

Forum:[Hack Forums](#)

Thread: [Forensics WorkShop Part 2](#)

CyberStrike - July 6, 2018, 6:28 am

Foreword: I encourage everyone to participate, whether or not you have done this before or not, hands on is the best way to learn and I have included resources on volatility, which is a commonly used memory forensics framework. The solution will be posted on Monday, as to give everyone enough time to work on this challenge. If you can answer some questions great, if you can complete the whole challenge even better.

For an example of the write up, using pastebin for large blocks of text is fine and encouraged.

<https://hackforums.net/showthread.php?tid=5809120&pid=56810368#pid56810368>

Quote:Tools:

Volatility or Rekall
whois
reglookup
autopsy/foremost
Yara
Google
sha256sum
strings
VirusTotal

Once again no need for Kali/Caine/Deft/SANS Sift of course if you want you can use whatever you want.

Scenario: A friend from another country is a well known journalist, who writes articles exposing government corruption and civil rights abuses, unfortunately they have reason to suspect that they may have been infected by a malware from a government entity. and she needs your help.

Image Download: <http://www.mediafire.com/file/yxqodp1p2aca91x/0zapftis.rar>

Password: infected

RAR sha256sum: 0ab81aec6d61593a03a7b6fbda9266af8dd9c8df1b6477faa880fafd19cb21b10zapftis.rar

Extracted File Type: vmem

Quote:Resources:

<https://github.com/volatilityfoundation/volatility/wiki>

<https://resources.infosecinstitute.com/memory-forensics-and-analysis-using-volatility/>

<https://github.com/volatilityfoundation/volatility/wiki/Command-Reference>

Common Malware Registry locations:

<https://resources.infosecinstitute.com/common-malware-persistence-mechanisms/>

Yara Rules:

<https://github.com/Yara-Rules/rules>

Quote:Questions:

Questions on machine state:

What OS is used on the machine?

What processes are running and do any stand out?

What files are currently in the memory? Drivers and Windows objects, and do any of these stand out?

What networking connections and ports are present on the machine?

Do any of these connections or ports used stand out? If so why?

If there is a connection what country does this IP block belong to?

Malware Questions:

Is there malware present on the machine?

If there is malware dump the file and get the sha256 and identify the malware, also what has the malware changed to the system?

Have any commands been issued in a shell? If so what are these commands?

What methods of persistence are used in this malware?

Attribution:

What country could be responsible? Make sure to post relevant sources to support your conclusion.

Edit: Something I wanted to add, is that by understanding how a defender defends you can be a better attacker. For example you have to know what AV and figure out a way of bypassing that AV, the same principal here seeing how other attackers do their work will give you an idea of different tactics and techniques. Also seeing what an analyst can pick out of just a memory dump of a machine, which is what this is just a snapshot of a compromised machine, it can give you a better idea on how to avoid or hamper an analyst when they are looking at a machine you have compromised. So this is not just a look at a defender's toolset instead you can use it to further your attacks, and be more aware of what is left behind after an attack.

Originalkillit - July 6, 2018, 9:21 am

Buddy I am really new to this but I am interested in learning this.but I will give it a try and thank you for the resources I never knew about that except kali--->but kali freezes sometimes

while working so I will give it a try

ItsJigSaw - July 6, 2018, 10:25 am

Feelsbad i wont be home untill monday evening. Will check the results tho, rly interested.
Great post.

CyberStrike - July 6, 2018, 2:22 pm

Give it a shot ItsJigSaw, even if it is solved you can use the solutions if you get stuck. Originalkillit, interesting what graphics card do you got in that machine? Also is it VM or installed to HD?

Fred213 - July 7, 2018, 2:35 am

(Jul 6, 2018 10:25 AM)ItsJigSaw Wrote: [\[CITE\]](#) Feelsbad i wont be home untill monday evening. Will check the results tho, rly interested.

Great post.

CAN YOU PLZ REPLY MY MSG?

CyberStrike - July 7, 2018, 5:44 am

Alright just finished had multiple interruptions tonight, took about 6 hours to finish, solution will be posted on Monday. If someone get's stuck post here we can all help one other out.

ItsJigSaw - July 7, 2018, 6:27 am

(Jul 7, 2018 02:35 AM)Fred213 Wrote: [\[CITE\]](#) CAN YOU PLZ REPLY MY MSG?

I dont have a msg from u in my inbox.

CyberStrike - July 8, 2018, 4:53 am

If anyone needs help, get's stuck, even wants more resources so they can attempt the challenge on their time feel free to post I'll be more than happy to help.

Originalkillit - July 8, 2018, 5:15 am

(Jul 8, 2018 04:53 AM)sirru5h Wrote: [\[CITE\]](#) If anyone needs help, get's stuck, even wants more resources so they can attempt the challenge on their time feel free to post I'll be more than happy to help.

Great thank for fixing the links all links are 100% working

?

CyberStrike - July 8, 2018, 5:21 am

(Jul 8, 2018 05:15 AM)Originalkillit Wrote: [\[CITE\]](#) Great thank for fixing the links all links are 100% working

?

Excellent I apologize for that, I used links from the first challenge and assumed that they were all working fine, that said if you refer to the first one you will find that this challenge follows much of the first one.

CyberStrike - July 9, 2018, 6:41 pm

Complete write up:

<https://pastebin.com/DgsYHPXi>

(I included a link to solve the majority of the challenge although a few things we do are a bit more involved)

DLL List:

<https://pastebin.com/JUk8yj3d>

Filescan:

<https://pastebin.com/7w6zStHh>

SVCscan:

<https://pastebin.com/fEtZcHzd>

TimeLine of Compromise:

<https://pastebin.com/FeVaF2Qn>

PID 1956 ThreadScan:

<https://pastebin.com/WQDXFjLx>

Originalkillit - July 10, 2018, 6:04 am

(Jul 9, 2018 06:41 PM)sirru5h Wrote: [\[CITE\]](#) Complete write up:

<https://pastebin.com/DgsYHPXi>

(I included a link to solve the majority of the challenge although a few things we do are a bit more involved)

DLL List:

<https://pastebin.com/JUk8yj3d>

Filescan:

<https://pastebin.com/7w6zStHh>

SVCscan:

<https://pastebin.com/fEtZcHzd>

TimeLine of Compromise:

<https://pastebin.com/FeVaF2Qn>

PID 1956 ThreadScan:

<https://pastebin.com/WQDXFjLx>

Thank you buddy I am going through it and I want you to keep that link alive I am using it for a month now to learn

Spoiler [\(Click to View\)](#) Just downloaded everything ? ?
?

CyberStrike - July 10, 2018, 6:12 am

(Jul 10, 2018 06:04 AM)Originalkillit Wrote: [\[CITE\]](#) Thank you buddy I am going through it and I want you to keep that link alive I am using it for a month now to learn

Spoiler [\(Click to View\)](#) Just downloaded everything ? ?
?

Those links shouldn't expire also I used pastbin for everything due to the amount of text involved.
Good luck!