



Únik citlivých firemných údajov

Marek Mateáš



Prípád

V poisťovni vzniklo podozrenie na hromadné sťahovanie databázových súborov, ktoré obsahovali citlivé osobné údaje klientov, ako sú mená, adresy a rodné čísla. Podľa analýzy sieťových záznamov bolo zistené, že neobvyklý objem prenesených dát súvisí s konkrétnym zamestnancom a jeho počítačom. Zatiaľ však nie je jasné, či je tento zamestnanec priamo zodpovedný za tento incident. Je možné, že niekto z IT tímu mohol neoprávnene získať prístup k jeho zariadeniu a vykonať túto činnosť.



5WH

Who? (Kto?) • Podozrivý zamestnanec

What? (Čo sa stalo?) • Bolo zaznamenané hromadné sťahovanie databázových súborov obsahujúcich citlivé údaje klientov.

When? (Kedy sa to stalo?) • Incident nastal v čase, keď došlo k sťahovaniu veľkého objemu citlivých údajov.

Where? (Kde sa to stalo?) • Fyzicky / • Digitálne

Why? (Prečo sa to stalo?) • Motivácia páchatel'a môže byť finančný zisk predajom citlivých údajov tretím stranám.

How? (Ako?) • Predpokladá sa že išlo o interný útok alebo externý útok



Hypotézy

Hypotéza 1: Zamestnanec mohol sám neoprávnene stiahnuť citlivé údaje z firemného systému s úmyslom ich získať a následne ich prediť tretej strane. Tento krok by mohol byť motivovaný finančným ziskom.

Hypotéza 2: Zamestnanci IT oddelenia majú prístup k technickým nástrojom na manipuláciu s prenosom dát a sieťovými nastaveniami. Je možné, že jeden z týchto zamestnancov zneužil svoj prístup na to získať osobné údaje na predaj alebo iné nelegálne účely.

Hypotéza 3: Zamestnanec mohol byť obeťou škodlivého softvéru, ako je malware alebo vírus, ktorý infikoval jeho počítač. Tento škodlivý kód mohol útočníkovi umožniť získať neoprávnený prístup k systému a vykonať prenos citlivých dát bez vedomia zamestnanca. V takomto prípade je potrebné podrobiť počítač dôkladnej analýze, aby sa zistilo, či existujú dôkazy o prítomnosti škodlivého softvéru alebo známkach infekcie.



Hypotéza 1 a 2 - Nekonkluzívna

Počas analýzy sa zistilo, že zamestnankyňa komunikovala s IT technikom, pričom sa zmieňovala o svojej finančnej núdzi a že niečo veľké sa koná vo firme.

![User 'tracysumtwelve' has logged in : Mon Jun 2 16:02:42 2012]
joe.sum.twelve@gmail.com<tab><tab>Regarding Terry<tab>Joe,

Soryry to bothre er you, but I have a serious question about Terry and her school. Her tutition is getting a bit too much for me right now and I coudId use a little help. I hate to impose on you for this, but is there any way you would be hillinwilling to help me aout with her uttuition for this syear?

Please get back to me,
TracyHi Engyod!

That sounds great, I'll giebeve you a all scall soeme time and we can figure out some plans

![LogKext Daemon created new logfile : Mon Jun 2 12:00:04 2012]

ing interesting. everybErvcverybody around the office seems to be buzzed about a foreign exhibit thats supposed to is supposed to be coming over. There hasn't been any official release in writing but we have been going through a qquite an ordeal with all this paperwork. From what I can tell, this exhibitbit has to be a big deal. I'll let you know if I found out anything else.

Coral,private school financial aid
legalBee



Hypotéza 1 a 2 - Nekonkluzívna

Ďalej sa počas analýzy zistilo, že v komunikácii sa spomínali dokumenty týkajúce sa poistenia, ktorým zamestnankyňa venovala zvýšenú pozornosť. Z rozhovoru tiež vyplynulo, že tieto dokumenty môžu mať hodnotu.

hunCoral<tab>coralbluetwo@hotmail.com<tab>legalBeePerrpePerry,

I know what you meanj. If anything comes up around the office that we can maybe... get in on... , , please lets try to do so. Kiddo is getting really bent out of shape ab
ou t possibly having to switch schools. I have been paying some more attention to the mmomemos and papers that come across my desk. We get a bunch of insurance type documents
that plac vale values on a certain objects. If anything stands out, I

[LogKext Daemon starting up : Fri Jun 29 09:04:12 2018]

[User 'tracysumtwelve' has logged in : Fri Jun 29 09:14:10 2018]



Hypotéza 1 a 2 - Nekonkluzívna

Ďalej bolo z komunikácie je zistené, že si uvedomovali, že tým riskujú svoje pracovné miesta.

```
! [User 'tracysumtwelve' has logged in : Fri Jun 29 10:33:25 2018]
```

```
9<del>legalBee
```

```
<del><del><del><del>
```

```
Be careful! We have enough problems as it is, we can't get <del><del><del><del>be getting in trouble or losing our jobs. Nothing special has turned up here, but I am still keeping an eye out. We usually sot<del><del><del>start to host some interesting events this time of the year, I'm sure som
```

