

Únik výrobnéj stratégie pre batériový modul

Samuel Csomor

Prezentácia:

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

Prípad:

Firma MotionNextGroup je dlhoročný výrobca komponentov do automobilov so spaľovacím motorom. Vzhľadom na dopyt po elektrických autách sa firma rozhodla vytvoriť stratégiu na nasledujúce roky a hľadať komponenty, ktoré by mohli dodávať.

Firma vytvorila stratégiu pre batériový modul a udržiavala ju v tajnosti pred oficiálnym uvedením na trh a nájdením potenciálnych odoberateľov. Avšak konkurencia začala prezentovať batériový model, ktorý bol totožný s modelom firmy MotionNextGroup.

Firma používa svoje vlastné servery a komunikácia je šifrovaná. Stratégiu, poznalo len pár zamestnancov, ktorí mali na starosť jej vývoj.

Firma MotionNextGroup najala tím forenzných analytikov, aby prešetrili možný únik informácií, analyzovali dostupné digitálne dôkazy a identifikovali prípadného páchatela alebo spôsob úniku dát. Celá stratégia pre batériový modul bola uložená len na jednom zariadení. Zariadenie je izolované od internetovej aj lokálnej siete. Firma poskytla plný prístup a povolenie k prehľadaniu digitálnych stôp na zariadení za dohľadu ich pracovníkov z IT oddelenia. Taktiež firma MotionNextGroup je ochotná poskytnúť kamerový záznam, ktorý sleduje dané zariadenie.

Typ digitálnej stopy:

Zariadenie na ktorom sa nachádza daný batériový model.

Videozáznam z bezpečnostných kamier.

5 WH:

Kto: Zamestnanec/zamestnanci MotionNextGroup alebo externá osoba, ktorá mala prístup k stratégií batériového modulu.

Prešetrovanie kamerového záznamu a informácie zo zariadenia by malo odhaliť podozrivého zamestnanca/zamestnancov alebo externá osoba.

Čo: Stratégia pre batériový model.

Kedy: Presný čas incidentu nie je vopred známy, preto forenzný tím analytikov vykoná koreláciu časových údajov – videozáznam s bezpečnostných kamier a systémové logy zariadenia.

Kde: Vo firme MotionNextGroup, v kancelárskom priestore kde sa nachádzalo zariadenie obsahujúce stratégiu pre batériový model.

Firma nás ubezpečila, že údaje boli uložené výhradne na tomto zariadení a neboli distribuované v žiadnych iných systémoch firmy. Preto sa forenzný tím analytikov zameria na toto konkrétne zariadenie.

Prečo: Zamestnanec/zamestnanci alebo externá osoba mohla predať stratégiu za účelom obohatenia alebo z rôznych osobných motívov.

Budeme pracovať rôznymi verziami motívov a postupne ich vylučovať.
Výsluchom podozrivých páchateľov, by sme sa mali dopracovať ku skutočnému motívu.

Ako: Pravdepodobne pripojením USB zariadenia (USB kľúč alebo externý disk)

Skúmaním záznamu z bezpečnostných kamier a histórie logov by sme mali zistiť spôsob, akým páchateľ vyviezol citlivé údaje z firmy.

1. Hypotéza:

Zamestnanec/zamestnanci alebo externá osoba, odcudzila údaje s účelom ich následného predaja alebo iného osobného zisku a ponúkla ich konkurencii.

2. Hypotéza:

Zamestnanci/zamestnanec vyviezol citlivé údaje z firmy, a následne sa k nim mohli dostať iné osoby bez jeho vedomia, ktoré tieto údaje poskytl konkurencii.

3. Hypotéza:

Firma MotionNextGroup úmyselne poskytla svoje citlivé údaje konkurencii za účelom ich diskreditácie a poškodenia reputácie.

Ciele vyšetrovania:

