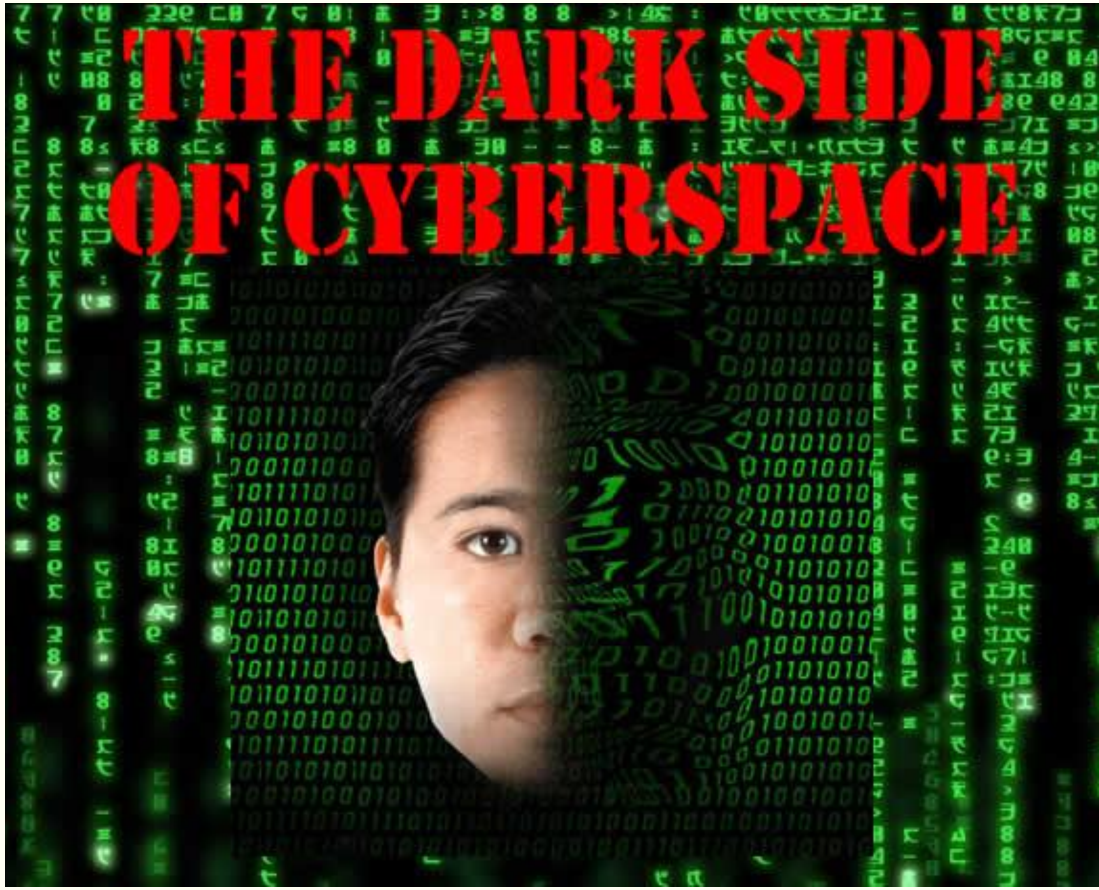
CYBER SPYING IN WORLD TODAY

Cyber espionage

Adil Akhmetzhanov IS-147R



Content

- Cyber spying
- Spyware
- Features of functioning
- History and development
- Scope of Use
- Methods of treatment and prevention
- Reference

Cyber spying

Cyberespionage or computer spying (also used the term "cyber reconnaissance") - a term denoting tend to steal information in order to obtain personal, economic, political or military superiority, carried out with the use of bypass (hacking) computer security systems, with the use of malware software, including "Trojan horses" and spyware. Typically, cyber-espionage operations are illegal in the country of victim, while in the aggressor country they are support at the highest levels.

Spyware

Spyware (spyware software) - a program that surreptitiously installed on your computer to collect information about your computer configuration, user, user activity without consent. Can also perform other actions: changing the settings, software installation without the user's knowledge, redirecting user actions. Now, there are many definitions and interpretations of the term spyware.

Features of functioning

Spyware can carry out a wide range of tasks, such as:

- Collect information about the habits of Internet use and the most frequently visited sites (tracking software);
- Remember keystrokes (Keyloggers) and record screenshots (screen scraper) to continue to send information to the creator spyware;
- Illegally and remotely control a computer (remote control software) - backdoors, botnets, droneware;
- Installed on the user's computer additional programs;
- Used for unauthorized analysis of security systems (security analysis software) - scanners of ports and vulnerabilities and burglars of passwords;
- Change the settings of the operating system (system modifying software) - rootkits interceptors control (hijackers) and so on. - resulting in a reduction of speed of Internet connection or loss of connection itself, the opening of other home pages or removal of certain programs;

HISTORY AND DEVELOPMENT

History and development

According to AOL and National Cyber-Security Alliance of 2005, 61% of respondents of computers contain some form of spyware, of which 92% of users were not aware of presence spyware on their machines, and 91% reported that they did not give permission for the installation of spyware.

