	07	00	00	AD	03	00	00	03	00	00	00	46	00	00	00	a.....F...
152B9AEB0	51	75	E7	0A	94	05	00	00	61	CA	65	01	45	07	00	00	Quç."...aEe.E...
152B9AEC0	45	07	00	00	11	00	00	00	61	CA	65	01	45	07	00	00	E.....aEe.E...
152B9AED0	45	07	00	00	89	4F	B3	05	39	4A	12	00	0E	00	00	00	E...%O1.9J.....
152B9AEE0	31	61	CE	0A	ED	DA	C9	00	85	03	F8	00	19	A1	51	00	laí.íÜĚ.....ř...~Q.

V obraze RAM pamäte možno vidieť digitálne ostatky spomínaného vírusu.

Po analýze RAM obrazu Martinovho PC som identifikoval zvyšky podozrivého procesu, ktorý bol spustený krátko pred útokom. Ďalej som extrahoval obsah zvyškov vírusu a porovnal ho so vzorkou získanou z USB zariadenia.

Hashe získané z USB:

Algorithm	Hash	Path
-----	----	----
SHA1	5019E2F7BE64755383C8B3D5B7947C556E1D77A0	E:\setup.exe

Algorithm	Hash	Path
-----	----	----
MD5	D3B9F0FF9520BA54D272513838D1CE14	E:\setup.exe

Hashe získané z RAM obrazu Martinovho PC:

Algorithm	Hash	Path
-----	----	----
SHA1	5019E2F78E64755383C8B3D587947C556E1D77A0	D:\setup.exe

Algorithm	Hash	Path
-----	----	----
MD5	D3B9F0FF9520BA54D272513838D1CE14	D:\setup.exe

Našli sme zhodu. To znamená, že v Martinovom počítači sa vírus nachádzal tiež.

Prepojenie USB s Martinovým PC

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
3A84BEFC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
3A84BEFD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
3A84BEFE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
3A84BEFF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
3A84BF000	68	62	69	6E	00	90	08	00	00	10	00	00	00	00	00	00	hbin.....
3A84BF010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
3A84BF020	88	FF	FF	FF	6E	6B	20	00	DA	33	A9	C2	D6	8B	DB	01	.`nk.Ú3@ÄÖ<Ů.
3A84BF030	03	00	00	00	48	64	06	00	06	00	00	00	00	00	00	00	Hd.....
3A84BF040	C0	92	08	00	FF	FF	FF	FF	00	00	00	00	FF	FF	FF	FF	Ř'.....
3A84BF050	58	BB	01	00	FF	FF	FF	FF	70	01	00	00	00	00	00	00	X».....p.....
3A84BF060	00	00	00	00	00	00	00	00	00	00	00	00	26	00	00	00	&...
3A84BF070	7B	37	66	31	30	38	61	32	38	2D	39	38	33	33	2D	34	{7f108a28-9833-4
3A84BF080	62	33	62	2D	62	37	38	30	2D	32	63	36	62	35	66	61	b3b-b780-2c6b5fa
3A84BF090	35	63	30	36	32	7D	00	00	F8	FE	FF	FF	6E	6B	20	00	5c062}..řť`nk .
3A84BF0A0	DA	33	A9	C2	D6	8B	DB	01	03	00	00	00	20	90	08	00	Ú3@ÄÖ<Ů.....
3A84BF0B0	01	00	00	00	00	00	00	00	E0	8F	08	00	FF	FF	FF	FF	řŽ.....
3A84BF0C0	01	00	00	00	D8	8F	08	00	58	BB	01	00	FF	FF	FF	FF	ŘŽ..X».....
3A84BF0D0	02	00	00	00	00	00	00	00	1C	00	00	00	1C	01	00	00	
3A84BF0E0	00	00	00	00	B8	00	00	00	23	23	3F	23	53	54	4F	52	,...##?#STOR
3A84BF0F0	41	47	45	23	56	6F	6C	75	6D	65	23	5F	3F	3F	5F	55	AGE#Volume#??_U
3A84BF100	53	42	53	54	4F	52	23	44	69	73	6B	26	56	65	6E	5F	SBSTOR#Disk&Ven
3A84BF110	4B	69	6E	67	73	74	6F	6E	26	50	72	6F	64	5F	44	61	Kingston&Prod Da
3A84BF120	74	61	54	72	61	76	65	6C	65	72	5F	33	2E	30	26	52	taTraveler 3.0&R
3A84BF130	65	76	5F	50	4D	41	50	23	30	38	36	30	36	45	36	44	ev_PMAP#08606E6D
3A84BF140	34	31	38	41	42	45	42	31	36	37	31	37	35	42	41	33	418ABEB167175BA3
3A84BF150	26	30	23	7B	35	33	66	35	36	33	30	37	2D	62	36	62	&0#{53f56307-b6b
3A84BF160	66	2D	31	31	64	30	2D	39	34	66	32	2D	30	30	61	30	f-11d0-94f2-00a0
3A84BF170	63	39	31	65	66	62	38	62	7D	23	7B	37	66	31	30	38	c91efb8b}#{7f108
3A84BF180	61	32	38	2D	39	38	33	33	2D	34	62	33	62	2D	62	37	a28-9833-4b3b-b7
3A84BF190	38	30	2D	32	63	36	62	35	66	61	35	63	30	36	32	7D	80-2c6b5fa5c062}
3A84BF1A0	E0	FE	FF	FF	53	00	54	00	4F	00	52	00	41	00	47	00	řť`S.T.O.R.A.G.
3A84BF1B0	45	00	5C	00	56	00	6F	00	6C	00	75	00	6D	00	65	00	F \ V o l u m e

