Threats, Vulnerabilities, & Countermeasures

Module 7

Module Objectives

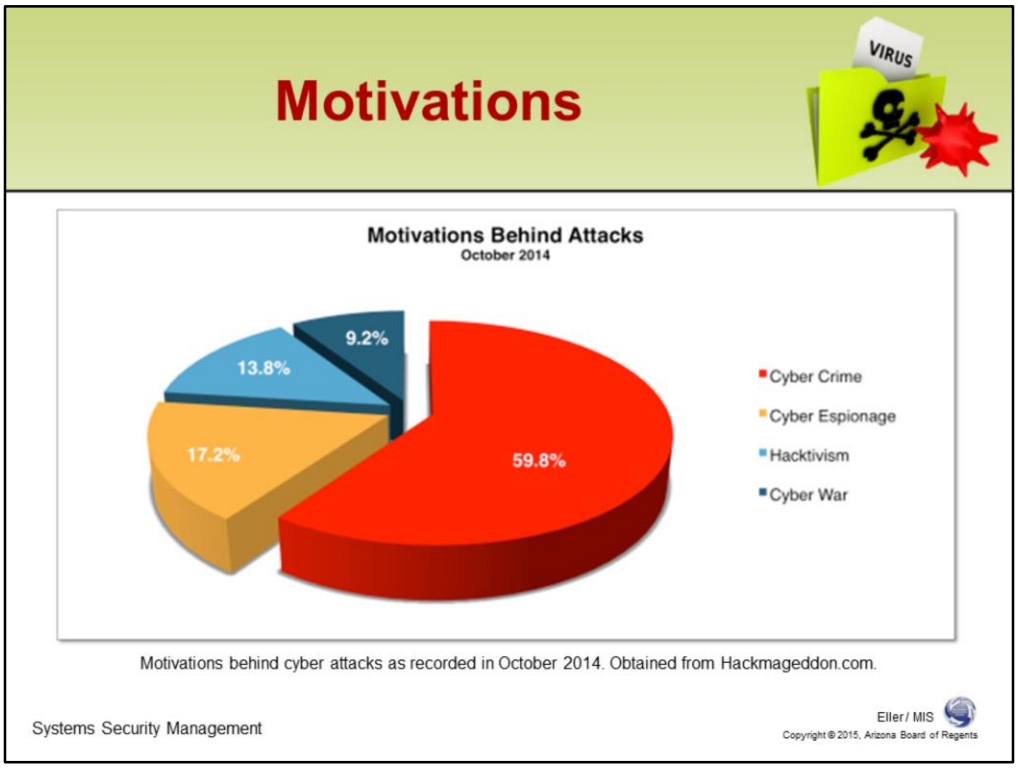
- Viruses
- Virus Classifications
- Worms
- Trojan Horses
- Malicious Software and Automated Tools
- Botnets
- Keystroke Monitoring
- Brute Force & Dictionary Attacks
- Social Engineering
- Tying it All Together
- Awareness, Training, and Education (AT&E) as Countermeasures
- Data Mining
- Database Inference
- Protecting Systems
- Risk Management Concepts
- Next Module…

Systems Security Management

Eller / MIS

At the end of the module, you should be able to:

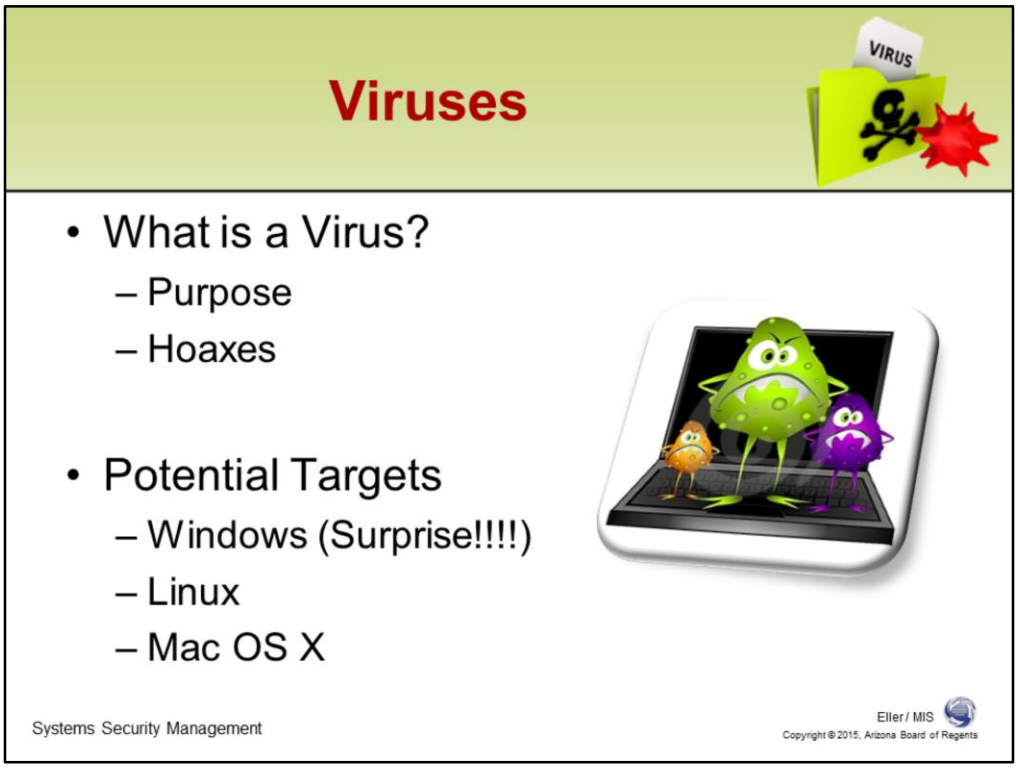
- Describe what a virus is and how virus classification can define the type of virus affecting a system.
- Describe what a worm is and how it differs from a virus.
- Describe what a Trojan horse is and how it differs from a virus or worm.
- Understand the difference between malicious software and automated tools.
- Describe what a botnet is and how it is used.
- Understand what keystroke monitoring and why this is a security risk.
- Understand what brute force and dictionary attacks are and how they are successful.
- Describe the concept of social engineering and how it is used to breach security.
- Understand how awareness, training, and education can all be used as countermeasures.
- Understand data mining and database inference and how they can be used to breach systems.
- Understand how to protect systems.
- Describe basic risk management concepts.



Motivations

Often we hear in the news about cyber attacks that have occured around the world. For years, the most common motivations for cyber attacks include cyber crime, cyber espionage, hacktivism, and cyber warfare. For the month of October 2014, cyber crime "leads the Motivations Behind Attacks chart with nearly 60% (10 points below the previous month, but always at a remarkable level). Cyber Espionage jumps at number two with a new record (17.2%). Hacktivism ranks at number three with a "modest" 13.8%. You will notice also a small presence of attacks related to Cyber War (9.2%)" (Passeri, 2014). With cyber crime, this included brute force attacks against Dropbox and K-Mart. Cyber espionage was the motivation behind attacks against mostly governments and defense contractors; this included the revelation by US-CERT that the BlackEnergy malware toolkit had been discovered hiding inside United States industrial control systems for at least 3 years. Hacktivism continues to be a real threat to organizations and governments alike, with website defacements on Google's Indonesian Search page and various governments including Ukraine, China, and the Pakistan People's Party among many more. The final motivation this month involved cyber warfare which included government launched attacks between India and Pakistan as well as an alleged (and unconfirmed) attack against the Warsaw Stock Exchange.

As you can see there are several motivators for cyber attacks. This module will explain the threats and vulnerabilities that make each of these possible and will discuss ways in which to combat these attempts.



Viruses

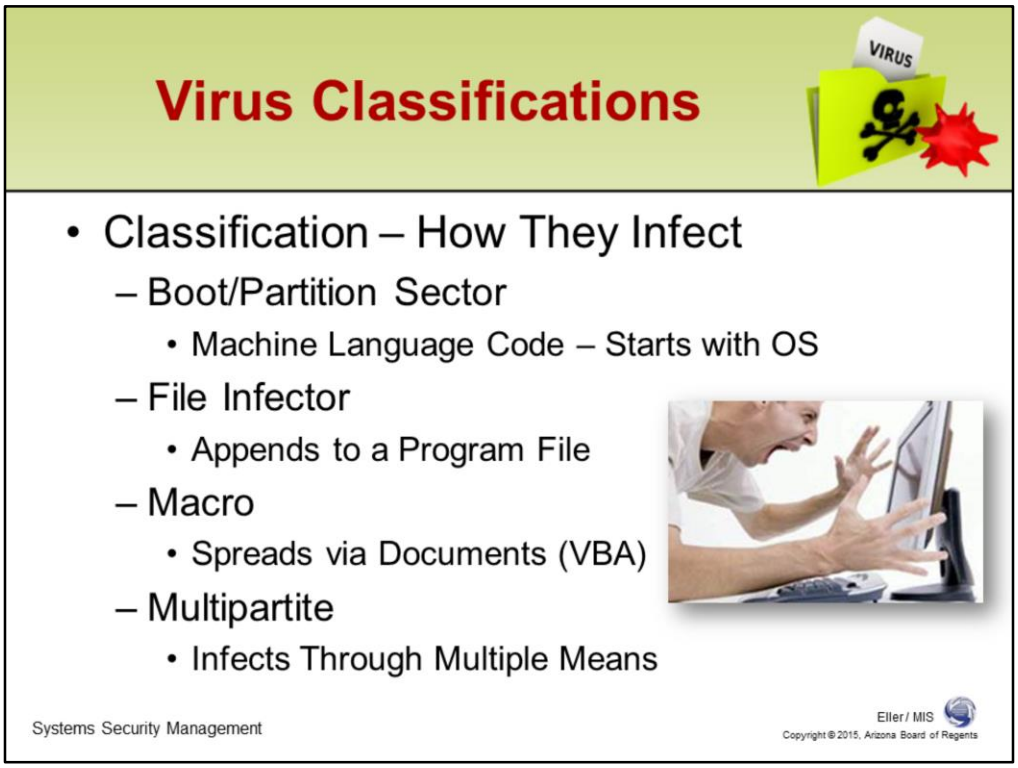
What is a Virus?

