National Cyber Security Awareness Month
(October 2008) Newsletter Series (3 of 4)

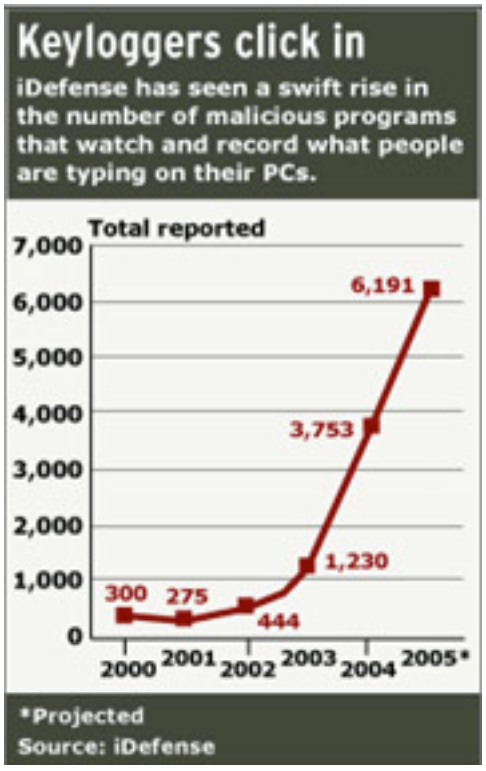
What You Don't Know Can Hurt You

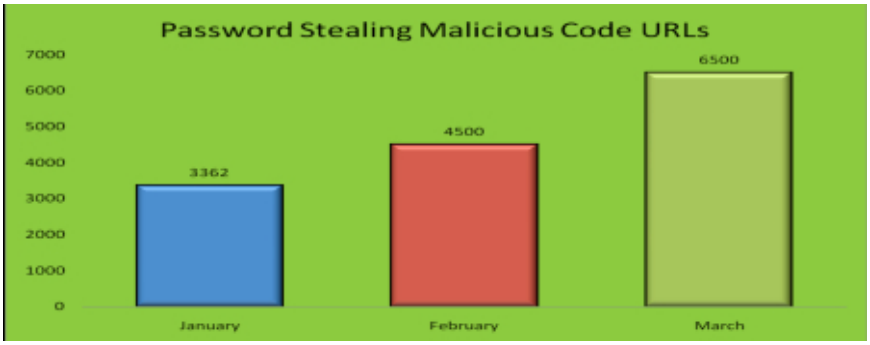
"A computer lets you make more mistakes faster than any invention in human history - with the possible exceptions of handguns and tequila."
~ Mitch Ratliff

Keyloggers – Clandestinely captures keystrokes, screen shots & possibly even web cam video.

For the first half of 2008, password stealers that targeted online games were in first place on the top ten malware list, and, in looking at those included in the password stealer category, game-related malware took 50 percent of the top ten spots (X-Force June 2008).

IDefense (a VeriSign company that specializes in security intelligence) depicts an almost exponential growth in the development of malware designed to capture what you type at your computer. The Anti Phishing Work Group (APWG) reported back in March 2008 that the number of compromised websites that were hosting keylogging applications rose to 6,500.





The result is more keyloggers hosted on more compromised web sites. Yet keep in mind, that most keyloggers are still distributed via email attachments. If they have your user id and password its game over, no university or government can protect you.

ClickJacking – Clickjacking gives an attacker the ability to trick a user into clicking on something only barely or momentarily noticeable on a web page. Once the user clicks, usually on a link but it can be anywhere on the page, a new Web site may appear or software may be downloaded. For example a malicious button that has been overlayed on top of an existing legitimate web page button such that when a user clicks it they believe they are clicking the legitimate button instead of a malicious overlay.

The following YouTube video of a clickjack Proof of Concept (PoC) was put together by a security researcher to show how a user tricked into playing a game may unknowingly grant someone full access to their webcam and microphone. Thereby allowing others to peer into their home via a webcam and eavesdrop on their conversations via a PC microphone.

Our Unintentional Participation in the War of the Virtual Worlds

Unfortunately in the virtual world of the internet computers are attacked all the time. If you have a firewall on your home computer you can see how often you are port scanned. Port scanning in the virtual world is equivalent to someone casing the joint in the real world.

Now on TV (and occasionally in the real world) you will hear about someone being forced to participate in a crime against their will. Have you ever harmed someone unintentionally? How about unknowingly? The following are four very real ways, if we are not careful, that we may be doing just that.

Distributed Denial of Service (DDOS) Attacks – DDOS involves using compromised computers to flood a business with requests for online services to such a point that the business struggles to support their online customers and in some cases may be blown off the internet for hours or possibly days. Crippling DDOS cyber attacks against the countries of Estonia and Georgia are high profile examples of such attacks.

The number of DDOS attacks went up over 300% from 50,650 in 2006 to 157,348 reported so far in 2008 (Shadow Server Foundation). In the case of the Estonia and Georgia DDOS attacks, the motivation was political. The typical motivation for DDOS attacks are financial, including anything from taking a competitor off the internet to holding an organization's access to the internet ransom.

BotNets & Zombies – A zombie (compromised computer) is typically rented for malicious use as part of a botnet (coordinated network of compromised computers). The Shadow Server Foundation estimates that there are upwards of 3,000 botnets controlling upwards of 500,000 zombie computers. The typical zombie is an under protected home computer.

SPAM – The potential use of our WIU or personal email accounts to SPAM others.

Over this past summer four University of Otago staff members responded to a spear Phishing scam with their email IDs and passwords which were later used to send out 1.5 million SPAM messages. With the

ability to send out over 130 billion SPAM messages per day the top botnets propagating SPAM can adversely affect email delivery on the Internet.

SPAM Capacity of Botnets		
Botnets	**# of Bots per Botnet**	**Per Day SPAM Sending Capacity**
Srizbi	315,000	60 billion
Rustock	150,000	30 billion
Cutwail	125,000	16 billion
Ozdok	35,000	10 billion
Bobax	185,000	9 billion
Nuscrypt	20,000	5 billion
Storm	85,000	3 billion
Grum	50,000	2 billion
Total	965,000	135 billion
Source: SecureWorks, April 2008		

Warez - Warez involves illegally obtained software. Botnets are typically used to steal, store or propagate warez, thereby making zombie computers part of the supply chain for illegally obtained software.

"The fascinating thing about this is that the people who owned those computers actually had no idea they were attacking another government. The notion of a personal computer is really counterintuitive. There is no such thing as a personal computer. Everyone's computer can be used to attack another country."
~ Lauri Almann Estonia's Undersecretary of Defense

We've spent the last three weeks familiarizing ourselves with malware and social engineering including some of their consequences. We will conclude this National Cyber Security Awareness month newsletter series next week with steps to protect ourselves, our computers and each other. So for now, think before you click!!!

Regards,

Michael Rodriguez CTSO @ Western Illinois University
MA-Rodriguez@wiu.edu