

Krádež SSD z firmy

Vladyslav Mykhailovskyi

Opis prípadu:.....	2
5WH.....	2
Hypotézy:.....	3
Typ analyzovanej digitálnej stopy:.....	4
Použitý dataset: http://roussev.net/t5/t5.html	4
Bitové kópie:.....	4
Informácie o skúmanom zariadení:.....	4
Použité nástroje:.....	5
Bezpečnostné opatrenia:.....	7
Záver.....	11
Literatúra.....	12

[Prezentacia](#)

Opis prípadu:

Spúšťajú sa bezpečnostné alarmy v **Neuron Dynamics**, špičkovom výskumnom startupe AI. Spoločnosť sa špecializuje na kvantové šifrovanie a nedávne prelomy v ich modeloch strojového učenia vzbudili záujem konkurentov a dokonca aj zahraničných subjektov.

Bezpečnostné zábery ukazujú že **maskovaný zlodej** prešiel cez poplašný systém a vnikol do serverovne. Po jeho odchode sa ďalšie dni zistí, že bolo ukradnuté iba jedno SSD. Polícia ho našla v odpadkovom koši na druhý deň vedľa stanice metra

Ciele:

- **Detekcia manipulácie** – skontrolovať, či sa na nej nenachádzajú známky manipulácie s údajmi, šifrovanie alebo pokusov o prepísanie údajov.
- **Sledovanie súborov** – identifikovať ku ktorým suborom sa pristupovalo, skopírovali alebo odstránili pred stratou SSD.
- **Obnova dát** – Zistiť, či je možné obnoviť nejaké dáta, aj keď bol SSD naformátovaný alebo čiastočne vymazaný.
- **Identifikácia používateľa** – extrahovať metadáta, protokoly alebo akékoľvek identifikovateľné informácie, ktoré by mohli viesť k páchatelovi.

5WH

Who(Kto?)

- Podozrivý je neznámy, ale zdá sa, že má pokročilé znalosti o bezpečnostnom systéme Neuron Dynamics.

What(Čo?)

- Zo serverovej miestnosti bol ukradnutý vysokohodnotný NVMe SSD s označením Project Eclipse.
- SSD disk neskôr našli rozbitý v odpadkovom koši v metre.

When(Kedy?)

- Ku krádeži došlo 28.2.2025 o 2:47, keď bola bezpečnosť minimálna.
- SSD disk našli o dva dni neskôr neďaleko stanice metra.

Where(Kde?)

- Zločin sa odohral v zabezpečenej serverovej miestnosti Neuron Dynamics.
- SSD disk neskôr objavili vo verejnom odpadkovom koši neďaleko rušnej stanice metra.

Why(Prečo?)

- SSD obsahoval citlivé vlastníctvo súvisiace s AI.
- Medzi možné motívy patrí **firemná špionáž**, **sabotáž** alebo **neúspešná lúpež**.

How(Ako?)

- Zlodej obišiel biometrické zabezpečenie pomocou klonovaného RFID odznaku.
- Použitá tepelná kamufláž, aby sa zabránilo infračerveným senzorom.
- SSD bol neskôr rozbitý, možno na zničenie dôkazov alebo zavádzanie vyšetrovateľov.

Hypotézy:

1) Firemná špionáž (ukradnutá a skopírovaná pred zničením)

Konkurenčná spoločnosť alebo zahraničný subjekt najali zlodeja, aby ukradol disk. Údaje SSD mohli byť klonované na iný disk predtým, ako boli rozbité. Zničenie SSD mohlo byť spiestrením, aby to vyzeralo ako nevydarená krádež.

2) Insider sabotáž (zakrytie úniku)

Zamestnanec Neuron Dynamics unikol údaje a zinscenoval krádež. Zničenie SSD malo skryť dôkazy o neoprávnenom prístupe k dátam.

3) Neúspešná lúpež (zlodej sa vystrašil)

Zlodej plánoval ukradnúť a predať SSD, ale spanikáril a zničil ho, keď si uvedomil, že sa k nemu blíži polícia. Jednotka SSD sa mohla pri úteku náhodne poškodiť.

