Ian Waweru

Susan Zehra

Cyber fundamentals

11/6/2022

Rootkit and Cyber chain

 Cybercriminals will do anything to get into your computer system. They can infect a computer by using viruses, worms, malware, and more. These malicious programs can be very dangerous to a system. A rootkit is an example of a type of malware that can give a cybercriminal the ability to take over a computer system. Rootkit malware is dangerous it can cause major damage to a system and it’s also hard to locate and dispose of. A cybercriminal can do a couple of things once they’ve controlled your system. For instance, they can obtain your password and with that, a hacker can access your credit card information. Since rootkits are hard to detect it can cause damage for a long time. There are times when it can be impossible to fix, and the only option would be to erase the computer operating systems. There are five types of rootkits that can cause major problems for systems. The first type is called hardware or firmware rootkit. This malware can infect a system hard drive and that gives hackers the ability to intercept data that’s written on a disk. The second type is known as the Bootloader rootkit. This type of rootkit affects the computer’s bootloader by replacing it with a hacked one. The third type is known as a memory rootkit. This type of attack targets computers’ random-access memory (RAM) and disrupts it. The fourth type is called application rootkit and it attacks files in a system and converts them into application rootkits. The final type of rootkit is called a kernel-mode rootkit. This type of rootkit targets the core of a computer, and it can give hackers the ability to change its operating systems. There isn’t a lot we can do to defend against this type of attack because they can be difficult to discover. There are a couple of ways that we prevent an attack from occurring. For example, don’t ignore system updates, watch out for phishing emails, and be careful what you download. Organizations have found ways to protect themselves from hackers and one example of that would be the use of a cyber kill chain. The cyber kill chain is like a model that the military would use. The model shows us in steps how a hacker could attack a system based on occurring attacks. The goal of this framework is to get a defender to understand an attack and give them a better chance of stopping attackers. The cyber kill chain model can help us get a few steps ahead of an attacker by intercepting them and giving the defenders a chance to detect them. There are seven important steps this model follows. The first step is called reconnaissance and it talks about how hackers will target an individual based on their internet search or even through a phone call. A company can stop these attacks by taking cell phones from employees before discussing sensitive information. The second step is called weaponization and they can neutralize attacks through security controls. The third type is called delivery and these attacks are caused by infected USB drives and can be stopped by other technical industries. People also can help stop phishing attacks by making sure not to click on random emails. The fourth and fourth steps are known as exploitation and installation. Exploitation states that employees should be aware of systems by making sure they are running and updated. They should also ensure that the anti-virus running for the protection of sensitive data. Installation states that companies have updated the protection of their devices and malware can’t get installed upon them. The final two steps are called: command and control, actions on objectives. Command and control state that once a hacker gains control of a system you must contact them to gain control. Action and objective state that we should be more aware of these attacks, and they can be prevented by using stronger passwords or detecting login behaviors. I think that these steps will benefit in combating rootkit attacks. One step I would add is the addition of a VPN. Companies can benefit from using their server rather than a public one and making it even more difficult for hackers to exploit.