

UNIVERZITA SV. CYRILA A METODA V TRNAVE
FAKULTA PRÍRODNÝCH VIED

ÚNIK DÔVERNÝCH ÚDAJOV

Obsah

1. Prípravná fáza.....	3
2. Identifikácia.....	5
3. Zber	11
4. Vyťažovanie	15
5. Analýza	22
5.1. Analýza digitálnej stopy č.001	22
5.2. Analýza digitálnej stopy č.002	23
5.3. Časová os udalostí	31
5.4. Vyhodnotenie hypotéz.....	36
Záver.....	38
Zdroje.....	39

1. Prípravná fáza

Prípad

M57.biz je populárny webový startup, ktorý vytvára online kolekciu body art. Súbor s tabuľkou obsahujúci dôverné informácie zamestnancov bol zverejnený ako príloha na fóre „technickej podpory“ na webovej stránke konkurenta. Súbor pochádza z pracovného laptopu finančnej riaditeľky - Jean Jones. K týmto materiálom má prístup len niekoľko oprávnených zamestnancov, vrátane Jean. Po nahlásení udalosti sa uskutočnilo vypočutie zamestnancov spoločnosti M57.biz. Prezidentka spoločnosti, Alison Smith, uviedla, že nemá o tomto súbore žiadnu znalosť a vyhlásila, že Jean nepožiadala o vytvorenie uvedenej tabuľky. Jean toto tvrdenie vyvrátila s tým, že jej Alison dala pokyn, aby vypracovala tabuľku s údajmi o zamestnancoch a odoslala e-mailom v rámci prípravy na nové kolo financovania.

Predmet vyšetrovania

Identifikácia potenciálnych digitálnych stôp a ich následná analýza s cieľom potvrdiť alebo vyvrátiť forenznú hypotézu, resp. potvrdiť určité výsledky týkajúce sa prípadu zverejnenia dokumentu spoločnosti M57.biz na verejnom fóre konkurencie.

Očakávaný výsledok vyšetrovania

- Preukázanie, kto a kedy dokument vytvoril, upravoval a komu bol odoslaný.
- Overenie tvrdení Jean a Alison (príkaz na vytvorenie a odoslanie tabuľky).
- Identifikácia spôsobu úniku (e-mail, nahratie, zdieľanie, malware...).
- Zistenie, či išlo o úmyselný alebo neúmyselný čin.
- Zhromaždenie dôkazov vhodných na interné alebo právne použitie.

Príspevky / vedecké články

1. Advanced Evidence Collection and Analysis of Web Browser Activity:

https://dfrws.org/sites/default/files/session-files/2011_USA_paper-advanced_evidence_collection_and_analysis_of_web_browser_activity.pdf?utm_source=chatgpt.com

Tento článok sa zameriava na pokročilé metódy zhromažďovania a analýzy údajov o aktivite webových prehliadačov, čo je kľúčové pri vyšetrovaní únikov citlivých informácií prostredníctvom internetových aktivít.

2. Tor Forensics on Windows OS:

https://dfrws.org/sites/default/files/session-files/2015_EU_pres-tor_forensics_on_windows_os.pdf?utm_source=chatgpt.com

Tento príspevok skúma forenznú analýzu používania siete Tor na operačnom systéme Windows, čo je relevantné pri vyšetrovaní prípadov, kde mohli byť firemné dáta exfiltrované cez sieť.

2. Identifikácia

Zhrnutie rozhovorov

Jean Jones (Finančná riaditeľka)

- Alison ju požiadala, aby pripravila tabuľku ako súčasť nového kola financovania, a aby jej ju poslala e-mailom.

Alison Smith (Prezidentka spoločnosti)

- Nepožiadala Jean o vytvorenie tabuľku.
- Tabuľka jej nikdy nebola na e-mail doručená.

Fakty o spoločnosti M57.biz

- Štartovací kapitál: 3 mil. USD.
- Spoločnosť je aktuálne vo fáze uzatvárania investičného kola v hodnote 10 mil. USD.
- 2 zakladatelia / vlastníci.
- Prvý rok bolo prijatých 10 zamestnancov.
- Zamestnanci IT oddelenia pracujú z domu. Majú denne online meetingy a raz týždenne osobné stretnutia v kancelárii.
- Zamestnanci z marketingového a BizDev oddelenia pracujú prevažne z hotelových izieb alebo kaviarní, nakoľko sú väčšinou na cestách. Osobné stretnutia v kancelárii majú raz za dva týždne.
- Preposielanie dokumentov medzi zamestnancami je zvyčajne prostredníctvom e-mailu.

Aktuálni zamestnanci spoločnosti M57.biz

- Prezidentka spoločnosti: Alison Smith
- Finančná riaditeľka: Jean Jones
- IT oddelenie: Bob Blackman, Carole Canfred, Dave Daubert, Emmy Arlington
- Marketingové oddelenie: Gina Tangers, Harris Jenkins
- Business development (BizDev): Indy Counterching

Typ analyzovanej digitálnej stopy

1. Metadáta uniknutého súboru:

- Meno autora

- Dátum vytvorenia, poslednej úpravy a prístupu
 - Umiestnenie súboru (názov súbor je už známy)
2. E-mailová komunikácia:
 - E-maily medzi Jean a Alison (žiadosť o tabuľku, odoslanie súboru)
 - Prílohy zhodné so zverejneným súborom
 - Dátum a čas odoslania
 - Iní príjemcovia alebo preposlanie e-mailu
 3. História prehliadača a sieťovej aktivity:
 - Návštevu fóra konkurencie
 - Príspevky alebo nahratie súborov (upload links)
 - Autentifikačné cookies – prihlásenie na fórum
 4. Aktivita používateľa:
 - Kedy bol súbor otvorený naposledy
 - Ktoré programy boli použité (napr. Excel, Outlook)
 - Názvy nedávno otvorených súborov
 5. USB a externé zariadenia – setupapi.dev.log, register USBSTOR:
 - Použitie USB disku
 - Čas pripojenia a názov zariadenia
 - Možnosť kopírovania súboru na externé úložisko
 6. Prenos súborov - Cloud/FTP aplikácie, Dropbox, Google Drive:
 - Inštalácia alebo použitie cloudových nástrojov
 - Logy a história synchronizácie
 - Zostatky po odinštalovaných aplikáciách (napr. Dropbox cache)
 7. Logy systému a bezpečnostné udalosti:
 - Kto a kedy sa prihlásil do systému
 - Nezvyčajné prihlasovanie (napr. cez RDP – Remote Desktop Protocol, pod iným kontom)
 - Záznamy o chybách alebo pokusoch o vzdialený prístup
 8. Kamerové záznamy z priestorov spoločnosti M57.biz

9. Kontrola podozrivej aktivity:

- Spustiteľné súbory a skripty v podozrivých umiestneniach (Temp, Startup, Downloads)
- Autostart aplikácie (Registry Keys)

Digitálne zariadenia súvisiace s prípadom

- Pracovný laptop Jean Jones – primárne dôkazové zariadenie
 - Súbor s dôvernými údajmi bol údajne vytvorený na tomto zariadení.
 - Jean tvrdí, že súbor odoslala e-mailom, čo by malo byť zachytené v Outlooku alebo inom e-mailovom klientovi.
- Pracovný laptop alebo e-mailový účet Alison Smith – na overenie výpovede
 - Alison tvrdí, že súbor nepožadovala a nedostala e-mailom.
 - Je potrebné preveriť jej e-mailovú schránku (napr. inbox, spam, zmazané).
- Webový server konkurencie – miesto zverejnenia súboru
 - Je na ňom zverejnený dôverný dokument.
 - Môže obsahovať:
 - metadáta o príspevku (dátum, čas),
 - IP adresu alebo používateľský účet, cez ktorý bol súbor nahraný.
- Mobilné zariadenie Jean Jones
 - V tomto prípade nie je explicitne spomenutý mobil, ale ak vyšetrovanie ukáže známky vzdialeného prístupu, je dobré ho preveriť.
- Mobilné zariadenie Alison Smith
 - V tomto prípade nie je explicitne spomenutý mobil, ale ak vyšetrovanie ukáže známky vzdialeného prístupu, je dobré ho preveriť.
- Kamery nainštalované v priestoroch spoločnosti M57.biz.
 - V priestoroch spoločnosti M57.biz sú nainštalované kamery, z ktorých by sa dalo zistiť, kto každý vstúpil do kancelárie Jean Jones.

Pozn.: Daný scenár obsahoval iba obraz disku z laptopu Jean Jones, preto ďalej uvádzam iba toto zariadenie, avšak kvôli správnosti som vyššie uviedla aj ďalšie zariadenia, ktoré by v skutočnosti mohli obsahovať potenciálne digitálne stopy.

5WH (Kiplingova metóda)

Kto (Who)

- Jean Jones – Finančná riaditeľka, ktorá povedala, že vytvorila tabuľku na pokyn prezidentky a odoslala ju e-mailom.
- Alison Smith – Prezidentka spoločnosti, ktorá poprela, že by požiadala o tabuľku alebo ju dostala.
- Zamestnanci IT, marketingu a BizDev – Majú obmedzený alebo žiadny prístup k dôverným finančným dokumentom. Ich prístupové práva môžu byť ale dôležité.
- Konkurencia – Na ich fóre bola tabuľka zverejnená.

Kde (Where)

- Súbor bol uverejnený online na fóre technickej podpory konkurenta.
- Jeho pôvodným zdrojom je laptop Jean Jones.
- Zamestnanci pracujú na rôznych miestach (home office, hotely, kaviarne), čo môže predstavovať zvýšené riziko kybernetického útoku.

Kedy (When)

- Udalosť bola nahlásená prezidentkou spoločnosti, Alison Smith, 21.7.2008 14:50.
- Čas zverejnenia na fóre je 20.7.2008 o 23:59, tzn. súbor už bol zverejnený v čase, keď bola udalosť nahlásená.
- Jean Jones údajne vytvorila tabuľku v rámci prípravy na investičné kolo – tzn. v nedávnej minulosti, pravdepodobne v priebehu niekoľkých dní.

Čo (What)

- Dôverný súbor s údajmi o zamestnancoch bol verejne zverejnený ako príloha na fóre konkurencie.
- Súbor pochádza z laptopu finančnej riaditeľky, na ktorý má prístup len obmedzený počet ľudí.
- Obe hlavné zúčastnené osoby (Jean a Alison) poskytli protichodné výpovede.

Prečo (Why)

- Interný konflikt, napr. medzi Jean a Alison.
- Pokus o diskreditáciu spoločnosti počas kľúčového financovania (v hodnote 10 mil. USD).
- Nedbanlivosť pri zaobchádzaní s dátami – možné nechcené zverejnenie.
- Zámerné uniknutie údajov buď z vnútra spoločnosti, alebo externým aktérom.

