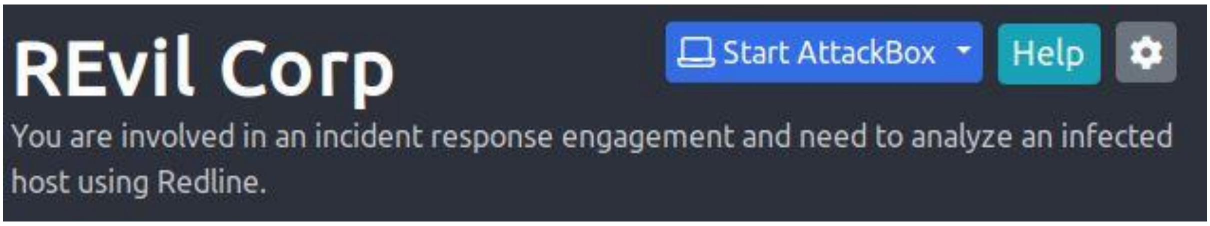
TRY HACK ME: Write-Up REvil Corp – Malware Analysis with FireEye RedLine



REvil Corp

You are involved in an incident response engagement and need to analyze an infected host using Redline.

Task 1 Investigating the Compromised Endpoint –

Scenario: One of the employees at Lockman Group gave an IT department the call; the user is frustrated and mentioned that all of his files are renamed to a weird file extension that he has never seen before. After looking at the user's workstation, the IT guy already knew what was going on and transferred the case to the Incident Response team for further investigation.

You are the incident responder. Let's see if you can solve this challenge using the infamous Redline tool. Happy Hunting, my friend!

To start your investigation, open the Mandiant Analysis file in the Analysis File folder on the Desktop.

Note: Loading the Mandiant Analysis file may take 2-3 minutes.

Deploy the machine attached to this task; it will be visible in the split-screen view once it is ready.

If you don't see a virtual machine load then click the Show Split View button.

If you wish to access the virtual machine via Remmina, use the credentials below.

Machine IP: 10.10.121.155

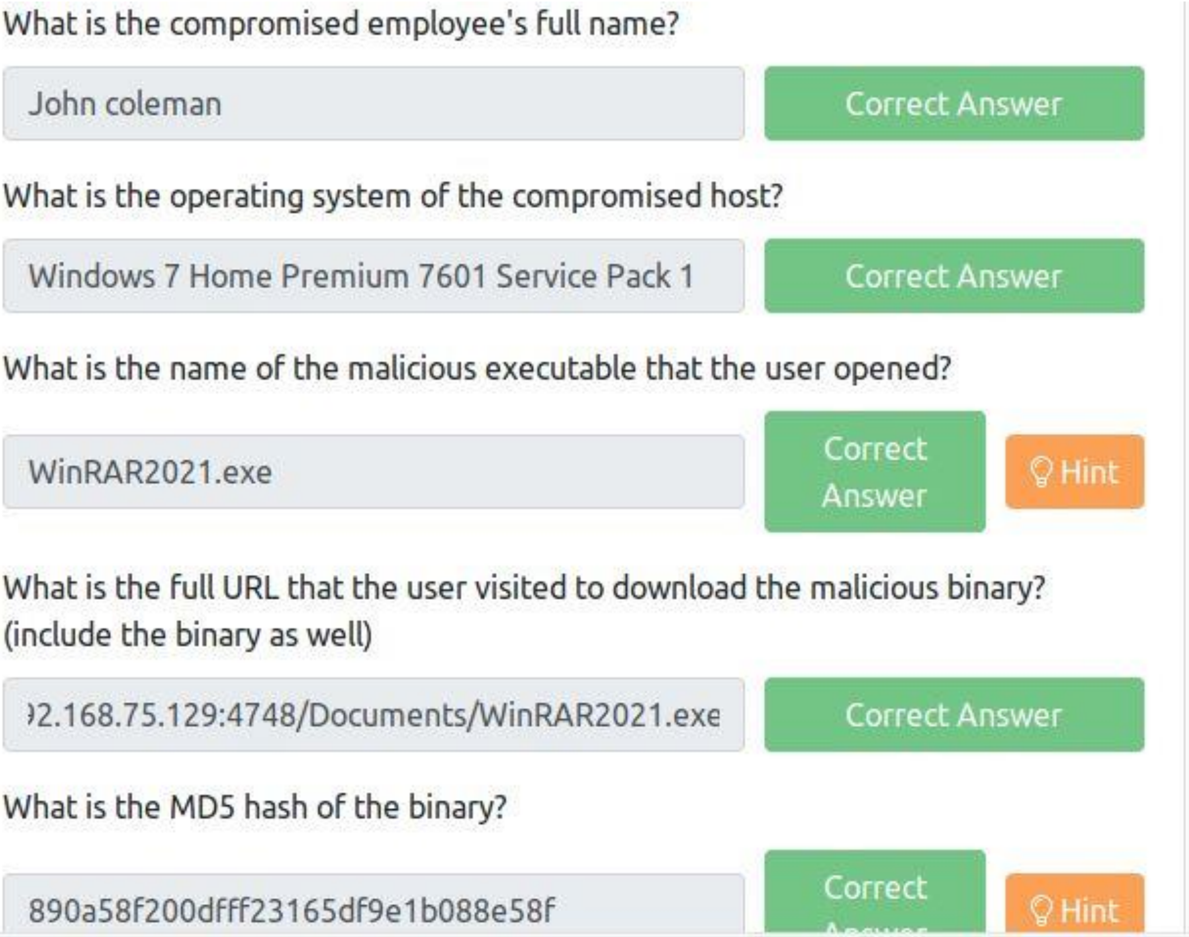
User: administrator

Password: letmein123!

Accept the Certificate when prompted, and you should be logged into the remote system now.

Note: The virtual machine may take up to 3 minutes to load.

Answer to the questions of this section-



What is the compromised employee's full name?

John coleman

What is the operating system of the compromised host?

Windows 7 Home Premium 7601 Service Pack 1

What is the name of the malicious executable that the user opened?

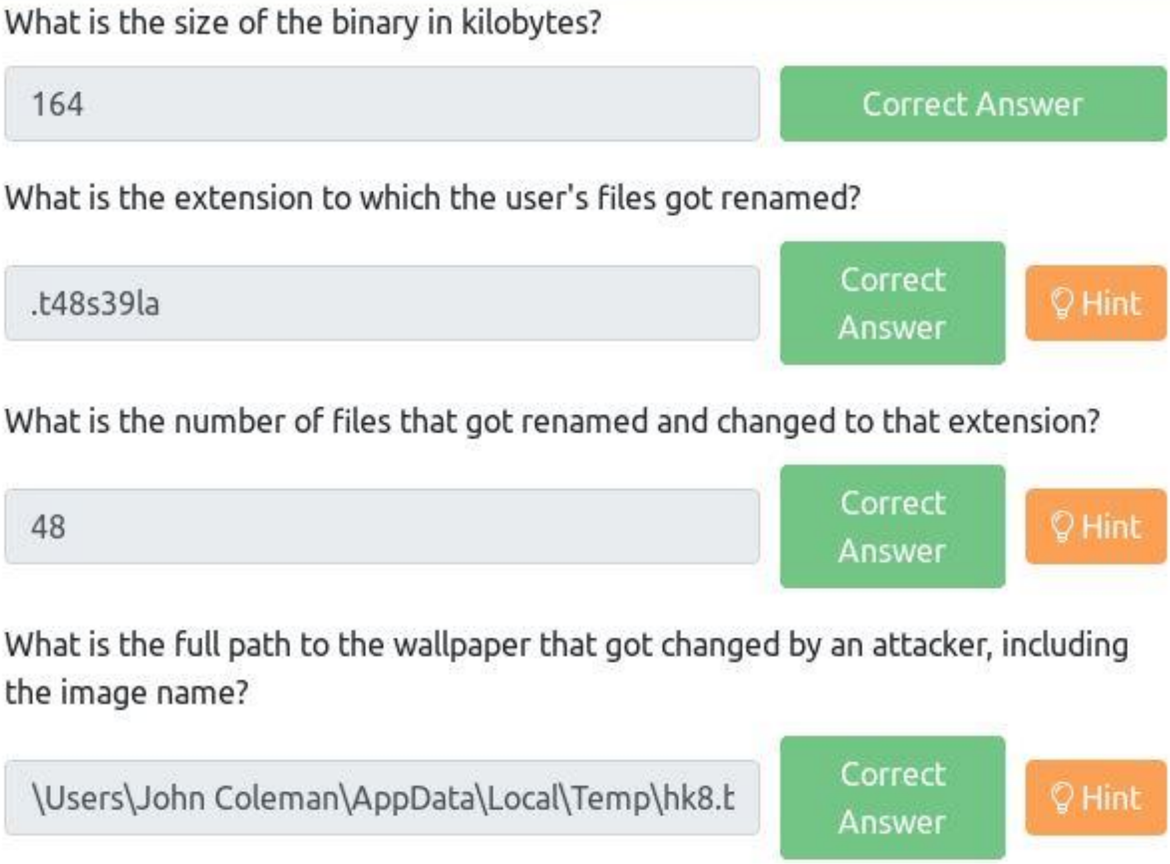
WinRAR2021.exe

What is the full URL that the user visited to download the malicious binary? (include the binary as well)

92.168.75.129:4748/Documents/WinRAR2021.exe

What is the MD5 hash of the binary?