V obraze RAM pamäti boli nájdené aj pozostatky USB zariadenia Kingston DataTraveler nájdeného v serverovni firmy.

V tejto časti prípadu bolo potrebné získať Martinovu výpoveď. Bol preto predvolaný na výsluch jedným z našich vyšetrovateľov. Tu je správa z výsluchu:

Prípado: Útok na firmu SoftCom Solutions s.r.o. – výpoved' Martina Molnára

Dátum: 01.04.2025 | Miestnosť B1, budova 3 | Vyšetrovateľ: Ing. T. Kováč, CFE

„Dobrý deň, volám sa Martin Molnár, som IT technik vo firme SoftCom Solutions a pracujem tu už tretí rok. Chcem na začiatok povedať, že som nevinný a nikdy by som úmyselne nepoškodil firmu, pre ktorú robím a ktorá ma živí. Áno, vírus bol spustený na mojom počítači, ale ja som to neurobil. Som si istý, že niekto sa musel dostať k môjmu PC a vírus tam naschvál spustil, aby to vyzeralo, že som to bol ja.

V deň útoku som do kancelárie prišiel až poobede, okolo 16:30. Viac mi totiž vyhovuje pracovať poobede a v noci. Určite som si len niekam odskočil a počítač som zabudol zamknúť. Priznávam – bola to chyba, ale vtedy som vôbec netušil, že by mi niekto z kolegov mohol niečo takéto spraviť.

To USB zariadenie, na ktorom vraj bol ten vírus, som ja nikdy nepoužil. Ani si nepamätám, že by som ho videl. Kľúč do PC mohol niekto zapojiť v mojej neprítomnosti. Viem, že máme otvorené pracovné priestory a do našej časti občas chodí aj Rasťo z vedľajšieho oddelenia – medzi nami to nikdy veľmi neklapalo.

Prosím, neverte tomu, že by som mal motiváciu na niečo takéto. Ja som si vždy robil svoju prácu poctivo, nemám žiadne konflikty a nikdy som nič neukradol. Chcem, aby sa celá vec dôkladne prešetrla, pretože som neprávom obvinený.“

Koniec výpovede Martina Molnára.

Našťastie ma napadlo že pred pár týždňami vedenie firmy oznámilo, že bol nainštalovaný nový 24/7 kamerový systém kvôli zvýšeniu bezpečnosti a nočnému prespávaniu niektorých zamestnancov. Ak si dobre pamätám, jedna z nových kamier je umiestnená aj v hlavnej kancelárii, v ktorej má stôl aj hlavný podozrivý Martin Molnár.

11-02-2025 Tue 22:14:05



Názov: CCTV_11_02_2025.mp4

Veľkosť súboru: 2,17 GB

Vytvorenie videozáznamu: 11.2.2025

Prevzatie videozáznamu: 1.4.2025

MD5 HASH: 8A3F2E1D7CB4B9120FF9D67A1E8CC2A4

SHA1 HASH: F19D5A4E1B9AC73E2F8E0AB8B3D7C5F5B8DA9113

MD5 checksum: 8A3F2E1D7CB4B9120FF9D67A1E8CC2A4

SHA1 checksum: F19D5A4E1B9AC73E2F8E0AB8B3D7C5F5B8DA9113

Záznam z bezpečnostnej kamery som dostal ešte v ten istý deň, keď som kontaktoval vedenie firmy. Konal som rýchlo. Záznam som okamžite vyzdvihol, overil si jeho integritu, vyhotovil jeho pracovnú kópiu a začal pracovať.

