04- Identifying Social Engineering and Malware

Ahmed Sultan
Senior Technical Instructor
ahmedsultan.me/about

Outlines

4.1- Compare and Contrast Social Engineering

4.2- Analyze Indicators of Malware-Based Attacks

Labs

Lab 5: Installing, Using, and Blocking a Malware-based Backdoor

4.1- Compare and Contrast Social Engineering

4.2- Analyze Indicators of Malware-Based Attacks

SOCIAL ENGINEERING

- Adversaries can use a diverse range of techniques to compromise a security system.
- A prerequisite of many types of attacks is to obtain information about the network and security system.
- **Social engineering** refers to means of either eliciting information from someone or getting them to perform some action for the threat actor.
- **Social engineering** is one of the most common and successful malicious techniques, Because it exploits basic human trust.
- It can also be referred to as "hacking the human".

SOCIAL ENGINEERING (cont.)

- Typical social engineering intrusion scenarios include:
  - ✓An attacker creates an executable file that prompts a network user for their password, and then records whatever the user inputs, The attacker then emails the executable file to the user with the story that the user must double-click the file and log on to the network again to clear up some logon problems the organization has been experiencing that morning, After the user complies, the attacker now has access to their network credentials.
  - ✓An attacker contacts the help desk pretending to be a remote sales representative who needs assistance setting up remote access, Through a series of phone calls, the attacker obtains the name/address of the remote access server and login credentials, in addition to phone numbers for remote access and for accessing the organization's private phone and voice-mail system.

IMPERSONATION

- **Impersonation** simply means pretending to be someone else.
- It is one of the basic social engineering techniques.
- Impersonation is possible where the target cannot verify the attacker's identity easily, such as **over the phone** or via an **email message**.
- The classic impersonation attack is for the social engineer to phone into a department, claim they have to adjust something on the user's system remotely, and get the user to reveal their password.

DUMPSTER DIVING AND TAILGATING

- **Dumpster Diving**
  - ✓ Dumpster diving refers to combing through an organization's (or individual's) garbage to try to find useful documents (or even files stored on discarded removable media).

- **Tailgating**
  - ✓ Tailgating is a means of entering a secure area without authorization by following close behind the person that has been allowed to open the door or checkpoint.

PIGGY BACKING

- **Piggy backing**
  - ✓is a similar situation, but means that the attacker enters a secure area with an employee's permission.
  - ✓Alternatively, piggy backing may be a means of an insider threat actor to allow access to someone without recording it in the building's entry log.

IDENTITY FRAUD

- **Identity fraud**
  - ✓is a specific type of impersonation where the attacker uses specific details of someone's identity.
  - ✓A typical consumer identity fraud is using someone else's name and address to make a loan application or using stolen credit card details to start a mobile phone contract.

- **Note:**
  - ✓**Identity Fraud:** making up an identity.
  - ✓**Identity Theft:** stealing someone else's identity.