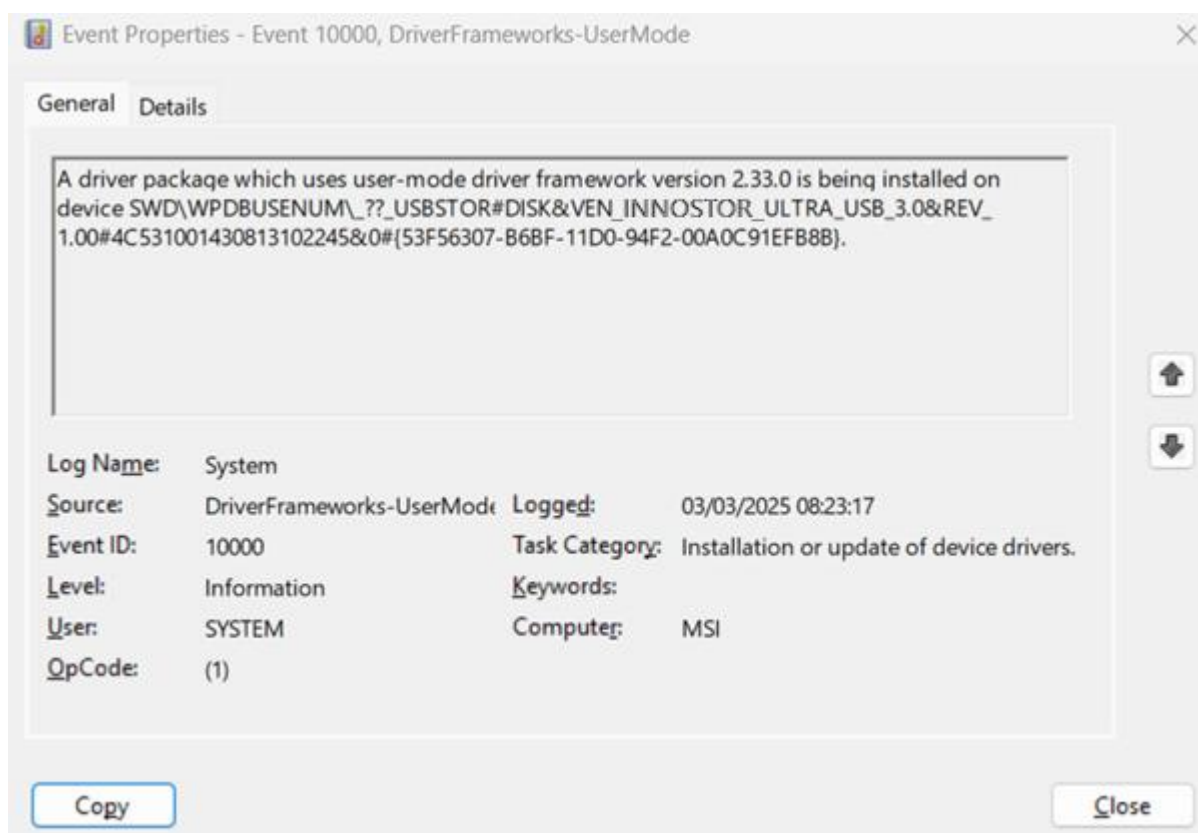
Identifikovať zdroj úniku – zistiť, ktorý zamestnanec/zamestnanci alebo externá osoba mala prístup k citlivým údajom.

Vyšetrenie možného kontaktu – zistiť či existuje nejaká forma komunikácie medzi zamestnancom/zamestnancami a konkurenciou. V prípade tretej osoby zistiť jej spojenie či už s konkurenciou alebo zamestnancom.

Motívy páchatela/páchateľov – zistiť, či išlo o finančnú odmenu alebo tam bol iný záujem.

Vytažovanie Digitálnych dôkazov a stôp

Prvý získaný digitálny dôkaz



Obr. č. 1 Event Log, kde bolo pripojené USB

Po prehladaní poskytnutých systémových logov od spoločnosti MotionNextGroup - a to výhradne pod dohľadom jej IT oddelenia - sa forenznému tímu podarilo identifikovať udalosť, v ktorej bol k notebooku pripojený externé médium, konkrétne USB kľúč.

Z tohto logu sa podarilo zistiť:

