William Adams
4/2/2024
Lab03- Hunting in memory
IS-3523

In the last lab of this course, we are using SimSpace as we did in the previous labs to analyze the memory file that was provided and check for malicious activity within it. During my analysis of the memory file, I will be using memory forensics techniques to be able to identify any suspicious activity within the file. The lab pdf file discusses how we will be using the application Volatility during the lab to help us identify if there was any unauthorized access or malicious activity within the file. I have never used or have any real experience with the application Volatility, but with the research I have done on the application, I am confident I can navigate through the application. This last lab in this course will help me gain some more knowledge within the landscape of cyber and it will give me some more experience with doing investigations on incidents.

In this lab, both the win-hunt and the kali-hunt are available for use, both having the application Volatility which is nice that there are a lot of VMs that are available for use during this lab. I decided to use the first win-hunt machine that I saw and was ready to start my lab and analyze the file. The lab PDF mentions that the “KobayashiMaru.vmem” file is located in the shared files folder and after looking, it was in there. After finding the file I was now looking at how to start to analyze this file with the application Volatility. As I previously mentioned earlier in this paper, I have never had experience with this application, the professor gave us a cheat for commands for Volatility so this will be very helpful with the investigation process. I opened up the command line prompt on the machine and decided to run the command “volatility.exe -f KobayashiMaru.vmem pslist” so that I could see what running processes there are on the file. After running this command, there was a lot of different information to analyze to see if anything abnormal was on the files running processes. After doing some research on the names that have popped up on the output, I have found some alerts that can cause some concern about malicious activity happening on the file. There was a total of 5 names that popped out to me as a concern for malicious activity that may be occurring (cryptocat.exe, hxdef100.exe, isasses.exe, bircd.exe, and poisonivy.exe). All of these files raised some red flags for me when doing some further research on them.

Starting with the file “crptrcat.exe”, I don’t believe that I have seen this file before but after doing some searches on the file I realized that this could be potentially malicious. “Cryptcat” is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol while encrypting the data being transmitted.” (Kali 2024) Being able to encrypt data may not be a major red flag but malicious hackers can abuse this technique, especially over a network. “CRYPTCAT's ransom-demanding message informs victims that their files have been encrypted. It warns against using third-party decryption tools as that will result in permanent data loss. Victims are instructed to contact the attackers and send them a single file to test decryption. Afterwards, they will receive payment instructions for the decryption key.” (Meskauskas) After reading this information from this article, an alarm was set off in my head. Malicious hackers could have used this .exe to encrypt the data and use it as ransomware, I would later look out for any other signs of a ransomware attack.

After exploring how “crptcat” can potentially be a malicious application that was used in this potential attack. The next file that I found to be potentially malicious was a file named “hxdef100.exe”, I had never heard of this potentially malicious file so I had to do some research on it so I could make my opinion on it. “Hacker Defender (hxdef) is a user-mode rootkit written in Delphi. The rootkit can hide files, processes, system services, system drivers, registry keys and values, open ports, cheat with free disk space. Program also masks its changes in memory and hides handles of hidden processes. Program installs hidden backdoors, register as hidden system service, and installs hidden system driver." (Hacker 2014) Hacker Defender (hxdef) exhibits characteristics commonly associated with malicious software, including evasion of detection, establishment of persistence, unauthorized access provision, and system resource manipulation, which is very alarming that this file was present when analyzing the output.

The last file that I found to be potentially malicious when I ran the command was "poison.ivy". I actually do remember this file from the previous lab that we had to do with the Daniel Faraday user that we had to analyze. I remember during the last lab when I saw the name poison ivy, I first thought of something bad because of just the name alone. "A remote administration tool (RAT) that bypasses the security features of a program, computer or network to give unauthorized access or control to its user." (Backdoor) With this finding, it was almost clear to me that something malicious was going on with this file. Poison.ivy has been around for years with putting on malware computers and it has functions that it can employ to its target system.

After finding all of those potential malicious files in the output that was looking into, I decided to look more into to see what operating system was being used. In the cheat sheet that the professor provided us, I saw that "imageinfo" has some information about the source OS that can be valuable to know. I typed the same command as before, but I replaced plist with imageinfo. The output I got was interesting, it gave me two suggested operating systems (WinXPSP2x86 or WinXPS3x86) but then at the end of the line, it says "instantiated with WinXPSP2x86 operating system.