SHOULDER SURFING AND LAUNCHTIME ATTACKS

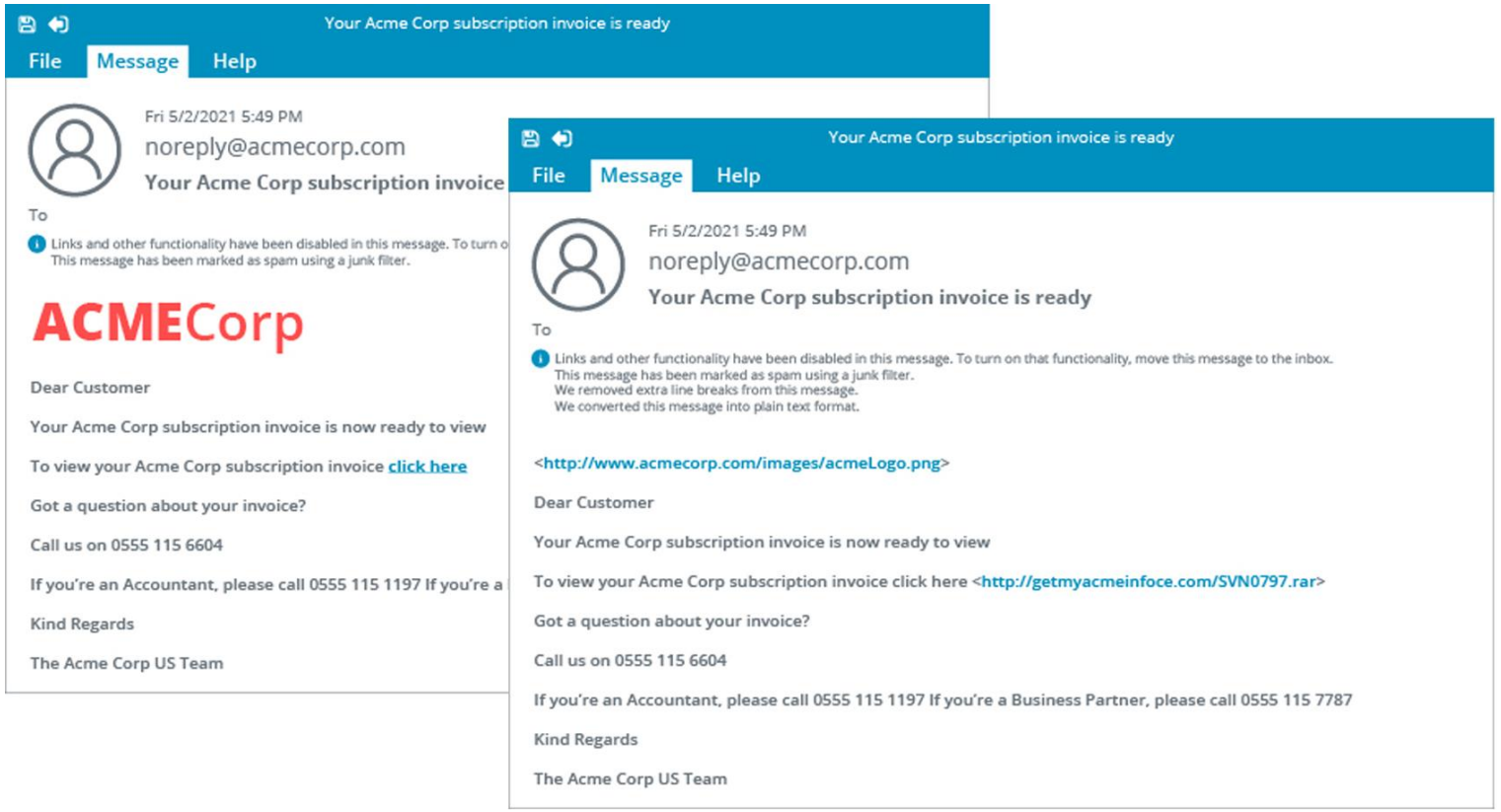
- **Shoulder Surfing**
  - ✓a threat actor can learn a password or PIN (or other secure information) by watching the user type it.
  - ✓Despite the name, the attacker may not have to be in close proximity to the target—they could use high-powered binoculars or CCTV to directly observe the target remotely.

- **Lunchtime attacks**
  - ✓If a user leaves a workstation unattended while logged on, an attacker can physically gain access to the system.
  - ✓Most operating systems are set to activate a password-protected screen saver after a defined period of no keyboard or mouse activity, Users should also be trained to lock or log off the workstation whenever they leave it unattended.

PHISHING

- **Phishing**
  - ✓is a combination of social engineering and spoofing.
  - ✓It persuades or tricks the target into interacting with a malicious resource disguised as a trusted one, traditionally using email as the vector.
  - ✓A phishing message might try to convince the user to perform some action, such as installing disguised malware or allowing a remote access connection by the attacker.
  - ✓Other types of phishing campaign use a spoof website set up to imitate a bank or e-commerce site or some other web resource that should be trusted by the target.
  - ✓The attacker then emails users of the genuine website informing them that their account must be updated or with some sort of hoax alert or alarm, supplying a disguised link that actually leads to the spoofed site.
  - ✓When the user authenticates with the spoofed site, their logon credentials are captured.

PHISHING (cont.)



SPEAR PHISHING

- **Spear phishing**
  - ✓a phishing scam where the attacker has some information that makes an individual target more likely to be fooled by the attack.
  - ✓Each phishing message is tailored to address a specific target user.
  - ✓The attacker might know the name of a document that the target is editing, for instance, and send a malicious copy, or the phishing email might show that the attacker knows the recipient's full name, job title, telephone number, or other details that help convince the target that the communication is genuine.

