Alex Smetana

CIS361

04/14/2023

*Part 1 - Refer to the SANS Incident Handlers Handbook (https://www.sans.org/white-papers/33901/Links to an external site.) - Using this as a guide, put together an equipment list for an incident response team using Amazon, Newegg, or any other major online retailer.*

## Accident and Incident Logbook

Used for documentation of the who, what, where when and why during an incident.

Price: $3.57

| | |
|---|---|
| | Accident & Incident Log: Black Leather: Record Accidents & Injuries in your Business, Store, Company, Shop, Restaurant, Hotel, Home & more. \| Journal, ... \| 8”x 10” Large \| 100 pages<br><br>https://www.amazon.com/Accident-Incident-Log-Accidents-Restaurant/dp/1539660346/ref=sr_1_4?crid=2EMWEZMMM2A5A&keywords=Incident+handler+journals&qid=1681511157&sprefix=incident+handler+journals%2Caps%2C133&sr=8-4 |

## USB Flash Storage

Flash Storage designed for the purpose of having up to data AV Software that can read and write to a computer in the event of an incident response. Preference to as much as storage as practical with a minimum of 8GB of storage.

Price: $28.61 (10 pack) or $2.81 per USB

| | |
|---|---|
| | 32GB USB 2.0 Flash Drive Pnstaw Swivel Memory Stick Thumb Drive Pen Drives Jump Drive for Data Storage, File Sharing(10 Pack,Multi-Color)(32GB)<br><br>https://www.amazon.com/Pnstaw-Swivel-Storage-Sharing-Multi-Color/dp/B07DNQ92F2/ref=sr_1_2_sspa?crid=2KVM2VEG9Z2K7&keywords=USB%2BDrives&qid=1681511253&sprefix=usb%2Bdrives%2Caps%2C129&sr=8-2-spons&spLa=ZW5jcnlwdGVkUXVhbGlmaWVyPUExMDJFSFg3SzBKNUlVJmVuY3J5cHRlZElkPUEwNjk1MjE1RDU1V00wU1dKVEszJmVuY3J5cHRlZEFkSWQ9QTAxOTk3MjIyTDRLNDIyOTA1UllDJndpZGdldE5hbWU9c3BfYXRmJmFjdGlvbj1jbGlja1JlZGlyZWN0JmRvTm90TG9nQ2xpY2s9dHJ1ZQ&th=1 |

## Computer and Network Repair Toolkit

Basic toolkit used to fix hardware with the ability to both add and remove components. In the event of an incident response, it is vital to have access to tools to help with any physical hardware issues.

Price: $39.99

| | |
|---|---|
| | Hi-Spec 39pc Electronics Repair & Opening Tool Kit Set for Laptops, Phones, Devices, Computer & Gaming Accessories. Precision Small Screwdrivers with Pentalobe Bits for iPhones & MacBooks<br>https://www.amazon.com/Hi-Spec-Electronics-Computers-Controllers-Gadgets/dp/B08HRXXHN4/ref=sr_1_1_sspa?crid=1HZ0T8LU3U01N&keywords=computer%2Band%2Bnetwork%2Btool%2Bkit&qid=1681511328&sprefix=computer%2Band%2Bnetwork%2Btool%2Bkit%2Caps%2C130&sr=8-1-spons&spLa=ZW5jcnlwdGVkUXVhbGlmaWVyPUExSkVPRklETDJVM1o3JmVuY3J5cHRlZElkPUEwMzI4ODIyMzgwSklGSjRNMDJaUiZlbmNyeXB0ZWRBZElkPUEwMDMxMjgzMzVEVjVFTEE5NDA5USZ3aWRnZXROYW1lPXNwX2F0ZiZhY3Rpb249Y2xpY2tSZWRpcmVjdCZkb05vdExvZ0NsaWNrPXRydWU&th= |

## Computer- Laptops

Either can be desktops or laptops. Used to have forensic software, logging software and anti-malware utilities. Ideally with up-to-date specs with a minimum of 16gbs of ram, i7 processor, and 500 gb storage (preferably ssd).  The two models below include Apple and Windows machines that meet those requirements however expensive.

