Forensics Cryptowall

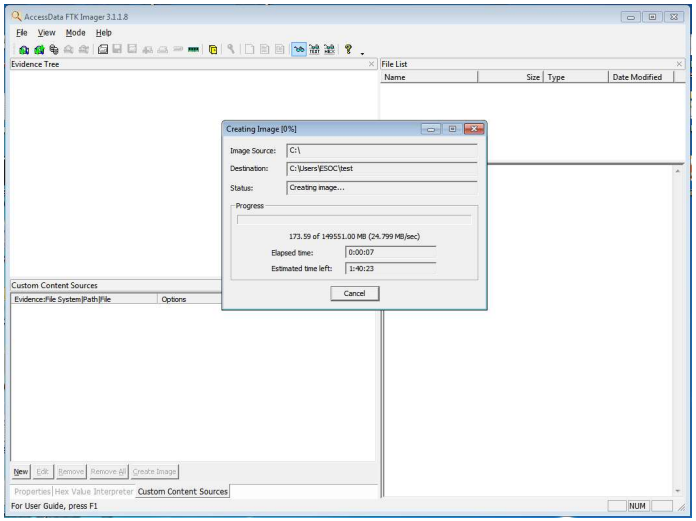
Joe Wu

Overview

- A few months ago, a mortgage specialist found some applications on his workstation were not working, he created a ticket with help desk to solve the problem, then they found out that all the user documents on the disk were encrypted by Cryptowall. The corporate security was contacted, SOC was requested to investigate how the malware infection happened.
- SOC did network traffic analysis and host analysis and did not find anything conclusive. Therefore, we asked the infected user machine be delivered to our forensic lab.
- The goal is to find out the root cause of malware from what is remaining on the infected machine.
- How to do the forensics?

Evidence collection

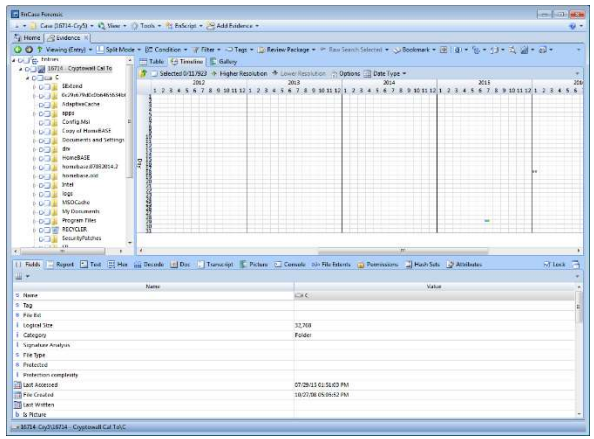
- First, to get a forensic image from the hard disk. Tool used was FTK imager. The output is a .E01 file.



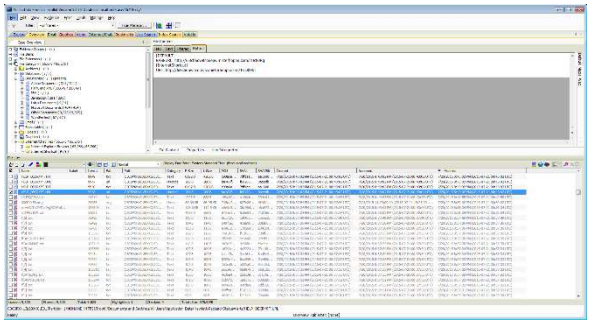
- Then, to collect evidences using forensic software: Encase, FTK, autopsy, and other tools like pasco.