Hypotéza 1 a 2 - Nekonkluzívna

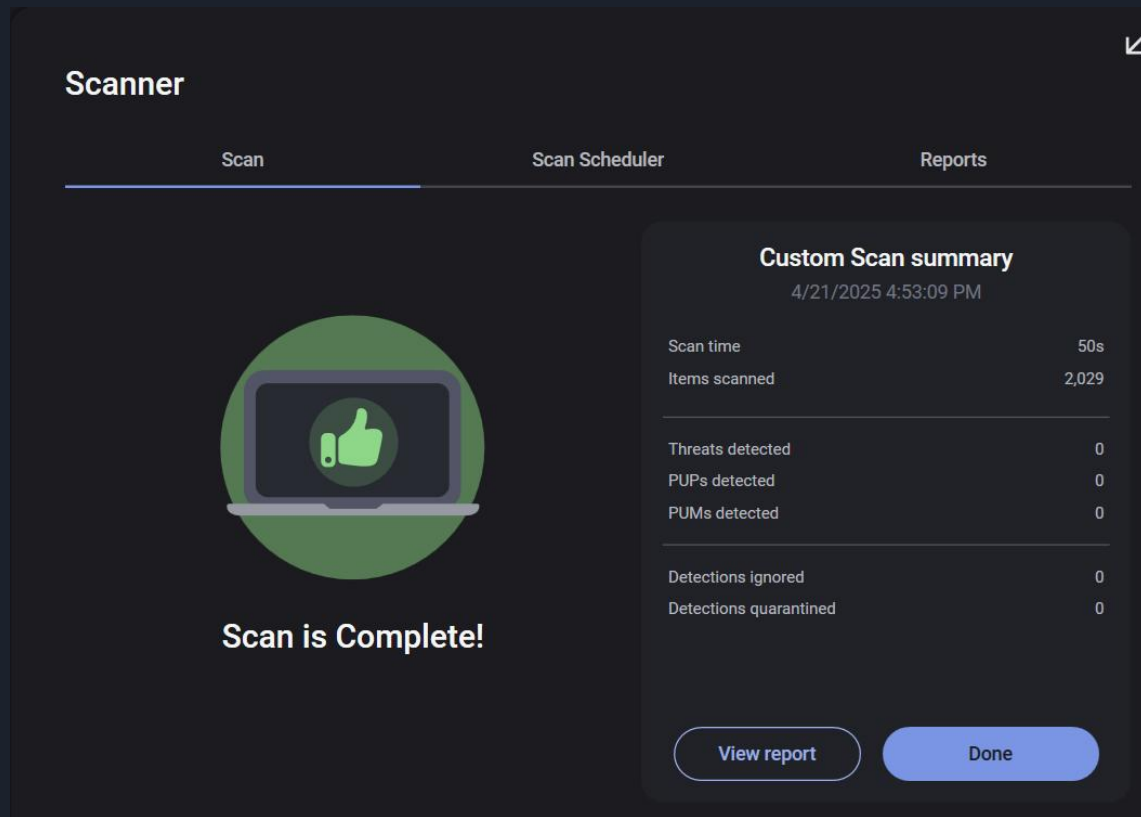
Počas analýzy databáz a ich metadát, vrátane časových údajov o ich stiahnutí, bolo zistené, že všetky databázové súbory sa nachádzajú v časovom rámci, v ktorom boli odoslané príslušné e-maily. Na základe týchto zrovnalostí je pravdepodobné, že k útoku došlo už v roku 2018, pričom dôkazy boli následne úmyselne zamaskované IT technikom.

Name	S	C	O	Modified Time	Change Time	Access Time
01-18.db			2	2017-10-07 21:00:50 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-02.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-03.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-04.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-05.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-06.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-07.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-08.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-09.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-10.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-11.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-12.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-13.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-14.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-15.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-16.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-17.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-18.sql	▼		2	2018-07-14 10:03:24 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-01.sql	▼		2	2018-07-20 10:02:58 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00
01-01.xml	▼		2	2018-07-22 11:17:22 GMT+01:00	0000-00-00 00:00:00	2025-03-28 00:00:00 GMT+01:00

Hypotéza 3

Zamietnutá -

Súbory sme prešli
softvérom Malwarebytes
pre malware a vírusy





Zabezpečenie zariadení a programy

AutoPsy, verzia 4.21.0

FTK Imager, verzia 4.7.3.81

HxD editor

Kópie – Boli vytvorené 3 kópie na 3 HDD disky, z toho 2 sme uložili do stráženého trezoru a 1 na ktorej sa robila analýza

- **Notebook** – Pri zabezpečovaní sme ho vložili do Faradayovho vrečka, aby sme zablokovali všetky bezdrôtové signály. Potom sme ho umiestnili do pevného kufríka, aby sme zabránili jeho poškodeniu počas prepravy.



Záver

Hypotéza 1 a 2 – Nekonkluzívna

Zamestnankyňa kontaktovala IT technika kvôli finanšnej núdzi, je potvrdené stiahnutie súborov ale predaj už nebolo potvrdené

Hypotéza 3 – Zamietnutá

Výsledok antivírusovej kontroly bol negatívny – neboli zistené žiadne škodlivé súbory ani znaky kompromitácie systému.

Odporúčané kroky:

Výsluch zamestnankyne

Zlepšenie bezpečnosti a pravidelné audity

Ďakujem za pozornosť