Typ analyzovanej digitálnej stopy:

Rôzne datové typy - .HTML, .DOC, .PDF, .PPT, .XLS, .TXT, .JPG, .JPEG, .GIF

Logy - Skontrolované predchádzajúce logy, aby sa zistil čas strávený manipuláciou s údajmi zo strany zlodēja

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

Bitové kópie:

- Bitová kópia SSD bola vytvorená na počítači umiestnenom v serverovej miestnosti forenznej analýzy na ďalšie preskúmanie
- Druhá bitová kópia bola uložená na externom pevnom disku

Udaje o bitovej kopii:

Case Information:

Acquired using: ADI4.7.3.81

Case Number: case1

Evidence Number: 001

Unique description: case

Examiner: Vladyslav Mykhailovskyi

Notes:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 124,519

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 2,000,409,264

[Physical Drive Information]

Drive Model: Micron_3400_MTFDKBA1T0TFH

Drive Serial Number: 0000_0000_0000_0001_00A0_7521_32DF_DA0D.

Drive Interface Type: SCSI

Removable drive: False

Source data size: 976762 MB

Sector count: 2000409264

[Computed Hashes]

MD5 checksum: ace188923fe87679511a25b82ab9e270

SHA1 checksum: d41a7135832b191131a5df931301c1d22952cf83

Image Information:

Acquisition started: Mon Mar 17 13:56:56 2025

Acquisition finished: Mon Mar 17 14:05:11 2025

Image Verification Results:

Verification started: Mon Mar 17 14:05:11 2025

Verification finished: Mon Mar 17 14:06:14 2025

MD5 checksum: ace188923fe87679511a25b82ab9e270 : verified

SHA1 checksum: d41a7135832b191131a5df931301c1d22952cf83 : verified

Informácie o skúmanom zariadení:

Micron_3400_MTFDKBA1T0TFH

SSD bol v tranzite medzi systémami. Pred krádežou bol pravdepodobne ponechaný na pracovnej stanici alebo v zabezpečenej skrinke.



Fizicke vlastnosti:

Značka a model: Micron 3400 MTFDKBA1T0TFH (1TB)

Rozhranie: PCIe 4.0 x4 (NVMe 1.4)

Ovládač: Micron DM02A1

Typ NAND: 176-vrstvová TLC NAND Flash

Podpora šifrovania: hardvérové šifrovanie AES-256 (povolené)

Kapacita: 1 TB

Faktor tvaru: M.2 2280

Výdrž (TBW): 600 TB

Rychlost:

All	5 ▾	8GiB ▾	C: 88% (817/929GiB) ▾	MB/s ▾
	Read (MB/s)		Write (MB/s)	
SEQ1M Q8T1	6357.34		3868.54	
SEQ1M Q1T1	2723.97		3735.86	
RND4K Q32T1	390.22		297.23	
RND4K Q1T1	33.35		138.47	

Použité nástroje:

FTK Imager 4.7.3.81 - nástroj na vytvorenie obrazov disku a RAM

HxD - nástroj na preskúmanie obrazu RAM

Autopsy 4.22.0 - nástroj na prehliadanie a analýzu obrazov diskov

CrystalDiskMark 8 - nástroj na meranie rýchlosti pevného disku

Chain of custody:

Číslo		Typ Súboru	Folder	Obnovený súbor	Ano	Veľkosť	1,176,419 KB
Popis prípadu		Krádež SSD z firmy					
Názov súboru		t5					
Miesto získania digitálnej stopy		serverová miestnosť Neuron Dynamics					
Poznámky							
Digitálny otlačok (hash)	MD5	ad1a2534f17bc4cdf1bf7aae8dbb1bc7					
	SHA1	ab623335e152b73f2cbdf6249ad929d8acf37ff2					
Časova pečiatka		Akcia vykonaná s digitálnou stopou					
Pondelok 17 Marca 13:56:56 2025		Logovacie súbory prístupu k súboru zip boli rovnaké ako v čase zločinu					
Pondelok 17 Marca 13:57:07 2025		Výber hashu pre budúce preskúmanie súborov					
Pondelok 17 Marca 14:05:11 2025		Odosielanie podľa výsledného hash					