890a58f200dfff23165df9e1b088e58f



What is the size of the binary in kilobytes?

164

What is the extension to which the user's files got renamed?

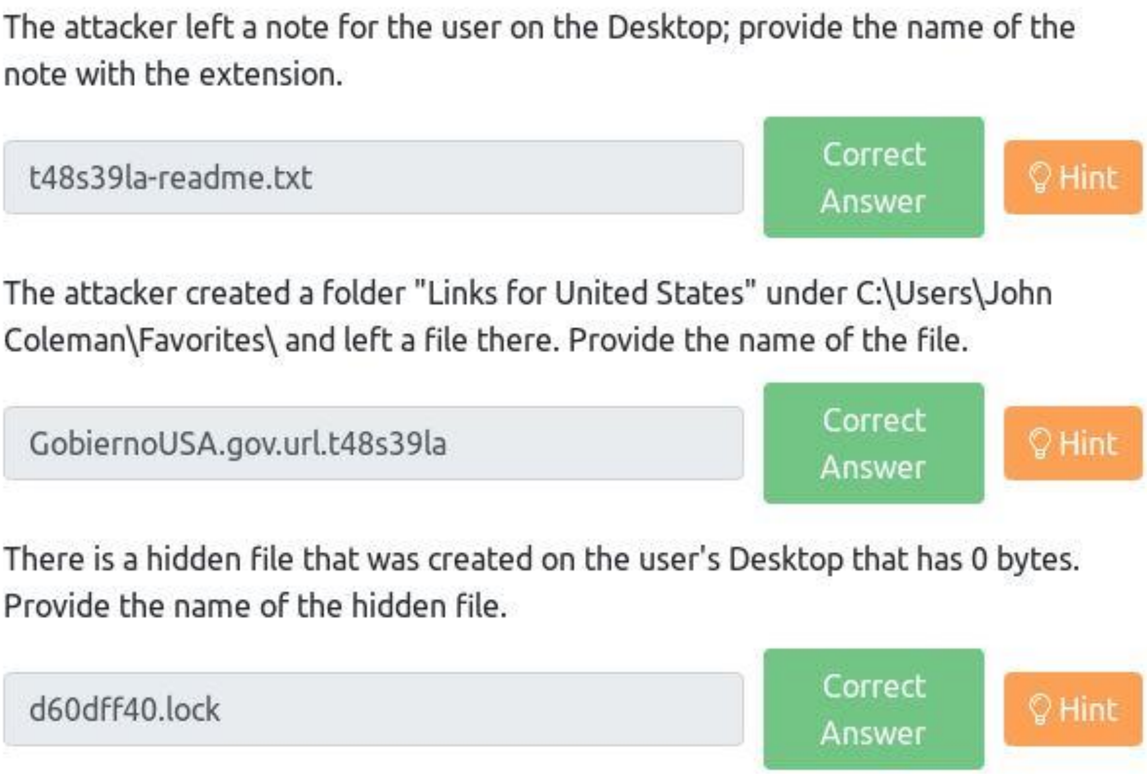
.t48s39la

What is the number of files that got renamed and changed to that extension?

48

What is the full path to the wallpaper that got changed by an attacker, including the image name?

\Users\John Coleman\AppData\Local\Temp\hk8.t



The attacker left a note for the user on the Desktop; provide the name of the note with the extension.

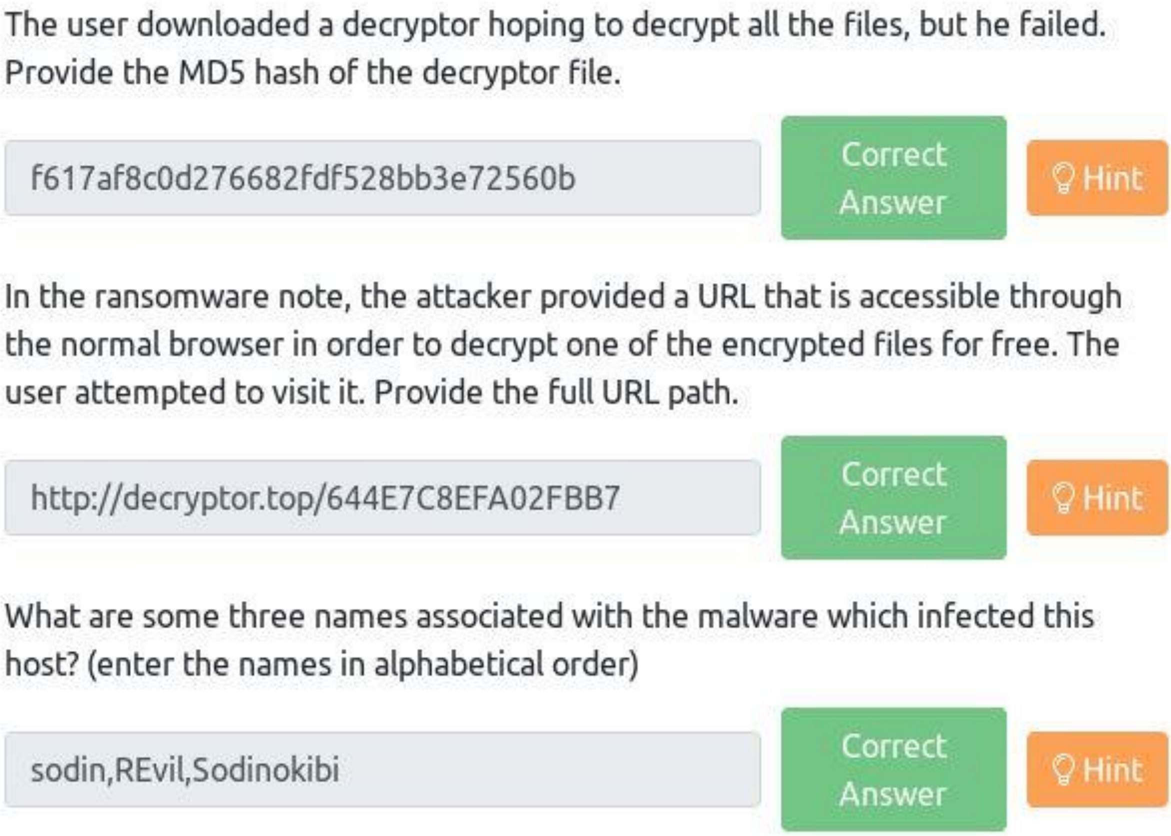
t48s39la-readme.txt

The attacker created a folder "Links for United States" under C:\Users\John Coleman\Favorites\ and left a file there. Provide the name of the file.

GobiernoUSA.gov.url.t48s39la

There is a hidden file that was created on the user's Desktop that has 0 bytes. Provide the name of the hidden file.

d60dff40.lock



The user downloaded a decryptor hoping to decrypt all the files, but he failed. Provide the MD5 hash of the decryptor file.

f617af8c0d276682fdf528bb3e72560b

In the ransomware note, the attacker provided a URL that is accessible through the normal browser in order to decrypt one of the encrypted files for free. The user attempted to visit it. Provide the full URL path.

