
Forensics Cryptowall

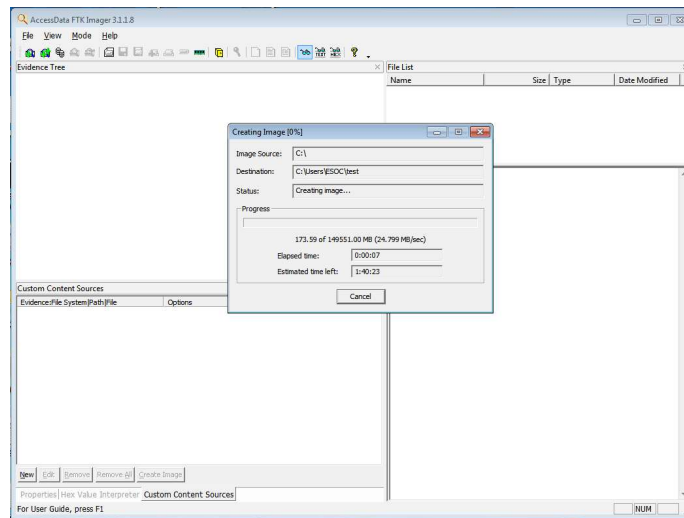
Joe Wu

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

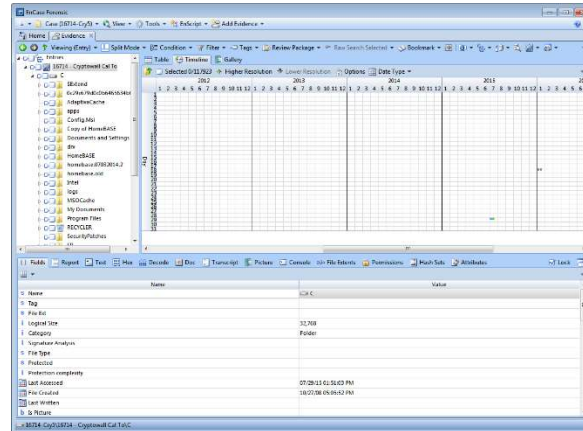
- First, to get a forensic image from the hard disk. Tool used was FTK imager. The output is a .E01 file.



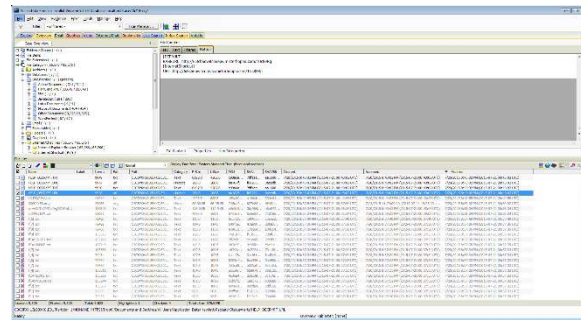
- Then, to collect evidences using forensic software: Encase, FTK, autopsy, and other tools like pasco.

Tools

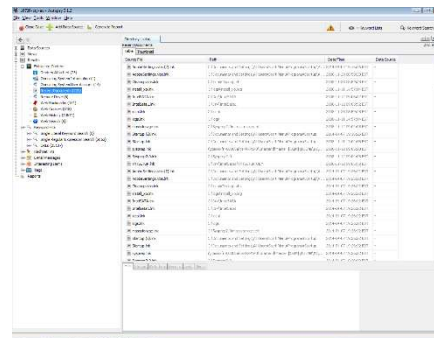
■ Encase



■ FTK



■ Autopsy

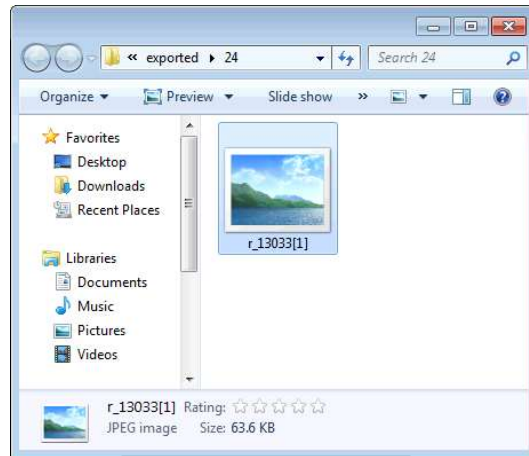


■ Pasco

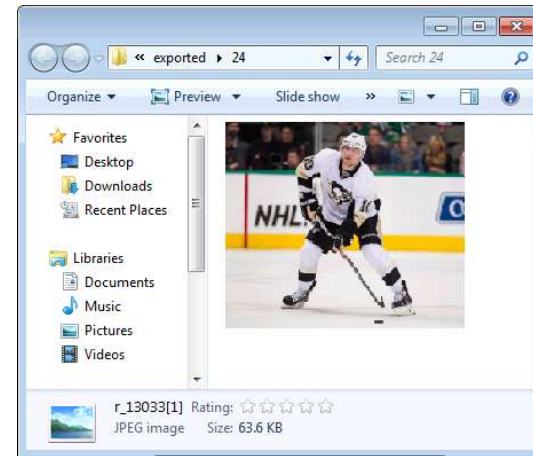


Challenge 1

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”

