

Forum:[Hack Forums](#)

Thread: [Cridex-A journey into Incident Handling](#)

CyberStrike - April 3, 2019, 2:33 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 a week from now 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. The main thing is just to learn even if you just read through that's fine.

Cridex Information:

<https://www.webopedia.com/TERM/C/cridex-malware.html>
<https://www.symantec.com/security-center/writeup/2015-012314-0117-99>

Why this section?

After seeing the thread below it appears that some of the sub-sections would be appropriate as we are dealing with a banking trojan/stealer.

<https://hackforums.net/showthread.php?tid=5928245>

Another and more important reason is to allow others to be exposed to what an incident response handler's common tools are and how tracking down of malware from a memory dump (RAM) as well as the malicious IPs involved works. This will not just be all forensics since we will also be developing IOC's and perhaps looking at some of the functionality.

Tools:

Volatility/ Rekall/Redline or Whatever you wish
whois
reglookup
autopsy/foremost/Digital Forensics FrameWork
Yara
Google
sha256sum
strings
VirusTotal
hexeditor
Reverse.it (your choice)

Resource/Reference:

<https://www.howtoforge.com/tutorial/how-to-install-and-use-volatility-memory-forensic-tool/>
<https://github.com/volatilityfoundation/volatility/wiki>

<https://linux.die.net/man/1/reglookup>

<https://bruteforcelab.com/yara-a-beginners-guide.html>

<https://linux.die.net/man/1/foremost>

<https://linux.die.net/man/1/strings>

No need to use a specialized distro such as SANS SIFT/Caine/Kali/DEFT I do suggest use a VM of course and no AV, since it can delete some of the extracted files. (I will be doing this on Ubuntu myself)

What is in this memory dump?

A VMEM file, which is a VMware RAM dump, this one being of Cridex banking trojan. A VMEM is NOT executable and to extract the malware you would need to dump the addresses where in the malware resides from the VMEM. It's not like you open the zip file and bang there is a virus or anything of the sort, even if you dumped all the executables in the VMEM you still have to double click the file to actually be infected and be on Windows. This particular RAM dump was gotten from Volatility

<https://github.com/volatilityfoundation/volatility/wiki/Memory-Samples>

This memory dump is called “ Malware - Cridex ”

Scenario:

At your work there was one of the managers is complaining that their bank account shows strange withdrawals, of course they decided to mix business and personal lives so to make sure that the machine is not infected you've been asked to take a look at the machine. So far one machine has been compromised now management wants you to put your skills to work and figure out what happened, then develop IOCs (Indicators of Compromise) to be able to quickly triage any further infected machines.

Questions:

0)What OS is the compromised machine?

1) What processes are running?

2) What connections are active, and processes making these connections?

3) What ports are the connections and processes from question 2 which are being used?

4) Perform a WHOIS on all connections and post suspicious IP results

5) Do any processes which are making connections connecting to a suspicious IP/Domain?

6) Are any processes suspicious? If so why?

Extra:

Malware Analysis (Extra)

7) Dump the suspicious process and include the sha256sum of the file

8) What family is the malware from?

9) Are there any interesting strings in the malware that can help us further figure out what this malware is targeting?

10) Develop IOC (Indicators of Compromise) to help quickly identify other infected machines

For large blocks of text use pastbin/hastebin/ghostbin your choice

File Size: 38.9mb

sha256: 6453d0986352f7d5287cb90eeb6b72bc7bc16b03e964bb5767d93f85c3a483b2

Edit: Had questions about the end date.

Edit to the Edit: Just finished, while I couldn't extract a full payload I ended up breaking into sections vadinfo and vaddump will be crucial when doing this.

CyberStrike - April 10, 2019, 3:12 pm

The amount of text was quite significant so I went with pastbin

<https://pastebin.com/tjsBpmRN>

Being that this was injected into another process it made it a bit more interesting and obviously the connection artifacts meant a little extra work and required more enumeration and leg work. I think that the mutex's really gave the first indication of what malware it was.

I do have two pictures which I wanted to include

First the sites that this malware is targeting (a small snippet)

Second picture is of the various IP's used by the attacker as infrastructure.

tcsh - April 10, 2019, 3:21 pm

Impressive work and an interesting read

CyberStrike - April 10, 2019, 3:45 pm

(Apr 10, 2019 03:21 PM)tcsh Wrote: [\[CITE\]](#) Impressive work and an interesting read

I appreciate the kind words I planned originally on getting malware and dumping the RAM from my own but with just two days it'd be a real time crunch. I also wanted to rebuild the entire payload just not enough time. That said I did find a few good tutorials on it so that might be another project for a weekend. I do plan on doing an incident response how to tutorial one day.

tcsh - April 10, 2019, 5:03 pm

(Apr 10, 2019 03:45 PM)CyberStrike Wrote: [\[CITE\]](#) I appreciate the kind words I planned originally on getting malware and dumping the RAM from my own but with just two days it'd be a real time crunch. I also wanted to rebuild the entire payload just not enough time. That said I did find a few good tutorials on it so that might be another project for a weekend. I do plan on doing an incident response how to tutorial one day.

Sounds like some good ideas. I'll be looking forward to the read :)