**Handouts of Lecture 22 Professional Practices (IT)**

**Lecture Title: Malware**

**Conficker**

The Conficker (or Downadup) worm, which appeared on Windows computers in November 2008, is notable because computer security experts have found it particularly difficult to eradicate. The worm is able to propagate in several ways. The original variant of the worm spread to computers that were not up-to-date with the latest security patches from Microsoft. The second version of the worm, which appeared about a month later, had two new features that accelerated its spread: the ability to invade computers with weak password protection and the ability to propagate through USB memory sticks and shared files on local area networks.

Early in 2009, between 8 and 15 million computers were infected with Conficker, including portions of military networks in France, the United Kingdom, and Germany.

**Cross-Site Scripting**

Cross-site scripting is another way in which malware may be downloaded without a user’s knowledge. Web sites that allow users to read what other users have posted are vulnerable to this security problem. The attacker injects a client-side script into a Web site. When an innocent user visits the site sometime later, the user’s browser executes the script, which may steal cookies, track the user’s activity, or perform another malicious action.

**Drive-By Downloads**

Many malware creators have hacked into legitimate Web sites and installed software booby traps. In some cases, simply visiting a compromised Web site can result in the unintentional downloading of software, called a drive-by download. Another kind of drive-by download occurs when a Web surfer encounters a pop-up window asking permission to download software. The user approves the download, thinking the code is necessary to view the content on the Web site, but in actuality the download contains malware. The drive-by download problem is growing. The Google Anti-Malware Team has discovered more than three million URLs that initiate drive-by downloads. That may not seem like so many URLs, given the size of the Web, but hackers target the most popular Web sites. As a result, about 1.3 percent of queries to Google’s search engine result in a malicious URL appearing somewhere in the results page.

**Trojan Horses and Backdoor Trojans**

A Trojan horse is a program with a benign capability that conceals a sinister purpose. When the user executes a Trojan horse, the program performs the expected beneficial task. However, the program is also performing actions unknown to, and not in the best interests of, the user. A recent example of a Trojan horse is Mocmex, first uncovered in 2008 in digital picture frames manufactured in China. It spread from digital picture frames to computer hard drives and other portable storage devices people attached to their PCs.

The purpose of the Trojan horse appeared to be to steal passwords to online computer games. A backdoor Trojan is a Trojan horse that gives the attacker access to the victim’s computer. For example, a backdoor Trojan may purport to cleanse malware from a computer, but in actuality it installs spyware.

**Rootkit**

A rootkit is a set of programs that provide privileged access to a computer. Once installed, a rootkit is activated every time the computer is booted. Rootkits are difficult to detect because they start running before the operating system has completed booting up, and they can use security privileges to mask their presence.

**Spyware and Adware**

Spyware is a program that communicates over an Internet connection without the user’s knowledge or consent. Spyware programs can monitor Web surfing, log keystrokes, take snapshots of the computer screen, and send reports back to a host computer. Spyware is often part of a rootkit.

***Adware*** is a type of spyware that displays pop-up advertisements related to what the user is doing. Since people would not intentionally download a spyware program, spyware must get installed using subterfuge. Free software downloaded from the Internet often contains spyware. Alternatively, the spyware may be a Trojan horse, tricking users into downloading it because they think it serves a useful purpose. A Trojan horse containing spyware is an example of a backdoor Trojan. A 2006 survey of US consumers with broadband Internet connections found that 89 percent of them had spyware on their computers.

**Bots**

A bot is a particular kind of backdoor Trojan that responds to commands sent by a command-and-control program located on an external computer. The first bots supported legitimate applications: Internet Relay Chat channels and multiplayer Internet games. Today, however, bots are frequently used to support illegal activities. A collection of bot-infected computers is called a botnet, and a person who controls a botnet is called a bot herder. Botnets can range in size from a few thousand computers to over a million computers. In most cases, people have no idea that their PCs have been compromised and are part of a botnet.

It’s been estimated that as much as 90 percent of spam is distributed through botnets. Bots can also be used as spyware, stealing files or logging keystrokes to gain credit card numbers or other sensitive information. Botnets can also be used to support distributed denial-of-service attacks. The sophistication of bots continues to increase. Computers typically have signature-based detection schemes to identify and destroy bots by looking for particular patterns in their underlying machine code. To counter these detection schemes, programmers are now creating bots that are able to spin off functionally equivalent bots with somewhat different machine code.

**Defensive Measures**

Three defensive measures are important in protecting personal computers from malware: security patches, antimalware tools, and firewalls.

Some kinds of malware exploit vulnerabilities in software systems, and software makers respond by modifying their code to remove the vulnerabilities. At regular intervals software makers release security patches so that the users of the software can update their systems to remove the vulnerabilities that have been uncovered. In fact, most worms exploit vulnerabilities for which security patches have already been created. That means they can only infect those computers that have not been kept up-to-date with the latest patches.

Antimalware tools are designed to protect computers against malware, such as viruses, worms, Trojan horses, adware, and spyware. Antimalware software can be used to scan a computer’s hard drive, detecting files that appear to contain viruses or spyware, and deleting the files (with the user’s approval). The rapid rate at which new malware appears necessitates frequent updating of these tools.