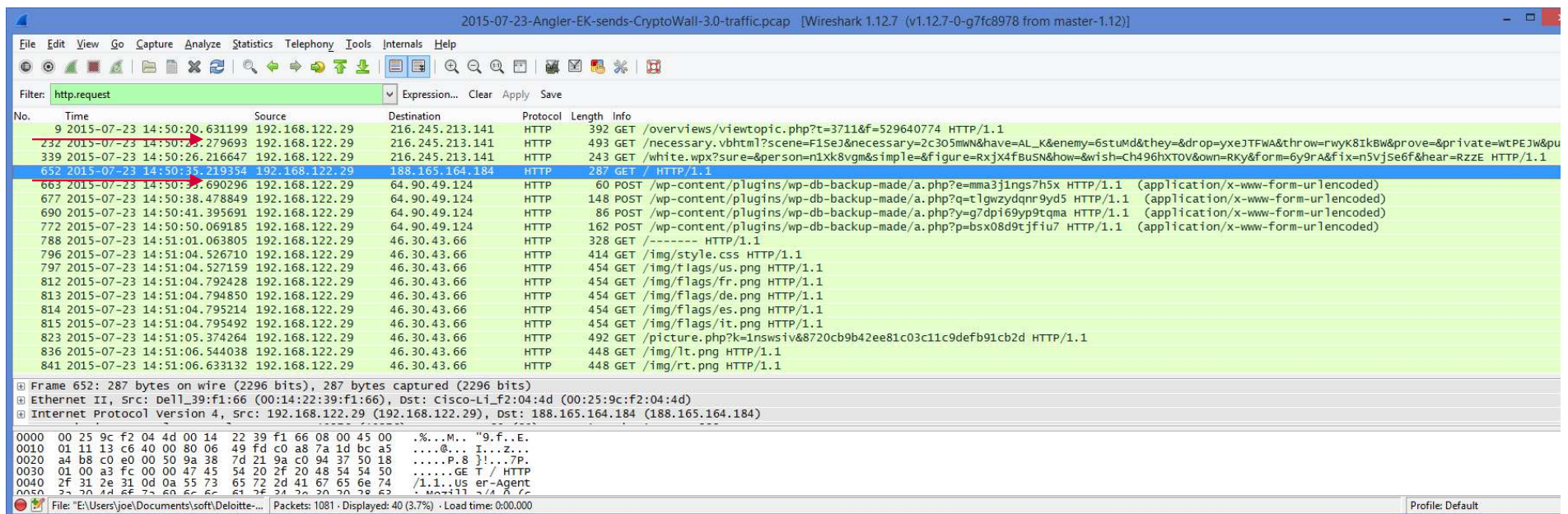
KB is available at sharepoint:

<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.



2015-07-23-Angler-EK-sends-CryptoWall-3.0-traffic.pcap [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

