DOI: https://doi.org/10.33994/kndise.2023.68.46
УДК 343.98

Іван Володимирович Старенький
судовий експерт
сектору досліджень телекомунікаційних систем та засобів
лабораторії досліджень об'єктів інформаційних технологій, телекомунікаційних систем та засобів

ORCID: http://orcid.org/0009-0004-2271-8512
E-mail: ivan_starenkii@ukr.net

Олександра Ігорівна Донченко
судовий експерт
лабораторії досліджень об'єктів інформаційних технологій, телекомунікаційних систем та засобів

ORCID: http://orcid.org/0009-0005-3907-2372
E-mail: donchenko2707@gmail.com

Одеський науково-дослідний інститут судових експертиз Міністерства юстиції України

ВИЯВЛЕННЯ СЛІДІВ ВИКОРИСТАННЯ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ТИПУ «STEALER» В ПАМ'ЯТІ НАКОПИЧУВАЧА ІНФОРМАЦІЇ

В роботі розглянуто послідовність дій експерта при дослідженні побітової копії цифрового накопичувача інформації з метою виявлення серед наявних та видалених даних, відомостей щодо використання програмного забезпечення «Mars Stealer», що позиціонується як програмний продукт типу «Stealer», з подальшим дослідженням виявлених зразків за допомогою спеціалізованого криміналістичного програмного забезпечення.

Ключові слова: *цифровий носій інформації, образ, файл, стилер, програмне забезпечення, операційна система, віртуальна машина.*

Постановка проблеми. Актуальність даного дослідження обумовлюється тим, що жертвою програмного забезпечення (ПЗ) типу «Stealer» [1] (далі «стилер») може стати будь-який користувач електронно-обчислювальної машини (ЕОМ), що працює на базі певної операційної системи (ОС), у більшості випадків, це користувачі «Windows», що мають вихід до мережі Інтернет. Левова частка «зараження» ЕОМ шкідливим програмним забезпеченням (ШПЗ) відбувається через необачність користувачів при роботі в мережі Інтернет. Наприклад, це може бути електронний лист, що в своїй текстовій частині містить приховане URL-посилання, що здійснює завантаження виконуючого файлу

«стилеру», з його подальшою ініціалізацією у випадку здійснення кліку на URL-посилання; або це може бути спеціально організований WEB-сайт в мережі Інтернет, замаскований під ресурс по завантаженню безоплатного ПЗ по активації різноманітних програмних продуктів (ПП), наприклад, «Microsoft Office», «Активація Windows» тощо.

Також, у випадку успішності свого відпрацювання, ПЗ типу «стилер» можна оцінювати як ПП, що націлений на організацію витоку приватної інформації на окремо виділений в мережі Інтернет С2-сервер. Що робить ПЗ такого типу вкрай небезпечним, адже зловмисник може отримати інформацію щодо авторизаційних даних до банківських рахунків, закритих WEB-ресурсів державного або корпоративного рівня, тощо.

Аналіз останніх досліджень і публікацій. На жаль на просторах вітчизняної судової експертизи, даному питанню з точки зору наукового підходу не приділено дуже багато уваги. Більшість експертів, які в ході своєї роботи зустрічаються з ПЗ типу «стилер», користуючись напрацьованим за період своєї експертної діяльності досвідом, знають, що до найбільш розповсюджених та популярних «стилерів», серед зловмисників, відносяться: «Mars Stealer», «Raccoon», «RedLine Stealer», «Predator the thief», «BlackGuard», «Jester Stealer» та «AZORult».

Коли експерт з власного досвіду знає «як працює» той чи інший «стилер», то у відповідному руслі і формуються експертні дослідження. І саме тому у більшості випадків на вітчизняному рівні, питанню дослідження такого типу ПЗ присвячено дуже мало матеріалів. Саме тому, авторами даної роботи було розпочато роботу над написанням (з подальшим публікуванням) статей та тез, присвячених даній тематиці [2].

Мета дослідження. Експериментальним шляхом визначити характерні ознаки використання програмного забезпечення «Mars Stealer», що позиціонується як ПП типу «Stealer», що містяться в пам’яті серед наявних та видалених даних накопичувача інформації.

