

Únik citlivých .env informácií z interného nástroja firmy PRK s.r.o.

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

Popis prípadu

V spoločnosti PRK s.r.o. došlo k vážnemu bezpečnostnému incidentu, keď nastalo odcudzenie citlivých .env informácií z interného nástroja na správu užívateľov. Medzi uniknutými údajmi sa nachádzali API kľúče, prihlasovacie údaje do databázy, autentifikačné tokeny, šifrovacie kľúče a prihlasovacie údaje do cloudových služieb. Únik pravdepodobne nenastal priamym zdieľaním od programátorov, ale existuje podozrenie na únik cez nástroje používané pri nasadzovaní kódu, kontrole kvality kódu alebo v rámci CI/CD pipeline.

Predmet vyšetrovania

- Identifikácia spôsobu úniku citlivých .env súborov
- Určenie presnej cesty, ktorou unikli tieto informácie
- Identifikácia možných zodpovedných osôb
- Stanovenie časovej osi incidentu
- Návrh opatrení na zabránenie podobným únikom v budúcnosti

Typ analyzovanej digitálnej stopy

Budem hľadať digitálne stopy z nasledujúcich zariadení:

- Vývojárske počítače programátorov
- Build servery
- Deployment servery
- VPN server
- Git server s interným repozitárom
- CI/CD servery
- Logging servery
- Monitoring systémy

Zameriavam sa na súbory typu:

- .env súbory
- AI chat histórie
- Commit histórie
- Logy deployment nástrojov
- Memory dump súbory (.mem)
- Log súbory (.log)

Aplikovanie 5WH

What (Čo): Únik citlivých .env súborov obsahujúcich API kľúče, prihlasovacie údaje, tokeny a šifrovacie kľúče. Ohrozenie bezpečnosti a integrity systémov spoločnosti PRK s.r.o.

When (Kedy): Presný čas úniku zatiaľ nie je stanovený. Potreba analýzy časových pečiatok v log súboroch a systémových záznamoch.

Where (Kde): Primárne miesto úniku pravdepodobne v rámci CI/CD pipeline, deployment nástrojov, alebo pri používaní AI asistentov.

Who (Kto): – Doposiaľ neidentifikovaný páchateľ/páchatelia. Existuje podozrenie na neúmyselné zdieľanie citlivých údajov pri používaní AI nástrojov alebo na osobu s prístupom k CI/CD pipeline.

Why (Prečo): Možné scenáre: neúmyselný únik, zámerné zneužitie prístupu, kybernetický útok.

How (Ako): – Pravdepodobne prostredníctvom CI/CD pipeline, code review nástrojov alebo AI asistentov. Možnosť neúmyselného zahrnutia citlivých údajov v zdieľaných materiáloch.

Hypotézy

Hypotéza 1: Únik cez CI/CD pipeline

- Autentifikačné údaje mohli byť omylom zahrnuté v konfigurácii CI/CD nástrojov
- Šifrovacie kľúče mohli byť uložené v nešifrovanej podobe v cache pamäti buildu
- Chyba v nastavení prístupových práv mohla umožniť prístup k citlivým údajom neautorizovaným osobám
- Preukázateľné kontrolou log súborov CI/CD nástrojov a histórie buildov

Hypotéza 2: Únik cez code review nástroje

- Citlivé údaje mohli byť omylom zahrnuté v komentároch alebo zdrojovom kóde
- Code review nástroje mohli ukladať alebo indexovať citlivé údaje
- Prístupové práva k histórii code review mohli byť príliš benevolentné
- Preukázateľné kontrolou histórie code review a konfigurácie nástrojov

Hypotéza 3: Neúmyselný únik cez AI nástroje

- Vývojári mohli neúmyselne zahrnúť citlivé údaje pri komunikácii s AI asistentmi
- AI chat história mohla byť uložená alebo prístupná tretím stranám
- Nedostatočné povedomie o rizikách zdieľania kódu s AI nástrojmi
- Preukázateľné kontrolou histórie chatov s AI a analýzou poskytnutých promptov

Hypotéza 4: Kompromitácia vývojárskeho prostredia

- Malware alebo škodlivý kód mohol získať prístup k citlivým údajom
- Neoprávnený prístup k vývojárskym staniciam
- Zneužitie legitímnych prístupov na exfiltráciu údajov
- Preukázateľné kontrolou memory dumpov a analýzou malware