WHALING AND VISHING

- **Whaling**
  - ✓ a spear phishing attack directed specifically against upper levels of management in the organization (CEOs and other "big fish").
  - ✓ Upper management may also be more vulnerable to ordinary phishing attacks because of their reluctance to learn basic security procedures.

- **Vishing**
  - ✓ a phishing attack conducted through a voice channel (telephone or VoIP, for instance).
  - ✓ For example, targets could be called by someone purporting to represent their bank asking them to verify a recent credit card transaction and requesting their security details.
  - ✓ It can be much more difficult for someone to refuse a request made in a phone call compared to one made in an email.

SPAM AND HOAXES

- **Spam**
  - ✓ is used as the vector for many attacks.
  - ✓ Threat actors harvest email addresses from marketing lists or databases of historic privacy breaches, or might try to target every email address at a certain company.

- **Hoaxes**
  - ✓ An email alert or web pop-up will claim to have identified some sort of security problem, such as virus infection, and offer a tool to fix the problem.
  - ✓ The tool ofcourse will be some sort of Trojan application.

4.1- Compare and Contrast Social Engineering

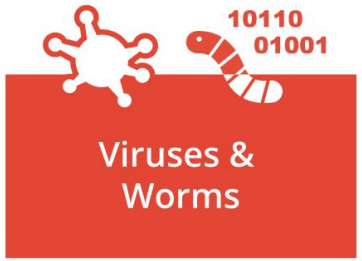
4.2- Analyze Indicators of Malware-Based Attacks

MALWARE CLASSIFICATION

- Many of the intrusion attempts perpetrated against computer networks depend on the use of malicious software, or malware.
- **Malware** is usually simply defined as software that does something bad, from the perspective of the system owner.
- Some malware classifications, such as **Trojan**, **virus**, and **worm**, focus on the vector used by the malware.
- The vector is the method by which the malware executes on a computer and potentially spreads to other network hosts.

MALWARE CATEGORIES

- **Viruses and worms**
  - ✓These represent some of the first types of malware and spread without any authorization from the user by being concealed within the executable code of another process.
  - ✓These type of malware is primarily designed to replicate, but may drop any type of payload.



MALWARE CATEGORIES (cont.)

- **Trojan**
  - ✓Malware concealed within an installer package for software that appears to be legitimate.
  - ✓This type of malware does not seek any type of consent for installation and is actively designed to operate secretly.

MALWARE CATEGORIES (cont.)

- **Potentially unwanted programs (PUPs)**
  - ✓Software installed alongside a package selected by the user or perhaps bundled with a new computer system.
  - ✓Unlike a Trojan, the presence of a PUP is not automatically regarded as malicious.
  - ✓It may have been installed without active consent or consent from a purposefully confusing license agreement.
  - ✓This type of software is sometimes described as grayware rather than malware.

COMPUTER VIRUSES

- A computer virus is a type of malware designed to replicate and spread from computer to computer, usually by "infecting" executable applications or program code.
- There are several different types of viruses and they are generally classified by the different types of file or media that they infect:

✓ Non-resident/file infector—the virus is contained within a host executable file and runs with the host process, The virus will try to infect other process images on persistent storage and perform other payload actions, It then passes control back to the host program.

✓ Memory resident—when the host file is executed, the virus creates a new process for itself in memory, The malicious process remains in memory, even if the host process is terminated.

COMPUTER VIRUSES (cont.)

- There are several different types of viruses and they are generally classified by the different types of file or media that they infect (cont.)

  - ✓ Boot—the virus code is written to the disk boot sector or the partition table of a fixed disk or USB media, and executes as a memory resident process when the OS starts or the media is attached to the computer.

  - ✓ Script and macro viruses—the malware uses the programming features available in local scripting engines for the OS and/or browser, such as PowerShell, Windows Management Instrumentation (WMI), JavaScript, Microsoft Office documents with Visual Basic for Applications (VBA) code enabled, or PDF documents with JavaScript enabled.

COMPUTER VIRUSES (cont.)

- What these types of viruses have in common is that they must infect a host file or media.
- An infected file can be distributed through any normal means—on a disk, on a network, as an attachment to an email or social media post, or as a download from a website.

COMPUTER WORMS

- A computer worm is memory-resident malware that can run without user intervention and replicate over network resources.
- A virus is executed only when the user performs an action such as downloading and running an infected executable process, attaching an infected USB stick, or opening an infected Word document with macros enabled.
- By contrast, a worm can execute by exploiting a vulnerability in a process when the user browses a website, runs a vulnerable server application, or is connected to an infected file share.

