Identifying Malware Threats and Protecting Information Resources

Jacob Wolstenholme

Saint Leo University

In today's world of advanced technology, computer attacks and security breaches are spreading across the globe. These computer attacks, also known as malware, has become easier to perform as technology allows hackers, which can be someone inside or outside an organization, to design an application that steals personal information and destroy computer data without being exposed (Comodo 2019). Malware is any program or file that is harmful to computers or networks (Bidgoli 2019). A malicious software is a range of software programs developed with malicious intent and installed on a computer without consent (Armendariz 2019). There is possibly more malware on the web than valid software (BullGuard 2012). There are many different malware attacks that can steal the information assets of an organization. Without proper action taken to defend these attacks, the number of malware attacks will only continue to grow.

The first and most well-known type of malware attack is a virus. Viruses consist of self-propagating program code that attaches itself to other files. When a user uses the program or operating system containing the virus, the cycle continues. They are transmitted through a network, email attachment, or a message board (Bidgoli 2019). When the software is used by the computer's owner, the software spreads the virus. The one major thing about a virus is that it needs a host to do an action before it can start doing damage to a computer (BullGuard 2012). Viruses are the only type of malware that "infects" other files. This makes viruses hard to get rid of because the virus is executed from a legitimate program (Grimes 2019). One common virus known today is what is called an FBI virus, or an FBI Moneypack scam. An FBI virus is aggressive malware that presents itself as an official FBI alert. It tricks you by claiming your computer is blocked due to a copyright violation while a menacing virus locks down the computer's system. There is no means of closing the pop-up alert, and it forces you to pay to

unlock your computer (Armendariz 2019). Fortunately, there are several ways to help get rid of a virus. The most practical way is to install and update an antivirus program to help prevent the virus from spreading (Bidgoli 2019). Another way to protect yourself from a virus attack is to run periodic scans with the software to improve the chance of detecting and removing a threat of a virus (Norton 2018).

Another type of malware attack is a worm, which is very similar to a virus. Worms are independent programs that can quickly spread without the user's knowledge and can replicate itself to eat up a computer's resources. The major difference a worm has compared to a virus is that a worm does not need to attach to a host to spread, making them very destructive (Bidgoli 2019). As worms self-replicate, they exploit other files and programs to do the dirty work, which includes consuming computer memory and reducing computer performance (Grimes 2019). One common worm today is one known as WannaCry. WannaCry is a ransomware worm that is distributed by malspam, which is unsolicited email spam. When a user open the email, the worm uses ransomware to extort the user into paying to unlock the device, while the worm itself self-propagates to the rest of the computer (Armendariz 2019). There are a couple of ways to help get rid of worms. The first is to immediately disconnect or turn off the device to prevent data from being transmitted to the hacker as quickly as possible. Another method is to create backups of files and programs so that when the worm attack destroys the original files and programs, the user still has data that is not infected by the attack. Backup software, a CD, or a flash drive can help create backups of files and programs. Users can prevent both viruses and worms by monitoring their online behavior. They should be aware of what they are clicking on, and avoid suspicious-looking websites and advertisements. The big thing to remember is that if something seems too good to be true software, then it probably is malicious software (Norton 2018).

A type of malware attack that is growing in popularity is a trojan horse. Trojan programs contain code that is intended to disrupt a computer, network, or website. They are usually hidden inside a commonly used program, making them hard to detect (Bidgoli 2019). A trojan horse will gain control of a computer and help install other types of malware used to manipulate the computer without the user's knowledge (Comodo 2019). It is able to conceal its attack by pretending to be a genuine application. Users believe they are getting useful software but in reality they are installing malware into their computer (BullGuard 2012). Similar to a virus, a trojan horse must be activated by the user to do its work, and usually first arrives as an email with a macro-enabled word attachment or as an attached PDF with an embedded link. Examples of a trojan horse is a fake antivirus program and a rootkit. A fake antivirus program pops up and claims you are infected, then it instructs you to run a program to clean your computer. The user takes the bait and installs the software, and the trojan takes root (Grimes 2019). A rootkit conceals malware from antivirus detection, making the user of malware activities that are going on in their computer (Comodo 2019). Two other types of modern trojan horses are Suspicious.Emit and Emotet. Suspicious.Emit is a severe backdoor trojan horse that allows a remote attacker to gain unauthorized access to your computer, and insert a code to thwart detection. Then the hacker places an autorun file to steal your data and possibly spread it to other computers or remote hosts. Emotet is an advanced trojan program that spreads rapidly and attempts to obtain the user's online banking information, making the attack very costly (Armendariz 2019). Trojan horses are hard to defend because they are easy to write. In order for a trojan horse to be prevented, it is recommended that a user reinstalls the operating system. Users should be careful in installing software and look into it to see if anything seems suspicious. Some threats can be very severe and very sophisticated, hiding deep in the system and going

unnoticed by antivirus software. Reinstalling the operating system is the best chance of getting rid of the malware before it starts to spread (Norton 2018).