Kamera umiestnená v hlavnej kancelárii zreteľne zaznamenala Martina Molnára, ako o 21:20 prichádza ku svojmu pracovnému stolu. O 21:26 bolo posledné zaznamenané upravenie vírusu na Martinovom PC. O 22:14 bol súbor naposledy otvorený. V obidvoch časoch sa Martin nachádzal v pri svojom PC. To potvrdzuje jeho vinu.

Zoznam veľkých dôkazov v prípade:

Označenie dôkazu	Názov dôkazu / popis	Typ dôkazu	Miesto nálezu	Význam
D0	USB_Image	Obraz USB zariadenia	Serverovňa firmy	Získanie setup.exe a jeho hashu
D1	setup.exe extrahovaný z USB zariadenia	Spustiteľný súbor	USB kľúč nájdený v serverovni	Zhodný hash ako ransomvér z infikovanej siete
D2	SETUP.EXE.pf	Prefetch súbor	PC Martina Molnára	Potvrdzuje spustenie ransomvéru z Martinovho PC
D3	ram_dump.mem	Obraz pamäte RAM (32,9 GB)	PC Martina Molnára	Obsahuje pozostatky ransomvéru, stopy po USB zariadení
D4	CCTV_11_02_2025.mp4	Kamerový záznam	Vedenie firmy	Videozáznam Martina pri počítači v čase útoku
D5	MD5 + SHA1 hash všetkých dôkazov	Overenie integrity	Všetky dôkazy	Potvrdzuje pravosť a nezmenený stav súborov

Zhrnutie prípadu

- Ohlásenie ransomvérového útok na firmu SoftCom Solutions s.r.o.
- Nájdenie USB zariadenia v serverovni firmy
- Prenos USB zariadenia a ostatných dôkazov do laboratória a bezpečné uskladnenie
- Získanie obrazu USB zariadenia a prešetrenie obrazu
- Z USB extrahovaný súbor setup.exe – zhodný hash so škodlivým ransomvérom zo siete
- Vyšetrovanie pracovných PC zamestnancov
- Nájdený prefetch súbor SETUP.EXE.pf na Martinovom PC potvrdzuje spustenie súboru
- Zistenie časov poslednej úpravy a otvorenia prefetch súboru SETUP.EXE
- Získanie RAM obrazu a následné skúmanie
- RAM obraz z Martinovho PC obsahuje pozostatky ransomvéru
- RAM obraz Martinovho PC obsahuje pozostatky z pripojenia USB zariadenia
- Martin sa vyhovára na kolegu, nepriznáva svoju vinu
- Kamerový záznam zo dňa 11. 2. 2025 zachytáva Martina pri práci na PC v čase, kedy bol naposledy nejakým spôsobom upravený a otvorený súbor SETUP.EXE – Martin je vinníkom
- Vyvrátenie ostatných hypotéz

Vyvrátenie/Potvrdenie hypotéz

Hypotéza 1: Hackerská skupina špecializujúca sa na ransomvérové útoky

Prečo je táto hypotéza nepravdivá?

-Analýza skúmaného ransomvéru neukázala zhodu s databázami známych ransomvérových útokov od skupín ako LockBit, REvil, BlackCat a pod.

Hashe získané z USB:

Algorithm	Hash	Path
-----	----	----
SHA1	5019E2F7BE64755383C8B3D5B7947C556E1D77A0	E:\setup.exe

Algorithm	Hash	Path
-----	----	----
MD5	D3B9F0FF9520BA54D272513838D1CE14	E:\setup.exe

Hashe známych ransomvérových vírusov známych skupín:

Black Basta

Algorithm	Hash	Path
-----	----	----
MD5	1559DE4D31B01EAE2B3C4FBF05EF5C4A	E:\Black_Basta_vzorka.exe

Algorithm	Hash	Path
-----	----	----
SHA1	88DEC83F2618FA775C87180753FF9B496666F3BF	E:\Black_Basta_vzorka.exe

LockBit

Algorithm	Hash	Path
-----	----	----
SHA1	9578B45D5A9E99CAE95BE7845681644AE391C836	E:\LockBit_vzorka.exe

Algorithm	Hash	Path
-----	----	----
MD5	12E64891469FCE7D79CAAB048BD8B0E2	E:\LockBit_vzorka.exe

Akira

Algorithm	Hash	Path
-----	----	----
SHA1	28B53835FE92C3FA6E0C422FC3B17C6BC1CB27E0	E:\Akira_vzorka.exe

Algorithm	Hash	Path
-----	----	----
MD5	6C73CC4C494BE8F4E680DE1A20262C8A	E:\Akira_vzorka.exe

-Žiadne stopy po externom prieniku do systému. V sieťových logoch neboli zaznamenané žiadne podozrivé pripojenia z vonkajšej siete v čase predchádzajúcom útoku.