Виклад основного матеріалу. Як було зазначено в [2], ПЗ типу «стилер» є таким собі комплексом, що складається з двох частин: WEB-панелі, розміщеній на WEB-ресурсі в мережі Інтернет, та виконуючого файлу-ініціатора, так званий «build»-файл, що запускається на ураженій ЕОМ.

В даній роботі, експериментальним шляхом, авторами було розглянуто питання щодо виявлення слідів використання ПЗ «Mars Stealer» в пам’яті накопичувача інформації шляхом використання ПЗ «Autopsy – Digital Forensics» [3] (далі «Autopsy»). Даний експеримент вдалося реалізувати завдяки наявного у розпорядженні авторів зразку виконуючого build-файлу ПЗ «Mars Stealer», який було вилучено під час виконання реальної експертизи (на момент написання даної статті С2-сервер, з яким встановлював зв'язок build-файл, вже не діяв), та який було використано при написанні попередньої роботи [2].

Експертами було організовано декілька ізольованих віртуальних машин (ВМ) на основі ОС «Windows 10», на яких було ініціалізовано виконання виконуючого файлу «Build.exe», що є частиною ПЗ «Mars Stealer» (належність файлу «Build.exe» до ПЗ «Mars Stealer», було встановлено під

час виконання експертизи). Таким чином, в даній частині експерименту, експертами було змодельована ситуація зараження накопичувача персонального комп'ютера (ПК) ПЗ типу «стилер».

Далі, з віртуального накопичувача інфікованої ВМ, експертами, з використанням Live-дистрибутиву ОС «Kali Linux» [4] було створено побітову копію носія інформації з розширенням «*.dd», який в подальшому було просканово за допомогою ПЗ «Autopsy».

В першу чергу, аби знайти точний або вірогідний момент запуску виконуючого файлу, що є частиною ПЗ типу «стилер», необхідно переглянути історію запуску програм у розділі «Run Programs». Серед історії запущених процесів та програм потрібно ідентифікувати процеси, які не відносяться до стандартного переліку процесів ОС, та більш детально їх дослідити.

На рис. 1-2 наведено приклад виявлення запуску виконуючого файлу «Build.exe», з фіксацією дати запуску та визначенням директорії, в якій міститься даний виконуючий файл, в пам'яті накопичувача інформації.

Source Name	S	C	O	Program Name	Username	Date/Time
BACKGROUNDTASKHOST.EXE-145A3777.pf				BACKGROUNDTASKHOST.EXE		2023-05-12 11:21:14 EEST
BACKGROUNDTASKHOST.EXE-858A19DE.pf				BACKGROUNDTASKHOST.EXE		2023-05-12 11:33:59 EEST
BUILD.EXE-EF6B6D31.pf				BUILD.EXE		2023-05-12 11:58:03 EEST
BYTECODEGENERATOR.EXE-C1E9BCE6.pf				BYTECODEGENERATOR.EXE		2023-05-12 11:33:49 EEST

Рис. 1. Фрагмент історії запуску процесів програмних продуктів в середовищі ОС

Type	Value
Program Name	BUILD.EXE
Path	/USERS/TEST2/DESKTOP
Date/Time	2023-05-12 11:58:03 EEST
Count	1
Comment	Prefetch File
Source File Path	/img_image2.dd/vol_vol3/Windows/Prefetch/BUILD.EXE-EF6B6D31.pf
Artifact ID	-9223372036854773775

Рис. 2. Додаткові відомості щодо процесу «BUILD.EXE»

Знайшовши в історії запущених процесів потрібний нам процес, можемо скористатися програмним модулем ПЗ «Autopsy» – «Timeline», по встановленню переліку подій (з можливістю вибору діапазону), що відбувалися до та після запуску процесу «BUILD.EXE», див. рис. 3-4.

З метою внесення ясності, для читачів, які не знайомі з ПЗ «Autopsy», на рис. 5 авторами наведено розшифрування значень літер, якими в середовищі ПЗ «Autopsy» позначається певний тип події, що відбувалася на накопичувачі інформації.