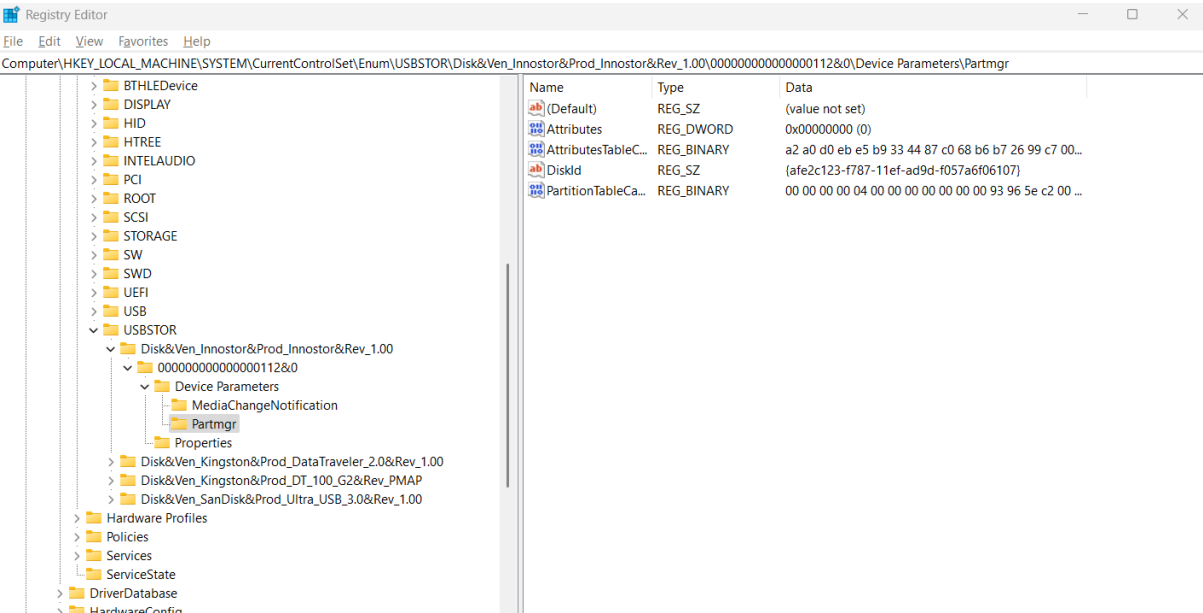
Prvý kontakt zariadenia

– Event ID 10000 pri DriverFrameworks-UserMode sa zaznamenáva vtedy, keď Windows

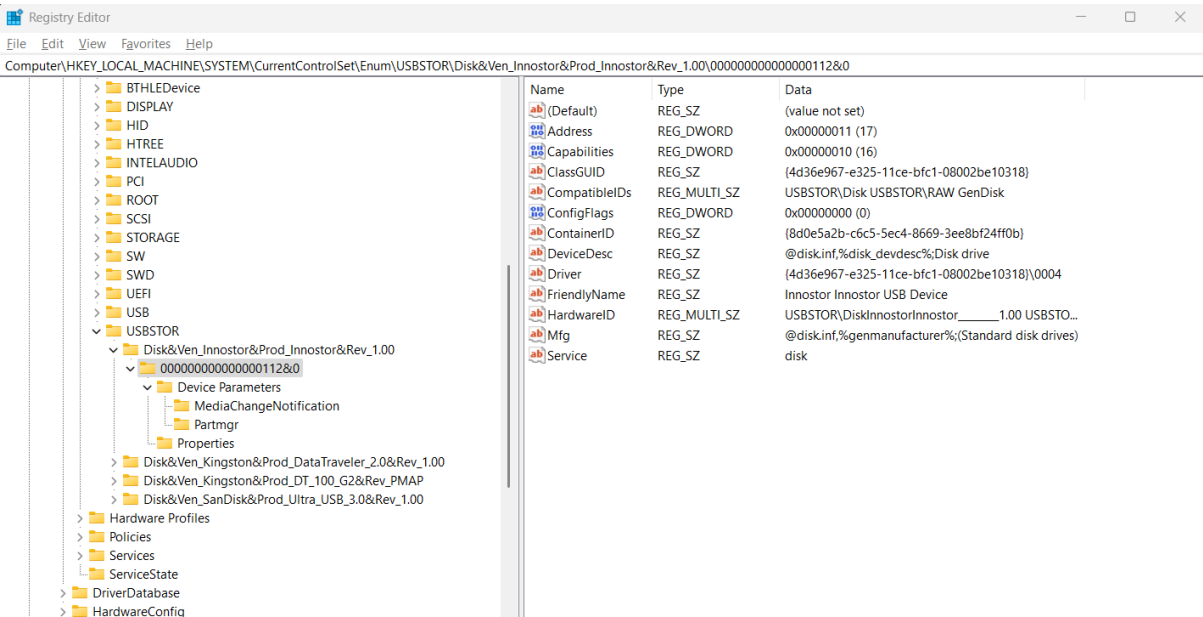
prvýkrát zaregistruje hardvér alebo nainštaluje/aktualizuje jeho ovládač. Z toho vyplýva, že USB kľúč nebol na počítači používaný pred 3. marcom 2025.

Kritický časový úsek

– 08:23 UTC je bod, okolo ktorého treba pozrieť kamerový záznam.



Obr. č.2 Dôkaz pripojenia cudzieho USB zariadenia



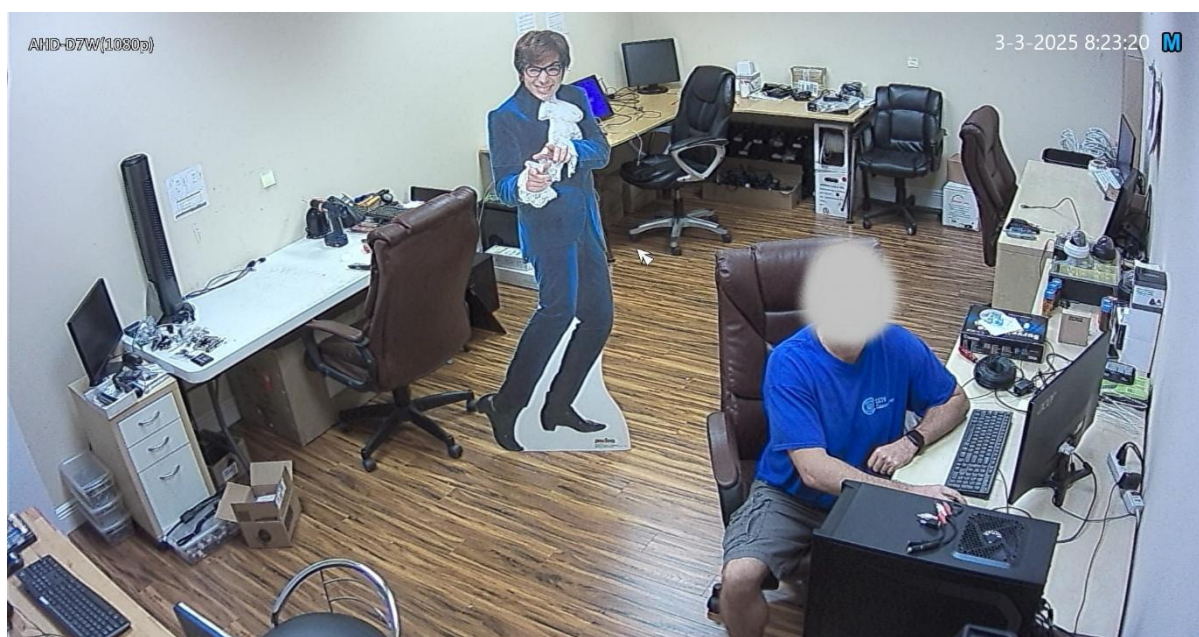
Obr. č.3 USB Innoston.

