

Digitálna forenzná analýza

Útok na sieť

Vypracoval: Michal Borák

Školský rok:2024/2025

Obsah

1. Popis prípadu	3
2. 5WH Analýza	4
3. Hypotézy	5
4. Cieľ vyšetrovania	6
5. Hľadané informácie	7
6. Očakávané výsledky	9
7. Identifikácia zariadení	10
8. Analýza incidentu a dôkazový materiál	12
9. Záver	16

Obsah Obrázkov

Obrázok 1HP EliteBook 845 G8 - PCSK225	10
Obrázok 2USB Emtec CC350-32GB	10
Obrázok 3Autopsy_1	12
Obrázok 4Autopsy_2	12
Obrázok 5Autopsy_3	12
Obrázok 6Kamerový záznam	15
Obrázok 7RFID log	15

1. Popis prípadu

Dňa 25. marca 2025 zaznamenala spoločnosť TechSolutions s.r.o. vážny bezpečnostný incident, ktorý spôsobil úplný výpadok jej IT infraštruktúry. V ranných hodinách boli viaceré servery náhle nedostupné a na ich obrazovkách sa objavilo oznámenie informujúce o zašifrovaní dát a požiadavke na výkupné vo výške 3 bitcoinov. Tento útok bol neskôr identifikovaný ako ransomvérový útok vykonaný prostredníctvom fyzického prístupu k serverovej infraštruktúre.

Po preskúmaní prístupových logov a kamerových záznamov zo serverovne sa zistilo, že do zabezpečeného priestoru v čase medzi 12:39 a 12:50 prenikla neautorizovaná osoba s použitím prístupovej karty, ktorá bola nahlásená ako stratená dva dni pred incidentom. Na zázname z bezpečnostnej kamery je vidieť osobu v každodennom oblečení s kapucňou a rúškom, čo znemožnilo jej okamžitú identifikáciu.

Po kontrole fyzických zariadení v serverovni bol v zadnom porte jedného z hlavných serverov nájdený neoznačený USB kľúč. Zariadenie bolo forenzne zaistené a následne analyzované, pričom sa potvrdilo, že obsahovalo súbory určené na automatické spustenie ransomvérového skriptu. Tento skript po vložení USB do servera automaticky spustil šifrovanie všetkých lokálnych aj sieťových diskov, ku ktorým mal server prístup.

Neskôr sa vyšetrovanie zameralo aj na jedného zo zamestnancov firmy, ktorému patrila zneužitá prístupová karta. Hoci tvrdil, že kartu stratil, forezná analýza jeho firemného laptopu a RAM pamäte odhalila, že v dňoch pred incidentom vyhľadával informácie o fungovaní ransomvéru, vytváraní automatických spúšťačích skriptov na USB zariadeniach a návody na obídenie firemných bezpečnostných politík. Tieto zistenia naznačujú, že zamestnanec mohol mať vedomosti, motiváciu alebo dokonca priamy podiel na príprave útoku.

Vďaka pravidelnému vytváraniu offline záloh však nebolo potrebné zaplatiť výkupné a prevádzku spoločnosti sa podarilo do 48 hodín plne obnoviť. Incident však odhalil viaceré slabiny v zabezpečení a stal sa impulzom na rozsiahle zmeny v oblasti fyzickej aj digitálnej bezpečnosti v rámci spoločnosti.

2. 5WH Analýza

Who? (Kto?)

Útočník, ktorý získal fyzický prístup do serverovne spoločnosti TechSolutions s.r.o. pomocou odcudzenej prístupovej karty. Hoci identita páchatel'a nebola ihneď známa, kamerové záznamy a následná analýza digitálnych dôkazov nasmerovali podozrenie na jedného zo zamestnancov – pracovníka IT oddelenia, ktorého karta bola použitá a ktorého firemný laptop obsahoval digitálne stopy súvisiace s plánovaním útoku.

What? (Čo?)