Також зазначимо, що на момент запуску файлу «Build.exe» будь-які WEB-оглядачі перебували у вимкненому стані, в реальних умовах, є велика вірогідність того, що інфікування ЕОМ буде проведено хоча б з одним активно працюючим WEB-оглядачем, історію запуску якого можна отримати з теки «Windows/Prefetch» та зіставити з запуском потенційного ШПЗ з метою знаходження «дотичних точок».

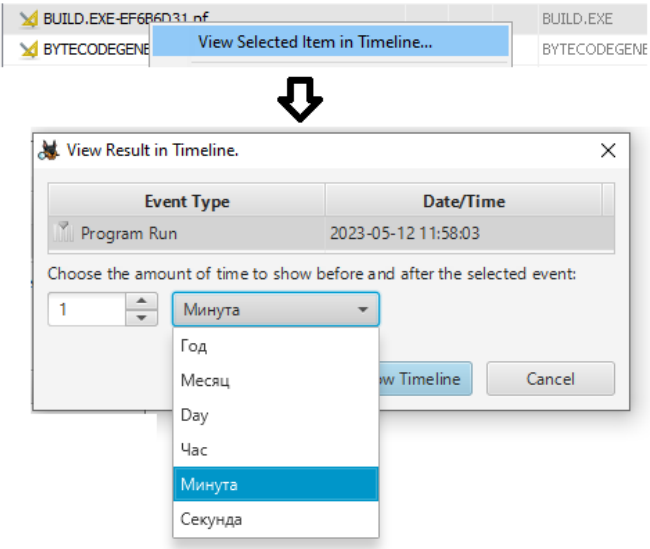


Рис. 3. Налаштування перегляду подій до/після запуску процесу

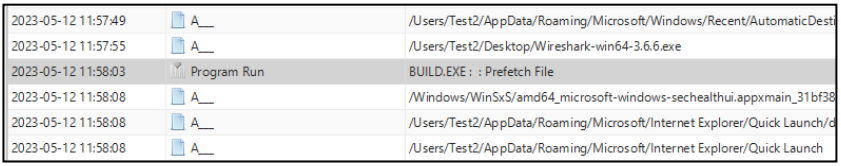


Рис.4. Перегляд процесів та подій, що відбувалися на накопичувачі інформації в програмному модулі «Timeline» ПЗ «Autopsy»

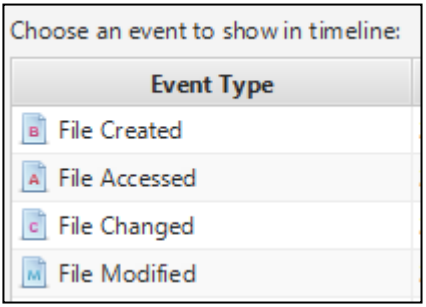
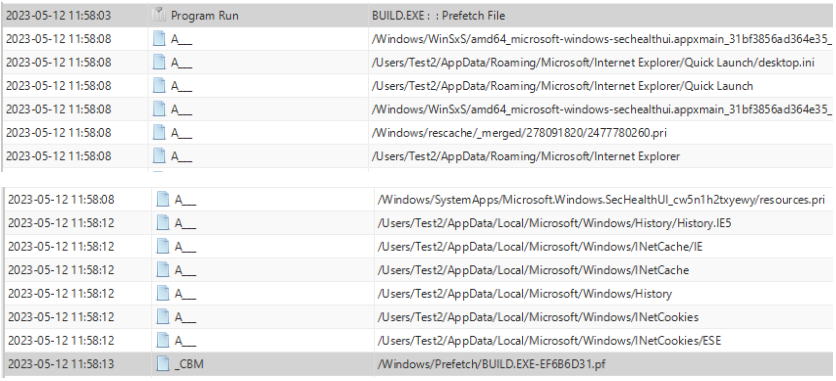


Рис. 5. Розшифровка значень літер, що присвоюються подіям, що відбувалися на накопичувачі інформації:
«B» – створення файлу; «A» – доступ до файлу; «C» – повідомлення про внесення зміни у файл; «M» – зміна у первинний стан файлу

Вже на першій хвилині своєї роботи після запуску, процес «BUILD.EXE» було змінено, про що свідчать атрибути стану події «_CBM», а між самим процесом запуску файлу, та внесенням зміни в його процес здійснювався доступ до файлів директорій WEB-оглядача «Microsoft Edge», яка знаходиться в прихованій теці «AppData» користувача ОС, див. рис. 6-7.



