TryHackMe: REvil Corp

Recently, I completed a TryHackMe room called REvil Corp. It is an intermediate level room that involves analysing a memory dump using Redline. The room being rated as medium difficulty is likely a bit of a stretch, if you have completed the redline room on TryHackMe, this challenge is super easy. Those who enjoy challenges involving memory analysis with tools like Volatility should also find this room quite enjoyable. For my first challenge with redline, I am happy with how it went.

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.

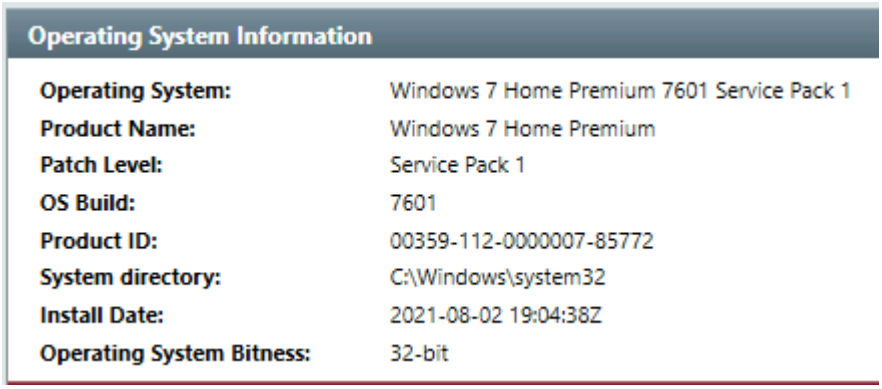
What is the compromised employee's full name?

Once Redline has processed the analysis file, you can navigate to the System Information tab to find the compromised username:

Answer: John Coleman

What is the operating system of the compromised host?

The Operating System info can also be found in the System Information tab:

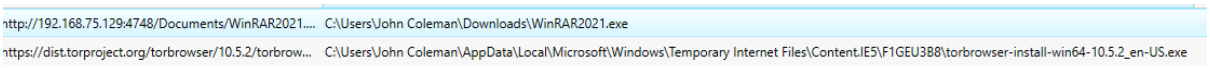


Operating System Information	
Operating System:	Windows 7 Home Premium 7601 Service Pack 1
Product Name:	Windows 7 Home Premium
Patch Level:	Service Pack 1
OS Build:	7601
Product ID:	00359-112-0000007-85772
System directory:	C:\Windows\system32
Install Date:	2021-08-02 19:04:38Z
Operating System Bitness:	32-bit

Answer: Windows 7 Home Premium 7601 Service Pack 1

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

If you look at the File Download History, you can see that two files have been downloaded:



ttp://192.168.75.129:4748/Documents/WinRAR2021....	C:\Users\John Coleman\Downloads\WinRAR2021.exe
ttps://dist.torproject.org/torbrowser/10.5.2/torbrow...	C:\Users\John Coleman\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\F1GEU3B8\torbrowser-install-win64-10.5.2_en-US.exe

The Tor Browser download appears to be legitimate, however, WinRAR2021.exe looks very suspicious.

Answer: WinRAR2021.exe

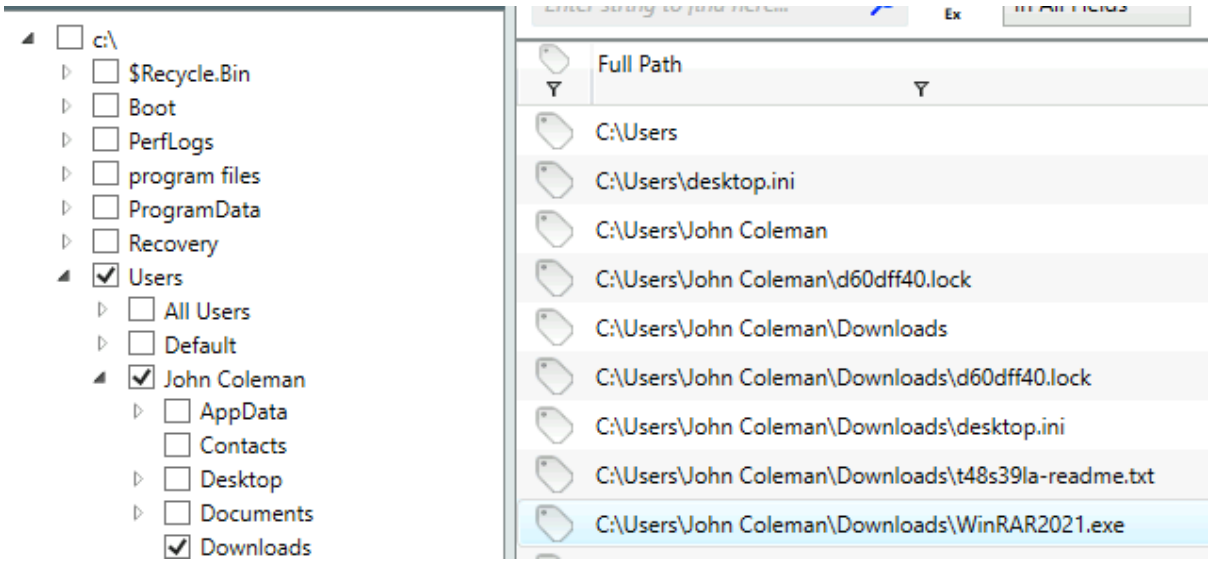
What is the full URL that the user visited to download the malicious binary? (include the binary as well)

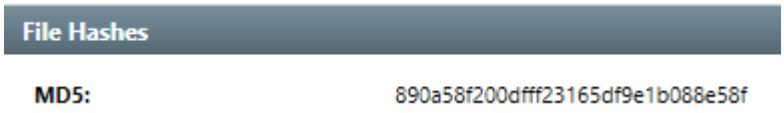
The URL can be seen in the File Download History in the second column.