Price: $1699 (Apple)

| | |
|---|---|
| | Apple 2022 MacBook Pro Laptop with M2 chip: 13-inch Retina Display, 16GB RAM, 512GB SSD Storage, Touch Bar, Backlit Keyboard, FaceTime HD Camera. Works with iPhone and iPad; Space Gray<br>https://www.amazon.com/Apple-2022-MacBook-Laptop-chip/dp/B0B8TGFLY2/ref=sr_1_1?crid=218SW5G9X2NJ2&keywords=Macbook%2B16%2Bgb%2Bram&qid=1681510336&sprefix=macbook%2B16%2Bgb%2Bram%2Caps%2C127&sr=8-1&th=1 |

Price: $1385 (Microsoft)

| | |
|---|---|
| | Microsoft Surface Pro 9 (2022), 13" 2-in-1 Tablet & Laptop, Thin & Lightweight, Intel 12th Gen i7 Fast Processor for Multi-Tasking, 16GB RAM, 256GB Storage with Windows 11, Graphite<br>https://www.amazon.com/Microsoft-Lightweight-Processor-Multi-Tasking-Graphite/dp/B0B9PWT1MX/ref=sr_1_1?crid=37Q2LM0SZW3TW&keywords=surface%2B16gb%2Bram%2Bi7&qid=1681510737&s=books&sprefix=surface%2B16gb%2Bram%2Bi7%2Cstripbooks%2C116&sr=1-1&th=1 |

## External Hard drives

Used for backup of storage/forensic data storage. Either SSD or disc however, preferably a minimum of 1 TB storage. Depends on the budget.

Price: $198 (Non SSD)

| | |
|---|---|
| | WD 10TB Elements Desktop External Hard Drive, USB 3.0 external hard drive for plug-and-play storage - WDBWLG0100HBK-NESN<br><br>https://www.amazon.com/10TB-Elements-Desktop-Drive-WDBWLG0100HBK-NESN/dp/B07G3QMPB5/ref=sr_1_4?crid=30VIF2GQ3D0WA&keywords=10%2Btb%2Bexternal%2Bharddrive%2Bssd&qid=1681510447&sprefix=10%2Btb%2Bexternal%2Bhardrive%2Bssd%2Caps%2C120&sr=8-4&th=1 |

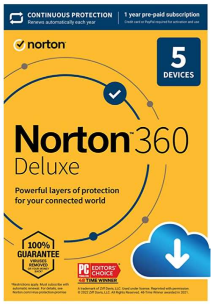
Price: $139 (SSD)

| | |
|---|---|
| | SanDisk 2TB Extreme Portable SSD - Up to 1050MB/s - USB-C, USB 3.2 Gen 2 - External Solid State Drive - SDSSDE61-2T00-G25<br><br>https://www.amazon.com/SanDisk-2TB-Extreme-Portable-SDSSDE61-2T00-G25/dp/B08HN37XC1/ref=sr_1_1_sspa?crid=30VIF2GQ3D0WA&keywords=10%2Btb%2Bexternal%2Bharddrive%2Bssd&qid=1681510447&sprefix=10%2Btb%2Bexternal%2Bhardrive%2Bssd%2Caps%2C120&sr=8-1-spons&spLa=ZW5jcnlwdGVkUXVhbGlmaWVyPUExWjQ5NkJOWVY2UTI5JmVuY3J5cHRlZElkPUEwMTQyODU1RktCVU41U09ZNVhNJmVuY3J5cHRlZEFkSWQ9QTAxMzg4NzlLU0lCRzVXVzVNU0Qmd2lkZ2V0TmFtZT1zcF9hdGYmYWN0aW9uPWNsaWNrUmVkaXJlY3QmZG9Ob3RMb2dDbGljaz10cnVl&th=1 |

## Antivirus Software

AV software in a 5 pack.

