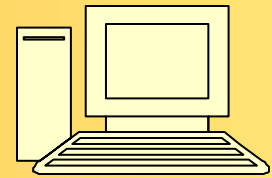


BAY BYTES

Greater Tampa Bay Personal Computer User Group, Inc.



Newsletter

Issue 9

September 2011

24th Year of People Helping People!



In This Issue

Rootkit Infection	Cont.	2
Laptop Setup		3
Laptop Setup	Cont.	4
Add Tabs to Office		4
Multi-Billion Dollar Computer		5
TLD-4 Botnet		6
TLD-4 Botnet	Cont.	7
TLD-4 Botnet	Cont.	8
Some Things to look into		9
The lighter side		10

Don't forget to visit our club's site at:

<http://gtbpcug.org>

As well Don Miller's and Darrell Manns' :

<http://www.dmanns.org/dmiller/>

Rootkit infection requires Windows reinstall, says Microsoft

New malware hides in the PC's Master Boot Record, fools cleaning attempts

Gregg Keizer

Microsoft clarified its MBR Rootkit removal advice after this story was posted. www.computerworld.com

Microsoft is telling Windows users that they'll have to reinstall the operating system if they get infected with a new Rootkit that hides in the machine's boot sector. A new variant of a Trojan Microsoft calls "Popureb" digs so deeply into the system that the only way to eradicate it is to return Windows to its out-of-the-box configuration, Chun Feng, an engineer with the Microsoft Malware Protection Center (MMPC), said last week on the group's blog.

"If your system does get infected with Trojan:Win32/Popureb.E, we advise you to fix the MBR and then use a recovery CD to restore your system to a pre-infected state," said Feng.

A recovery disc returns Windows to its factory settings.

Malware like Popureb overwrites the hard drive's master boot record (MBR), the first sector -- sector 0 -- where code is stored to bootstrap the operating system after the computer's BIOS does its start-up checks. Because it hides on the MBR, the rootkit is effectively invisible to both the operating system and security software.

According to Feng, Popureb detects write operations aimed at the MBR -- operations designed to scrub the MBR or other disk sectors containing attack code -- and then swaps out the write operation with a read operation.

Continued on the next page

Although the operation will seem to succeed, the new data is not actually written to the disk. In other words, the cleaning process will have failed.

Feng provided links to MBR-fixing instructions for XP, Vista and Windows 7

Rootkits are often planted by attackers to hide follow-on malware, such as banking password-stealing Trojans. They're not a new phenomenon on Windows.

In early 2010, for example, Microsoft contended with a rootkit dubbed "Alureon" that infected Windows XP systems and crippled machines after a Microsoft security update.

At the time, Microsoft's advice was similar to what Feng is now offering for Popureb.

"If customers cannot confirm removal of the Alureon rootkit using their chosen anti-virus/anti-malware software, the most secure recommendation is for the owner of the system to back up important files and completely restore the system from a cleanly formatted disk," said Mike Reavey, director of the Microsoft Security Response Center (MSRC), in February 2010.

Since then, Microsoft has added a check for the Aluereon rootkit to all security updates so that when the malware is detected, the updates are not installed.

Gregg Keizer covers Microsoft, security issues, Apple, Web browsers and general technology breaking news for Computerworld. Follow Gregg on Twitter at @gkeizer or subscribe to Gregg's RSS feed . His e-mail address is gkeizer@computerworld.com.



“A technician did set up my laptop, now what do I do?”

By Gregory West, Member of the Computer Operators of Marysville and Port Huron, MI, and Sarnia Computer User Group, Canada

<http://gregorywest.wordpress.com/>

prospector16 (at) gmail.com

Ah, the wonderment of getting a new computer. No more having to watch others show off their computer skills as they demonstrate their new digital slide show, or listen about how they talk with relatives across three oceans for hours at no cost. With your new computer you are ready to join the online communities around the globe.

Three gigabytes of random access memory, 500 gigs of hard drive, a one year subscription to some antivirus / malware protection software utility and you are “good to go,” says the clerk in the computer store.

“But does it come with a manual,” you ask?

“The manual is in the OS software,” the clerk says as he gets you to sign his copy of the credit card slip. “Have a nice day,” he hollers as you lug the computer through the doors towards home.

“Ya right,” you mutter under your breath

So many choices, too many decisions, but at least you finally got it home. Once you open the lid and go to turn on the new computer you realize that you have no idea what you are doing. In fact, you don't know a gigabyte from a Tyrannosaurus Rex, and you couldn't care less. All you want is to go on the Internet and check your email, surf some websites and maybe learn how to get those 265 photos from your digital camera.