Hypotéza 5: Úmyselný únik citlivých informácií

- Zamestnanec s legitímnym prístupom mohol zámerne zdieľať citlivé údaje
- Mohla nastať kompromitácia užívateľského účtu s vysokými oprávneniami
- Motívom mohla byť finančná odmena, pomsta alebo sabotáž
- Preukázateľné analýzou prístupových logov a neobvyklých vzorov správania

Ciel' vyšetrovania

1. Identifikácia spôsobu úniku citlivých údajov

- Lokalizovať konkrétny bod úniku údajov (.env súborov) z infraštruktúry
- Určiť, ktoré nástroje alebo procesy boli zneužívané alebo nesprávne nakonfigurované
- Prepojiť identifikované zraniteľnosti s konkrétnymi komponentmi systému

2. Určenie rozsahu úniku informácií

- Identifikovať všetky kompromitované prístupové údaje a tokeny
- Kvantifikovať rozsah možných škôd na základe kompromitovaných údajov
- Stanoviť časovú os úniku a potenciálne trvanie expozície

3. Identifikácia zodpovedných osôb alebo aktérov

- Určiť, či bol únik spôsobený internou chybou, nedbalosťou alebo externým útokom
- Identifikovať konkrétne osoby podieľajúce sa na úniku, či už úmyselne alebo neúmyselne
- Zdokumentovať aktivity podozrivých účtov pre možné disciplinárne alebo právne konanie

4. Prevencia budúcich únikov

- Identifikovať systémové zraniteľnosti, ktoré umožnili únik
- Navrhnuť konkrétne bezpečnostné opatrenia na elimináciu identifikovaných rizík
- Vytvoriť odporúčania pre zlepšenie procesov a školenie zamestnancov

5. Zabezpečenie kompromitovaných systémov

- Pripraviť plán na zmenu všetkých kompromitovaných prihlasovacích údajov
- Navrhnuť postup pre revokáciu a nahradenie všetkých API kľúčov a tokenov
- Definovať bezpečné postupy pre generovanie a správu nových prihlasovacích údajov

Stanovenie poradia vyšetrovacích cieľov

1. Identifikácia projektového tímu a ich pracovných staníc (Malware)

Identifikovali sme 2 osoby pracujúce na projekte:

- 1 back-end vývojár (Java, Spring)
- 1 front-end vývojár (Vue.js)

Analyzovali sme pracovné stanice všetkých členov tímu a skontrolovali sme či na pc nieje malware

- Po dôkladnom preverení antivírusovým programom sa nenašli na daných staniciach žiadne vírusy

3. Kontrola vývoja na domácich strojoch

Preverili sme, či členovia tímu nevyvíjali kód na svojich súkromných zariadeniach, čo by mohlo obísť firemné bezpečnostné politiky. Repozitár je nastavený tak, že by nemohli vyvíjať na svojich strojoch, čo znamená, že nemohli si dať kód na svoje zariadenia.

Všetky vývojové aktivity prebiehali výhradne na firemných zariadeniach v zabezpečenom prostredí. Nebola zistená žiadna práca na domácich zariadeniach, ktorá by mohla viesť k úniku citlivých údajov.

4. Analýza CI/CD pipeline

Dôkladne sme preverili celú CI/CD pipeline, ktorá predstavuje kritický bod potenciálneho úniku:

- Kontrola konfiguračných súborov Jenkins, GitHub Actions
- Preverenie skriptov používaných pri buildoch
- Analýza prístupových práv k buildovacím serverom
- Kontrola webhook konfigurácií
- Audit integrácií tretích strán
- Analýza cache a dočasných súborov na buildovacích serveroch

Všetky automatizované procesy boli správne nakonfigurované s použitím bezpečnostných praktík pre prácu s citlivými informáciami. Nenašli sa žiadne dôkazy o exportovaní .env súborov do logov alebo o nesprávnom nakladaní s citlivými premennými.

Vyvrátenie Hypotézy o úniku cez logovacie systémy

Hoci bola primárna kontrola zameraná na logy CI/CD pipeline, preskúmali sme aj dostupné logy aplikácie a systémové logy na relevantných serveroch. Počas analýzy neboli nájdené žiadne záznamy, ktoré by indikovali neúmyselné alebo nesprávne logovanie obsahu .env súborov alebo iných citlivých premenných v rámci štandardného logovania aplikácie alebo systému.