Tools

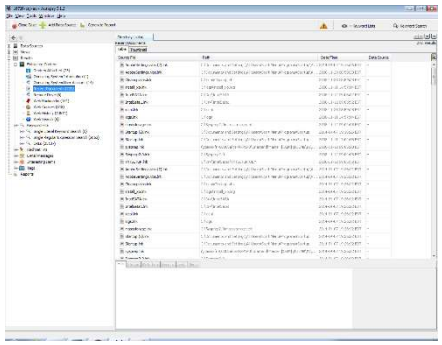
- Encase



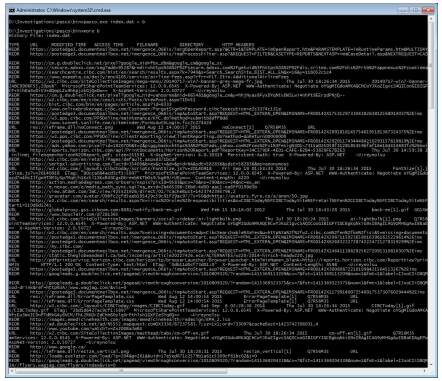
- FTK



- Autopsy

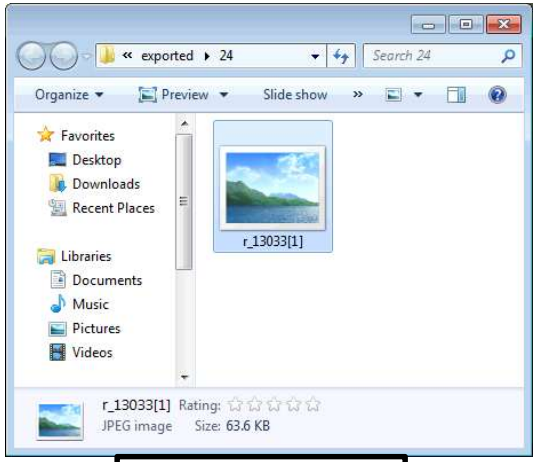


- Pasco

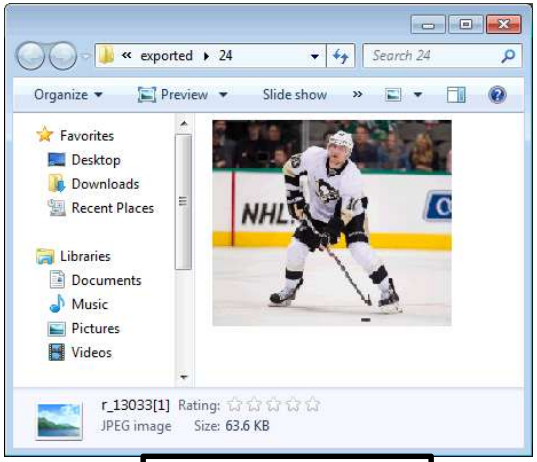


Challenge 1

How to read this?



Before decryption



After decryption

- The first problem is that all user emails, browsing history, windows event logs are encrypted by company encryption software Credant. I have to decrypt to get meaningful info from these files on disk.
- Use Encase and FTK to decrypt.
- "How to Decrypt Credant-encrypted files in Encase Forensic"

KB is available at sharepoint:

https://teams.com/sites/sao/Knowledge%20Base%20Articles/How%20to%20Decrypt%20Credant-encrypted%20files%20in%20Encase%20Forensic.pptx