Ako (How)

- Zachytenie dát pri prenose (ak bol odoslaný z nezabezpečenej siete).
- Získaný cez phishing, malware alebo fyzický prístup.
- Nahratý omylom na verejné fórum (napr. zmätenie diskusného vlákna s e-mailovou prílohou).
- Preposlaný tretím subjektom bez vedomia Jean.

Ciele vyšetrovania

- Overiť pôvod súboru a manipuláciu s ním (otvorenie, úpravy, zdieľanie).
- Odhaliť spôsob úniku dokument z laptopu Jean na webovú stránku konkurenta.
- Zistiť, kedy prišlo k úniku informácií.
- Overiť tvrdenia Jean Jones a Alison Smith.
- Zistiť, či došlo k úmyselnému alebo neúmyselnému úniku informácií.

Hypotézy

1. Jean Jones skutočne vytvorila súbor na základe pokynu Alison Smith a poslala jej ho e-mailom.
 - Potvrdená: Ak sa nájde e-mail s prílohou a metaúdaje potvrdia vytvorenie súboru Jean.
 - Vyvrátená: Ak sa e-mail nenájde alebo má súbor iného autora.
2. Jean Jones súbor vytvorila, ale omylom ho zdieľala na fóre (napr. zámenou s iným súborom).
 - Potvrdená: Ak existujú dôkazy o tom, že sa Jean prihlasovala na fórum alebo mala záznam o nahratí súboru.

3. Jean Jones súbor vytvorila, ale niekto iný mal prístup k jej laptopu alebo e-mailu a zverejnil ho.
 - Potvrdená: Ak sa nájde dôkaz o neoprávnenom prístupe (malware, vzdialené pripojenie).
4. Súbor zverejnil iný interný zamestnanec s prístupom k dokumentu.
 - Potvrdená: Ak metaúdaje alebo logy ukážu prístup iného používateľa.
5. Externý útočník získal súbor cez zraniteľnosť systému (napr. nezabezpečené Wi-Fi, phishing).
 - Potvrdená: Ak sa nájde dôkaz kompromitácie systému (napr. logy útoku, podozrivý softvér).
6. Súbor nikdy nebol odoslaný Alison Smith a jej tvrdenie je pravdivé.
 - Potvrdená: Žiadna e-mailová komunikácia o tabuľke sa nenašla, Jean má súbor len lokálne.
7. Alison Smith klame a snaží sa poprieť svoju účasť, aby sa chránila.
 - Potvrdená: Ak sa nájde e-mail s prílohou a žiadosťou z jej strany, alebo dôkaz, že ho čítala.

3. Zber

Laptop Jean Jones bol zaistený po zaznamenaní údajov z neho na mieste činu. Pevný disk a operačná pamäť laptopu Jean Jones bol naklonované v súlade s firemnou politikou. Bolo zabezpečené dobrovoľné odovzdanie dôkazov, súhlas a prístup k počítaču bol poskytnutý bez porušenia práva na súkromie podozrivej osoby.

Zaistené digitálne zariadenie

1. Pracovný laptop Jean Jones



Obrázok 1 Pracovný laptop Jean Jones

- Model: Dell Latitude D630
- Operačný systém: Windows XP Service Pack
- Procesor:
 - Model: Intel Core 2 Duo
 - Frekvencia: 1.8 GHz
 - Architektúra: Intel x86
- RAM:
 - Typ: DDR2 SDRAM

- Kapacita: 4 GB
- Frekvencia: 667 MHz
- Úložisko:
 - Typ: 2.5" SATA HDD
 - Kapacita: 160 GB
 - Rýchlosť otáčok: Zvyčajne 5400 RPM
- Vlastnosti úložiska:
 - Životnosť: Približne 3–5 rokov bežného používania
 - Rýchlosť čítania/zápisu:
 - Čítanie: cca 40–60 MB/s
 - Zápis: cca 30–50 MB/s
 - Prístupová doba: 12–15 ms

Zaistené potenciálne digitálne stopy

1. Obráz pamäte RAM vo formáte RAW

- MD5 Hash: D9B1A9868C6BF5EC7F26D9C5D82AD32B
- SHA-1 Hash: F18883E34ECFCD67907E9B56EB5F3A6020F6C6BF
- Jedna hlavná a jedna pracovná kópia pamäte RAM boli vytvorené v softvéri Magnet RAM Capture (v1.2.0). Hlavná kópia bola uložená na USB disku. Pracovná kópia sa použila na účely vyšetrovania po potvrdení zhody hashov.

2. Obráz pevného disku vo formáte EnCase

- MD5 Hash: 78a52b5bac78f4e711607707ac0e3f93
- SHA-1 Hash: ba7dc57e08bb6e3393ace15c713ae04feadcd181
- Jedna hlavná a jedna pracovná kópia disku boli vytvorené v softvéri Exterro FTK Imager (v4.7.3.81). Hlavná kópia bola uložená na SSD s HW šifrovaním. Pracovná kópia sa použila na účely vyšetrovania po potvrdení zhody hashov.

Nástroje použité pre zber potenciálnych digitálnych dôkazov

- Magnet RAM Capture v1.2.0 – zachytenie operačnej pamäte
- Exterro FTK Imager v4.7.3.81 – vytvorenie forenzného obrazu disku

Postup zberu potenciálnych digitálnych dôkazov

1. Laptop Jean Jones

Charakter zaist'ovania: Živé zaist'ovanie

1.1 Príprava pred zaistením

- Overenie oprávnenia na zaistenie zariadenia.
- Použitie písomného protokolu o zaistení zariadenia.
- Pripravenie zabezpečeného pracovného prostredia (fyzicky aj digitálne).
- Oboznámenie sa so špecifikom prípadu – zariadenie je zapnuté, vyžaduje sa živé zaist'ovanie.

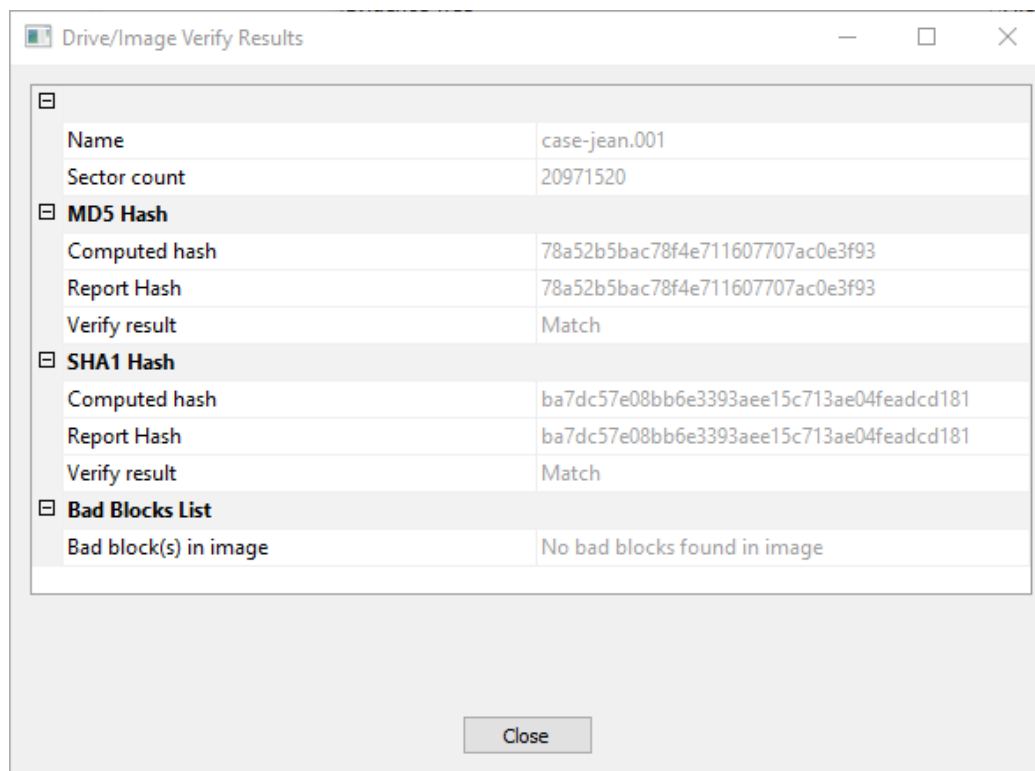
1.2 Zaistenie zariadenia

A. Zachytenie operačnej pamäte (volatile memory)

- Pripojenie čistého USB so spusteným nástrojom Magnet RAM Capture.
- Vytvorenie obrazu operačnej pamäte (formát RAW).
- Hashovanie obrazu RAM hneď po vytvorení (MD5/SHA-1).

B. Zachytenie disku

- Spustenie Exterro FTK Imager z externého SSD.
- Vytvorenie kompletného obrazu disku.
- Overenie integrity pomocou hashov (MD5 a SHA-1).



Obrázok 2 Hash obrazu disku

Spôsob uchovania digitálnych dôkazov

Zachovanie dôvernosti

- Všetky kópie (RAM a disk) sú uchovávané v zabezpečenom úložisku (zamknutá skrinka).
- Prístup kú kópiám má iba poverený vyšetrovací tím.

Zachovanie integrity

- Každý súbor má hash (MD5 a SHA-1) uložený samostatne.
- Zmeny sú sledované – žiadna modifikácia bez zaznamenania a autorizácie.
- Periodická re-verifikácia hashov počas vyšetrovania.

Zachovanie dostupnosti

- Minimálne dve kópie každého dôkazu – hlavná a pracovná.
- Kópie sú uchovávané na oddelených miestach.
- Je vedená dokumentácia o mieste uloženia, dátume, prístupe a zodpovednej osobe.

