

Отчёт по кейсу: RomCom

Автор: HTB Sherlocks | Дата: 15.09.2025

1. Введение

Сьюзан работает в исследовательской лаборатории международной больницы Форела. С её компьютера поступило предупреждение от Microsoft Defender, и она также упомянула, что при извлечении документа из полученного файла возникло множество ошибок, но документ открылся без проблем. Согласно последним данным об угрозах, WinRAR используется для получения первоначального доступа к сетям, а WinRAR — одна из программ, которые используют сотрудники. Вы — аналитик по угрозам с опытом работы в DFIR. Вам предоставили упрощённую схему для начала расследования, пока команда SOC изучает среду на предмет других признаков атаки

2. Объекты исследования

Имя файла	Источник	Размер	MD5 / SHA256
2025-09-02T083211_pathology_department_incidentalert.vhdx	Получено: HTB Sherlocks / 11.09.2025	306 184 192 байт	MD5: 53e478204486ff1ebb6b7d6881a6af69 SHA256: cccd85ef47fd372a1ebf0f759d212dda378a8b0832bd98d4263eb6a9c7d99ee1

3. Chain of Custody (цепочка хранения доказательств)

Хэш-сумма:

MD5 53e478204486ff1ebb6b7d6881a6af69

SHA256 cccd85ef47fd372a1ebf0f759d212dda378a8b0832bd98d4263eb6a9c7d99ee1

```
C:\Users\Ярослава>certutil -hashfile "C:\Users\Ярослава\Downloads\RomCom\2025-09-02T083211_pathology_department_incidentalert.vhdx" MD5
Хэш MD5 C:\Users\Ярослава\Downloads\RomCom\2025-09-02T083211_pathology_department_incidentalert.vhdx:
53e478204486ff1ebb6b7d6881a6af69
CertUtil: -hashfile - команда успешно выполнена.
```

4. Инструменты и окружение

- AccessData FTK Imager 4.7.1.2
- R-STUDIO Network 9.4
- MFTECmd tool
- Timeline Explorer tool

5. Методология

- Анализ MFT
- Анализ USNJournal
- Evaluating evidence of CVE-2025-8088

6. Ход исследования (пошагово)

1. CVE-2025-8088 — идентификатор критической уязвимости «нулевого дня» в архиваторе WinRAR, обнаруженной в середине июля 2025 года. Эта уязвимость позволяет злоумышленникам размещать вредоносные исполняемые файлы в защищённых системных папках при открытии жертвой специально созданного архива.
2. Монтирование диска с помощью СПО AccessData FTK Imager. Открывая смонтированный диск в Проводнике, мы видим папку C (подразумевается диск C:\) с файлом \$MFT и файл «2025-09-02T08_32_11_5202830_CopyLog.csv».
3. Скачиваем MFTECmd и Timeline Explorer для работы с файлом MFT. Запускаем с помощью командной строки MFTECmd и создаем .csv файл с образа \$MFT с названием **20250915140257_MFTECmd_\$MFT_Output.csv**

```
C:\Users\Public\MFTECmd>.\MFTECmd.exe -f "C:\Users\Public\<div data-bbox="142 706 858 743" data-label="List-Group">
4. Далее открываем его в Timeline Explorer. Ищем архив .rar, который был загружен по условиям задания: Pathology-Department-Research-Records.rar
```

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

20250915140257_MFTECmd_\$MFT_Output.csv

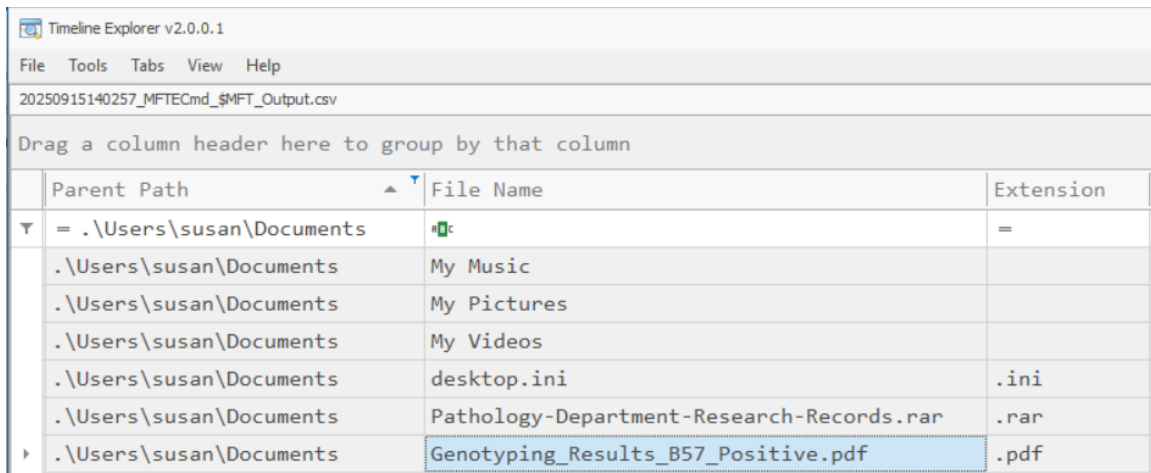
Drag a column header here to group by that column

Enter text to search...

