UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH
PRÍRODOVEDECKÁ FAKULTA

VPLYV ANTI-FORENZNÝCH TECHNÍK NA DIGITÁLNE FORENZNÉ VYŠETROVANIE

2023 **Zuzana HENNELOVÁ**

Obsah

Úvod **3**

1 Prístupy k určovaniu vplyvu **4**

1.1 Úrovne vplyvu 4

1.2 Matica vplyvu 4

1.3 Hodnotiace techniky 5

2 Mazanie súborov **7**

2.1 Vplyv mazania súborov na artefakty 7

2.2 Vplyv mazania súborov na detekciu anomálií 8

3 Alternatívne dátové toky **11**

3.1 Vplyv ukrývania v ADS na artefakty 11

4 Šifrovanie **12**

4.1 Vplyv šifrovania na artefakty 12

5 Timestomping **14**

5.1 Vplyv timestompingu na artefakty 15

5.2 Vplyv timestompingu na detekciu anomálií 16

6 Vyhodnotenie **18**

7 Záver **20**

8 Zoznam použitej literatúry **21**

Úvod

S výraznými technologickými pokrokmi vzniká v kybernetickom priestore aj množstvo príležitostí pre útočníkov. Aby bolo možné eliminovať následky vzniknutého bezpečnostného incidentu a zabrániť vzniku ďalších, je potrebné zisťovať kto a akým spôsobom vykonal útok, aké zraniteľnosti zneužil, aké použil príkazy, s akými zariadeniami komunikoval a k akým dátam pristupoval. Na tieto otázky sa snaží odpovedať digitálna forenzná analýza, v rámci ktorej dochádza k zaisteniu digitálnych stôp, ich spracovaniu, analýze a vyhodnoteniu. Na druhej strane sú však útočníci, ktorí sa častokrát pokúšajú zahladiť za sebou stopy, ktoré zanechali v kompromitovaných systémoch. Za týmto účelom používajú rôzne anti-forenzné techniky na oklamanie rôznych automatizovaných nástrojov a na spomalenie a zavádzanie forenzných vyšetrovateľov pri analýze digitálnych stôp.

Anti-forenzné techniky môžu do istej miery ovplyvniť proces a výsledky forenznej analýzy, a preto je dôležité sa nimi zaoberať. Nie každá technika je rovnako efektívna a práve touto efektivitou, resp. vplyvom sa zaoberáme v tejto práci.

V súčasnosti existuje množstvo anti-forenzných techník, a kým niektoré z nich je možné rýchlo odhaliť, iné sú ťažko detekovateľné. Časovo je teda nevýhodné riešiť pri každej forenznej analýze to, či nebola niektorá z techník použitá, ale malo by sa určiť, ktoré techniky sú natoľko závažné, že je potrebné sa nimi zaoberať a naopak, ktoré techniky nie je potrebné riešiť. K tomu by malo dopomôcť práve preskúmanie vplyvu rôznych anti-forenzných techník na forenzné vyšetrovanie.

V oblasti automatizácie forenznej analýzy je ešte väčšmi dôležité prihliadať na anti-forenzné techniky, keďže ich použitie môže úplne zmeniť výsledky behu rôznych analytických programov. V práci otestujeme anti-forenzné techniky pri vyhľadávaní anomálií nad dátami vyextrahovanými z disku a popíšeme rozdiely vzniknuté použitím konkrétnej techniky.

Keďže sme nenašli literatúru ohodnocujúcu vplyv anti-forenzných techník, v rámci práce popíšeme okrem vplyvu vybraných 4 anti-forenzných techník aj nami navrhnuté spôsoby jednotného ohodnotenia, ktoré bude možné aplikovať na všetky existujúce, ale aj ešte nevymyslené anti-forenzné techniky.

1 Prístupy k určovaniu vplyvu

Na stanovenie miery vplyvu anti-forenznej techniky na artefakt sme definovali 2 nižšie popísané spôsoby. Kým prvý neberie do úvahy žiadne okolnosti, druhý zohľadňuje aj náročnosť detekcie použitej techniky. Na vyhodnotenie vplyvu pri detekcii anomálií použijeme 3 hodnotiace techniky.

1.1 Úrovne vplyvu

Vplyv anti-forenznej techniky na kvalitu artefaktu bez prihliadnutia na iné okolnosti (náročnosť detekcie, dôležitosť artefaktu) je možné charakterizovať nasledujúcimi 4 úrovňami vplyvu:

- **Žiadny vplyv:** anti-forenzná technika artefakt neovplyvňuje.
- **Malý vplyv:** technika mení umiestnenie artefaktu a/alebo vytvára falošné artefakty
- **Stredný vplyv:** technika čiastočne mení obsah a/alebo modifikuje metadáta artefaktu.
- **Vysoký vplyv:** technika zatají existenciu daného artefaktu, odstráni artefakt (a stopy po jeho existencii) a/alebo ho nenávratne prepíše.