Prehľadali sme aj Register editor a našli sme záznamy v nasledujúcich kľúčoch, ktoré potvrdzujú pripojenie externého zariadenia, konkrétne USB kľúča "Innostor Usb Device":

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\USBSTOR\Disk&Ven_Innostor&Prod_Innostor&Rev_1.00\0000000000000000112&0: Tento kľúč obsahoval detailné informácie o konkrétnej inštancii pripojeného USB kľúča, vrátane identifikátorov výrobcu (Ven_Innostor) a produktu (Prod_Innostor).

Tieto záznamy v Editore registrov poskytujú dodatočné dôkazy o pripojení USB kľúča k analyzovanému notebooku a dopĺňajú informácie získané z logov operačného systému.

Druhý získaný digitálny dôkaz



Obr. č. 4 Obráz z kamerového záznamu

Vďaka informáciám získaných z Event Logov, hlavne času – 03/03/2025 o 08:23:17 UTC – sa podarilo odhaliť podozrivého páchatel'a, ktorého firma MotionNextGroup identifikovala ako ich zamestnanca – Pavol Nový.

Na tomto základe bol vybavený súdny príkaz na vydanie USB kľúča od podozrivého zamestnanca – Pavol Nový. Pri zaistení USB kľúča bola vyhotovená podrobná fotodokumentácia a zoznam všetkých údajov, ktoré sa týkajú zariadenia. USB kľúč bol zabezpečený v špeciálnom obale na ochranu pred akýmkoľvek fyzickým poškodením alebo zneužitím. Po zabezpečení a dokumentovaní zariadenia bol USB kľúč pripojený

iba k špecializovaným zariadeniam na forenznú analýzu, aby sa zabránilo akémukoľvek nezabezpečenému prístupu. Počas celého procesu boli uplatnené prísne bezpečnostné opatrenia. Forezný tím vyhotovil tri kópie a začal na nich hľadať relevantné dôkazy. Súčasne bola z forezného hľadiska vyhotovená kópia videozáznamu, na ktorom je zachytený Pavol Nový v čase 08 : 23 – 08 : 30 UTC, ako vkladá USB kľúč do notebooku s dôverným dokumentom.

Tretí získaný digitálny dôkaz



Obr. č. 5 USB zariadenie použité pri odcudzení dát

Technické parametre USB flash disku

Model	Innoston USB Device (pravdepodobne s čipom Innoston IS916 alebo IS917)
--------------	--

Kapacita	~4 GB
Rozhranie	USB 3.0
Typ pamäte	TLC NAND Flash
Životnosť	okolo 500 - 1 500 prepisovacích cyklov
Rozmery	6 x 2,8 x 1 cm
Rýchlosť čítania	50 - 100 MB/s
Rýchlosť zápisu	15 - 30 MB/s
Prístupová doba čítania	~0,3 - 0,8 ms
Prístupová doba zápisu	~1 - 3 ms

Kopia USB kľúča bola vytvorená v Exterro® FTK® Imager 4.7.3.81

Čas vytvorenia: Mon Mar 16 10:25:21 2025

Počet kópii: 3

MD5 hash: 366eb0013b2ccb76f88031fffb5487b3

SHA: 3a700ad8bcf351291dc8132cfce9cb239f2db968

Počet súborov :6758

Cylinders: 489

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 7,864,320

[Physical Drive Information]