2023-05-12 11:58:03	Program Run	BUILD.EXE : : Prefetch File
2023-05-12 11:58:08	A__	/Windows/WinSxS/amd64_microsoft-windows-sechealthui.appxmain_31bf3856ad364e35_
2023-05-12 11:58:08	A__	/Users/Test2/AppData/Roaming/Microsoft/Internet Explorer/Quick Launch/desktop.ini
2023-05-12 11:58:08	A__	/Users/Test2/AppData/Roaming/Microsoft/Internet Explorer/Quick Launch
2023-05-12 11:58:08	A__	/Windows/WinSxS/amd64_microsoft-windows-sechealthui.appxmain_31bf3856ad364e35_
2023-05-12 11:58:08	A__	/Windows/rescache/_merged/278091820/2477780260.pri
2023-05-12 11:58:08	A__	/Users/Test2/AppData/Roaming/Microsoft/Internet Explorer
2023-05-12 11:58:08	A__	/Windows/SystemApps/Microsoft.Windows.SecHealthUI_cw5n1h2txyewy/resources.pri
2023-05-12 11:58:12	A__	/Users/Test2/AppData/Local/Microsoft/Windows/History/History.IE5
2023-05-12 11:58:12	A__	/Users/Test2/AppData/Local/Microsoft/Windows/INetCache/IE
2023-05-12 11:58:12	A__	/Users/Test2/AppData/Local/Microsoft/Windows/INetCache
2023-05-12 11:58:12	A__	/Users/Test2/AppData/Local/Microsoft/Windows/History
2023-05-12 11:58:12	A__	/Users/Test2/AppData/Local/Microsoft/Windows/INetCookies
2023-05-12 11:58:12	A__	/Users/Test2/AppData/Local/Microsoft/Windows/INetCookies/ESE
2023-05-12 11:58:13	_CBM	/Windows/Prefetch/BUILD.EXE-EF6B6D31.pf

Рис. 6. Перегляд процесів, що відбувалися між запуском файлу «Build.exe» та внесенням змін в його процес

Далі, на рис. 7-8 наведено звернення до Cache-інформації WEB-оглядача «Internet Explorer» та звернення до теки «Windows/SoftDistribution/», яка використовується службою оновлення Windows для завантаження оновлень на комп'ютер з подальшим встановленням, а також зберігає відомості про всі раніше встановлені оновлення. Після встановлення вони залишаються там ще деякий час, а потім видаляються системою автоматично.

Можна зробити висновок, що з великою долею вірогідності таким чином, процес «BUILD.EXE» збирав свідчення щодо версії ОС, яка була встановлена в середовищі ВМ.

На рис. 9 наведено звернення до теки WEB-оглядача «Google Chrome», з подальшим утворенням в кореневій директорії виконуючого файлу «Build.exe» (в нашому випадку, це «Робочий стіл») файлу «I5PPP8YC», який є sqlite3 базою даних (див. рис. 10).

2023-05-12 11:58:58	A__	/Users/Test2/AppData/Local/Microsoft/Windows/Explorer/thumbcache_32.db
2023-05-12 11:58:58	A__	/Users/Test2/AppData/Local/Microsoft/Windows/Explorer/thumbcache_96.db
2023-05-12 11:58:58	A__	/Users/Test2/AppData/Local/Microsoft/Windows/Explorer/iconcache_256.db
2023-05-12 11:58:58	A__	/Users/Test2/AppData/Local/Microsoft/Windows/Explorer/thumbcache_768.db
2023-05-12 11:58:58	A__	/Users/Test2/AppData/Local/Microsoft/Windows/Explorer/iconcache_48.db
2023-05-12 11:58:58	A__	/Users/Test2/AppData/Local/Microsoft/Windows/Explorer/thumbcache_16.db