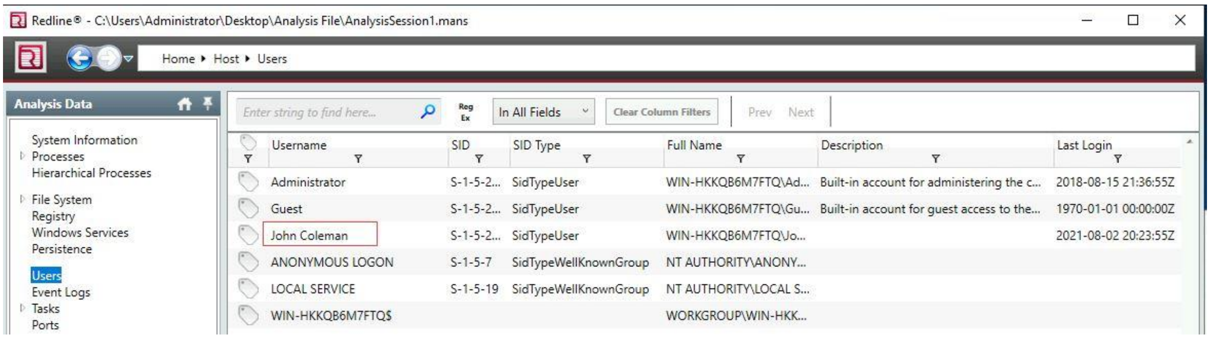
http://decryptor.top/644E7C8EFA02FBB7

What are some three names associated with the malware which infected this host? (enter the names in alphabetical order)

sodin,REvil,Sodinokibi

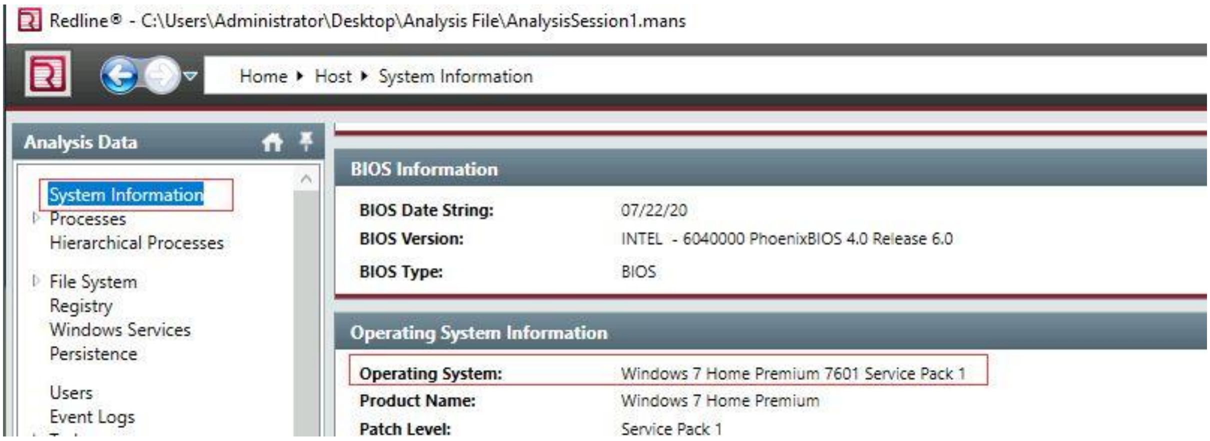
Answers-

1) Navigate to users



Username	SID	SID Type	Full Name	Description	Last Login
Administrator	S-1-5-2...	SidTypeUser	WIN-HKKQB6M7FTQ\Ad...	Built-in account for administering the c...	2018-08-15 21:36:55Z
Guest	S-1-5-2...	SidTypeUser	WIN-HKKQB6M7FTQ\Gu...	Built-in account for guest access to the...	1970-01-01 00:00:00Z
John Coleman	S-1-5-2...	SidTypeUser	WIN-HKKQB6M7FTQ\Jo...		2021-08-02 20:23:55Z
ANONYMOUS LOGON	S-1-5-7	SidTypeWellKnownGroup	NT AUTHORITY\ANONY...		
LOCAL SERVICE	S-1-5-19	SidTypeWellKnownGroup	NT AUTHORITY\LOCAL S...		
WIN-HKKQB6M7FTQ$			WORKGROUP\WIN-HKK...		

2) Navigate to System Information



BIOS Information

BIOS Date String: 07/22/20

BIOS Version: INTEL - 6040000 PhoenixBIOS 4.0 Release 6.0

BIOS Type: BIOS

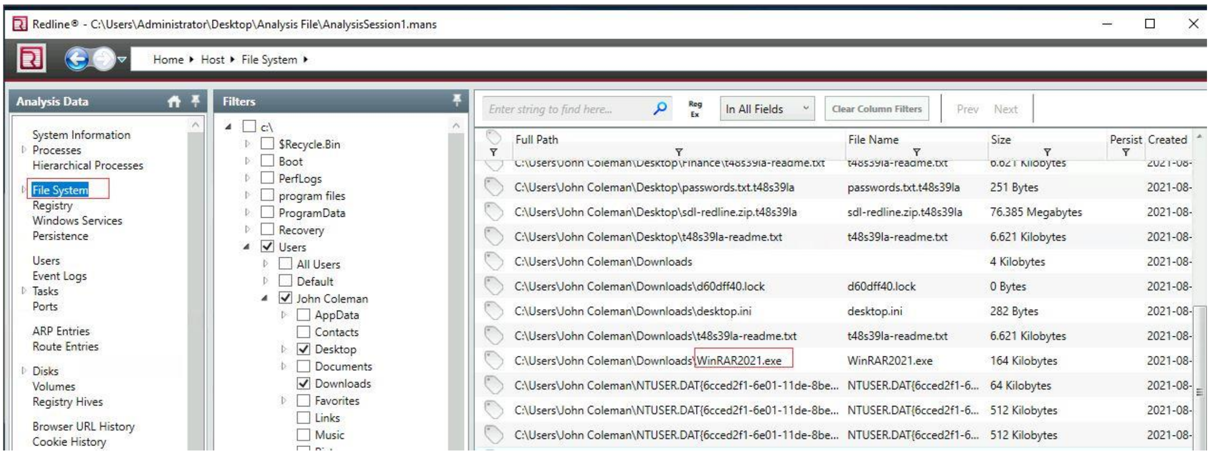
Operating System Information

Operating System: Windows 7 Home Premium 7601 Service Pack 1

Product Name: Windows 7 Home Premium

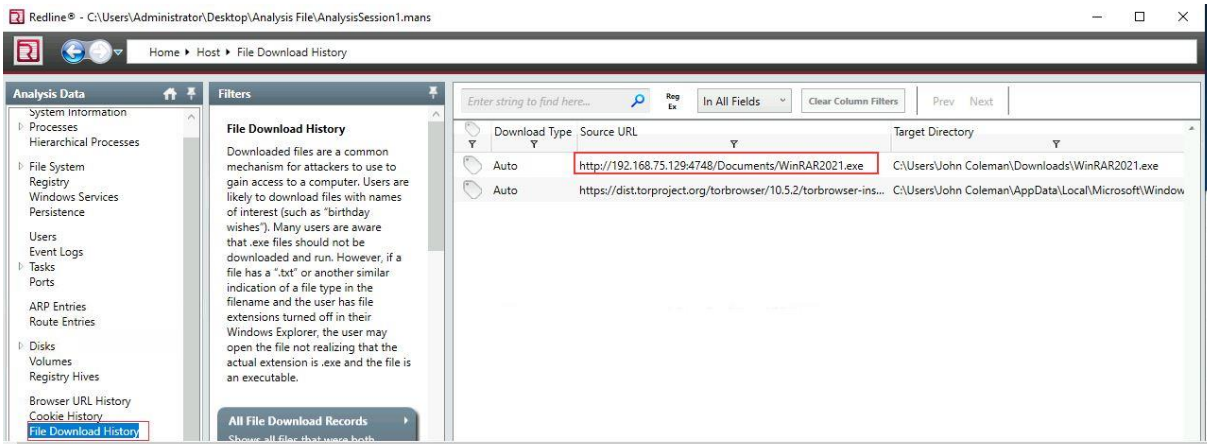
Patch Level: Service Pack 1

3) Navigate to File System



Full Path	File Name	Size	Persist	Created
C:\Users\John Coleman\Desktop\Finance\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes		2021-08-
C:\Users\John Coleman\Desktop\passwords.txt.t48s39la	passwords.txt.t48s39la	251 Bytes		2021-08-
C:\Users\John Coleman\Desktop\sdl-redline.zip.t48s39la	sdl-redline.zip.t48s39la	76.385 Megabytes		2021-08-
C:\Users\John Coleman\Desktop\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes		2021-08-
C:\Users\John Coleman\Downloads		4 Kilobytes		2021-08-
C:\Users\John Coleman\Downloads\d60dff40.lock	d60dff40.lock	0 Bytes		2021-08-
C:\Users\John Coleman\Downloads\desktop.ini	desktop.ini	282 Bytes		2021-08-
C:\Users\John Coleman\Downloads\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes		2021-08-
C:\Users\John Coleman\Downloads\WinRAR2021.exe	WinRAR2021.exe	164 Kilobytes		2021-08-
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	64 Kilobytes		2021-08-
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	512 Kilobytes		2021-08-
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	512 Kilobytes		2021-08-