Simply put, a virus is a program designed to do something specific, usually something the computer user would consider to be disruptive. In some cases a virus could be used to destroy files on a hard drive while in others it is meant to disrupt productivity by forcing system reboots. In reality, most viruses are written by someone wanting to be able to say they were able to breach a system. Sometimes the purpose of a virus is to hijack a system for financial benefit or to create a network of zombie computers.

In some cases you may have seen an e-mail forwarded from someone you know warning about a specific virus. Sometimes these e-mails contain viruses themselves, other times they are hoaxes meant to scare the recipient into forwarding the e-mail to more people in an effort to continue to spread the hoax. Most people will agree that viruses, regardless of their purpose, are a general pain to have to deal with. Throughout this module we will learn how to identify and reduce the ability for viruses and other malicious software to take hold within our organizations.

Potential Targets

Truthfully, viruses are usually written to target a specific operating system, web browser, or application. In general, a virus can and will target Windows-based systems, Linux-based systems, and even Mac OS X-based systems.



Virus Classifications

Classification Type: How Viruses Infect

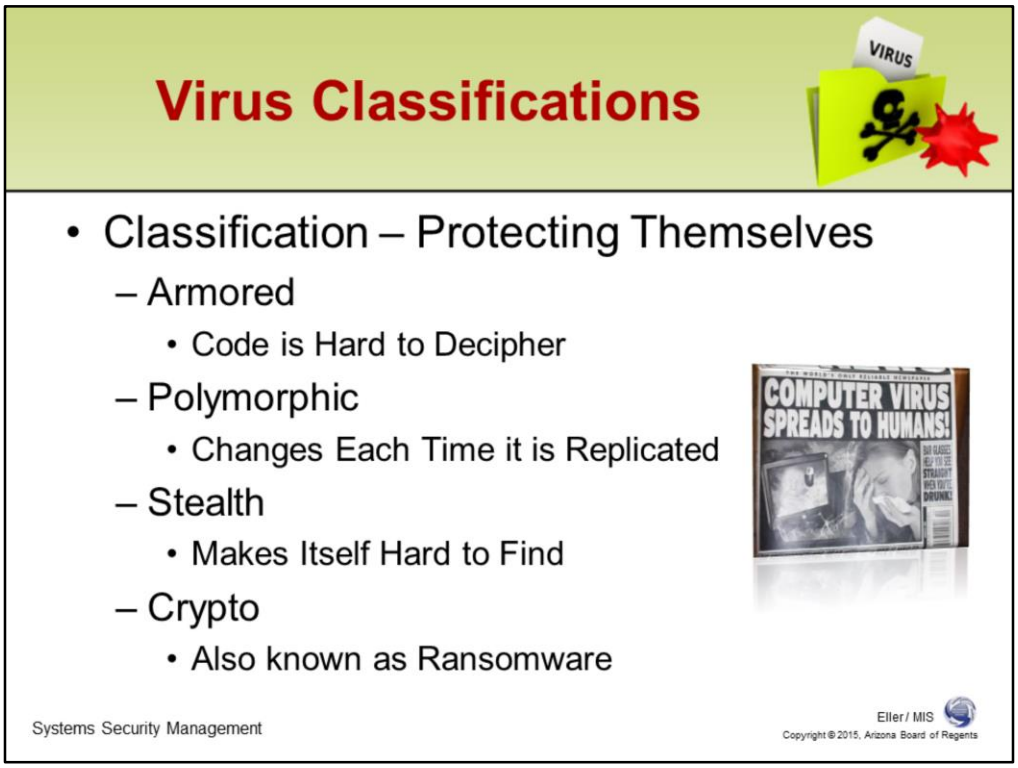
Some viruses are classified by the manner in which they infect computer systems. In general there are four primary classifications for how viruses infect systems, including the following:

Boot/Partition Sector Viruses – Boot or Partition Sector viruses are written in machine language code, so they are very specific to the type of hardware used. For example, a boot sector virus written for PCs will not be able to infect a Mac. In order to affect how the computer operates, the virus will be loaded into memory as the Operating System boots up. This makes the virus much more difficult to remove from the system as it is not running inside the OS, it is running alongside the OS and stored away from the file system.

File Infector Viruses – A file infector virus is designed to append itself to a program file in the OS. For example, if your computer was infected with a file infector virus that attached itself to winword.exe, every time you open Microsoft Word you would execute the virus code as well.

Macro Viruses – Macro viruses are spread through document sharing using the Visual Basic for Applications (VBA) macro language. Macros are small programs that are written to accomplish a specific task automatically. Usually these are written in order to help users be more productive when they have repetitive tasks to accomplish. Virus writers take advantage of this programming language to have infected documents cause a user's computer to execute a set of instructions for malicious purposes.

Multipartite Viruses – Multipartite viruses are designed to infect through multiple means, so the initial infection may come as an e-mail attachment a user opens, then the virus code may be designed to scan that user's address book to replicate itself and send our e-mails to everyone on their list while it also opens a network connection and scans for computers on the local network that are vulnerable to a specific attack in order to further replicate itself.



Virus Classifications (continued)

Classification Type: Protecting Themselves

Some viruses are classified based on how they are written to protect themselves. In other words, how they try to prevent someone from removing them from an infected computer system. Some of the classifications include:

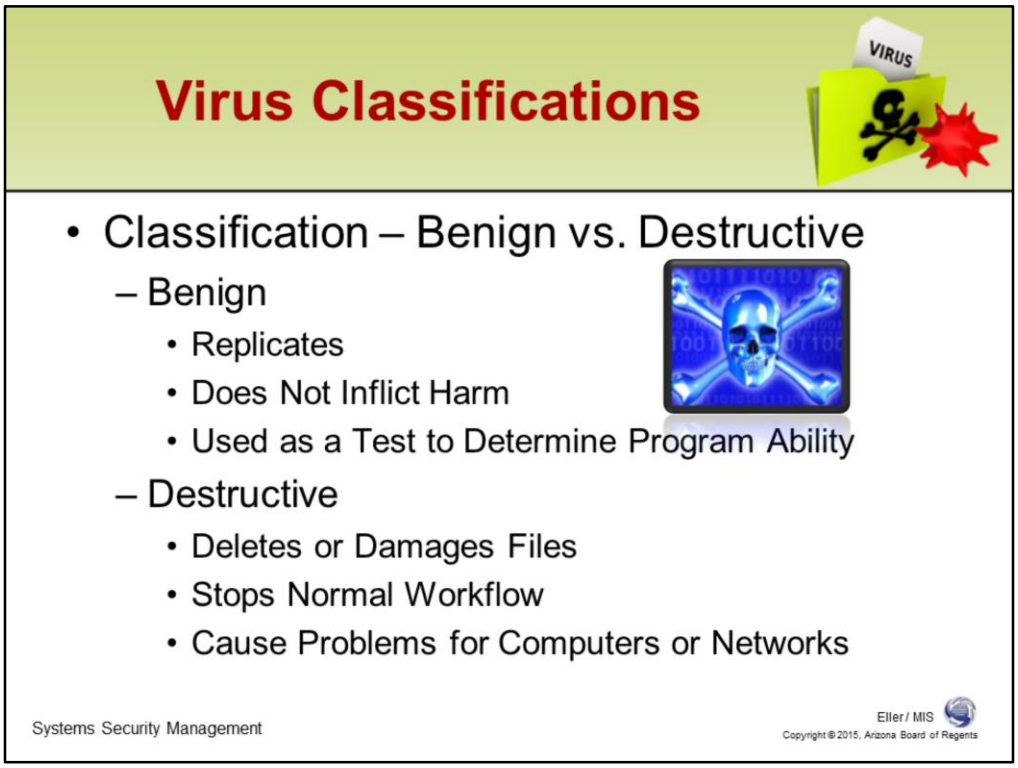
Armored Viruses – The code for an armored virus is designed to be hard to decipher. Sometimes the virus writer will work to make it appear as if the virus was designed to do one thing when in reality it does something completely different. Some may use encryption in order to hide the code from virus researchers to maximize its potential impact.

Polymorphic Viruses – Polymorphic viruses are designed to change every time the virus replicates itself. This is done to try and make it more difficult for virus researchers to come up with effective countermeasures quickly. Think of this as being similar to a mutating virus that infects people and makes existing vaccines irrelevant.

Stealth Viruses – Stealth viruses are designed to hide themselves as effectively as possible. An example of this would be a virus that masks itself as a valid system process (such as svchost.exe) on a Windows system. If you were to open a Task Manager on your Windows-based computer and look at the running processes, you would see several svchost.exe processes running simultaneously. This is completely normal and nothing to worry about, but a clever virus writer could design his or her virus to hide itself as this legitimate process to try and avoid detection.

Crypto Viruses – A crypto virus is a virus that infects a computer, encrypts all the user files and folders and demands a payment in BitCoin within a certain time period to receive the decryption key. If payment is not made, then once the deadline passes, the key is deleted from the Command and Control (CNC) server and the files are permanently unrecoverable.

It is important to note that just because there are different virus classifications does not mean a virus is required to fit into just a single category.



