Network Intrusion and Malware Analysis on a Network

Heather J. Hirschey

Network Defense and Security

COM - 450

Saint Leo University

Abstract

This paper is about the primary network security tools equipped in most companies or businesses, depending on their size. Along with what happens when malware gets on to your network. What are the different types of malware software out there, and what information or goal is the malware trying to accomplish? Then your last line of defense incident responders and their process to tackle the malware.

Network Intrusion and Malware Analysis on a Network

In today's world, there are constant attacks on a business' network. As a business, they must take proper action to prevent these attacks; otherwise, they might lose everything depending on the severity of the attack. The incident responders must know what tools are installed on their network that helps in the prevention of malicious activity. They also need to have a deep understanding of how the malware got on to the network and the different types of malware. They also need to understand the behavior and the goals of the specific malware that intruded on to the network. Finally, how they react and what the procedures do they typically follow once the malware is detected.

Network Security

Most companies have a standard use of different network security tools that help prevent malicious activity on their network. The first one is access control, which is the control of users and what type of access they are allowed. “Using security policies, you can restrict network access to only recognized users and devices or grant limited access to noncompliant devices or guest users (Types of Network Security, 2019).” Once a user has access to their device that they are using there needs to have adequate protection. One part of this is application security. Application security is the combination of hardware and software to monitor issues, keep up-to-date software, and patch software when needed. E-mail security is a key part. With an abundance of threats that happen through e-mail, for example, phishing, malware, scams, and suspicious links, this needs to have the proper security to prevent these threatening e-mails coming through the network. E-mail security software filters out incoming threats to the network along with the ability to prevent outgoing mail from preventing the share of certain information. Web security also helps limit “internet access for employees, intending to prevent them from accessing sites

that could contain malware. It also blocks other web-based threats and works to protect a customer's web gateway (Types of Network Security, 2019)." There is also antivirus and anti-malware software that is usually installed on all workstations to monitor the network in real-time they also provide scans of the workstations to check if the is suspicious files or behavior. Most antivirus and anti-malware software offer removal capabilities. After the workstations are protected, there are measures to take to help protect the overall network security. A firewall is a common element used as they operate as a guard between a network and the wider internet. Firewalls can filter incoming and sometimes outgoing traffic by the rules and policies set in place by a company that prevents threats from accessing the network. Depending on the size of the company, they might also have network segmentation. Dividing and sorting the network into different sections can limit access to employees, isolate compromised devices, and is easier for implementing certain policies on the network. The last important tool to help network security is security information and event management (SIEMs). These security systems usually consist of host-based and network-based intrusion detection systems (IDS) along with intrusion prevention systems (IPS). "The concept of an IDS is a system that watches internal hosts or networks for symptoms of compromise or intrusion…The IPS strives to detect the attempt to attack or intrude before it has the opportunity to be successful. Once an attempt is detected, the IPS can respond to prevent the success of the attempt rather than waiting until after
a successful breach to respond (Stewart, 2014, p.37)." All of these network security tools help prevent malicious activity from getting on the network. Still, sometimes that is not enough, and you have to have designated people ready to respond to the incidents that do happen. They must find out how the malware got on the network in the first place and what type of malware it is.

Malware on the Network

One of the first questions asked when malware is found on the network is where did it come from? Answering this question is very important to ensure that how the malware got on the network does not happen again if possible. Most attackers leverage one of the following weaknesses: physical vulnerabilities, network design vulnerabilities, network configuration vulnerabilities, protocol vulnerabilities, application vulnerabilities, control vulnerabilities, and human vulnerabilities (Datt, 2016, p. 30). When the analyst finds the specific vulnerability, then they must take preventive action, so the hole is no longer on the network. They must also identify what type of malware is on the network.

When referring to malware on the network, it is any malicious software. There are a variety of different types of malware, which "we will break them down into six categories: viruses; worms; trojans; rootkits; spyware; and malicious adware/scareware (Schneider, 2012)." Each of these different types of malware can do different things and have different goals once they get on the network.

Behavior and Goals of the Malware

Viruses are very similar to a biological virus, except they infect computer files when the user that has an infected computer opens other files; those files get infected, and if the user passes those files to another computer, that computer now becomes infected as well. Some computer virus is designed to stop your computer from operating as normal by damaging programs, snapping computer memory, or flooding with network traffic. Others delete your files or reformat your hard drive. All of this is designed to cause your computer's performance to slow down, data loss, computer crashes, or for your computer to behave erratically.