5. Kontrola Git repozitárov

Uskutočnili sme rozsiahlu analýzu Git histórie:

- Kontrola všetkých commitov od začiatku projektu
- Využitie špecializovaných nástrojov na detekciu citlivých údajov v histórii
- Analýza súborov .gitignore a ich správneho používania

Analýza odhalila správne nastavené .gitignore súbory, ktoré vylučovali .env súbory z commitov. Neboli nájdené žiadne commity obsahujúce citlivé prístupové údaje v histórii repozitára.

6. Kontrola prístupových práv k repozitárom

Preverili sme všetky nastavenia týkajúce sa prístupu k repozitárom:

- Audit všetkých užívateľov s prístupom k projektu
- Kontrola visibility nastavení repozitárov (Visible / Private)

Po analýze týchto možných scenárov sme identifikovali to že pri CI/CD únik nenastal taktiež ani na git to nebolo omylom commitnute taktiež aj vyvojárske stanice sú v poriadku

7. Vytvorenie memory dumpov a ich analýza

Pri forenznej analýze únikov citlivých informácií sme sa zamerali na získanie a spracovanie dát priamo z operačnej pamäte vývojárskych staníc. Tento krok bol kľúčový, pretože operačná pamäť obsahuje aktuálne spustené procesy, otvorené súbory a aplikácie bez ohľadu na to, či boli dáta uložené na disk.

Proces získavania memory dumpov

Použité nástroje a ich úloha

1. AccessData FTK Imager 4.7.1.2

- Primárny nástroj použitý na vytvorenie kompletných memory dumpov z oboch vývojárskych staníc
- Použitý v režime "Capture Memory", ktorý zabezpečil získanie celého obsahu operačnej pamäte
- Automaticky vygeneroval metadáta a výpočet integrity (hash) dumpov
- Výstup: kompletné .mem súbory s veľkosťou 16 a 32GB

8. Analýza získaných memory dumpov

Proces získavania memory dumpov

V rámci vyšetrovania úniku citlivých .env informácií sme vykonali forenznú analýzu operačnej pamäte dvoch vývojárskych staníc. Na tvorbu memory dumpov sme použili **AccessData FTK Imager 4.7.1.2**, ktorý umožňuje získať kompletný obraz operačnej pamäte na živom systéme.

Postup získavania dát:

1. **Príprava prostredia** - zabezpečenie vývojárskych staníc v prevádzke bez vypnutia
2. **Spustenie FTK Imager** s administrátorskými právami
3. **Použitie funkcie "Capture Memory"** z menu nástroja
4. **Zadanie metadát** pre prípad:
 - Case Number: PRK-ENV-01/02
 - Evidence Number: 001/002
 - Unique description: Memory dump vývojárskej stanice
 - Examiner: Bezpečnostný analytik PRK
5. **Vytvorenie memory dumpu**

Získané digitálne stopy

Digitálna stopa č. 1 - Vývojárska stanica č. 1

Created By AccessData® FTK® Imager 4.7.1.2
Case Information:

Acquired using: ADI4.7.1.2
Case Number: PRK-ENV-01
Evidence Number: 001
Unique description: Memory dump vývojárskej stanice
Examiner: Bezpečnostný analytik PRK
Notes: Memory dump prvej vývojárskej stanice

Číslo: 001
Typ súboru: .mem
Obnovený súbor: Nie
Veľkosť: 16384 MB
Popis prípadu: Únik citlivých .env informácií PRK s.r.o.
Názov súboru: dev-station-1-memory.mem
Miesto získania digitálnej stopy: Vývojárska stanica č. 1
Poznámky: Získané so súhlasom vedenia a IT oddelenia

Časové pečiatky
Access: [2024-03-15 10:30:00]
Modify: [2024-03-15 10:30:00]
Change: [2024-03-15 10:30:00]

Digitálny odtlačok
MD5: a4e7c8f91b3d6e25d7c9a8b3f5e1d2c0
SHA1: 5e7a9c6b3d2e1f4a8b7c6d5e4f3a2b1c0d9e8f7a

Časová pečiatka | Akcia vykonaná s digitálnou stopou

2024-03-15 10:30:00 | Vytvorenie memory dumpu
2024-03-15 10:45:20 | Kontrola integrity a hash verifikácia
2024-03-15 11:30:00 | Začiatok forenznej analýzy

Digitálna stopa č. 2 - Vývojárska stanica č. 2

Created By AccessData® FTK® Imager 4.7.1.2
Case Information:
Acquired using: ADI4.7.1.2
Case Number: PRK-ENV-02
Evidence Number: 002
Unique description: Memory dump vývojárskej stanice
Examiner: Bezpečnostný analytik PRK
Notes: Memory dump druhej vývojárskej stanice

Číslo: 002
Typ súboru: .mem
Obnovený súbor: Nie

Veľkosť: 32768 MB

Popis prípadu: Únik citlivých .env informácií PRK s.r.o.