Vyšetrovanie dôkazov

Uskutočnil sa hĺbkový prieskum reťazca "delete". Našlo sa 16 výsledkov

Checksum	Search (16 hits)	
Offset	Excerpt (hex)	Excerpt (text)
21F4AF3A	78 00 00 00 00 00 46 61 69 6C 65 64 20 74 6F 20 64 65 6C 65 74 65 20 25 53 2C 20 65 72 72 6F 72	x.....Failed to delete %S, error
21F83131	00 01 00 07 03 00 CA 00 00 00 2D 00 00 00 FF FE 44 65 6C 65 74 65 20 49 66 20 46 75 6C 6C 1A 00	Ë...ÿDelete If Full..
21F8F77D	65 73 10 00 00 80 00 00 00 00 00 00 00 FF FE 44 65 6C 65 74 65 20 49 66 20 46 75 6C 6C 3A 00	es...Ë...ÿDelete If Full..
21F8F7A0	00 02 00 0F 04 00 1E 00 00 00 08 00 00 00 FF FE 44 65 6C 65 74 65 20 49 66 20 46 75 6C 6C 04 00	ÿDelete If Full..
21F80DCE	75 6C 74 21 0A 00 46 61 69 6C 65 64 20 74 6F 20 64 65 6C 65 74 65 20 22 25 53 22 2C 20 65 72 72	ult!..Failed to delete "%S", err
22008F81	00 01 00 07 03 00 CA 00 00 00 2D 00 00 00 FF FE 44 65 6C 65 74 65 20 49 66 20 46 75 6C 6C 1A 00	Ë...ÿDelete If Full..

Spomedzi nich sa nepodarilo odstrániť 3 súbory a zvyšok bol odstránený úspešne

```
21F4AF30 46 61 69 6C 65 64 20 74 6F 20 64 65 6C 65 74 65 Failed to delete
21F4AF40 20 25 53 2C 20 65 72 72 6F 72 3A 30 78 25 78 00 %S, error:0x%x.

21F8F770 00 00 80 00 00 00 00 00 00 00 00 00 FF FE 44 65 6C ..Ë.....ÿDel
21F8F780 65 74 65 20 49 66 20 46 75 6C 6C 3A 00 1E 00 0A ete If Full:....
21F8F790 00 02 00 0F 04 00 1E 00 00 00 0B 00 00 00 FF FE .....ÿ
21F8F7A0 44 65 6C 65 74 65 20 49 66 20 46 75 6C 6C 04 00 Delete If Full..
21F8F7B0 00 80 00 00 00 00 00 00 00 00 00 2D 00 31 00 2A 00 .Ë.....-..l.*.
```

Ďalšie vyhľadávanie sa týkalo reťazca „log“, aby sa skontrolovali existujúce protokoly a zistil sa čas, ktorý zlodej strávil vo vnútri.

Checksum	Search (1692 hits)	
Offset	Excerpt (hex)	Excerpt (text)
47AF952	57 69 74 68 46 6C 61 67 73 00 42 63 64 53 65 74 4C 6F 67 67 69 6E 67 00 42 63 64 53 65 74 53 79	WithFlags.BcdSetLogging.BcdSetSy
48CC1C5	52 F8 B7 04 08 14 6D A3 75 D1 59 94 94 A5 13 2F 6C 4F 47 35 34 91 B1 6B C3 3F 28 DF E8 D7 3F 21	Rø...mEuŇV""¥./IOG54!±kÃ?(Bèx?!
48A2B6B	54 F5 26 5F 10 EB 4C 27 48 5A 3D CF 91 16 C5 6E 4C 4F 47 5A C5 74 6C A4 D1 F3 4A 69 76 FD 12 88	Tö...ēL'HZ=Ŧ.Ān LOGZĀtlpŇoJivý."
4C91632	3B 4C 0A 92 22 46 1B DF C4 A9 BD D5 13 24 39 F6 6C 6F 67 13 DA 33 8D 4F EA DB 4A 7B D9 4A 00 BE	;L.""F.BĀ@½Ö.S9ølog.Ú3.OēŬJ(ŬJ.¼
547B0A7	F7 F9 E5 0A 74 71 46 D0 F1 65 E6 EA 25 5D 0B 3A 6C 4F 67 74 2D 1E 5E D3 60 B5 18 32 5E FA F6 21	÷ûā.tqFDñææé%].IOgt-.^Ŏµ.2^úö!
549438A	FF 71 A4 85 EA E7 33 01 63 D6 96 03 D6 2F 92 5A 4C 4F 47 B9 B1 7E 95 6D 83 05 86 C9 0B B2 CF 69	ÿq#...ēç3.cÖ-.Ö/'ZLOG¹±~*mf,tĚ.Ŧi