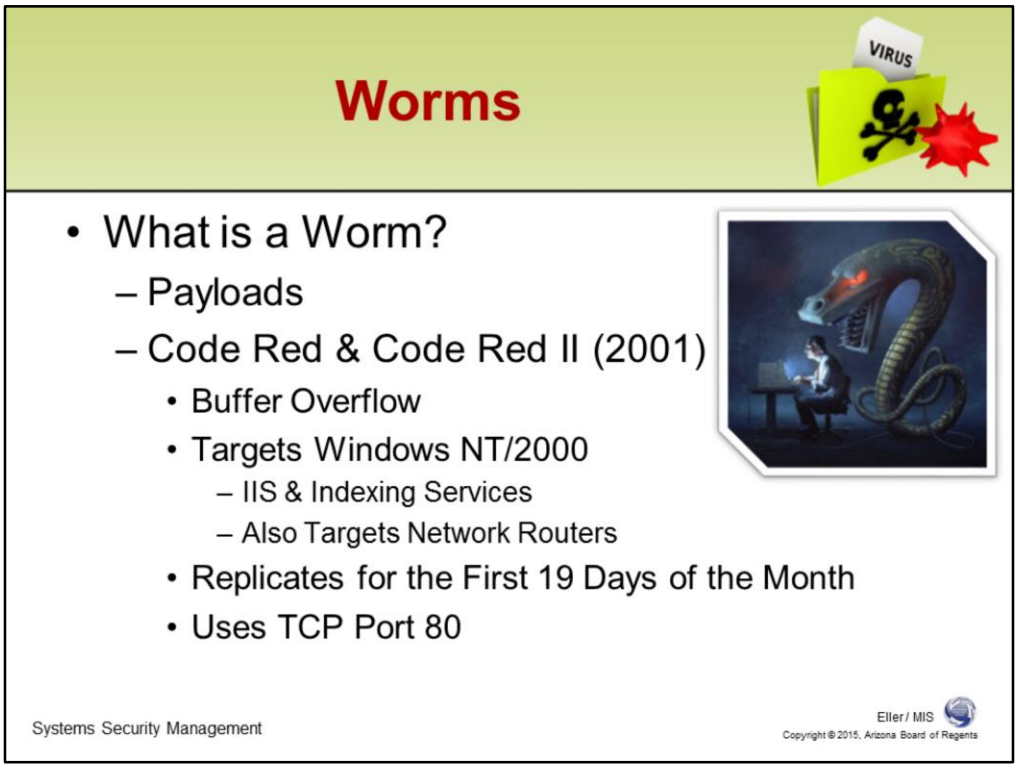
Virus Classifications (continued)

Classification Type: Benign vs. Destructive

Benign – A benign virus is usually a prank virus that does not cause damage. In the late 90s and early 2000s, a prank email was sent around claiming to be a gift from the Coca Cola company; when clicking on the executable embedded in the email, your PC's CD-ROM drive would open. Other benign viruses included a command that would open dozens of pop-up "buttons" on your desktop, or one that would "flip" the user's screen output upside down or sideways.

Destructive – Destructive viruses are designed to delete or damage files on a computer system, stop or hinder a normal workflow, or generally cause problems for computer or networks. Most viruses you hear about on the news are classified as destructive viruses.

Something else important to note is sometimes a virus will turn out to be benign, but not because the virus writer did not try to make it destructive. Viruses are just as affected by coding bugs as regular applications are and it may turn out to be benign because the virus was written with buggy code and not tested before the virus writer released it to the wild.



Worms

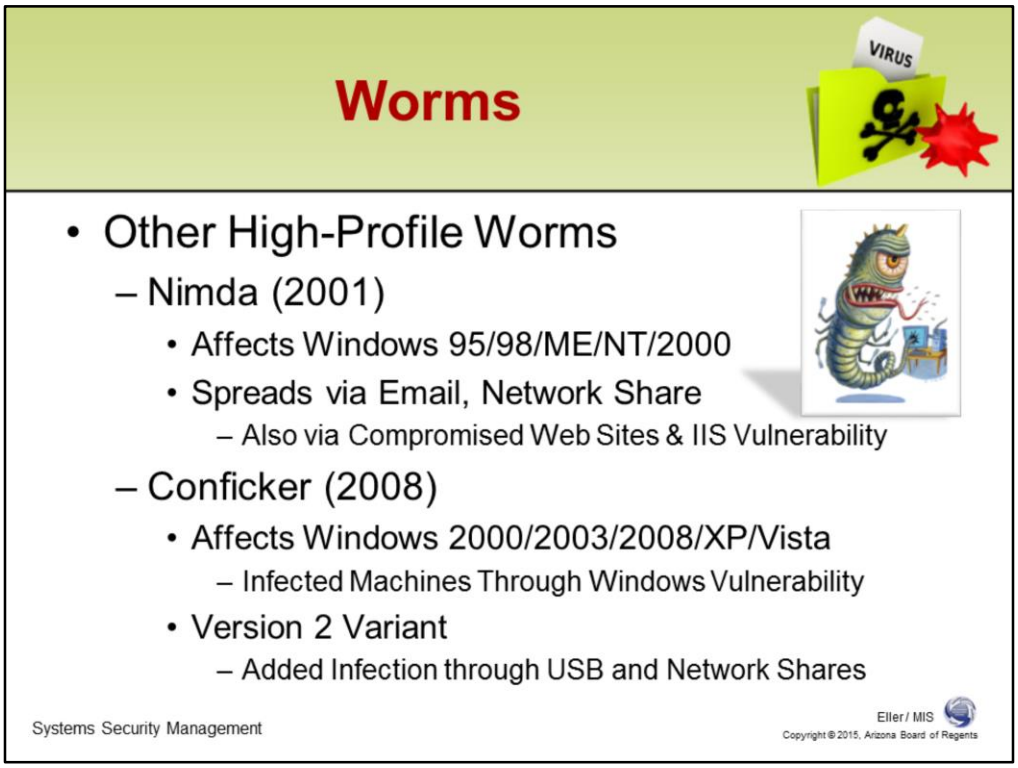
What is a Worm?

A worm is a type of virus designed to infect a system and unleash its payload. Worms are named after their ability to scan a network for vulnerabilities and how they "burrow" into vulnerable systems as they replicate themselves, similar to real worms. There are thousands of worms that have been seen in the wild over the years and we will discuss a few you may or may not have heard of.

Code Red and Code Red II

The Code Red worm variants were originally released in 2001 and designed to infect systems through a vulnerability known as a buffer overflow. This worm targeted systems running Windows NT and Windows 2000, specifically looking for systems running Microsoft Internet Information Services or Search Indexing Services to infect. It was also possible for network devices such as routers or modems that had web-based interfaces for configurations to become infected as well.

The Code Red worms were designed to replicate automatically across a network during only the first 19 days of each month using TCP Port 80 (the standard port used by web servers). The replication activity caused by the worm was very disruptive on networks with infected computers, and the more computers that became infected, the more network traffic would be generated by the worm replication.



Worms (continued)

Other high-profile worms you may have heard of include:

Nimda

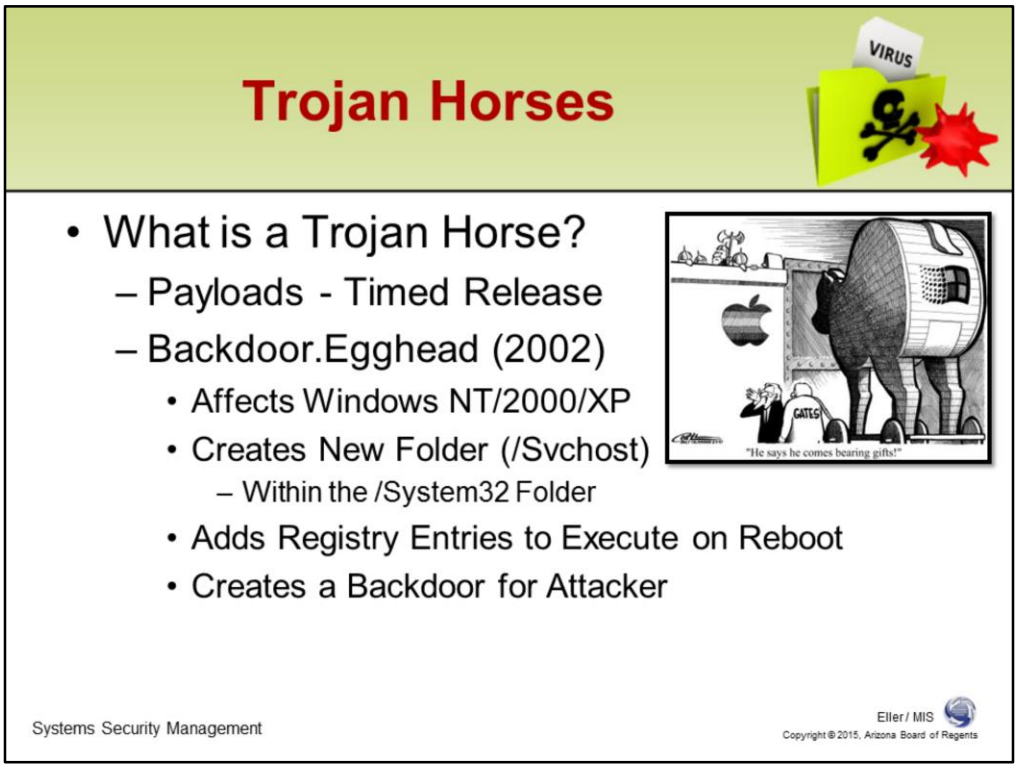
The Nimda worm made headlines in 2001 when it was released because it was one of the first viruses to severely cripple networks worldwide. The worm was designed to take advantage of a vulnerability in Windows 95, 98, ME, NT, and 2000. What made this worm even more problematic is the fact that it could infect systems via e-mail, scanning for vulnerable network shares, compromised web sites, and servers running Microsoft Internet Information Services.

Microsoft took a huge hit to its reputation over this worm, resulting in more highly publicized releases of security patches. While Microsoft had previously released a server software package called Windows Software Update Services, it was not a package that had seen wide adoption by corporations because this type of security threat had not been seen previously. Despite the bad press for Microsoft, the reality was this worm took advantage of a vulnerability in the Windows operating systems that Microsoft had released a patch for months prior to the release of the worm. Unfortunately it took this kind of highly-publicized worm attack to get organizations to start taking security more seriously.