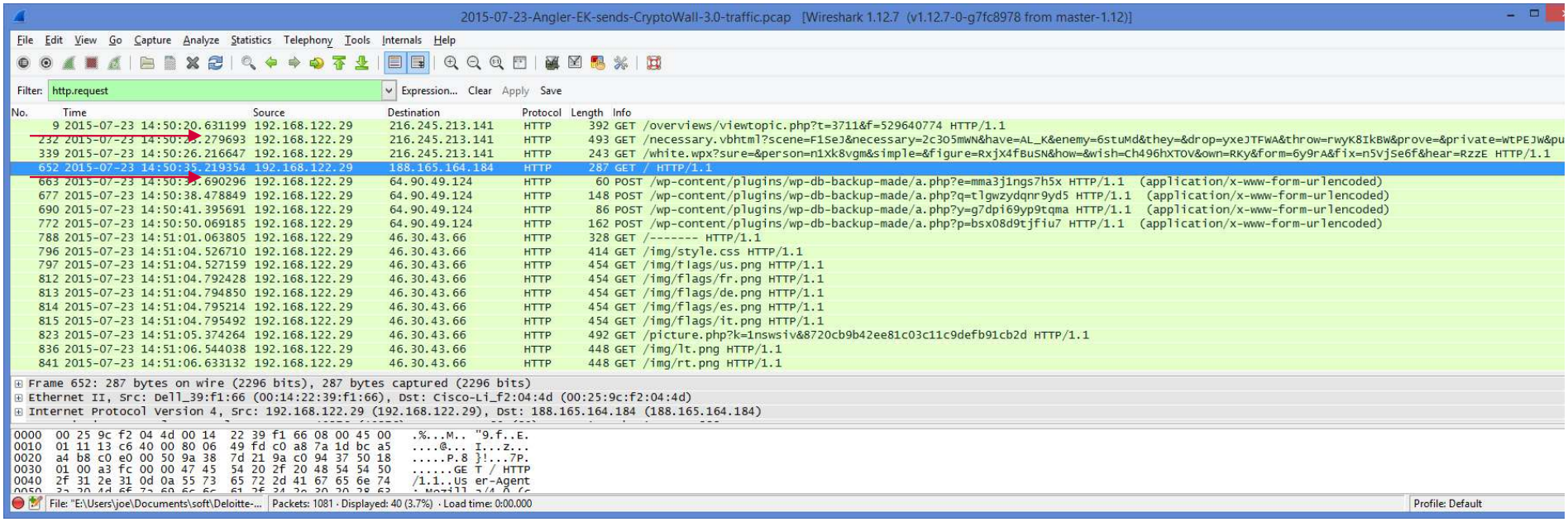
Challenge 2

When is the infection point?

- This is a key question that determines what files to examine. It's been said that Cryptowall encrypts user files one week after it gets into a user system? Is it true?

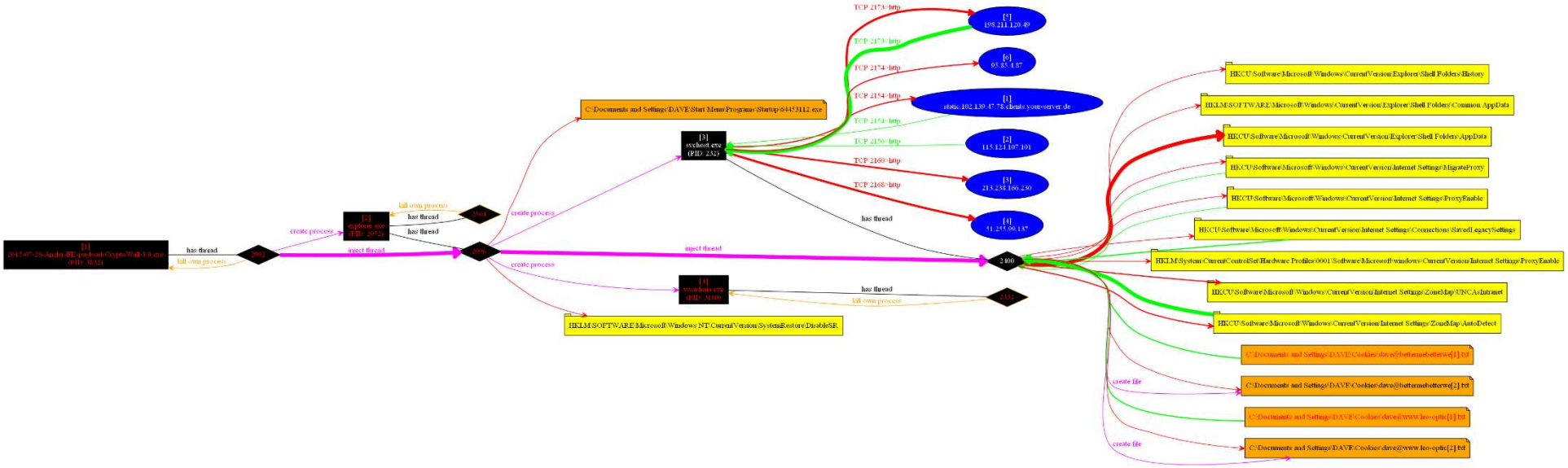
– Setup a lab and test a cryptowall sample.

