CYSE 462: Assignment 11
Rootkit: Cyber Kill Chain

Kevin Durand
Kdura002

Rootkit Overview

Rootkits are malicious software that are able to find their way into a computer system that offer administrative access to a malicious user, on a computer or server. When the rootkit is set up it poses as either a legitimate program, or is inserted as a vulnerability into a system, and is accepted as a boot program. When the computer first boots up, this program is able to start running in the background as a kernel level program; after the program is run, the malicious user is now granted administrative access to the computer. Another way is to write the program to a disk, through BIOS, and then implant themselves and steal data from that disk. There are many different rootkits, and these were just two examples.

Cyber Kill Method

There is a particular model for how an attacking program, like the aforementioned rootkit, is able to find its way into the system; this model is labeled the Cyber Kill model and has seven steps. Most programs, as detailed by the first step, are for the software to gain information about the system; during this detection phase the attacker is looking for a way into the system. Next, once the program has sniffed out possible modes of entry, they enter into the system to start their attack; this second step is known as the weaponization phase, with the information gained they are able to start their attack. For certain rootkits the weaponization phase is when they use a program's vulnerability to gain access to the computer system. Now that the program is able to access your system it goes into the next phase of the model, or the delivery phase; very concisely the program uses the newly found entry to deliver the actual program. With the delivery of the malicious software, there is now the exploit phase/installation phase where the program executes whatever attack it was going to do, generally by first installing into the system.

With the program installed and running, it is now time for the program to send back out information; at this point the program reaches back out to the attacker, letting them know access is granted and giving means to continue further attacks. Lastly, in the cement phase, the program puts itself into the system, making sure to not allow the program to be removed by the host computer. This model explains the steps for how a typical program is able to attack your computer.

Expanding Cyber Kill Method

While the cyber kill model presents a good understanding of how programs attack a host computer, rootkits have a distinct way to be activated that is not covered. One of the ways that a rootkit is able to gain access is through social engineering; some rootkits pose as legitimate programs or extensions to programs being downloaded. In order to cover the trojan horse rootkits, conning needs to be added as a method before or after the detection phase; the reason why this needs to exist is because when the program is presented as legitimate software, it is as if the software is conning a person into initiating the attack unknowingly. Next, in this same example, another method should be added as a sub-method to delivery, called downloading. When the person has been successfully conned by the attack, they then need to download the program and allow it access to their computer. Delivery is different from downloading in that the action of letting the program onto the system falls on the host, but not the attacker. The best way to combat these steps, would be to teach users discretion and knowledge about how such attacks are able to be employed.

References

1. https://us.norton.com/blog/malware/what-is-a-rootkit-and-how-to-stop-them
2. https://www.netskope.com/security-defined/cyber-security-kill-chain
3. https://www.imperva.com/learn/application-security/rootkit/