4) Navigate to File Download History

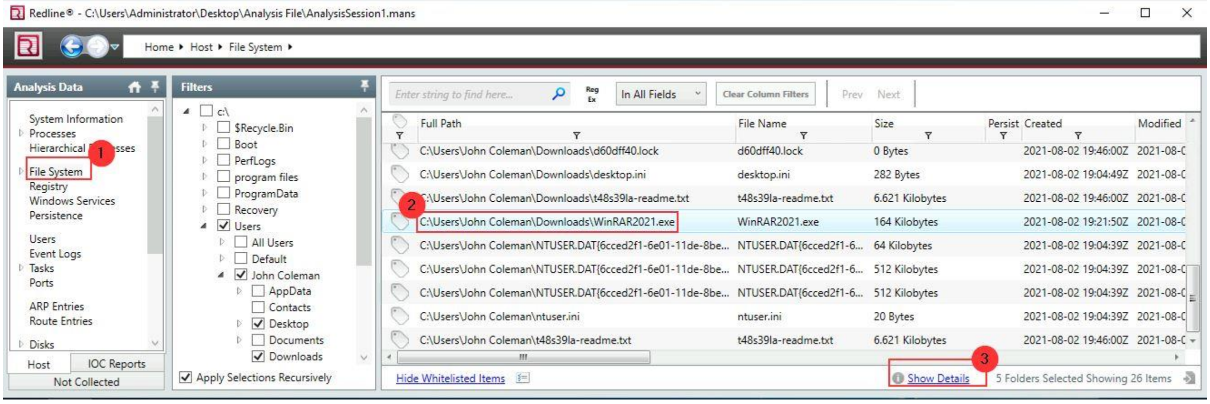


File Download History

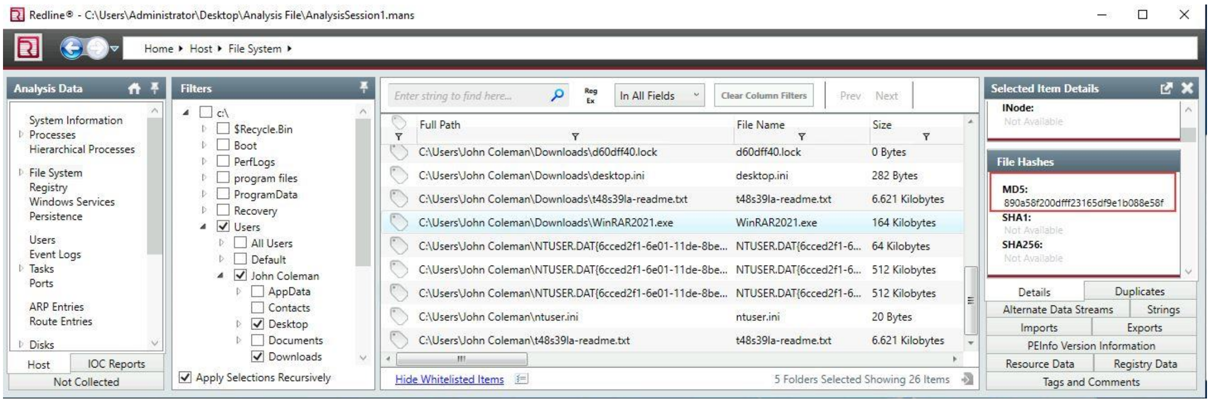
Downloaded files are a common mechanism for attackers to use to gain access to a computer. Users are likely to download files with names of interest (such as "birthday wishes"). Many users are aware that .exe files should not be downloaded and run. However, if a file has a ".txt" or another similar indication of a file type in the filename and the user has file extensions turned off in their Windows Explorer, the user may open the file not realizing that the actual extension is .exe and the file is an executable.

Download Type	Source URL	Target Directory
Auto	http://192.168.75.129:4748/Documents/WinRAR2021.exe	C:\Users\John Coleman\Downloads\WinRAR2021.exe
Auto	https://dist.torproject.org/torbrowser/10.5.2/torbrowser-ins...	C:\Users\John Coleman\AppData\Local\Microsoft\Window

5) Navigate to File System



Full Path	File Name	Size	Persist	Created	Modified
C:\Users\John Coleman\Downloads\d60dff40.lock	d60dff40.lock	0 Bytes		2021-08-02 19:46:00Z	2021-08-C
C:\Users\John Coleman\Downloads\desktop.ini	desktop.ini	282 Bytes		2021-08-02 19:04:49Z	2021-08-C
C:\Users\John Coleman\Downloads\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes		2021-08-02 19:46:00Z	2021-08-C
C:\Users\John Coleman\Downloads\WinRAR2021.exe	WinRAR2021.exe	164 Kilobytes		2021-08-02 19:21:50Z	2021-08-C
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	64 Kilobytes		2021-08-02 19:04:39Z	2021-08-C
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	512 Kilobytes		2021-08-02 19:04:39Z	2021-08-C
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	512 Kilobytes		2021-08-02 19:04:39Z	2021-08-C
C:\Users\John Coleman\ntuser.ini	ntuser.ini	20 Bytes		2021-08-02 19:04:39Z	2021-08-C
C:\Users\John Coleman\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes		2021-08-02 19:46:00Z	2021-08-C

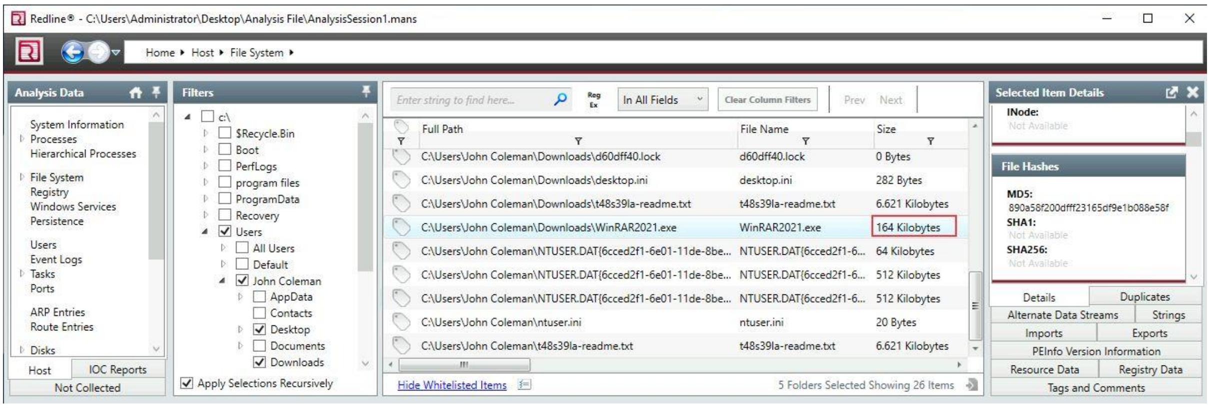


Full Path	File Name	Size
C:\Users\John Coleman\Downloads\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Downloads\desktop.ini	desktop.ini	282 Bytes
C:\Users\John Coleman\Downloads\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes
C:\Users\John Coleman\Downloads\WinRAR2021.exe	WinRAR2021.exe	164 Kilobytes
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	64 Kilobytes
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	512 Kilobytes
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	512 Kilobytes
C:\Users\John Coleman\ntuser.ini	ntuser.ini	20 Bytes
C:\Users\John Coleman\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes

INode: Not Available

MD5: 890a58f200dfff23165df9e1b088e58f
SHA1: Not Available
SHA256: Not Available

6) Navigate to File System

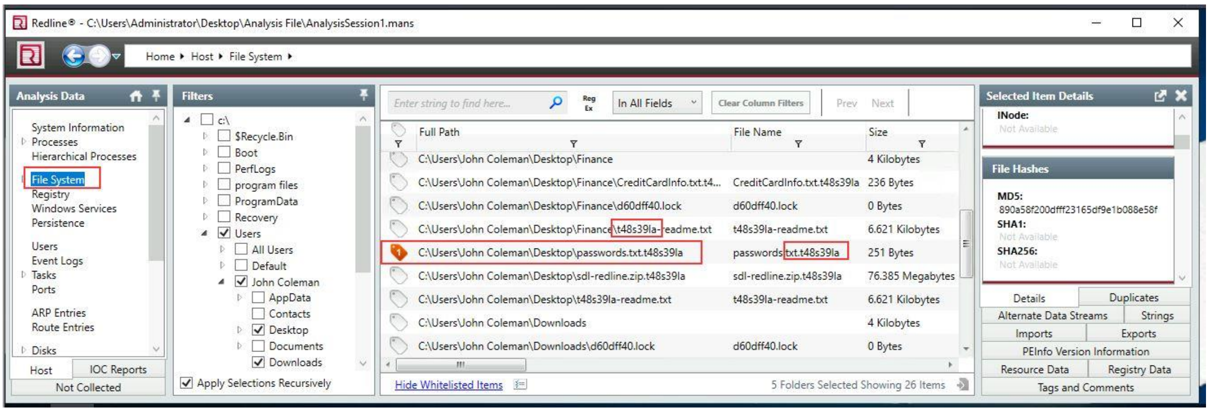


Full Path	File Name	Size
C:\Users\John Coleman\Downloads\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Downloads\desktop.ini	desktop.ini	282 Bytes
C:\Users\John Coleman\Downloads\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes
C:\Users\John Coleman\Downloads\WinRAR2021.exe	WinRAR2021.exe	164 Kilobytes
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	64 Kilobytes
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	512 Kilobytes
C:\Users\John Coleman\NTUSER.DAT{6cced2f1-6e01-11de-8be...	NTUSER.DAT{6cced2f1-6...	512 Kilobytes
C:\Users\John Coleman\ntuser.ini	ntuser.ini	20 Bytes
C:\Users\John Coleman\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes

INode: Not Available

MD5: 890a58f200dfff23165df9e1b088e58f
SHA1: Not Available
SHA256: Not Available

7) Navigate to File System



Filters:
- □ c:\
  - □ $Recycle.Bin
  - □ Boot
  - □ PerfLogs
  - □ program files
  - □ ProgramData
  - □ Recovery
  - ☑ Users
    - □ All Users
    - □ Default
    - ☑ John Coleman
      - □ AppData
      - □ Contacts
      - ☑ Desktop
      - □ Documents
      - ☑ Downloads

☑ Apply Selections Recursively

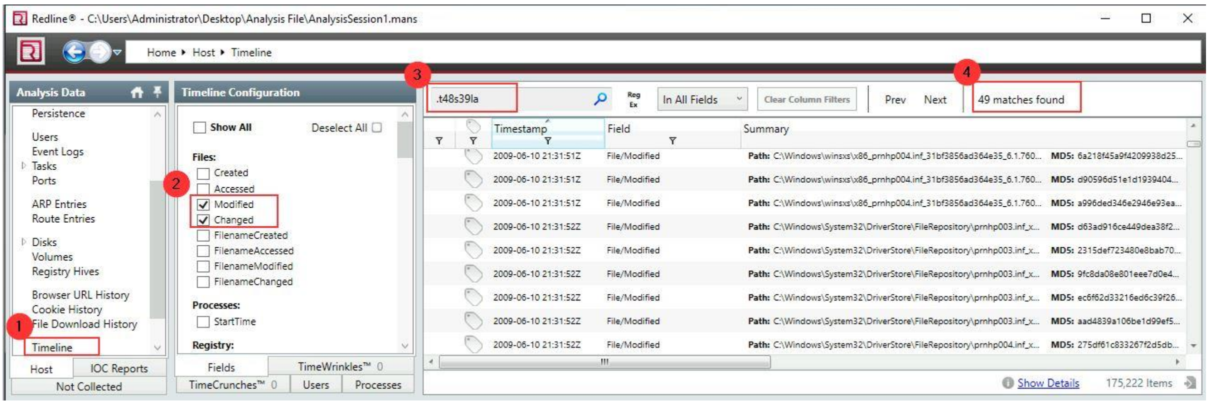
Full Path	File Name	Size
C:\Users\John Coleman\Desktop\Finance		4 Kilobytes
C:\Users\John Coleman\Desktop\Finance\CreditCardInfo.txt.t4...	CreditCardInfo.txt.t48s39la	236 Bytes
C:\Users\John Coleman\Desktop\Finance\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Desktop\Finance\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes
C:\Users\John Coleman\Desktop\passwords.txt.t48s39la	passwords.txt.t48s39la	251 Bytes
C:\Users\John Coleman\Desktop\sdl-redline.zip.t48s39la	sdl-redline.zip.t48s39la	76.385 Megabytes
C:\Users\John Coleman\Desktop\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes
C:\Users\John Coleman\Downloads		4 Kilobytes
C:\Users\John Coleman\Downloads\d60dff40.lock	d60dff40.lock	0 Bytes

Hide Whitelisted Items — 5 Folders Selected Showing 26 Items

INode: Not Available

MD5: 890a58f200dfff23165df9e1b088e58f
SHA1: Not Available
SHA256: Not Available

8) Navigate to TimeLine and select TimeLine Configuration -> File -> modified and changed



Timeline Configuration: □ Show All — Deselect All □

Files:
- □ Created
- □ Accessed
- ☑ Modified
- ☑ Changed
- □ FilenameCreated
- □ FilenameAccessed
- □ FilenameModified
- □ FilenameChanged

Processes:
- □ StartTime

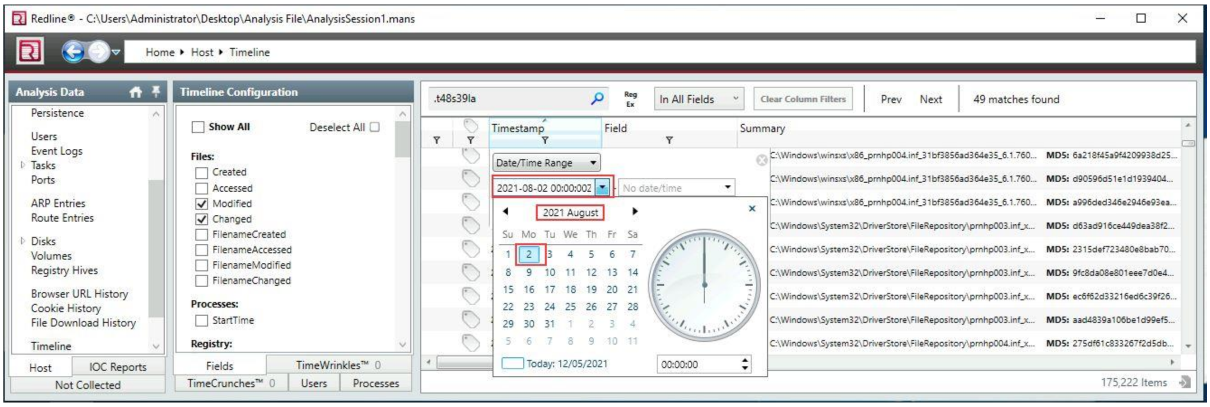
Registry:

Search: .t48s39la — In All Fields — 49 matches found

Timestamp	Field	Summary	
2009-06-10 21:31:51Z	File/Modified	**Path:** C:\Windows\winsxs\x86_prnhp004.inf_31bf3856ad364e35_6.1.760...	**MD5:** 6a218f45a9f4209938d25...
2009-06-10 21:31:51Z	File/Modified	**Path:** C:\Windows\winsxs\x86_prnhp004.inf_31bf3856ad364e35_6.1.760...	**MD5:** d90596d51e1d1939404...
2009-06-10 21:31:51Z	File/Modified	**Path:** C:\Windows\winsxs\x86_prnhp004.inf_31bf3856ad364e35_6.1.760...	**MD5:** a996ded346e2946e93ea...
2009-06-10 21:31:52Z	File/Modified	**Path:** C:\Windows\System32\DriverStore\FileRepository\prnhp003.inf_x...	**MD5:** d63ad916ce449dea38f2...
2009-06-10 21:31:52Z	File/Modified	**Path:** C:\Windows\System32\DriverStore\FileRepository\prnhp003.inf_x...	**MD5:** 2315def723480e8bab70...
2009-06-10 21:31:52Z	File/Modified	**Path:** C:\Windows\System32\DriverStore\FileRepository\prnhp003.inf_x...	**MD5:** 9fc8da08e801eee7d0e4...
2009-06-10 21:31:52Z	File/Modified	**Path:** C:\Windows\System32\DriverStore\FileRepository\prnhp003.inf_x...	**MD5:** ec6f62d33216ed6c39f26...
2009-06-10 21:31:52Z	File/Modified	**Path:** C:\Windows\System32\DriverStore\FileRepository\prnhp003.inf_x...	**MD5:** aad4839a106be1d99ef5...
2009-06-10 21:31:52Z	File/Modified	**Path:** C:\Windows\System32\DriverStore\FileRepository\prnhp004.inf_x...	**MD5:** 275df61c833267f2d5db...