Price: $139 (5 Pack)

| | |
|---|---|
|  CONTINUOUS PROTECTION<br>Renews automatically each year<br>1 year pre-paid subscription<br>norton<br>5 DEVICES<br>Norton 360<br>Deluxe<br>Powerful layers of protection for your connected world<br>100% GUARANTEE<br>PC EDITORS' CHOICE | Norton 360 Deluxe, 2023 Ready, Antivirus software for 5 Devices with Auto Renewal - Includes VPN, PC Cloud Backup & Dark Web Monitoring [Download]<br><br>https://www.amazon.com/NEW-Norton-360-Deluxe-Monitoring/dp/B07Q33SJDW/ref=sr_1_4?crid=3KWZ0WI7UEVZQ&keywords=antimalware%2Bsoftware%2B2023&qid=1681510603&sprefix=antimalware%2Bsoftware%2B2023%2Caps%2C121&sr=8-4&th=1 |

## Hard Drive Duplicator

Hard Drive allowing to make copies of hard drives. Useful in the event of an incident response to make forensic copies of hard drives. Depends on size of business and budget.

Price: $255

| | |
|---|---|
| | Systor 1:1 HDD/SSD Hard Drive Duplicator - 5.4GB/Min - Standalone Copier & Eraser/Sanitizer for Multiple SATA 3.5 Disk & 2.5 Solid State Drives - Copy Speeds of up to 90MB/Sec (SYS101HS-DP)<br>https://www.amazon.com/Systor-Systems-Duplicator-Sanitizer-SYS101HS-DP/dp/B00DWICN66/ref=sr_1_1_sspa?crid=2PFUGIGIY74YK&keywords=hard+drive+duplicator&qid=1681511425&sprefix=hard+duplica%2Caps%2C130&sr=8-1-spons&psc=1&smid=A30PGHIJ94I2C1&spLa=ZW5jcnlwdGVkUXVhbGlmaWVyPUEzMk1TMjdJRUFaWEdSJmVuY3J5cHRlZElkPUEwOTk3OTM2MkJDN1pTSDNTQlIwUiZlbmNyeXB0ZWRBZElkPUEwODU1MTc5MVhERFAwSjRPODZCMCZ3aWRnZXROYW1lPXNwX2F0ZiZhY3Rpb249Y2xpY2tSZWRpcmVjdCZkb05vdExvZ0NsaWNrPXRydWU= |

Price: $1370 (SSD)

| | |
|---|---|
| | Systor 1:11 HDD/SSD Hard Drive Duplicator - 5.4GB/Min - Standalone Copier & Eraser/Sanitizer for Multiple SATA 3.5 Disk & 2.5 Solid State Drives - Copy Speeds of up to 90MB/Sec (SYS1011HS-DP)<br>https://www.amazon.com/Systor-Systems-Duplicator-Sanitizer-SYS1011HS-DP/dp/B01K5XTVNI/ref=sr_1_10?crid=2PFUGIGIY74YK&keywords=hard%2Bdrive%2Bduplicator&qid=1681511425&sprefix=hard%2Bduplica%2Caps%2C130&sr=8-10&th=1 |

## Forensic Software

Price: Open Software

| | |
|---|---|
| | Autopsy<br>https://www.autopsy.com/download/ |

Price: Perputual License: $3,995 One Year License: $2,227

| | |
|---|---|
| FTK® Forensic Toolkit<br>The Gold Standard in Digital Forensics For Over 15 Years<br>DOWNLOAD FREE FTK® IMAGER<br>SCHEDULE A MEETING | FTK<br>https://www.exterro.com/forensic-toolkit |

Part 2 - Choose one of the incident playbooks from this site (https://www.incidentresponse.org/playbooks/Links to an external site.) and submit a guide for first responders for ONE of these incidents. As a guide for first responder, it should focus on the following:

# Malware Outbreak – First Responder Guide

## Preparation

1. Conduct regular awareness training.
    a. Educating the people in the company is critical to reducing malware outbreaks. Conduct seasonal awareness training and send out regular phishing scams throughout the company.
2. Define the members of the Incident Response Team
    a. Determine the Teams Roles. Assign team members to roles that they are qualified for that work with each other's strengths.
    b. Keep up to date on training. Make sure that the team is well prepared and ready to jump into action to deal with an incident response at any time.
3. Acquire the necessary tools (hardware and software) to assist in malware incident handling.
    a. Having up-to-date tools is vital in the event of an incident response. For example, this would include AV software, computers, and forensic software.
4. Define Escalation Paths
    a. Escalation paths are crucial as incidents may increase or decrease as information is gathered.
5. Backup of Systems
    a. Backups of information should be kept securely and reviewed at the start of any incident.
    b. Backups should be updated periodically and determined that it is up to date.

## Detection + Analyzation

1. Monitor for Threat Indicators
    a. Monitor the network flow- determine any unknown or unexpected in going or out. This can be done through packet analyzing software such as Packet Tracer.
    b. Determine if there is any degraded processing capability.
    c. Always monitor your AV software. It is important to check if it has any out of the ordinary behavior. For example, AV gets disabled for any unknown reason.
2. Define the Risk Factors.
    a. Determine the risk of PII of customer and employee data being affected.
    b. Determine the risk factors that are posed to the business.
3. Investigate Malware to determine its characteristics.
    a. Preserve a Forensic copy of the malware. Most importantly, this includes getting its hash value.
    b. Analyze the Malware into software (Example: Virus Total) to determine its classification.
    c. Determine the affected range of the malware. The spread of malware is crucial to identifying the spread of compromised information.
    d. Understanding as much information about the malware's behavior will be useful in containing the outbreak.

## Containment

1. Determine the reach of the outbreak.
    a. Identify the Systems that have been affected and isolate them. For example, examining your desktops, laptops, servers, and VM's.
2. Determine what information has been compromised.
    a. Document any compromised information. It is crucial to know what information was compromised. It is important to isolate the information to prevent more information from being compromised.
3. Determine how the malware gained access.
    a. Determine the vulnerability being exploited. This is crucial to the containment of the malware. If it was determined how the malware gained access, then the vulnerability should be blocked.
    b. View reports and record details.
4. Preserve any evidence found for forensic review.
    a. Any evidence found will be helpful later to help prevent any sort of outbreak from happening in the future.
5. Identify what tools were used to detect the incident.
    a. For example, firewalls, scanners, and AV software.

## Eradication

1. Stop the spread of the Malware.
    a. If malware was determined to be spreading through the firewalls, strengthen them to help stop the spread. For example:
        i. Adjust Firewall and AV settings.
        ii. Disable any services,
        iii. Run in sand box.
2. Preserve any artifacts, systems, and relevant backups.
    a. It is crucial that the information be taken and documented. Any information will be helpful in the recover stage.
3. Eradication of Malware
    a. Once all the data is preserved, remove the malware. Use any tools necessary to remove it. For example, clean/quarantine with AV or malware removal tool.

## Recover

1. Recover Systems
    a. Once the malware has been eradicated, restore the systems back to original state (if backups are available).
2. Recover Lost Data
    a. If any data was lost, try your best to recover the data.
3. Perform an incident review.
    a. Determine the cause and effect of the malware outbreak.
    b. Make changes to prevent another outbreak from happening again.
4. Follow data breach laws.
    a. If a data breach occurs, comply with all state data breach laws.

## Resources

*Guide to Malware Incident Prevention and Handling for Desktops ... - NIST*. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-83r1.pdf.

"Malware Incident Response Playbook." *FRSecure*, 16 Dec. 2022, https://frsecure.com/malware-incident-response-playbook/.

"Malware Outbreak: Incident Response Playbooks Gallery." *Incident Response Consortium*, https://www.incidentresponse.org/playbooks/malware-outbreak.