### **REvil Corp — TryHackMe**

**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.

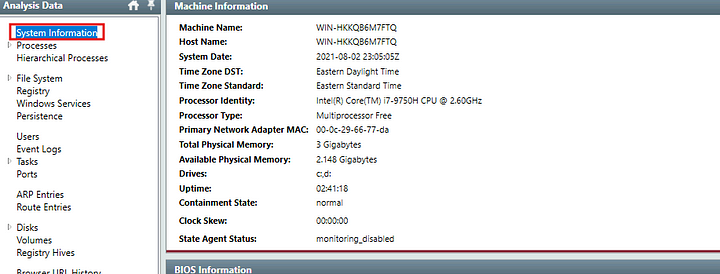
**You** are the incident responder. Let’s see if you can solve this challenge using the infamous Redline tool. Happy Hunting, my friend!

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

TASKS

1. **What is the compromised employee’s full name?**

Open the analysis file in Redline and go to System Information.

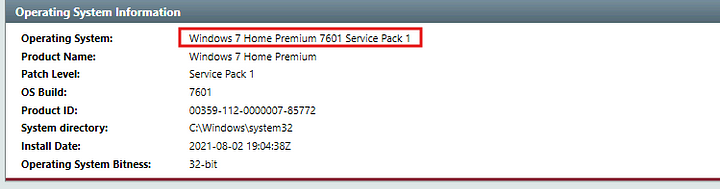


To find the User name, we can head to the bottom of this page to User Information tab.



**Answer:** John Coleman

**2. What is the operating system of the compromised host?**

****

**Answer:** Windows 7 Home Premium 7601 Service Pack 1

**3. What is the name of the malicious executable that the user opened?**

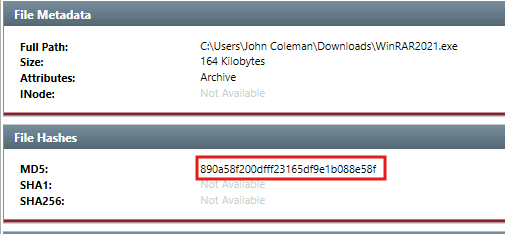
In the File download history, there a re two files. But one of these files was downloaded using an internal IP address.



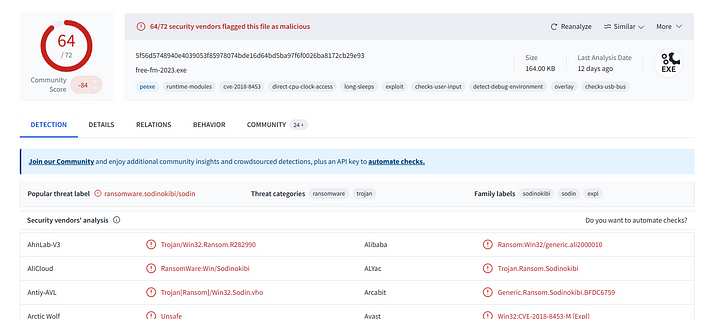
Then search this file in the file system.



We can double click on this record to find out its hash.



Now that we have the hash of the file, we can leverage Threat intelligence to find out if this is malicious. Submit the hash to VirusTotal.



It is indeed malicious.

**Answer:** WinRAR2021.exe

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

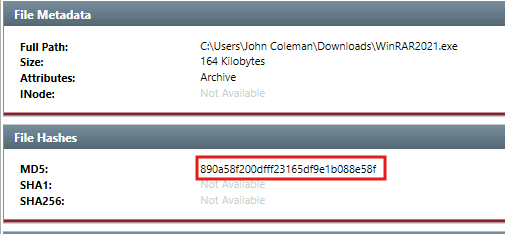
We saw this in the downloads section.



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

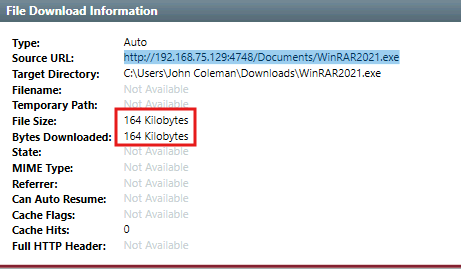
**4. What is the MD5 hash of the binary?**

We already obtained this in the previous question.