1.2 Matica vplyvu

Ako jednu z možností pre porovnávanie vplyvu rôznych techník na artefakty sme navrhli maticu vplyvu anti-forenznej techniky na artefakt (Tabuľka 1). Matica berie do úvahy náročnosť detekcie použitia danej anti-forenznej techniky a stav artefaktu. Na výstupe sú 3 úrovne vplyvu na artefakt:

- **Malý vplyv** značí to, že daná anti-forenzná technika sa zameriava na artefakty, ktoré je možné nahradiť inými alebo sú artefakty čiastočne zotaviteľné a samotná detekcia použitia techniky je triviálna, pretože v systéme zanecháva očividné stopy. Malý vplyv má aj kombinácia náročne detekovateľnej techniky spolu s nahraditeľným artefaktom, keďže po zistení použitia danej techniky stačí nahradiť ovplyvnený artefakt iným.

- **Stredný vplyv** zodpovedá buď takmer nemožnej detekcii ale nahraditeľnému artefaktu, alebo čiastočne zotaviteľnému artefaktu a náročnej detekcii, resp. nezotaviteľnému artefaktu ale triviálnej detekcii.
- **Vysoký vplyv** budú mať techniky, ktoré úplne znehodnotia artefakt a ich detekcia je náročná alebo takmer nemožná. Veľký vplyv má aj takmer nedetekovateľná technika, ktorá ovplyvňuje čiastočne nahraditeľný artefakt. Takéto techniky budú mať veľký význam pri automatizácii procesov forenznej analýzy, ako aj pri manuálnej analýze.

Vplyv anti-forenznej techniky na artefakt		stav artefaktu		
		je nahraditeľný	dá sa čiastočne zotaviť	nedá sa zotaviť ani nahradiť
detekcia	takmer nemožná			**vysoký vplyv**
	náročná		**stredný vplyv**	
	triviálna	**malý vplyv**		

Tabuľka 1: Matica vplyvu

V tabuľke nie je uvedená možnosť, kde artefakt je síce technikou ovplyvnený, ale nie je relevantný pre forenznú analýzu, pretože takéto artefakty nebudeme ohodnocovať. Rovnako neuvádzame možnosť nemožnej detekcie, pretože aj techniky, ktoré sú na teoretickej úrovni nedetekovateľné, môžu mať nedokonalú praktickú aplikáciu (ľudský faktor), ktorá predsa len zanechá v systéme stopy.

1.3 Hodnotiace techniky

- *Presnosť (precision):* slúži na ohodnotenie miery správne identifikovaných anomálií (True Positive, ozn. TP) k všetkým identifikovaným anomáliám, teda tým správne identifikovaným, ale aj nesprávne identifikovaným (False Positive, ozn. FP).

$$Presnosť = \frac{TP}{TP + FP}$$

- *Senzitivita (recall):* meria počet správne identifikovaných anomálií (TP) vzhľadom na všetky anomálie, ktoré by reálne mali byť označené. Je to teda podiel TP a súčtu TP a nesprávne neidentifikovaných anomálií (False Negative, ozn. FN).

$$Senzitivita = \frac{TP}{TP + FN}$$

- *F1-skóre (F1-Score):* kombinuje presnosť a senzitivitu, najlepšia výsledná hodnota je 1, počíta sa nasledovným vzorcom:

$$F1 - skóre = 2 * \frac{presnosť * senzitivita}{presnosť + senzitivita}$$

Maximálna možná hodnota pre všetky tieto ohodnotenia je 1 (Kanstrén, 2020). Najväčšiu váhu budeme pri určovaní vplyvu prikladať práve F1-skóre, keďže je kombináciou predchádzajúcich dvoch hodnôt.

Tieto ohodnotenia použijeme nad predpripravenými dátami a budeme vychádzať z článku Detection of relevant digital evidence in the forensic timelines (2022), ktorý skúma viaceré metódy hľadania anomálií nad prípadom ukradnutej sečuánskej omáčky[1]. My použijeme iba jednu zo skúmaných metód na detekciu anomálií, a to Empirical-Cumulative-distribution-based Outlier Detection (ECOD). ECOD budeme spúšťať s použitím rôznych nastavení nad originálnymi predspracovanými dátami, ako aj nad dátami upravenými podľa príslušnej anti-forenznej techniky.

Na vyhodnotenie použijeme jednak súčet nájdených anomálií za všetky behy programu a ich ohodnotenie precíznosti, ako aj priemerné hodnoty pre 5 nastavení, ktoré dávajú pre originálne dáta najlepšie výsledky.

[1] https://dfirmadness.com/the-stolen-szechuan-sauce/

2 Mazanie súborov

Táto technika patrí k najprirodzenejším spôsobom, ako odstrániť zo systému stopy po útoku. V prípade bežného odstránenia súboru, je daný súbor premiestnený do koša, odkiaľ je možné súbor obnoviť. V súborovom systéme sa takéto odstránenie prejavuje tak, že miesta v pamäti, kde bol súbor uložený sa označia ako nealokované. Samotné dáta súboru však ostávajú v pamäti, kým nie sú prepísané. Takéto dáta je potom možné vyextrahovať z pamäte, a to aj v prípade, keď súbory odstránime aj z koša.

Za účelom bezpečného odstránenia súborov boli vyvinuté viaceré nástroje. Ich prítomnosť v zariadení však nemusí znamenať aktivitu útočníka. Tieto nástroje totiž môžu byť používané v bežnom živote napr. pri práci s citlivými, dôvernými údajmi, ktoré je potrebné zlikvidovať podľa stanovených štandardov.