Filter: http.request

No.	Time	Source	Destination	Protocol	Length	Info
9	2015-07-23 14:50:20.631199	192.168.122.29	216.245.213.141	HTTP	392	GET /overviews/viewtopic.php?t=3711&f=529640774 HTTP/1.1
232	2015-07-23 14:50:28.279693	192.168.122.29	216.245.213.141	HTTP	493	GET /necessary.vbhtml?scene=F1sej&necessary=2c305mnw&have=AL_K&enemy=6stumd&they=&drop=yxejTFwA&throw=rwyk8IkBw&prove=&private=WTPEJw&pu
339	2015-07-23 14:50:26.216647	192.168.122.29	216.245.213.141	HTTP	243	GET /white.wpx?sure=&person=n1Xk8vgm&simple=&figure=Rxjx4fBuSN&how=&wish=Ch496hXTOV&own=RKY&form=6y9rA&fix=n5VjSe6f&hear=RzZE HTTP/1.1
652	2015-07-23 14:50:35.219354	192.168.122.29	188.165.164.184	HTTP	287	GET / HTTP/1.1
663	2015-07-23 14:50:35.690296	192.168.122.29	64.90.49.124	HTTP	60	POST /wp-content/plugins/wp-db-backup-made/a.php?e=mma3jlngs7h5x HTTP/1.1 (application/x-www-form-urlencoded)
677	2015-07-23 14:50:38.478849	192.168.122.29	64.90.49.124	HTTP	148	POST /wp-content/plugins/wp-db-backup-made/a.php?q=tlgwzdydnr9yd5 HTTP/1.1 (application/x-www-form-urlencoded)
690	2015-07-23 14:50:41.395691	192.168.122.29	64.90.49.124	HTTP	86	POST /wp-content/plugins/wp-db-backup-made/a.php?y=g7dpi69yp9tqma HTTP/1.1 (application/x-www-form-urlencoded)
772	2015-07-23 14:50:50.069185	192.168.122.29	64.90.49.124	HTTP	162	POST /wp-content/plugins/wp-db-backup-made/a.php?p=bsx08d9tjfiu7 HTTP/1.1 (application/x-www-form-urlencoded)
788	2015-07-23 14:51:01.063805	192.168.122.29	46.30.43.66	HTTP	328	GET / HTTP/1.1
796	2015-07-23 14:51:04.526710	192.168.122.29	46.30.43.66	HTTP	414	GET /img/style.css HTTP/1.1
797	2015-07-23 14:51:04.527159	192.168.122.29	46.30.43.66	HTTP	454	GET /img/flags/us.png HTTP/1.1
812	2015-07-23 14:51:04.792428	192.168.122.29	46.30.43.66	HTTP	454	GET /img/flags/fr.png HTTP/1.1
813	2015-07-23 14:51:04.794850	192.168.122.29	46.30.43.66	HTTP	454	GET /img/flags/de.png HTTP/1.1
814	2015-07-23 14:51:04.795214	192.168.122.29	46.30.43.66	HTTP	454	GET /img/flags/es.png HTTP/1.1
815	2015-07-23 14:51:04.795492	192.168.122.29	46.30.43.66	HTTP	454	GET /img/flags/it.png HTTP/1.1
823	2015-07-23 14:51:05.374264	192.168.122.29	46.30.43.66	HTTP	492	GET /picture.php?k=Inswsiv&8720cb9b42ee81c03c11c9defb91cb2d HTTP/1.1
836	2015-07-23 14:51:06.544038	192.168.122.29	46.30.43.66	HTTP	448	GET /img/lt.png HTTP/1.1
841	2015-07-23 14:51:06.633132	192.168.122.29	46.30.43.66	HTTP	448	GET /img/rt.png HTTP/1.1

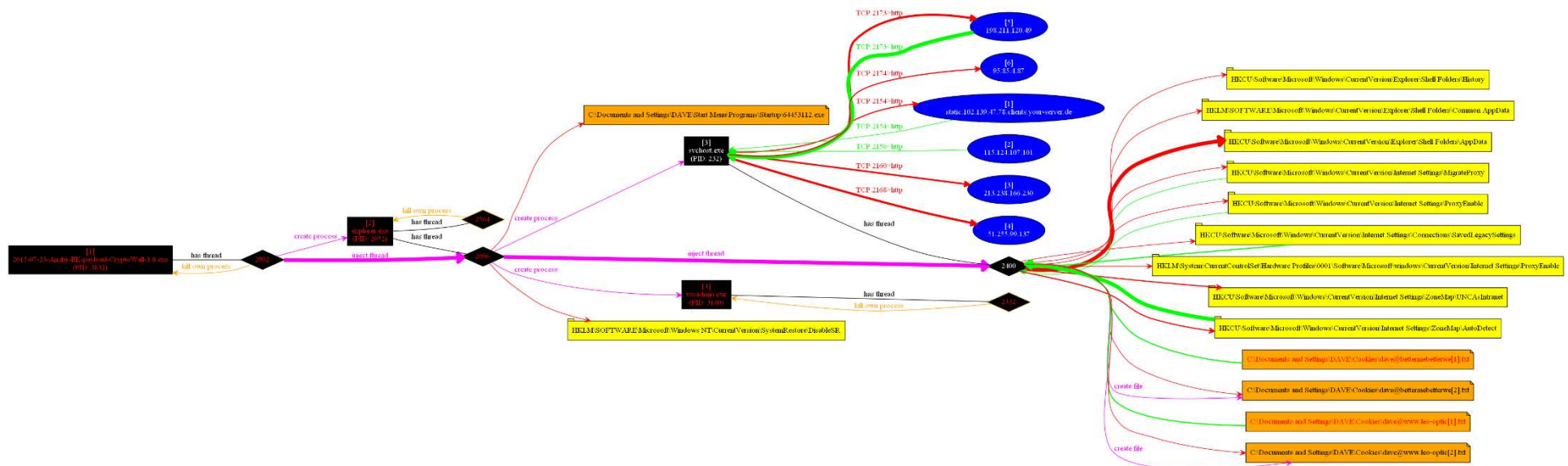
Frame 652: 287 bytes on wire (2296 bits), 287 bytes captured (2296 bits)
Ethernet II, Src: Dell_39:f1:66 (00:14:22:39:f1:66), Dst: Cisco-Li_f2:04:4d (00:25:9c:f2:04:4d)
Internet Protocol Version 4, Src: 192.168.122.29 (192.168.122.29), Dst: 188.165.164.184 (188.165.164.184)