4. Vytvážovanie

Použité nástroje

- Exterro FTK Imager v4.7.3.81 – získanie geometrie disku
- Autopsy v4.22.0 – kategorizácia údajov z obrazu disku

Geometria pevného disku

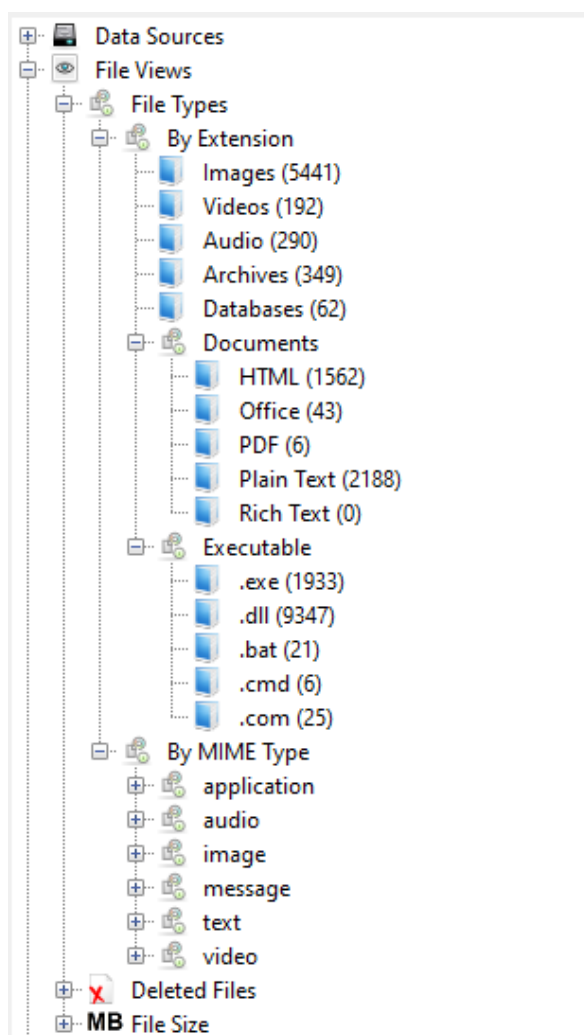
[-] Disk	
[-] Verification Hashes	
MD5 verification hash	78a52b5bac78f4e711607707ac0e3f93
[-] Drive Geometry	
Bytes per Sector	512
Sector Count	20,971,520

Obrázok 3 Geometria pevného disku

Systémové informácie

- Name: JEAN-13FBF038A3
- Program Name: Microsoft Windows XP Service Pack 3
- Processor Architecture: x86
- Temporary Files Directory: %SystemRoot%\TEMP
- Path: C:\WINDOWS
- Product ID: 55274-640-0690141-23940
- Owner: Jean User

Kategorizácia údajov z obrazu disku Jean Jones



Obrázok 4 Prehľad súborov

Typy súborov podľa prípony	Typ súboru	Počet súborov	Prípony súborov
	Obrázky	5441	.jpg, .jpeg, .png, .psd, .nef, .tiff, .bmp, .tec, .tif, .webp
	Videá	192	.aaf, .3gp, .asf, .avi, .m1v, .m2v, .m4v, .mp4, .mov, .mpeg, .mpg, .mpe, .mp4, .rm, .wmv, .mpv, .flv, .swf
	Audio	290	.aiff, .aif, .flac, .wav, .m4a, .ape, .wma, .mp2, .mp1, .mp3, .aac, .mp4, .m4p, .m1a, .m2a, .m4r, .mpa, .m3u, .mid, .midi, .ogg

	Archívy	349	.zip, .rar, .7zip, .7z, .arj, .tar, .gzip, .bzip, .bzip2, .cab, .jar, .cpio, .ar, .gz, .tgz, .bz2
	Databázy	62	.db, .db3, .sqlite, .sqlite3
Dokumenty	HTML	1562	.htm, .html
	Office	43	.doc, .docx, .odt, .xls, .xlsx, .ppt, .pptx
	PDF	6	.pdf
	Plain Text	2188	.txt
	Rich Text	0	.rtf
Spustiteľné súbory	.exe	1933	.exe
	.dll	9347	.dll
	.bat	21	.bat
	.cmd	6	.cmd
	.com	25	.com

Tabuľka 1 Typy súborov podľa prípony

Kategórie súborov určené na analýzu

Prehľad, ktoré časti v Autopsy je potrebné analyzovať pre každú digitálnu stopu:

1. Metadáta uniknutého súboru

- Data Artifacts - Metadata (75 nálezov)
- Data Artifacts - Recent Documents
- File Types - Documents (najmä Office, PDF)
- Analysis Results - EXIF Metadata

2. E-mailová komunikácia

- Data Artifacts - E-Mail Messages (261 správ)
- Data Artifacts - Communication Accounts (11 účtov)
- Prílohy v emailoch

3. História prehliadača a sieťovej aktivity

- Data Artifacts - Web History (5339 záznamov)
- Data Artifacts - Web Bookmarks (97)
- Data Artifacts - Web Cookies (406)
- Data Artifacts - Web Downloads (3)
- Data Artifacts - Web Search (238)
- Potrebne analyzovať hlavne cookies a prihlásenia na fórum konkurencie

4. Aktivita používateľa

- Data Artifacts - Recent Documents (9)
- Data Artifacts - Run Programs (126 programov)
- Data Artifacts - Installed Programs (40 programov)
- Ktoré súbory boli naposledy spúšťané a otvorené
- Aké programy boli používané

5. USB a externé zariadenia

- Data Artifacts - USB Device Attached (14 zariadení)
- Názov USB zariadenia, časy pripojenia a ID zariadení

6. Prenos súborov - Cloud/FTP aplikácie

- Data Artifacts - Installed Programs (Dropbox, Google Drive, FTP klienti)
- Data Artifacts - Web History (zistiť, či Jean navštevovala webové rozhrania cloud služieb)

7. Logy systému a bezpečnostné udalosti

- Data Artifacts - Operating System Information
- Data Artifacts - Installed Programs (ak bol inštalovaný RDP klient alebo iné nástroje)

8. Kontrola podozrivej aktivity

- File Types - By Extension - Executable (.exe, .dll, .bat, .cmd)
- Data Artifacts - Run Programs
- Analysis Results - Extension Mismatch Detected (223 prípadov)
- Analysis Results - User Content Suspected (97 prípadov)
- Podozrivé .exe súbory v miestach ako Temp, Startup

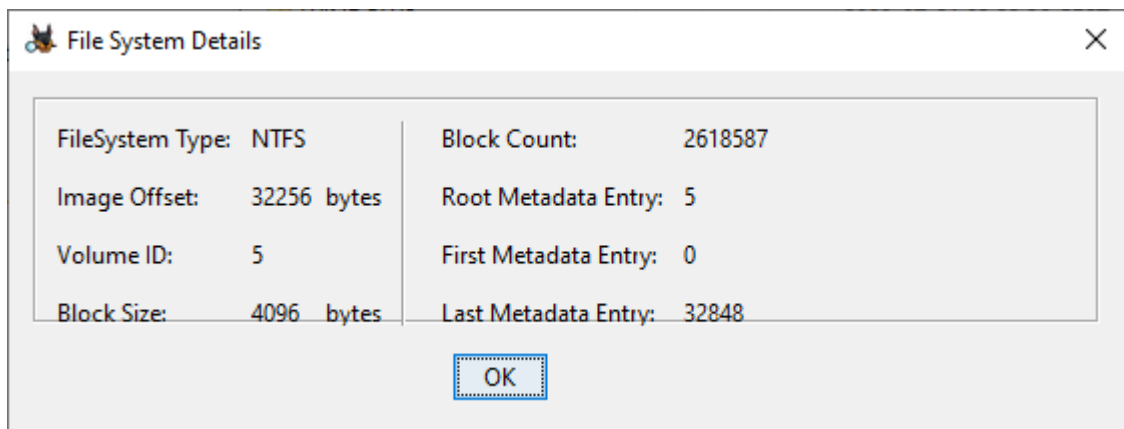
Dodatočné poznámky:

- Deleted Files – môžu tam byť zmazané dôkazy
- Keyword Hits – hľadanie mien, emailov, názvov súborov, cloudových služieb
- Web Categories – kategorizácia webov, ktoré Jean navštívila (hľadanie návštevy fór)

Súborový systém

Identifikovaný súborový systém: NTFS (New Technology File System)

- typický pre pracovné Windows laptopy
- podporuje práva, ACL, a obnovu zmazaných dát



Obrázok 5 Detaily súborového systému

Reťazec starostlivosti (Chain of custody)

Číslo:	001	Typ súboru:	raw	Obnovený súbor:	nie	Veľkosť:	17.9 GB
Popis prípadu:		Únik dôverných informácií					
Názov súboru:		memdump					
Miesto získania digitálnej stopy:		Pracovný laptop Jean Jones					
Poznámky:		Zaistenie potenciálnej digitálnej stopy z operačnej pamäti					
Časové pečiatky							

Access:	21/07/2008 16:38:29		Modify:	Change:	
Digitálny odtlačok (heš)	MD5	D9B1A9868C6BF5EC7F26D9C5D82AD32B			
	SHA1	F18883E34ECFCD67907E9B56EB5F3A6020F6C6BF			
Časová pečiatka		Akcia vykonaná s digitálnou stopou			
21/07/2008 16:38:29		Vytvorenie kópie operačnej pamäti.			
21/07/2008 16:53:08		Kontrola integrity obrazu overením zhody digitálnych otláčkov.			
21/07/2008 16:56:25		Zaistenie ukončené.			

Tabuľka 2 Chain of custody: obraz RAM

Číslo:	002	Typ súboru:	EnCase	Obnovený súbor:	nie	Veľkosť:	2.9 GB
Popis prípadu:	Únik dôverných informácií						
Názov súboru:	nps-2008-jean						
Miesto získania digitálnej stopy:	Pracovný laptop Jean Jones						
Poznámky:	Zaistenie potenciálnej digitálnej stopy z obrazu disku						
Časové pečiatky							
Access:	21/07/2008 17:10:05		Modify:		Change:		
Digitálny odtlačok (heš)	MD5	78a52b5bac78f4e711607707ac0e3f93					

	SHA1	ba7dc57e08bb6e3393aee15c713ae04feadcd181
Časová pečiatka	Akcia vykonaná s digitálnou stopou	
21/07/2008 17:10:05	Vytvorenie dvoch kópií operačnej pamäti.	
21/07/2008 17:25:10	Kontrola integrity obrazu overením zhody digitálnych otlačkov.	
21/07/2008 17:28:35	Zaistenie ukončené.	

Tabuľka 3 Chain of custody: obraz disku

5. Analýza

Použité nástroje

- Autopsy v4.22.0 sa použil na analýzu obrazu disku
- HxD Editor 2.5.0.0 (x86-64) sa použil na analýzu obrazu operačnej pamäte
- Exterro FTK Imager v4.7.3.81 pre doplnenie analýzy obrazu disku
- Kernel Outlook PST Viewer v20.3 pre prehliadanie PST súboru

Pred začatím analýzy bola overená integrita forenzných obrazov s využitím hash algoritmov – MD5 a SHA-1.

