Purpose - The documentation will outline the actions to take when malware and security issues have been detected on a University owned device.

Our Product - At the time of this writing, Microsoft SCCM and SCEP is used on Windows 7 or 8.x, and Windows Defender on Windows 10. SCEP is used on MACS and in VDI without alert or reporting capabilities. Daily quick scans occur at noon every day with full scans occurring on the weekend.

Alerts and Help Desk Ticket Workflow – there are two processes for malware notifications.

1. Alerts flow from SCCM directly to technicians via email or into the iSupport Help Desk system. In some cases, Security may generate an iSupport case (SCCM categories are outlined at SCCM Malware Alerts).
2. Security reviews and generates Help Desk tickets to Technicians if the malware fits the HIT LIST for high priority issues. Malware in the HIT LIST includes; **Trojans, Ransomware (Crypto), Password stealer, Worm or Exploit (i.e. Conficker)**. Even though our anti-virus product SCEP found and likely removed the malware, it is unknown whether or not that malware was on the computer for a period or if remnants are left.

Note: *The Help Desk tickets from Security for HIT LIST items will either have a* ***recommended or required*** *reimaging action based upon the Detection Modes listed below. The ticket information will include PC name and some additional reminders. In addition, Security will use the Splunk security tool to do a full scan if an item on the HIT LIST is detected. For required reimages, the Help Desk ticket should be entered as an emergency priority. The priority can be adjusted for required reimages after the computer is pulled off-line.*

SCCM Console –technicians should review malware detail information for the computer in SCCM. This can help you determine whether the malware was caught, stopped, cleaned, where it was located or if it still exists on the machine. See SCCM Console Guidelines for further information.

Detection Mode

Infection status likely clean

- By malware caught in **real-time** and likely stopped by the antimalware product.
- By Browser Helper Object (**BHO**) similar to real-time but a protection mechanism in IE.
- By IOfficeAntivirus (**IOAV**) detection feature in Windows\Office and MpOAV.dll module. IOAV is a mechanism to scan a file before opening or sending via email.

Infection Status Unknown

- By **User**, meaning the files or browsing files went into the users Local App Data before being detected.
- By **System**, which means from a scheduled scan. In the last case, the malware did reside on the computer for a period before being discovered.
- By network real-time inspection (**NRI)** likely found by behavior monitoring.

Notes: *C:\Windows\CCM\Logs\EndpointProtection.log* on a PC may be helpful. When reviewing information on a computer as shown below, take into account the amount of malware cleaned. Is it one item or more? The computer below had found items indicating a required reimage and education requirement.

SCCM Console **Detection Mode** Information Screen Shot.

Threat Name	Detection Time	Category	Severity	Action	State Name	Detection Mode	Process	Path	User Name
Ransom:JS/FakeBsod.A	3/6/2016 4:44...	Trojan	Severe	Remove	Success	System	Unkno...	containerf...	NT AUTHO...
Rogue:JS/FakeCall.D	3/19/2016 4:31...	Trojan	Severe	Remove	Success	System	Unkno...	containerf...	NT AUTHO...
Rogue:JS/FakeCall.D	4/10/2016 4:35...	Trojan	Severe	Remove	Success	System	Unkno...	containerf...	NT AUTHO...
Rogue:JS/FakeCall.D	4/11/2016 10:1...	Trojan	Severe	Remove	Success	BHO	Unkno...	webscript:...	UTAD\haja...

Guidelines

The required **Reimage process** is based off the Security's **HIT LIST.**

- ACTIONS
  - Take the computer off the network and move to an IT location.
  - Only log into the machine with the local LAPS account. **DO NOT** login with UTAD credentials while it is on the network.
- COMMUNICATION
  - Follow the SOP notification process to the user for taking a machine by contacting the user directly and leaving a yellow IT communication card.
  - Provide a loaner computer if necessary.
  - Follow up daily with the user as needed.
  - Confer with the user the required files to be backed up.
  - Ask the user if they normally save files to H or Z drives.
  - Verify files on shares were not encrypted by Ransomware.
  - Document information in the ticket.
- BACKUP
  - Security may take a backup image remotely and silently in some cases. Technician will still need to backup and reimage even if you know this process has occurred.
  - Backup user files to an external device. Copy to another computer that is not on the network and perform additional scanning if necessary.
  - Reimage computer only after confirming files the user needs are intact. Instruct users to save files to their H or Z drives.
  - See link for documented current backup processes used by IT tech support areas for the Desktop Backup Processes.
- REIMAGING
  - After confirming all files have been backed up, reimage the machine using standard IT tools.
  - Restore backup files.
  - Run SCEP scan remotely using the console.
- EDUCATION
  - Education user on how to avoid phishing scams (See **Education** section below).

The **Reset User Password** occurs, if a **Trojan, exploit or password stealer** occurred.

- *Actions*
  - Contact the user directly in person or by phone. Let them know their credentials may have been compromised by malicious software.
  - Direct them to the ***MyUTaccount*** maintenance site to change their password using a different computer.
  - Notify Security if necessary.
  - Update Help Desk ticket.
  - Education user on how to avoid phishing scams (See **Education** section below).

The **Clean Process** occurs, if Potential Unwanted Software is found that is not in the HIT LIST and SCEP was not able to clean the computer.

- *Actions*
  - Notify the user that their computer has unwanted software on their computer.
  - Determine if files need to be backed up.
  - Remote scan the computer using a free tool like Stinger.
  - Install or use another piece of free or purchased software like SuperAntispyware or Malwarebytes to remove the malware.
  - Update Help Desk ticket.
  - If malware cannot be removed, backup files, reimage and move files back.
  - Education user on how to avoid phishing scams (See **Education** section below).

The **Update Process** occurs, if malware is seen like browser modifier, unwanted software, or other types of malware due to vulnerabilities in older browsers, add-ins to browsers, and third party applications.

- *Actions*
  - Verify Windows updates and SCUP 3rd party application are working properly, update manually if needed.
  - Update browser to the latest version if possible and apply patches.
  - Update third party apps or remove if possible.
  - Backup files and reimage if necessary.
  - Update Help Desk ticket.
  - Education user on how to avoid phishing scams (See **Education** section below).

EDUCATION

- Educate the user on how to avoid malware and avoid phishing scams. https://www.microsoft.com/Security/portal/mmpc/help/infection.aspx
- For machines not on our network, educate the users on bringing in UT laptops so updates occur. Also let them know that free anti-virus information is available on the https://myutaccount.utoledo.edu website.
- Educate the user about *H:\ for Home or Personal folder use* and the *Z:\ for departmental shares*.
- See the IT Security site for additional details at http://www.utoledo.edu/it/security.

Terms and Reference Sites

Current SCEP Threat Categories:

Adware, Backdoor, Behavior, Browser Modifier, Exploit, Hack Tool, Program Unwanted, Password Stealer, Potential Unwanted Software, Ransomware, Trojan Dropper, Trojan Downloader, Trojan DDoS, Trojan Monitoring Software, Stealth Notifier, Software Bundler, Settings Modifier, Virus Tool, Worm.

How does malware infect your PC? – Education Material

https://www.microsoft.com/Security/portal/mmpc/help/infection.aspx

Microsoft Malware Encyclopedia

https://www.microsoft.com/Security/portal/threat/threats.aspx

Free Scan Tools

https://www.microsoft.com/Security/scanner/en-us/default.aspx

http://www.mcafee.com/us/downloads/free-tools/stinger.aspx also available in SCCM Application Catalog

Bootable Scan Tools

http://pcsupport.about.com/od/system-Security/tp/free-bootable-antivirus-software.htm