Tento fakt som si overil priamo u tímu správcov siete firmy SoftCom Solutions, ktorý mi emailom zaslal tento report:

Analýza firewall logov, IDS/IPS výpisov a DNS požiadaviek v čase pred incidentom a počas neho (10. 2. – 12. 2. 2025) nepreukázala žiadnu neštandardnú alebo podozrivú sieťovú aktivitu smerujúcu do siete firmy.

Záver hypotézy: Žiadny dôkaz nepodporuje hypotézu o útoku známej ransomvérovej skupiny.

Hypotéza 2: Interný zamestnanec

-Na USB kľúči nájdenom v kancelárii sa nachádzal súbor setup.exe so zhodným hashom ako ransomvér zo siete firmy.

-Prefetch súbor SETUP.EXE.pf na počítači Martina Molnára dokazuje spustenie vírusu z Martinovho PC.

-Pozostatky vírusu boli nájdené aj v RAM obraze z Martinovho PC.

-Kamerový záznam z 11. februára 2025 zachytáva Martina, ako aktívne používa svoj PC v čase, kedy bol vírus naposledy upravený aj otvorený.

Záver hypotézy: Hypotéza potvrdená na základe viacerých dôkazov.

Hypotéza 3: Konkurenčná firma chcela poškodiť firmu alebo získať dáta

Prečo je táto hypotéza nepravdivá?

-Záznamy o úniku dát neexistujú. Nebola zaznamenaná žiadna sieťová aktivita smerom von, ktorá by poukazovala na únik citlivých firemných údajov.

Priamym dôkazom je výpis sieťových logov z firemného servera SoftCom Solutions. Z logov nie je možné nájsť žiadnu neštandardnú komunikáciu smerujúcu von zo siete.

```
# Vypis sietovych spojeni - odchadzajuce spojenia (OUTBOUND)
# Firma: SoftCom Solutions s.r.o.
# Datum: 2025-02-11
# Hostname: WORKSTATION-05
# IP: 192.168.1.45

[16:03:14] 192.168.1.45 -> 8.8.8.8:53 (DNS - Google) ALLOW
[16:08:27] 192.168.1.45 -> 142.250.184.110:443 (www.google.com) ALLOW
[16:20:42] 192.168.1.45 -> 13.107.4.50:443 (www.microsoft.com) ALLOW
[16:37:03] 192.168.1.45 -> 104.18.21.123:443 (cloudflare.com) ALLOW
[17:02:09] 192.168.1.45 -> 40.112.72.205:443 (login.microsoftonline.com) ALLOW
[17:19:51] 192.168.1.45 -> 140.82.121.4:443 (github.com) ALLOW
[18:06:34] 192.168.1.45 -> 172.217.22.14:443 (accounts.google.com) ALLOW
[18:49:12] 192.168.1.45 -> 151.101.129.140:443 (cdnjs.cloudflare.com) ALLOW
[19:24:56] 192.168.1.45 -> 185.199.109.154:443 (raw.githubusercontent.com) ALLOW
[20:03:43] 192.168.1.45 -> 216.58.214.174:443 (drive.google.com) ALLOW
[21:15:19] 192.168.1.45 -> 13.107.6.156:443 (office365.com) ALLOW
[22:30:04] 192.168.1.45 -> 185.60.216.35:443 (msedge.net - cache) ALLOW
[23:11:39] 192.168.1.45 -> 8.8.4.4:53 (DNS - Google backup) ALLOW
[23:47:08] 192.168.1.45 -> 13.224.102.19:443 (aws.amazon.com) ALLOW
```

-Kód ransomvéru neobsahuje backdoor ani funkcionality na export súborov – jeho jediným účelom je zašifrovať obsah disku a žiadať výkupné.