Našlo sa 1692 výsledkov. Medzi nimi sa nenašiel záznam o dátume činu. Pravdepodobne zlodej nič nerobil.

000108.jpg			2011-02-08 15:37:52 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	137413
000109.jpg			2011-02-08 15:37:52 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	31046
000110.jpg			2011-02-08 15:37:52 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	92856
000111.doc			2011-02-08 15:37:52 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	376832
000112.doc			2011-02-08 15:37:52 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	296370
000113.doc			2011-02-08 15:37:54 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	14170112
000114.doc			2011-02-08 15:37:54 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	19968
000115.doc			2011-02-08 15:37:54 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	179712

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContextAnnotationsOther Occurrences

0°117%Reset



Medzi uvedenými obrázkami bola mladá žena ktorá je pracovníčkou spoločnosti

000123.doc			2011-02-08 15:37:54 CET
000124.doc			2011-02-08 15:37:54 CET
000125.doc			2011-02-08 15:37:54 CET
000126.doc			2011-02-08 15:37:56 CET
000127.doc			2011-02-08 15:37:56 CET
000128.doc			2011-02-08 15:37:56 CET
000129.doc			2011-02-08 15:37:56 CET
000130.doc			2011-02-08 15:37:56 CET

HexTextApplicationFile MetadataOS AccountData Artifacts

StringsExtracted TextTranslation

Page: 1 of - PageMatches on page: - of - Match

PAGE
Page 1 of 22

FORT MYERS BEACH
TOWN COUNCIL
Town Hall- Council Chambers

2523 Estero Boulevard

Ft. Myers Beach, Fl 33931
Special Meeting

000123.doc				2011-02-08 15:37:54 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST
000124.doc				2011-02-08 15:37:54 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST
000125.doc				2011-02-08 15:37:54 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST
000126.doc				2011-02-08 15:37:56 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST
000127.doc				2011-02-08 15:37:56 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST
000128.doc				2011-02-08 15:37:56 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST
000129.doc				2011-02-08 15:37:56 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST
000130.doc				2011-02-08 15:37:56 CET	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST	2025-04-04 15:47:15 CEST

Hex	Text	Application	File Metadata	OS Account	Data Artifacts	Analysis Results	Context	Annotations	Other Occurrences
Strings									
Extracted Text									
Translation									
Page: 1 of - Page									
Matches on page: - of - Match									
100%									
Reset									
Members Present: Councilman Garr Reynolds, Vice Mayor Don Massucco, and Mayor Dennis Boback. Absent: Councilman Bill Shenko, Jr. Councilman Charles Meador, Jr. Town Staff Present: Town Attorney Anne Dalton, Town Manger Rachel Lambert, Community Development Director Jerry Murphy and Public II. PLEDGE OF ALLEGIANCE AND INVOCATION: All present stood for the recitation of the Pledge of Allegiance. III. INVOCATION: Town Manager Rachel Lambert gave the invocation. IV. PUBLIC COMMENT: Mayor Boback opened public comment · Pat McKalan, 2532 Estero Blvd., right across the street. He asks Council to consider taking some remedial action to somehow reduce the eff area of Diamondhead to just south of Red Coconut, we are covered with a form of sludge. I call it that because it is a decomposition of the ve close to the beach or walk on the beach, or have anything to do with the beach. Basically, we are at the point now where that area of the l into the water, you wouldn't want to be in it. Part of the problem that we are asking you to address is that hasn't gone away due to rain or t a high tide and was wind driven from the south as we caught the backside of Alberto passing by. So it drove it very high on the beach. Se t to dissolve it but as to pack it down and to cause a crust form on top of it; plus there are large lumps five to six inches in diameter that are ss this issue. we are not asking that you violate your own Town ordinances by raking it or trving to actually remove. but if you could possibl									