Now that I have found the correct operating system that was being used, I believe I should be able to use "dlllist" to get a deeper idea of what the processes were on the files. I typed in the command "volatility.exe -f KobayashiMaru.vmem –-profile=WinXPSP2x86 dlllist" and after typing the command in I was provided with tons and tons of pages of information. After looking at the output I did notice that the files we had previously talked about did appear (poison.ivey and crptrcat). There wasn't anything else that really caught my eye when trying to analyze the many pages of data that were present. There was only one thing that I saw that was something that could be something new that I haven't discovered yet. When looking down through the output, in the middle of the output I noticed that there was a hidden process that was showing up named "iroffer.exe" which raised some questions. After doing some research on the process it made certain that this was some sort of backdoor. "Iroffer.exe is a process registered as a backdoor vulnerability which may be installed for malicious purposes by an attacker allowing access to your computer from remote locations, stealing passwords, Internet banking, and personal data. This process is a security risk and should be removed from your system. Non-system processes like iroffer.exe originate from software you installed on your system." (Iroffer) With this file being hidden as well, it also leaves room for questions about why it was hidden in the first place.

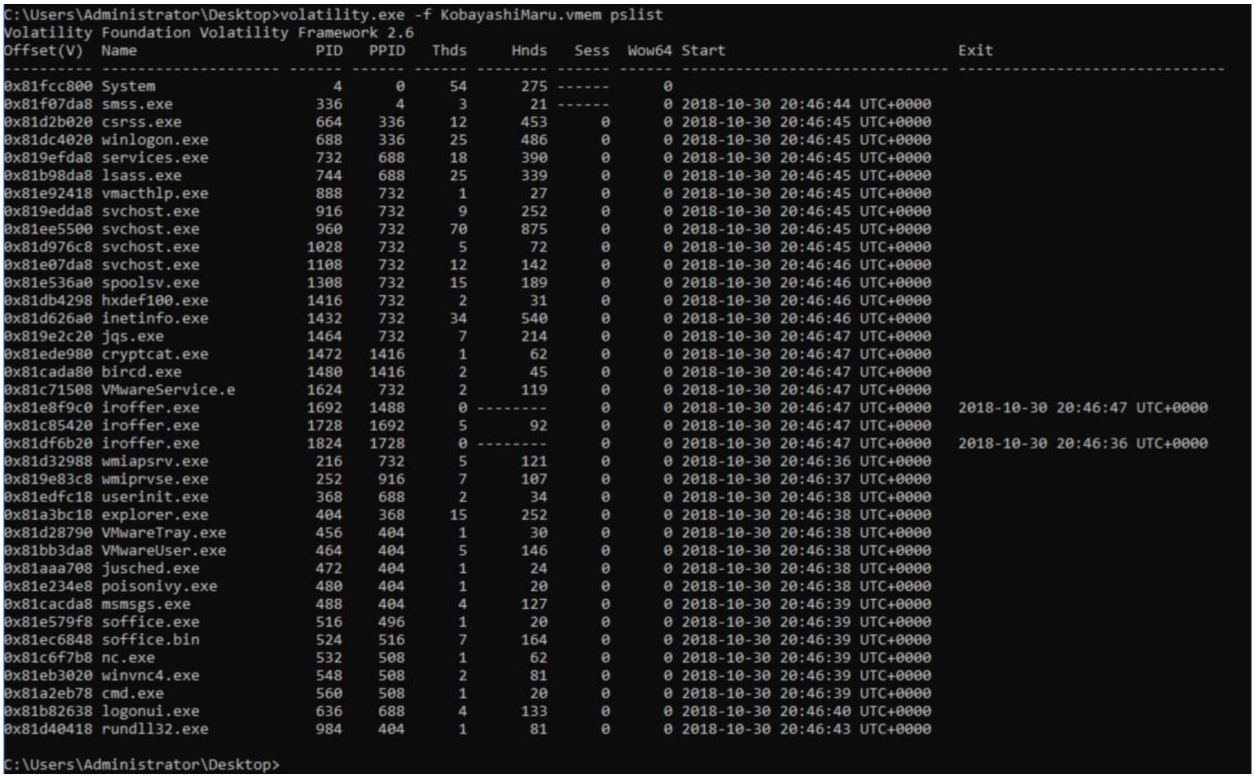
After doing the investigation on the memory file and coming away with some solid evidence of what was going on. I was now looking towards using a forensics tool that I could use to further view the potentially malicious activity that was happening on the file. The desktop of the win machine I was using, had Autopsy on it so I decided to use the application to see if I could find any new data that I hadn't already discovered. I have used this application in previous courses, so I was familiar with the layout of the application and how to navigate it. I decided to upload the memory file onto the application and get started on my investigation. When my memory file was done uploading, I went to the consoles to see if I could find any other information that I hadn't been able to see before. I noticed how "nc.exe" was being used in a process, we have used Netcat in previous labs so I was familiar with what exactly it can do. Netcat itself isn't malicious but if used in a malicious way it can cause some concern for a system. "The ways Netcat can be used for nefarious purposes, such as backdoor access, creating rogue tunnels to get around firewalls, sniff traffic one should not have access to, and for transferring files discreetly to the compromised systems even when one does not have direct connectivity." (Kanclirz 2008) With Netcat being this powerful of a tool, the malicious hackers in this specific case could have used it to gain further access to the systems. The last observation that I made was that this computer also belonged to Daniel Faraday, which I thought was interesting. I didn't notice anything else in the other sections that were different from the Volatility commands that could help me with my investigation.