Názov súboru: dev-station-2-memory.mem

Miesto získania digitálnej stopy: Vývojárska stanica č. 2

Poznámky: Získané so súhlasom vedenia a IT oddelenia

Časové pečiatky

Access: [2024-03-16 09:15:00]

Modify: [2024-03-16 09:15:00]

Change: [2024-03-16 09:15:00]

Digitálny odtlačok

MD5: b5f8d9e2c3a7b6f1d4e5c9a8b7d6e3f2

SHA1: 7e6f5d4c3b2a1f0e9d8c7b6a5f4e3d2c1b0a9f8e7

Časová pečiatka | Akcia vykonaná s digitálnou stopou

2024-03-16 09:15:00 | Vytvorenie memory dumpu

2024-03-16 09:30:45 | Kontrola integrity a hash verifikácia

2024-03-16 10:15:00 | Začiatok forenznej analýzy

Proces analýzy memory dumpov

Po vytvorení dumpov sme pristúpili k ich systematickej analýze pomocou nasledujúcich nástrojov:

1. HxD (Hexadecimálny editor)

- Slúžil na manuálne prehliadanie a vyhľadávanie v binárnych dátach
- Umožnil vyhľadávanie podľa textových reťazcov ako "openai", "chat.openai", ".env"
- Poskytol hexadecimálne a textové zobrazenie nájdených dát
- Kľúčový nástroj pre identifikáciu konkrétnych URL adries ChatGPT v pamäti

2. Autopsy

- Komplexný nástroj pre forenznú analýzu digitálnych dôkazov
- Automatické vyhľadávanie podľa kľúčových slov
- Extrakcia artefaktov webových prehliadačov (cookies, cache, histórie)
- Analýza reťazcov v pamäti súvisiacich s API kľúčmi a heslami

3. Doplnkové nástroje

- Magnet RAM Capture - sekundárne overenie nálezov
- Belkasoft Live RAM Capturer - analýza procesov a modulov v pamäti

Výsledky analýzy

Pomocou nástroja HxD sme identifikovali tieto kľúčové hexadecimálne výpisy:

```
// Digitálna stopa č. 1:
007CB8260 65 4D 65 22 2C 22 40 69 64 22 3A 22 68 74 74 70 eMe","@id":"http
007CB8270 73 3A 2F 2F 63 68 61 74 2E 6F 70 65 6E 61 69 2E s://chat.openai.
007CB8280 63 6F 6D 2F 63 68 61 74 2F 3F 6D 6F 64 65 6C 3D com/chat/?model=
007CB8290 67 70 74 2D 34 2D 74 75 72 62 6F 2D 70 72 65 76 gpt-4-turbo-prev
007CB82A0 69 65 77 2F 23 63 69 74 61 63 6B 65 72 2D 63 6F iew/#citacker-co
007CB82B0 64 65 2D 64 65 76 73 22 23 72 69 63 68 53 6E 69 de-devs"#richSni
```

```
// Digitálna stopa č. 2:
008AD9C10 65 4D 65 22 2C 22 40 69 64 22 3A 22 68 74 74 70 eMe","@id":"http
008AD9C20 73 3A 2F 2F 63 68 61 74 2E 6F 70 65 6E 61 69 2E s://chat.openai.
008AD9C30 63 6F 6D 2F 73 68 61 72 65 2F 38 32 34 37 63 37 com/share/8247c7
008AD9C40 37 66 2D 36 38 35 64 2D 34 37 61 32 2D 61 66 33 7f-685d-47a2-af3
008AD9C50 30 2D 36 31 37 35 37 66 35 36 32 38 65 30 22 23 0-61757f5628e0"#
008AD9C60 66 65 61 74 75 72 65 73 2D 64 65 76 65 6C 6F 70 features-develop
```

Výpisy z hexadecimálnej analýzy sme dekodovali a identifikovali:

1. Z prvej vývojárskej stanice:

- URL adresa: <https://chat.openai.com/chat/?model=gpt-4-turbo-preview/#citacker-code-devs>
- Identifikátor projektu: "citacker-code-devs"
- Model AI: gpt-4-turbo-preview (najnovší dostupný model)
- Adresa zachytená na pozícii 007CB8260 v memory dumpe