5.1. Analýza digitálnej stopy č.001

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
47AE72200	72	65	6A	65	63	74	65	64	4C	49	22	3A	66	61	6C	73	rejectedLI":false
47AE72210	65	2C	22	63	6F	6E	73	65	6E	74	65	64	41	6C	6C	22	e,"consentedAll"
47AE72220	3A	66	61	6C	73	65	2C	22	67	72	61	6E	75	6C	61	72	:false,"granular
47AE72230	53	74	61	74	75	73	22	3A	7B	22	76	65	6E	64	6F	72	Status":{"vendor
47AE72240	43	6F	6E	73	65	6E	74	22	3A	22	4E	4F	4E	45	22	2C	Consent":"NONE",
47AE72250	22	76	65	6E	64	6F	72	4C	65	67	49	6E	74	22	3A	22	"vendorLegInt":
47AE72260	41	4C	4C	22	2C	22	70	75	72	70	6F	73	65	43	6F	6E	ALL","purposeCon
47AE72270	73	65	6E	74	22	3A	22	4E	4F	4E	45	22	2C	22	70	75	sent":"NONE","pu
47AE72280	72	70	6F	73	65	4C	65	67	49	6E	74	22	3A	22	41	4C	rposeLegInt":"AL
47AE72290	4C	22	2C	22	70	72	65	76	69	6F	75	73	4F	70	74	49	L","previousOptI
47AE722A0	6E	41	6C	6C	22	3A	66	61	6C	73	65	2C	22	64	65	66	nAll":false,"def
47AE722B0	61	75	6C	74	43	6F	6E	73	65	6E	74	22	3A	74	72	75	aultConsent":tru
47AE722C0	65	7D	2C	22	68	61	73	43	6F	6E	73	65	6E	74	44	61	e),"hasConsentDa
47AE722D0	74	61	22	3A	66	61	6C	73	65	2C	22	63	6F	6E	73	65	ta":false,"conse
47AE722E0	6E	74	65	64	54	6F	41	6E	79	22	3A	66	61	6C	73	65	ntedToAny":false
47AE722F0	7D	7D	2C	22	76	65	72	73	69	6F	6E	22	3A	31	7D	00	},"version":1}).
47AE72300	7A	00	00	00	72	00	00	00	68	74	74	70	73	3A	2F	2F	z...r...https://
47AE72310	77	77	77	2E	63	73	6F	6F	6E	6C	69	6E	65	2E	63	6F	www.csoonline.co
47AE72320	6D	2F	61	72	74	69	63	6C	65	2F	35	37	30	36	39	37	m/article/570697
47AE72330	2F	31	35	2D	73	69	67	6E	73	2D	79	6F	75	76	65	2D	/15-signs-youve-
47AE72340	62	65	65	6E	2D	68	61	63	6B	65	64	2D	61	6E	64	2D	been-hacked-and-
47AE72350	68	6F	77	2D	74	6F	2D	66	69	67	68	74	2D	62	61	63	how-to-fight-bac
47AE72360	6B	2E	68	74	6D	6C	0A	39	35	31	33	39	33	30	37	34	k.html.951393074
47AE72370	37	39	39	37	36	30	33	39	30	36	00	00	00	00	00	00	7997603906.....
47AE72380	00	00	00	00	00	00	00	00	C9	CF	20	FC	8F	9B	10	00	ĚD už>...
47AE72390	C0	4D	4B	15	17	8E	D0	95	C9	00	00	00	8F	9B	FF	FF	RMK..ŽB+Ě...Ž>''
47AE723A0	00	00	29	02	4E	56	52	4D	00	00	00	00	00	00	00	00	..).NVRM.....
47AE723B0	D4	47	F0	CA	00	00	00	00	D0	03	1F	02	81	9B	FF	FF	ÔGdĚ....Ď....>''
47AE723C0	00	00	00	00	00	00	00	00	A0	84	87	FE	8F	9B	FF	FF	„ťž>''
47AE723D0	00	00	00	00	00	00	00	00	C0	BC	51	F4	8F	9B	FF	FF	ŘIQôž>''
47AE723E0	C0	C6	71	FC	8F	9B	FF	FF	D4	47	F0	CA	00	00	00	00	ŘCqūž>''ÔGdĚ....
47AE723F0	C8	5C	F2	FE	8F	9B	FF	FF	38	8A	E3	3A	05	F8	FF	FF	Č\ŋťž>''ôšā:..Ě''
47AE72400	68	8B	E3	3A	05	F8	FF	FF	00	00	00	00	00	00	00	00	h<ā:..Ě''.....
47AE72410	D8	FF	FF	FF	00	00	00	00	90	3A	56	EE	8F	9B	FF	FF	Ř''''':Viž>''
47AE72420	18	00	00	00	00	00	00	00	08	00	00	00	00	00	00	00	:Viž>''
47AE72430	08	00	00	00	00	00	00	00	38	8A	E3	3A	05	F8	FF	FF	8šā:..Ě''
47AE72440	68	8B	E3	3A	05	F8	FF	FF	00	00	00	00	00	00	00	00	h<ā:..Ě''.....
47AE72450	D8	FF	FF	FF	00	00	00	00	90	3A	56	EE	8F	9B	FF	FF	Ř''''':Viž>''
47AE72460	18	00	00	00	00	00	00	00	08	00	00	00	00	00	00	00	:Viž>''
47AE72470	08	00	00	00	00	00	00	00	38	8A	E3	3A	05	F8	FF	FF	8šā:..Ě''

Checksum	Search (1774 hits)	
Offset	Excerpt (hex)	Excerpt (text)
23223CD	69 67 6E 73 2D 79 6F 75 76 65 2D 62 65 65 6E 2D 68 61 63 6B 65 64 2D 61 6E 64 2D 68 6F 77 2D 74	igns-youve-been-hacked-and-how-t
6E6E547	69 67 6E 73 2D 79 6F 75 76 65 2D 62 65 65 6E 2D 68 61 63 6B 65 64 2D 61 6E 64 2D 68 6F 77 2D 74	igns-youve-been-hacked-and-how-t
6E6E711	69 67 6E 73 2D 79 6F 75 76 65 2D 62 65 65 6E 2D 68 61 63 6B 65 64 2D 61 6E 64 2D 68 6F 77 2D 74	igns-youve-been-hacked-and-how-t
9553BFC	2B 69 66 2B 69 2B 68 61 76 65 2B 62 65 65 6E 2B 68 61 63 6B 65 64 26 6F 71 3D 68 6F 77 2B 74 6F	+if+i+have+been+hackedgq=how+to
B3F79DB	2B 69 66 2B 69 2B 68 61 76 65 2B 62 65 65 6E 2B 68 61 63 6B 65 64 26 6F 71 3D 68 6F 77 2B 74 6F	+if+i+have+been+hackedgq=how+to
C75C816	77 2D 69 66 2D 79 6F 75 76 65 2D 62 65 65 6E 2D 68 61 63 6B 65 64 01 00 00 00 02 00 00 00 1A 00	w-if-youve-been-hacked.....
E8D4395	69 67 6E 73 2D 79 6F 75 76 65 2D 62 65 65 6E 2D 68 61 63 6B 65 64 2D 61 6E 64 2D 68 6F 77 2D 74	igns-youve-been-hacked-and-how-t
E8D4A4D	6D 70 75 74 65 72 20 68 61 73 20 62 65 65 6E 20 68 61 63 6B 65 64 2E 20 49 6E 20 74 68 65 20 65	mputer has been hacked. In the e
E8D4D54	6D 70 75 74 65 72 20 68 61 73 20 62 65 65 6E 20 68 61 63 6B 65 64 2E 20 49 6E 20 74 68 65 20 65	mputer has been hacked. In the e
EC53440	2B 69 66 2B 69 2B 68 61 76 65 2B 62 65 65 6E 2B 68 61 63 6B 65 64 26 6F 71 3D 68 6F 77 2B 74 6F	+if+i+have+been+hackedoq=how+to

Obrázok 6 Obraz operačnej pamäte

Zistený nález v obraze operačnej pamäti

V nástroji HxD bola vykonaná analýza dátových zvyškov, počas ktorej sa identifikovali texty naznačujúce, že Jean navštevovala webové stránky súvisiace s identifikovaním hackerských útokov. Na základe toho možno usudzovať, že mala podozrenie, že sa stala obeťou kybernetického útoku.

5.2. Analýza digitálnej stopy č.002

1. Slack priestor

- Súbor: m57biz.xls-slack
- Cesta: /Documents and Settings/Jean/Desktop/m57biz.xls
- Veľkosť: 3072 bajtov

Interpretácia: Slack obsahuje zvyškové dáta z klastra prideleného súboru.

2. Linky (LNK súbory) a artefakty Recent Documents

- m57biz.lnk v:
 - /Recent/
 - /Office/Recent/
- Veľkosť: ~408–468 bajtov
- Dátum: 2008-07-20 03:28:04

Interpretácia: Jean otvorila súbor cez MS Excel, čo spôsobilo uloženie LNK súborov ako „nedávno otvorené dokumenty“.

3. Prefetch evidencia

- Súbor: EXCEL.EXE-1C75F8D6.pf
- Cesta: /WINDOWS/Prefetch/
- Dátum: 2008-07-20 03:27:50

Interpretácia: Excel bol spustený krátko pred otvorením súboru, čo podporuje hypotézu o aktívnom použití dokumentu.

4. Registry a index.dat artefakty

- Súbor m57biz.xls sa objavuje v:
 - NTUSER.DAT (RecentDocs, AIM chat, atď.)

- index.dat v IE history

Interpretácia - dokument bol:

- prezeraný cez Excel
- uložený ako príloha e-mailu

5. Unallocated fragments

- Súbor bol detekovaný aj v unallocated častiach disku:
 - Unalloc_56125_4328603136_6097866240
 - Unalloc_56125_40448_2907565568

Interpretácia: Staršie alebo zmazané inštancie tohto súboru. Možné sú fragmenty po odstránení/presune.

6. Fyzická prítomnosť súboru „m57biz.xls“

Súbor sa nachádzal priamo na pracovnej ploche používateľa Jean.

- Cesta: /Documents and Settings/Jean/Desktop/m57biz.xls
- Veľkosť: 291840 B
- Stav: Allocated (platný/prítomný súbor)

A. Obsah súboru

HexTextApplicationFile MetadataOS AccountData ArtifactsAnalysis ResultsContext

StringsExtracted TextTranslation

Page: 1 of 1 Page←→Matches on page: - of - Match←→100%🔍🔍

Sheet1

M57.biz company					
Name		Position	Salary	SSN (for background check)	
Alison	Smith	President	\$140,000	103-44-3134	
Jean	Jones	CFO	\$120,000	432-34-6432	
Programmers:					
Bob	Blackman	Apps 1	90,000	493-46-3329	
Carol	Canfred	Apps 2	110,000	894-33-4560	
Dave	Daubert	Q&A	67,000	331-95-1020	
Emmy	Arlington	Entry Level	57,000	404-98-4079	
Marketing					
Gina	Tangers	Creative 1	80,000	980-97-3311	
Harris	Jenkins	G & C	105,000	887-33-5532	
BizDev					
Indy	Counterching		Outreach	240,000	123-45-6789
Annual Salaries				\$1,009,000	
Benefits		30%	\$302,700		
Total Salaries + Benefits				\$1,311,700	
Monthly burn				\$109,308.33	

&C&G

Obrázok 7 Obsah súboru

- Súbor obsahuje osobné údaje zamestnancov (mená, platy, pozície a SSN – ide jednoznačne o citlivé dáta).

Interpretácia: Podpora hypotézy, že dokument mohol byť požadovaný pre investorov – ako tvrdí Jean.