Fyzické vloženie neautorizovaného USB zariadenia do jedného zo serverov v serverovni, ktoré obsahovalo skript na automatické spustenie ransomvéru. Tento ransomvér zašifroval všetky prístupné súbory a znefunkčnil IT systémy spoločnosti. Útočník následne požadoval výkupné za dešifrovanie údajov.

When? (Kedy?)

Incident sa odohral 25. marca 2025, v čase medzi 12:39 a 12:50, kedy bol zaznamenaný neoprávnený vstup do serverovne a následné narušenie systémov. Šifrovanie dát prebiehalo v priebehu niekoľkých minút od momentu spustenia skriptu.

Where? (Kde?)

V serverovni spoločnosti TechSolutions, kde sú umiestnené všetky centrálné servery. Do priestoru má prístup len obmedzený počet autorizovaných zamestnancov, čo výrazne zúžilo okruh podozrivých.

Why? (Prečo?)

Hlavným motívom útoku bola pravdepodobne finančná motivácia – cieľom bolo vydierať firmu prostredníctvom výkupného za dešifrovanie dát. Alternatívne mohol byť útok vedený ako akt pomsty, sabotáž alebo zneužitie zistených bezpečnostných slabín.

How? (Ako?)

Útočník sa fyzicky dostal do serverovne pomocou „strateného/odcudzeného“ RFID prístupu. Následne vložil do jedného zo serverov USB zariadenie s automaticky spustiteľným skriptom, ktorý inicializoval ransomvér. Ten sa rozšíril po vnútornej sieti a zašifroval všetky dostupné dáta. Skript nevyžadoval žiadnu interakciu, čím umožnil rýchly a nenápadný priebeh útoku.

3. Hypotézy

Hypotéza 1: Útok bol vykonaný fyzickým vložení USB zariadenia so škodlivým kódom do servera

Predpokladá sa, že útočník získal fyzický prístup do serverovne, kde následne vložil USB zariadenie obsahujúce ransomvér. Skript uložený na USB bol nakonfigurovaný tak, aby sa po pripojení automaticky spustil a zašifroval všetky pripojené disky. Táto hypotéza vychádza z nálezu USB zariadenia v porte servera a jeho následnej analýzy, ktorá odhalila prítomnosť súborov typu autorun.inf a šifrovacích PowerShell skriptov.

Hypotéza 2: Útočník využil odcudzenú alebo zneužitú prístupovú kartu zamestnanca

Vzhľadom na to, že do serverovne je možný vstup len cez čítačku RFID kariet, a v čase útoku bola zaznamenaná aktivita jednej z existujúcich kariet, predpokladá sa, že útočník zneužil alebo odcudzil kartu oprávneného zamestnanca. Táto hypotéza je podporená aj tým, že dotýčny zamestnanec kartu krátko pred incidentom nahlásil ako stratenú.

Hypotéza 3: Útok bol plánovaný interne a vykonaný osobou s technickými znalosťami

Digitálna analýza RAM pamäte firemného laptopu podozrivého zamestnanca odhalila viaceré vyhľadávania týkajúce sa ransomvéru, vytvárania škodlivých skriptov na USB zariadeniach a obchádzania bezpečnostných politík. Tieto informácie naznačujú, že zamestnanec mal potrebné technické vedomosti a mohol plánovať alebo vykonať útok osobne.

Hypotéza 4: Dátové súbory boli pred šifrovaním exfiltrované na iné médium alebo externý server

Hoci ransomvér zvyčajne šifruje dáta bez ich odoslania, jedna z hypotéz pracuje s možnosťou, že boli ešte pred šifrovaním vytvorené kópie dát a tie boli uložené na ďalšie médium, prípadne prenesené cez sieť. Táto hypotéza je testovaná analýzou sieťových logov a pamäťových výpisov na prítomnosť dôkazov o exfiltrácii dát.