Answer: http://192.168.75.129:4748/Documents/WinRAR2021.exe

What is the MD5 hash of the binary?

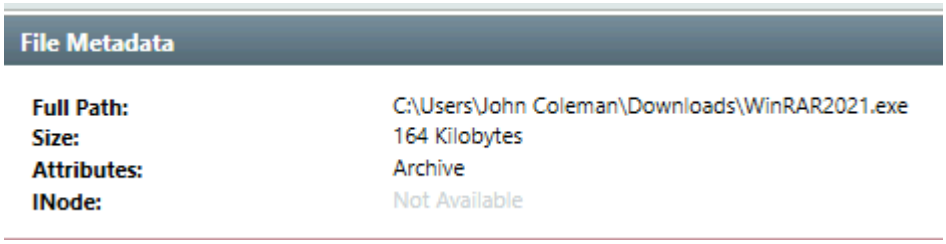
Redline has a nice File System feature that collects a lot of information about a file, including its MD5 hash. If you navigate to the installation directory, which in this case is the Downloads folder, and double click the binary, we can see a plethora of information about the given file:





Answer: 890a58f200dfff23165df9e1b088e58f

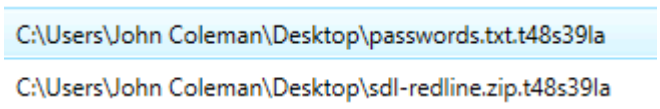
What is the size of the binary in kilobytes?



Answer: 164

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

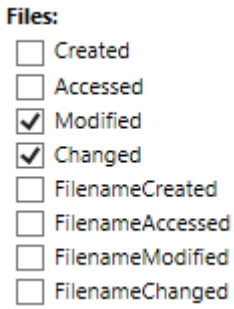
Based on the question, we are likely dealing with some sort of ransomware. If you look at the File System again, we can see that a lot of the files have the file extension .t48s39la:



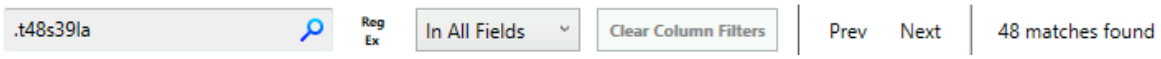
Answer: .t48s39la

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

To answer this question, we can use the timeline and select the Modified and Changed checkboxes under the Files option:



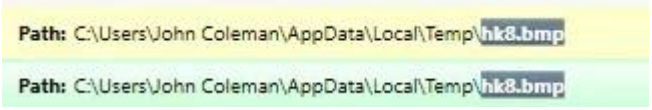
Make sure to check the Deselect All checkbox prior to selecting the Modified and Changed options. We can now search for the file extension and look at the number of matches found:



Answer: 48

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

Staying in the Timeline tab, you can filter for the .bmp file extension to find the path to the wallpaper that got changed by the attacker:



Answer: C:\Users\John Coleman\AppData\Local\Temp\hk8.bmp

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

Fortunately for us, there are not many documents found on the Desktop, making it easy to find the note:

Answer: 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.

If you navigate to this directory using the File System, you can find the following:

Full Path	File Name
C:\Users\John Coleman\Favorites	
C:\Users\John Coleman\Favorites\d60dff40.lock	d60dff40.lock
C:\Users\John Coleman\Favorites\desktop.ini	desktop.ini
C:\Users\John Coleman\Favorites\Links for United States	
C:\Users\John Coleman\Favorites\Links for United States\d60dff40.lock	d60dff40.lock
C:\Users\John Coleman\Favorites\Links for United States\desktop.ini	desktop.ini
C:\Users\John Coleman\Favorites\Links for United States\GobiernoUSA.gov.url.t48s39la	GobiernoUSA.gov.url.t48s39la
C:\Users\John Coleman\Favorites\Links for United States\t48s39la-readme.txt	t48s39la-readme.txt
C:\Users\John Coleman\Favorites\Links for United States\USA.gov.url.t48s39la	USA.gov.url.t48s39la
C:\Users\John Coleman\Favorites\t48s39la-readme.txt	t48s39la-readme.txt

Answer: 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.

File Name	Size
	4 Kilobytes
d.e.c.r.yp.tor.exe	66.5 Kilobytes
d60dff40.lock	0 Bytes

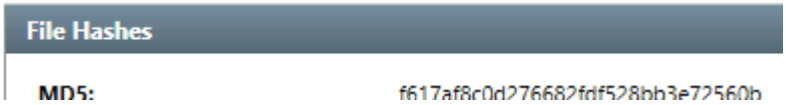
Answer: d60dff40.lock

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

The decryptor can be found in John Colemans desktop directory:

d.e.c.r.yp.tor.exe

Double click the file to view its details:



Answer: 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.

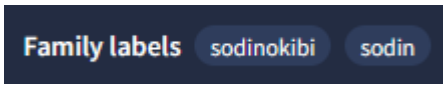
After taking a look at the Browser URL History, we can see a very suspicious link that was visited:

URL	http://decryptor.top/644E7C8EFA02FBB7
URL	http://decryptor.top/644E7C8EFA02FBB7

Answer: http://decryptor.top/644E7C8EFA02FBB7

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

This requires some external research, which we can initiate using the MD5 hash of the malware:



Starting with VirusTotal, we can see that this binary is associated with Sodinokibi and Sodin. Looking through the detection results, we can also see that it is detected as Revil.

Answer: REvil,Sodin,Sodinokibi