Dôveryhodným dôkazom pre vyvrátenie tohto bodu je správa od môjho kolegu Karola z vyšetrovacieho tímu. Ten si dal tú námahu ransomvér reverzne analyzovať. Tu je jeho správa,

v ktorej popisuje funkcie ransomvéru:

Nástroj použitý: Ghidra (NSA), verzia 10.3

Platforma: Windows x64

Dátum analýzy: 2025-04-06

Analytik: Ing. Karol Kopecký

```
FUN_140001020 -> EncryptDirectory(LPCTSTR path)
- rekurzívne prechadza adresar C:\Users\ a šifruje subory pomocou AES-256
- pouziva kryptograficku kniznicu CryptoAPI (CryptAcquireContext, CryptEncrypt)

FUN_140001410 -> CreateNote(LPCTSTR fileName)
- vytvara README.txt s vykupnym v kazdom zasifrovanom adresari

FUN_140001780 -> DeleteShadowCopies()
- spusta prikaz: vssadmin delete shadows /all /quiet

FUN_140001A10 -> SetWallpaper()
- meni pozadie plochy na subor ransom_bg.bmp

## Neboli detekovane ziadne funkcie typu:
- send(), recv(), connect() (ziadne TCP spojenia)
- WinHttpRequest, WinInet, CURL, FTP funkcie
- fopen/fread/fwrite na vzdialene cesty alebo upload
- ziadne base64, XOR ani socket kodovanie pre exfiltráciu
```

-Neboli zaznamenané žiadne phishingové útoky, ktoré by mohla konkurencia využiť na infiltráciu do siete firmy SoftCom Solutions.

Tu vyšetrovateľom pomohol opäť tím správcov siete, ktorí zaslali toto vyhlásenie:

„Po preverení e-mailovej komunikácie zamestnancov neboli zistené žiadne phishingové pokusy. Neexistuje dôkaz, že by bol ransomvér do systému zavlečený prostredníctvom e-mailu.“

Záver hypotézy: Neexistuje žiadny dôkaz o tom, že by išlo o útok zo strany konkurencie. Útočník nemal záujem o údaje, len o výkupné.

Hypotéza 4: Náhodný plošný útok skupiny alebo jednotlivca

Prečo je táto hypotéza nepravdivá?

-Ransomvér bol spustený lokálne zo zariadenia pripojeného cez USB. To je v rozpore s typickým plošným útokom.

Jasným potvrdením tohto bodu je nájdenie dôkazu o pripojení USB zariadenia do PC Martina Molnára.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
3A84BEFC0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
3A84BEFD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
3A84BEFE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
3A84BEFF0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
3A84BF000	68	62	69	6E	00	90	08	00	00	10	00	00	00	00	00	00	hbin.....
3A84BF010	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
3A84BF020	88	FF	FF	FF	6E	6B	20	00	DA	33	A9	C2	D6	8B	DB	01	...`nk .ú3@ÃÖ<Ů.
3A84BF030	03	00	00	00	48	64	06	00	06	00	00	00	00	00	00	00	Hd.....
3A84BF040	C0	92	08	00	FF	FF	FF	FF	00	00	00	00	FF	FF	FF	FF	R'.....
3A84BF050	58	BB	01	00	FF	FF	FF	FF	70	01	00	00	00	00	00	00	X»...`p.....
3A84BF060	00	00	00	00	00	00	00	00	00	00	00	00	26	00	00	00	&...
3A84BF070	7B	37	66	31	30	38	61	32	38	2D	39	38	33	33	2D	34	{7f108a28-9833-4
3A84BF080	62	33	62	2D	62	37	38	30	2D	32	63	36	62	35	66	61	b3b-b780-2c6b5fa
3A84BF090	35	63	30	36	32	7D	00	00	F8	FE	FF	FF	6E	6B	20	00	5c062}..řť`nk .
3A84BF0A0	DA	33	A9	C2	D6	8B	DB	01	03	00	00	00	20	90	08	00	ú3@ÃÖ<Ů.....
3A84BF0B0	01	00	00	00	00	00	00	00	E0	8F	08	00	FF	FF	FF	FF	řŽ.....
3A84BF0C0	01	00	00	00	D8	8F	08	00	58	BB	01	00	FF	FF	FF	FF	ŘŽ..X».....
3A84BF0D0	02	00	00	00	00	00	00	00	1C	00	00	00	1C	01	00	00	
3A84BF0E0	00	00	00	00	B8	00	00	00	23	23	3F	23	53	54	4F	52	,##?#STOR
3A84BF0F0	41	47	45	23	56	6F	6C	75	6D	65	23	5F	3F	3F	5F	55	AGE#Volume#??_U
3A84BF100	53	42	53	54	4F	52	23	44	69	73	6B	26	56	65	6E	5F	SBSTOR#Disk&Ven
3A84BF110	4B	69	6E	67	73	74	6F	6E	26	50	72	6F	64	5F	44	61	Kingston&Prod_Da
3A84BF120	74	61	54	72	61	76	65	6C	65	72	5F	33	2E	30	26	52	taTraveler 3.0&R
3A84BF130	65	76	5F	50	4D	41	50	23	30	38	36	30	36	45	36	44	ev_PMAP#08606E6D
3A84BF140	34	31	38	41	42	45	42	31	36	37	31	37	35	42	41	33	418ABEB167175BA3
3A84BF150	26	30	23	7B	35	33	66	35	36	33	30	37	2D	62	36	62	&0#{53f56307-b6b
3A84BF160	66	2D	31	31	64	30	2D	39	34	66	32	2D	30	30	61	30	f-11d0-94f2-00a0
3A84BF170	63	39	31	65	66	62	38	62	7D	23	7B	37	66	31	30	38	c91efb8b}#{7f108
3A84BF180	61	32	38	2D	39	38	33	33	2D	34	62	33	62	2D	62	37	a28-9833-4b3b-b7
3A84BF190	38	30	2D	32	63	36	62	35	66	61	35	63	30	36	32	7D	80-2c6b5fa5c062}
3A84BF1A0	E0	FE	FF	FF	53	00	54	00	4F	00	52	00	41	00	47	00	řť`S.T.O.R.A.G.
3A84BF1B0	45	00	5C	00	56	00	6F	00	6C	00	75	00	6D	00	65	00	E \ V o l u m e