Because of the increased use of social media, social engineering is becoming more of a common malware attack. Social engineering is when a hackers uses “people skills” to trick others into revealing private information, taking advantage of the human element of security systems (Bidgoli 2019). It is a technique that has the user willingly give up their personal information and possibly install malware. Two types of social engineering attacks are fake downloads and phishing links. A fake download occurs when a message flashes on your screen saying there is a threat detected and asking if you want to download an antivirus software. The user downloads the software and ends up being a malware attack. A phishing link is a link that redirects the user to a fake website that contains malware, tricking the user into sending personal information to the hacker. Users can protect themselves from social engineering by downloading trustworthy antivirus software, using a free website scanner on the Internet to verify that the link is safe, and, when the apparent attack is in the form of an email, contact the person in a separate email to confirm that the email is legit (Comodo 2019).

Malware does not have to be in just one form for it to attack a computer. A malware attack can be a blended threat that contains characteristics of multiple forms of malware that can damage a computer or network in a number of ways (Bidgoli 2019). Most malware today is a comination of traditional programs. For example, a malware attack can start out like a trojan in concealing its attacks, but then once executed, it becomes a worm and spreads across other networks (Grimes 2019). It is also common for a malware attack to conduct identity theft by stealing a password and then steal money out of a bank account and/or steal banking information from a user or a business. This is usually done as a phishing or social engineering attack

(BullGuard 2012). One modern type of this attack is Loyphish, which uses a malicious phishing web page that is used to steal the login credentials for your bank account. It does this by disguising itself as a legitimate banking web page and tricks you into completing an online form, submitting information to a remote attacker (Armendariz 2019).

All of these types of malware attacks should make users concerned with the protection of their device. Fortunately, as the amount of malware attacks that can be executed have increased, so have the amount of actions that can be done to prevent a malware attack from happening. Many measures can be taken to help stop a malware attack, including: biometric security measures, non-biometric security measures, physical security measures, and access controls. Biometric security measures use a physiological element unique to a person that cannot be stolen, lost, copied, or passed on to others. This includes facial recognition, fingerprints, and retinal scanning. Non-biometric security measures use software systems to validate the integrity of a user. This includes callback modems, firewalls, and intrusion detection systems (IDSs). Physical security measures control access to computers and networks, securing them from theft. This includes cable shielding and corner bolts. Access controls are designed to protect systems from unauthorized access in order to preserve data integrity. This includes using passwords, virtual private networks (VPNs), and data encryption. According to Bidgoli, the main guidelines for building a comprehensive security system to prevent a malware attack are as follows: raise employee awareness, use strong passwords, install software updates, limit computer access to authorized personnel only, use biometric and/or non-biometric security measures, and keep sensitive data in secure locations (Bidgoli 2019).

Malware attacks are becoming more common by the day and are causing massive amounts of damage (Norton 2018). Millions of hackers across the globe are trying to get into

someone's computer to steal their information and destroy their device. Users should not wait until they get attacked before taking action. They should take the necessary steps to protect themselves and minimize the risk of being a victim of a malware attack. Without taking proper precautions, users face the risk of losing their data and/or their personal information.

References

A definition of malware. (2012). Retrieved October 12, 2019, from https://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/malware-definition,-history-and-classification.aspx.

Armendariz, T. (2019, June 24). Top Malware Threats and How to Protect Yourself. Retrieved October 12, 2019, from https://www.lifewire.com/top-malware-threats-153641.

Bidgoli, H. (n.d.). *Management Information Systems* (9th ed.). Cengage. doi: 2019.

Grimes, R. A. (2019, May 1). 9 types of malware and how to recognize them. Retrieved October 12, 2019, from https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html.

NortonOnline. (2018). What to do If you're a victim of malware. Retrieved October 12, 2019, from https://us.norton.com/internetsecurity-how-to-what-to-do-if-youre-a-victim-of-malware.html.

What are Malware Threats? (2019, January 15). Retrieved October 12, 2019, from https://enterprise.comodo.com/what-are-malware-threats.php.