2. Z druhej vývojárskej stanice:

- URL adresa: <https://chat.openai.com/share/8247c77f-685d-47a2-af30-61757f5628e0#features-develop>
- Zdieľaný chat s unikátnym identifikátorom
- Spojenie s vývojovou časťou projektu: "features-develop"
- Adresa zachytená na pozícii 008AD9C10 v memory dumpe

Analýza v nástroji Autopsy

Pomocou nástroja Autopsy sme identifikovali:

- Výskyt kľúčových reťazcov ".env" v blízkosti URL adries ChatGPT
- Potenciálne environmentálne premenné vrátane API kľúčov
- Časovú os aktivít súvisiacich s používaním ChatGPT
- Artefakty webových prehliadačov potvrdzujúce návštevy OpenAI stránok

9.Export OpenAI Chatov

Po identifikácii URL adries ChatGPT v memory dumpoch vývojárskych staníc sme získali prístup k používateľským účtom OpenAI na základe prihlasovacích údajov uložených v prehliadačoch. Následne sme vykonali export komunikácie z týchto účtov.

Postup získania exportov

1. **Prihlásenie do účtov** - použili sme cookies a aktívne relácie identifikované v pamäťových dumpoch
2. **Export chatov** - využitie funkcie "Export data" v nastaveniach účtu OpenAI
3. **Overenie integrity** - kontrola exportovaných súborov a ich formátov

Získané dôkazy

Z exportov sme identifikovali nasledujúce kritické konverzácie:

Konverzácia č. 1: Refaktoring kódu a dotazy na nástroje

Aky model je optimalny na refaktoring kodu aký nástroj použiť keď používam vue js a flask a spring javu c o je optimalny nástroj na optimalnu orietnaciú v kode.

Konverzácia č. 2: DB Konfigurácia a Spojenie

```
// Odoslaný kód s DB prihlasovacími údajmi
DB_USER=prk_pwuser
DB_PASSWORD=a1AT2FFi9Pyn
DB_HOST=ep-new-cloud-112541.us-east-2.aws.neon.tech
DB_NAME=neondb
```

Konverzácia č. 3: Button disabled API

```
// Dotaz o API vlastnostiach PrimeVue komponentov
Obsahuje tento button api na disable?
```

Konverzácia č. 4: Nuxt scroll middleware

```
// Dotaz o fungovaní Nuxt middleware kódu
co robí tento kod.
```

Konverzácia č. 5: Vue title nastavenie

```
// Otázka týkajúca sa nastavenia title stránky
Co sa nachádza v tomto kode ako tam pridám title stránky?
```

Analýza a dôsledky

Analýza exportovaných chatov jednoznačne potvrdila hypotézu č. 3 o neúmyselnom úniku citlivých údajov prostredníctvom AI nástrojov. Vyšetrenie preukázalo, že:

- **Zdieľanie prihlasovacích údajov:**
- Vývojári priamo kopírovali obsah .env súborov do ChatGPT pri riešení problémov s pripojením k databáze

- Únik nastal pri konverzácii č. 2, kde boli odoslané kompletne prihlasovacie údaje k produkčnej databáze
- **Časová súvislosť:**
- Konverzácia č. 2 prebehla približne v rovnakom čase, kedy boli zaznamenané prvé neautorizované prístupy k databáze
- Timestamp chatu korešponduje s časovými záznamami v databázových logoch
- **Nedostatočné povedomie o bezpečnostných rizikách:**
- Vývojári si neboli vedomí rizík spojených so zdieľaním citlivých údajov s externými AI službami
- Chýbajúce školenie o bezpečnom používaní AI nástrojov

Tieto nálezy definitívne potvrdzujú, že k úniku citlivých informácií došlo prostredníctvom AI chatbotov, kde boli zdieľané kompletne prihlasovacie údaje do produkčnej databázy v rámci žiadostí o pomoc s vývojom aplikácie.

10. Vytvorenie Bitových kopíí

Boli vytvorené dve bitové kópie. Jedna kópia sa nachádza u bezpečnostného analytika na šifrovanom externom disku Western Digital My Passport 4TB a druhá kópia je uložená v zabezpečenom dátovom trezore IT oddelenia.