Рис. 7. Звернення до Cache-файлів WEB-оглядача «Internet Explorer»

2023-05-12 11:58:59	_C_M	/Windows/SoftwareDistribution/DataStore/Logs
2023-05-12 11:58:59	AC_M	/Windows/SoftwareDistribution/DataStore/Logs/edb.chk
2023-05-12 11:58:59	A___	/Windows/SoftwareDistribution/DataStore
2023-05-12 11:58:59	A___	/Windows/WinSxS/amd64_microsoft-windows-w..ient-core.resources_31bf3856
2023-05-12 11:58:59	AC_M	/Windows/Logs/WindowsUpdate/WindowsUpdate.20230512.114737.526.12.etl
2023-05-12 11:58:59	A___	/Windows/SoftwareDistribution
2023-05-12 11:58:59	AC_M	/Windows/SoftwareDistribution/DataStore/Logs/edb.log
2023-05-12 11:58:59	A___	/Windows/Logs/WindowsUpdate
2023-05-12 11:58:59	AC_M	/Windows/SoftwareDistribution/DataStore/DataStore.jfm
2023-05-12 11:58:59	AC_M	/Windows/SoftwareDistribution/DataStore/DataStore.edb

Рис.8. Звернення до файлів директорії «Windows/SoftDistribution/»

2023-05-12 12:01:34	A___	/Users/Test2/AppData/Local/Google/Chrome/User Data/Crowd Deny
2023-05-12 12:01:34	_C_M	/Users/Test2/Desktop
2023-05-12 12:01:34	A___	/Users/Test2/AppData/Local/Google/Chrome/User Data/Default/Network
2023-05-12 12:01:34	A___	/Users/Test2/AppData/Local/Google/Chrome/User Data
2023-05-12 12:01:34	A___	/Users/Test2/AppData/Local/Google/Chrome/User Data/AutofillStates
2023-05-12 12:01:34	A___	/Users/Test2/AppData/Local/Google/Chrome/User Data/ClientSidePhishing
2023-05-12 12:01:34	A___	/Users/Test2/AppData/Local/Google/Chrome/User Data/Crashpad/attachments
2023-05-12 12:01:34	A___	/Users/Test2/AppData/Local/Google/Chrome/User Data/Default/Network/Cookies
2023-05-12 12:01:34	A___	/Users/Test2/AppData/Local/Google/Chrome/User Data/CertificateRevocation
2023-05-12 12:01:34	A___	/Users/Test2/AppData/Local/Google/Chrome/User Data/Local State
2023-05-12 12:01:34	Program Run	WERFAULT.EXE : : Prefetch File
2023-05-12 12:01:34	A_B_	/Users/Test2/Desktop/I5PPP8YC

Рис. 9. Перегляд історії процесів, що зверталися до файлів директорії WEB-оглядача «Google Chrome» та утворення файлу «I5PPP8YC»

Metadata

Name:	/img_image2.dd/vol_vol3/Users/Test2/Desktop/I5PPP8YC
Type:	File System
MIME Type:	application/x-sqlite3

Рис. 10. Інформація щодо файлу «I5PPP8YC»

За допомогою ПЗ «DB Browser for SQLite» [5] було встановлено структуру та інформаційне наповнення файлу «I5PPP8YC», що наведені на рис. 11-12.