Conficker

One of the more recent worms to see a highly publicized release was the Conficker worm. Released in late 2008, this worm was designed to take advantage of a vulnerability in multiple versions of Windows including, Windows 2000, Server 2003, Server 2008, XP, and Vista. The worm would replicate itself by scanning a network for vulnerable systems and automatically transmitting itself to the affected system. The Conficker version 2 variant worked the same way as the original version; however, it added the ability to replicate itself via USB memory sticks and vulnerable network shares.

A key difference between a virus and a worm is that a virus requires human intervention to spread (for example, via email attachment), whereas a worm is design to propagate itself without assistance in your system and over the network.

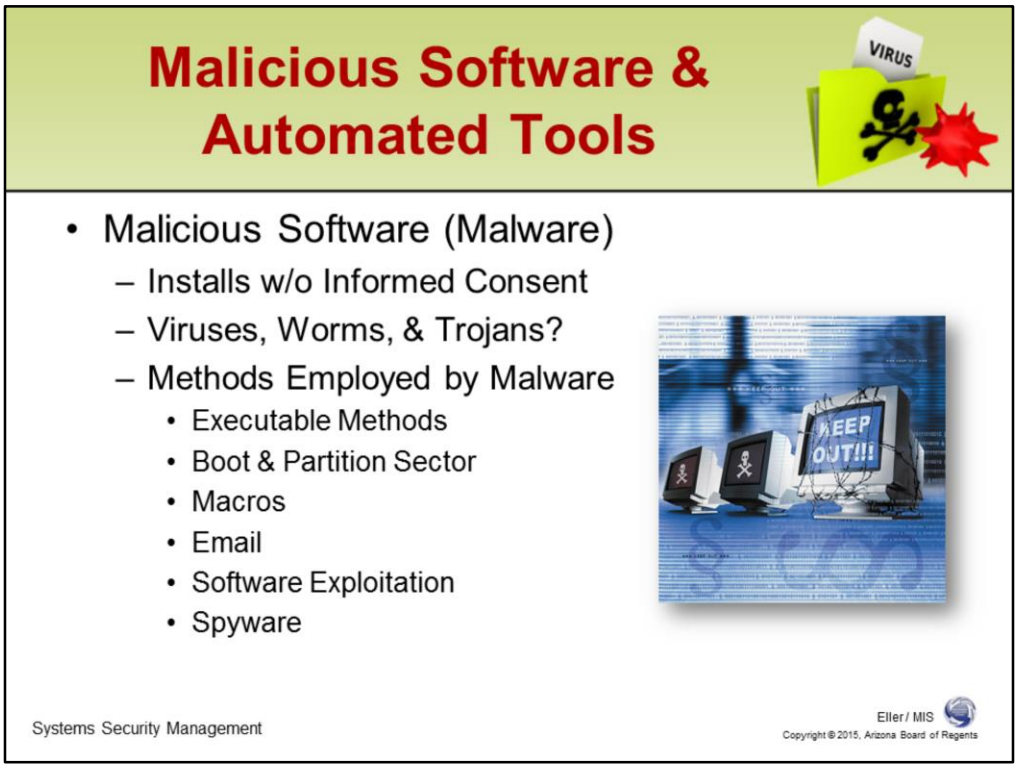


Trojan Horses

A Trojan Horse is a type of virus that, similar to its namesake, hides its payload for a timed release. A Trojan is propagated via what appears to be benign, or useful software, which includes a hidden malicious payload. A Trojan Horse you may have heard of is:

Backdoor.Egghead

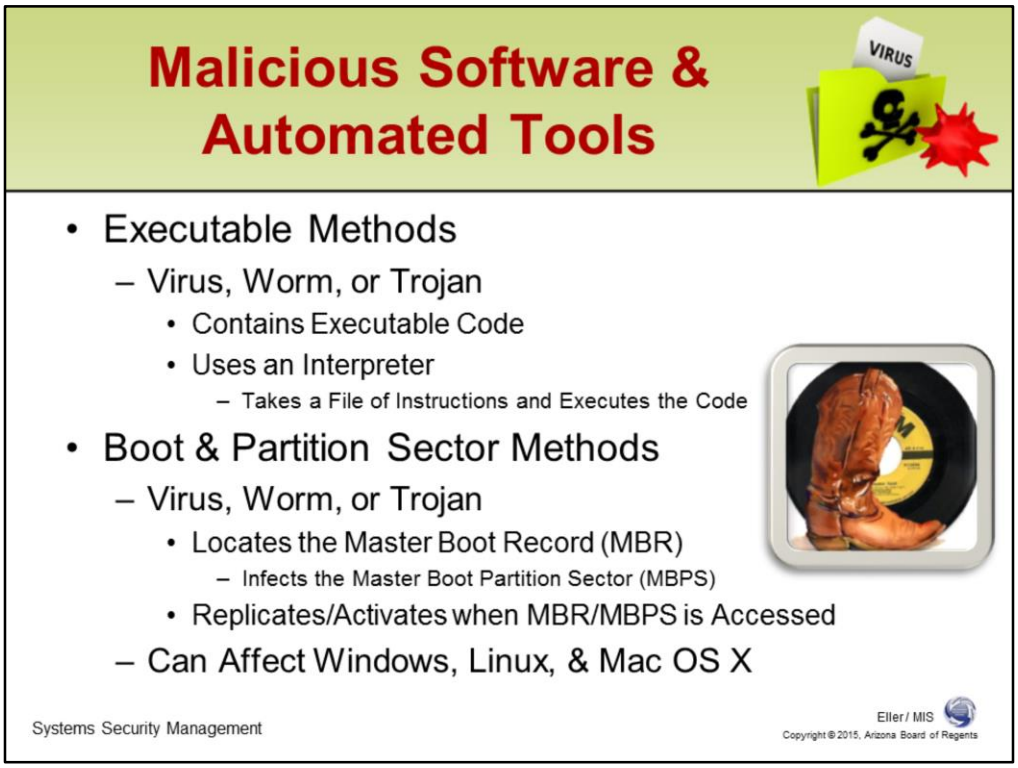
Released into the wild in 2002, Backdoor.Egghead was designed to affect Windows NT, 2000, and XP systems through a common vulnerability in the operating systems. The Trojan created a new folder named "svchost" under the c:\windows\system32 folder. The Trojan then added registry entries designed to execute on reboot which would create a backdoor for the attacker. The backdoor would provide the attacker with administrative access to the infected computer.



Malicious Software and Automated Tools

Malicious software, or malware, is software that is installed on a computer without the user's informed consent. So, does this make malware a virus, worm or Trojan horse? Well yes and no. Some of the methods employed by malware writers in order to get the software installed and running are similar to how viruses infect machines. These methods include:

- Executables
- Boot and Partition Sector
- Macros
- E-mail
- Software Exploitation
- Spyware



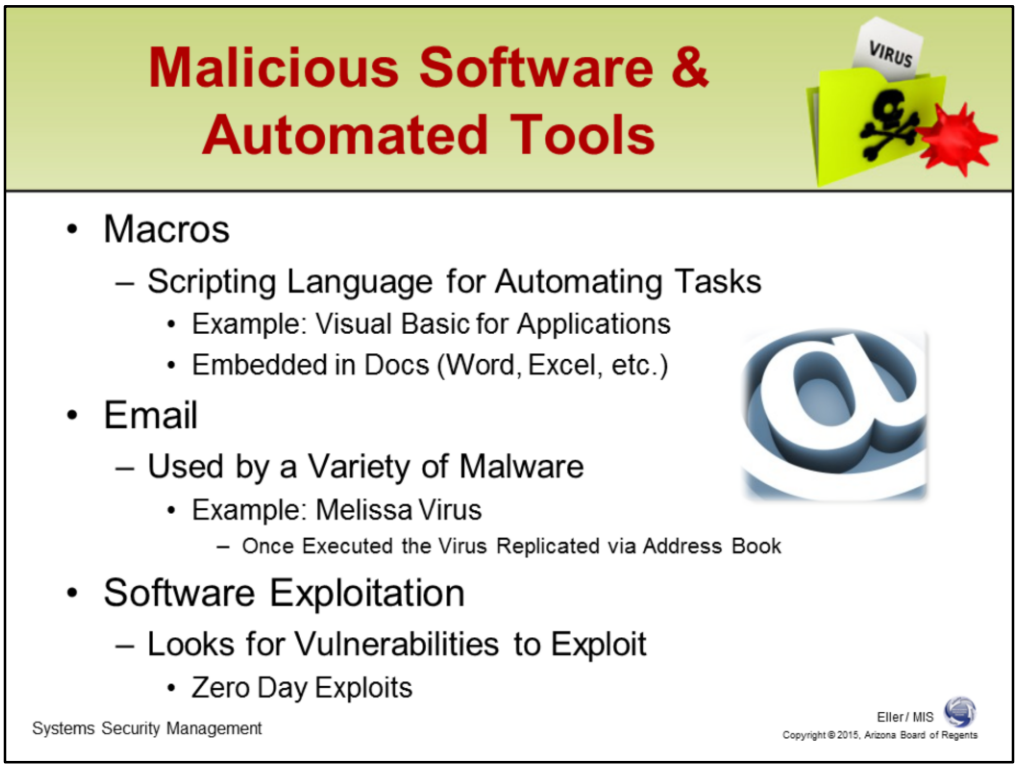
Malicious Software and Automated Tools (continued)

Executable Methods

Malware distributed through executable methods are classic viruses, worms, or Trojans. The downloaded file contains executable code and uses an interpreter to take the file and execute the commands contained within.

Boot and Partition Sector Methods

Malware that invades a system using boot or partition sector methods are also considered to be a type of virus, worm or Trojan. The malware locates the Master Boot Record and infects the Master Boot Partition Sector. The malware then replicates or activates whenever the MBR or MBPS is accessed. This type of malware can affect any operating system, including Windows, Linux, and Mac OS X.