2.1 Vplyv mazania súborov na artefakty

Na testovanie sme použili 2 nástroje určené na mazanie: BitKiller verzie 2.0 [2] a Eraser verzie 6.2.0 [3]. Autorom nástroja BitKiller je Hasan N. Genc a z priloženej dokumentácie vyplýva, že BitKiller najprv prepíše zvolený súbor podľa vybranej metódy, a potom zmenší veľkosť súboru na 0. Ďalej je súbor 10-krát náhodne premenovaný a vymaže sa. Postup použitý nástrojom Eraser nie je popísaný.

Oboma nástrojmi sme zopakovali rovnaký postup odstraňovania (PDF súborov) a v prípade BitKillera sme vyskúšali všetkých 5 ponúkaných metód. Potom sme vytvorili obraz disku pomocou Access Data FTK Imager verzie 7.4.1 [4] a nahrali ho do nástroja Autopsy verzie 4.19.3 [5]. Tam sa nám podarilo v oboch prípadoch nájsť odkazy odstránených súborov s ich pôvodným názvom a umiestnením, ako aj záznam o spustení nástroja na mazanie v prefetch súboroch. Detekcia mazania súboru je pomocou týchto artefaktov jednoduchá. Okrem nich sú zachytené záznamy o zmene aj v denníku (journal), konkrétne sa odtiaľ dá vyčítať pôvodný názov súboru a čas jeho manipulácie, a navyše je vidieť na aké náhodné reťazce sa mení názov súboru. Ukážka z denníka je na obrázku č. 1.

[2] https://sourceforge.net/projects/bitkiller/
[3] https://eraser.heidi.ie/download/
[4] https://www.exterro.com/ftk-imager
[5] https://www.autopsy.com/download/

V logoch neboli nájdené žiadne relevantné záznamy, a taktiež sa v žiadnom prípade nepodarilo extrahovať z pamäte odstránené súbory pomocou nástroja Bulk Extractor [6] ani scalpel 2.0 [7].

Name	UpdateTimestamp	UpdateReasons
ziadost_vzor.pdf	23.1.2023 13:40	DataExtend
ziadost_vzor.pdf	23.1.2023 13:40	DataOverwrite|DataExtend
ziadost_vzor.pdf	23.1.2023 13:40	DataOverwrite|DataExtend|DataTruncation
ziadost_vzor.pdf	23.1.2023 13:40	DataOverwrite|DataExtend|DataTruncation|Close
ziadost_vzor.pdf	23.1.2023 13:40	IndexableChange|BasicInfoChange
ziadost_vzor.pdf	23.1.2023 13:40	IndexableChange|BasicInfoChange|Close
ziadost_vzor.pdf	23.1.2023 13:40	BasicInfoChange
ziadost_vzor.pdf	23.1.2023 13:40	BasicInfoChange|Close
ziadost_vzor.pdf	23.1.2023 13:40	RenameOldName
k(gcEQXgEwghZz=d	23.1.2023 13:40	RenameNewName
k(gcEQXgEwghZz=d	23.1.2023 13:40	RenameNewName|Close
k(gcEQXgEwghZz=d	23.1.2023 13:40	BasicInfoChange
k(gcEQXgEwghZz=d	23.1.2023 13:40	BasicInfoChange|Close
k(gcEQXgEwghZz=d	23.1.2023 13:40	RenameOldName
2NLk5=2}kV]t6u]t	23.1.2023 13:40	RenameNewName
2NLk5=2}kV]t6u]t	23.1.2023 13:40	RenameNewName|Close
2NLk5=2}kV]t6u]t	23.1.2023 13:40	BasicInfoChange
2NLk5=2}kV]t6u]t	23.1.2023 13:40	BasicInfoChange|Close
2NLk5=2}kV]t6u]t	23.1.2023 13:40	RenameOldName

Obrázok 1: Výber z denníka (mazanie)

Mazanie súboru má teda vplyv iba na samotné dáta súboru, ktoré sa nepodarilo vôbec zotaviť a na ostatné artefakty technika nemá **žiadny vplyv**. Úroveň vplyvu na dáta súboru je síce **vysoká**, ale po prihliadnutí na jednoduchosť detekcie techniky je vplyv na dáta podľa matice vplyvu **stredný**.

2.2 Vplyv mazania súborov na detekciu anomálií

V predspracovaných dátach sme simulovali mazania súboru štyrmi rôznymi spôsobmi. Prvé 2 spôsoby simulujú obyčajné odstránenie súboru, a to nastavením veľkosti súboru (a jeho prislúchajúceho LNK súboru) na 0 a jeho označením ako nealokovaný. To sa v porovnaní so simuláciou použitia aplikácie na mazanie ukázalo ako menej efektívne a ďalej to nebudeme brať do úvahy.

[6] https://downloads.digitalcorpora.org/downloads/bulk_extractor/
[7] https://github.com/machn1k/Scalpel-2.0

Simulácia kompletného vymazania sa v dátach prejavila ako odstránenie relevantných záznamov z dát. Záznamy súvisiace s MFT a denníkom sme neodstraňovali, keďže ani aplikácie do týchto záznamov nezasahujú.

