



SVECC Newsletter

Sunland Village East Computer Club

June 2009

Volume 6 issue 6

Inside this issue:

Malware	2
Malware	3
Send Out	4
White on Blue	4
Power Supply	5
Calendar	7
Exit Laughing	8

Monthly Reminders:

- Run Disk Cleanup
- Run CC Cleaner
- Defrag your hard drive
- Manually Update Windows
- Update Super Anti-spyware
- Run your Anti-virus

Pop-ups Friend or Foe?

Lets talk about Pop-ups.

Pop-ups are unsolicited ads that actually do pop-up on your Desktop or in your Browser. (Internet Explorer, Firefox, etc.)

Those that appear in a Browser Window can be turned off as part of your browser settings. Controls for pop-ups are found under tools.

Pop-ups that appear on your desktop are another matter. They indicate that your system has been compromised.

An example of recent pop-ups are those that indicate you have either spyware or viruses, and offer to correct these problems if you click on a box within the pop-up.

Again these pop-ups indicate that you al-

ready have a serious problem, do not make it worse by down loading these so called helpers.

Keep in mind it often takes over an hour to perform a virus or spyware scan, so how could this so called indicator have done this job in a few seconds.

What should you do?

First; you need to run a good anti-spyware program. The computer club recommends either Super AntiSpyware or Malware Bytes. Either of these excellent programs can help eliminate the spyware that is creating the pop-ups.

Second; you should never open these so called helpers and download their products. If you do, you will have insured that your computer becomes infected and

often times turned into part of a Botnet.

How can you eliminate these viruses if you do click on the download?

Your best bet is to take your computer to a reputable service center and have your drive formatted and Windows reinstalled.

Shops like Serving Online Seniors or SoftQue can pull off all of your personal data, format your drive and return to you a safe, protected computer.

We have talked about these situations at many of our regular meetings and in spite of that, your help group has worked on over 10 of these infections in the closing weeks of our club activities.

Have a great summer and practice safe computing. jz

Malware the rest of the story

By Mary Landesman
Technical Editor, Microsoft Security Research and Response



A significant evolution has occurred in the malware landscape over the past five years — a change of intent from amateur virus writers seeking attention to professional criminals seeking profit. But in the past year, a more abrupt shift has taken place: a change in target, with users squarely in the bulls-eye.

To a certain extent, malicious software has always relied upon the user. In the Sneaker-net era, the boot sector virus often relied on the user to inadvertently leave a floppy disk in the drive during boot-up. And more currently, profit-driven programs routinely try to trick the user into installing software that, unbeknownst to them, will deliver incessant pop-up advertising or redirect their Internet browsing. Yet once the software is installed, the users themselves become superfluous. The target was the computer and the objective was met.

Today's malware is decidedly different. Instead of hijacking the computer for illicit

gains, today's malware is intent on hijacking the user for hard currency, credit card fraud, and outright identity theft. In the current landscape, malware is no longer the end to the means, but rather the means through which the end is reached.

Spam, Scams, and Social Engineering

In 2006, the Microsoft Exchange Hosted Filtering (EHF) service, part of Microsoft Exchange Hosted Services, processed over 110 billion inbound e-mail messages of which 91.56% were classified as spam. Formerly considered a mere nuisance, spam is now the tool of choice for criminal profiteers.

To achieve their goal, criminals typically control large botnets, collections of sometimes tens of thousands of computers infected by backdoor Trojans. The Trojans used to form the botnets are typically installed by downloaders and droppers which, ironically, frequently reach their victims through spam.

In addition to botnets, peer-to-peer (P2P) file-sharing networks are breeding grounds for

malware. Attackers deliberately seed these file shares with backdoor Trojans and downloaders, using file names that match popular program, music, or other coveted files.

Compromised instant messaging and social networking accounts allow attackers to contact others from the context of a trusted friend, thus attachments or links sent to those users are more likely to be trusted as well.

In 2006, 20 percent of all scans by the Windows Live OneCare safety scanner detected some form of malware, and the overwhelming majority was some form of downloader, dropper, or backdoor Trojan. To hide these Trojans, the use of rootkits is on the rise. In the first half of 2006, the safety scanner removed 5,349 instances of rootkits. In the second half of the year, the number increased over four-fold to 21,935.

These carefully hidden botnets provide attackers with a distributed network of compromised systems from which they can work to defraud others with near anonymity.

(Continued on page 3)

To a certain extent, malicious software has always relied upon the user.