Drive Model: Innostor Innostor USB Device

Drive Serial Number: 000000000000000112

Drive Interface Type: USB

Removable drive: True

Source data size: 3840 MB

Sector count: 7864320

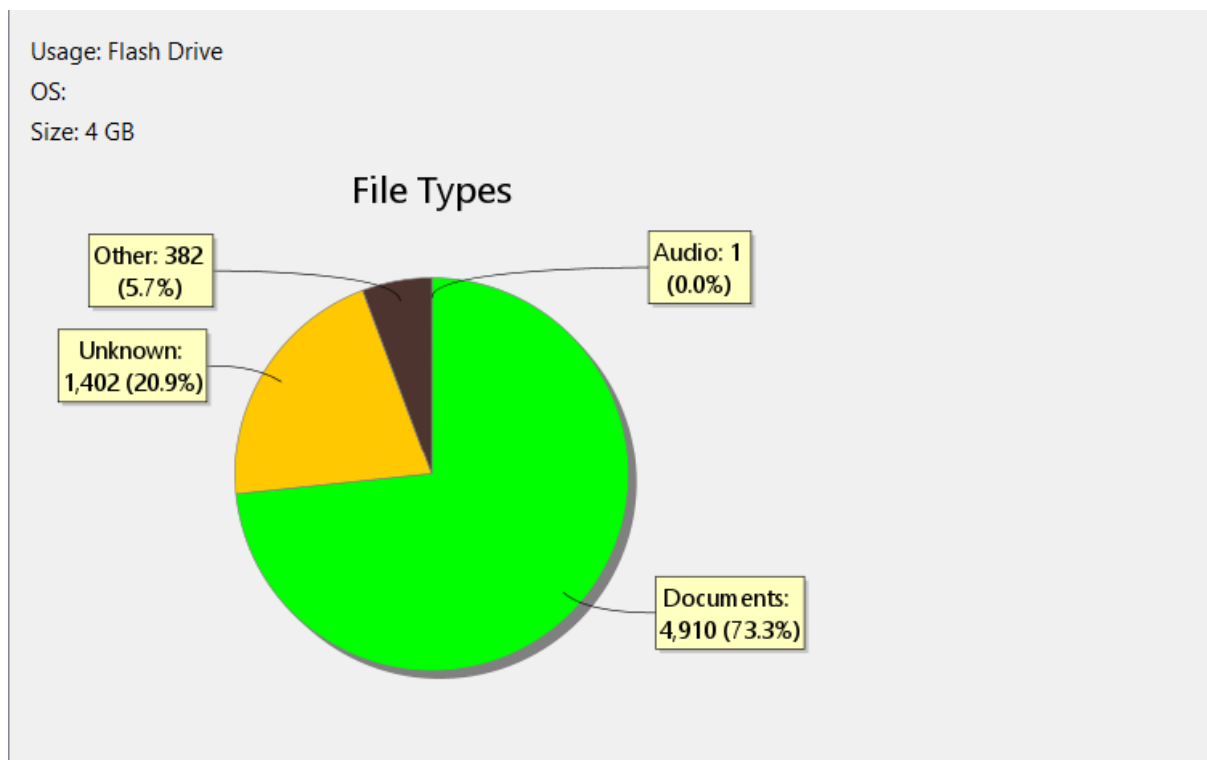
Reťazec starostlivosti

Číslo:	1	Typ súboru:	001 FILE	Obnovený súbor:	Nie	Veľkosť:	1,536,000 kB
Popis prípadu:		Únik výrobnnej stratégie pre batériový modul					
Názov súboru:		Usbklucobraz4GB.001					
Miesto získania digitálnej stopy:		USB kľúč získaný od podozrivého zamestnanca.					
Poznámky:		Digitálna kopia USB kľúča					
Časové pečiatky							
Access:	16.3.2025 17:45:31		Modify:	17.3.2025 8:43:34		Change:	
Digitálny odtlačok (heš)	MD5	366eb0013b2ccb76f88031fffb5487b3					
	SHA1	3a700ad8bcf351291dc8132cfce9cb239f2db968					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
16.3.2025 17:39:15		Kontrola zhody digitálneho odtlačku (HASH-u)					
17.3.2025 8:31:59		Následná extrakcia obsahu a práca s forenznými artefaktami					

Číslo:	2	Typ súboru:	video	Obnovený súbor:	nie	Veľkosť:	78,400 kB
Popis prípadu:		Únik výrobnnej stratégie pre batériový modul					
Názov súboru:		video					
Miesto získania digitálnej stopy:		Firma MotionNextGroup poskytla záznam s bezpečnostnej kamery					
Poznámky:							
Časové pečiatky							
Access:	17.2.2025 10:08:24	Modify :	17.2.2025 10:09:29	Change:			
Digitálny odtlačok (heš)	MD5	d9b43c2ef6501b7716c748ff2e3be8af					
	SHA1	19f4d8acc3e17a01e9c2b6c46be4d0d8f4c08e7b					
Časová pečiatka		Akcia vykonaná s digitálnou stopou					
15.3.2025 12:30:58		Získavanie dát – hľadanie podozrivého					
16.3.2025 10:20:50		Dokončenie zberu dát					

Analýza získaných dôkazov

Hľadaný typ súboru: **DOCX (Microsoft Word)** – interná stratégia batériového modulu bola uchovávaná práve v tomto formáte.



Obr. č. 6 Všetky typy súborov, ktoré USB kľúč obsahuje

Obraz pamäte

V rámci vyšetrovania USB kľúča, ktorý bol zaistený od podozrivého Pavla Nového, budeme pri forenznej analýze tohto zariadenia hľadať konkrétne kľúčové slová, ktoré môžu naznačovať, že sa daný dokument nachádza na USB kľúči. Pre túto analýzu budeme vyhľadávať nasledovné kľúčové výrazy, ktoré môžu súvisieť s dokumentmi týkajúcimi sa technických informácií:

1. **Motion**
2. **Verzia**
3. **LiFePO4**

Tieto výrazy môžu byť prítomné v dokumentoch alebo súboroch, ktoré obsahujú informácie o batériách, ich špecifikáciách, alebo iných technických detailoch súvisiacich s danými technológiami. Ich výskyt na USB kľúči bude slúžiť ako indikátor možného obsahu dokumentov relevantných pre vyšetrovanie.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	49	6E	74	65	72	6E	C3	BD	20	73	74	72	61	74	65	67	InternÃ½ strateg
00000010	69	63	6B	C3	BD	20	64	6F	6B	75	6D	65	6E	74	20	E2	ickÃ½ dokument á
00000020	80	93	20	4D	6F	74	69	6F	6E	4E	65	78	74	47	72	6F	e" MotionNextGro
00000030	75	70	0D	0A	4E	C3	A1	7A	6F	76	3A	20	53	74	72	61	up..NÃ½zov: Stra
00000040	74	C3	A9	67	69	61	20	76	C3	BD	76	6F	6A	61	20	61	tÃ½gia vÃ½voja a
00000050	20	75	76	65	64	65	6E	69	61	20	62	61	74	C3	A9	72	uvedenia batÃ½r
00000060	69	6F	76	C3	A9	68	6F	20	6D	6F	64	75	6C	75	20	6E	iovÃ½ho modulu n
00000070	61	20	74	72	68	0D	0A	4F	7A	6E	61	C4	8D	65	6E	69	a trh..OznaÃ½eni
00000080	65	3A	20	44	C3	94	56	45	52	4E	C3	89	20	E2	80	93	e: DÃ½VERNÃ½: áe"
00000090	20	4C	45	4E	20	50	52	45	20	49	4E	54	45	52	4E	C3	LEN PRE INTERNA
000000A0	89	20	50	4F	55	C5	BD	49	54	49	45	0D	0A	44	C3	A1	% POUÃ½ITIE..DÃ½;
000000B0	74	75	6D	20	76	79	74	76	6F	72	65	6E	69	61	3A	20	tum vytvorenia:
000000C0	31	32	2E	20	6D	61	72	65	63	20	32	30	32	35	0D	0A	12. marec 2025..
000000D0	56	65	72	7A	69	61	3A	20	31	2E	33	20	E2	80	93	20	Verzia: 1.3 áe"
000000E0	66	69	6E	C3	A1	6C	6E	61	20	69	6E	74	65	72	6E	C3	finÃ½lna internÃ½
000000F0	A1	20	76	65	72	7A	69	61	0D	0A	0D	0A	31	2E	20	C3	: verzia....1. Ã½

Obr. č. 7 Nájdienie kľúčového slova - Motion

000000D0	56 65 72 7A	69 61 3A 20 31 2E 33 20 E2 80 93 20	Verzia: 1.3 á€"
000000E0	66 69 6E C3 A1 6C 6E 61 20 69 6E 74 65 72 6E C3		finÁ;lna internÁ
000000F0	A1 20 76 65 72 7A 69 61 0D 0A 0D 0A 31 2E 20 C3		; verzia....1. Á
00000100	9A 76 6F 64 0D 0A 54 C3 A1 74 6F 20 73 74 72 61		švod..TÁ;to stra
00000110	74 C3 A9 67 69 61 20 64 65 66 69 6E 75 6A 65 20		tÁ@gia definuje
00000120	74 65 63 68 6E 6F 6C 6F 67 69 63 6B C3 BD 20 73		technologickÁ% s
00000130	6D 65 72 2C 20 76 C3 BD 72 6F 62 6E C3 A9 20 63		mer, vÁ%robnÁ@ c
00000140	69 65 6C 65 20 61 20 6F 62 63 68 6F 64 6E C3 BD		iele a obchodnÁ%
00000150	20 70 6C C3 A1 6E 20 70 72 65 20 6E 6F 76 C3 BD		plÁ;n pre novÁ%
00000160	20 62 61 74 C3 A9 72 69 6F 76 C3 BD 20 6D 6F 64		batÁ@riovÁ% mod
00000170	75 6C 20 75 72 C4 8D 65 6E C3 BD 20 70 72 65 20		ul urÁ.enÁ% pre
00000180	65 6C 65 6B 74 72 69 63 6B C3 A9 20 76 6F 7A 69		elektrickÁ@ vozi
00000190	64 6C C3 A1 2E 20 44 6F 6B 75 6D 65 6E 74 20 6A		dlÁ;. Dokument j
000001A0	65 20 76 C3 BD 73 6C 65 64 6B 6F 6D 20 64 6C 68		e vÁ%sledkom dlh
000001B0	6F 64 6F 62 C3 A9 68 6F 20 69 6E 74 65 72 6E C3		odobÁ@ho internÁ