Hypotéza 5: Incident bol vykonaný externou osobou bez priameho vzťahu k firme

Alternatívna hypotéza predpokladá, že útok bol vykonaný neznámou osobou zvonku, ktorá sa dostala ku karte a poznala fyzické rozloženie budovy. Táto verzia by znamenala vážny únik interných informácií a slabiny v zabezpečení, ktoré umožnili tretej strane pripraviť cielený útok bez pomoci zvnútra firmy.

4. Cieľ vyšetrovania

Cieľom forenzného vyšetrovania je zistiť presný spôsob realizácie ransomvérového útoku, identifikovať zodpovednú osobu a zabezpečiť všetky relevantné digitálne dôkazy pre interné aj prípadné právne konanie. Vyšetrovanie sa zameriava na analýzu fyzicky zaisteného USB zariadenia, preskúmanie záznamov z prístupového systému a bezpečnostných kamier, ako aj detailnú digitálnu forenznú analýzu operačnej pamäte a firemného laptopu podozrivého zamestnanca.

Jedným z hlavných cieľov je overiť, či bolo USB zariadenie aktívne použité na spustenie škodlivého skriptu, a či tento skript spôsobil šifrovanie dát na serveroch. Zároveň je potrebné zistiť, či došlo k exfiltrácii citlivých údajov pred samotným šifrovaním.

Dôležitou súčasťou vyšetrovania je aj analýza operačnej pamäte (RAM) z laptopu, ktorá môže odhaliť, či podozrivý zamestnanec vyhľadával informácie o ransomvéroch, automatizácii útokov či zraniteľnostiach v bezpečnostných systémoch. Ak sa preukáže, že zamestnanec aktívne vyhľadával alebo pripravoval nástroje použité pri útoku, môže to predstavovať kľúčový dôkaz o jeho podiele na incidente.

Vyšetrovací proces má tiež za úlohu identifikovať bezpečnostné nedostatky, ktoré umožnili realizáciu útoku, a na ich základe navrhnúť účinné preventívne opatrenia, ktoré zabránia opakovaniu podobných incidentov v budúcnosti.

5. Hľadanie informácie

Počas forenzného vyšetřovania sa zameriavam na identifikáciu a analýzu všetkých relevantných digitálnych aj fyzických stôp, ktoré môžu objasniť spôsob útoku, identitu páchatel'a a jeho motiváciu.

V rámci USB zariadenia, ktoré je nájdené pripojené k serveru, hľadám:

- Automaticky spúšťané skripty, ako napríklad „autorun.inf“, „.bat“ alebo „.ps1“ súbory, ktoré môžu iniciovať ransomvér po vložení do systému.
- Simulované šifrovacie skripty, ktoré naznačujú zámer infikovať zariadenia v sieti (napr. „encrypt_network.bat“).
- Výkupné správy typu „ransom_note.txt“, ktoré sú typické pre ransomvérové útoky.
- Časové pečiatky a metadáta týchto súborov, ktoré môžu pomôcť určiť moment ich vytvorenia alebo úpravy.
- Pripojenie súborov so zariadením, na ktorom mohli byť pripravené.

V rámci firemného laptopu podozrivého zamestnanca analyzujem:

- Obsah operačnej pamäte, zameraný na vyhľadávanie fragmentov textu, histórie prehliadania, spustených procesov a zvyškov škodlivých príkazov.
- Výskyt kľúčových výrazov ako „how to create ransomware“, „usb autorun script payload“, „powershell encrypt shared folders“, „ransomware builder github“ a podobné.
- Záznamy o činnosti používateľ'a, ktoré môžu naznačovať úmysel pripraviť útok.
- Prítomnosť zvyškov skriptov, dočasných súborov a otváraných dokumentov relevantných pre prípad.
- Možné stopy o kopírovaní súborov na USB médium, alebo pripojenie konkrétneho USB zariadenia k tomuto laptopu.