Bezpečnostné opatrenia

1. Zabezpečenie dôkazov

- Memory dumpy vývojárskych staníc sú uchovávané na šifrovaných externých médiách
- Exporty AI chatov sú uložené v zabezpečenom digitálnom formáte s kontrolnými súčtami

2. Dokumentácia a reťazec dôkazov

- Každá extrakcia memory dumpu je zaznamenaná v protokole s časovými pečiatkami
- Všetky exporty chatov obsahujú metadáta potvrdzujúce ich autenticitu
- Pre každý získaný memory dump je vytvorený kontrolný súčet (hash)
- Zachovaný je chronologický záznam všetkých manipulácií s digitálnymi dôkazmi

3. Ochrana údajov počas analýzy

- Analýza memory dumpov prebieha v izolovanom prostredí bez pripojenia na internet
- Na prístup k exportom AI chatov sa používajú jednorazové prihlasovacie údaje
- Obsahy .env súborov sú počas analýzy maskované a šifrované
- Vylúčené je použitie AI nástrojov pri analýze samotných dôkazov

4. Ochrana citlivých informácií

- Odhalené prihlasovacie údaje sú okamžite označené na zmenu
- Všetky API kľúče identifikované v chatových konverzáciách sú rotované
- Správy o incidente neobsahujú pôvodné hodnoty kompromitovaných údajov

Preventívne opatrenia a odporúčania

Na základe výsledkov forenznnej analýzy a zistených skutočností odporúčame nasledujúce preventívne opatrenia, ktoré pomôžu zabrániť podobným únikom citlivých informácií v budúcnosti:

1. Nasadenie vlastnej AI infraštruktúry

Implementácia privátneho LLM riešenia:

- **Nasadenie lokálneho DeepSeek modelu** na firemných serveroch, ktorý bude dostupný výhradne z internej siete
- **Vytvorenie izolovaného prostredia** pre používanie AI asistentov pri vývoji
- **Implementácia zabezpečenej komunikácie** s interným AI systémom
- **Zavedenie on-premise riešenia** bez závislosti na externých poskytovateľoch AI služieb

Technické špecifikácie navrhovaného riešenia:

Model: DeepSeek Coder 33B alebo DeepSeek 67B

Hardvér: NVIDIA A100 80GB GPU

Konfigurácia: Quantizácia na 4-bit presnosť pre efektívne využitie zdrojov

Dostupnosť: Len z firemnej VPN/intranetu

Dodatočná ochrana: Šifrovanie komunikácie a aktívny monitoring obsahu

Chain of Custody

Digitálna stopa č. 1

Číslo: 001
Typ súboru: .mem
Obnovený súbor: Nie
Veľkosť: 16384 MB
Popis prípadu: Únik citlivých .env informácií PRK s.r.o.
Názov súboru: dev-station-1-memory.mem
Miesto získania
digitálnej stopy: Vývojárska stanica č. 1
Poznámky: gZískané so súhlasom vedenia a IT oddelenia

Časové pečiatky

Access: [2024-03-15 10:30:00]

Modify: [2024-03-15 10:30:00]

Change: [2024-03-15 10:30:00]

Digitálny odtlačok (heš)

MD5: a4e7c8f91b3d6e25d7c9a8b3f5e1d2c0

SHA1: 5e7a9c6b3d2e1f4a8b7c6d5e4f3a2b1c0d9e8f7a

Časová pečiatka Akcia vykonaná s digitálnou stopou

2024-03-15 10:30:00 Vytvorenie memory dumpu

2024-03-15 10:45:20	Kontrola integrity a hash verifikácia
2024-03-15 11:30:00	Začiatok forenznej analýzy

Digitálna stopa č. 2

Číslo: 002
Typ súboru: .mem
Obnovený súbor: Nie
Veľkosť: 32768 MB
Popis prípadu: Únik citlivých .env informácií PRK s.r.o.
Názov súboru: dev-station-2-memory.mem
Miesto získania digitálnej stopy: Vývojárska stanica č. 2
Poznámky: Získané so súhlasom vedenia a IT oddelenia

Časové pečiatky

Access: [2024-03-16 09:15:00]
Modify: [2024-03-16 09:15:00]
Change: [2024-03-16 09:15:00]

Digitálny odtlačok (heš)

MD5: b5f8d9e2c3a7b6f1d4e5c9a8b7d6e3f2
SHA1: 7e6f5d4c3b2a1f0e9d8c7b6a5f4e3d2c1b0a9f8e7

Časová pečiatka	Akcia vykonaná s digitálnou stopou
-----------------	------------------------------------

2024-03-16 09:15:00	Vytvorenie memory dumpu
2024-03-16 09:30:45	Kontrola integrity a hash verifikácia
2024-03-16 10:15:00	Začiatok forenznej analýzy