“So now what,” you say aloud to yourself? “Where do I begin,” you ask your dog in desperation as she gives you that puzzled look.

There is an easy way to learn the various computer functions you need to catch up with your computer geek of a neighbor. First, you can take a formal course at your local college. These courses usually range from beginner to advanced. You can also take online courses (courses offered over the Internet), but this takes a special skill, as many people are not used to working alone and need to get out into a classroom set up with real humans. You can also join a local computer group. Here you will find people with similar interests who provide various seminars on tech-related issues.

I have been on a computer since 1972 where an IBM System/360 Operating System was the popular system in data processing centers. Over the years I have received computer training from all methods mentioned about. In fact, today I am taking two computer courses from books that came with DVD training programs

Continued on the next page

However, if you simply need to know one certain function on the computer, learn a software program, or how to troubleshoot a problem in your computer, I suggest Google's YouTube videos. Computer instructors, tech companies, libraries, schools and many knowledgeable individuals upload training videos to YouTube. Here you not only get free training, but targeted training. For instance, if you need to know how to install a USB flash drive in Windows 7, you simply go to youtube.com on the Internet and there will be many videos to help you through this process.

One tip for searching within YouTube for help, try using the term: "tutorials" with your search. Sometimes this will give you a full training course on the particular subject you are interested in learning. I use YouTube all the time when I need help with a particular computer program. But it doesn't stop there either. I wanted to learn how to winterize my RV and save the hundred dollar fee, so I searched for videos on YouTube and have winterized my own trailer ever since for only the cost of antifreeze

Gregory West is a Mac Instructor for Lambton College. He is also Webmaster at Central United Church, the home of Sarnia's new Community Computer Training Centre at: <http://goo.gl/76H15>. This is free and open to the public as a community service. Learn at your own speed.

Add Tabs to Your Office Documents

By Parker Monroe

If you would like to have more than one document open when using one of the following Microsoft Office programs, such as Word, Excel and/or PowerPoint, and would like to have tabs (similar to those used in Internet Explorer), so you can quickly go to any of those open documents, point your browser to:

<http://office-tabs.com/download.htm>

and download the free (for personal use) utility, either OfficeTabs.exe or OfficeTabs64.exe.

Note: OfficeTabs.exe is for the 32-bit version of Microsoft Office.

The tabs can be installed in Microsoft Office 2003, 2007 and 2010.

After installation, be sure to double-click on the "Office Tabs Center" icon that will now appear on your Desktop, so you can customize the tabs for each Office program.

For more info, point your browser to <http://tinyurl.com/3osptr6>

Multi-billion-dollar military computer system suffers bugs

By Deanna Glick – July 20, 2011

The Army's \$2.7 billion computing system designed to share real-time intelligence with troops fighting in Afghanistan and Iraq reportedly doesn't work and efforts to fix it haven't been successful, according to recent published reports.

In fact, the system has hurt, rather than helped, efforts to fight insurgents because it doesn't work properly, POLITICO reported last month.

The Army computer system is a cloud-based network designed to collect information from multiple sources for real-time analysis by battlefield commanders, according to POLITICO. For example, a commander searching for an insurgent leader would benefit from being able to collect reports of that leader's locations and plot them on a map to make tracking easier. However, the search tool made finding the reports difficult and the mapping software was not compatible.

After seeing a memo from the top military intelligence officer in Afghanistan regarding the faulty system, lawmakers sought urgent funding in fiscal 2011 for an alternative system. According to Extreme Tech, the Army refused, and instead rolled out a software update that was meant to fix any issues. Unfortunately, according to the former intelligence officers, the system is still unusable.

While it's not likely to solve the Army's computer woes, certain specialized computer tools can make a world of difference in average PC users' lives.

Several tools are available that automatically maintain your computer and help it retain peak performance.

AOL's Computer Checkup, for example, keeps PCs optimized and secure by repairing file fragments, spyware, outdated drivers and cluttered registries that can lead to slow performance and compromise your security. It will also recover files you accidentally deleted. Plus, the program is easy for beginners to run, but plenty powerful for advanced users.

System Mechanic is another user-friendly PC tool that repairs common problems such as slowdowns, crashes and freezes, leading to smoother, quicker and more reliable operation. The software cleans up hard disk clutter for faster performance and longer life.

Is Your Internet Security up to Date?

Antivirus up to date?

Firewall?

Windows up to date?

Spy Ware?

See how to protect your computer at:

<http://gtbpcug.org/protect/>



More about Internet Threats

Is The New TDL-4 Botnet Really 'Indestructible'?