Zároveň kontrolujem aj ďalšie možné zdroje dôkazov, ako sú:

- Záznamy z prístupového systému RFID čítačky, ktoré určujú čas a spôsob vstupu do serverovne.
- Videozáznam z bezpečnostnej kamery pri vstupe do serverovne, ktorý vizuálne zachytáva pohyb podozrivej osoby.
- Logy zo siete a firewallov, ktoré by mohli indikovať pokus o odoslanie dát alebo komunikáciu so škodlivým externým serverom.

Cieľom je vytvoriť ucelený a dôkazne podložený obraz o incidente – od prípravy útoku, cez jeho vykonanie až po následné dôsledky – a získať dôkazy, ktoré môžu byť použité v internom vyšetrovaní alebo právnom konaní voči zodpovednej osobe.

6. Očakávané výsledky

Očakávaným výsledkom forenzného vyšetrovania je jednoznačné potvrdenie alebo vyvrátenie hypotéz súvisiacich s ransomvérovým útokom prostredníctvom fyzicky pripojeného USB zariadenia.

Vyšetrovanie má priniesť dôkazy, ktoré:

- Potvrdia, že útok bol vykonaný vložení USB zariadenia so škodlivým skriptom do servera, čím došlo k automatickému spusteniu ransomvéru a následnému zašifrovaní dát.
- Odhalia konkrétne škodlivé súbory uložené na USB zariadení, ako aj ich štruktúru, spôsob spustenia a cieľové adresáre v systéme.
- Určia časové pečiatky a aktivitu súvisiacu s USB zariadením, vrátane jeho prvého pripojenia, poslednej modifikácie súborov a identifikácie systému, na ktorom bolo použité.
- Zistia, či došlo k exfiltrácii dát pred samotným šifrovaním, alebo či bol útok výhradne deštruktívneho charakteru.
- Preukázu, či podozrivý zamestnanec mal vedomosť o spôsobe útoku a či vyhľadával alebo pripravoval nástroje použité počas incidentu.
- Nájdu sa v operačnej pamäti (RAM) dôkazy o príprave útoku, napríklad fragmenty textu, histórie vyhľadávania, príkazy PowerShellu, zvyšky spustených skriptov alebo dôkazy o manipulácii so škodlivým kódom.

Cieľom je taktiež pripraviť komplexnú forenznú správu, ktorá bude obsahovať všetky zhromaždené dôkazy, použitú metodológiu, časový priebeh útoku a odporúčania na základe zistených slabín v zabezpečení.

V ideálnom prípade sa očakáva:

- Jednoznačná identifikácia osoby zodpovednej za útok,
- Obnovenie všetkých systémov z offline záloh bez zaplataenia výkupného,
- Zabezpečenie organizácie pred ďalšími podobnými incidentmi prostredníctvom odporúčaných preventívnych opatrení.

7. Identifikácia zariadení

1. Firemný laptop (HP EliteBook 845 G8 – PCSK225)

Zariadenie používané zamestnancom IT oddelenia, podozrivým z prípravy útoku.

- Evidenčné číslo: 01
- Názov zariadenia: PCSK225
- Typ: Notebook (HP EliteBook 845 G8)
- Procesor: AMD Ryzen 7 PRO 5850U with Radeon Graphics (1.90 GHz)
- Operačný systém: Windows 11 Pro, verzia 24H2
- RAM: 16,0 GB (využitelná 15,3 GB)
- Diskové úložisko: 477 GB SSD
- Inštalácia systému: 22. 11. 2024
- Sieťová identita: PCSK225.corp. techsolutions.com
- Zistenia analýzou:
 - História vyhľadávania týkajúce sa ransomvéru, autorun skriptov, USB exploitov.
 - Stopy po tvorbe alebo testovaní skriptov na automatizovaný útok cez USB.
 - Potenciálne fragmenty škodlivého kódu v RAM pamäti.



Obrázok 1HP EliteBook 845 G8 - PCSK225

2. USB zariadenie (Emtec C350 – 32GB USB 2.0)

Zariadenie nájdené v porte servera, ktoré bolo použité na fyzické spustenie ransomvérového útoku.