Malware the rest of the story (continued)

For example, botnets formed by the Rustock Trojan spread the volume of spam over a wide range of IP addresses in order to bypass threshold restrictions imposed by many ISPs specifically to discourage spamming.

The spam sent goes far beyond simple unwanted advertising. In addition to seeding Trojans, spam often contains a colorful array of scams orchestrated with the intent of gaining users' trust and, eventually, their money.

A few such scams include:

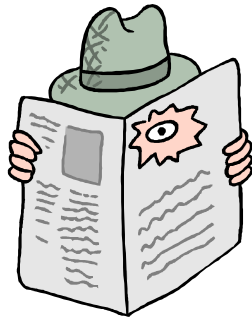
- Lottery scams -- E-mail that fraudulently claims the recipient has won a large sum of money. Respondents are instructed to send processing fees to release the nonexistent winnings.

- Pump and dump stock schemes -- Scammers buy a stock low and try to inflate its price through erroneous claims made in e-mail, selling the stock when prices rise and leaving victims with a worthless portfolio.

- International dating scams -- The promise of

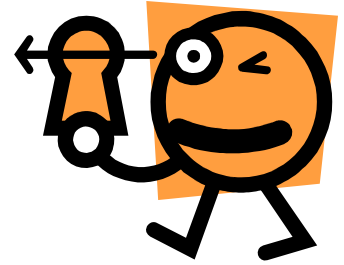
romance entices victims to send money for airline tickets, long-distance phone calls, or fees to bribe emigration officials. Despite the payouts, the object of their affection never appears.

- Nigerian 419 scams -- Named for the section of Nigerian penal code that outlaws this fraudulent activity, the scam predictably entices victims with the promise of large sums of cash. Respondents are cajoled into paying certain fees and bribes, in a similar fashion to lottery and dating scams.

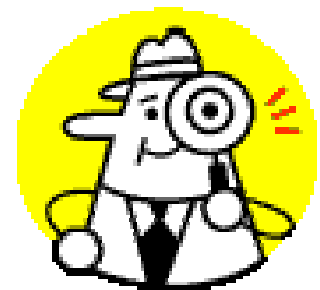


These virtual equivalents of yesteryear's snake oil salesman are just the tip of the iceberg. Zero-day vulnerabilities can fetch prices up to \$25,000 on the Internet black market. In turn, these vulnerabilities are used in highly targeted, methodical attacks aimed at corporate espionage.

Today's malware focus is no longer a battle to dominate the computer; it is increasingly a battle for control of the user's assets. With money as the motive and the user as the target, we can expect to see an even greater number of cleverly disguised scams, phishing, and other socially engineered attacks in the future. The use of targeted rootkit-enabled Trojans will also likely continue to increase across a broad range of vectors, including social networking sites, file sharing networks, e-mail, and instant messaging. Further, it can be expected that these social engineering and traditional malware threats will continue to be supplemented by cross-site scripting attacks and other forms of exploit. Holistically applied filtering, prevention, and detection technologies will obviously play the key role in front line defense, dramatically reducing the user's chance of exposure. But should a wily con artist sneak past those defenses, users must also be empowered with tools, education and resources to assist them in recognizing and responding appropriately.



Lottery scams
-- E-mail that fraudulently claims the recipient has won a large sum of money.



Send Attachments out for Scan

Send attachments out for a virus scan

How many times must we say it. **DON'T OPEN E-MAIL or TEXT MESSAGE FILE ATTACHMENTS!** The file attachment is the modern day equivalent of the letter bomb. They don't look any different from the outside, but when you open them...watch out! This blanket advice will keep you safe if you never open a file attachment, but what happens when you think an attachment might be legit, but can't be sure? The next time you have a file attachment that you think you want to open, but aren't sure, send it

out for a free analysis by a couple of dozen virus scanning engines. You can send the file(s) by e-mail:



Create a new message or forward the message with the attachment to scan@virustotal.com as the destination address of your email.

1. Write SCAN in the

Subject field (remove the old subject line if you are forwarding a message).

2. If you are not forwarding the message, attach the file to be scanned. Files cannot exceed 10 MB in size. If the attached file is larger, the system will reject it automatically.

3. You will receive an email with a report of the file analysis. Response time will vary depending on the load of the system at the time of placing your request.

How many times must we say it. DON'T OPEN E-MAIL or TEXT MESSAGE FILE ATTACHMENTS!

Remember Word perfect Blue?

