Differentiate between Gootkit, Bootkit and Rootkit

Along with the development of the technology world in general and the internet in particular, security threats are also evolving in both quantity and danger level.

Along with the development of the technology world in general and the internet in particular, security threats are also increasingly evolving in both quantity and danger level.

If you are interested in network security / information security, Gootkit, Bootkit and Rootkit are probably concepts you've heard about. So what is the difference between these 3 concepts? We will learn together shortly.

What is gootkit?

1. Gootkit is a trojan malware, first discovered in 2014.
2. Gootkit has the ability to hack into bank accounts, steal login information and manipulate online transactions.
3. Gootkit uses the following three modules: The Loader, The Main Module, and the Web Injection Module (malware injection module). The Loader is the first stage of the attack process, when the trojan sets up a continuous environment. The Main Module will then create a proxy server that works with the Web Injection Module.
4. Gootkit has no known propagation process. It uses phishing email, taking advantage of toolsets like Neutrino, Angler and RIG to spread to the targeted systems.

What is rootkit?

1. Rootkits are secret computer software designed to perform a variety of malicious activities, including password theft and credit card information or online banking information.
2. Rootkits can also give an attacker the ability to disable security software and record information as you type, simplifying the process of stealing information for cyber criminals.
3. There are 5 types of rootkits: hardware or firmware rootkits, bootloader rootkits, memory rootkits, application rootkits, and application rootkits (kernel).
4. Rootkits can take advantage of phishing emails and infected mobile applications to spread into large-scale systems.

What is bootkit?

1. Bootkits are a more advanced, complex and dangerous type of rootkit that targets the Master Boot Record on the computer's physical motherboard.
2. Bootkit can destabilize the system and lead to a 'blue screen' error or prevent the operating system from starting.
3. In some cases, the bootkit may display a warning and require a ransom to restore the computer to normal operation.
4. Bootkits generally spread via floppy disks and other bootable media. However, recently, this malware has also been recorded for distribution via phishing email software programs or free download data.

Understanding the basic differences for these 3 malicious agents plays a very important role in the construction of defense systems as well as troubleshooting of security incidents.