



Neautorizovaný prenos dát

JAKUB MIHÁLIK

2024/2025

Úvod do prípadu

- ▶ Spoločnosť DataSecure zaznamenala anomáliu v prenose dát, ktorá naznačuje možný únik citlivých informácií.
- ▶ Interný bezpečnostný systém zaznamenal pripojenie neznámeho USB zariadenia k firemnému notebooku v čase, keď došlo k náhlemu zvýšeniu sieťovej aktivity.
- ▶ Po ďalšej analýze sa zistilo, že niektoré súbory boli buď skopírované, alebo vymazané.

Cieľ vyšetrovania

- ▶ Overiť, či USB zariadenie obsahuje stopy o neoprávnenom prenose dát.
- ▶ Preskúmať uložené súbory, metadáta a históriu používania USB zariadenia.
- ▶ Analyzovať sieťové a systémové logy na odhalenie podozrivých činností.
- ▶ Určiť možného páchatela na základe zhromaždených digitálnych dôkazov.

Zaistené dôkazy

- ▶ USB kľúč s dátami
- ▶ Notebook (pracovný počítač)
- ▶ Kamery

Hypotézy

- ▶ USB zariadenie bolo použité na exfiltráciu dát.
- ▶ USB obsahovalo škodlivý kód na manipuláciu s dátami.
- ▶ Firemný notebook bol kompromitovaný fyzickým prístupom
- ▶ Externej osobe bolo umožnené vykonať analýzu a manipuláciu s dátami na firemnom zariadení

Popis vyšetrovania - Arnes 2017

Identifikácia

- Overenie, či USB obsahuje dôkazy o neautorizovanom prenose firemných dát.

Zaistovanie a zber

- Zaistenie USB, vytvorenie forenznej kópie a zaznamenanie technických údajov.

Vyťažovanie

- Vyhľadanie podozrivých súborov, dátumov zmien a prepojení na firemné dáta.

Analýza

- Preskúmanie obsahu USB, metadát a hľadanie znakov škodlivých aktivít.

Prezentácia

- Vypracovanie správy s dôkazmi, časovou osou a návrhmi na zlepšenie bezpečnosti.

Case View Tools Window Help

+ Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Listing /img_D: 3011 Results

Table Thumbnail Summary

Save Table as CSV

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags
file_1013.xml				2025-03-21 17:44:58 SEČ	0000-00-00 00:00:00	2025-03-21 00:00:00 SEČ	2025-03-21 17:44:58 SEČ	190	Alloca
file_1014.xml				2025-03-21 17:44:58 SEČ	0000-00-00 00:00:00	2025-03-21 00:00:00 SEČ	2025-03-21 17:44:58 SEČ	190	Alloca
file_1015.log				2025-03-21 17:44:58 SEČ	0000-00-00 00:00:00	2025-03-21 00:00:00 SEČ	2025-03-21 17:44:58 SEČ	152	Alloca
file_1016.json				2025-03-21 17:44:58 SEČ	0000-00-00 00:00:00	2025-03-21 00:00:00 SEČ	2025-03-21 17:44:58 SEČ	174	Alloca
file_1017.log				2025-03-21 17:44:58 SEČ	0000-00-00 00:00:00	2025-03-21 00:00:00 SEČ	2025-03-21 17:44:58 SEČ	152	Alloca
file_1018.json				2025-03-21 17:44:58 SEČ	0000-00-00 00:00:00	2025-03-21 00:00:00 SEČ	2025-03-21 17:44:58 SEČ	174	Alloca
file_1019.csv				2025-03-21 17:44:58 SEČ	0000-00-00 00:00:00	2025-03-21 00:00:00 SEČ	2025-03-21 17:44:58 SEČ	152	Alloca
file_102.json				2025-03-21 17:44:58 SEČ	0000-00-00 00:00:00	2025-03-21 00:00:00 SEČ	2025-03-21 17:44:58 SEČ	174	Alloca
file_1020.txt				2025-03-21 17:44:58 SEČ	0000-00-00 00:00:00	2025-03-21 00:00:00 SEČ	2025-03-21 17:44:58 SEČ	142	Alloca
file_1021.csv				2025-03-21 17:44:58 SEČ	0000-00-00 00:00:00	2025-03-21 00:00:00 SEČ	2025-03-21 17:44:58 SEČ	152	Alloca

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Strings Extracted Text Translation Viewer for Operating System accounts related to the selected node.

Page: 1 of - Page Matches on page: - of - Match 100% Reset Text Source: File Text

<log><user>jdoe</user><access>unauthorized</access><time>2025-03-20T12:35:00</time></log>
LgZvkKcMVE9C5z7KscIzJEeqszclveDVfEk2H7mM64TznUUDpGSbAMtx2UImQqAzurV52R5YNF4RgPqUCypaQBSNWJfGNS7wxk