Имя	Тип	Схема
Таблицы (2)		
cookies		CREATE TABL
meta		CREATE TABL
Индексы (1)		
cookies_unique_index		CREATE UNIQ
Представления (0)		
Триггеры (0)		

Рис. 11. Структура файлу «I5PPP8YC»

creation_utc	host_key	top_frame_site_key	name	val
Фильтр	Фильтр	Фильтр	Фильтр	Фил
13328353993911738	.google.com		AEC	
13328353999321112	.mozilla.org		_ga	
13328353997362807	.mozilla.org		_gat_UA-36116321-1	
13328353997303878	.mozilla.org		_gid	
13328353997471980	www.mozilla.org		moz-stub-attribution-code	
13328353997472538	www.mozilla.org		moz-stub-attribution-sig	
13328353993911583	.google.com		1P_JAR	
13328354051375896	www.google.com		DV	
13328354050903812	.google.com		NID	
13328354050903859	.google.com		SNID	
13328354053143237	.yadro.ru		VID	
13328354052949544	.lostfilm.tv		_ga	
13328354045901554	.mozilla.org		_ga_MQ7767QQQW	

Рис. 12. Частковий вміст таблиці «cookies»

Як видно з рис. 12, файл «I5PPP8YC» містить в собі інформацію щодо cookies різних WEB-ресурсів, що відвідувалися встановленими в пам'яті накопичувача ОС WEB-оглядачами, а саме, «Google Chrome» та «Mozilla Firefox».

Далі в історії процесів було виявлено два процеси, що є звітом щодо припинення роботи виконуючого файлу «Build.exe» (див. рис.13), через невстановлену помилку.

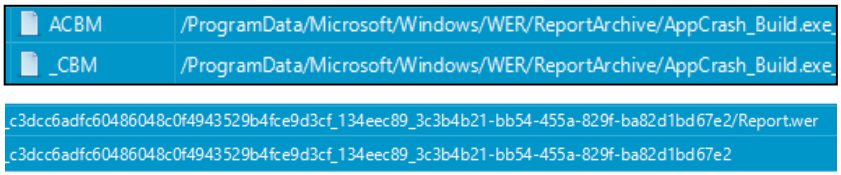


Рис. 13. Процес створення файлу «Report.wer»

З великою долею вірогідності дана помилка виникла через те, що C2-сервер, до якого повинен звертатися під час свого виконання файл «Build.exe» перестав функціонувати, і скоріш за все, файл «I5PPP8YC» не містить в собі інформації щодо історії переглядів WEB-ресурсів в мережі Інтернет, збережених в WEB-оглядачах авторизаційних даних, а містить лише cookies, та через відсутність з'єднання з C2-сервером був «вимушений» вивантажитися в кореневій теці виконуючого файлу «Build.exe».

Сам файл «Report.wer» містить в собі інформацію щодо бібліотек, з якими файл «Build.exe» вступав у взаємодію, під час своєї роботи.

Висновки. На основі проведеного експерименту можна зробити наступні висновки:

1. ПЗ «Autopsy» є гарним інструментом для спроби відтворення та відстеження подій та процесів, що відбувалися на накопичувачі інформації.

2. Шляхом дослідження подій та процесів в пам'яті накопичувача інформації, вдалося встановити послідовність дій експерта для виявлення виконуючого файлу(ів) стороннього ПЗ, яке може бути шкідливим.

3. У випадку, коли дослідження виявленого виконуючого build-файлу проводиться не відразу після отримання об'єктів дослідження, а через якийсь певний час, наприклад протягом 90 календарних днів, є велика імовірність «втратити» зв'язок з С2-сервером, до якого звертається build-файл. Але, з метою встановлення IP-адреси, до якої звертається файл-ініціатор на ураженій ЕОМ, рекомендується багаторазово виконувати запуск build-файлу (це може збільшити шанси на виявлення IP-адреси С2-серверу) паралельно відстежуючи Інтернет трафік, що буде проходити через ВМ.

4. Виконуючий файл-ініціатор на ураженій ЕОМ ПЗ «Mars Stealer», навіть при наявності помилки в свої роботі, буде «вимушений» зберегти зібрану на ураженій ЕОМ інформацію в кореневу теку розташування самого Build-файлу.

5. По результатам проведеної роботи можна встановити характерні ознаки використання ПЗ «Mars Stealer», що позиціонується як ПЗ типу «стилер», до яких відноситься журналювання кількості запусків виконуючого Build-файлу, та взаємодія з теками WEB-оглядачів, встановлених в пам'яті накопичувача інформації, а також взаємодія з чисельною кількістю бібліотек.