COMPUTER WORMS (cont.)

- The primary effect of the first types of computer worm is to rapidly consume network bandwidth as the worm replicates.
- A worm may also be able to crash an operating system or server application (performing a **Denial of Service attack**).
- Also, like viruses, worms can carry a payload that may perform some other malicious action.

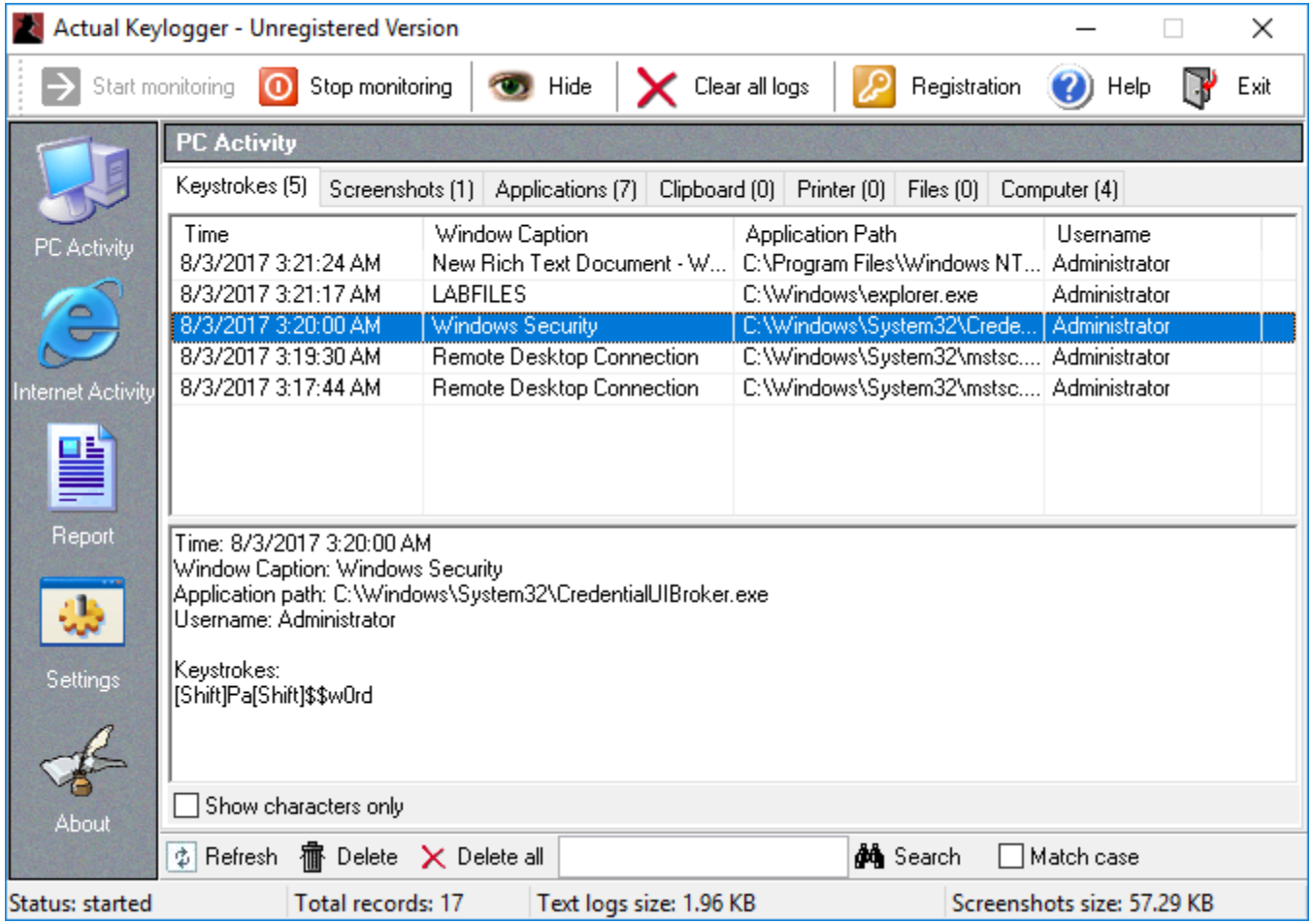
SPYWARE, KEYLOGGERS AND ADWARE

- **Spyware**
  - ✓ This is malware that can perform adware-like tracking, but also monitor local application activity, take screenshots, and activate recording devices, such as a microphone or webcam.