Questions for the lab

The first question that was asked in this lab was **What operating system is the computer using?** What version? After analyzing the data that I got from Volatility, I can say that the computer was running WinXPSP2x86. The next question that was asked in the lab pdf was **How much RAM is included in the analysis?** For this question, I was a little confused because I don't remember looking at the RAM in this memory file. With the operating system being present, I would believe that the RAM being used is below 4GB because we do know that the operating system is Windows XPSPx86. I didn't find this data from a command or application, but I would be interested to find out. For the next question in the lab **View the running processes. Does this look like your average box? a. What processes look abnormal? What makes them abnormal?** After doing a long and extensive investigation on the memory file this does not look like your "average box" at all, there were a ton of different processes that were found that were alarming for malicious activity. There were processes such as poison.ivy.exe, hxdef100.exe, and crptrcat.exe. After doing my research on these processes they all came back to be malicious all in their ways for a system. None of these processes are files you would want to see on your computer. The next question asks **Can you find user account names? Passwords? If not, why not?** I did find the user was Daniel Faraday while using the application Autopsy, but for the passwords for this specific case, I did not find anything. For the previous lab, I connected myself with the two machines and was able to change the password that way, for this lab, I couldn't find the passwords through Volatility, I thought with me being able to use the command "imageinfo" I would be able to use that the operating system and then be able to use that information to be able to get the hashes for the passwords and then be able to hash them out. I was not able to recover the SAM and SYSTEM. The next question the lab asked is **View the Dynamically Linked Libraries. Does this look like your average box? A. What DLLs look abnormal?** I would say that this does not looked like your average box just based off of how many of the processes were hidden, I mentioned earlier in my lab that iroffer.exe was hidden and that raised some questions for me so I would say that these processes being hidden can make it even more difficult to tell what has happened on a file memory after being attack. The next question the lab ask is **Can you associate any Processes (PIDs), DLLs, and executables?** I would associate say that poisonivy.exe is associated in some way with pid 480. **View the files associated with the processes. a. Do any files or file paths look abnormal? Reference the file path if available.** I would say yes just based off the hidden files that I saw with some of the processes. The last question that the lab asked was **Explain what you think happened to this box. Have you seen anything before?** What I think happened with this specific box was that it got infected with poisonivy.exe and it spread all throughout the computer. If I had to guess to what exactly happened for all of this to happen on a computer, I believe that it could have been a phishing attack where the user clicked on an email and not knowing infected his computer with malware and it began to spread. The next part of the question asks to have I seen anything before, I'm guessing that means have I seen a infected machine like this before, and the answer to that is no. I have never been in this position where I have seen a computer have that much potential malware on its computer.