6. Отримані результати експерименту, що наведено в даній роботі, можуть бути використані при проведені експертиз за експертною спеціальністю 10.9 «Дослідження комп'ютерної техніки та програмних продуктів», при дослідженні накопичувачів інформації, серед наявних та видалених даних яких було виявлено інформацію щодо зразків виконуючих файлів ПЗ «Mars Stealer», що підтверджується зібраними свідченнями в ході проведення експертизи.

Перелік посилань

1. Державна служба спеціального зв'язку та захисту інформації України. URL:https://www.cip.gov.ua/ua (дата звернення 10.05.2023).

2. Старенький І. Дослідження Build-файлів потенційно шкідливого програмного забезпечення типу «Stealer». *Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності: постійно діюча Міжнар. наук.-практ. конф.* (м. Кропивницький, 24 березня 2023 р.). Кропивницький, 2023.

3. Autopsy – Digital Forensics. URL: https://www.autopsy.com/ (дата звернення 10.05.2023).

References

1. State Special Communications Service of Ukraine. Retrieved from: https://www.cip.gov.ua/ua (access date 10.05.2023) (in Ukrainian).

2. Starenkyi, I. (2023). Investigation of Build files of potentially malicious software type «Stealer». *The ongoing international scientific and practical conference «Actual issues of improving forensic and law enforcement activities».* (Kropyvnytskyi, March 24). (in Ukrainian)

3. Autopsy – Digital Forensics. Retrieved from: https://www.autopsy.com/ (access date 10.05.2023) (in Ukrainian).

4. Kali Linux. URL: https://uk.wikipedia.org/wiki/Kali_Linux (дата звернення 10.05.2023).

5. DB Browser for SQLite. URL: https://sqlitebrowser.org/ (дата звернення 10.05.2023).

4. Kali Linux. Retrieved from: https://uk.wikipedia.org/wiki/Kali_Linux (access date 10.05.2023) (in Ukrainian).

5. DB Browser for SQLite. Retrieved from: https://sqlitebrowser.org/ (access date 10.05.2023) (in Ukrainian)

DETECTION OF TRACES OF THE USE OF SOFTWARE SUCH AS «STEALER» IN THE MEMORY OF THE STORAGE DEVICE

I. Starenkyi
O. Donchenko

The purpose of this work is to use an experimentally way to determine the characteristic features of the use of the software «Mars Stealer», which is positioned as a software product of the «Stealer» type, which is contained in the memory among the available and deleted data of the information storage device.

The following conclusions can be drawn on the basis of the conducted experiment:

1. Autopsy» software is a good tool for trying to reproduce and trace the events and processes that took place on the storage device;

2. By studying the events and processes in the memory of the information storage, it was possible to establish the sequence of actions of the expert to detect the executable file(s) of third-party software that may be malicious;

3. In the case when the research of the detected executable build file is not carried out immediately after receiving the research objects, but after a certain time, for example, within 90 calendar days, there is a high probability of «losing» communication with the C2 server, which the build – file calls. But, in order to establish the IP address to which the file-initiator try to connect on the affected computer, it is recommended to repeatedly run the build-file (this may increase the chances of detecting the IP address of the C2 server) while simultaneously monitoring the Internet traffic, which will go through a virtual machine;

4. The executing file-initiator on the affected PC by the «Mars Stealer» software, even if there is an error in its work, will be «forced» to save the information collected on the affected PC in the root directory of the location of the Build file itself;

5. Based on the results of the work carried out, it is possible to establish the characteristic features of the use of the «Mars Stealer» software, which is positioned as a «stealer» type of software, which include logging the number of launches of the executing Build-file, and interaction with the folders of WEB browsers installed in the memory storage of information, as well as interaction with a large number of libraries.

6. The obtained results of the experiment given in this paper can be used when conducting examinations in the expert speciality 10.9 «Research of computer equipment and software products», in the study of information storage devices, among the available and deleted data of which information about samples of executable files of the «Mars Stealer» software, which is confirmed by the evidence collected during the examination.

Key words: digital media, image, file, stealer, software, operating system, virtual machine.