Bola prítomná na mimoriadnom stretnutí

Bezpečnostné opatrenia:

Overenie hash (SHA-256, MD5) bolo vykonané, aby sa potvrdilo, že po obnovení SSD
nedošlo k žiadnej manipulácii. Tiež vytvorenie forenzej kópie obnoveného SSD pomocou
FTK Imager

Dokumentácia spotrebiteľského reťazca:

Dodržiaval sa prísny protokol o úschove, ktorý dokumentoval každý vykonaný forenzný
krok. Všetky forenzné kópie SSD boli uložené v zabezpečenom trezore, aby sa zabránilo
kontaminácii. Bola vytvorená podrobná správa o incidente a zdieľaná s orgánmi činnými v
trestnom konaní v oblasti kybernetickej bezpečnosti.

Kontrola prístupu:

Snímače odtlačkov prstov a sietnice obmedzujú prístup do kritických oblastí.

Záver

Žena sa nechcela podeliť o dôležitú informáciu, ktorú našla na SSD. Vedela, že to nemôže vymazať, lebo logy sú neustále kontrolované, potom si najala maskovaného muža, aby ukradol vopred pripravené SSD a zlikvidoval ho. Muž si nebol istý, kde ho nechať a zvolil variantu vyhodit' ho

Hypotéza 1: Firemná špionáž

Údaje boli osobné a netýkali sa konkrétnej nepriateľskej spoločnosti

Výsledok: **Nepotvrdila sa**

Hypotéza 2: Insider sabotáž

Žena bola spolupracovníčkou spoločnosti. Úmyselne sa snažila zbaviť sa údajov

Výsledok: **Potvrdila sa**

Hypotéza 3: Neúspešná lúpež

Maskovaného muža zamestnal pracovník firmy. Nemal za cieľ predávať SSD

Výsledok: **Nepotvrdila sa**

Literatúra

How to perform SSD Forensics | Part — I

Tento výskum predstavuje základy forenznej analýzy pevných diskov (SSD). Skúma výzvy, ako je vyrovňavanie opotrebovania, TRIM a zber odpadu, ktoré komplikujú obnovu dát.

Dokument tiež poskytuje metodológie a nástroje používané pri forenznom vyšetrowaní SSD

<https://medium.com/@songchai.d01/how-to-perform-ssd-forensics-part-i-1158dd3975e8>

Solid State Drive Forensics: Where Do We Stand?

Tento dokument skúma súčasný stav forenznej analýzy SSD, pričom zdôrazňuje pokroky a obmedzenia v obnove dát a forenznych technikách. Diskutuje o vplyve architektúry SSD na tradičné forenzne metódy a predstavuje potenciálne riešenia na prekonanie problémov s nestálosťou údajov.

<https://markscanlon.co/papers/SSDForensics.pdf>

Digital Forensic Practices and Methodologies for AI Speaker Ecosystems

Tento výskum skúma forenzné techniky pre inteligentné reproduktory poháňané AI, ako sú Amazon Echo a Google Home. Skúma dátové úložiská, komunikačné protokoly a potenciálne forenzné artefakty. Štúdia tiež diskutuje o výzvach pri extrakcii a analýze hlasových interakcií pri zabezpečení integrity údajov a súkromia.

<https://dfrws.org/presentation/diaganalyzer-user-behavioranalysis-and-visualization-using-windows-diagnostics-logs/>