In conclusion to this lab, I enjoyed being able to learn some new skills with new security tools and thought I did a solid job in seeing what exactly what on with this computer. I wasn't able to recover the passwords for the account, which was frustrating, but I do think I recovered some good data on what went on with this potentially infected machine. I thought that this lab was a great way to test my skills and to get to use security tools in a real-life scenario, being able to identify different types of malwares on a machine was interesting. I have never used Volatility before this lab, but it was honestly very simple to use, and it was an effective way to retrieve data from the memory file. I can confidently say in my analyst that the machine that I did my investigation was infected with multiple types of malwares.

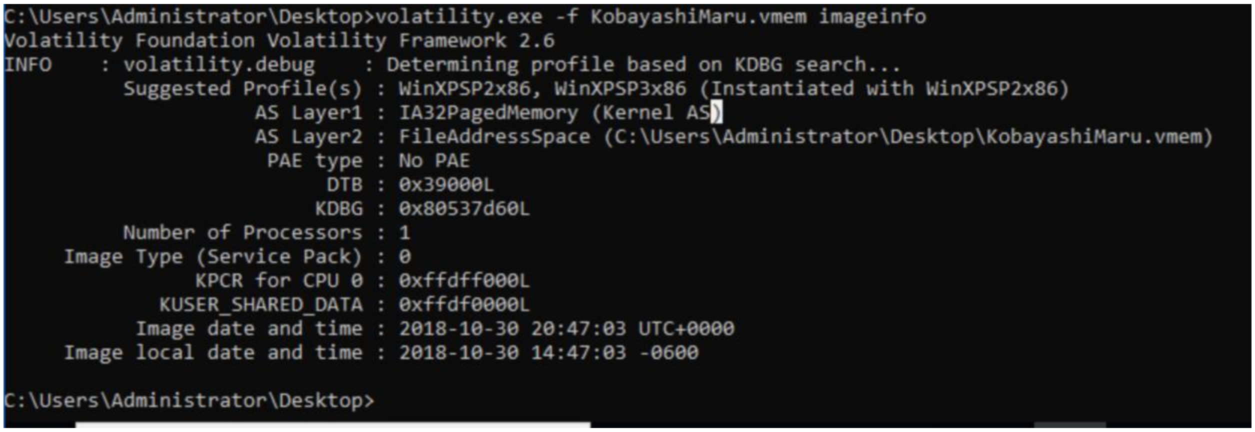
Appendices



```
C:\Users\Administrator\Desktop>volatility.exe -f KobayashiMaru.vmem pslist
Volatility Foundation Volatility Framework 2.6
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x81fcc800 System                    4      0     54      275 ------      0
0x81f07da8 smss.exe                336      4      3       21 ------      0 2018-10-30 20:46:44 UTC+0000
0x81d2b020 csrss.exe               664    336     12      453      0      0 2018-10-30 20:46:45 UTC+0000
0x81dc4020 winlogon.exe            688    336     25      486      0      0 2018-10-30 20:46:45 UTC+0000
0x819efda8 services.exe            732    688     18      390      0      0 2018-10-30 20:46:45 UTC+0000
0x81b98da8 lsass.exe               744    688     25      339      0      0 2018-10-30 20:46:45 UTC+0000
0x81e92418 vmacthlp.exe            888    732      1       27      0      0 2018-10-30 20:46:45 UTC+0000
0x819edda8 svchost.exe             916    732      9      252      0      0 2018-10-30 20:46:45 UTC+0000
0x81ee5500 svchost.exe             960    732     70      875      0      0 2018-10-30 20:46:45 UTC+0000
0x81d976c8 svchost.exe            1028    732      5       72      0      0 2018-10-30 20:46:45 UTC+0000
0x81e07da8 svchost.exe            1108    732     12      142      0      0 2018-10-30 20:46:46 UTC+0000
0x81e536a0 spoolsv.exe            1308    732     15      189      0      0 2018-10-30 20:46:46 UTC+0000
0x81db4298 hxdef100.exe           1416    732      2       31      0      0 2018-10-30 20:46:46 UTC+0000
0x81d626a0 inetinfo.exe           1432    732     34      540      0      0 2018-10-30 20:46:46 UTC+0000
0x819e2c20 jqs.exe                1464    732      7      214      0      0 2018-10-30 20:46:47 UTC+0000
0x81ede980 cryptcat.exe           1472   1416      1       62      0      0 2018-10-30 20:46:47 UTC+0000
0x81cada80 bircd.exe              1480   1416      2       45      0      0 2018-10-30 20:46:47 UTC+0000
0x81c71508 VMwareService.e        1624    732      2      119      0      0 2018-10-30 20:46:47 UTC+0000
0x81e8f9c0 iroffer.exe            1692   1488      0 --------      0      0 2018-10-30 20:46:47 UTC+0000   2018-10-30 20:46:47 UTC+0000
0x81c85420 iroffer.exe            1728   1692      5       92      0      0 2018-10-30 20:46:47 UTC+0000
0x81df6b20 iroffer.exe            1824   1728      0 --------      0      0 2018-10-30 20:46:47 UTC+0000   2018-10-30 20:46:36 UTC+0000
0x81d32988 wmiapsrv.exe            216    732      5      121      0      0 2018-10-30 20:46:36 UTC+0000
0x819e83c8 wmiprvse.exe            252    916      7      107      0      0 2018-10-30 20:46:37 UTC+0000
0x81edfc18 userinit.exe            368    688      2       34      0      0 2018-10-30 20:46:38 UTC+0000
0x81a3bc18 explorer.exe            404    368     15      252      0      0 2018-10-30 20:46:38 UTC+0000
0x81d28790 VMwareTray.exe          456    404      1       30      0      0 2018-10-30 20:46:38 UTC+0000
0x81bb3da8 VMwareUser.exe          464    404      5      146      0      0 2018-10-30 20:46:38 UTC+0000
0x81aaa708 jusched.exe             472    404      1       24      0      0 2018-10-30 20:46:38 UTC+0000
0x81e234e8 poisonivy.exe           480    404      1       20      0      0 2018-10-30 20:46:38 UTC+0000
0x81cacda8 msmsgs.exe              488    404      4      127      0      0 2018-10-30 20:46:39 UTC+0000
0x81e579f8 soffice.exe             516    496      1       20      0      0 2018-10-30 20:46:39 UTC+0000
0x81ec6848 soffice.bin             524    516      7      164      0      0 2018-10-30 20:46:39 UTC+0000
0x81c6f7b8 nc.exe                  532    508      1       62      0      0 2018-10-30 20:46:39 UTC+0000
0x81eb3020 winvnc4.exe             548    508      2       81      0      0 2018-10-30 20:46:39 UTC+0000
0x81a2eb78 cmd.exe                 560    508      1       20      0      0 2018-10-30 20:46:39 UTC+0000
0x81b82638 logonui.exe             636    688      4      133      0      0 2018-10-30 20:46:40 UTC+0000
0x81d40418 rundll32.exe            984    404      1       81      0      0 2018-10-30 20:46:43 UTC+0000

C:\Users\Administrator\Desktop>
```

