A rootkit is one of the most difficult types of malware to find and remove. Once a rootkit installs itself on your computer, it will boot up at the same time as your PC. There are various forms of rootkits which different degrees of severity. Below is an illustration of the layered differences in the severity:

In week 5 lecture, we discussed about the most severe rootkits which are the kernel rootkits. This type of rootkit is designed to function at the level of the operating system itself. This means the rootkit can effectively add new code to the OS, or even delete and replace OS code.

Rootkits have a tendency to target important structures within the Windows operating system for the purposes of stealth and persistence. This is also known as hooking. Below are some examples:

* System Service Descriptor Table (SSDT) – is an internal dispatch table within Microsoft Windows. This is a structure that is normally “hooked” by a rootkit. The SSDT table holds the pointer to kernel functions, which are used upon system call invocation.
* Interrupt Descriptor Table (IDT) – is used by the processor to determine the correct response to interrupts and exceptions. Some Windows programs hook calls to the IDT. This involves writing a kernel mode driver that intercepts calls to the IDT and adds in it’s own processing.

Below is a simple example of how a rootkit can manipulate calls to the IDT.

[ROOTKIT PICTURES]

Furthermore, below is an article of a rootkit attack involving the Windows SSDT.

<http://resources.infosecinstitute.com/hooking-system-service-dispatch-table-ssdt/#gref>

Most recently, bad actors have started to migrate towards to digital certificates as a means to successfully installing malware on a victims machine. A certificate is issued by an organization recognized as “trusted’ by the parties involved and is used ordinarily for operations of public key cryptography.

However, digital certificates can be used abused to conduct illicit activities like cyber espionage, sabotage or aid in the dissemination of malware. This is a highly valuable asset for actors since it can grant their application low level access to the victims machine.