Analýza USB zariadenia

ext-jm-ram.raw

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00804AA0	64	65	76	69	63	65	20	6F	72	20	61	64	64	72	65	73	device or address
00804AB0	73	00	00	00	00	00	00	00	6E	6F	20	73	75	63	68	20	s.....no such
00804AC0	64	65	76	69	63	65	00	00	6E	6F	20	73	75	63	68	20	device..no such
00804AD0	66	69	6C	65	20	6F	72	20	64	69	72	65	63	74	6F	72	file or director
00804AE0	79	00	00	00	00	00	00	00	6E	6F	20	73	75	63	68	20	y.....no such
00804AF0	70	72	6F	63	65	73	73	00	6E	6F	74	20	61	20	64	69	process.not a di
00804B00	72	65	63	74	6F	72	79	00	6E	6F	74	20	61	20	73	6F	rectory.not a so
00804B10	63	6B	65	74	00	00	00	00	6E	6F	74	20	61	20	73	74	cket....not a st
00804B20	72	65	61	6D	00	00	00	00	6E	6F	74	20	63	6F	6E	6E	ream....not conn
00804B30	65	63	74	65	64	00	00	00	6E	6F	74	20	65	6E	6F	75	ected...not enou
00804B40	67	68	20	6D	65	6D	6F	72	79	00	00	00	00	00	00	00	gh memory.....
00804B50	6E	6F	74	20	73	75	70	70	6F	72	74	65	64	00	00	00	not supported...
00804B60	6F	70	65	72	61	74	69	6F	6E	20	63	61	6E	63	65	6C	operation cancel
00804B70	65	64	00	00	00	00	00	00	6F	70	65	72	61	74	69	6F	ed.....operatio
00804B80	6E	20	69	6E	20	70	72	6F	67	72	65	73	73	00	00	00	n in progress...
00804B90	6F	70	65	72	61	74	69	6F	6E	20	6E	6F	74	20	70	65	operation not pe
00804BA0	72	6D	69	74	74	65	64	00	6F	70	65	72	61	74	69	6F	mitted.operatio
00804BB0	6E	20	6E	6F	74	20	73	75	70	70	6F	72	74	65	64	00	n not supported.
00804BC0	6F	70	65	72	61	74	69	6F	6E	20	77	6F	75	6C	64	20	operation would
00804BD0	62	6C	6F	63	6B	00	00	00	6F	77	6E	65	72	20	64	65	block...owner de
00804BE0	61	64	00	00	00	00	00	00	70	65	72	6D	69	73	73	69	ad.....permissi
00804BF0	6F	6E	20	64	65	6E	69	65	64	00	00	00	00	00	00	00	on denied.....
00804C00	70	72	6F	74	6F	63	6F	6C	20	65	72	72	6F	72	00	00	protocol error...
00804C10	70	72	6F	74	6F	63	6F	6C	20	6E	6F	74	20	73	75	70	protocol not sup
00804C20	70	6F	72	74	65	64	00	00	72	65	61	64	20	6F	6E	6C	ported..read onl
00804C30	79	20	66	69	6C	65	20	73	79	73	74	65	6D	00	00	00	y file system...
00804C40	72	65	73	6F	75	72	63	65	20	64	65	61	64	6C	6F	63	resource deadloc
00804C50	6B	20	77	6F	75	6C	64	20	6F	63	63	75	72	00	00	00	k would occur...
00804C60	72	65	73	6F	75	72	63	65	20	75	6E	61	76	61	69	6C	resource unavail
00804C70	61	62	6C	65	20	74	72	79	20	61	67	61	69	6E	00	00	able try again...
00804C80	72	65	73	75	6C	74	20	6F	75	74	20	6F	66	20	72	61	result out of ra
00804C90	6E	67	65	00	00	00	00	00	73	74	61	74	65	20	6E	6F	nge.....state no
00804CA0	74	20	72	65	63	6F	76	65	72	61	62	6C	65	00	00	00	t recoverable...
00804CB0	73	74	72	65	61	6D	20	74	69	6D	65	6F	75	74	00	00	stream timeout..
00804CC0	74	65	78	74	20	66	69	6C	65	20	62	75	73	79	00	00	text file busy...
00804CD0	74	69	6D	65	64	20	6F	75	74	00	00	00	00	00	00	00	timed out.....
00804CE0	74	6F	6F	20	6D	61	6E	79	20	66	69	6C	65	73	20	6F	too many files o
00804CF0	70	65	6E	20	69	6E	20	73	79	73	74	65	6D	00	00	00	pen in system...
00804D00	74	6F	6F	20	6D	61	6E	79	20	66	69	6C	65	73	20	6F	too many files o
00804D10	70	65	6E	00	00	00	00	00	74	6F	6F	20	6D	61	6E	79	pen.....too many
00804D20	20	6C	69	6E	6B	73	00	00	74	6F	6F	20	6D	61	6E	79	links..too many
00804D30	20	73	79	6D	62	6F	6C	69	63	20	6C	69	6E	6B	20	6C	symbolic link l
00804D40	65	76	65	6C	73	00	00	00	76	61	6C	75	65	20	74	6F	evels...value to
00804D50	6F	20	6C	61	72	67	65	00	77	72	6F	6E	67	20	70	72	o large.wrong pr

Checksum Search (9396 hits)

Záznam o
připojení
neznámého
USB

Preverenie záznamov z kamier

- ▶ Po preverení kamerového systému spoločnosti DataSecure bola zachytená osoba
- ▶ Slabé osvetlenie, ale tvár osoby je jasne rozpoznateľná
- ▶ Osoba nemá prekrytú tvár, sú viditeľné fyzické črty
- ▶ Video ukazuje otvorenie dverí a vstup do kancelárie
- ▶ V kancelárii došlo k pripojeniu neautorizovaného USB zariadenia
- ▶ Identifikácia tváre umožnila spojiť osobu s digitálnymi dôkazmi.

Záver vyšetrovania

- ▶ Forenzná analýza USB zariadenia, systémových logov a kamerových záznamov potvrdila únik citlivých dát
- ▶ Páchateľom bol interný zamestnanec, identifikovaný vďaka digitálnym dôkazom a záznamu z kamier
- ▶ Neboli zistené žiadne známky vonkajšieho útoku, škodlivého softvéru ani neúmyselného prenosu dát
- ▶ Výsledky vyšetrovania poskytujú pevný základ pre právne kroky a návrhy na zlepšenie bezpečnosti

Ďakujem za
pozornosť