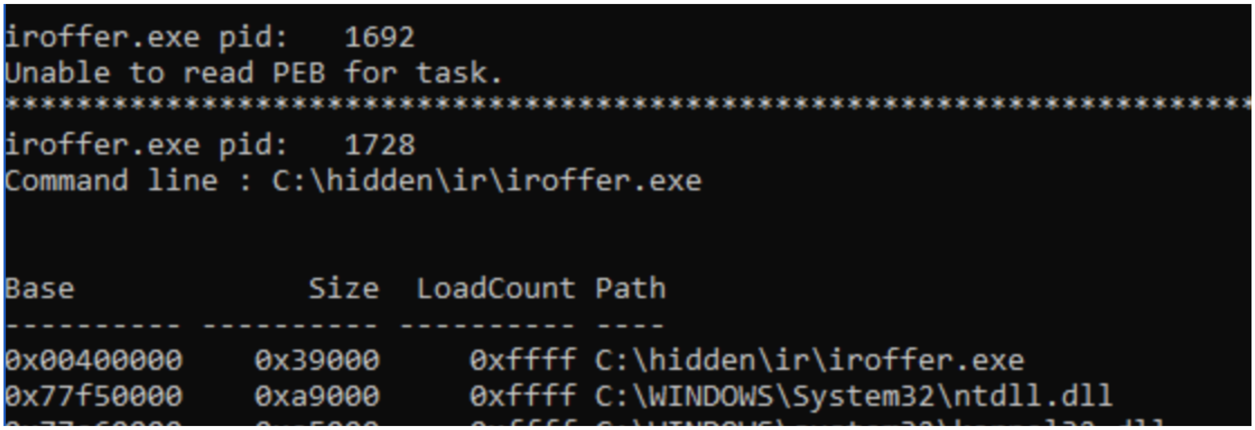
Figure 1In this screenshot, I have shown the application Volatility being run with the command “pslist”.



```
C:\Users\Administrator\Desktop>volatility.exe -f KobayashiMaru.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (C:\Users\Administrator\Desktop\KobayashiMaru.vmem)
                      PAE type : No PAE
                           DTB : 0x39000L
                          KDBG : 0x80537d60L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2018-10-30 20:47:03 UTC+0000
     Image local date and time : 2018-10-30 14:47:03 -0600

C:\Users\Administrator\Desktop>
```

