

Forum:[Hack Forums](#)

Thread: [Extract live data from a memory dump](#)

banderas20 - July 2, 2019, 3:20 pm

Hi.

I have a Windows memory dump and I am analyzing it with Volatility.

I have seen many interesting processes. However, I would need to get some live data regarding these processes.

Such as linked Paths, opened documents, passwords entered, and so on.

¿How can achieve this?

Many thanks!

CyberStrike - July 2, 2019, 3:53 pm

Live data? Umm it's not live anymore it's a snapshot of memory, that said with nothing more than strings and grep you can extract passwords, and volatility does have plugins for that. You will probably use foremost and or scapel to extract documents and files, you can use even a hexeditor for this.

~Chester~ - July 3, 2019, 3:27 am

pciscreamer

mounts live memory as a file system

CyberStrike - July 3, 2019, 3:54 am

(Jul 3, 2019 03:27 AM)~Chester~ Wrote: [\[CITE\]](#) pciscreamer

mounts live memory as a file system

Just looked this up interesting way of doing it, well done sir.

Sitrep - July 3, 2019, 5:01 pm

Are you sure that you have a memory dump and not a ".pcap" (wireshark) network logg?

~Chester~ - July 3, 2019, 5:45 pm

(Jul 3, 2019 03:54 AM)CyberStrike Wrote: [\[CITE\]](#) Just looked this up interesting way of doing it, well done sir.

yea its really cool to use. kinda flakey, but can be insanely useful for DMA based game cheats.

Asdethprime - July 4, 2019, 12:59 am

<https://docs.microsoft.com/en-gb/windows/win32/api/debugapi/nf-debugapi-debugactiveprocess>

That's the official way to do it.

banderas20 - July 4, 2019, 11:14 am

(Jul 3, 2019 03:27 AM)~Chester~ Wrote: [\[CITE\]](#) pciscreamer

mounts live memory as a file system
I can't seem to find that software.

The thing is, I have a memory dump in which appears the process "Truecrypt.exe" and a mounted volume, and I want to find the key.

I issue:

volatility truecryptmaster
volatility truecryptsummary
volatility truecryptpassphrase

The 2 firsts give me results, but the last one yields no results. I expect to find the key that must be stored somewhere in memory.

¿How can I achieve that?

Thanks!

~Chester~ - July 5, 2019, 4:39 am

(Jul 4, 2019 11:14 AM)banderas20 Wrote: [\[CITE\]](#) I can't seem to find that software.

The thing is, I have a memory dump in which appears the process "Truecrypt.exe" and a mounted volume, and I want to find the key.

I issue:

volatility truecryptmaster
volatility truecryptsummary
volatility truecryptpassphrase

The 2 firsts give me results, but the last one yields no results. I expect to find the key that must be stored somewhere in memory.

¿How can I achieve that?

Thanks!pciescreamer isnt a software. its an fpga board you plug into one of your free pcie slots and it intercepts bus traffic. It does bundle with a software that will allow you to mount the memory system as an "explorer" type drive.

if you are referring to an attack to grab an encryption key stored in memory, afaik the only way to do this is with subzero temperatures on the affected ram chip then dumping memory.

Heres some info(see page 73):

<https://www.uvm.edu/~ddeutl/TOEC2010/TrueCrypt/TrueCrypt%20User%20Guide.pdf>

Asdethprime - July 6, 2019, 2:16 am

You are trying to find a fully automated way of extracting keys (private keys) from a programs RAM... BRA!!

They don't always work that way.