Show Details — 175,222 Items

9) Navigate to Timeline – 2nd August 2021 to 3rd August 2021

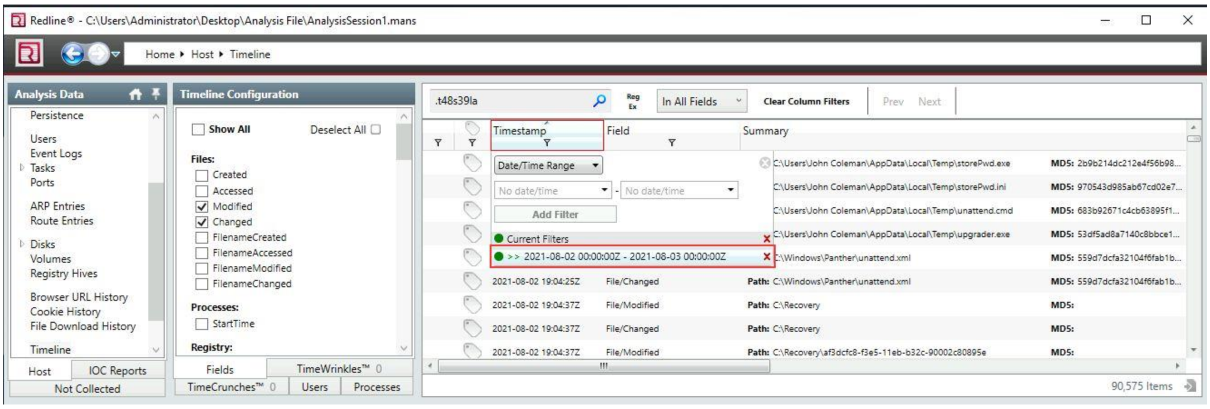


Search: .t48s39la — In All Fields — 49 matches found

Date/Time Range: 2021-08-02 00:00:00Z - No date/time

Su	Mo	Tu	We	Th	Fr	Sa
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31	1	2	3	4
5	6	7	8	9	10	11

175,222 Items



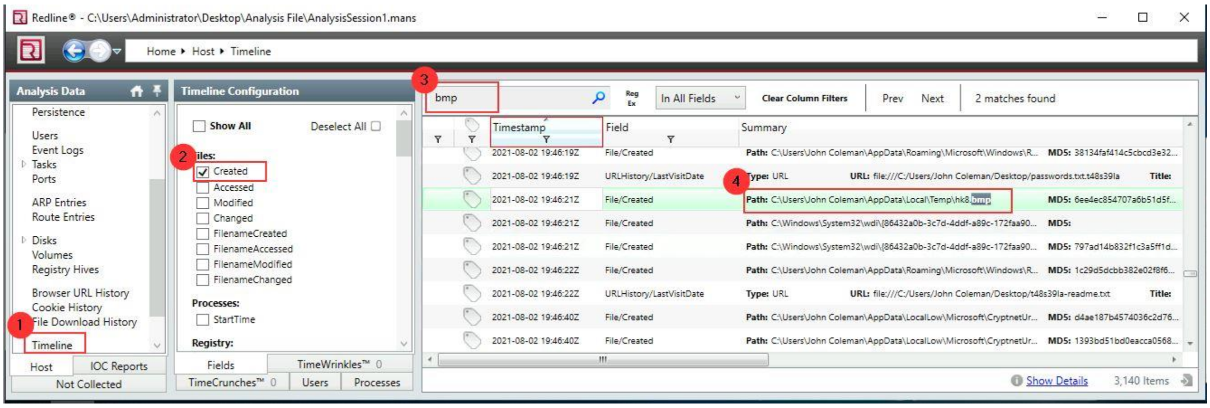
Search: .t48s39la — In All Fields — Clear Column Filters

Current Filters: >> 2021-08-02 00:00:00Z - 2021-08-03 00:00:00Z

Timestamp	Field	Summary	
		C:\Users\John Coleman\AppData\Local\Temp\storePwd.exe	**MD5:** 2b9b214dc212e4f56b98...
		C:\Users\John Coleman\AppData\Local\Temp\storePwd.ini	**MD5:** 970543d985ab67cd02e7...
		C:\Users\John Coleman\AppData\Local\Temp\unattend.cmd	**MD5:** 683b92671c4cb63895f1...
		C:\Users\John Coleman\AppData\Local\Temp\upgrader.exe	**MD5:** 53df5ad8a7140c8bbce1...
		C:\Windows\Panther\unattend.xml	**MD5:** 559d7dcfa32104f6fab1b...
2021-08-02 19:04:25Z	File/Changed	**Path:** C:\Windows\Panther\unattend.xml	**MD5:** 559d7dcfa32104f6fab1b...
2021-08-02 19:04:37Z	File/Modified	**Path:** C:\Recovery	**MD5:**
2021-08-02 19:04:37Z	File/Changed	**Path:** C:\Recovery	**MD5:**
2021-08-02 19:04:37Z	File/Modified	**Path:** C:\Recovery\af3dcfc8-f3e5-11eb-b32c-90002c80895e	**MD5:**

90,575 Items

And select TimeLine Configuration -> File -> created, search for bmp extension



bmp

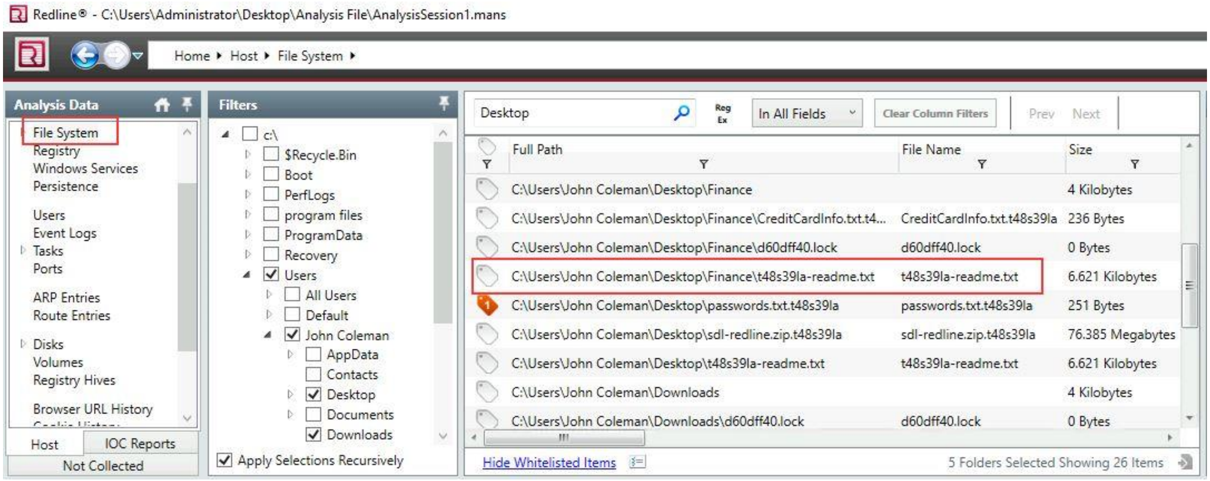
In All Fields

2 matches found

Timestamp	Field	Summary
2021-08-02 19:46:19Z	File/Created	**Path:** C:\Users\John Coleman\AppData\Roaming\Microsoft\Windows\R... **MD5:** 38134faf414c5cbcd3e32...
2021-08-02 19:46:19Z	URLHistory/LastVisitDate	**Type:** URL **URL:** file:///C:/Users/John Coleman/Desktop/passwords.txt.t48s39la **Title:**
2021-08-02 19:46:21Z	File/Created	**Path:** C:\Users\John Coleman\AppData\Local\Temp\hk8.bmp **MD5:** 6ee4ec854707a6b51d5f...
2021-08-02 19:46:21Z	File/Created	**Path:** C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90... **MD5:**
2021-08-02 19:46:21Z	File/Created	**Path:** C:\Windows\System32\wdi\{86432a0b-3c7d-4ddf-a89c-172faa90... **MD5:** 797ad14b832f1c3a5ff1d...
2021-08-02 19:46:22Z	File/Created	**Path:** C:\Users\John Coleman\AppData\Roaming\Microsoft\Windows\R... **MD5:** 1c29d5dcbb382e02f8f6...
2021-08-02 19:46:22Z	URLHistory/LastVisitDate	**Type:** URL **URL:** file:///C:/Users/John Coleman/Desktop/t48s39la-readme.txt **Title:**
2021-08-02 19:46:40Z	File/Created	**Path:** C:\Users\John Coleman\AppData\LocalLow\Microsoft\CryptnetUr... **MD5:** d4ae187b4574036c2d76...
2021-08-02 19:46:40Z	File/Created	**Path:** C:\Users\John Coleman\AppData\LocalLow\Microsoft\CryptnetUr... **MD5:** 1393bd51bd0eacca0568...

