CS566 - Securing the Enterprise Infrastructure with Cyber Security Techniques

Module 5: Control Setup and How to Protect Windows from Malware

Module Introduction

Readings

Note: The following readings may require you to be logged in to the Saudi Digital Library. You may do that here (https://lms.seu.edu.sa/bbcswebdav/xid-27610786_1).

Required

Chapter 15: Threat and Incident Management in *Effective Cybersecurity: A Guide to Using Best Practices and Standards*

Lima, A., Sousa, B., Cruz, T., & Simões, P. (2017). **Security for mobile device assets: A survey (https://search-proquest-com.sdl.idm.oclc.org/docview/1897672229?accountid=142908)**. Paper presented at the International Conference on Cyber Warfare and Security (pp. 227-XVI). Reading, UK: Academic Conferences International Limited.

Shah, N., & Farik, M. (2017). **Ransomware - Threats, vulnerabilities and recommendations (http://www.ijstr.org/final-print/june2017/Ransomware-Threats-Vulnerabilities-And-Recommendations.pdf)**. *International Journal of Scientific & Technology Research, 6*(6), 307-309. Retrieved from http://www.ijstr.org/final-print/june2017/Ransomware-Threats-Vulnerabilities-And-Recommendations.pdf

Recommended

Sadaqat, R. (2017, May 21). **Don't know it? Don't open it, experts at GISEC 2017 say (https://search-proquest-com.sdl.idm.oclc.org/docview/1900544763?accountid=142908)**. *TCA Regional News*.

Tam, K., Feizollah, A., Anuar, N. B., Salleh, R., & Cavallaro, L. (2017). **The evolution of android malware and android analysis techniques (https://www.researchgate.net/publication/312376862_The_Evolution_of_Android_Malware_and_Android_Analysis_Techn**
ACM Computing Surveys, 49(4), 1-41. Retrieved from https://www.researchgate.net/publication/312376862_The_Evolution_of_Android_Malware_and_Android_Analysis_Techniques

For Your Success

As you progress through the module, consider the devastating impact that malware can have on organizations and individuals.

To do this week:

- Your second Critical Thinking assignment is due; it examines the issue of malware. Review the assignment early in the week and contact your instructor if you have any questions or concerns.
- There is also another required Live Session with your instructor this week; plan to attend.

Learning Outcomes

1. Define the purpose of malware.
2. Identify the effects of malicious code.
3. Analyze how malicious code spreads and operates, and where it resides.
4. Explain how antivirus and anti-spyware software work.
5. Examine best practices for malware prevention.

1. Malware, Antivirus Software, and Anti-Spyware Software

Click to Enlarge

Protecting your PC and other devices from malware requires dedication and the ability to pay attention to details. Today, malware targets not only PCs but mobile devices as well. According to Patil and Patil (2015), malware is a bigger problem than most people think. According to Kujawa et. al. (2019), in 2018, the United States ranked first in consumer and business malware detections. In addition, in 2018 European, Middle Eastern, and African businesses had a "…150 percent increase in Trojan activity" (Kujawa et. al., 2019, p. 19). A person can be victimized by malware through a web browser, email, social media, and more. It is imperative to be careful on your mobile device since instant messaging and downloaded files are a source of malware as well. It is critical that your PC or mobile device has a security program installed to provide proactive protection to minimize the chance of infection.

What is Malware?

Malicious is a term used for any type of software code or script that is designed to do damage to another system. *Malware* (sometimes called *malicious code*) is a type of software designed to take over or damage a computer without the user's knowledge or approval. Malware is designed to cause unwanted effects, security vulnerabilities, or even critical damage.

Click on the following tabs as Solomon (2014) listed them as three of the primary purposes of malware:

Purpose 1 **Purpose 2** **Purpose 3**

Disrupt computer operations

Malicious software refers to a wide range of security threat terms such as viruses, worms, Trojan horses, and malicious active content (Patil & Patil, 2015). It may take the form of Java Applets, ActiveX Controls, or even browser plug-ins. There are many more types of code, so it is important to stay abreast of security threats to defend your system properly. Once your device is infected, the malware may enter your network drives and spread causing overloads, stealing data or passwords, manipulating your file structure, or even reformatting your hard drive.

