SO YOU THINK YOU'VE BEEN COMPROMISED…

DATA PRESERVATION

Organizations that face a potential threat from the presence of malicious software/actors on their systems often do not know how to properly react to suspected intrusions. Whether organizations conduct their own computer forensics or outsource it to a third party, it is important to understand that digital evidence can be fragile. Some of the most important forensic evidence can be found in areas that are considered volatile or in places easily overwritten or lost when the system is shut down. Any action performed on a system makes changes to memory, files, and logs. This loss of data makes investigations more difficult, as forensics investigators rely on these fragile artifacts to determine the extent of a compromise. Proper incident response should always consider the critical need to preserve forensic data as one of the pillars in their response plan and procedures.

After identifying a suspected compromise, responders should work to consolidate and review network-level logging. Once a system is identified as being possibly compromised, responders should be very careful about making any changes to the system. While some changes may be obvious, such as the installation of new programs or applications, others are less so. For this reason, ICS-CERT has assembled a list of suggested things to avoid and things that should be done to preserve important data.

DON'TS OF INCIDENT RESPONSE

Do Not Turn Off The System

- Turning off the system will result in lost forensic memory artifacts. When a computer is turned off, it initiates a series of commands that make changes to the hard drive and result in the loss of volatile data stored in registries, caches, and random access memory (RAM).

Do Not Immediately Disconnect From Network

- Disconnecting from the network before imaging system memory and hard drives can tip off an attacker and result in the loss of malware and indicators needed for a successful response. At the same time, staying connected to the network could continue to expose the victim to data exfiltration and lateral movement of the attacker. Responders are encouraged to weigh the costs and benefits of either action before committing to a decision.

Do Not Run Anti-Virus Programs

- The use of anti-virus products on a compromised system can be very invasive since they access virtually every file on the system. This can cause file last-access times to change, system logs to roll over, and add additional data points that must be analyzed by the forensic investigator.

Do Not Run Registry Or File Cleaner Programs

- Registry or file cleaner programs destroy useful forensic artifacts in the registry and memory.

Do Not Install Or Run Any Additional Tools

- By running or installing programs, changes are made to the system that may result in forensic data loss. The exception to this rule would be running programs necessary to image the system.

DO'S OF INCIDENT RESPONSE

In order to preserve needed forensic data, the following lists of software and commands could be used to acquire, first, a memory capture then an image of the hard drive. The tools below are referenced as examples rather than endorsements. There are proprietary and open source alternatives that implement similar features with varying levels

of effectiveness. The website www.forensicswiki.org/wiki/Tools is a good resource for identifying other tool options and usage instructions.

MEMORY CAPTURE

The volatile memory in a system is a gold mine of forensics data, often containing information that cannot be found on the hard drive or anywhere else. Some advanced malware has even evolved to erase any sign of its presence except for the code in memory that it needs to run. For these reasons, those responding to an incident should make every effort to capture a memory image using the following software, or software of similar capability:

DumpIt (www.moonsols.com/wp-content/plugins/download-monitor/download.php?id=7)

- Double click to execute from USB. The memory capture is saved to the directory the DumpIt executable is run from.

FTK Imager Lite (www.accessdata.com/support/product-downloads#F0TKImager)

- Install application or extract 'FTK Imager.exe' onto a large external USB drive.
- Start 'FTK Imager.exe' → File → Capture Memory → Select options in dialog windows
- It is recommended that you output the memory capture to an external drive (e.g., USB Drive).

HARD DRIVE IMAGE

After the acquisition of a memory capture, incident responders should capture an image of the hard drive as part of their data collection. Hard drives can contain a variety of operating system artifacts and logs that can be very helpful for establishing what happened on a system. While there are multiple software and hardware-based tools for duplicating hard drives for forensic analysis, we've included two common solutions:

dd Utility (Linux System)

- *dd if=<Input> of=<Output> bs=4096 conv=noerror,sync*

  Input—Path to the physical disk or partition to be imaged
  Ouptut—Destination path of forensic image
  bs—Block size
  noerror—Do not stop processing on an error.
  sync—Pads every input block to the bs value.

FTK Imager (www.accessdata.com/support/product-downloads#FTKImager)

- Install application or extract 'FTK Imager.exe'
- Start 'FTK Imager.exe' → File → Create Disk Image → Select options in dialog windows
- Choose "Physical Drive" and the corresponding disk that you wish to image.
- Choose "Logical Drive" if you're imaging a RAID or an encrypted drive and the drive to image (usually C:\)
- Add an image destination on the external USB drive. Don't check the box to "Pre-calculate Progress Statistics" as it will only waste time. Don't use the source drive as the destination or you may simply fill the entire source drive.
- Choose "E01" as the destination image type
- Fill in the evidence item information with the name of the person that duplicated the drive and the source system's hostname.
- Choose the destination folder and image filename. Name the file using the hostname of the computer.
- Use the defaults for Image Fragment Size and Compression. ***DO NOT*** *use AD Encryption.*
- Click "start" to begin imaging.
- Ensure that the verification step succeeds.
- Once FTK Imager is complete, remove the external USB drive from the victim computer.
- Ensure that the <filename>.txt file exists in the destination directory.