<http://www.popsci.com/technology/article/2011-06/new-tdl-4-botnet-really-indestructible>

An elusive malware program has quietly co-opted more than four million PCs, and no one seems to know how to stop it.

By Clay Dillow

What makes this one so dangerous is it places itself in the master boot record. Once inside, TDL-4 takes up residence in the master boot record (MBR), which means it can run before the computer is actually booted up. The MBR is also rarely combed over by a standard anti-virus scanner, giving TDL added invisibility. Read below or Google "tdl-4" for more info.

How a Botnet Works From one computer to many computers to mayhem. Tom-b via Wikimedia

This week's big cyber news comes packing quite a headline: More than four million PCs have been infected by a malicious program known as TDL-4, a botnet that is so sneaky, so evasive, so hard to detect and disinfect that it is "practically indestructible." That quote comes courtesy of security researchers Sergey Golovanov and Igor Soumenkov of Kaspersky Labs, a cyber security firm and maker of anti-virus software. It's a scary thought: a botnet so sophisticated that it can't be detected and dismantled. But is it true?

There's no question that Golovanov and Soumenkov know their stuff, and their analysis of the emerging TDL-4 threat is thorough. But can a malicious program really be indestructible?

Continued on the next page

What is TDL-4?

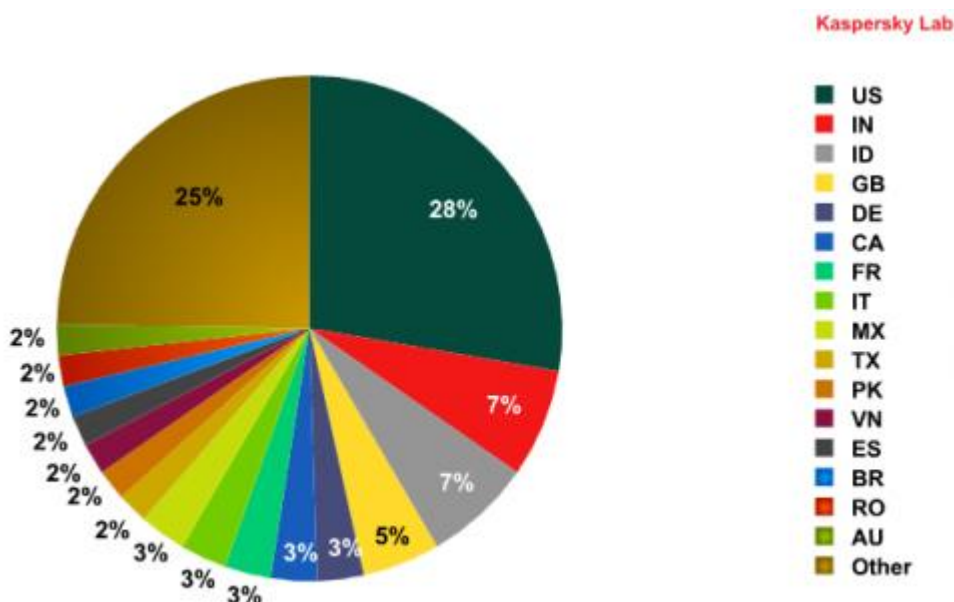
TDL-4 is the fourth generation of the TDL malware (Kaspersky also identifies the family as TDSS), and Golovanov and Soumenkov call it “the most sophisticated threat today.” In that, we can likely agree with them. TDL-4 packs all kinds of neat/scary tricks to conceal itself deep within hard drives, evading most virus scanning software as well as more proactive detection methods. It communicates in encrypted code, and contains a serious rootkit component--a rootkit being a program that allows an operator access to a computer even while hiding itself from the user, network administrators and automated security measures.

TDL-4 isn't one itself, but it's malicious because it facilitates the creation of a botnet--a network of infected computers that can be used in concert to carry out tasks like distributed denial-of-service attacks (which have been used to take down many major servers, including The Pirate Bay, Twitter, Facebook, and MasterCard.com), the installation of adware and spyware, or spamming. It currently has 4.5 million machines under its control and counting. The infecting file is usually found lurking around adult sites, pirated media hubs, and video and media storage sites.

What Makes It “Indestructible?”

Golovanov and Soumenkov summarize this nicely: "The malware writers extended the program functionality, changed the algorithm used to encrypt the communication protocol between bots and the botnet command and control servers, and attempted to ensure they had access to infected computers even in cases where the botnet control centers are shut down. The owners of TDL are essentially trying to create an 'indestructible' botnet that is protected against attacks, competitors, and anti-virus companies."

