INFOSEC101
CONFIDENTIALITY • INTEGRITY • AVAILABILITY

February 21,2014 Release #254

--Begin Transmission--

BOOT SECTOR MALWARE

Lets take a look at it:

Boot sector malware spreads by modifying the program that enables your computer to start up.
Compared to other types of malware, a boot sector virus can be fairly benign - simply taking room up in memory. However, a boot sector virus can also contain a malicious payload.

When you turn on a computer, the hardware looks for the boot sector program, which is usually on the hard disk (but can be on a CD/DVD or Flash Drive), and runs it. This program then loads the rest of the operating system into memory.

Boot sector malware replaces the original boot sector with its own, modified version (and usually hides the original somewhere else on the hard disk). The next time you start up, the infected boot sector is used and the malware becomes active.

Boot sectors are now used by some malware designed to load before the operating system in order to conceal its presence (e.g., TDL rootkit).

How to deal with it:

- The simplest method to prevent a boot sector viruses is to change the CMOS settings to boot from the local C:\ drive first, rather than from floppy. Most modern BIOS is already configured to boot from the hard drive first.
- To combat this behavior, the System BIOS often includes an option to prevent software from writing to the first sector of any attached hard drives; it could thereby protect the Master Boot Record containing the partition table from being overwritten accidentally, but not the Volume Boot Records in the bootable partitions.
- Depending on the BIOS, attempts to write to the protected sector may be blocked with or without user interaction. Most BIOSes, however, will display a popup message giving the user a chance to override the setting.

--End of Transmission --

Information Security: It's a Shared Responsibility

REFERENCES

http://www.sophos.com/en-us/threat-center/threat-analyses/threatsaurus/a-to-z-of-threats/b/boot-sector-malware.aspx

http://en.wikipedia.org/wiki/Boot_sector

//antivirus.about.com/od/antivirusglossary/g/bootsectorviru

Document Code: 2014ICT_15SECA008