- **Keylogger**
  - ✓ Is spyware that actively attempts to steal confidential information by recording keystrokes.
  - ✓ The attacker will usually hope to discover passwords or credit card data.

- **Adware**
  - ✓ This is a class of PUP/grayware that performs browser reconfigurations, such as allowing changing default search providers, opening sponsor's pages at startup, adding bookmarks, and so on, Adware may be installed as a program or as a browser extension/plug-in.

SPYWARE, KEYLOGGERS AND ADWARE (cont.)



BACKDOORS AND REMOTE ACCESS TROJANS (RAT)

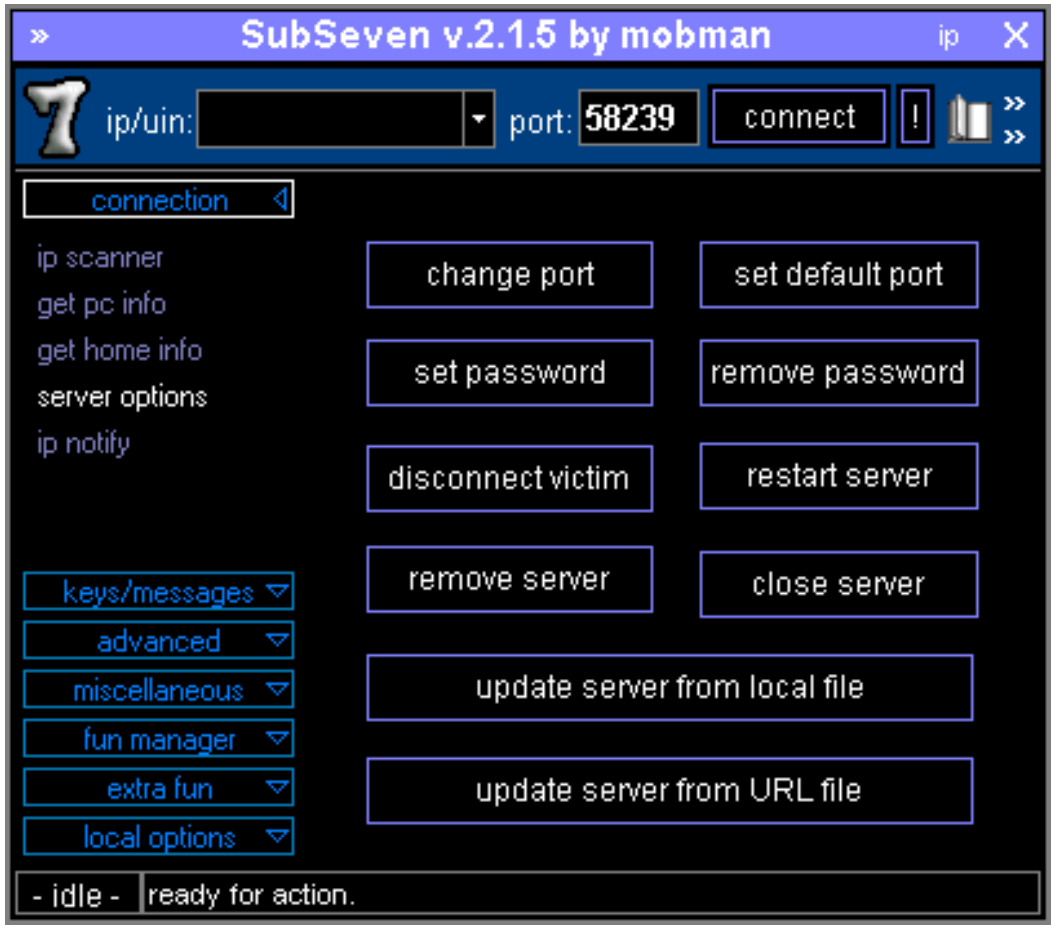
- **Backdoor**
  - ✓ Is any type of access method to a host that circumvents the usual authentication method and gives the remote user administrative control.

- **A remote access trojan (RAT)**
  - ✓ Is backdoor malware that mimics the functionality of legitimate remote control programs, but is designed specifically to operate covertly.
  - ✓ Once the RAT is installed, it allows the threat actor to access the host, upload files, and install software.