Making your documents feel blue

There was a time when the dominant word processing program of the day (Word Perfect) used a blue background with white letters and many contend that it was much easier

on the eyes. Today's dominant word processor is Microsoft Word and the default display is a white background with black letters. If you want to relive the Word Perfect days or see if the blue background reduces eye strain, launch Word

and click on the Tools menu, the on Options.

Click on the General tab, place a checkmark in the "Blue background, white text" option and click on OK. If you don't like it, go back in and remove the checkmark.

Power Supply Tips

By Dan Hanson, the Great Lakes Geek, Computers Assisting People, Ohio

We have all experienced the computer crashing seemingly for no reason. When it does, we blame Windows or a hardware problem or maybe a power surge or undervoltage. All are possible culprits but one often overlooked possibility is the power supply of the computer.

The power supply is the metal box with a cooling fan next to it. Typically it's in a back corner of the case and you plug your power cord into it. When you plug the power cable into the wall, the power supply converts the AC (alternating current) that runs through your home or office into the DC (direct current) that the computer needs.

If you bought your computer from a superstore or discount retailer it may have a low-cost, low-capacity power supply installed which may not be enough to handle all the things you do with your PC.

If you have upgraded your PC with newer or more components (like another CD or DVD player/burner, more RAM or another hard drive) then the power supply that came with your system may not be up to the task.

The physics of power supplies (ambient tem-

peratures, 3.3V vs. 5V vs. 12V, etc) make it so that a power supply rated at certain wattage, say 300W, may not really provide that maximum wattage load. Some experts claim that power supplies are most efficient at 30-70% of their maximum capacity. So if you are nearing that maximum, you can be in for trouble.

Because the power supply gets a rush of AC (alternating current) when the computer is turned on and it heats and cools each time it is used, it is more prone to failure than many other components in your PC. You may notice a slight burning smell before it shuts down. Sometimes the cooling fan stops working and the system overheats.

Newer systems let you monitor the status of the power supply from Windows. Servers and other mission critical computers often have more than one power supply so that when one dies, the other kicks in and the system stays operational.

So what can you do?

Next time you buy a PC, don't just get a cheapo system with a sub-standard power supply unless you never plan on adding memory, drives or other components to the machine.

Take care of your power supply by keeping the cooling fan away from the wall or anything else that

might block the air flow and make the fan work harder (and die sooner).

Keep the PC off the carpet or other surfaces where it may suck in particles and clog the fan. Cooler is always better with electronic components.

Periodically, blow out the fan and case with compressed air to get rid of dust and other particles that may clog up the fan and overheat the system components.

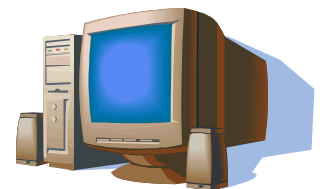
Add up the wattage of the components in your system to see if you are near the maximum of the power supply. E-mail us at dan@greatlakesgeek.com for a list of Estimated Power Requirements of common PC components.

If that is too difficult for you, look to see if most of the slots in the back of your PC are filled and if the drive bays in the front are being used. Those are indications that you may be close to maxing out your power capacity.

If you have a need, you can buy and install (or have someone else install) a new, heavy duty power supply. They come in several standard form factors to fit in most PCs. Warning this may not be a project for beginners though.



If you have a need, you can buy and install (or have someone else install) a new, heavy duty power supply.





911 Call to help group

What it costs elsewhere

Geek Squad in home call \$149.00 per hour

Serving Online Seniors in home call \$85.00 per hour

On line help \$79.95 subscription + \$24.95 per month

a gratuity to your SVECC helper is recommended

Name _____ Phone _____

Address _____

Brief problem description

Computer Help Group

Group Leader Joe Zagar

Joe Zagar	480-373-9373	all systems and programs
Jeff Bowlds	480-984-5309	all systems and programs
Levern Swensen	480.986-5997	Hardware Installation
Warren Sommerfeld	480-984-1525	Photo editing



June 2009

SUN	MON	TUE	WED	THU	FRI	SAT
	1 Defrag your computer	2	3	4	5	6
7	8	9 Patch Tuesday	10 Run Custom Windows Update	11	12	13
14	15 Run Anti- virus	16	17	18	19	20
21	22 Run Anti- spyware	23	24	25	26	27
28	29	30				

SVECC

Editor
Joe Zagar

President
Delores Bruno

Sunland Village East Computer Club

Founded for the Residents of
Sunland Village East

Mission: To help each other learn about Computers

Membership is open to all residents of SVE

Dues are \$20.00 per Year

Due October 1st



SVECC

Making your computer
Work for You

We are on the
Web SVECC.Com

Knee Problems