-Žiadne iné firmy v rovnakom čase neboli napadnuté týmto ransomvérom. V prípade plošného útoku by boli zaznamenané ďalšie podobné incidenty.

Záver hypotézy: Nešlo o náhodný plošný útok.

Chain of custody obrazu operačnej pamäte Martinovho PC:

Číslo:	02	Typ súboru:	.mem	Obnovený súbor:	Nie	Veľkosť:	32,9GB
Popis prípadu:		Kybernetický útok na firmu SoftCom Solutions					
Názov súboru:		ram_dump.mem					
Miesto získania digitálnej stopy:		Kancelária firmy SoftCom Solutions					
Poznámky:		Kópia obrazu RAM pamäte Martinovho PC spravená pomocou FTK® Imager 4.7.3.81, skúmaná pomocou HxD					
Časové pečiatky							
Access:	16.3.2025 15:27:10		Modify:	16.3.2025 15:27:10		Change:	-
Digitálny odtlačok (heš)	MD5	162C75B966A4995C01126C74FD9429C0					
	SHA1	579921EA78863BAED9AAB537CCF5BEBE50D9E3B3					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
16.3.2025 15:27:10		Vyhotovenie obrazu RAM pamäte					
16.3.2025 16:47:53		Vyťažovanie informácií z obrazu RAM pamäte					
16.3.2025 16:52:18		Overenie integrity obrazu RAM					
16.3.2025 17:25:29		Uloženie obrazu RAM do trezoru k ostatným dôkazom					

Štúdie:

<https://dfrws.org/presentation/duck-hunt-memory-forensics-of-usb-attack-platforms/>

Štúdia sa zameriava na forenznú analýzu USB útokov v systéme Windows 10, skúma zariadenia Hak5 USB Rubber Ducky a Bash Bunny. Autori vyvinuli plugíny pre Volatility, usbhunt a dhcphunt, ktoré dokážu z pamäte systému extrahovať jedinečné identifikátory zariadení, diagnostické udalosti ovládačov a DHCP logy. Výsledky ukazujú, že niektoré indikátory kompromitácie (IOCs) zostávajú v pamäti aj 24 hodín po útoku, čo umožňuje ich neskoršiu analýzu.

https://dfrws.org/presentation/volgpt-evaluation-on-triaging-ransomware-process-in-memory-forensics-with-large-language-model/?utm_source=chatgpt.com

Štúdia volGPT predstavuje novú metódu na identifikáciu ransomvérových procesov v pamäťových dumpoch pomocou veľkého jazykového modelu (LLM) a nástroja Volatility. Experimenty ukázali, že volGPT je presnejší a rýchlejší pri detekcii ransomvéru než existujúce metódy. Táto metóda poskytuje lepšie vysvetlenia pri analýze ransomvéru.