encription
ethical hacking services

Spyware vs. Viruses

A Comparison of Today's Top Computer-Based Threats

In this age of broadband, wireless, and network interconnectivity, we enjoy the unprecedented power of information exchange at our fingertips. But along with the overwhelming benefits of all this phenomenal connectivity comes numerous threats to computer security – including productivity, data integrity, and confidentiality. The top two categories of computer threats today are viruses and spyware.

The first recorded widespread instance of a computer threat was in 1986 when a piece of code started to replicate itself to other floppy disks or files. Eventually, the term "virus" was coined and started this threat category of malicious software, which is now a mature but continuously evolving threat. A virus can destroy your computer or data, cause system crashes, or perform other malicious activities. In general, viruses are inherently malicious, designed to be destructive in nature.

Spyware, on the other hand, which started to spread wildly in 2002, is intended to operate "under the radar". Rather than destroying information, which is the intent of many viruses, spyware exists to steal information and report back to the writer or a designated third party. As with viruses and other computer-bourne threats, the spyware problem continues to grow and evolve, continuously finding new techniques to infect new systems and remain in place.

The following explores some of the differences between Spyware and Viruses.

Who creates Spyware and Virus programs?

Most virus writers develop their programs predominantly to show the world how smart they are. As such, most are bent on infecting as many users as possible, to claim some degree of notoriety – and therefore bragging rights. Many want to impress their friends and fellow writers. Others use their creations to "battle" other writers, to prove their technical expertise – a kind of game, with computer users as the innocent victims. By spraying the world's computers with the equivalent of electronic graffiti, virus authors' motivations are clearly towards being popular, showing off their programming prowess or simply with the intent of wreaking some havoc in the digital world.

Spyware programs, on the other hand, are written by software developers seeking financial gain. Spyware is the equivalent of a cash register or cash point in which the authors have many ways of making money – and new revenue schemes continuously emerge. The amount of revenue made from spyware depends on the number of computers infected, and the amount of time it can remain on the computer, free to communicate information back to a web server. Most spyware is adware and makes its money by showing some sort of ads or by hijacking web browsers to pages that can generate revenue for the authors.

What are the resources available for each threat author?

Virus writers are armed with their personal knowledge of systems and are often part of a group of writers who exchange information to progress their ability in attacking a system. They create without any monetary motivation. Buggy or non-working code is common.

Conversely, spyware authors often have access to more extensive funding. They can afford to have a development process complete with labs and a testing environment to apply Quality Assurance to the programs that they are developing. Some mainstream advertisers have willingly funded spyware companies by paying for the ability to develop highly-targeted advertising campaigns. With all the money being made, most authors also have access to books, as well as the ability to purchase legitimate software and attend professional training courses.

What about the legality of the by-product?

Since viruses often lead to loss of data or corruption of the system, they have been perennially tagged as malicious, thus making their creation illegal in most countries around the world.

Spyware, however, resides in more of a grey area. Some freeware such as an electronic wallet that keeps track of your credit card numbers and passwords may function as spyware and show ads based on your shopping habits. But a user may feel the functionality of the freeware is worth the privacy invasion and the inconvenience of the pop-up ads generated by the spyware.

Plenty of spyware is also made to appear as formal software with corresponding End User Licensing Agreements (EULAs), which are not present with viruses. Some EULAs are very open about what they will do to the user's computer and how they can use the user's data – but the EULA may be as long as 20 pages or more of legal language that no average person can reasonably be expected to read or understand in its entirety. A classic spyware EULA trick is to state that part of the EULA is on a website which may change and it is the user's responsibility to check the web site for any changes. Many EULAs also state that the user implicitly agrees to any and all changes by continuing to run the software. Some even include double-negative statements like "Do you want to discontinue the uninstallation?"

This is the tricky part with spyware since it can generate defamation lawsuits against security vendors that attempt to eradicate these infections – creating a legal battle that would simply never occur in the virus world.

How do they get distributed?