V tabuľke 2 uvádzame rozdiel počtu určených anomálií oproti pôvodným výsledkom. Všetky počty sú výsledkom sčítania všetkých anomálií nájdených počas celého behu určovania anomálií na základe rôznych kritérií.

Rozdiely voči originálu	**Správne určené**		**Nesprávne určené**	
	názov	inode	názov	inode
Odstránenie súboru	-116	**-35**	+460	+53
Odstránenie súboru aj LNK	**-190**	-45	**+528**	**-6**

Tabuľka 2: Rozdiel identifikovaných anomálií (mazanie súborov)

Pri odstránení textového súboru a jeho odkazu bol počet správne identifikovaných anomálií na základe názvu súborov vo všetkých behoch o 190 menší oproti originálu, čo je najväčší rozdiel pre správne určené anomálie. Pre forenzného analytika to znamená **menšiu presnosť výsledkov**. Počet nesprávne identifikovaných anomálií sa naopak zvýšil o 528, čo je opäť najväčšie z navýšení a prináša **veľa nesprávne určených anomálií**, ktoré by musel forenzný analytik preskúmať. Pri odstránení aj LNK súboru neboli rozdiely až tak výrazné.

Pri identifikácii anomálií na základe inodov a odstránení iba súboru sa počet správne určených anomálií znížil najmenej. Pri odstránení súboru aj jeho odkazu sa počet nesprávne určených anomálií dokonca znížil, teda forenzný analytik by musel preskúmať o 6 nepodstatných záznamov menej.

V tabuľke 3 uvádzame porovnanie hodnôt z kapitoly 1.3. Ukázalo sa, že odstránenie súboru (aj jeho odkazu) môže vylepšiť hodnoty sledovaných parametrov, hoci sme predpokladali presný opak. Príčinou môže byť menší počet záznamov, ktoré musí algoritmus vyhodnotiť.

	Presnosť		Senzitivita		F1 skóre	
	názov	inode	názov	inode	názov	inode
Originál	0.1859	0.2830	0.0761	**0.0220**	0.1080	**0.0409**
Odstránenie súboru	0.1787	0.2733	0.0789	0.0229	0.1094	0.0422
Odstránenie súboru aj LNK	**0.1758**	**0.2911**	**0.0827**	0.0229	**0.1125**	0.0424

Tabuľka 3: Porovnanie kvality detekcie anomálií (mazanie súborov)

Ak porovnáme odstránenie súboru a odstránenie súboru aj jeho odkazu, prvá možnosť dosahuje nižšiu celkovú presnosť, pravdepodobne preto, že neodstránené LNK súbory bez samotného súboru, na ktorý odkazujú, môžu pôsobiť výstrednejšie.

Na porovnanie sme zisťovali aj priemer najlepších 5 nastavení pre výsledky v originálnych dátach. Priemerné hodnoty sú v tabuľke 4. Je vidieť, že pre hľadanie anomálií podľa názvu je najhoršia celková precíznosť pre zmazanie súboru aj jeho odkazu. Pri hľadaní podľa inodu sú výsledky menej jednoznačné. Hodnoty originálu a hodnoty odstráneného súboru s odkazom sú zhodné a majú najhoršiu senzitivitu aj F1 skóre.

		TP	FP	Presnosť	Senzitivita	F1 skóre
názov	**Originál**	14,0	57,2	0,1967	0,8235	0,3175
	Zmazaný súbor	14,0	57,2	0,1967	0,8235	0,3175
	Zmazaný súbor a odkaz	13,0	57,6	**0,1842**	**0,7647**	**0,2969**
inode	**Originál**	12,0	10,2	0,5513	0,8000	0,6483
	Zmazaný súbor	11,6	10,2	0,5434	0,8286	0,6521
	Zmazaný súbor a odkaz	12,0	10,2	0,5513	0,8000	0,6483

Tabuľka 4: Priemer piatich najlepších nastavení (mazanie súborov)

3 Alternatívne dátové toky

V súborovom systéme NTFS môžu súbory obsahovať viaceré dátové toky. Základný dátový tok obsahuje samotné dáta súboru, alternatívne dátové toky (ADS) obsahujú dodatočné informácie o súboroch (napr. autor dokumentu, počet strán).

Každý súbor môže mať viacero ADS. Dôležitá je z hľadiska forenznej analýzy informácia, že pridanie ADS vôbec nemení veľkosť súboru, teda aj v zdanlivo obyčajnom súbore môže byť ukrytý celý zdrojový kód malvéru, škodlivý spustiteľný súbor a i. Avšak stačí v príkazovom riadku pri vypisovaní obsahu priečinka použiť príkaz *dir /r* a zobrazia sa aj všetky ADS.