Malicious Software and Automated Tools (continued)

Macros

As previously discussed, Macros are a scripting language used for automating tasks. Malware containing macros are typically distributed by sharing infected documents such as Word or Excel documents.

E-mail

A variety of malware has used e-mail as a means of propagation. One example is the Melissa Virus. Once the Melissa Virus malware attachment was executed by the user, the virus would automatically replicate itself by sending the original e-mail from that user to everyone on their address book.

Software Exploitation

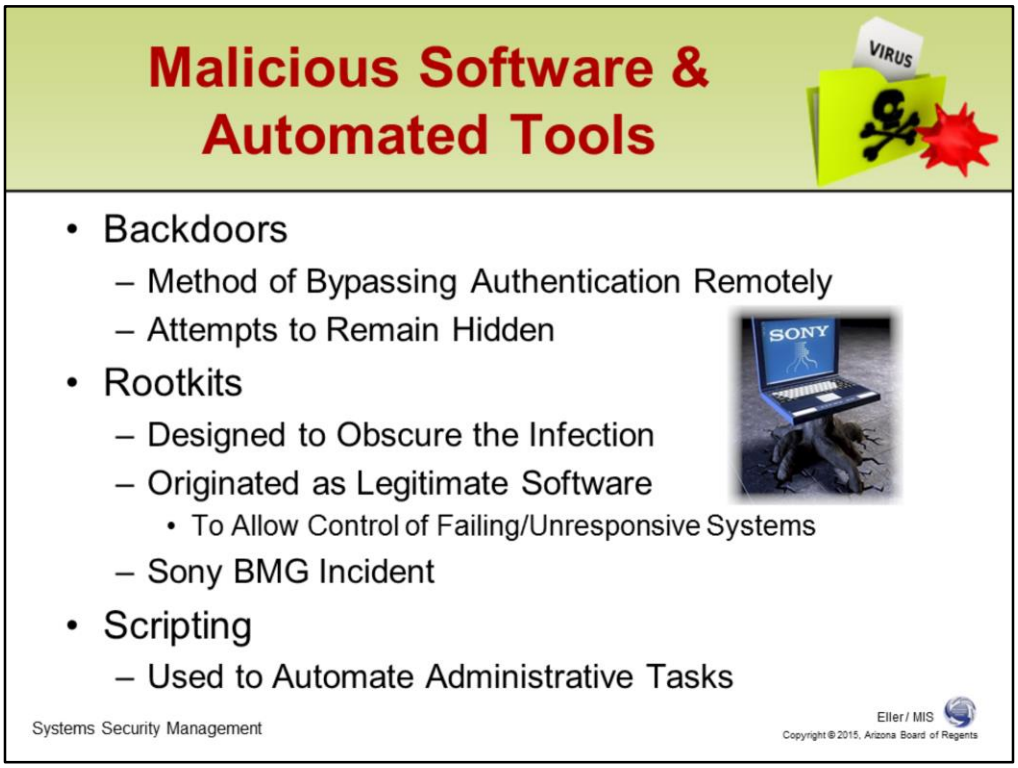
Malware using the Software Exploitation Method looks for vulnerabilities to exploit in an operating system. Specifically this type of malware is looking for zero day exploits, or vulnerabilities which are so new that patches to fix them do not yet exist.

Malicious Software and Automated Tools (continued)

Spyware (or Adware)

Spyware is one of the most common forms of malware. Typically spyware does not self replicate. This type of malware uses deception or vulnerabilities to infect a computer system and then is used to report information back to the spyware author. Examples of spyware include:

- Keyloggers
- Browser Hijacking
- Identify Theft & Fraud
- Cookie Monitoring



Malicious Software and Automated Tools (continued)

Backdoors

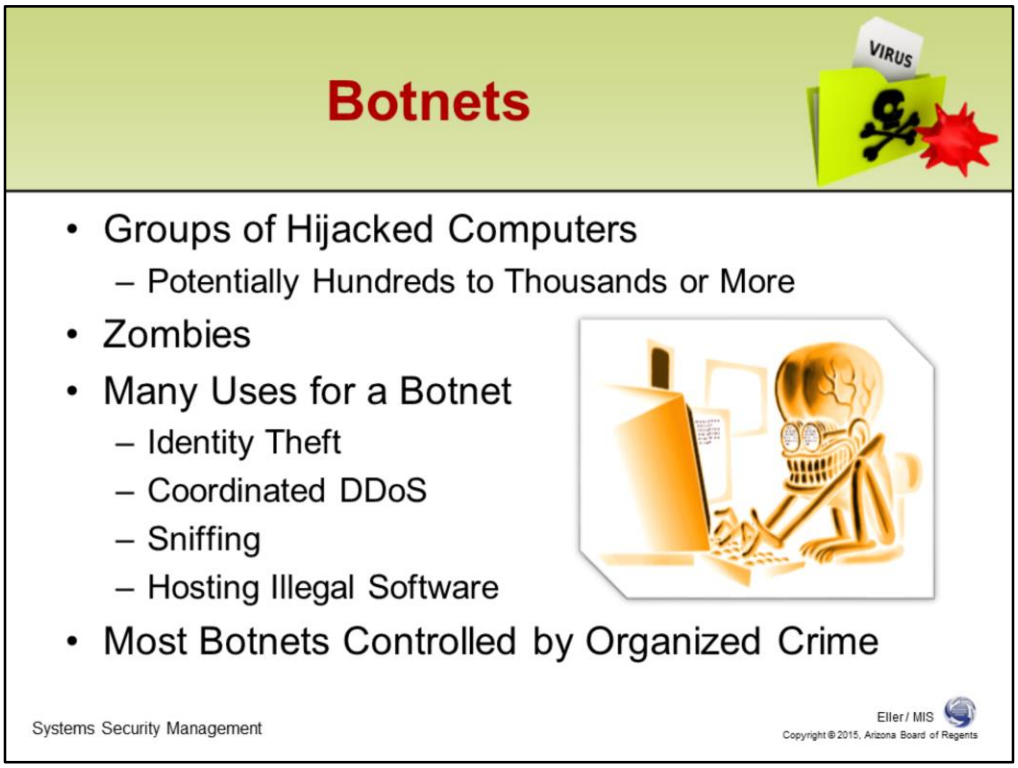
A backdoor is a type of malware method used in order to bypass authentication remotely. The author of the malware is granted administrative-level access to the infected systems and attempts to remain hidden in order to keep the unauthorized access open for as long as possible.

Rootkits

Rootkits are a piece of software that is installed and designed to obscure the infection. Rootkits originated as legitimate software in order to allow SysAdmins the ability to control failing or unresponsive systems in the event that normal means for controlling the systems was unavailable. More often now they are used to remotely control systems through the use of backdoors. One of the most famous incidents with rootkits involved Sony's BMG music group. Hundreds of CD titles were loaded with a digital rights management software designed to prevent people from ripping music from the discs. What Sony BMG did not disclose was the DRM software installed a rootkit on every computer the CD was played on. Ultimately this was a PR nightmare for Sony BMG, who had to issue apologies and refunds or replacement CDs at no charge without the DRM component.

Scripting

Another way to install malware on a system is through the use of scripting. Normally scripting is used by SysAdmins to automate administrative tasks; however, malware authors found ways to use scripting to spread malware in a manner similar to that employed by Macros, only without the need to open an infected document. Many times, just opening an infected web site will execute scripted malware.



Botnets

Botnets are groups of hijacked computers. Typically botnets are created through the distribution of some form of malware that creates a backdoor for the botnet herder to control the system. Most botnets are composed of potentially hundreds or even thousands or more systems. Each infected system is referred to as a zombie and is named such due to fact that these systems are simply awaiting commands from the botnet herder in order to launch an attack. Without the commands the zombies will not do anything.

There are many uses for a botnet, including:

- Identity Theft
- Coordinated Distributed Denial of Service (DDoS) Attacks
- Sniffing
- Hosting Illegal Software

Most botnets are controlled by organized crime syndicates and are used for various activities the groups can make a profit with. Sometimes a group controlling a botnet will sell or rent the botnet to other organized crime groups for their use for a price. The control of botnets is a very profitable illegal venture that law enforcement organizations have been trying to shut down. The problem for law enforcement is that for every botnet it shuts down another one appears to take its place. This is primarily due to the distributed nature of the zombies themselves.

Keystroke Monitoring

- A Form of Spyware
  - Hardware & Software Keyloggers
  - Used to Record All Keystrokes
    - Usually Transmitted to a Remote Attacker
  - Keystrokes Can Include Sensitive Information
    - Identity Theft
    - Active Attacks
  - Countermeasures
    - Hardware & Software

Systems Security Management

Eller / MIS

Keystroke Monitoring

Keystroke Monitoring, also known as keylogging, is a form of spyware. Keyloggers include both hardware and software options that are used to record all keystrokes on a computer and transmit them to a remote attacker. These keystrokes can include sensitive information such as passwords, bank account information, credit card numbers, among others, which can easily be used for identity theft. Keyloggers can also be used for active attacks. By transmitting keystrokes to an attacker, the attacker can then remotely access the system and launch attacks on other systems from that machine. There are various countermeasures to combat keyloggers, including both hardware and software anti-spyware solutions.

Password Attacks

- Online Attacks
  - Passive
  - Active
- Offline Attacks
  - Dictionary Attacks
  - Hybrid Attacks
  - Brute Force Attacks
- Countermeasures
  - Lockout and Password Policies
  - IDS Logs
  - Increased Security for Password Database

Systems Security Management

Eller / MIS

Password Attacks

There are two main types of password attacks that a system can be confronted with – online and offline, both with different methods of attack, some more detectable than others.