Digitálna stopa č. 3

Číslo: 003
Typ súboru: .html
Obnovený súbor: Nie
Veľkosť: 2.4 MB
Popis prípadu: Únik citlivých .env informácií PRK s.r.o.
Názov súboru: openai-chat-export.html
Miesto získania digitálnej stopy: Export z ChatGPT účtu
Poznámky: Získané na základe dôkazov z memory dumpov

Časové pečiatky

Access: [2024-03-17 14:20:00]
Modify: [2024-03-17 14:20:00]
Change: [2024-03-17 14:20:00]

Digitálny odtlačok (heš)

MD5: c7d9f8e6a5b4c3d2e1f0a9b8c7d6e5f4
SHA1: 1a2b3c4d5e6f7g8h9i0j1k2l3m4n5o6p7q8r9s0t

Časová pečiatka Akcia vykonaná s digitálnou stopou

2024-03-17 14:20:00	Export ChatGPT histórie
2024-03-17 14:35:00	Kontrola integrity a hash verifikácia
2024-03-17 15:00:00	Analýza obsahu komunikácie

Vyvrátenie pôvodných hypotéz

Na základe vykonanej analýzy a získaných dôkazov môžeme systematicky vyvrátiť pôvodne stanovené hypotézy, s výnimkou tej, ktorá bola potvrdená:

- **Vyvrátenie Hypotézy 1 (Únik cez CI/CD pipeline):** Dôkladná kontrola konfiguračných súborov CI/CD nástrojov (Jenkins, GitHub Actions), build skriptov, prístupových práv a cache na build serveroch nepreukázala žiadne známky úniku `.env` súborov alebo nesprávneho zaobchádzania s citlivými premennými v rámci automatizovaných procesov. Všetky konfigurácie boli v súlade s bezpečnostnými praktikami (viď sekcia 3).
- **Vyvrátenie Hypotézy 2 (Únik cez code review nástroje / Git):** Analýza Git histórie pomocou špecializovaných nástrojov potvrdila, že `.env` súbory boli správne vylúčené pomocou `.gitignore` a žiadne citlivé údaje neboli nájdené priamo v commitoch ani v komentároch v rámci histórie repozitára. Prístupové práva k repozitárom boli taktiež správne nastavené (viď sekcie 4 a 5).
- **Potvrdenie Hypotézy 3 (Neúmyselný únik cez AI nástroje):** Analýza memory dumpov odhalila aktívne používanie ChatGPT na vývojárskych staniciach (viď sekcia 8). Následný export a analýza chatovej histórie z vývojárskej stanice č. 1 (16GB RAM) priamo preukázali, že vývojári zdieľali obsah `.env` súboru, vrátane prihlasovacích údajov k databáze, s AI asistentom pri hľadaní pomoci s kódom. Časová os tejto komunikácie koreluje s časom zaznamenaných neautorizovaných prístupov (viď sekcia 9).
- **Vyvrátenie Hypotézy 4 (Kompromitácia vývojárskeho prostredia):** Antivírusová kontrola pracovných staníc neodhalila prítomnosť žiadneho malwaru (viď sekcia 1). Analýza memory dumpov taktiež neukázala žiadne stopy po škodlivom kóde alebo neoprávnenom prístupe, ktorý by mohol viesť k exfiltrácii dát z vývojárskych staníc iným spôsobom ako cez zdieľanie do AI chatu (viď sekcia 8).
- **Vyvrátenie Hypotézy 5 (Úmyselný únik citlivých informácií):** Analýza prístupových logov a vzorov správania užívateľov neodhalila žiadne anomálie, ktoré by naznačovali úmyselné konanie zo strany zamestnancov. Spôsob úniku (zdieľanie v AI chate pri riešení technického problému) silne naznačuje neúmyselnosť a nedostatok povedomia o rizikách, nie zámerné zneužitie (viď sekcia 9).
- **Vyvrátenie Hypotézy o úniku cez logovacie systémy:** Hoci bola primárna kontrola zameraná na logy CI/CD pipeline (viď sekcia 3), preskúmali sme aj dostupné logy aplikácie a systémové logy na relevantných serveroch. Počas analýzy neboli nájdené žiadne záznamy, ktoré by indikovali neúmyselné alebo nesprávne logovanie obsahu `.env` súborov alebo iných citlivých premenných v rámci štandardného logovania aplikácie alebo systému. Dôkazy naďalej jednoznačne smerujú k úniku prostredníctvom AI nástrojov.