BACKDOORS AND REMOTE ACCESS TROJANS (RAT) (cont.)

- A compromised host can be installed with one or more bots.
- **A bot** is an automated script or tool that performs some malicious activity.
- A group of bots that are all under the control of the same malware instance can be manipulated as a **botnet.**
- A **botnet** can be used for many types of malicious purpose, including triggering distributed denial of service (DDoS) attacks, launching spam campaigns, or performing cryptomining.

BACKDOORS AND REMOTE ACCESS TROJANS (RAT) (cont.)



BACKDOORS AND REMOTE ACCESS TROJANS (RAT) (cont.)

- NOTE:

  - *Backdoors can be created in other ways than infection by malware.*
  - *Programmers may create backdoors in software applications for testing and development that are subsequently not removed when the application is deployed.*
  - *Backdoors are also created by misconfiguration of software or hardware that allows access to unauthorized users.*
  - ***Examples:** include leaving a router configured with the default administrative password, having a Remote Desktop connection configured with an unsecure password, or leaving a modem open to receive dial-up connections.*

ROOTKITS

- In Windows, malware can only be manually installed with local administrator privileges.
- This means the user must be confident enough in the installer package to enter the credentials or accept the User Account Control (UAC) prompt.
- Windows tries to protect the system from abuse of administrator privileges.
- Critical processes run with a higher level of privilege (SYSTEM).
- Consequently, Trojans installed in the same way as regular software cannot conceal their presence entirely and will show up as a running process or service.

ROOTKITS (cont.)

- Often the process image name is configured to be similar to a genuine executable or library to avoid detection.
- **For Example:** a Trojan may use the filename "run32d11" to masquerade as "run32dll".
- To ensure persistence (running when the computer is restarted), the Trojan may have to use a registry entry or create itself as a service, which can usually be detected fairly easily.

ROOTKITS (cont.)

- The malware may be able to use an exploit to escalate privileges after installation.
- Malware running with this level of privilege is referred to as a **rootkit**.
- The term derives from UNIX/Linux where any process running as root has unrestricted access to everything from the root of the file system down.

RANSOMWARE AND CRYPTO-MALWARE

- **Ransomware**
  - ✓ Is a type of malware that tries to extort money from the victim.
  - ✓ One class of ransomware will display threatening messages, such as requiring Windows to be reactivated or suggesting that the computer has been locked by the police because it was used to view pornography or for terrorism.
  - ✓ This may apparently block access to the file system by installing a different shell program, but this sort of attack is usually relatively simple to fix.
  - ✓ The **crypto-malware** class of ransomware attempts to encrypt data files on any fixed, removable, and network drives.
  - ✓ If the attack is successful, the user will be unable to access the files without obtaining the private encryption key, which is held by the attacker. If successful, this sort of attack is extremely difficult to mitigate, unless the user has up to date backups of the encrypted files.

RANSOMWARE AND CRYPTO-MALWARE (cont.)

- One example of this is **Cryptolocker**, a Trojan that searches for files to encrypt and then prompts the victim to pay a sum of money before a certain countdown time, after which the malware destroys the key that allows the decryption.

MALWARE INDICATORS

- Given the range of malware types, there are many potential indicators.
- Some types of malware display obvious changes, such as adjusting browser settings or displaying ransom notices.
- If malware is designed to operate covertly, indicators can require detailed analysis of process, file system, and network behavior.

MALWARE INDICATORS (cont.)

- **Antivirus Notifications**
  - ✓ Most hosts should be running some type of antivirus (A-V) software.
  - ✓ These suites are better conceived of as endpoint protection platforms (EPPs) or next-gen A-V.
  - ✓ These detect malware by signature regardless of type, though detection rates can vary quite widely from product to product.
  - ✓ Many suites also integrate with user and entity behavior analytics (UEBA) and use AI-backed analysis to detect threat actor behavior that has bypassed malware signature matching.

MALWARE INDICATORS (cont.)

- **Sandbox Execution**
  - ✓ If it is not detected by endpoint protection, you may want to analyze the suspect code in a sandboxed environment.
  - ✓ A sandbox is a system configured to be completely isolated from its host so that the malware cannot "break out."
  - ✓ The sandbox will be designed to record file system and registry changes plus network activity.
  - ✓ **Cuckoo** is packaged software that aims to provide a turnkey sandbox solution (cuckoosandbox.org).

MALWARE INDICATORS (cont.)