0000 00 25 9c f2 04 4d 00 14 22 39 f1 66 08 00 45 00 .%.M.. "9.f..E.
0010 01 11 13 c6 40 00 80 06 49 fd c0 a8 7a 1d bc a5 ...@... I...2...
0020 a4 b8 c0 e0 00 50 9a 38 7d 21 9a c0 94 37 50 18P.8 }!...7P.
0030 01 00 a3 fc 00 00 47 45 54 20 2f 20 48 54 54 50GE T / HTTP
0040 2f 31 2e 31 0d 0a 55 73 65 72 2d 41 67 65 6e 74 /1.1..US er-Agent
0050 32 30 44 46 7c 6c 6c 61 36 24 20 20 20 20 20 20 ..0011 3/4 0 0 0

File: "E:\Users\joe\Documents\soft\Deloitte-... Packets: 1081 · Displayed: 40 (3.7%) · Load time: 0:00.000 Profile: Default

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:

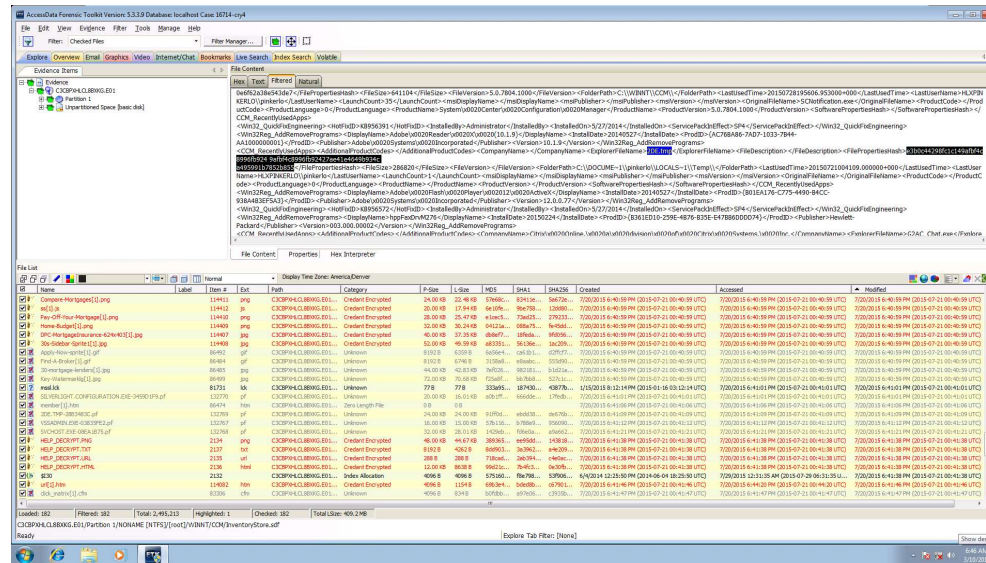
Cryptowall starts action very quick after getting into a user system.

- 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, credent encryption log, prefetch, file property hash, inventory history, windows event logs, registry, CCM, temp folder, browsing history, cookies, disk slack spaces...

Timeline analysis

■ Built a timeline

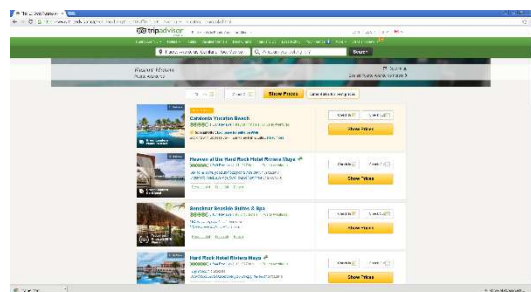
- 1) user login in the afternoon at time: Jul-20 22:30:0 UTC (user local time is 7/20 4:30:0 PM, user timezone is Mountain Daylight Time)
- 2) user typed URL <http://tripadvisor.com> to plan a trip in Mexico. time:07-21 00:10:45 UTC
- 3) that site linked to other websites: including match.com. time: 07-21 00:31:02 UTC
- 4) match.com contained advertisements 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](http://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.

Event: 1, 2, 3, 4, ...

Timeline

Timeline analysis - Malvertising

- From the timeline, we can see user browsed a known Malvertising serving site: match.com, 10 minutes later, silverlight vulnerability was exploited, 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