Viruses typically propagate either via email – by tricking the user into launching an attachment that contains the virus code – or by exploiting system vulnerabilities. Once the code is executed, viruses are typically programmed to take control of the user's system, enabling them to perform a wide array of activities.

Spyware, in contrast, is often bundled with freeware. A simple agreement to a plug-in install on a website you visited can lead to the introduction of spyware on a system. It is usually part of an army of distribution points where spyware from quasi-legitimate companies will put up some sort of End User License Agreement (EULA) that may or may not specifically reveal its intent to monitor your computer usage and to transmit such information to the web for the spyware company's purposes. Spyware companies find comfort in the small percentage of people who actually read a EULA in its entirety, especially a long EULA – and of those who *do* read it, few of them will actually understand the often complex Legal prose. As a result, the vast majority of users simply click "Yes I Agree", without bothering to read the full agreement. Spyware companies pay a bounty per installation of their spyware, which makes it attractive to freeware authors to bundle spyware payloads with their creations as a way to generate revenue.

What is the user experience during installation?

Viruses typically install with minimal or no interaction with the user. When the code is executed, the objective of a virus is to surreptitiously perform its propagation routine, prior to administering its payload – which can include such malicious activities as data destruction, degradation or elimination of system performance.

The level of user interaction employed by spyware varies dramatically from case to case. As mentioned above, some spyware is appended to freeware and relies on the user "agreeing" to a complicated EULA – either by barraging the user with confusing questions and messages to prey on the user's impatience, or by tricking the user into agreeing to something he/she did not fully understand. Other common installation methods utilised by spyware authors require absolutely no user interaction, whatsoever. In "drive-by downloads", just visiting an infected Web site is sufficient to install spyware on a user's system with neither their permission, nor their knowledge. Porn and on-line shopping sites are both notorious for this type of spyware installation. Spyware is also frequently installed by hijacking *legitimate* software, so the user unknowingly obtains the spyware infection along with the desired software. These are just a few vehicles that enable spyware to be silently installed, without the presence of a EULA, an uninstaller, or anything else that would require any action on the part of the end user.

How difficult is it to get rid of your system of these threats?

Virus writers are more interested in spreading the infection the next computer than they are with ensuring that the program remains installed on a compromised system. This is because the payload in a virus is typically executed immediately, so the damage is done. For this reason, most viruses can be successfully removed by utilizing a good antivirus product which has been updated to include detection and removal for the specific virus or family of viruses.

But spyware is a waiting game. Since its intent is to capture and report personal information, its real value resides in how long it can remain installed on the infected system. The longer it remains installed, the more likely it is to capture the information it was programmed to steal. Therefore, spyware implements a variety of techniques to remain installed in a system. A simple "Add/Remove Programs" can appear to resolve the problem, but the action really only removes the program's visible components, while retaining the collection agent. Another common technique is for spyware is via a partnership agreement that binds it to a freeware in such a way that the freeware cannot be used unless the spyware is also installed.

Spyware exhibits a strong will to live profitably on one machine, rather than to spread like viruses. It can function as a virtual cash point, generating cash for its creators, but only as long as it can keep running on a machine. Many spyware programs are programmed to go great lengths to stay alive, or to reinstall following any attempt to remove them.

User Impact

While viruses tend to be more dangerous in nature, spyware is more of a nuisance. The pain from viruses can be loss of data or a corrupt PC. With spyware, the loss is of privacy and productivity, from the nuisance of popup ads and degradation of system performance, to the theft of personal – and sometimes *sensitive* – information.

Looking Forward

In the digital age, networks and systems are continuously evolving to become more robust, thereby maximizing our convenience and productivity. But with this progress comes new avenues for threats to the security of those networks. Spyware and viruses are likely to continuously evolve for the foreseeable future, as their authors seek out new ways to infect systems and accomplish their tasks. By understanding these threats and taking proactive measures against them, users can enjoy a rich on-line experience, while taking comfort in the safety that they have protected themselves from these and other attacks.

encription limited are experts in the detection and resolution of vulnerabilities which can be exploited by spyware.

Give us a call 01905 754440 or www.encription.co.uk to see how we can help you BEFORE the damage is done.