B. Pôvod súboru

```

-----METADATA-----
Content-Type: application/vnd.ms-excel
X-TIKA:Parsed-By: org.apache.tika.parser.DefaultParser
X-TIKA:Parsed-By-Full-Set: org.apache.tika.parser.DefaultParser
dc:creator: Alison Smith
dcterms:created: 2008-06-12T15:13:51Z
dcterms:modified: 2008-07-20T01:28:03Z
extended-properties:Application: Microsoft Excel
extended-properties:Company: M57.BIZ
extended-properties:TotalTime: 0
meta:last-author: Jean User

```

Obrázok 8 Vnútorne metadáta súboru

NTFS Information	
MFT Record Number	32,712 (33497088)
Date Changed (MFT)	20/07/2008 01:28:04
Resident	False
Offline	False
Sparse	False
Temporary	False
Owner SID	S-1-5-21-484763869-796845957-839522115-1004
Owner Name	Jean
Group SID	S-1-5-21-484763869-796845957-839522115-513
Group Name	None
Filename Date Created (MFT)	20/07/2008 01:28:03
Filename Date Modified (MFT)	20/07/2008 01:28:03
Filename Date Accessed (MFT)	20/07/2008 01:28:03
Filename Date Changed (MFT)	20/07/2008 01:28:03
Filename File Size (MFT)	291,840
Filename Physical Size (MFT)	294,912
INDX Entry Filename	m57biz.xls
INDX Entry File Size	291,840
INDX Entry Physical Size	294,912
Date Created Index Entry Time	20/07/2008 01:28:03
Date Modified Index Entry Time	20/07/2008 01:28:03
Date Accessed Index Entry Time	20/07/2008 01:28:03
Date Changed Index Entry Time	20/07/2008 01:28:04

Obrázok 9 NTFS informácie súboru

- Autor dokumentu podľa vnútorných metadát súboru: Alison Smith
- Posledný editor podľa vnútorných metadát súboru: Jean User
- Vlastník súboru na disku podľa NTFS informácií: Jean

C. Časové údaje

The screenshot shows the 'File Metadata' tab in a forensic tool. It displays various attributes for a file named 'm57biz.xls'. The 'Modified', 'Accessed', 'Created', and 'Changed' timestamps are all set to 2008-07-20 03:28:03 CEST, except for 'Changed' which is 04 seconds later. Below this, the 'From The Sleuth Kit istat Tool:' section provides MFT entry details, including sequence numbers and timestamps in both CEST and UTC (CES).

Attribute	Value
Name:	/img_case-jean.001/vol_vol2/Documents and Settings/Jean/Desktop/m57biz.xls
Type:	File System
MIME Type:	application/vnd.ms-excel
Size:	291840
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2008-07-20 03:28:03 CEST
Accessed:	2008-07-20 03:28:03 CEST
Created:	2008-07-20 03:28:03 CEST
Changed:	2008-07-20 03:28:04 CEST
MD5:	e23a4eb7f2562f53e88c9dca8b26a153
SHA-256:	34456b5f714dc9d8dd23c742d54c3f5f582ecb042bc1c4d3042b88203863779f
Hash Lookup Results:	UNKNOWN
Internal ID:	4014

From The Sleuth Kit istat Tool:

MFT Entry Header Values:
Entry: 32712 Sequence: 2
\$LogFile Sequence Number: 172434688
Allocated File
Links: 1

\$STANDARD_INFORMATION Attribute Values:
Flags: Archive
Owner ID: 0
Security ID: 1067 (S-1-5-21-484763869-796845957-839522115-1004)
Created: 2008-07-20 03:28:03.656250000 (CES)
File Modified: 2008-07-20 03:28:03.953125000 (CES)
MFT Modified: 2008-07-20 03:28:04.046875000 (CES)
Accessed: 2008-07-20 03:28:03.953125000 (CES)

Obrázok 10 Metadáta súborového systému

- Vytvorenie (vnútorné metadáta): 2008-06-12T15:13:51Z (UTC) – zrejme vytvorené Alison.
- Vytvorenie (súborové metadáta) je o 38 dní neskôr než dokumentové created - typické pre kopírovanie.
- V súborových metadátach je Changed len 1s po Created - normálne pri kopírovaní na disk, kde systém zapisuje nové vlastnosti (napr. atribúty súboru).
- Posledná úprava v súborových metadátach: 2008-07-20 01:28:03Z (čo zodpovedá približne 03:28 CEST v NTFS).

- Všetky NTFS časové pečiatky sú takmer identické: súbor bol vytvorený, otvorený a uložený v rovnakom čase — tzn. krátkodobú interakciu.

Pozn.: Dátumy úpravy a dátumy súborového systému sú s rozdielom 2 hodín, pretože vnútorné metadáta sú uložené v UTC (Z znamená Zulu time = UTC) a súborový systém ukazuje lokálny čas (CEST = Central European Summer Time, teda UTC+2).

Interpretácia: Čas vytvorenia dokumentu a jeho posledné uloženie sú od seba dva mesiace, čo je nezvyčajné. Súbor obsahuje Alison Smith ako autora súboru. To naznačuje, že Alison vytvorila súbor pred dvoma mesiacmi.

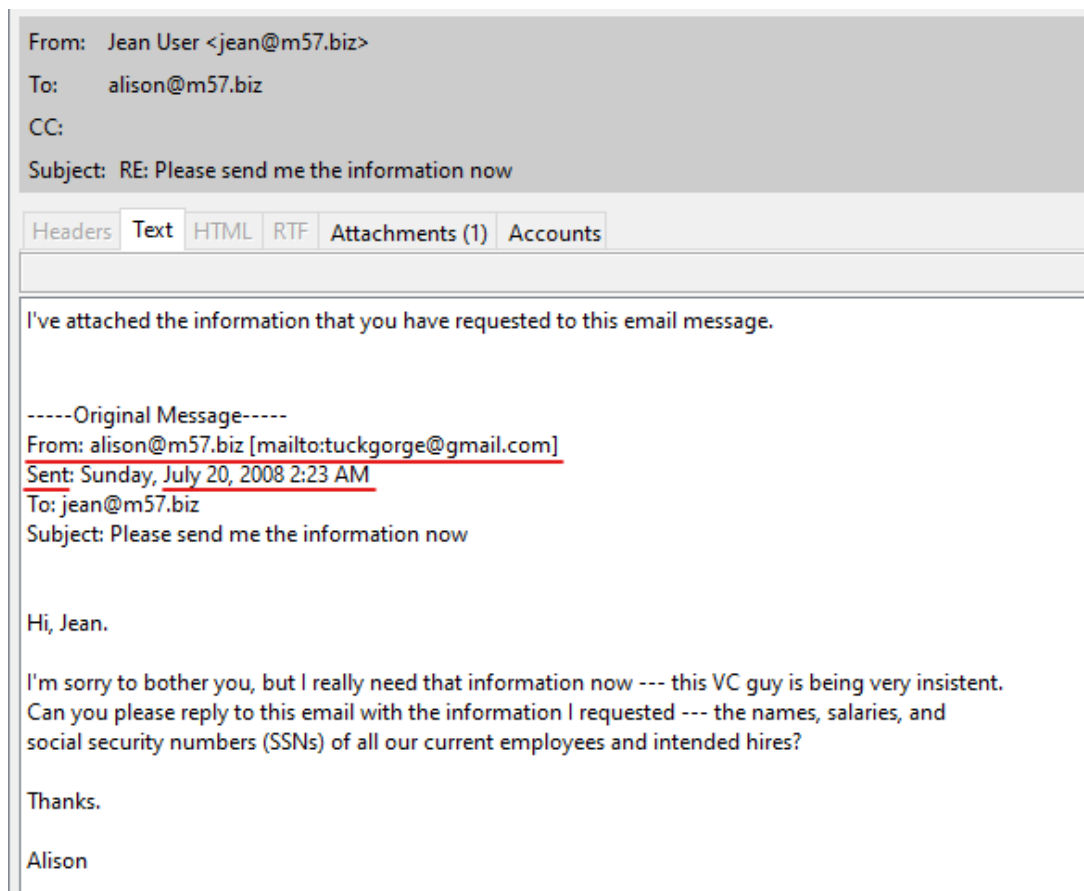
7. Súbor vo vnútri outlook.pst

Metadata	
Name:	/img_case-jean.001/vol_vol2/Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst/m57biz.xls
Type:	Derived
MIME Type:	application/vnd.ms-excel
Size:	291840
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2008-07-20 03:28:03 CEST
Accessed:	0000-00-00 00:00:00
Created:	2008-07-20 03:28:03 CEST
Changed:	0000-00-00 00:00:00
MD5:	e23a4eb7f2562f53e88c9dca8b26a153
SHA-256:	34456b5f714dc9d8dd23c742d54c3f5f582ecb042bc1c4d3042b88203863779f
Hash Lookup Results:	UNKNOWN
Internal ID:	63207

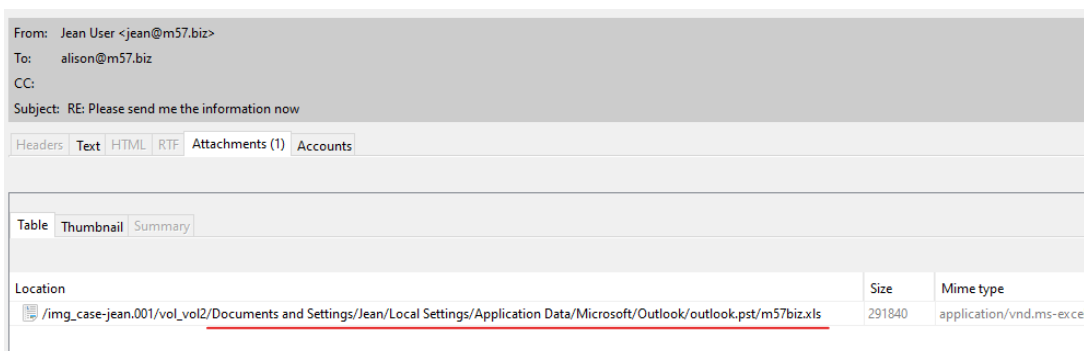
Obrázok 11 Metadáta súborového systému

- Cesta: /Documents and Settings/Jean/Local Settings/Application Data/Microsoft/Outlook/outlook.pst/m57biz.xls
- Veľkosť: 291840 bajtov
- Dátum: 2008-07-20 03:28:03 CEST v NTFS
- Súbor má rovnaký hash ako súbor na ploche, čo potvrdzuje identickú kópiu

A. Vyhľadanie e-mailovej komunikácie obsahujúcu súbor „m57biz.xls“ ako prílohu



Obrázok 12 Email s prílohou



Obrázok 13 Príloha e-mailu

- Jean prišiel spoofnutý e-mail od neznámeho útočníka, ktorý predstieral, že je Alison Smith, pričom skutočná adresa odosielateľa je „tuckgorge@gmail.com“
- Jean poslala útočníkovi kompromitovaný súbor e-mailom.