- Traffic sample shows that cryptowall post-infection happens 15 seconds after user visiting a compromised site and landing page.



Challeng 2 - continue

- Setup a lab and test a cryptowall sample.
  - Cryptowall process flow chart shows:
    - Create process explorer.exe
    - Run vssadmin.exe
    - Modfiy registry
    - Internet activity
    - Launch svchost.exe, run injected code



Challenge 2 - continue

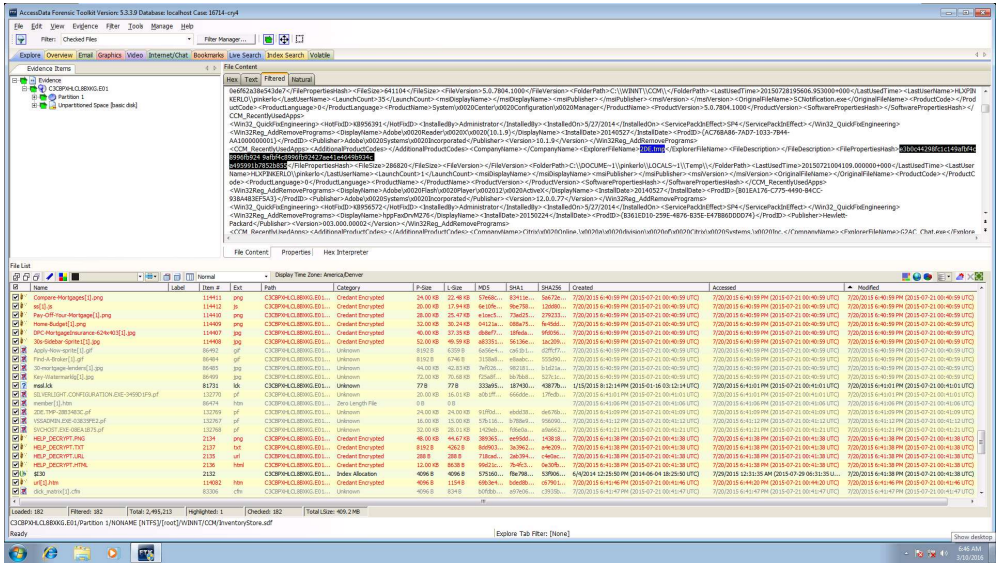
- Lab result:

  Cryptowall starts action very quick after getting into a user system.
- This is reasonable considering the efforts the malware actor spends on breaking into a system, he certainly doesn't want to waste time to get caught by AV, IPS before he starts the business.
- Now I know I should look at the events of seconds to minutes before the malware action.

Challenge 3

What to look at? Where are the events?

- FTK provides a list of files and disk unallocated spaces, you can sort by time.



- However, you still need to manually find events in the content of artifacts, such as NTFS indexing, credant encryption log, prefetch, file property hash, inventory history, windows event logs, registery, CCM, temp folder, browsing history, cookies, disk slack spaces...