Worms are similar to viruses, except they do not need a user's interaction, and they duplicate themselves from computer to computer. Worms have the ability to modify and delete

files, and they can inject malicious software, steal data, install a backdoor, allow someone else controls over the computer, or just make copies of the worm.

Trojans or Trojan horse is a mechanism of delivering malware that is embedded inside a program. A perfectly good program can be taken and then have malware embedded into it, so once it is executed, the malware is also executed. Due to it being able to carry any payload wanted by an adversary, several different goals could be possible; it all depends on what payload is being used.

Rootkits are the toolkits for the adversary. They act “like a device driver and positions itself between the kernel and the hardware. From there, the rootkit can selectively hide files on storage devices and active process in memory from being viewable, accessible, or detectible by the OS (Stewart, 2014, p.128)." With a rootkit installed on a device, the adversary can completely take over the computer, which they can use it in other malicious ways.

Spyware is used to gather information on a user. Different types of spyware go after different things, but they have the ability to keystroke logging, browsing data, login credentials, applications launched, e-mails, instant messages, files, screen captures, audio, camera, and network activity.

Adware is used for advertisements. It uses a version of spyware to gather information on what the user likes and is currently searching or interested in to provide advertisements for the user. It also makes sure these advertisements are relevant to you by looking at the device location. It is used to make money for its developers. Sometimes the ads can be hijacked by criminals and have malware in it, also called malvertising.

How do Incident Responders Handle it

Once one of the forms of malware is found on the network and is identified, then an Incident Responder must act quickly. They usually have the following questions that they try to answer. “Who is behind the incident? What actually happen? Where was the impact felt? Or which resources were compromised? Why was it done? How was it done (Datt, 2016, p. 3)?” Incident-responders have come up with a six-step process to react to the situation correctly. The six-step process is 1. Planning and preparation 2. Identification and evaluation 3. Containment and mitigation 4. Eradication and recovery 5. Investigation and closure 6. Lessons learned. "During an incident, it is important that the team document everything that happens because investigating computer crime is complex and involved. Missteps can render evidence unusable in a court of law. This means that team members must be knowledgeable about the proper procedures and must have had training on how to secure and isolate the scene to prevent contamination (Gregg, 2015, p.380).” Most analysts start with static analysis using antivirus scanning, hashing (the fingerprint of the malware), finding strings, packed and obfuscation, portable executable file format, and linked libraries. With dynamic analysis, they look at running the malware in sandboxes, on an isolated virtual machine, monitor with Process Monitor, viewing process with Process Explorer, comparing registry snapshots with Regshot, faking a network, packet sniffing with Wireshark, and using INetSim. With these two different types of analysis, you can gather a lot of information on what the program/code is doing. After finding the information that is needed from the analysis, you can proceed with the six-step process to secure the network from the harm of the malware.

Conclusion

Unfortunately, malware is one of the most common computer intrusions, and once it is on your computer, it could infect your network. Knowing what type of malware is on your computer or

network and what information it is trying to obtain can be beneficial in the analysis and stoppage of the malware. Incident Responders also need to know and understand the different goals that come with a different type of malware. Most importantly, they need to understand how the malware came on to the network and how to prevent it from happening again, along with removing the malware from the network. It is important to remember that "no single tool can do everything. A lone IDS cannot provide true security. However, when combined with firewalls, encryption, system hardening, physical security, policies such as incident response, and malware analysis, an IDS can start to enhance security and play an effective role (Gregg, 2015, p. 397).”

References

Datt, S. (2016). *Learning network forensics: identify and safeguard your network against both internal and external threats, hackers, and malware attacks.* Birmingham, (U.K.): Packt Publishing.

Gregg, Michael. *The Network Security Test Lab : A Step-By-Step Guide*, John Wiley & Sons, Incorporated, 2015. ProQuest Ebook Central, http://ebookcentral.proquest.com/lib/saintleo/detail.action?docID=4040350. Created from saintleo on 2020-04-14 19:24:51.

Schneider, D. (2012). The state of network security. *Network Security, 2012*(2), 14-20. doi:10.1016/S1353-4858(12)70016-8

Stewart, J. M. (2014). *Network security, firewalls, and VPNs*. Burlington, MA: Jones & Bartlett Learning.

Types of Network Security. (2019, October 16). Retrieved from https://www.solarwindsmsp.com/blog/types-of-network-securit