A firewall is a software application installed on a single computer that can selectively block network traffic to and from that computer. A firewall gives the user the ability to control which programs running on the computer are able to access the Internet. One weakness of firewalls is that they are vulnerable to being manipulated by malware. If a computer is infected by a piece of malware, the malware may be able to shut down the firewall, since it is running on the same computer.

**Cyber Crime and Cyber Attacks**

The Internet plays a vital role in the economic life of developed nations. Its effects include streamlining interactions between manufacturers and their suppliers, stimulating the creation of new companies, fostering the development of new business models, making online videoconferencing much more affordable, and changing how people shop. Today, there are more than 80 million dot-com domains. Annual ecommerce sales now exceed $1 trillion. Given the amount of money changing hands, it’s not surprising that organized crime is active on the Internet. The economic importance of Internet based activities also makes Internet infrastructure an attractive target for politically motivated attacks. We begin this section by reviewing three common Internet-based attacks. We then explore how these attacks have been used as a means to achieve criminal or political ends.

**Phishing and Spear Phishing**

A phishing (pronounced “fishing”) attack is a large-scale effort to gain sensitive information from gullible computer users. An attacker sends out millions of email messages from a botnet. The messages inform the recipients that one of their accounts has been compromised and directs them to connect to a Web site to resolve the problem. Targeted users that click on the link encounter an impostor Web site designed to resemble the genuine ecommerce site. Once on the site, they are asked for a login name, password, and other private information. Information collected by the imposter site can then be used for identity theft. According to an industry study, there were at least 67,000 phishing attacks worldwide in the second half of 2010. An interesting development is the increase in phishing attacks on Chinese ecommerce sites, indicating the growing importance of the Chinese economy.

***Spear phishing*** is a variant of phishing in which the attacker selects email addresses that target a particular group of recipients. For example, an attacker may target elderly people judged to be more gullible or members of a group that have access to valuable information.

**SQL injection**

It is a method of attacking a database-driven Web application that has improper security. The attacker accesses the application like any other client of the application, but by inserting (injecting) an SQL query into a text string from the client to the application, the attacker can trick the application into returning sensitive information.

**Denial-of-Service and Distributed Denial-of-Service Attacks**

A denial-of-service (DoS) attack is an intentional action designed to prevent legitimate users from making use of a computer service. A DoS attack may involve unauthorized access to one or more computer systems, but the goal of a DoS attack is not to steal information. Instead, the aim of a DoS attack is to disrupt a computer server’s ability to respond to its clients. Interfering with the normal use of computer services can result in significant harm. A company selling products and services over the Internet may lose business. A military organization may find its communications disrupted. A government or nonprofit organization may be unable to get its message out to the public. A DoS attack is an example of an “asymmetric” attack, in which a single person can harm a huge organization, such as a multinational corporation or even a government.

Since terrorist organizations specialize in asymmetric attacks, some fear that DoS attacks will become an important part of the terrorist arsenal. In a distributed denial-of-service (DDoS) attack, the attacker rents access to a botnet from a bot herder. At the selected time, the command-and-control computer sends the appropriate instructions to the bots, which launch their attack on the targeted system.

**Cyber Crime**

Criminal organizations have discovered that a great deal of money can be made from malware, so many of them have entered the arena, raising the stakes for corporations and individuals trying to protect their systems and sensitive information, respectively.

* Jeanson James Ancheta
* Pharmamaster
* Albert Gonzalez
* Avalanche Gang

Israeli company Blue Security created a spam deterrence system for people tired of receiving unwanted email. Blue Security sold the service to businesses, but individuals could protect their home computers for free. About half a million people signed up for this free service. Users loaded a bot called Blue Frog on their computers. The bot integrated with Yahoo! Mail, Gmail, and Hotmail, checking incoming email messages for spam. When it discovered a spam message, the bot would contact a Blue Security server to determine the source of the email. Then the bot would send the spammer an opt-out message. Spammers who indiscriminately sent emails to millions of addresses started receiving hundreds of thousands of opt-out messages, disrupting their operations. Six of the world’s top ten spammers agreed to use Blue Security’s filtering software to remove Blue Frog users from their email lists.

One spammer, nicknamed PharmaMaster, did not back down. He threatened Blue Frog users with messages such as this one: “Unfortunately, due to the tactics used by Blue Security, you will end up receiving this message or other nonsensical spams 20–40 times more than you would normally”. He followed through on his threats on May 1, 2006, by sending Blue Frog users 10 to 20 times as much spam as they would normally receive. The next day PharmaMaster went after Blue Security itself. He launched a massive DDoS attack from tens of thousands of bots targeting Blue Security’s servers. The huge torrent of incoming messages disabled the Blue Frog service. Later DDoS attacks focused on other companies providing Internet services to Blue Security. Finally, the spammer targeted the businesses that paid for Blue Security’s services. When Blue Security realized it could not protect its business customers from DDoS attacks and virus-laced emails, it reluctantly discontinued its service. “We cannot take the responsibility for an everescalating cyberwar through our continued operations,” wrote Eran Reshef, CEO of Blue Security. “We are discontinuing all of our anti-spam activities”. Blue Security’s decision to fight bots with bots—always controversial—was ultimately unsuccessful.

***Reference***

***Lecture 22 slides: Computer and network security(Cont.)***

***Gao, Y. (2012). Ethics for the Information Age by Michael J. Quinn. World Libraries, 20(1).***