Záver

Forenznou analýzou memory dumpov získaných z dvoch vývojárskych staníc sme identifikovali URL adresy vedúce na platformu ChatGPT. Následný export chatových konverzácií z vývojárskej stanice č. 1 (16GB RAM) odhalil, že k úniku citlivých .env informácií došlo prostredníctvom zdieľania kompletných prihlasovacích údajov k produkčnej databáze v rámci komunikácie s AI asistentom. Časová pečiatka tejto komunikácie korešponduje s obdobím prvých zaznamenaných neautorizovaných prístupov. Jednoznačne sme potvrdili Hypotézu č. 3 (Neúmyselný únik cez AI nástroje) a vylúčili ostatné scenáre. Nenašli sme žiadne dôkazy o prítomnosti malwaru, kompromitácii vývojárskeho prostredia, ani o úmyselnom konaní. Na základe zistení odporúčame implementáciu privátneho AI riešenia založeného na modeli DeepSeek Coder v rámci firemnej infraštruktúry, zavedenie vzdelávacích programov pre vývojárov o bezpečnom používaní AI nástrojov a okamžitú zmenu všetkých kompromitovaných prihlasovacích údajov.

Linky o digitálnej forenznej analýze zariadenia

- <https://www.nu.edu/blog/what-is-computer-forensics/>

What is Computer Forensics?

Tento článok poskytuje základný prehľad o počítačovej forenznej analýze, jej histórii a vývoji. Vysvetľuje hlavné princípy získavania digitálnych dôkazov, ich zabezpečenia a analýzy. Popisuje rôzne oblasti využitia vrátane vyšetrovania kybernetických zločinov, firemných incidentov a súkromných vyšetrovaní. Článok tiež uvádza potrebné zručnosti a certifikácie pre profesionálov v tejto oblasti.

- <https://www.sciencedirect.com/science/article/pii/S266591072100030X>

Digital forensics investigation: A systematic literature review

Vedecká štúdia poskytujúca systematický prehľad literatúry v oblasti digitálnej forenznej analýzy. Článok analyzuje aktuálne metodológie, nástroje a postupy používané pri forenznych vyšetrovaniach. Identifikuje kľúčové výzvy v tejto oblasti vrátane problémov s cloud computingom, IoT zariadeniami a šifrovaním. Štúdia tiež navrhuje rámec pre štandardizáciu forenznych postupov a poukazuje na budúce smery výskumu.

- <https://dfrws.org/presentation/database-forensic-analysis-through-internal-structure-carving/>

Database Forensic Analysis Through Internal Structure Carving

Prezentácia zameraná na špecializovanú techniku forenznej analýzy databáz pomocou "carvingu" interných štruktúr. Vysvetľuje, ako možno obnoviť a analyzovať databázové záznamy aj v prípadoch, keď boli poškodené alebo zámerne vymazané. Popisuje metódy na identifikáciu a rekonštrukciu databázových objektov priamo z úložných médií bez potreby funkčného databázového systému.

- <https://dfrws.org/presentation/carving-database-storage-to-detect-and-trace-security-breaches/>

Carving Database Storage to Detect and Trace Security Breaches

Táto prezentácia sa zameriava na využitie techník "carvingu" databázových úložísk na odhalenie bezpečnostných narušení. Ukazuje, ako možno analyzovať nízkoúrovňové databázové štruktúry na identifikáciu neoprávnených zmien, injekcie SQL kódu a iných typov útokov. Prezentácia obsahuje praktické príklady a prípadové štúdie demonštrujúce, ako tieto techniky pomohli pri vyšetrovaní skutočných bezpečnostných incidentov.

...

```
if __name__ == '__main__':  
    init_db()  
    app.run(debug=True, port=5000)
```

Co sa nachadza na tomto page preco mi nejde prepojenie s databazou

```
DB_USER=prk_pwuser
DB_PASSWORD=a1AT2FFi9Pyn
DB_HOST=ep-new-cloud-112541.us-east-2.aws.neon.tech
DB_NAME=neondb
```

```
<template>
  <DocComponent
    title="Vue Button Component"
    header="Button"
    description="Button is an extension to standard input element with icons and theming."
    :componentDocs="docs"
    :apiDocs="['Button', 'ButtonGroup']"
    :ptTabComponent="ptComponent"
    :themingDocs="themingDoc"
  />
</template>
```

...