Explore some common types of malware by clicking on the following radio buttons:

Hackers may use malware to gain remote access to a user's computer. This remote access is also called a *backdoor*. According to Patil and Patil (2015), backdoors can be created for various reasons. Authorized personnel may establish a backdoor for troubleshooting purposes, while hackers create backdoors to gain access to the confidential information of a company or customer. Some backdoors are even created by accident. Regardless of how the backdoor is created, it is a serious security threat and should be addressed as soon as it is identified.

Click to Enlarge

Hackers are everywhere, and computers can easily become infected with malware. Kumar, Punitha, Raghunath, and Sathishkumar (2015) noted that computer viruses can replicate, making copy after copy of themselves until significant damage is done. Every virus is dangerous, as it may quickly use available resources and degrade the functionality of the system. Viruses running in the background may lead to system instability and crashes, and may even transmit themselves across networks and bypass security systems in place.

Spyware is a little different. It does not replicate itself within a system. Rather, it is software that secretly collects a user's information without that person's knowledge. This is commonly used for advertising purposes, but it can cause serious system problems as well. Spyware applications are typically a hidden part of freeware or shareware that may be downloaded from the Internet (Kumar et al., 2015). Once installed on the system, spyware observes the user's Internet activities and passes that background information along to another person or source. Users should be extremely cautious, as spyware can be used to gather passwords, email addresses, or credit card information.

Watch the following video, which contains an examination of the growing problem of ransomware:

Abu Dhabi Quick Look: Ransomware in the Middle East

(Source: http://www.youtube.com/watch?v=HoRVUMFZR4o)

Ransomware is a malicious denial-of-service attack that encrypts data for extortion, holding information hostage in return for money. This presentation will cover types of ransomware, their design, propagation, encryption, command and control, targets, payment, proactive defense, and reactive solutions. In particular, it will discuss the use and evolution of ransomware in the Middle East.

2. Best Practices for Malware Prevention

Take some time to view the following video to learn some of the best practices for removing malware:

Best Practices for Malware Removal

(Source: http://www.youtube.com/watch?v=WlASZInTvnQ)

A malware infection can be a challenge to remove. This video provides a list of best practices for removing malware from any system.

Just as critical as malware removal—if not more so—is *malware prevention*. It is important to keep software up to date, as the majority of malware infections take advantage of security vulnerabilities. According to Kumar et al., (2015), Microsoft typically releases its patch updates on the second Tuesday of the month. A good practice is to let the update happen automatically. If automatic updates are not an option, then you should ensure that you run the updates manually as soon as they become available. Another best practice is to use a web browser that is stable. For example, Firefox and Google Chrome have browsers that can update patches automatically. This is always a good thing when dealing with home users.

Summary

We explored the following concepts in this module:

- Malware is a significant problem for organizations, and the problem is growing at an increasing pace.
- Malware gets in the way of normal computer operation and threatens the security of information stored on the computers.
- The two most important concepts when combating malware are defense in depth and prevention.
- When planning to manage malware threats, prevention efforts are more productive than eradication.

Check Your Understanding

Click Here to Begin

References

Kujawa, A., Zamora, W., Umawing, J., Segura, J., Tsing, W., Arntz, P., & Boyd, C. (2019). *2019 state of malware.* Retrieved from https://resources.malwarebytes.com/files/2019/01/Malwarebytes-Labs-2019-State-of-Malware-Report-2.pdf

Kumar, C. R., Punitha, R., Raghunath, R., & Sathishkumar, K. (2015). Enhancing code aware routing by idling methods to improve energy efficiency in wireless networks. *International Journal of Applied Engineering Research*, *10*(4), 10731-10741.

Patil, D. R., & Patil, J. B. (2015). Survey on malicious web pages detection techniques. *International Journal of U- & E-Service, Science & Technology*, *8*(5), 195-205. Received from http://dx.doi.org/10.14257/ijunesst.2015.8.5.18

Solomon, M. G. (2014). *Security strategies in Windows platforms and applications* (2nd ed.). Burlington, MA: Jones & Bartlett Learning.