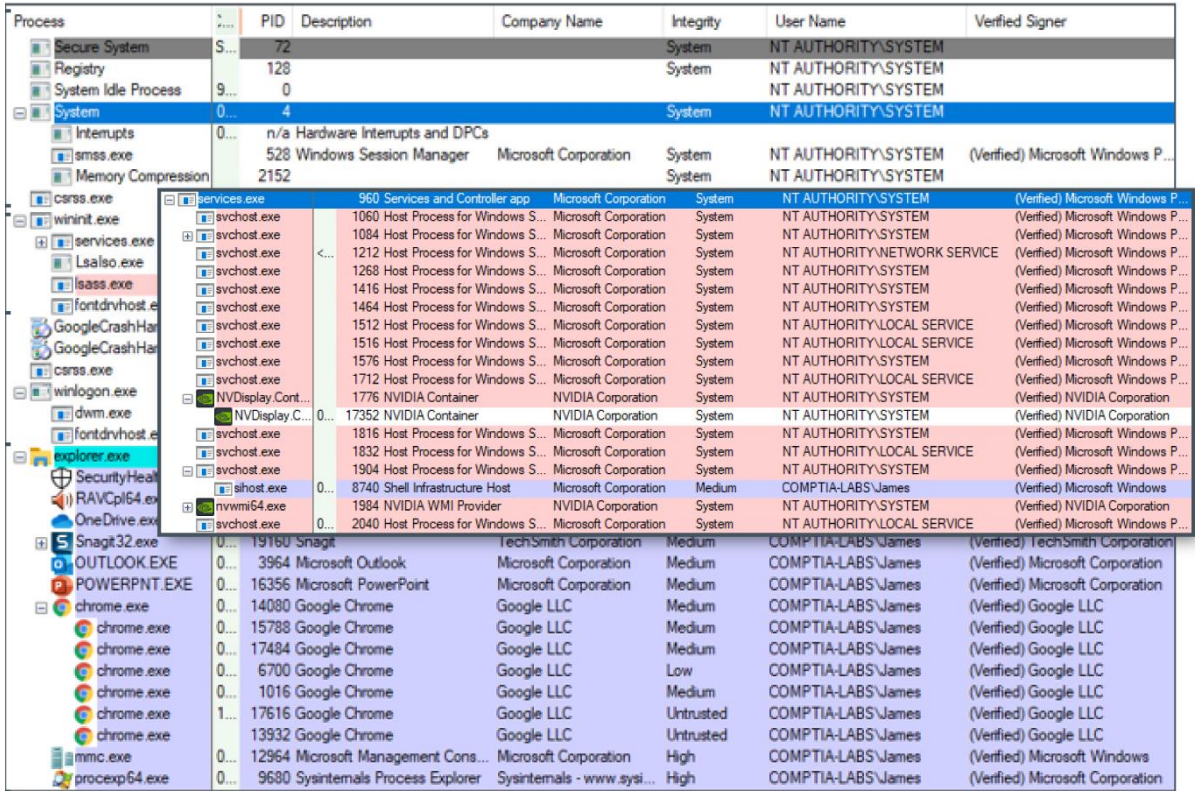
- **Resource Consumption**
  - ✓ Abnormal resource consumption can be detected using a performance monitor, Task Manager, or the **top** Linux utility.
  - ✓ Indicators such as excessive and continuous CPU usage, memory leaks, disk read/write activity, and disk space usage can be signs of malware, but can also be caused by many other performance and system stability issues.
  - ✓ Also, it is only really poorly written malware or malware that performs intensive operations (botnet DDoS and cryptoransomware, for instance) that displays this behavior.
  - ✓ Resource consumption could be a reason to investigate a system rather than definitive proof of infection.

MALWARE INDICATORS (cont.)

- **File System**
  - ✓ While fileless malware is certainly prevalent, file system change or anomaly analysis is still necessary.
  - ✓ Even if the malware code is not saved to disk, the malware is still likely to interact with the file system and registry, revealing its presence by behavior.
  - ✓ A computer's file system stores a great deal of useful metadata about when files were created, accessed, or modified.
  - ✓ Analyzing these metadata and checking for suspicious temporary files can help you establish your timeline of events for an incident that has left traces on a host and its files.

MALWARE INDICATORS (cont.)

- **File System (cont.)**



Lab

Lab 5: Installing, Using, and Blocking a Malware-based Backdoor