3.1 Vplyv ukrývania v ADS na artefakty

Vytvorili sme textový súbor, ktorému sme pridali ADS. Pridanie spôsobilo aktualizáciu časových pečiatok zobrazovaného súboru a záznamy o zmenách je možné vidieť aj v denníku (journal), kde sa ako dôvod aktualizácie metadát uvádza „StreamChange“, teda zmena dátového toku. V prípade otvorenia dátového toku dokonca vzniká nový odkaz. Záznamy o vzniku odkazu ako aj pridanie ADS sú vyextrahované z denníka na obrázku 2. Zároveň je možné všetky ADS jednoducho vypísať v príkazovom riadku

Name	UpdateTimestamp	UpdateReasons
obycajnySubor.txt	4.4.2023 14:50	StreamChange
obycajnySubor.txt	4.4.2023 14:50	NamedDataExtend|StreamChange
obycajnySubor.txt	4.4.2023 14:50	NamedDataExtend|StreamChange|Close
obycajnySubor.txt.lnk	4.4.2023 14:51	DataExtend|FileCreate|Close
obycajnySubor.txt.lnk	4.4.2023 14:51	DataExtend|FileCreate
obycajnySubor.txt.lnk	4.4.2023 14:51	FileCreate

Obrázok 2: Pridanie ADS zaznamenané v denníku

ADS má podľa kapitoly 1.1 **vysoký vplyv** na samotné dáta, keďže ich ukrýva, ale zároveň je detekcia ADS pomerne triviálna a dáta neodstraňuje ani nemodifikuje, teda podľa matice vplyvu majú alternatívne dátové toky iba **malý vplyv** na dáta.

4 Šifrovanie

Šifrovanie je veľmi účinná metóda zaisťujúca dôvernosť dát. Používa sa v každodennom živote, a za účelom ukrytia dát ju používajú aj útočníci. Šifrované môžu byť jednotlivé súbory, priečinky, partície aj celý disk. V prípade zašifrovania celého disku môže byť úplne znemožnená forenzná analýza.

Súčasným štandardom na šifrovanie dát je symetrický algoritmus AES s použitím aspoň 128-bitového šifrovacieho kľúča (Barker, 2020). Tento štandard ponúkajú mnohé neplatené aj platené nástroje. Prítomnosť šifrovaných súborov detegujú niektoré nástroje používané vo forenznej analýze na základe entropie. Zašifrovanie ovplyvní časové pečiatky šifrovaných súborov, resp. vytvorí nový šifrovaný súbor (v závislosti od použitej aplikácie), kde veľkosť súboru môže byť voči originálu pozmenená.

4.1 Vplyv šifrovania na artefakty

Použili sme nástroj AES Crypt [8] na zašifrovanie samostatného súboru. Nástroj je možné použiť cez príkazový riadok a zároveň sa zobrazuje ako možnosť pri kliknutí pravým tlačidlom na súbor. Po spustení nad konkrétnym súborom sa po zadaní hesla vytvorí nový rovnomenný súbor s príponou *.aes* a pôvodný súbor ostane nezmenený. Prvým problémom šifrovania súborov je teda samotná existencia pôvodného súboru. Ten musí byť dôkladne odstránený, inak by šifrovanie nemalo význam.

Samotný zašifrovaný súbor nie je možné priamo otvoriť bez zadania správneho hesla. Pri zobrazení textu je možné vidieť v hlavičke názov šifrovacieho algoritmu aj názov použitého programu a zvyšok dát je nečitateľný (viď obrázok 3). V systéme je navyše logovaná inštalácia samotného programu.

Obrázok 3: Obsah zašifrovaného súboru

[8] https://www.aescrypt.com/download/

Detekcia šifrovania súborov je triviálna, a samotné dáta je možné obnoviť iba v prípade zle odstráneného pôvodného súboru. Ak teda uvažujeme, že útočník dokáže odstrániť dáta nezašifrovaného súboru, šifrovanie má **vysokú** úroveň vplyvu na dáta a žiadny vplyv na ostatné artefakty podľa 1.1 a **stredný vplyv** na dáta podľa matice vplyvu (1.2).

Čo sa týka šifrovania celej partície alebo disku, je opäť veľmi jednoduché techniku detegovať, keďže dáta budú nečitateľné. Ovplyvnené však nebudú iba dáta konkrétnych súborov, ale všetko uložené na danej partícii, vrátane MFT, denníka, logov (ak sa jedná o partíciu, kde je uložený operačný systém), obsahu koša, prefetchov, odkazov atď.

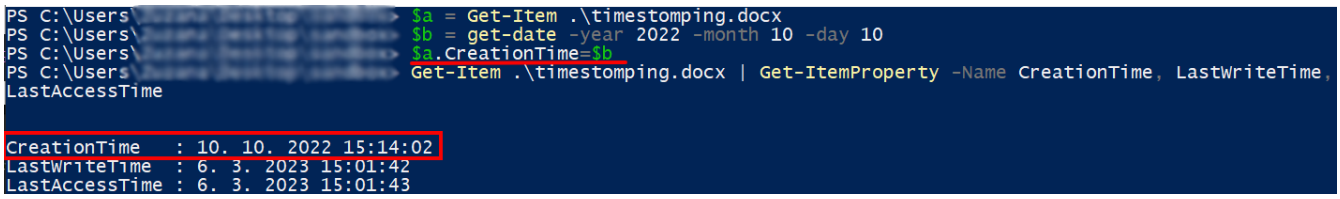
Podľa úrovní vplyvu má šifrovanie **vysoký vplyv** na všetky artefakty nachádzajúce sa na šifrovanej partícii/disku. Podľa matice vplyvu je to iba **stredný vplyv** vzhľadom na jednoduchosť detekcie. Ohodnotenie pomocou úrovne vplyvu je v tomto prípade výstižnejšie, keďže forenzná analýza zašifrovaného disku býva neúspešná.