3,140 Items

10) Navigate to File System



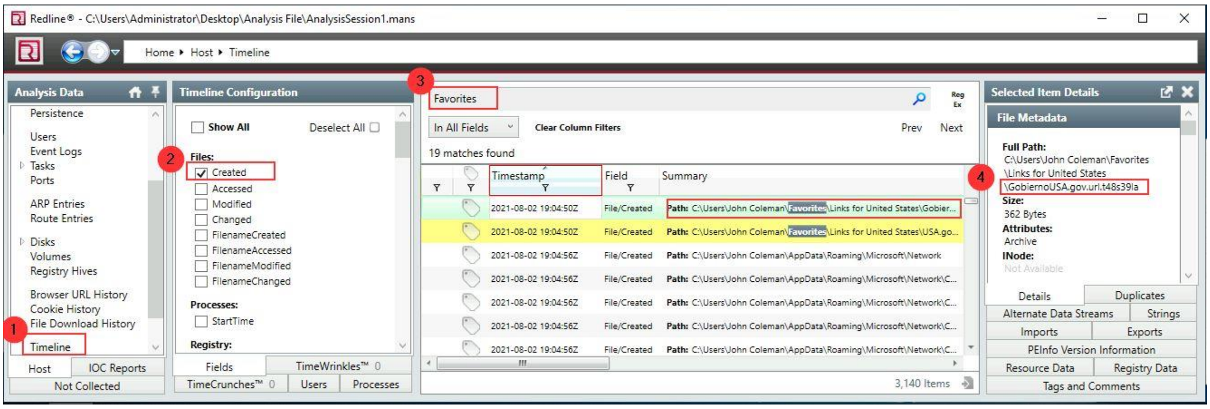
Desktop

In All Fields

Full Path	File Name	Size
C:\Users\John Coleman\Desktop\Finance		4 Kilobytes
C:\Users\John Coleman\Desktop\Finance\CreditCardInfo.txt.t4...	CreditCardInfo.txt.t48s39la	236 Bytes
C:\Users\John Coleman\Desktop\Finance\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Desktop\Finance\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes
C:\Users\John Coleman\Desktop\passwords.txt.t48s39la	passwords.txt.t48s39la	251 Bytes
C:\Users\John Coleman\Desktop\sdl-redline.zip.t48s39la	sdl-redline.zip.t48s39la	76.385 Megabytes
C:\Users\John Coleman\Desktop\t48s39la-readme.txt	t48s39la-readme.txt	6.621 Kilobytes
C:\Users\John Coleman\Downloads		4 Kilobytes
C:\Users\John Coleman\Downloads\d60dff40.lock	d60dff40.lock	0 Bytes

5 Folders Selected Showing 26 Items

11) Navigate to Timeline and select TimeLine Configuration -> File -> created, search for Favorites



Favorites

In All Fields

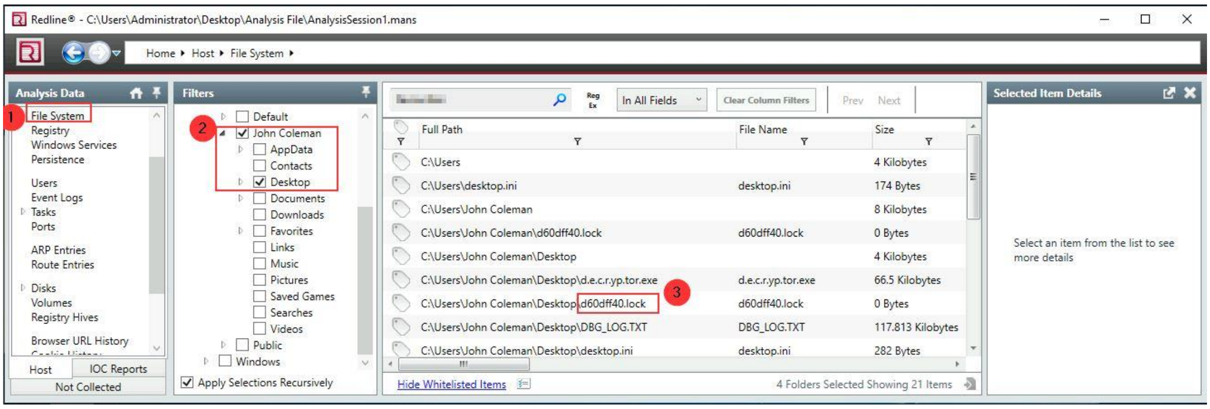
19 matches found

Timestamp	Field	Summary
2021-08-02 19:04:50Z	File/Created	**Path:** C:\Users\John Coleman\Favorites\Links for United States\Gobier...
2021-08-02 19:04:50Z	File/Created	**Path:** C:\Users\John Coleman\Favorites\Links for United States\USA.go...
2021-08-02 19:04:56Z	File/Created	**Path:** C:\Users\John Coleman\AppData\Roaming\Microsoft\Network
2021-08-02 19:04:56Z	File/Created	**Path:** C:\Users\John Coleman\AppData\Roaming\Microsoft\Network\C...
2021-08-02 19:04:56Z	File/Created	**Path:** C:\Users\John Coleman\AppData\Roaming\Microsoft\Network\C...
2021-08-02 19:04:56Z	File/Created	**Path:** C:\Users\John Coleman\AppData\Roaming\Microsoft\Network\C...
2021-08-02 19:04:56Z	File/Created	**Path:** C:\Users\John Coleman\AppData\Roaming\Microsoft\Network\C...

3,140 Items

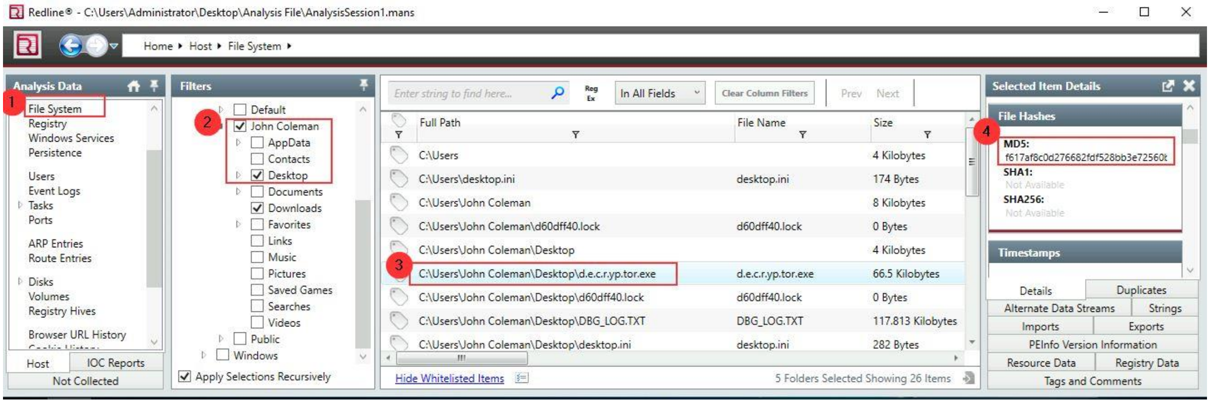
Full Path:
C:\Users\John Coleman\Favorites
\Links for United States
\GobiernoUSA.gov.url.t48s39la
Size:
362 Bytes
Attributes:
Archive
INode:
Not Available

12) Navigate to File System, select users -> john coleman -> Desktop



Full Path	File Name	Size
C:\Users		4 Kilobytes
C:\Users\desktop.ini	desktop.ini	174 Bytes
C:\Users\John Coleman		8 Kilobytes
C:\Users\John Coleman\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Desktop		4 Kilobytes
C:\Users\John Coleman\Desktop\d.e.c.r.yp.tor.exe	d.e.c.r.yp.tor.exe	66.5 Kilobytes
C:\Users\John Coleman\Desktop\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Desktop\DBG_LOG.TXT	DBG_LOG.TXT	117.813 Kilobytes
C:\Users\John Coleman\Desktop\desktop.ini	desktop.ini	282 Bytes

