Common InfoSec Terms

Virus

This is a broad term but refers to a malicious piece of code that can cause a computer system to malfunction in a variety of ways to the detriment of the machine or its user. Effects can range from upsetting the use of programs such as Word or Excel, making data inaccessible, slowing the speed of the machine to simply downloading advertisements. Basic viruses can be defended against using robust anti-virus software.

Worm

A worm is a form of virus that replicates itself and then moves to another computer or system quickly and without permission. It uses computer networks to duplicate rapidly and thrives on systems without adequate defenses in place. Again, antivirus software is a good place to start to defend against worms.

Trojan

A Trojan Horse is a virus/malware that disguises itself in some way with the intention of tricking the user to allow it onto the machine's system. It often hides itself within a folder of genuine files and when the unsuspecting victim opens the file, the malicious content executes. Businesses need to employ strong anti-malware and endpoint protection software to defend against Trojans and ensure they scan all incoming files. Effective firewalls are a good defensive technique against Trojans also.

Malware

Malware (short for malicious-software) is an umbrella term used to describe a host of different viruses, worms and Trojans ranging from the relatively harmless to the very malicious. It is Software or Firmware designed to infiltrate or damage a computer's system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner's data, applications, or operating system.

Adware

Adware (short for advertising-supported software) is a form of Malware that's purpose is to display advertisements. It commonly displays advertisements via pop ups on websites or in free versions of software. Adware often display itself in ways that are intrusive to the user causing a negative browsing experience. Although more annoying than harmful, Adware is often coupled with Spyware (see below).

Spyware

As the name suggests, Spyware is a form of Malware which spies or monitors victim machines in order to gain information which can be used for malicious purposes. Spyware can monitor a user's online activity, gain login credentials and even log the keystrokes users are inputting to their keyboard. It then reports this information back to its creator who can then use the information to access personal online accounts. Good anti-virus software and regular scanning are needed to avoid Spyware.

Ransomware

Ransomware is a form of malware that infects a victim's system by encrypting or blocking access to all folders and files on the user's network. The victim must then pay money (i.e. a ransom) for access to the

blocked files to be restored. Payment is usually demanded via an untraceable cryptocurrency such as Bitcoin. It is a favorite with organized hacking groups as it gives them a revenue stream to fund their extensive efforts.

Phishing

Phishing is the practice of a hacker attempting to fool an unsuspecting user into accessing a malicious link or downloading an infected file through the practice of Social Engineering. A Hacker will send an email to an employee pertaining to be from a legitimate business with offers via “The Link Below” or in “The Attachment.” The unsuspecting employee clicks the link or downloads the attachment which then downloads malware or ransomware. As the user allows the code to download or the link to execute, this can enable the malware to bypass traditional anti-virus software or inadequate firewalls, heightening the impact.

Social Engineering

Social Engineering goes hand in hand with Phishing and involves a hacker looking for information from an unsuspecting employee in a variety of ways to gather information to launch a targeted attack. For e.g. a hacker may make a phone call to the target company, asking for names of individuals and their job titles etc. They can then compose a Phishing email (see above) that will look much more realistic and more likely to gain a click or download.

DDoS attack

A Distributed Denial of Service (DDoS) attack is an attack on a website whereby hackers overload the target site with fake web traffic with the intention of it crashing due to an overload. Many small business websites fall victim to DDoS attacks as they lack basic security in place. This threat can be mitigated against with the application of a Web Application Firewall (WAF)

Rootkits

Type of malicious software that when installed without authorization, can conceal its presence and gain administrative control of a computer system. It differs from viruses and ransomware as the aim of a rootkit is to remain concealed from notice by the user, exfiltrating data overtime. Powerful anti-malware solutions are required to detect rootkits on computers.