5 Timestomping

Timestomping - modifikácia časových pečiatok, dokáže malou zmenou ovplyvniť zaužívané procesy forenznej analýzy. V praxi nie je vždy čas na analýzu všetkých zaistených súborov a dát a preto sa často analýza vykonáva iba v rámci určitého časového úseku. Zmena časových pečiatok tak môže spôsobiť vynechanie dôležitých stôp.

Časové pečiatky (MACB) sa v systéme Windows ukladajú v MFT (Master File Table) tabuľke v dvoch kópiách, kde jedna, SI (System Information), je bežne dostupná a druhá, FI (Filename Information), je prístupná len jadru operačného systému. Okrem toho môžu byť časové pečiatky získané aj z iných artefaktov ako sú nedávne súbory. Niektoré zmeny časových pečiatok môžu byť uložené v denníku.

Modifikácia je možná prostredníctvom príkazového riadku (obrázok 4), v ktorom je možné prepísať zobrazované časové pečiatky, avšak časové pečiatky Filename Information ostanú nezmenené.



Obrázok 4: Timestomping času vzniku súboru

Tým, že sa Filename Information časové pečiatky aktualizujú pri premiestnení súboru, je možné donútiť systém aktualizovať ich napr. premiestnením súboru (Palmbach, Breitinger, 2020).

Taktiež sú dostupné nástroje, ktoré je možné použiť za účelom timestompingu. Najviac spomínané nástroje sú nTimestopm [9], Timestomp [10] a SetMACE [11].

[9] https://github.com/limbenjamin/nTimetools
[10] https://github.com/jackson5sec/timestomp
[11] https://github.com/jschicht/SetMace

5.1 Vplyv timestompingu na artefakty

V PowerShelli je možné zmeniť časové pečiatky jednoduchým nastavením pečiatky súboru $a na dátum $b, napr. $a.CreationTime = $b. Možné je takto nastaviť pečiatku vzniku súboru, poslednej modifikácie a posledného prístupu. Tento prístup je možné skombinovať s premiestňovaním súboru. Vyskúšali sme oba tieto prístupy a v tabuľke 5 a 6 uvádzame vyextrahované časové pečiatky z MFT (Postup 1 je iba zmena pečiatok a postup 2 zahŕňa premiestňovanie).

Postup	Created SI	Created FI	LastModified SI	LastModified FI
1	10.10.2022 13:14	6.3.2023 14:01	11.11.2022 14:15	6.3.2023 14:01
2	15.10.2022 12:49		15.10.2022 12:49	

Tabuľka 5: Časové pečiatky z MFT (časť 1)

Postup	LastRecordChange SI	LastRecordChange FN	LastAccess SI	LastAccess FN
1	6.3.2023 14:16	6.3.2023 14:01	12.12.2022 14:16	6.3.2023 14:01
2	16.3.2023 13:56	16.3.2023 13:55	16.3.2023 13:57	16.3.2023 13:55

Tabuľka 6: Časové pečiatky z MFT (časť 2)

Je vidieť, že prvý postup nie je vôbec efektívny ale druhým spôsobom je možné nepriamo nastaviť aj systémové pečiatky (Filename Information). Pečiatky posledného prístupu nie sú modifikované, pretože sa so súborom ďalej manipulovalo. Za povšimnutie však stoja pečiatky Last Record Change, ktoré hovoria o poslednej aktualizácii metadát. Bez kontextu by to mohlo vyzerať tak, že bol súbor napr. iba presunutý (vtedy sa aktualizuje iba táto pečiatka) a otvorený. Na základe týchto údajov teda nie je možné jednoznačne potvrdiť timestomping.

Ak je manipulácia so súborom stále viditeľná v denníku, rovnako nie je možné odtiaľ jednoznačne určiť o aké zmeny sa jedná, pretože všetky úpravy pečiatok sa tam zaznamenávajú s rovnakým popisom (zmena jednej pečiatky je znázornená v tabuľke 7) a všetko by to mohli byť zmeny posledného pristúpenia k súboru. Ani na základe denníka teda nie je možné jednoznačne potvrdiť timestomping.

Name	UpdateTimestamp	UpdateReasons
timestomping.docx	6.3.2023 14:16	BasicInfoChange
timestomping.docx	6.3.2023 14:16	BasicInfoChange|Close

Tabuľka 7: Záznam z denníka pri zmene časovej pečiatky

Ďalším možným ukazovateľom timestompingu sú odkazy na súbory. Otestovali sme teóriu, že otvorenie súboru pri timestompingu aktualizuje časové pečiatky príslušných linkových súborov, podľa času nastaveného v súbore, čo sa ukázalo ako nepravdivé. Otvorenie súboru nastavilo časové pečiatky odkazu podľa systémového času. Preto sme odkazy modifikovali ručne, avšak nie je možné odkaz po premiestnení z pôvodného priečinka vrátiť späť. Preto je možné na odkazy aplikovať iba prvý spôsob timestompingu, ktorý spôsobuje rozpor medzi SI a FI pečiatkami. Vždy sa však dajú odkazy úplne odstrániť, hoc aj to by mohlo poukazovať na podozrivé dianie v systéme.