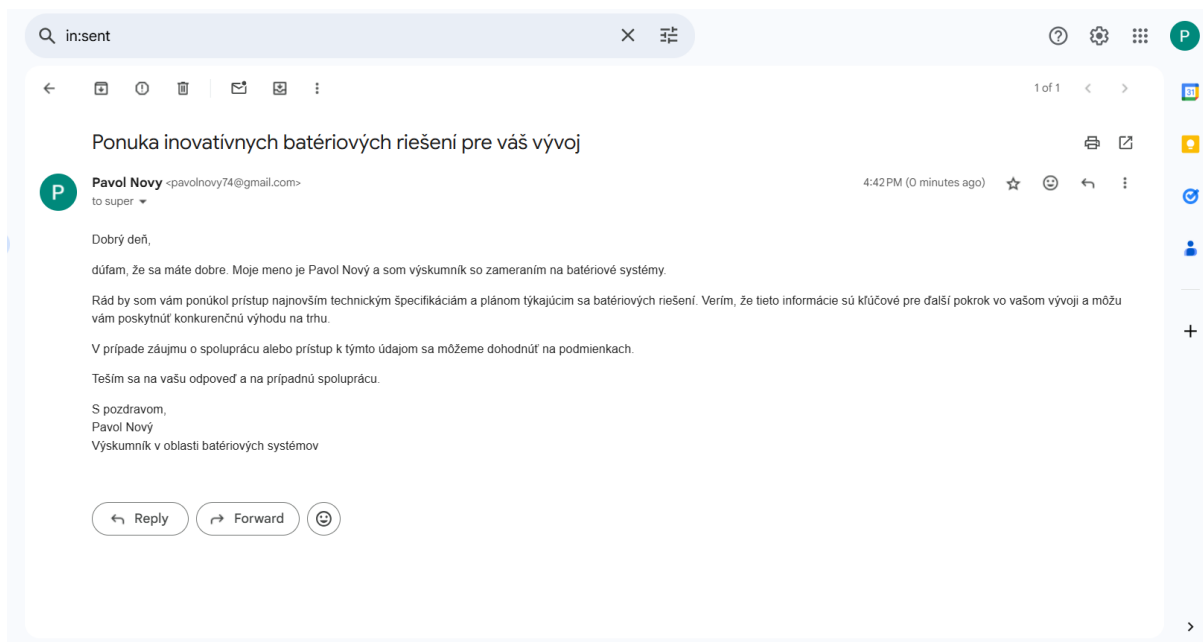
Obr. č. 8 Nájdenie kľúčového slova - Verzia

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000200	70	6F	6C	6F	C4	8D	6E	6F	73	74	69	20	4D	6F	74	69	poloÁ.nosti Moti
00000210	6F	6E	4E	65	78	74	47	72	6F	75	70	2E	0D	0A	0D	0A	onNextGroup.....
00000220	32	2E	20	54	65	63	68	6E	69	63	6B	C3	A1	20	C5	A1	2. TechnickÁ; Á;
00000230	70	65	63	69	66	69	6B	C3	A1	63	69	61	20	62	61	74	pecifikÁ;cia bat
00000240	C3	A9	72	69	6F	76	C3	A9	68	6F	20	6D	6F	64	75	6C	Á@riovÁ@ho modul
00000250	75	0D	0A	54	79	70	20	C4	8D	6C	C3	A1	6E	6B	6F	76	u..Typ Á.iÁ;nkov
00000260	3A	20	4C	C3	AD	74	69	75	6D	2D	C5	BE	65	6C	65	7A	: LÁ.tium-Á%vez
00000270	6F	2D	66	6F	73	66	C3	A1	74	6F	76	C3	A9	20	28	4C	o-fosfÁ;tovÁ@ (L
00000280	69	46	65	50	4F	34	29	0D	0A	0D	0A	4B	6F	6E	66	69	iFePO4)....Konfi
00000290	67	75	72	C3	A1	63	69	61	3A	20	39	36	20	C4	8D	6C	gurÁ;cia: 96 Á.l
000002A0	C3	A1	6E	6B	6F	76	20	7A	61	70	6F	6A	65	6E	C3	BD	Á;nkov zapojenÁ%
000002B0	63	68	20	73	C3	A9	72	69	6F	76	6F	0D	0A	0D	0A	4B	ch sÁ@riovo....K
000002C0	61	70	61	63	69	74	61	3A	20	31	36	30	20	41	68	2C	apacita: 160 Ah,
000002D0	20	6E	6F	6D	69	6E	C3	A1	6C	6E	65	20	6E	61	70	C3	nominÁ;lne napÁ
000002E0	A4	74	69	65	3A	20	33	30	37	20	56	0D	0A	0D	0A	52	stie: 307 V....R
000002F0	69	61	64	65	6E	69	65	3A	20	56	6C	61	73	74	6E	C3	iadenie: VlastnÁ

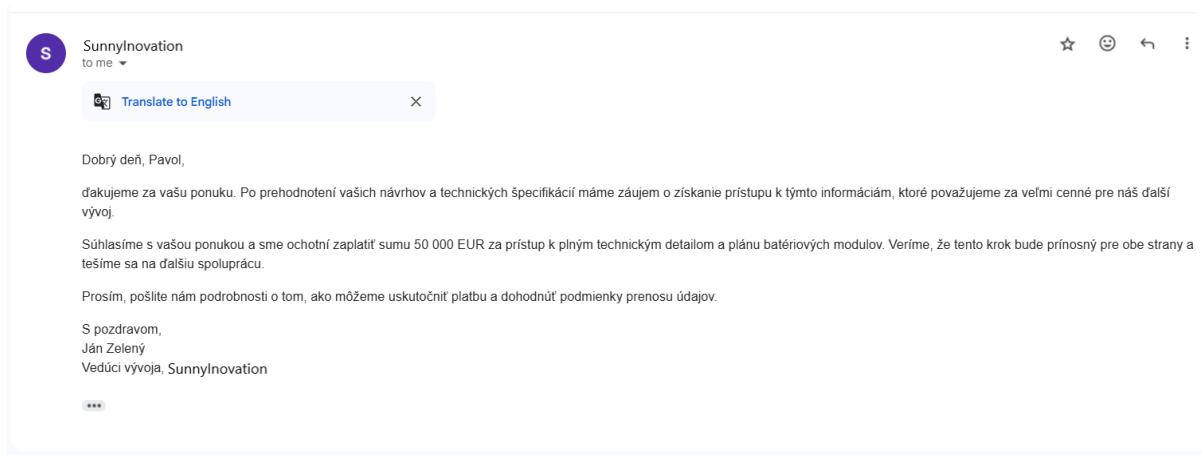
Obr. č. 9 Nájdenie kľúčového slova - LiFePO4