Online Attacks

Passive – One way to obtain passwords for a system would be for an attacker to sniff the wire, looking for either passwords transmitted in plain text or capture traffic to attempt a replay or Man-in-the-Middle attack. Alternatively an encrypted or hashed password can be captured and decrypted in an offline attack. The problem here is that an attacker needs some way to sniff the traffic, either by compromising the network the server is attached to, or by being an insider.

Active – Another way to gain access would simply be for an attacker to attempt logging in to a server with guessed usernames and passwords. If the SysAdmin forgot to change the default password for the system, or if the users are practicing poor security, this can be fairly successful. The problem with active attacks is that they tend to take quite a bit longer and are fairly easy to detect and block. We'll talk about that later.

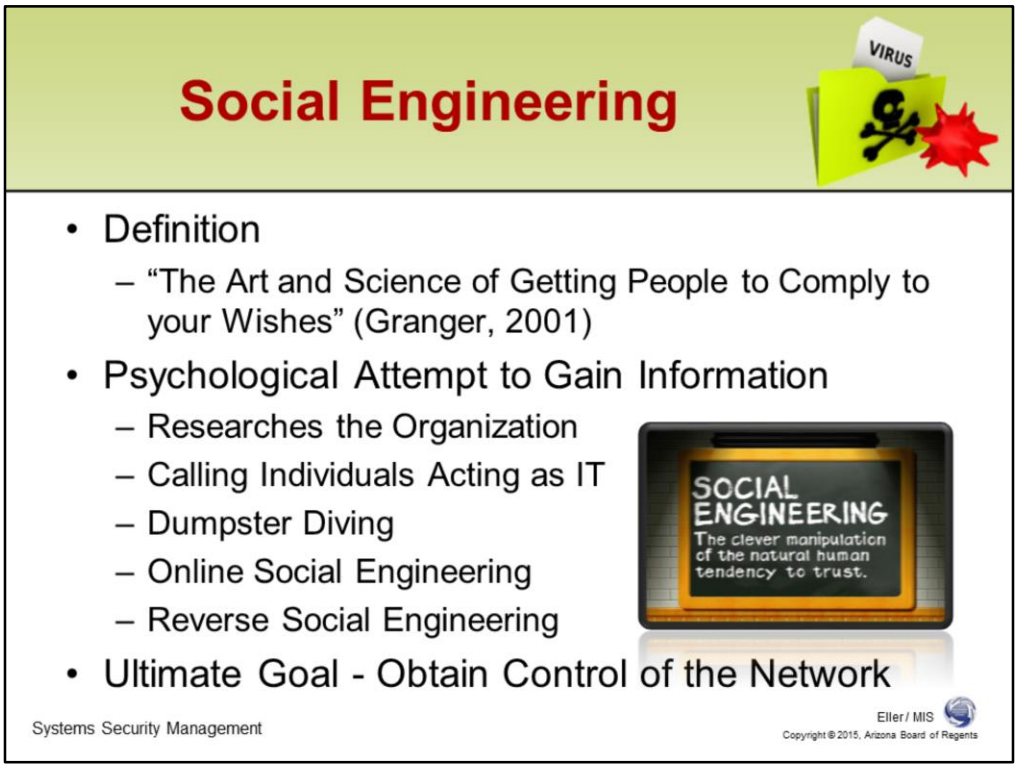
Offline Attacks

An offline attack occurs when an attacker breaches a system and obtains the password file, copying it to their system and using different methods to crack the passwords. Given enough time and processing power, this method is virtually guaranteed to crack every password in the list, no matter the length or complexity. There are three different methods used in offline cracking – dictionary, hybrid, and brute-force. The dictionary attack is by far the fastest and easiest method for cracking the majority of passwords in a list. It's accomplished by taking a text file of dictionary words, hashing them using the same algorithm/process as the original password, and comparing the hashes to the list of passwords obtained. If there's a match, then the attacker has a password he or she can use to access the system. An alternative to the dictionary attack is the hybrid attack; this attack uses a similar list to the dictionary attack but substitutes numbers for letters (for example, a zero for an O, or a 3 for an E) as well as appending numbers and symbols to the beginning and end of words. This takes a bit longer, but will crack even more of the passwords than a dictionary attack alone. Finally you have the brute-force method, which is just what it sounds like: the program bombards the target system, attempting every letter, number, and symbol combination possible until the remaining passwords are all cracked. Brute forcing is by far the most time and processor intensive, and is usually only used on the most complex passwords, but it is guaranteed to be 100% effective given enough time.

Countermeasures

Defenses for online attacks include a lockout policy, where an account is locked out for a period of time after a certain number of incorrect password guesses; IDS/IPS logs and monitoring to see if someone is attempting to login to many different accounts from a single IP address; as well as ensuring that the authentication traffic is encrypted from the user to the server, this helps to prevent passive attacks.

Offline attacks are trickier to detect and defend against; once the attacker has the password list your only hope is that your password encryption method is strong enough to withstand the attacks. One key to preventing this attack from being successful is to harden and secure your authentication servers. Ensuring that attackers can't get to your password database will go a long way towards protecting your environment.



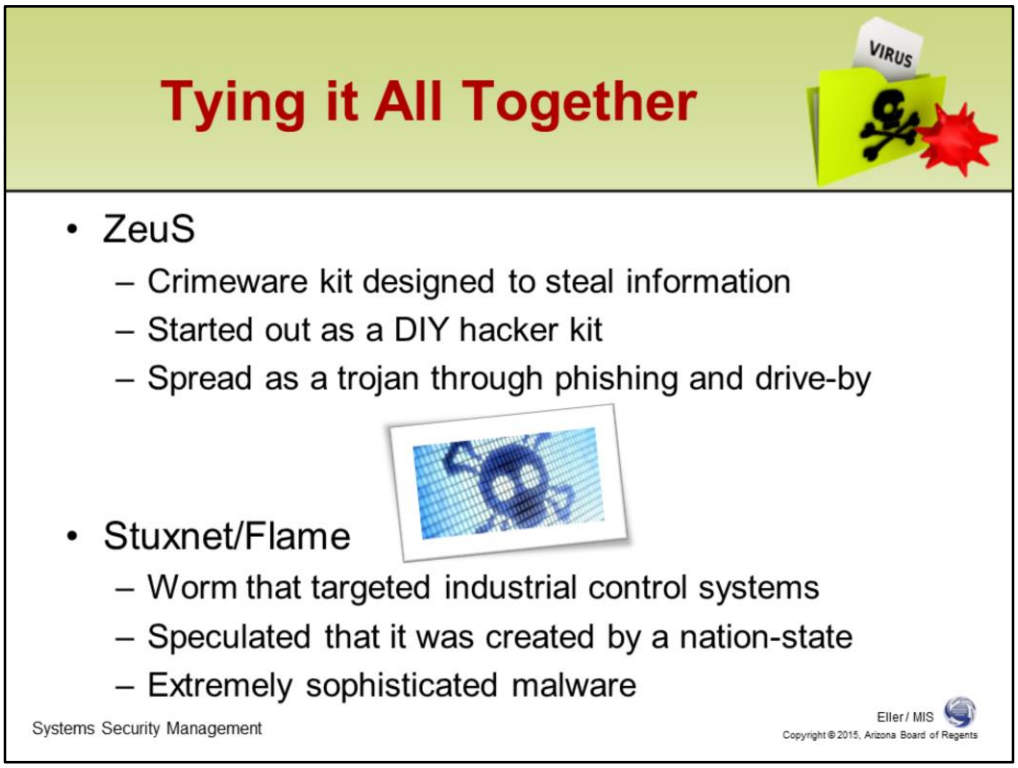
Social Engineering

Social engineering is defined as "the art and science of getting people to comply to your wishes" (Granger, 2001). The idea here is using psychology in an attempt to gain information from network users. Someone can use social engineering techniques to trick users into revealing information an attacker needs. This starts with the attacker researching the target organization. The initial research can then be used to allow the attacker to sound knowledgeable about the organization. The attacker can call individual users acting as an employee in the IT department asking technical questions. Even just getting the user to reveal their username would provide invaluable information to the attacker.

Another method of social engineering involves dumpster diving. With dumpster diving, the attacker is looking for any information that could help them gain access to network systems. Many organizations shred sensitive documents, but where do the shredded document go? Not every organization hires a third party to recycle the material, choosing to dispose of the shredded documents by throwing them in the dumpsters instead.

Online social engineering uses the same techniques, the attacker simply uses more technological means of obtaining the information, such as chat rooms, social media, or online video games. Reverse social engineering involves the attacker convincing the target they are in need of their help. This is usually accomplished by the attacker damaging the target's system and making themselves available to help repair the damage in order to gain information on the target network.