**Answer:** 890a58f200dfff23165df9e1b088e58f

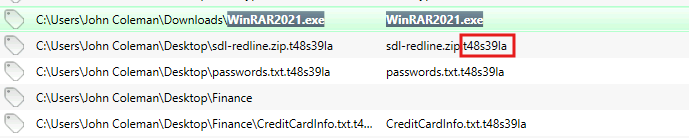
**5. What is the size of the binary in kilobytes?**

****

**Answer:** 164

**6. What is the extension to which the user’s files got renamed?**

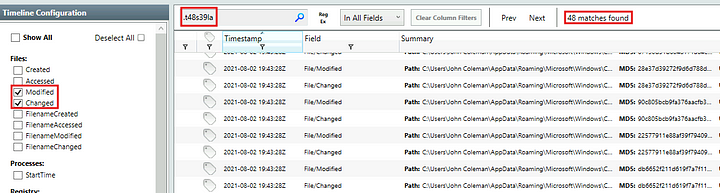
In the file system , If we search for the malicious file and then sort the files on creation time, we can see that all the files have the same extension.



**Answer:** .t48s39la

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

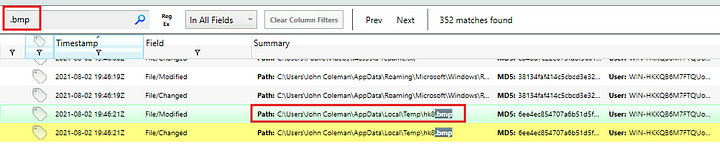
Go to Timeline, then select Modified and changes options. Now select for the extension.



Answer: 48

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

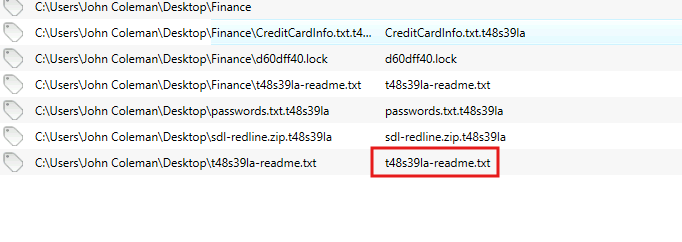
As per the hint, we need to search for bmp file extension in the Timeline section.



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

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

In the file system under the Desktop folder, there is a readme file.



**Answer:** t48s39la-readme.txt

**10. 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.**

****

**Answer:** GobiernoUSA.gov.url.t48s39la

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

****

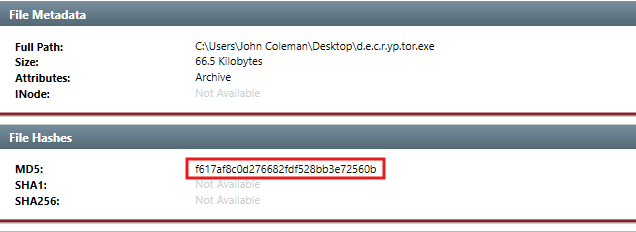
Answer: d60dff40.lock

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

In the user’s desktop folder, there is a file that spells decryptor.



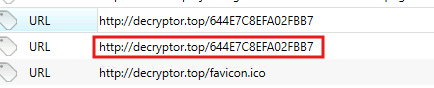
Double click on this to open further details.



**Answer:** f617af8c0d276682fdf528bb3e72560b

**13. 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.**

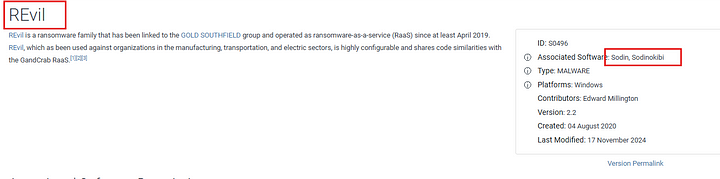
I searched for the word decrypt in the browser URL history tab and found the link.



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

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

Mitre’s ATT&CK has this listed and contains other names in it.



**Answer:** Revil,Sodin,Sodinokibi

This is the end of the walkthorugh.