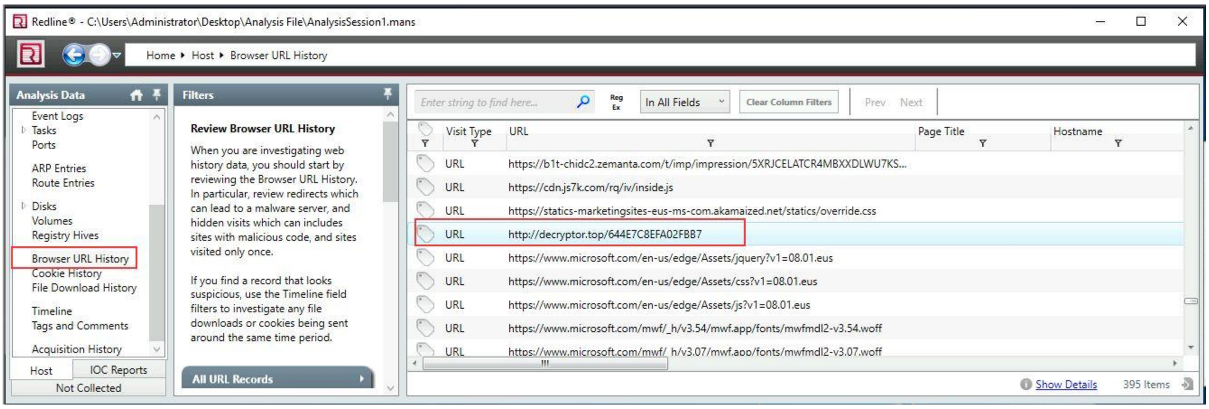
13) Navigate to File System and select john coleman -> d.e.c.r.y.p.tor.exe to look for MD5 hash



Full Path	File Name	Size
C:\Users		4 Kilobytes
C:\Users\desktop.ini	desktop.ini	174 Bytes
C:\Users\John Coleman		8 Kilobytes
C:\Users\John Coleman\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Desktop		4 Kilobytes
C:\Users\John Coleman\Desktop\d.e.c.r.yp.tor.exe	d.e.c.r.yp.tor.exe	66.5 Kilobytes
C:\Users\John Coleman\Desktop\d60dff40.lock	d60dff40.lock	0 Bytes
C:\Users\John Coleman\Desktop\DBG_LOG.TXT	DBG_LOG.TXT	117.813 Kilobytes
C:\Users\John Coleman\Desktop\desktop.ini	desktop.ini	282 Bytes

MD5:
f617af8c0d276682fdf528bb3e72560t
SHA1:
Not Available
SHA256:
Not Available

14) Navigate to Browser URL History and look decryptor in url



Review Browser URL History

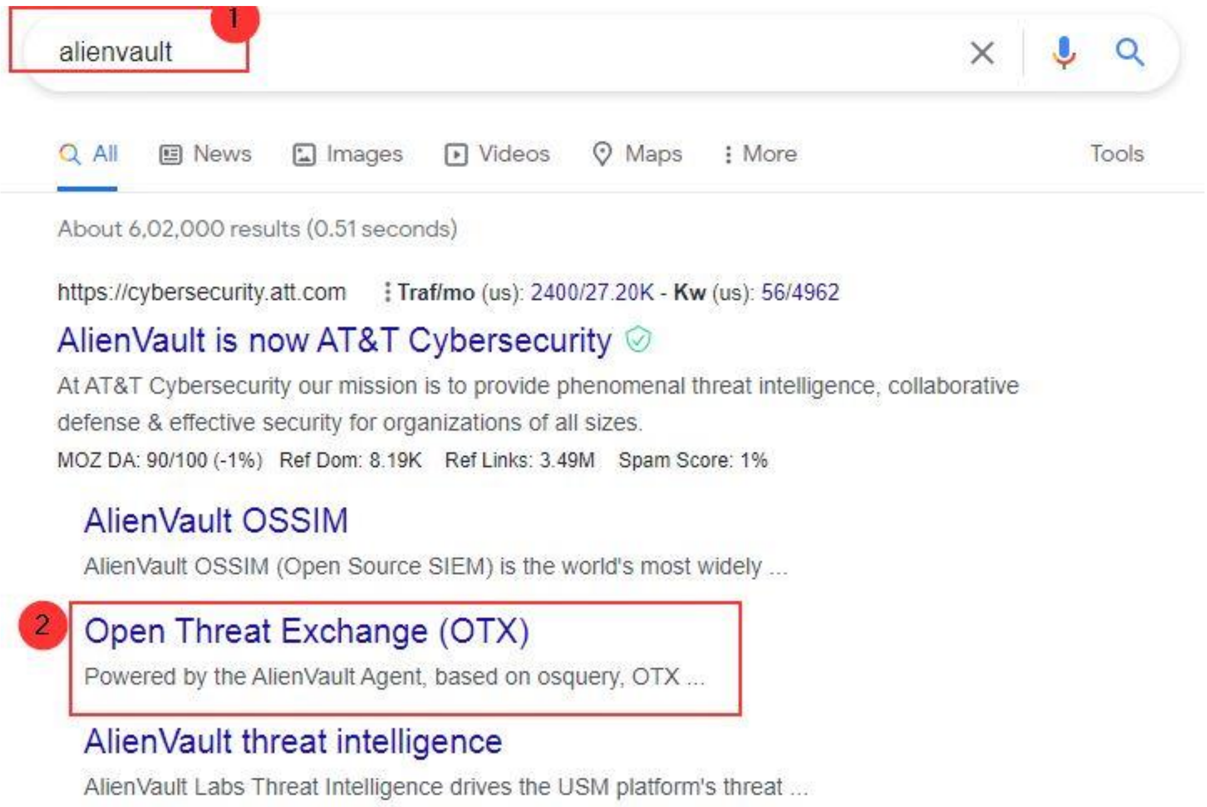
When you are investigating web history data, you should start by reviewing the Browser URL History. In particular, review redirects which can lead to a malware server, and hidden visits which can includes sites with malicious code, and sites visited only once.

If you find a record that looks suspicious, use the Timeline field filters to investigate any file downloads or cookies being sent around the same time period.

Visit Type	URL	Page Title	Hostname
URL	https://b1t-chidc2.zemanta.com/t/imp/impression/5XRJCELATCR4MBXXDLWU7KS...		
URL	https://cdn.js7k.com/rq/iv/inside.js		
URL	https://statics-marketingsites-eus-ms-com.akamaized.net/statics/override.css		
URL	http://decryptor.top/644E7C8EFA02FBB7		
URL	https://www.microsoft.com/en-us/edge/Assets/jquery?v1=08.01.eus		
URL	https://www.microsoft.com/en-us/edge/Assets/css?v1=08.01.eus		
URL	https://www.microsoft.com/en-us/edge/Assets/js?v1=08.01.eus		
URL	https://www.microsoft.com/mwf/_h/v3.54/mwf.app/fonts/mwfmdl2-v3.54.woff		
URL	https://www.microsoft.com/mwf/_h/v3.07/mwf.app/fonts/mwfmdl2-v3.07.woff		

15) Copy this malware hash – 890a58200dfff23165df9e1b088e58f and check in https://cybersecurity.att.com/open-threat-exchange

To look for related tags for this malware



About 6,02,000 results (0.51 seconds)

https://cybersecurity.att.com ⋮ Traf/mo (us): 2400/27.20K - Kw (us): 56/4962

AlienVault is now AT&T Cybersecurity

At AT&T Cybersecurity our mission is to provide phenomenal threat intelligence, collaborative defense & effective security for organizations of all sizes.

MOZ DA: 90/100 (-1%) Ref Dom: 8.19K Ref Links: 3.49M Spam Score: 1%

AlienVault OSSIM

AlienVault OSSIM (Open Source SIEM) is the world's most widely ...

Open Threat Exchange (OTX)

Powered by the AlienVault Agent, based on osquery, OTX ...

AlienVault threat intelligence

AlienVault Labs Threat Intelligence drives the USM platform's threat ...

That is all for this Write-up, hoping this will help you in solving the challenges of REvil Corp. Have Fun and Enjoy Hacking!

Do visit other rooms and modules on TryHackMe for more learning.

-by Shefali Kumai