B. Analýza e-mailovej komunikácie medzi Jean a tuckgeorge@gmail.com

Property Name	Property Tag	Property Type	Data
<FILTER>	<FILTER>	<FILTER>	<FILTER>
PR_SENT_REPRESENTING_NAME	0x0042001E	Extended ASCII string	<u>alison@m57.biz</u>
PR_RCVD_REPRESENTING_ENTRYID	0x00430102	Binary data	00 00 00 00 81 2B 1F A4 BE A3 10 19 9D 6E 00 DD 01 0F 54 C
PR_RCVD_REPRESENTING_NAME	0x0044001E	Extended ASCII string	Jean User
PR_RECEIVED_BY_SEARCH_KEY	0x00510102	Binary data	53 4D 54 50 3A 4A 45 41 4E 40 4D 35 37 2E 42 49 5A 00
PR_RCVD_REPRESENTING_SEARCH_KEY	0x00520102	Binary data	53 4D 54 50 3A 4A 45 41 4E 40 4D 35 37 2E 42 49 5A 00
PR_SENT_REPRESENTING_ADDRTYPE	0x0064001E	Extended ASCII string	SMTP
PR_SENT_REPRESENTING_EMAIL_ADDRESS	0x0065001E	Extended ASCII string	<u>tuckgorge@gmail.com</u>
PR_CONVERSATION_TOPIC	0x0070001E	Extended ASCII string	Please send me the information now
PR_RECEIVED_BY_ADDRTYPE	0x0075001E	Extended ASCII string	SMTP
PR_RECEIVED_BY_EMAIL_ADDRESS	0x0076001E	Extended ASCII string	jean@m57.biz
PR_RCVD_REPRESENTING_ADDRTYPE	0x0077001E	Extended ASCII string	SMTP
PR_RCVD_REPRESENTING_EMAIL_ADDRESS	0x0078001E	Extended ASCII string	jean@m57.biz

Hi, Jean.

I'm sorry to bother you, but I really need that information now --- this VC guy is being very insistent. Can you please reply to this email with the information I requested --- the names, salaries, and social security numbers (SSNs) of all our current employees and intended hires?

Thanks.

Alison

Obrázok 14 Informácie o odosielateľovi e-mailu

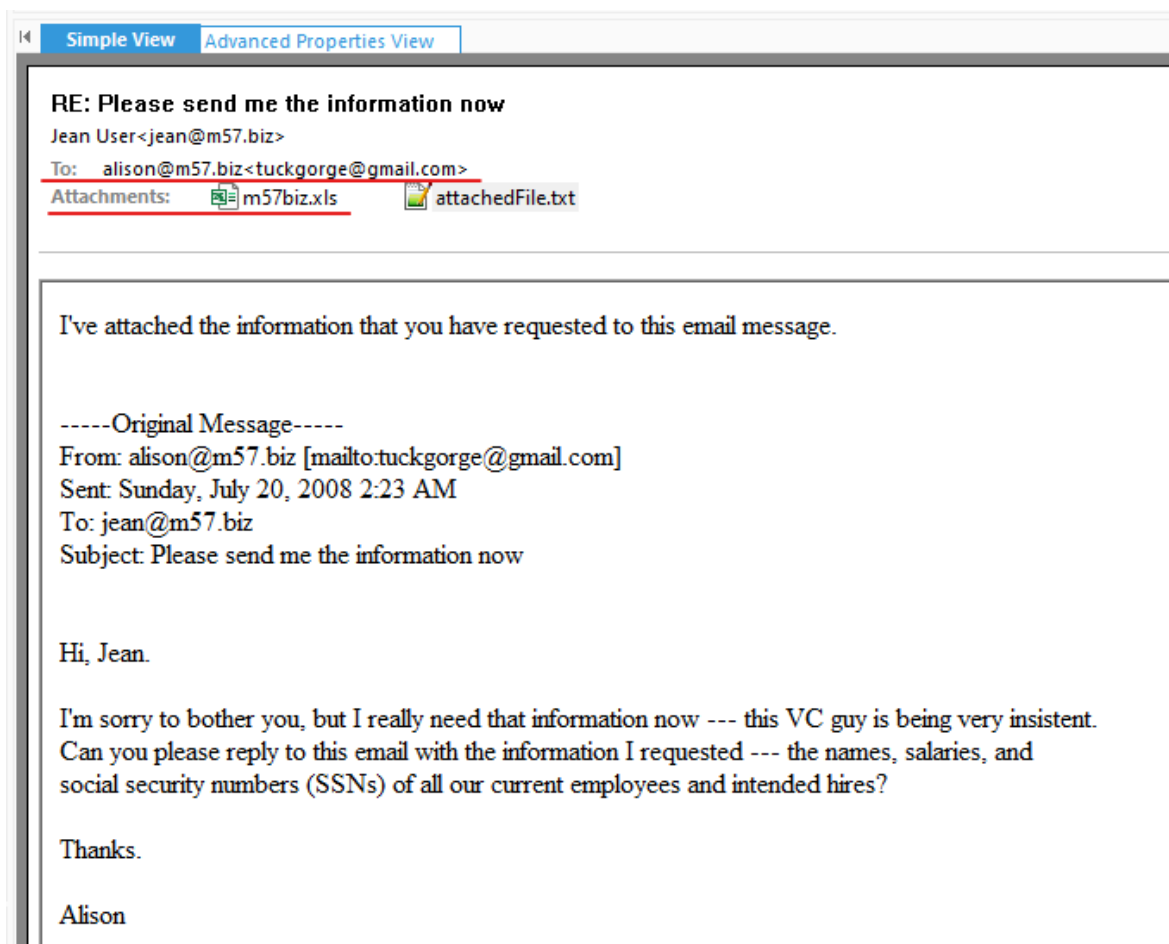
- Meno odosielateľa e-mailu je Alison Smith, ale e-mailová adresa odosielateľa je „tuckgorge@gmail.com“

Property Name	Property Tag	Property Type	Data
<FILTER>	<FILTER>	<FILTER>	<FILTER>
PR_TRANSPORT_MESSAGE_HEADERS	0x007D001E	Extended ASCII string	Return-Path: <simsong@xy.dreamhostps.com> X-Original-To: jean@
PR_SENDER_ENTRYID	0x0C190102	Binary data	00 00 00 00 81 2B 1F A4 BE A3 10 19 9D 6E 00 DD 01 0F 54 02
PR_SENDER_NAME	0x0C1A001E	Extended ASCII string	<u>alison@m57.biz</u>
PR_SENDER_SEARCH_KEY	0x0C1D0102	Binary data	53 4D 54 50 3A 54 55 43 4B 47 4F 52 47 45 40 47 4D 41 49 4C 2
PR_SENDER_ADDRTYPE	0x0C1E001E	Extended ASCII string	SMTP
PR_SENDER_EMAIL_ADDRESS	0x0C1F001E	Extended ASCII string	<u>tuckgorge@gmail.com</u>
PR_DISPLAY_TO	0x0E04001E	Extended ASCII string	<u>jean@m57.biz</u>
PR_MESSAGE_FLAGS	0x0E070003	Integer 32-bit signed	1
PR_MESSAGE_SIZE	0x0E080003	Integer 32-bit signed	2278
PR_BODY	0x1000001E	Extended ASCII string	Hi, Jean. I'm sorry to bother you, but I really need that information n
PR_INTERNET_MESSAGE_ID	0x1035001E	Extended ASCII string	<20080720012245.177343B1DA8@xy.dreamhostps.com>
PR_INTERNET_RETURN_PATH	0x1046001E	Extended ASCII string	<u>simsong@xy.dreamhostps.com</u>
PR_ICON_INDEX	0x10800003	Integer 32-bit signed	261
PR_LAST_VERB_EXECUTED	0x10810003	Integer 32-bit signed	103
PR_LAST_VERB_EXECUTION_TIME	0x10820040	Windows Filetime (64-bit)	20/07/2008 03:28:00
PR_CREATION_TIME	0x30070040	Windows Filetime (64-bit)	20/07/2008 03:26:11
PR_LAST_MODIFICATION_TIME	0x30080040	Windows Filetime (64-bit)	20/07/2008 03:28:42

Return-Path: <simsong@xy.dreamhostps.com>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx2.g.dreamhost.com
Received: from smarty.dreamhost.com [sd-green-bigip-66.dreamhost.com [208.97.132.66]]
by spunkymail-mx2.g.dreamhost.com (Postfix) with ESMTP id 2D1DC7278E
for <jean@m57.biz>; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
Received: from xy.dreamhostps.com [apache2-xy.xy.dreamhostps.com [208.97.188.9]]
by smarty.dreamhost.com (Postfix) with ESMTP id 138E5EE221
for <jean@m57.biz>; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
Received: by xy.dreamhostps.com (Postfix, from userid 558838)
id 177343B1DA8; Sat, 19 Jul 2008 18:22:45 -0700 (PDT)
To: jean@m57.biz
From: tuckgorge@gmail.com (alison@m57.biz)
subject: Please send me the information now
Message-Id: <20080720012245.177343B1DA8@xy.dreamhostps.com>
Date: Sat, 19 Jul 2008 18:22:45 -0700 (PDT)

Obrázok 15 PR_TRANSPORT_MESSAGE_HEADERS

- Návratová adresa je „simsong@xy.dreamhostps.com“



Obrázok 16 Odoslanie kompromitovaného súboru

- Jean odoslala kompromitovaný súbor, ktorý išiel v skutočnosti na adresu „tuckgorge@gmail.com“

Property Name	Property Tag	Property Type	Data
<FILTER>	<FILTER>	<FILTER>	<FILTER>
PR_DISPLAY_TO	0x0E04001E	Extended ASCII string	alison@m57biz
PR_MESSAGE_FLAGS	0x0E070003	Integer 32-bit signed	17
PR_MESSAGE_SIZE	0x0E080003	Integer 32-bit signed	297082
PR_SENTMAIL_ENTRYID	0x0E0A0102	Binary data	00 00 00 00 31 87 F3 41 5D E6 DD 44 A0 1C 79 7B 81 55 6C C2 80 00 00
PR_BODY	0x1000001E	Extended ASCII string	I've attached the information that you have requested to this email message. ---Origir
PR_INTERNET_MESSAGE_ID	0x1035001E	Extended ASCII string	<NNEEKAKACNP0IIIMAAIIKIECBCAA@jean@m57.biz>
PR_IN_REPLY_TO_ID	0x1042001E	Extended ASCII string	<20080720012245.177343B1DA8@xy.dreamhostps.com>
PR_ICON_INDEX	0x10800003	Integer 32-bit signed	-1
PR_CREATION_TIME	0x30070040	Windows Filetime (64-bit)	20/07/2008 03:26:17
PR_LAST_MODIFICATION_TIME	0x30080040	Windows Filetime (64-bit)	20/07/2008 03:28:47

Obrázok 17 PR_IN_REPLY_TO_ID

- Adresa tuckgorge@hotmail.com pochádzala z domény xy.dreamhostps.com

5.3. Časová os udalostí

Časové pečiatky môžu byť dôležitými dôkazmi na preukázanie spojenia medzi obvineným, počítačom a trestným činom, na ktorý bol použitý. Napriek tomu existujú obmedzenia

týkajúce sa časových a dátumových pečiatok - sú obmedzené na určité časové pásmo a ovplyvnené presnosťou vnútorných hodín počítača, ktoré sa dajú ľahko upraviť.