Pomocou timestompingu je teda možné dosiahnuť **vysoký vplyv** na MACB umiestnené v MFT. Ostatné artefakty neboli ovplyvnené. Rovnaké ohodnotenie vplyvu na jednotlivé artefakty dostávame aj z matice vplyvu, kde techniku timestompingu kategorizujeme ako takmer nedetekovateľnú.

Vyskúšali sme taktiež nástroj *nTimestomp* a *Timestomp*, tieto nástroje však dokázali modifikovať iba SI pečiatky.

5.2 Vplyv timestompingu na detekciu anomálií

V CSV súbore sme simulovali timestomping zmenou atribútov *date* a *time* pre súbor NoJerry.txt, konkrétne všetky jeho dáta okrem záznamov z denníka, keďže týmto záznamom nie je možné v systéme upraviť časové pečiatky. Dátum a čas sme nastavili na dobu pred útokom, konkrétne na deň 18.01.2023. Na týchto dátach sme hľadali anomálie na základe názvov súborov aj na základe inodov. Tým, že sme zmenili čas na dobu pred útokom, vyhľadávanie anomálií vlastne tieto upravené záznamy vôbec nebralo do úvahy.

Čo sa týka počtu správne a nesprávne určených anomálií, oproti originálu dopadla lepšie metóda vyhľadávania pomocou inodov. Oproti vyhľadávaniu podľa

názvov vznikli výrazné rozdiely, viď. tabuľka 8. V oboch prípadoch sa však vo všetkých behoch vyhľadávania anomálií našlo menej správnych a viac nesprávnych anomálií.

Rozdiely voči originálu	**Správne určené**		**Nesprávne určené**	
	názov	inode	názov	inode
Timestomping	**-662**	**-35**	**+1304**	**+163**

Tabuľka 8: Rozdiel identifikovaných anomálií (timestomping)

Pri pohľade na parametre hodnotiacich techník (tabuľka 9) je vidieť, že použitie timestompingu znížilo pri hľadaní podľa názvu všetky hodnoty. Pri vyhľadávaní podľa inodov je však celková presnosť výrazne menšia.

	Presnosť		**Senzitivita**		**F1 skóre**	
	názov	inode	názov	inode	názov	inode
Originál	0.1859	**0.2830**	**0.0761**	**0.0220**	**0.1080**	**0.0409**
Timestomping	**0.1549**	0.2657	0.0651	0.0229	0.0917	0.0421

Tabuľka 9: Porovnanie ohodnotenia precíznosti (timestomping)

V tabuľke číslo 10 sú porovnania priemerných hodnôt pre 5 najlepších nastavení vzhľadom na originálne dáta. Najhoršie obstála detekcia anomálií na základe názvov pre dáta s použitým timestompingom, ktorá má všetky sledované parametre najhoršie. Aj pri detekcii na základe inodov je však vidieť pri timestompingu pokles presnosti, senzitivity aj F1 skóre, hoci pri originálnych dátach bola táto forma detekcie presnejšia ako detekcia podľa názvu.

		TP	**FP**	**Presnosť**	**Senzitivita**	**F1 skóre**
názov	**Originál**	14.0	57.2	0.1967	0.8235	0.3175
	Timestomping	8.0	58.6	0.1204	0.4706	0.1916
inode	**Originál**	12.0	10.2	0.5513	0.8000	0.6483
	Timestomping	8.6	13.0	0.4141	0.6143	0.4902

Tabuľka 10: Priemer piatich najlepších nastavení (timestomping)

6 Vyhodnotenie

Popísali sme princípy 4 vybraných anti-forenzných techník, ktoré sme aj priamo otestovali. Odsledovali a popísali sme vplyv vykonania týchto techník na relevantné artefakty v operačnom systéme Windows 10. Výsledné vplyvy podľa úrovne vplyvu (1.1) a matice vplyvu (1.2) sú zhrnuté v tabuľke 11.

Spôsob porovnania	Anti-forenzná technika	Dáta	MFT
Úroveň vplyvu	**Mazanie súborov**	Vysoký	-
	ADS	Vysoký	-
	Šifrovanie súboru	Vysoký	-
	Šifrovanie disku	Vysoký	Vysoký
	Timestomping	Žiadny	Vysoký
Matica vplyvu	**Mazanie súborov**	Stredný	-
	ADS	Malý	-
	Šifrovanie súboru	Stredný	-
	Šifrovanie disku	Stredný	Stredný
	Timestomping	-	Vysoký

Tabuľka 11: Vplyv anti-forenzných techník

V tabuľke je viacero vplyvov vynechaných, keďže jednotlivé techniky zväčša nemajú cieľ modifikovať viacero artefaktov. Okrem cieleného artefaktu však môžu vzniknúť nové artefakty, ktoré zachytávajú dianie v zariadení pri aplikácii anti-forenznej techniky. Na základe nich je potom možné detegovať použitie anti-forenznej techniky. Konkrétne ovplyvnené artefakty, ktoré je možné použiť na detekciu, sú popísané v príslušných kapitolách.

