Cyber Snapshot

Exploring and Assessing Current Topics

MICHIGAN CYBER COMMAND CENTER (MC3)

January 13, 2021
CS-01-2021

CAPTURING RANDOM ACCESS MEMORY (RAM)

OVERVIEW:

Many forms of malware only reside in random access memory (RAM), which is a computer's temporary memory that resets after a power cycle. If an organization falls victim to a malware attack, such as ransomware or other fileless malware, they should consider immediately capturing/preserving evidence and disconnecting any infected machines from the network. Machines should not be restarted or shut down unless files are actively being encrypted. Critical evidence related to ransomware and other fileless malware may only be found in RAM data or the related pagefile.sys file.

FILELESS MALWARE:

Obtaining a RAM capture is especially important as a majority of malware is considered to be fileless. As the initial infection comes into the victim system, legitimate tools such as PowerShell are leveraged against the target system. This method is done to limit the likelihood that it will be detected by antivirus/malware detection applications. As antivirus/malware detection applications are for the most part signature based, it makes memory-based malware even more difficult to detect. This is all the more reason that capturing the memory from a computer is extremely important. Capturing memory allows for stable and static analysis of a volatile environment. Analysis can reveal malicious processes, commands executed, network connections, and newly scheduled/automated tasks. If a RAM capture is not immediately available, IT staff should capture and document live network connections, such as using a netstat command, prior to disconnecting the machine from the network.

RAM CAPTURE:

An organization has several options when it comes to collecting and analyzing RAM. The organization can use free forensic software such as MAGNET RAM Capture by Magnet Forensics, FTK Imager by AccessData, or various other applications to capture RAM on a Windows machine. Other software tools are available for the collection of RAM on Mac and Linux machines. After collecting RAM, the memory can be analyzed utilizing a free memory analysis tool, such as Volatility by The Volatility Foundation.

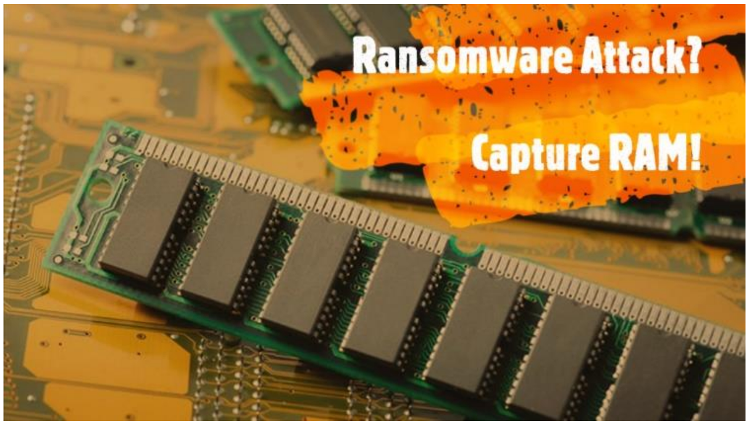

Image adapted from: avast.com

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. The information is designated UNCLASSIFIED – TLP: WHITE. Information found within this document can be shared without restriction. This document must not be reclassified in any way, whole or in part. Violation of this restriction will be cause for removal from MC3 distribution lists.

mc3@michigan.gov • 1-877-MI-CYBER • www.michigan.gov/mc3 Page 1 of 2

As an alternative option, an organization experiencing a malware attack can contact the Michigan Cyber Command Center (MC3) to initiate a criminal investigation and collect digital data to preserve and analyze the evidence. Part of this investigation would include the MC3 responding to the scene or working with the organization remotely to obtain a RAM capture and other related digital files. The remote option would involve the MC3 sending a RAM capture tool licensed to the MC3 that would not only capture RAM, but also capture associated logs and volatile files of interest. This data is encrypted as part of the capture process and can then be safely sent back to the MC3 for analysis. This tool can capture RAM on Windows, Mac, and Linux machines.

It should be noted if the infection is within a virtual machine, the virtual machine should be suspended and the various memory related files be copied out from within the virtual machine directory. Virtual machine memory can be analyzed just like normal RAM and therefore should be preserved when possible.

CONCLUSION:

To summarize, RAM should be captured during any malware incident. Many forms of malware, including files associated with ransomware, are fileless and therefore only present in memory. Capturing and subsequently analyzing RAM may provide valuable insight into how the malware executed as well as what files were imported/exported from the system. If an organization falls victim to a malware attack, they are highly encouraged to contact the MC3 for additional resources and assistance. Organizations are reminded that information provided to the MC3 related to a cyber security incident is confidential and is not available for release through the Freedom of Information Act (FOIA). Planning ahead of time is critical to capturing and preserving evidence in a timely manner. Feel free to contact the MC3 to discuss options for including RAM capture in your incident response plan.

As a reminder, there are several proactive steps an organization can take to protect themselves against malware attacks. These steps include disabling RDP (or using RDP behind a VPN), regularly backing up data and storing this data offline, providing cyber security awareness training to employees, and keeping software up to date.

ADDITIONAL RESOURCES:

The below resources can be found at www.michigan.gov/mc3

- Ransomware – Protecting Data
- Remote Desktop Protocol (RDP)
- Default Configurations – Security & Certificates

This document is the property of the Michigan Cyber Command Center (MC3) and is prepared for the limited purpose of information sharing. The information is designated UNCLASSIFIED – TLP: WHITE. Information found within this document can be shared without restriction. This document must not be reclassified in any way, in whole or in part. Violation of this restriction will be cause for removal from MC3 distribution lists.