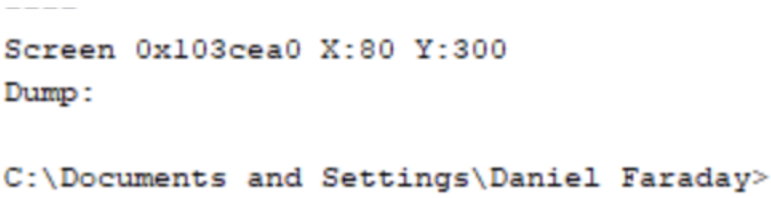
Figure 2In this screenshot I have shown the command being run to see information about the operating system that was being used.



```
iroffer.exe pid:   1692
Unable to read PEB for task.
************************************************************************
iroffer.exe pid:   1728
Command line : C:\hidden\ir\iroffer.exe


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00400000    0x39000     0xffff C:\hidden\ir\iroffer.exe
0x77f50000    0xa9000     0xffff C:\WINDOWS\System32\ntdll.dll
```

Figure 3In this screenshot i have shown the file "iroffer.exe" shown as hidden on the output of the command "volatility.exe -f KobayashiMaru.vmem –-profile=WinXPSP2x86 dlllist.



```
----
Screen 0x103cea0 X:80 Y:300
Dump:

C:\Documents and Settings\Daniel Faraday>
```

Figure 4 In this screenshot I have shown that the user was found as Daniel Faraday.

Citations

Backdoor. (n.d.). *Backdoor:W32/Poisonivy*. Backdoor:W32/PoisonIvy. https://www.f-secure.com/v-descs/backdoor-w32-poisonivy.shtml

Hacker-defender-hxdef. aldeid. (2014). https://www.aldeid.com/wiki/Hacker-Defender-hxdef

Hacker-defender-hxdef. aldeid. (2014). https://www.aldeid.com/wiki/Hacker-Defender-hxdef

Iroffer.exe. What is iroffer.exe? (n.d.). https://www.processlibrary.com/en/directory/files/iroffer/23813/

Kali. (2024, March 11). *Cryptcat: Kali linux tools*. Kali Linux. https://www.kali.org/tools/cryptcat/#:~:text=Cryptcat%20is%20a%20simple%20Unix,by%20other%20programs%20and%20scripts.

Kanclirz, J., & Publisher SummaryJust like the other network tools. (2008, July 5). *The Dark Side of Netcat*. Netcat Power Tools. https://www.sciencedirect.com/science/article/abs/pii/B9781597492577000054#:~:text=Unfortunately%2C%20just%20like%20most%20network,fits%20that%20requirement%20quite%20handily.

Meskauskas, T. (2022, September 6). *CRYPTCAT ransomware*. CRYPTCAT Ransomware - Decryption, removal, and lost files recovery. https://www.pcrisk.com/removal-guides/24737-cryptcat-ransomware