- Evidenčné číslo: 02
- Výrobca / Model: Emtec C350
- Kapacita: 32 GB
- Rozhranie: USB 2.0
- Prenosová rýchlosť:
 - Čítanie: až do 15 MB/s
 - Zápis: až do 5 MB/s
- Konektor: USB-A



Obrázok 2USB Emtec CC350-32GB

- Materiál: Plastový obal
- Farba: Modro-čierna
- Rozmery: cca 58 x 18 x 8 mm
- Hmotnosť: cca 8 g
- Zistenia analýzou:
 - Súbor autorun.inf spúšťajúci skript encrypt_network.bat
 - Skripty napísané v PowerShell, zamerané na zašifrovanie zdieľaných priečinkov a diskov
 - Dôkaz o predchádzajúcom pripojení k firemnému laptopu PCSK225
 - Metadáta indikujúce posledné úpravy deň pred útokom

Obe zariadenia boli po incidente zaistené v súlade s postupmi digitálnej forenzej analýzy, ich bitové obrazy boli vytvorené pomocou nástroja FTK Imager a ďalej analyzované v offline režime pomocou Autopsy a HxD.

Záver z analýzy USB image:

Forenzná analýza jasne dokazuje, že USB zariadenie obsahovalo škodlivý súborový obsah, ktorý bol zámerne pripravený na vykonanie ransomvérového útoku. Identifikované skripty, autorun súbor a výkupná správa podporujú hypotézu, že útok bol vykonaný fyzickým prístupom a mal byť čo najviac automatizovaný. Tieto dôkazy budú kľúčové pri dokazovaní pôvodu a spôsobu útoku.

Digitálna analýza RAM pamäte – výsledky z FTK Imager

V rámci forenzného vyšetrovania bol pomocou nástroja MRCv120 vytvorený obraz operačnej pamäte (RAM) zariadenia HP EliteBook 845 G8 (názov: PCSK225), ktoré patrí podozrivému zamestnancovi IT oddelenia. Tento RAM dump o veľkosti 17,4 GB bol následne analyzovaný v nástroji FTK Imager 4.7.3.8.1.

Po načítaní súboru memdump.mem do hexadecimálneho prehliadača bolo možné identifikovať viacero reťazcov, ktoré sú typické pre používateľské vyhľadávania v prehliadači a prácu so škodlivými nástrojmi.

Kľúčové nájdené reťazce:

1. how to create ransomware without coding

- Dôkaz, že používateľ mal záujem vytvoriť ransomvér pomocou nástrojov dostupných bez programovania.
- Ide o typické vyhľadávanie útočníkov začiatocníkov.

2. autorun.inf usb ransomware payload

- Jasný záujem o techniku fyzického útoku cez USB zariadenie s autorun skriptom.

3. encrypt shared folders powershell

- Narážka na zneužitie PowerShellu na šifrovanie firemných zdieľaných zdrojov, čo priamo korešponduje s nálezmi na USB kľúči.

4. ransomware builder github

- Používateľ sa zaujímal o nástroje a frameworky, ktoré umožňujú zostavenie vlastného ransomvéru z verejne dostupných zdrojov.

Tieto fragmenty textu sa nachádzali priamo v hexadecimálnom zobrazení pamäťového obrazu, čo naznačuje, že neboli len vyhľadávané, ale aj spracovávané počas aktívneho sedenia – pravdepodobne v prostredí prehliadača alebo editora.

Záver z analýzy RAM pamäte:

Získané dôkazy z RAM pamäte priamo podporujú hypotézu č. 3, že útok bol plánovaný interne a bol realizovaný osobou, ktorá mala technické vedomosti aj motiváciu. Zároveň poskytujú súvislosti medzi týmto zariadením a obsahom zaisteného USB, čo vytvára prepojenie medzi prípravou útoku a jeho vykonaním.