Tieto kľúčové slová boli identifikované v dokumentoch uložených na USB kľúči, čo naznačuje, že tieto informácie sú súčasťou obsahu zariadenia.

Ďalšie vyšetrovanie zahŕňalo vypočúvanie podozrivého Pavla Nového, ktorý bol počas výsluchu konfrontovaný s dôkazmi nájdenými na USB kľúči. Po dlhšom vypočúvaní a analýze jeho reakcií sa podozrivý nakoniec priznal k zneužitiu firemných informácií. Uviedol, že ponúkol a následne predal citlivé údaje konkurencii výmenou za finančnú odmenu. V rámci vyšetrovania bol poskytnutý prístup k jeho osobnému e-mailu, kde bola nájdená komunikácia, ktorá ho usvedčovala z tohto trestného činu. Tieto e-maily obsahovali detaily o predaji technologických informácií konkurencii, čo potvrdilo jeho úmysel získať nelegálny finančný zisk.



Obr. č. 10 *Komunikácia medzi páchatelom a konkurenciou*



Obr. č. 11 *Komunikácia medzi páchatelom a konkurenciou*

Hypotéza 1

Hypotéza 1 sa **potvrdila**.

Po vyšetrení digitálnych dôkazov, vrátane analýzy záznamu z bezpečnostných kamier, systémových logov a obsahu USB kľúča, sa podozrivý zamestnanec, Pavol Nový, priznal k odcudzeniu údajov s cieľom ich predaja konkurencii výmenou za finančnú odmenu. Komunikácia v jeho osobnom e-maile potvrdila jeho úmysel získať nelegálny finančný zisk predajom technologických informácií konkurencii, čím bola táto hypotéza potvrdená.

Hypotéza 2

Hypotéza 2 je **čiastočne potvrdená**.

Zamestnanec, Pavol Nový, vyviezol citlivé údaje z firmy, avšak tieto údaje sa nedostali k iným osobám. Namiesto toho samotný Pavol Nový predal tieto informácie konkurencii. Pri vyšetrení neboli zistené ďalšie osoby zapojené do procesu exportu alebo distribúcie týchto údajov.

Hypotéza 3

Hypotéza 3 sa **nepotvrdila**.

Pri vyšetrovaní neboli nájdené žiadne konkrétne dôkazy, ktoré by naznačovali, že firma MotionNextGroup úmyselne poskytla svoje citlivé údaje konkurencii za účelom diskreditácie alebo poškodenia reputácie konkurenčnej firme.

Záver

Forenzný tím potvrdil, že Pavol Nový odcudzil firemné údaje a predal ich konkurencii, firma MotionNextGroup podala trestné oznámenie na políciu. Podozrivý zamestnanec čelil obvineniu zo zločinu krádeže obchodného tajomstva a porušenia dôvernosti údajov.

Použitý softvér

1. Exterro® FTK® Imager 4.7.3.81
2. Belkasoft RAM capturer
3. Hxd

Použité Systémové nástroje

1. **Event Viewer** (Zobrazovač udalostí)
2. **Registry Editor** (Editor databázy Registry)

Literatúra

An Automated Timeline Reconstruction Approach for Digital Forensic Investigations

<https://dfrws.org/presentation/an-automated-timeline-reconstruction-approach-for-digital-forensic-investigations/>

Článok navrhuje metódu na automatickú rekonštrukciu „vysokoúrovňových“ forenzných udalostí (napr. pripojenie USB) z miliónov „nízkoúrovňových“ udalostí (napr. úprava súboru). Dáta sa ukladajú do SQLite, kde sú analyzované na vzory. Zachováva sa aj pôvod udalostí, čo umožňuje spätné vysledovanie zdroja. Výsledky sa dajú vizualizovať pomocou existujúcich nástrojov.

Secure USB Bypassing Tool

<https://dfrws.org/presentation/secure-usb-bypassing-tool/>

Článok sa zaoberá bezpečnostnými zraniteľnosťami USB pamätí, ktoré majú zabudované základné bezpečnostné funkcie prostredníctvom USB kontrolérov. Ukazuje, ako je možné tieto funkcie obísť pomocou príkazov USB kontroléra a predstavuje nástroj na obídenie týchto bezpečnostných mechanizmov.

Skúmané informácie boli získane z voľne dostupných datasetov. História logov je z lokálnych záznamov môjho počítača. Všetky mená osôb, názvy spoločností sú fiktívne. Akákoľvek zhoda je čisto náhodná.