Find

	Parent Path	File Name	Extensio	Is Directory
▼	D:	D:	= .rar	<input checked="" type="checkbox"/>
	.\Users\susan\AppData\Local\Temp\vmware-susan\VMwareDnD\9775F068	Pathology-Department-Research-Records.rar	.rar	<input type="checkbox"/>
	.\Users\susan\Documents	Pathology-Department-Research-Records.rar	.rar	<input type="checkbox"/>

По этому же пути Root\Users\susan\Documents\ находится файл **Genotyping_Results_B57_Positive.pdf**

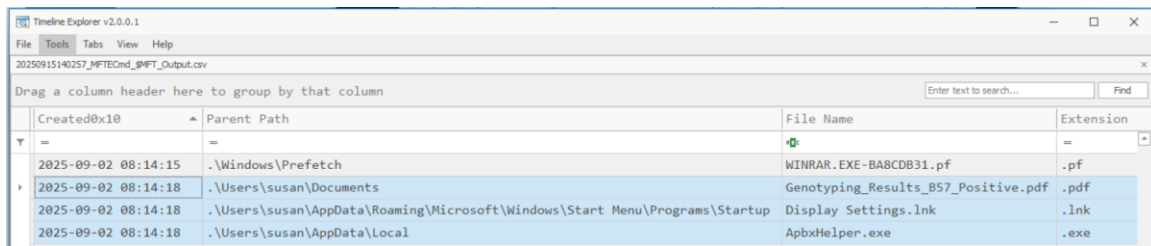


	Parent Path	File Name	Extension
▼	= .\Users\susan\Documents	My Music	
	.\Users\susan\Documents	My Pictures	
	.\Users\susan\Documents	My Videos	
	.\Users\susan\Documents	desktop.ini	.ini
	.\Users\susan\Documents	Pathology-Department-Research-Records.rar	.rar
▶	.\Users\susan\Documents	Genotyping_Results_B57_Positive.pdf	.pdf

5. С помощью Timeline Explorer изучаем время запуска архива: 02.09.2025 08:14:18

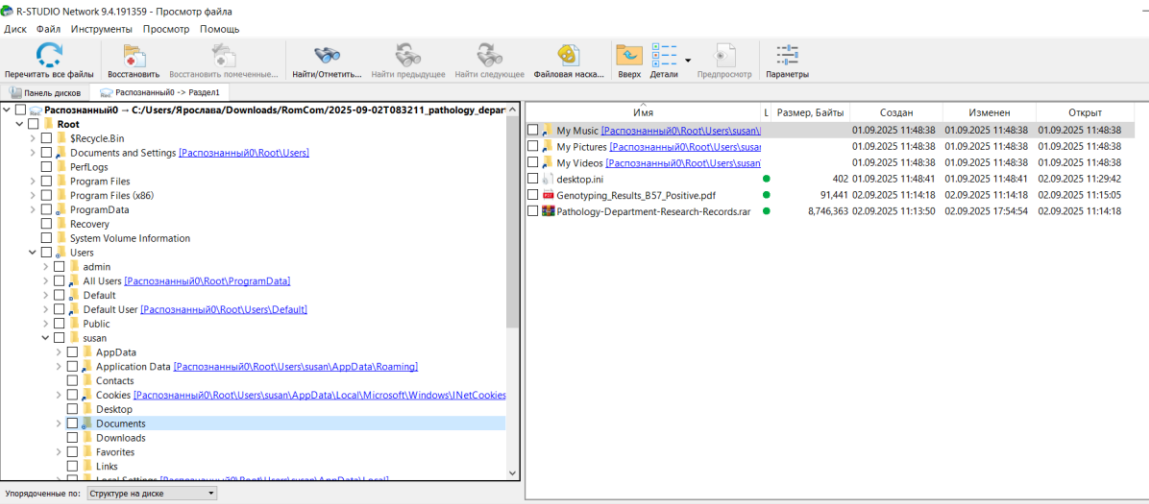
В это же время был создан исполняемый файл бэкдора, который распаковывается из архивного файла **Root\Users\susan\AppData\Local\ApbxHelper.exe**

Эксплойт также создаёт файл, который упрощает сохранение и выполнение бэкдора **Display Settings.lnk**



	Created0x10	Parent Path	File Name	Extension
▼	=		WINRAR.EXE-BABCD831.pf	.pf
▶	2025-09-02 08:14:15	.\Windows\Prefetch	Genotyping_Results_B57_Positive.pdf	.pdf
	2025-09-02 08:14:18	.\Users\susan\Documents	Display Settings.lnk	.lnk
	2025-09-02 08:14:18	.\Users\susan\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup	ApbxHelper.exe	.exe
	2025-09-02 08:14:18	.\Users\susan\AppData\Local		

6. С помощью программы R-STUDIO Network был получен доступ к содержимому диска.



7. Находки

	Имя	Путь
1.	Genotyping_Results_B57_Positive.pdf	Root\Users\susan\Documents\
2.	Pathology-Department-Research-Records.rar	Root\Users\susan\Documents\
3.	ApbxHelper.exe	Root\Users\susan\AppData\Local\
4.	Display Settings.lnk	Root\Users\susan\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

8. Выводы и рекомендации

Изучены уязвимость в WinRAR, а также утилита Timeline Explorer, позволяющая смотреть действия пользователя по временной шкале.

9. Приложение:



RomCom has been Solved

yayara has successfully solved RomCom from Hack The Box

#152

SHERLOCK RANK

15 Sep 2025

SOLVE DATE

Powered by  **HACKTHEBOX**