FOR528:
Ransomware
and Cyber Extortion

SANS.ORG/FOR528

Hands-on Malicious Script Analysis for Ransomware Response
With Ryan Chapman
FOR528 WORKSHOP

VIRTUAL MACHINE (VM) DOWNLOAD

IMPORTANT!!! Your workshop media is delivered via VM download. The media file for the workshop is 5GB. You need to allow time for the download and extraction to complete. Internet connections and speed vary greatly and are dependent on many different factors. Therefore, it is not possible to give an estimate of the length of time it will take to download your materials. Please start your workshop media download as soon as possible. You will need your workshop media immediately when you begin the workshop.

Download HERE
Password: jLgS5LqJMr8V
Access additional workshop materials here: https://for528.com/workshop

SYSTEM REQUIREMENTS FOR WORKSHOP

LAPTOP REQUIREMENTS

IMPORTANT!!! Bring your own system configured according to these instructions. If you do not carefully read and follow these instructions, you will not be able to fully participate in this hands-on workshop. Therefore, please arrive with a system meeting all the specified requirements.
Back up your system before workshop. Better yet, use a system without any sensitive/critical data. SANS is not responsible for your system or data.

MANDATORY WORKSHOP SYSTEM HARDWARE REQUIREMENTS

- CPU: 64-bit Intel i5/i7 (8th generation or newer), or AMD equivalent. An x64 bit, 2.0+ GHz or newer processor is mandatory for this workshop.
- CRITICAL: Apple systems using the M1/M2/M3/etc. processor line CANNOT perform the necessary virtualization functionality and therefore cannot in any way be used for this workshop.
- BIOS settings must be set to enable virtualization technology, such as "Intel-VTx" or "AMD-V" extensions. Be certain you can access your BIOS if it is password protected in case changes are necessary.
- 12GB of RAM or more is required. You will need to devote 8GB+ of RAM to the virtual machine you will use.
- 100GB of free storage space or more is required.

MANDATORY FOR528 HOST CONFIGURATION AND SOFTWARE REQUIREMENTS

- Your host operating system must be the latest version of Windows 10, Windows 11, or macOS 10.15.x or newer (if you are using a macOS host, please see the note about RE: M1/M2/M3/etc., processor incompatibility).
- Fully update your host operating system prior to the workshop to ensure you have the right drivers and patches installed.
- Linux hosts are not supported in the workshop due to their numerous variations. If you choose to use Linux as your host, you are solely responsible for configuring it to work with the workshop materials and/or VM.
- Local Administrator access is required. (Yes, this is absolutely required. Don't let your IT team tell you otherwise.) If your company will not permit this access for the duration of the workshop, then you should plan to bring a different laptop.
- Download and install VMware Workstation Pro 16.2.X+ or VMware Player 16.2.X+ (for Windows 10 hosts), VMware Workstation Pro 17.0.0+ or VMware Player 17.0.0+ (for Windows 11 hosts), or VMWare Fusion Pro 12.2+ or VMware Fusion Player 11.5+ (for macOS hosts) prior to the workshop beginning. If you do not own a licensed copy of VMware Workstation Pro or VMware Fusion Pro, you can download a free 30-day trial copy from VMware. VMware will send you a time-limited serial number if you register for the trial at their website. Also note that VMware Workstation Player offers fewer features than VMware Workstation Pro. For those with Windows host systems, Workstation Pro is recommended for a more seamless student experience.
- On Windows hosts, VMware products might not coexist with the Hyper-V hypervisor. For the best experience, ensure VMware can boot a virtual machine. This may require disabling Hyper-V. Instructions for disabling Hyper-V, Device Guard, and Credential Guard are contained in the setup documentation that accompanies your workshop materials.
- Download and install 7-Zip (for Windows Hosts) or Keka (for macOS hosts).