First things first: location, location, location. Once inside, TDL-4 takes up residence in the master boot record (MBR), which means it can run before the computer is actually booted up. The MBR is also rarely combed over by a standard anti-virus scanner, giving TDL



The Distribution of Known TDL-4 Botnet Infections: Kaspersky Labs

Continued on the next page

Then, TDL-4 does something else quite clever: it runs its own anti-virus program. The software contains code to remove around 20 of the most common malicious programs, wiping an infected machine clean of everyday malware that might draw a user's attention or cause an administrator to take a closer look. It can then download whatever malicious software it wants to in the place of the deleted programs. This version of TDL-4 also has added modules, like one that "fraudulently manipulates advertising systems and search engines" and another that establishes proxy servers on infected machines, which can be used to facilitate and hide other malicious cyber actions. But critical to TDL-4's indestructibility is the way it communicates between bots. There are a few things at play here. First, and perhaps most central, is a clever algorithm that encrypts the communication protocol between bots and the botnet command. This makes it virtually pointless to monitor traffic between the command server and infected machines.

Tags

Technology, Feature, Clay Dillow, botnets, computer viruses, cyber attacks, cybersecurity, malicious software, malware, military, tdl-4 But couldn't you trace those commands, encrypted though they may be, back to the source to catch the bad guys? TDL-4 has a trick up its sleeve here as well, this time in the form of a public peer-to-peer file sharing network called Kad. TDL-4's creators can issue several commands to their bot machines over this P2P network. This is key, because it means that if TDL-4's command servers get shut down, the program's creators can still access all the infected machines out there. In essence, command servers aren't really necessary at all. Destroying TDL-4 at the source is more or less impossible, because the source is distributed across the botnet network. There really is no single source.

But Is It Really "Indestructible?"

Writing for *Infoworld* today, Roger Grimes makes a valid point: "As a 24-year veteran of the malware wars, I can safely tell you that no threat has appeared that the antimalware industry and OS vendors did not successfully respond to. It may take months or years to kill off something, but eventually the good guys get it right."

Grimes' approach is the level-headed one. At one point Conficker was going to destroy the entire Internet as we knew it, but here we are today getting our daily dose of carefree lulz on the Web. TDL-4 will continue to confound and frustrate security experts for years most likely. But this too shall pass.

But that doesn't mean Golovanov and Soumenkov are necessarily wrong to call TDL-4 "indestructible." Perhaps the most noteworthy part of its title is the "4." It's just one bad seed in a malicious multigenerational family.

"We have reason to believe that TDSS will continue to evolve," they write. "The fact that TDL-4 code shows active development — a rootkit for 64-bit systems, the malware running prior to operating system start launches, the use of exploits from Stuxnet's arsenal, P2P technology, its own 'antivirus' and a lot more — place TDSS firmly in the ranks of the most technologically sophisticated, and most complex to analyze, malware." That is, until TDL-5!

<http://www.sevenforums.com/tutorials/20864-mbr-restore-windows-7-master-boot-record.html>

Some things to look into:

<http://www.wimp.com/driveengineered>

If you know anything about computer components, this video about how a hard drive is designed will amaze you. Make sure you watch it in full screen mode. Click on the link above to view the video.

<http://ireport.cnn.com/docs/DOC-628936?ref=email>

Member Ray Davis participated in a CNN reader contest and tried his hand in composing and presenting a song. Click above and listen.

http://techteachtoo.com/wp-content/uploads/2010/11/101110_OnlineCreditCardOptions.pdf

This might be of particular interest to our members – re safe ways to use credit cards on the Internet. It was written by Dave Palmer, who happens to be one of our members.

<http://techtalk.pcpitstop.com/2010/07/27/6-steps-to-remove-malware-completely/>

This could help saving your PC one of these days. However, the variety of tools and methods that are needed to clean up an infection also, IMHO, re-emphasizes the need for frequent backups of one's pc (s) to an external drive.

Unless one has tons of time to spare, and has regularly downloaded the latest versions of these tools (or can access them from another pc), the simplest and fastest way to surely get one's pc back in operation is to simply restore a recent backup. If restoring the last backup would result in the loss of one or more valuable documents that aren't present in the most recent backup, then before restoring the last backup, the user should attach the infected drive. via an external USB device, to another pc, and copy off those documents.

I fully appreciate that many folks don't back up their pc (s), for a variety of reasons (and excuses), but if one reads the entire page at the link you provided, that article should certainly encourage folks to at least consider doing so, especially as club members can still get the latest Acronis backup software through Gene Barlow.