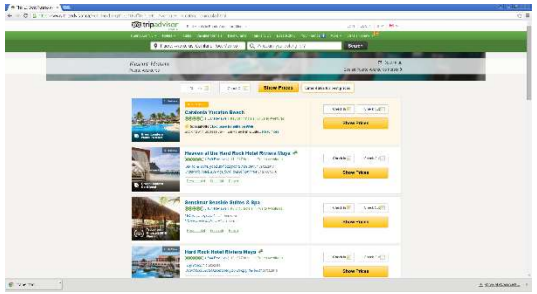
Timeline analysis

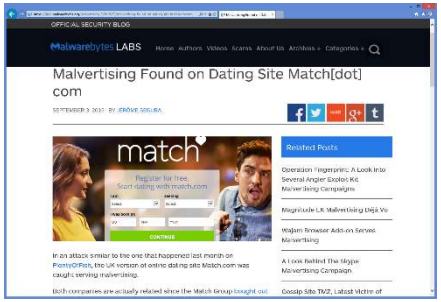
- Built a timeline

- 1) user login in the afternoon at time: Jul-20 22:30:0 UTC (user local time is 7/20 4:30:0 PM, user timezone is Mountain Daylight Time)
- 2) user typed URL http://tripadvisor.com to plan a trip in Mexico. time:07-21 00:10:45 UTC
- 3) that site linked to other websites: including match.com. time: 07-21 00:31:02 UTC
- 4) match.com contained advertisments that are hosted at openX adserver, yahoo.com, time: 07-21 00:31:02 UTC
- 4.1) IE History Index entry URL: PrivacIE:gstatic.com/s/roboto/*/5YB-ifwqHP20Yn46l_BDhA.eot accessed time: Jul 21 00:40:58 UTC hits: 25
- 4.2) ..IE5\0VAC36XA\fontawesome-webfont[2].eot time: Jul-21 00:40:58 UTC hits: 2
- 4.3) URL: PrivacIE:gstatic.com/s/ptsans/*/S1YQx4pVZa17uu0HWQd2fA.eot accessed time: 7/21 12:40:58 AM +00:00 hits: 4
- 4.4) URL: PrivacIE:gstatic.com/s/robotocondensed/*/Zd2E9abXLFGSr9G3YK2MsG8ITcfo9NwJpvZiO7_FxEg.eot accessed time: 7/21 12:40:58 AM +00:00
- 4.5) IE History Index entry URL: PrivacIE:sharpspring.com/client/*/ss.js accessed time: 7/21 12:40:59 AM +00:00 hits: 1
- 4.6) kickstarteli.com/molehills/*/viewtopic.php time: Jul-21 00:40:59 UTC
- 4.7) IE History Index entry URL: PrivacIE:sharpspring.com/client/*/noform.js accessed time: 7/21 12:40:59 AM +00:00 hits: 1
- 5) silverlight.configuration.exe was executed. time: 07-21 00:41:01 UTC
- 6) payload 2de.tmp was executed, time: 07-21 00:41:09 UTC
- 7) vssadmin.exe was executed, malware disabled Windows shadow copy to prevent file recovery. time:07-21 00:41:12 UTC
- 8) svchost.exe was executed, malware started an explorer process to run itself, time:07-21 00:41:21 UTC
- 9) first HELP_DECRYPT.URL was dropped. Cryptowall encryption started. time:07-21 00:41:38 UTC
- 10) last HELP_DECRYPT.PNG was dropped. Cryptowall encryption ended. time:07-21 00:51:00 UTC
- 11) rundll32.exe was executed. malware cleaning up. time:07-21 00:51:03 UTC
- 12) no events in the following half hour.

Timeline analysis - Malvertising

- From the timeline, we can see user browsed a known Malvertising serving site: match.com, 10 minutes later, silverlight vulnerability was explioted, cryptowall payload was executed, and encryption started.
- Here is reference link for Malvertising campaign used match.com and lead to Angler EK and cryptowall malware in July:
  https://blog.malwarebytes.org/malvertising-2/09/malvertising-found-on-dating-site-matchdotcom/
- Malvertising infection flow:
  - User visiting tripadvisor site:
  - Malvertising:
  - Malicious redirect:
  - Exploit kit (Angler):
  - vulnerability CVE-2023-23397 MS Office
  - Cryptowall





Malware Exploit - vulnerability

- CVE-2023-23397 Microsoft Office

Infection flow

- It is never too late to know the truth
- Forum pic