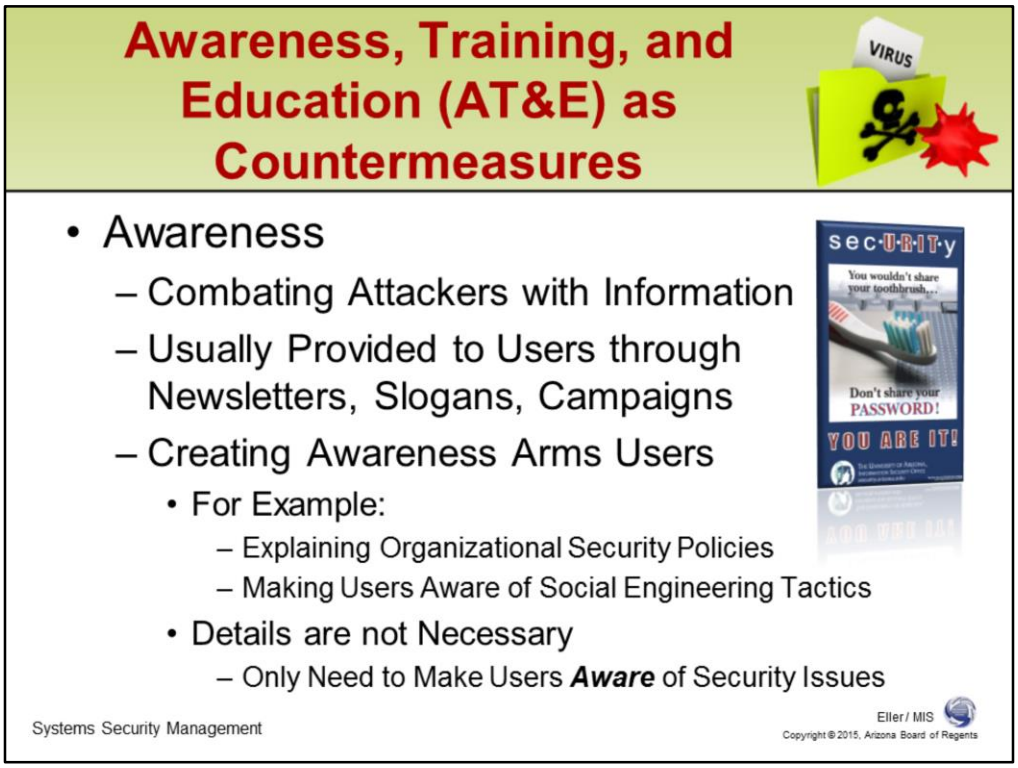
The ultimate goal of social engineering is to obtain control of the network by convincing the targets to give up control voluntarily.



Tying it All Together

"ZeuS (also known as Zbot, Kneber, PRG, NTOS, Wsnpoem and Gorhax) is a crimeware kit designed to steal banking information and credentials through various means. The Zeus trojan is spread mainly through drive-by downloads and phishing schemes. First identified in July 2007 when it was used to steal information from the United States Department of Transportation, it became more widespread in March 2009. In June 2009, security company Prevx discovered that Zeus had compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster, ABC, Oracle, Cisco, Amazon, and BusinessWeek." (Westmoreland, 2010).

Stuxnet was a computer worm discovered in June of 2010 that was designed to attack industrial systems, specifically programmable logic controllers being used to control centrifuges that were separating nuclear material in the nuclear plants of Iran. The worm was spread via thumb drive and had three modules: the main worm payload, a link file that automatically executed the propagated copies of the worm, and a rootkit that was responsible for hiding all the malicious processes and files related to the worm, ensuring detection was minimized. Reports indicated that over one fifth of all Iran's nuclear centrifuges were damaged by this worm. This worm was also notable for being what experts deemed the first nation-state cyber weapon, a joint project carried out by the US and Israel (Kelley, 2013).

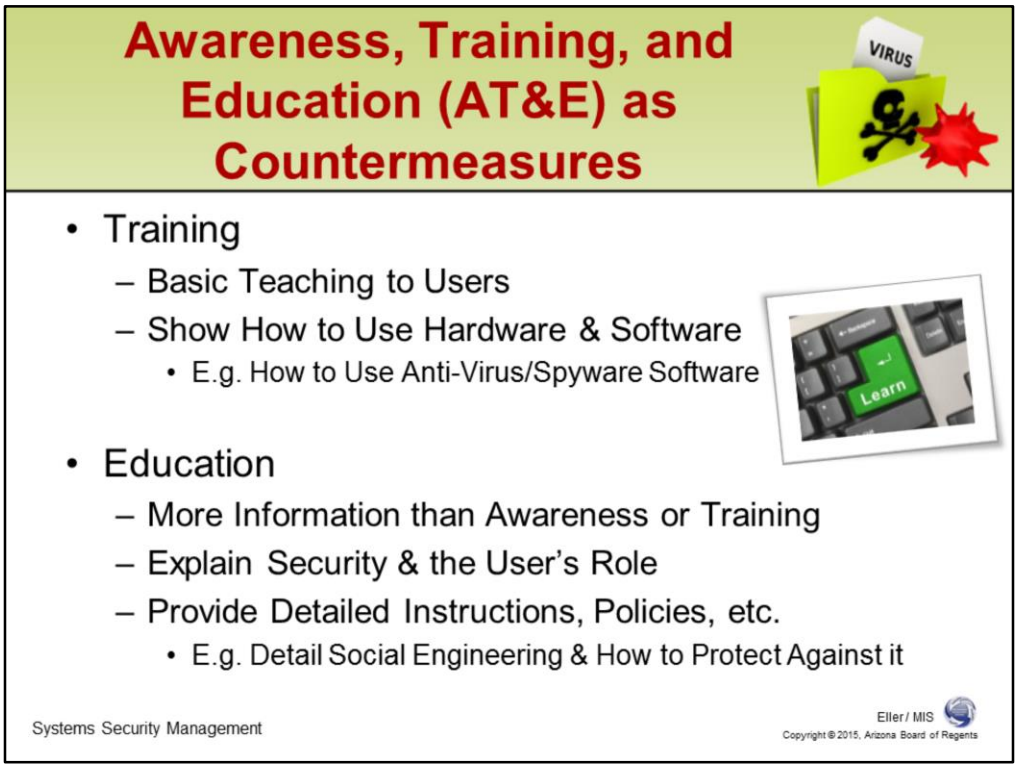


Awareness, Training, and Education (AT&E) as Countermeasures

Awareness

One of the most effective ways to combat attackers is through user awareness: combating attackers with good information. Awareness of security issues is usually provided to users through newsletters, slogans, or campaigns. Take the image to the right, this is a security awareness poster that has been seen all over the University of Arizona campus. The message? You wouldn't share your toothbrush, don't share your password! Using the slogan: secURITy: You Are IT! makes the poster even easier for users to remember. This kind of creativity in security campaigns has helped to raise awareness of security issues on our campus.

The bottom line is that creating awareness arms users with the information they need to combat potential attacks. This can be done by more clearly explaining organizational security policies or making users aware of social engineering techniques. Exact details are not necessary, the objective is only to make users ***aware*** of the existence of security threats.



Awareness, Training, and Education (AT&E) as Countermeasures (continued)

Training

Training as a countermeasure involves basic teaching to the users. Showing users how to use specific hardware or software correctly is the key to effective training. For example, showing users how to use anti-virus or anti-spyware software to help remove infections or detect them when they occur will help keep a network more secure.

Education

Education as a countermeasure involves providing considerably more information than either awareness or training. Fully explaining security policies and the user's role in ensuring systems remain secure is vital to educating users. Providing detailed instructions for certain security tasks and detailed policies helps to keep systems more secure. For example, by detailing social engineering and how to protect against it will reduce the potential for a social engineering attack from being successful.

Data Mining

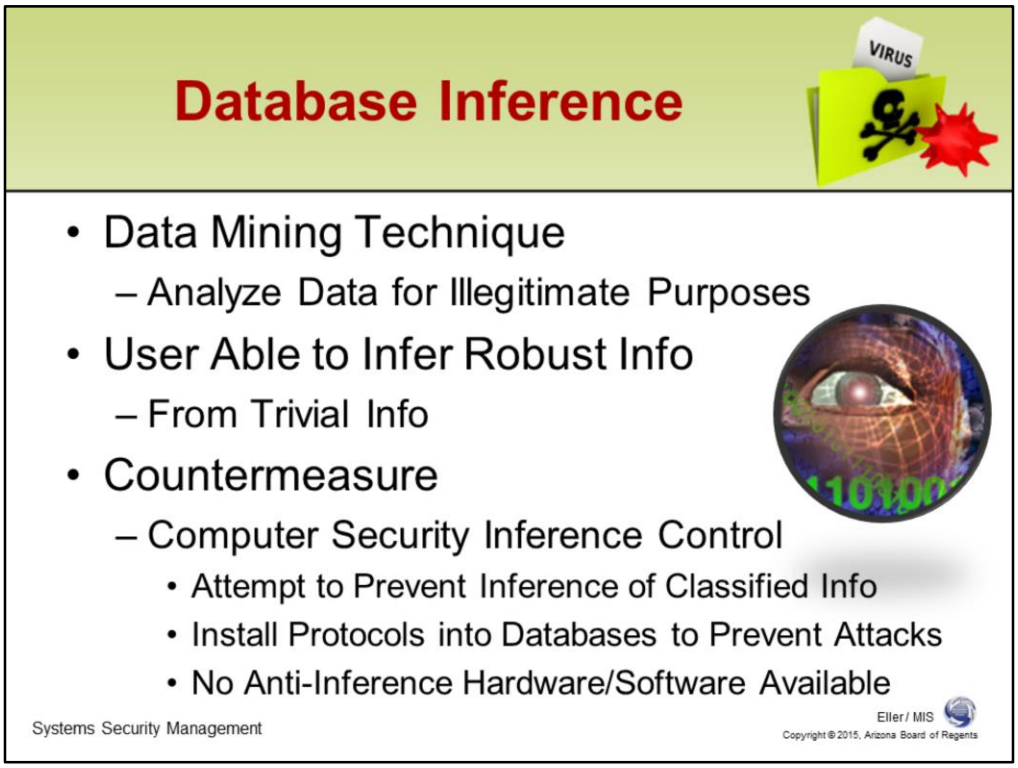
Data mining is a technique used to find relationships in data. Data mining is used to help detect fraudulent transactions, assessing the risks involved with specific activities, and even for simple product retailing.

In the realm of security, data mining techniques are used to analyze network traffic patterns in order to detect attacks. This is accomplished through the use of intrusion detection or prevention systems and attempts to block attacks as they happen.

Governments also use data mining techniques as a means of looking for terrorist activities over the Internet.

Data mining can provide a tremendous amount of information. The biggest problem with data mining as a countermeasure is that more often than not, the results need to be analyzed by people, and that can take a significant amount of time and manpower.