Je vidieť, že vplyvy podľa matice vplyvu sú miernejšie, čo je spôsobené prihliadnutím na náročnosť detekcie danej techniky. To však spôsobilo, že vplyvy šifrovania klesli na strednú úroveň, keďže je detekcia triviálna, avšak vieme, že žiadny z ovplyvnených artefaktov nie je možné obnoviť ani nahradiť iným. Na druhej strane, ukrývanie dát v ADS má síce veľký vplyv na dáta, je však jednoducho detekovateľný a dáta sa nestrácajú. V tomto prípade je preto vplyv podľa matice vplyvu výstižnejší.

Navrhnuté spôsoby určovania vplyvu na artefakty sú teda spoľahlivé iba do istej miery a možno by bolo presnejšie také ohodnotenie, ktoré berie do úvahy viacero faktorov.

Vplyv na hľadanie anomálií bolo možné popísať iba pre 2 z vybraných anti-forenzných techník. Dôvodom je nemožnosť aplikovať ADS a šifrovanie na extrahované tabuľkové dáta, ktoré máme k dispozícii.

S ohľadom na všetky behy programu sme vo výsledku dostali lepšie výsledné F1 skóre pre 5 zo 6 skúmaných prípadov. Výnimku predstavuje použitie detekcie anomálií na základe názvu pre timestomping. Toto sú však sumárne výsledky pre všetky behy programu, v ktorých sú mnohé nastavenia pri detekcii úplne neúspešné.

Relevantnejšie výsledky sme dostali pri porovnaní priemeru 5 najlepších nastavení pre beh programu. Zaznamenali sme mierny pokles F1 skóre pri mazaní súboru a jeho odkazu a výraznejšie zhoršenie F1 skóre pri použití timestompingu. To poukazuje na fakt, že výsledky detekcie anomálií pomocou nastavení, ktoré dávajú najlepšie výsledky pre pôvodné dáta, sa pri použití anti-forenzných techník zhoršia.

7 Záver

Načrtli sme princípy fungovania štyroch vybraných anti-forenzných techník a navrhli sme dva spôsoby, ktorými je možné jednotne popísať vplyv anti-forenznej techniky na artefakt. Tieto spôsoby sme použili na ohodnotenie vplyvov vybraných anti-forenzných techník. Vychádzali sme z informácií získaných otestovaním daných techník na operačnom systéme Windows 10.

Zistili sme, že najvýznamnejší vplyv na dáta má šifrovanie disku, po ňom sú na rovnakej úrovni mazanie a šifrovanie súborov, za nimi nasleduje timestomping a najmenší vplyv mala technika ukrývania dát v ADS. Na údaje z MFT má najväčší vplyv timestomping tesne nasledovaný šifrovaním disku.

Taktiež sme v tomto príspevku navrhli spôsob určenia vplyvu anti-forenzných techník na výsledky automatizovaného vyhľadávania anomálií nad dátami extrahovanými z disku. Toto ohodnotenie vplyvu sme aplikovali na mazanie súborov a timestomping, pretože nie každá technika sa dá aplikovať na už extrahovaných tabuľkových dátach. Výzvou bolo nájsť vhodné porovnanie originálnych výsledkov s výsledkami po aplikovaní anti-forenznej techniky. Vyskúšali sme niekoľko porovnaní a zistili sme, že má väčší význam porovnávať iba najlepšie dosiahnuté výsledky.

Ukázali sme, že timestomping dokáže zhoršiť presnosť, senzitivitu a F1 skóre výraznejšie ako mazanie súborov.

Cieľom bolo popísať vplyvy rôznych anti-forenzných techník na digitálne forenzné vyšetrovanie. To zahŕňalo popísanie vplyvu zvlášť na manuálnu forenznú analýzu a zvlášť na rôzne automatizované procesy. Jednotné popísanie vplyvov všetkých anti-forenzných techník môže pomôcť pri ďalšej automatizácii, kde je nevyhnutné sa vysporiadať aj s takýmito technikami útočníkov. Taktiež to pomôže pri definovaní postupov manuálnej forenznej analýzy, kde je rovnako potrebné brať do úvahy použitie anti-forenzných techník, ktoré môžu mať najvýraznejší vplyv na výsledky forenznej analýzy.

8 Zoznam použitej literatúry

Barker, E. (2020). Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms. *NIST Special Publication*, *800*(175B). https://doi.org/10.6028/NIST.SP.800-175Br1

Kanstrén, T. (2020). *A Look at Precision, Recall, and F1-Score*. Towards Data Science. https://towardsdatascience.com/a-look-at-precision-recall-and-f1-score-36b5fd0dd3ec

Markova, E., Sokol, P., & Kovacova, K. (2022). Detection of relevant digital evidence in the forensic timelines. *2022 14th International Conference on Electronics, Computers and Artificial Intelligence, ECAI 2022*. https://doi.org/10.1109/ECAI54874.2022.9847438

Palmbach, D., & Breitinger, F. (2020). Artifacts for Detecting Timestamp Manipulation in NTFS on Windows and Their Reliability. *Forensic Science International: Digital Investigation*, *32*. https://doi.org/10.1016/J.FSIDI.2020.300920