History and development

By 2006, spyware have become one of the prevailing threats to the security of computer systems using Windows. Computers in which Internet Explorer serves as the main browser are partially vulnerable not because Internet Explorer is most widely used, but due to the fact that its tight integration with Windows allows spyware access to key nodes OS.

kit phishing malware worm trojan
phishing malware worm trojan virus
ng malware worm trojan virus spam
ware worm trojan virus spam hacker
worm trojan virus spam hackers
rojan virus spam hackers spyware
virus spam hackers spyware securit
spam hackers spyware security root

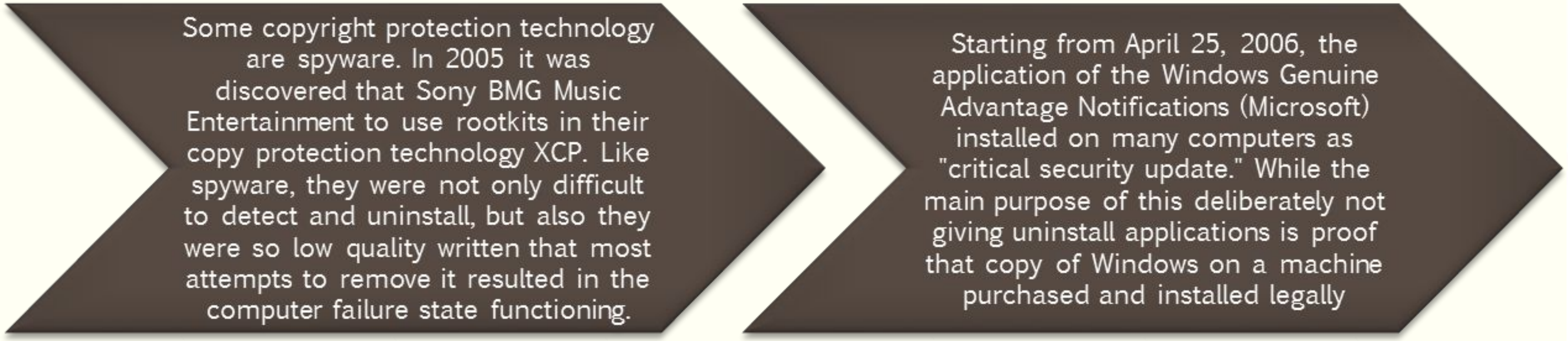
SCOPE OF USE

Among the possible applications of "potentially unwanted technologies" is both legitimate and fraudulent.

LEGITIMATE APPLICATIONS

- Tracking Software (tracking software) is widely used and legal for monitoring PCs.
- Adware can openly be included in composition of free and shareware software. The user agrees to view advertising to have any further opportunity (for example - to use this program free of charge). In this case, the presence of adware should clearly prescribed in the end-user agreement (EULA).
- Software modifications to the system can used for personalization of the desired user.
- Program the remote control and monitoring can used for remote technical support or access to their own resources, which are located on the remote computer.
- Program for automatic download can used to automatically updates, applications and OS updates.
- Program for the analysis of security systems used to study the vulnerability of computer systems and other perfectly legitimate purposes.
- Passive tracking technologies may be useful to personalize web pages visited by user.

DIGITAL COPYRIGHT PROTECTION



Some copyright protection technology are spyware. In 2005 it was discovered that Sony BMG Music Entertainment to use rootkits in their copy protection technology XCP. Like spyware, they were not only difficult to detect and uninstall, but also they were so low quality written that most attempts to remove it resulted in the computer failure state functioning.

Starting from April 25, 2006, the application of the Windows Genuine Advantage Notifications (Microsoft) installed on many computers as "critical security update." While the main purpose of this deliberately not giving uninstall applications is proof that copy of Windows on a machine purchased and installed legally

METHODS OF TREATMENT AND PREVENTION

MEASURES TO PREVENT INFECTION

Using browsers other than Internet Explorer - Opera, Mozilla Firefox, etc. While there is secure browser, Internet Explorer is at a greater risk of the infection due to its extensive user database.

Using the firewalls and proxy servers to block access to sites known to install spyware.

Using the hosts-file, preventing the possibility of connecting a computer to sites known to install spyware.

Download software only from a trusted source (preferably with the manufacturer's website), because some spyware can be embedded in software distribution packages.

Using anti-virus software with the most "fresh" virus databases.

Reference

- *Cyber Spying.* Copyright © Wikipedia 2001-2015. Retrieved March 04, 2015 from http://en.wikipedia.org/wiki/Cyber_spying
- *Spyware.* Copyright © Wikipedia 2001-2015. Retrieved March 04, 2015 from https://ru.wikipedia.org/wiki/Spyware

THANK YOU FOR YOUR ATTENTION