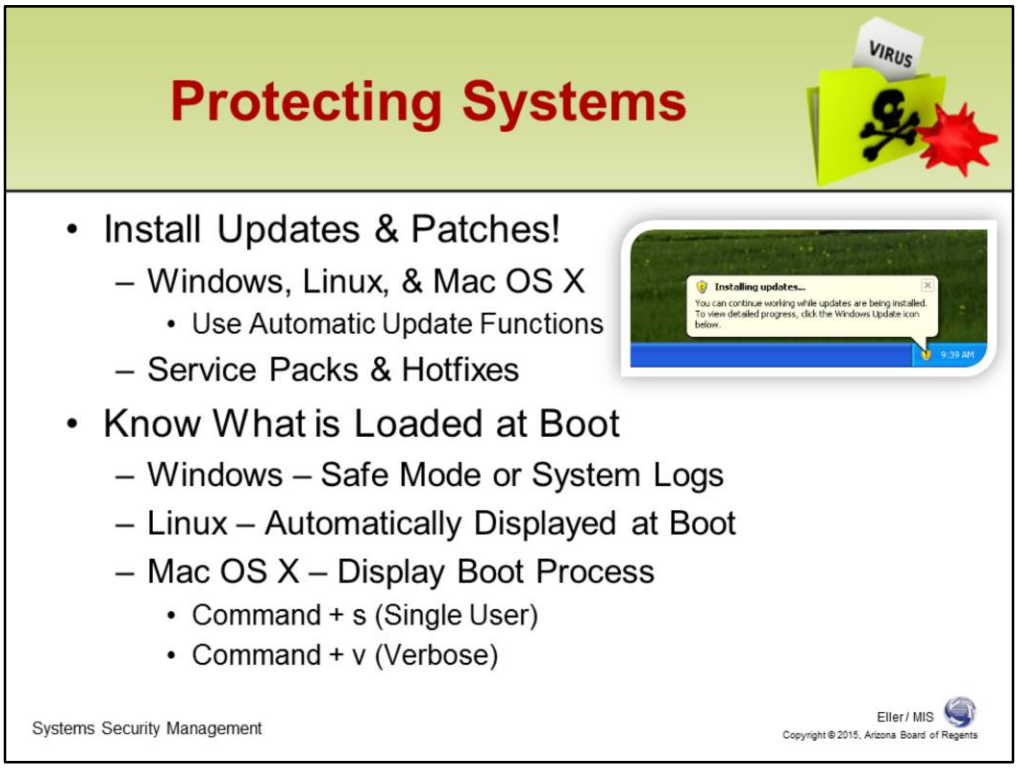
Due to the ever-evolving threat landscape, security providers are increasingly relying on next generation tools like Security Information Event Managers (SEIMs) as mentioned in module one. These tools provide better data and actionable intelligence and oftentimes are equipped with scripts and workflows to even take action automatically in the event that a specific threat is detected in order to deflect or even stop an attack in progress.



Database Inference

Database inference is a specific data mining technique that is used for analyzing data for illegitimate purposes. The key to database inference is it allows the attacker to infer robust information from the most trivial of information. In other words an attacker could infer specific details from only the most basic data points. For example, an attacker could gain access to a database field that contains a list of usernames. The attacker could infer those usernames are the beginning of e-mail addresses for the organization, thereby giving the attacker a potential list to sell to spammers.

An effective countermeasure for database inference is the adoption of Computer Security Inference Controls. This type of solution attempts to prevent the inference of classified information by installing specific protocols into databases designed to prevent attacks. While this can be an effective countermeasure, it is not foolproof. Unfortunately, at this time, there are no anti-inference hardware or software solutions available to completely protect against the technique. Especially since inference depends on the attacker's own ability to glean specifics out of minimal information.



Protecting Systems

There are several techniques a SysAdmin can use to help protect the systems under his or her purview. The most effective way to protect systems is to install updates and patches that are released by the OS and application developers. This includes Windows, Linux, and Mac OS X systems and software. Home and Small Business users can most effectively accomplish this by using the automatic update functions available in each OS. Larger organizations can adopt more centralized update systems to push patches and updates to client and server systems. Many software companies will release hotfixes for specific security issues and will later release service packs which combine a larger number of hotfixes in a single update to help simplify the process of security updates.

Another way to protect systems involves the user (and/or SysAdmin) knowing what is loaded when a system boots up. In Windows, the user or SysAdmin can boot into Safe Mode or examine system logs to gather this information. With Linux, the information is usually displayed automatically at boot time. Mac OS X can display the boot process information when specifically requested by the user. This is accomplished by pressing the Command key + S for single user mode or the Command key + V during the boot process for a more verbose listing of information.

Protecting Systems (continued)

Installing Malware scanners, including anti-virus, anti-malware, and anti-spyware software on systems will help detect and remove threats when they appear. In general the software will scan active memory, drives, e-mail, and file downloads for threats and will monitor the system for continuous protection. It is important to understand that some of these solutions are primarily a reactive technology, meaning the threat must exist before the software does anything to protect systems. Other solutions have the ability to do active protection that scan files as they are accessed by the system and monitor your activity during browsing sessions and while going about your daily routine, ensuring that you don't inadvertently open an attachment with a virus, or download a malicious file. It's important to do some research before purchasing or installing a solution so that you understand the software's capabilities as well as its limitations.

When installing system or driver files, the SysAdmin should ensure all files use digital signatures in order to prevent the installation of viruses or other malware on a system. Users and SysAdmins should also regularly create backups of critical systems and data, and when possible create repair disks to help restore systems in the event of a software failure. Finally, the organization must create and implement organizational policies pertaining to security using standard risk management techniques.

Risk Management Concepts

Risk management huge topic that takes a considerable amount of time to cover completely. SysAdmins need to understand these concepts in order to find ways to mitigate the risks associated with system security. In order to just understand the basics, there are six primary risk management concepts that should be used to examine risks. Remember, this will not go into detail, just the basics.

Identify – The first concept involves identifying the security risks to an organization. Are there things that users do (such as writing passwords on a sticky note and placing it under the keyboard) that could be considered a security risk?

Assess – Once a risk is identified, it must be examined and assessed. What is the severity of the risk? How could the risk affect the security of the organization's data or reputation?

Plan – Once the risk is better understood, the SysAdmin should develop a plan for addressing the risk. How should the company deal with the risk? Will the risk require a technological solution or might simple training or education remove the risk?

Track/Monitor – Once a plan has been developed and implemented, the SysAdmin must track or monitor the solution to ensure it is having the expected results.

Control (Eliminate, Mitigate, Accept) – Controlling the risk involves making the determination of whether or not the organization will eliminate the risk, mitigate the risk to reduce exposure, or accept the risk and move on.

Communicate/Document – Finally, communicating the results, either in person or through documentation to management will help to show the risk has been addressed.

Remember, you cannot ignore security risks forever. At some point, the risks must be understood and addressed in order to ensure system security.

Next Module…

- Encryption
- Encryption Techniques
- Internet Protocol Security
- Digital Signatures
- Message Digests
- PKI and Key Management
- Authentication
- Authentication Types
- Single Sign-On
- Domains
- Biometrics
- Privacy Issues

Systems Security Management

Eller / MIS

In the next module, we will be discussing authentication and encryption techniques used to secure systems. This includes:

- Encryption Techniques
- Internet Protocol Security
- Digital Signatures
- Message Digests
- PKI and Key Management
- Authentication Types
- Single Sign-On
- Domains
- Biometrics
- Privacy Issues

Resources

Chapple, M. (2009). Database security issue: Inference. *About.com*. Retrieved from http://databases.about.com/od/security/l/aainference.htm.

Chen, T., & Robert, J. (2004). The evolution of viruses and worms. *Statistical Methods in Computer Security*. Retrieved from http://vx.netlux.org/lib/atc01.html.

Difference between viruses, worms, and Trojan horses. (2009, June). *Tutorials*. Retrieved from http://www.tutoorials.com/2009/06/different-between-virus-worm-and-trojan.html.

Free Management Library. (2009). Risk management. *Authenticity Consulting LLC*. Retrieved from http://managementhelp.org/risk_mng/risk_mng.htm.

Granger, S. (2001, December 18). Social engineering fundamentals, part 1: Hacker tactics. *Security Focus*. Retrieved from http://www.securityfocus.com/infocus/1527.

Hacking. (2005, November 8). Robot wars: How botnets work. *WindowSecurity.com*. Retrieved from http://www.windowsecurity.com/articles/Robot-Wars-How-Botnets-Work.html.

Inference attack. (2009, September 7). *Wikipedia: The Free Encyclopedia*. Retrieved from http://en.wikipedia.org/wiki/Inference_attack.

Kelley, M. B. (2013, November 20). The Stuxnet attack on Iran's nuclear plant was 'far more dangerous' than previously thought. *Business Insider*. Retrieved from http://www.businessinsider.com/stuxnet-was-far-more-dangerous-than-previous-thought-2013-11.

Masood, S. G. (2004, May 20). Malware analysis for administrators. *Security Focus*. Retrieved from http://www.securityfocus.com/infocus/1780.

Mills, E. (2010, February 1). In Their Words: Experts Weigh in on Mac vs. PC Security. *CNET Tech News – InSecurity Complex Blog*. Retrieved from http://news.cnet.com/8301-27080_3-10444561-245.html.

Passeri, P. (2014, November 10). October 2014 Cyber Attack Statistics. Hackmageddon. Retrieved from http://hackmageddon.com/2014/11/10/october-2014-cyber-attacks-statistics/.

Seifert, J. W. (2007, January 18). Data mining and Homeland Security: An overview. *CRS Report for Congress*. Retrieved from http://www.fas.org/sgp/crs/intel/RL31798.pdf.

Westmoreland, R. S. (2010, February 7). ZeuS. *Antisource*. Retrieved from http://www.antisource.com/article.php/zeus-botnet-summary.

What types of spyware are out there? (2009). *Top Ten Reviews*. Retrieved from http://anti-spyware-review.toptenreviews.com/types-of-spyware.html.