Obraz RAM bol získaný v offline režime a bol spracovaný bez zmien, pričom integrita dumpu bola overená hashom. Tento výstup bude použitý ako digitálny dôkaz v kompletnej forenznej správe.

Kamerový záznam a RFID log

Ďalším dôležitým prvkom dôkazového materiálu bol záznam z bezpečnostnej kamery, ktorá monitoruje vstup do serverovne, a logový výpis z RFID čítačky, ovládajúcej prístupové dvere.

Kamerový záznam z noci incidentu zachytáva osobu vstupujúcu do serverovne o 12:42 hod. Táto osoba mala prekrytú tvár kapucňou a rúškom, čo sťažovalo identifikáciu, no jej správanie a istý pohyb naznačujú znalosť prostredia.



Obrázok 6 Kamerový záznam

Záznam z RFID systému potvrdzuje, že na otvorenie dverí bola použitá prístupová karta zamestnanca Tomáša V., ktorá bola dva dni predtým oficiálne nahlásená ako stratená. Časová zhoda medzi prihlásením karty a vstupom osoby na kamerovom zázname potvrdzuje spojenie medzi fyzickým prístupom a realizáciou útoku.

Prístupový systém - udalosti							
DATUM A ČAS	POPIS	KARTA	ZAMESTNANEC	NOD	ČÍTAČ	OBJEKT	HODNOTA
25.03.2025 12:45	Prechod karty	Karta:7865999	Valný Tomáš ID:9956	Serverovna	serverovna_klona		

Výsledky hľadania 2

POPIS PROGRAMU SPUSTITE STLAČENÍM F1

NUM 22.4.2025 10:17:34 ADMINISTRATOR 100%

Obrázok 7 RFID log

Tieto dôkazy významne podporujú hypotézu, že útok bol vykonaný fyzicky, a že útočník buď získal kartu neoprávnene, alebo vedome využil identitu iného zamestnanca. Kombinácia fyzických a digitálnych dôkazov poskytuje ucelený pohľad na priebeh incidentu a jeho organizáciu.

9. Záver

Forenzné vyšetrovanie útoku na IT infraštruktúru spoločnosti TechSolutions s.r.o. preukázalo, že incident bol výsledkom cielene pripraveného ransomvérového útoku realizovaného prostredníctvom fyzicky pripojeného USB zariadenia. Útočník využil stratenú alebo odcudzenú prístupovú kartu na vstup do serverovne, kde následne pripojil USB kľúč obsahujúci škodlivý skript. Tento skript bol navrhnutý tak, aby sa po pripojení automaticky spustil a vykonal šifrovanie dát dostupných v rámci internej siete.

Digitálna analýza USB zariadenia potvrdila prítomnosť autorun súboru, spúšťačieho skriptu a výkupnej správy, ktoré sú typické pre ransomvérové útoky. Analýza RAM pamäte firemného laptopu podozrivého zamestnanca navyše odhalila fragmenty vyhľadávania súvisiacich s tvorbou ransomvéru a automatizovanými útokmi cez USB. Dôležitou súčasťou dôkazov bol aj videozáznam z bezpečnostnej kamery zachytávajúci vstup do serverovne a logy z RFID čítačky, ktoré potvrdili použitie strateného identifikátora.

Všetky nazbierané dôkazy podporujú hypotézu, že útok bol plánovaný interne a vykonaný osobou, ktorá mala technické schopnosti aj prístup k infraštruktúre. Vďaka prítomnosti pravidelných offline záloh sa firme podarilo obnoviť prevádzku bez nutnosti zaplataenia výkupného, čím sa minimalizovali škody.

Tento prípad poukázal na viaceré zraniteľnosti v oblasti fyzickej a systémovej bezpečnosti. Výsledky vyšetrovania slúžia nielen ako dôkazný materiál, ale aj ako základ pre prijatie účinných preventívnych opatrení na elimináciu podobných hrozieb v budúcnosti.