Nižšie uvedené časové pečiatky a udalosti boli vyplývajú z dôkazov a korelujú s Jeaniným miestnym časovým pásmom. Údaje neboli sfalšované - kontrolné súčty súboru sa zhodujú.

1. Sobota 19.7.2008 16:39:57 (PDT)

Jean dostala e-mail s adresou spiatocnej adresy simsong@xy.dreamhostps.com so žiadosťou o dôverné firemné informácie

Property Name	Property Tag	Property Type	Data
<FILTER>	<FILTER>	<FILTER>	<FILTER>
PR_DISPLAY_TO	0x00000001E	Extended ASCII string	jean@emo.biz
PR_MESSAGE_FLAGS	0x0E070003	Integer 32-bit signed	1
PR_MESSAGE_SIZE	0x0E080003	Integer 32-bit signed	2378
PR_BODY	0x1000001E	Extended ASCII string	Jean, One of the potential investors that I've been dealing with has
PR_INTERNET_MESSAGE_ID	0x1035001E	Extended ASCII string	<20080719233957.64C683B1DAE@xy.dreamhostps.com>
PR_INTERNET_RETURN_PATH	0x1046001E	Extended ASCII string	simsong@xy.dreamhostps.com
PR_ICON_INDEX	0x10800003	Integer 32-bit signed	261
PR_LAST_VERB_EXECUTED	0x10810003	Integer 32-bit signed	103
PR_LAST_VERB_EXECUTION_TIME	0x10820040	Windows Filetime (64-bit)	20/07/2008 01:44:00
PR_CREATION_TIME	0x30070040	Windows Filetime (64-bit)	20/07/2008 01:40:36
PR_LAST_MODIFICATION_TIME	0x30080040	Windows Filetime (64-bit)	20/07/2008 01:44:40

Jean,
 One of the potential investors that I've been dealing with has asked me to get a background check of our current employees. Apparently they recently had some problems at some other company they funded.
 Could you please put together for me a spreadsheet specifying each of our employees, their current salary, and their SSN?
 Please do not mention this to anybody.
 Thanks.
 (ps: because of the sensitive nature of this, please do not include the text of this email in your message to me. Thanks.)

Obrázok 18 1. e-mail od útočníka

Simple View Advanced Properties View			
Property Name	Property Tag	Property Type	Data
<FILTER>	<FILTER>	<FILTER>	<FILTER>
PR_RECEIVED_BY_NAME	0x0040001E	Extended ASCII string	Jean User
PR_SENT_REPRESENTING_ENTRYID	0x00410102	Binary data	00 00 00 00 81 2B 1F A4 BE A3 10 19 9D 6E 00 DD 01 0F 54
PR_SENT_REPRESENTING_NAME	0x0042001E	Extended ASCII string	alison@m57.biz
PR_RCVD_REPRESENTING_ENTRYID	0x00430102	Binary data	00 00 00 00 81 2B 1F A4 BE A3 10 19 9D 6E 00 DD 01 0F 54
PR_RCVD_REPRESENTING_NAME	0x0044001E	Extended ASCII string	Jean User
PR_RECEIVED_BY_SEARCH_KEY	0x00510102	Binary data	53 4D 54 50 3A 4A 45 41 4E 40 4D 35 37 2E 42 49 5A 00
PR_RCVD_REPRESENTING_SEARCH_KEY	0x00520102	Binary data	53 4D 54 50 3A 4A 45 41 4E 40 4D 35 37 2E 42 49 5A 00
PR_SENT_REPRESENTING_ADDRTYPE	0x0064001E	Extended ASCII string	SMTP
PR_SENT_REPRESENTING_EMAIL_ADDRESS	0x0065001E	Extended ASCII string	alison@m57.biz
PR_CONVERSATION_TOPIC	0x0070001E	Extended ASCII string	background checks
PR_RECEIVED_BY_ADDRTYPE	0x0075001E	Extended ASCII string	SMTP

Hex Preview Txt Preview Unicode Txt Preview

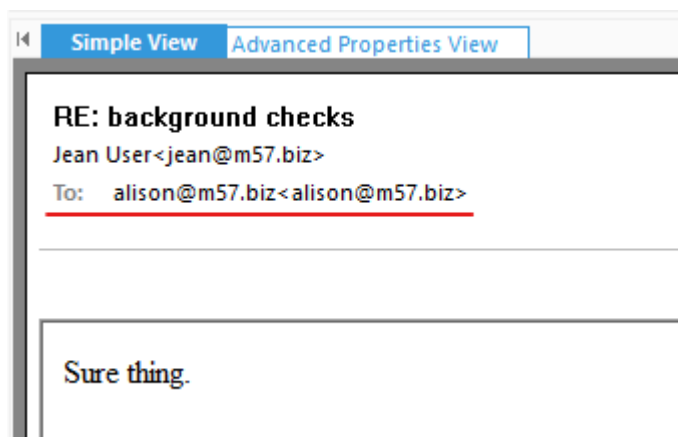
Return-Path: <simsong@xy.dreamhostps.com>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx8.g.dreamhost.com
Received: from smarty.dreamhost.com (sd-green-bigip-81.dreamhost.com [208.97.132.81])
by spunkymail-mx8.g.dreamhost.com (Postfix) with ESMTP id E32634D80F
for <jean@m57.biz>; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
Received: from xy.dreamhostps.com (apache2-xy.xy.dreamhostps.com [208.97.188.9])
by smarty.dreamhost.com (Postfix) with ESMTP id 6E408EE23D
for <jean@m57.biz>; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
Received: by xy.dreamhostps.com (Postfix, from userid 558838)
id 64C683B1DAE; Sat, 19 Jul 2008 16:39:57 -0700 (PDT)
To: jean@m57.biz
From: alison@m57.biz
subject: background checks
Message-Id: <20080719233957.64C683B1DAE@xy.dreamhostps.com>
Date: Sat, 19 Jul 2008 16:39:57 -0700 (PDT)

Obrázok 19 Spätná adresa zmenaná na Alison

- Predmet = background check
- Odpoveď na = alison@m57.biz, aby Alison Smith dostala odpoveď

2. Sobota 19.7.2008 16:44:00 (PDT)

Jean odpovedá na správu o 16:39:57 slovom „Jasné.“



Obrázok 20 Odpoveď Jean

3. Sobota 19.7.2008 16:50:20 (PDT)

Alison dostane neočakávanú odpoveď od Jean, na ktorú odošle odpoveď: „Čo je isté?“

Simple View Advanced Properties View			
Property Name	Property Tag	Property Type	Data
<FILTER>	<FILTER>	<FILTER>	<FILTER>
PR_SENDER_EMAIL_ADDRESS	0x0C1F001E	Extended ASCII string	alison@m57.biz
PR_DISPLAY_TO	0x0E04001E	Extended ASCII string	Jean User
PR_MESSAGE_FLAGS	0x0E070003	Integer 32-bit signed	1
PR_MESSAGE_SIZE	0x0E080003	Integer 32-bit signed	2336
PR_BODY	0x1000001E	Extended ASCII string	What's a "sure thing." ? -----Original Message----- From: Jean User [mailto:jean@m57.biz]
PR_INTERNET_MESSAGE_ID	0x1035001E	Extended ASCII string	<KAEIACFIHBPJMPKNIPKEAGCAA.alison@m57.biz>
PR_IN_REPLY_TO_ID	0x1042001E	Extended ASCII string	<NNEEKAKACNPOIIMAAIIEECACAA.jean@m57.biz>
PR_INTERNET_RETURN_PATH	0x1046001E	Extended ASCII string	alison@m57.biz
PR_CREATION_TIME	0x30070040	Windows Filetime (64-bit)	20/07/2008 02:01:07
PR_LAST_MODIFICATION_TIME	0x30080040	Windows Filetime (64-bit)	20/07/2008 02:01:07
PR_SEARCH_KEY	0x300B0102	Binary data	1A 71 C4 D9 85 D3 5C 48 BA 5C 03 D2 A2 6D CE 6D

Hex Preview Txt Preview Unicode Txt Preview

What's a "sure thing." ?

-----Original Message-----
From: Jean User [mailto:jean@m57.biz]
Sent: Sunday, July 20, 2008 12:46 AM
To: alison@m57.biz
Subject: RE: background checks

Sure thing.

Obrázok 21 E-mail od Alison

Hex Preview	Txt Preview	Unicode Txt Preview
Return-Path: <alison@m57.biz> X-Original-To: jean@m57.biz Delivered-To: x2789967@spunkymail-a2.g.dreamhost.com Received: from jean13bf038a3 (unknown [70.134.85.172]) by spunkymail-a2.g.dreamhost.com (Postfix) with ESMTP id 262C3881D0 for <jean@m57.biz> ; Sat, 19 Jul 2008 16:50:20 -0700 (PDT) From: "alex" <alison@m57.biz> To: "Jean User" <jean@m57.biz> Subject: RE: background checks Date: Sun, 20 Jul 2008 00:50:20 +0100 Message-ID: <KAEIACFIHBPJMPKNIPKEAGCAA.alison@m57.biz> MIME-Version: 1.0 Content-Type: text/plain; charset="iso-8859-1" Content-Transfer-Encoding: 7bit X-Priority: 3 (Normal)		

Obrázok 22 Spätná adresa

4. Sobota, 19.7.2008 18:22:45 (PDT)

Jean dostane ďalší e-mail so spätočnou cestou simsong@xy.dreamhostps.com (Obrázok 14 a Obrázok 15)

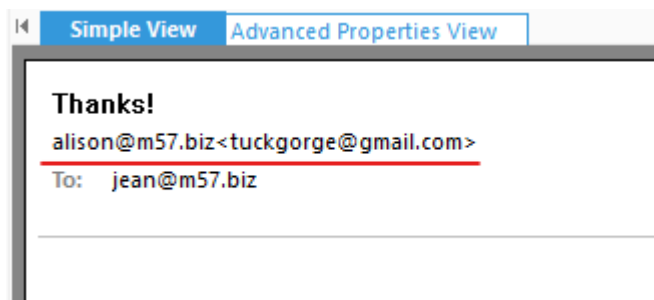
- Predmet = Prosím, pošli mi informácie teraz
- Odpovedať na = tuckgorge@gmail.com