<http://tinyurl.com/4s5mef8>

Reinstall Windows Without Losing Your Data.

The ultimate repair job doesn't have to be the ultimate disaster.

[Alternative Flash Player Auto-Updater 1.0.0.8](#)

Adobe's Flash Player has long been targeted by hackers and malware authors. Alternative Flash Player Auto-Updater lets you download and install Flash Player without having to download Adobe's download manager. It downloads the latest version and asks you whether the Adobe Update should be installed or not. You can choose to let it run at the start of Windows, this way you can be sure that your system will never run an outdated and an extremely dangerous version of Flash Player.

Club Member Doris Barrilleaux's Introduction to the Body Builders Hall of Fame

By Barbara Routen, Special Correspondent

Back in the mid-1950s, when Doris Barrilleaux arrived in the Brandon area, she started getting fit. Little did she know that her quest for a buff body would lead to a spot in the National Fitness Hall of Fame. Barrilleaux, 79, was inducted at a March 5 ceremony that coincided with the 2011 Arnold Sports Festival.

Presenting the award to Barrilleaux was actor, bodybuilder and former California Gov. Arnold Schwarzenegger, the festival's namesake, who gave her a congratulatory hug. When Barrilleaux began "body sculpting," as she called it, she dreamed that one day women's physiques would be as admired as men's.

"Women worked out and could only be recognized in the traditional beauty contest," she said. "All we could do was hand men their trophies. There were beauty contests but nothing for being fit."

She competed from 1978-80 and spent more than 30 years promoting women's fitness. She eventually became known as the "First Lady of Bodybuilding."

In October 1978, Barrilleaux, Suzanne Kosak and Linda Gleason formed the Superior Physique Association, Inc. and put on the Ms. Brandon Physique competition in 1979. "There were 13 contestants. I remember organizing, competing and even cooking for 50 people for the party at my home following the show. It was great fun and everyone was so enthusiastic," Barrilleaux said. In 1980 the Superior Physique Association created the first state competition, the Ms. Florida Physique.

The National Fitness Hall of Fame website states that Barrilleaux, "perhaps more than any other person in the history of the iron game, made national and international women's physique competition a reality ... as a bodybuilder, official, promoter, publisher and photographer." The site also mentions Barrilleaux's "stand against the growing use of steroids in the sport she had done so much to promote, which led her to walk away from her leadership role in the mid-'80s."

Barrilleaux's biggest challenge in passing along her message of physical fitness to other women was "convincing women they would not look like Arnold [Schwarzenegger] if they lifted weights," she said. "And then the darn steroids came in, and now some of them do." In 1978, Mr. Olympia Frank Zane said "the world wasn't ready for women bodybuilders, and I set out to prove him wrong," Barrilleaux said. "Last month at the Arnold, I admitted to him that he was right. I wasn't ready for the women who want to look like men."

Barrilleaux, a grandmother who said she feels about 50, bikes about five miles a day, swims in summer and keeps small weights under the sofa so she can do curls while watching television.

Barrilleaux has enjoyed "being a stewardess, traveling the world with bodybuilding, and all the friends I've made around the world," she said. "Just sitting at this computer I'm in contact with friends in Australia, Italy, Nassau, Canada and people all over the U.S."

Her current goal is to finish an autobiography she began about five years ago. "Had to learn so much computer technology to make it multimedia on DVD," she said. "Far too much to be a printed book; it could be an encyclopedia."



*Some Material appearing in this newsletter had been send to the editor by:
Parker Monroe, Charlie Vanderford and Doris Barrilleaux. Many thanks.*

Legal Notice

Bay Bytes, Copyright © 2011, is the official newsletter of the Greater Tampa Bay PC User Group, Inc. (GTBPCUG). The information in this newsletter is intended to help our members. It has come from many sources and cannot always be verified. It is recommended that you obtain professional advice from software and hardware distributors, manufacturers, salesmen, or other professionals dealing with the subjects that appear in this newsletter. Unless specifically stated otherwise, the opinions expressed in Bay Bytes articles and columns are those of the individual authors and do not represent an official position of, or endorsement by GTBPCUG. GTBPCUG is not affiliated with any company, vendor or equipment manufacturer. Permission for reproduction of Bay Bytes in whole or in part is hereby granted to other APCUG user groups for internal, non-profit use, provided credit is given to the author, GTBPCUG Bay Bytes along with the copyright notice. Other reproductions require the prior permission of the editor. When published, please send a copy of your newsletter to

editor@gtbpcug.org or mail to P.O.Box 501, Brandon, FL, 33509-0501.