5. Sobota, 19.7.2008 18:28:45 (PDT)

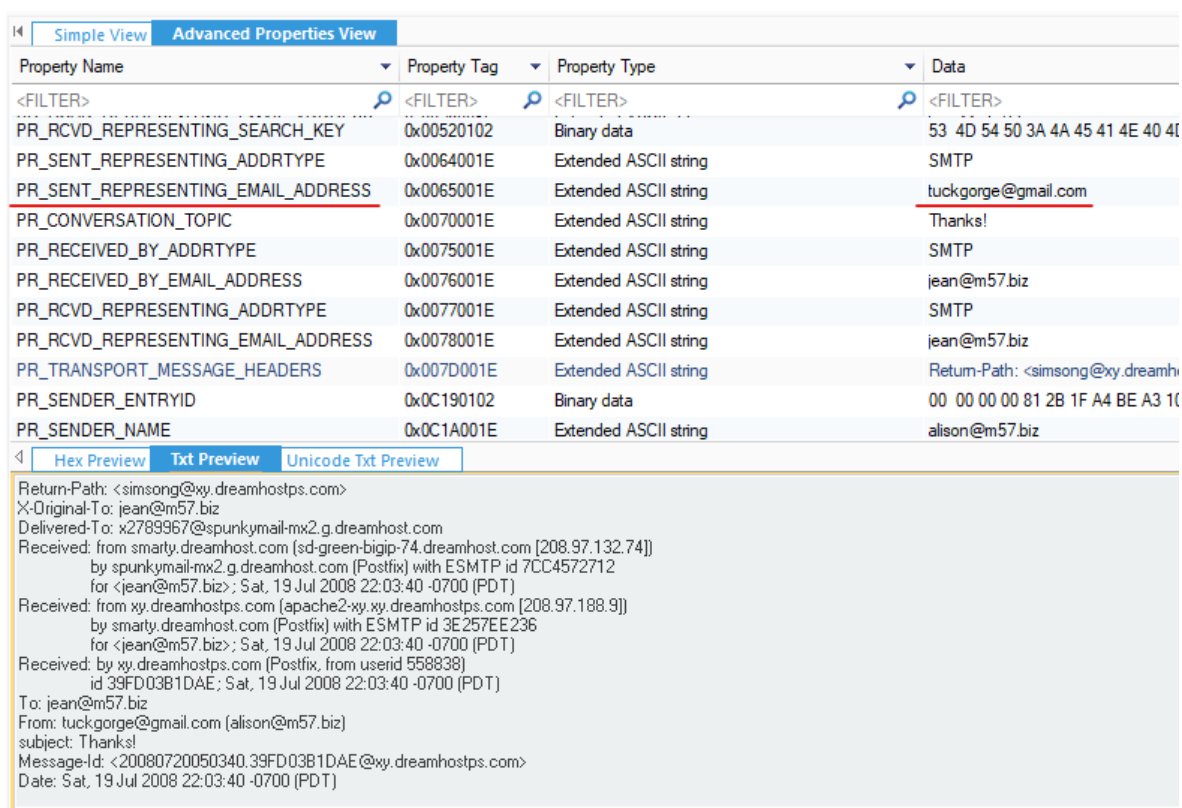
Jean odpovedá na správu o 18:22:45 prílohou s názvom M57biz.xls, pričom táto odpoveď (a tabuľka s firemnými údajmi) sa odošle na tuckgorge@gmail.com (Obrázok 16 a Obrázok 17)

6. Sobota, 19.7.2008 22:03:40 (PDT)

Jean dostane poslednú správu so spiatou cestou simsong@xy.dreamhostps.com



Obrázok 23 Posledný e-mail od útočníka



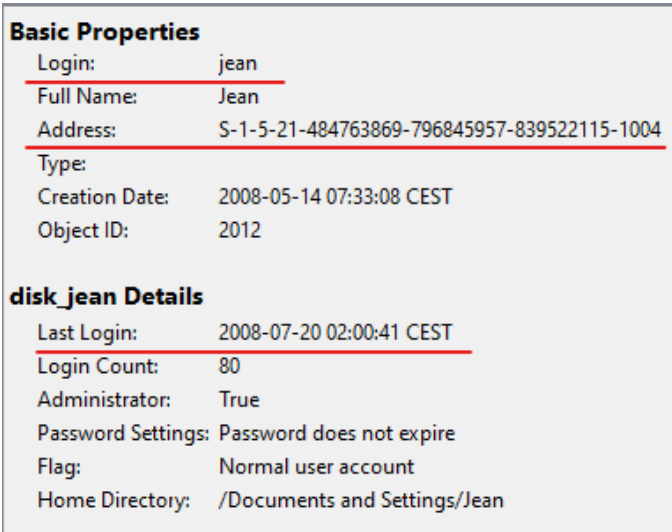
Property Name	Property Tag	Property Type	Data
<FILTER>	<FILTER>	<FILTER>	<FILTER>
PR_RCVD_REPRESENTING_SEARCH_KEY	0x00520102	Binary data	53 4D 54 50 3A 4A 45 41 4E 40 41
PR_SENT_REPRESENTING_ADDRTYPE	0x0064001E	Extended ASCII string	SMTP
PR_SENT_REPRESENTING_EMAIL_ADDRESS	0x0065001E	Extended ASCII string	tuckgorge@gmail.com
PR_CONVERSATION_TOPIC	0x0070001E	Extended ASCII string	Thanks!
PR_RECEIVED_BY_ADDRTYPE	0x0075001E	Extended ASCII string	SMTP
PR_RECEIVED_BY_EMAIL_ADDRESS	0x0076001E	Extended ASCII string	jean@m57.biz
PR_RCVD_REPRESENTING_ADDRTYPE	0x0077001E	Extended ASCII string	SMTP
PR_RCVD_REPRESENTING_EMAIL_ADDRESS	0x0078001E	Extended ASCII string	jean@m57.biz
PR_TRANSPORT_MESSAGE_HEADERS	0x007D001E	Extended ASCII string	Return-Path: <simsong@xy.dreamh
PR_SENDER_ENTRYID	0x0C190102	Binary data	00 00 00 00 81 2B 1F A4 BE A3 10
PR_SENDER_NAME	0x0C1A001E	Extended ASCII string	alison@m57.biz

Return-Path: <simsong@xy.dreamhostps.com>
X-Original-To: jean@m57.biz
Delivered-To: x2789967@spunkymail-mx2.g.dreamhost.com
Received: from smarty.dreamhost.com [sd-green-bigip-74.dreamhost.com [208.97.132.74]]
by spunkymail-mx2.g.dreamhost.com (Postfix) with ESMTP id 7CC4572712
for <jean@m57.biz>; Sat, 19 Jul 2008 22:03:40 -0700 (PDT)
Received: from xy.dreamhostps.com [apache2-xy.xy.dreamhostps.com [208.97.188.9]]
by smarty.dreamhost.com (Postfix) with ESMTP id 3E257EE236
for <jean@m57.biz>; Sat, 19 Jul 2008 22:03:40 -0700 (PDT)
Received: by xy.dreamhostps.com (Postfix, from userid 558838)
id 39FD03B1DAE; Sat, 19 Jul 2008 22:03:40 -0700 (PDT)
To: jean@m57.biz
From: tuckgorge@gmail.com (alison@m57.biz)
subject: Thanks!
Message-Id: <20080720050340.39FD03B1DAE@xy.dreamhostps.com>
Date: Sat, 19 Jul 2008 22:03:40 -0700 (PDT)

Obrázok 24 E-mail od útočníka

- Predmet = Ďakujem!
- Odpoveď na = tuckgorge@gmail.com

5.4. Vyhodnotenie hypotéz

Hypotéza	Stav	Zdôvodnenie
Jean vytvorila súbor na pokyn Alison a poslala ho e-mailom.	Zamietnutá	Súbor bol vytvorený Alison (Obrázok 8), ale Jean ho neposlala Alison – odpovedala na spoofnutý e-mail (Obrázok 16).
Jean súbor vytvorila a omylom ho zdieľala na fóre.	Zamietnutá	Neboli nájdené dôkazy o jej aktivite na fóre (<i>Adresa fóra nie je pre tento prípad známa</i>)
Jean súbor vytvorila, ale niekto iný ho zverejnil.	Zamietnutá	Súbor bol e-mailom odoslaný Jean osobne (Obrázok 16).
Interný zamestnanec zverejnil súbor.	Zamietnutá	Žiadne dôkazy o vnútornej manipulácii zo strany iných zamestnancov – Jean bola prihlásená v čase incidentu.  Obrázok 25 OS účet
Externý útočník získal súbor cez útok.	Potvrdená	Spoofing cez e-mail a sociálne inžinierstvo – Jean bola oklamaná (Obrázok 12 a Obrázok 16).
Súbor nikdy nebol odoslaný Alison, jej tvrdenie je pravdivé.	Potvrdená	Žiadna ďalšia kópia e-mailu s prílohou v PST neexistuje na disku Jean Jones (Obrázok 26) <i>Pozn.: Disk Alison nebol súčasťou tohto scenára.</i>

E-Mail From	Subject	Date Received	Has Attachments
Microsoft Outlook 2000	Welcome to Microsoft Outlook 2000!	2008-07-10 09:47:23 CEST	Yes
Microsoft Outlook 2000	Welcome to Microsoft Outlook 2000!	2008-07-06 09:38:43 CEST	Yes
Jean User <jean@m57.biz>	RE: Please send me the information now	2008-07-20 03:28:00 CEST	Yes
Microsoft Outlook 2000	Welcome to Microsoft Outlook 2000!	2008-07-10 09:47:23 CEST	Yes
Microsoft Outlook 2000	Welcome to Microsoft Outlook 2000!	2008-07-10 09:47:23 CEST	Yes
Google Alerts <googlealerts-noreply@google.com>	Google Alert - skin in the office	2008-07-18 05:19:43 CEST	
Google Alerts <googlealerts-noreply@google.com>	Google Alert - m57.biz	2008-07-16 20:55:25 CEST	
alex <alex@m57.biz>	FW: UFOs Over U.S. Military Sites?	2008-07-20 01:32:54 CEST	

Obrázok 26 E-mail s prílohou

Alison klame o tom, že si súbor neželala a nedostala ho.	Zamietnutá	Neexistujú dôkazy o tom, že by Alison dokument požadovala alebo prijala (Obrázok 16).
--	------------	---

Tabuľka 4 Vyhodnotenie hypotéz

Záver

Digitálna forenzná analýza odhalila, že k úniku dôverných údajov došlo v dôsledku sociálneho inžinierstva – Jean Jones bola oklamaná spoofnutým e-mailom, ktorý sa tváril ako interná žiadosť od prezidentky spoločnosti, Alison Smith.

Na základe poskytnutých dôkazov som dospela k záveru, že nešlo o interný sabotážny čin ani o vedomé zverejnenie, ale o neúmyselné zlyhanie jednotlivca, ktoré umožnilo externému útočníkovi získať citlivé firemné dáta.

Zdroje

1. DigitalCorpora. M57 Jean Scenario [online]. [cit. 2025-04-14]. Dostupné na: <https://digitalcorpora.org/corpora/scenarios/m57-jean/>
2. DigitalCorpora. Disk Image – nps-2008-jean.E01 [online]. [cit. 2025-04-14]. Dostupné na: <https://digitalcorpora.s3.amazonaws.com/corpora/drives/nps-2008-m57-jean/nps-2008-jean.E01>
3. DigitalCorpora. Disk Image – nps-2008-jean.E02 [online]. [cit. 2025-04-14]. Dostupné na: <https://digitalcorpora.s3.amazonaws.com/corpora/drives/nps-2008-m57-jean/nps-2008-jean.E02>