



THE RHODENIZER REPORT

SEPTEMBER 2009

www.rhodenizer.com

INSIDE THIS ISSUE:

ZOMBIES FOR RENT	1
MICROSOFT PUSHES IE 8 AS "CRITICAL"	1
GOVERNMENT COMPUTER ERROR?	2
QUESTIONS FROM THE INBOX	3
AMAZON TURNS BIG BROTHER	4
ABOUT RHODENIZER IT	4

ZOMBIES FOR RENT

Want to knock-out the website of your competitors?, or anyone else you don't like? How about sending a deluge of SPAM to overwhelm the e-mail system of a large corporation and shut it down for several hours?

A few years ago you would have needed to hire a hacker for tens of thousands of dollars to take out "a hit" on someone, but not today. Thanks to the multitudes of naive computer users with a propensity for downloading free goodies, you can now rent your own remote controlled "botnet" of zombies for about \$200.

No longer is it necessary for hackers to build their own base

of operations with expensive computer systems. Now, they launch coordinated attacks, or send out SPAM, using millions of infected PC's just like yours. These networks of zombie PC's called "botnets," are rented out through websites that make executing a denial-of-service (DOS) attack about as easy as ordering a movie from Netflix, and it takes about an hour.

Google "botnet" or "bot rent," and you'll find hacking forums with postings for botnet rentals. After downloading their control panel software, you can enter the name of the website you want attacked and schedule the exact time of the assault.



Payments are made by money transfers via Western Union.

In the recent Twitter attack, for example, hackers targeted a blogger known as "Cyxyemu" because of his criticisms of the Russian government. They launched a "DOS" attack, in which thousands of computers ping the target site simultaneously, overwhelming (cont. P.2)

THE TAKE-AWAY POINTS:

- **Zombies rent cheap. Your PC could be one.**
- **IE 8 browser is neither critical nor desirable.**
- **Social Security error blamed on computers.**
- **Amazon remotely deletes content on customer devices.**

MICROSOFT PUSHES IE 8 AS "CRITICAL"

If you're a faithful Windows updater, you probably have your PC set to download and install all "critical updates" from Microsoft automatically. If that's the case, you probably already have Internet Explorer version 8 on your PC.

If, however, you like to review the critical updates before you download them (like me) you may have noticed IE 8 listed among "Critical" updates that

Microsoft wants you to install. This is NOT a critical update. It may seem critical to Microsoft, since their web browser is rapidly losing market share to Firefox, but you don't need it if you use a current version of another web browser.

Firefox, Chrome, Safari, even the previous version of Internet Explorer (7) are all preferable to IE 8 because of the reported

compatibility issues. The only thing worse would be IE 6, which is downright dangerous.

If you already have IE 8, don't try to remove it. Others have reported disastrous results when they tried to go back. Just download Firefox and use that instead.

If you don't have IE 8, consider the update as optional—not critical... not even desirable.

GOVERNMENT COMPUTER ERROR?

Information Week magazine reports that the U. S. Social Security Administration is settling a class-action lawsuit brought by the National Senior Citizens Law Center.

The U. S. Government will now pay more than \$500 million in benefits they previously withheld from 80,000 people since 2007 because of a computer error.

Under current law, the government can withhold Social Security benefits from fugitive felons. The SSA tried to automate that process by having government com-

puters search for matching database records linking outstanding arrest warrants with the names of Social Security recipients. The problem occurred when Social Security payments were also withheld from those with long-dormant warrants and minor infractions, those who didn't know they had ever been issued a warrant, and those who had been charged but were never convicted of any crimes.

The bottom line here is that government IT workers made poor use of these databases

and did not fully understand the consequences of what they were doing. It took over two years to discover the error and force the government to correct it.

While this story may be an isolated incident, it begs the question: Is this an indication of how other government IT systems are being managed? And, is this what we can expect from a government run centralized healthcare system? - C.R.



ZOMBIES FOR RENT (CONT.)

(cont. from P.1) them in a massive traffic jam.

Security experts say the explosive growth of these botnets has led to a price war between criminal gangs. There are now dozens of botnets with a million plus zombie PC's that can be rented for about \$200 a day.

Now that these weapons of mass disruption are available to just about anyone, we are seeing a tremendous surge in attacks. According to a survey done by Chelmsford Massachusetts security firm Arbor Networks, about 700 "DOS" attacks were reported on Aug. 10, 2007. This year, on that day there were more than 1,300.

Attackers have a variety of motives. Some, like the Twitter assault, appear to be politically motivated. Others help cover up criminal activities. Security consultant Kevin Mandia says the banks that hire him often come under attack when hackers have stolen ATM information and don't want victims to notice their diminishing balances on the bank's website.

With these declining costs, "DOS" attacks can be used by a wider variety of people for various purposes. A disgruntled employee could hammer his company's website incessantly; a small business owner could knock out a rival's e-mail system on a

busy Monday morning. And, all with complete anonymity.

Some businesses and government agencies are adding extra capacity to their networks to better handle "DOS" attacks. But, more creative designs are needed. The only defensive action we can take at this time is to shut down servers under attack and wait until the storm passes.

Obviously, I don't recommend anyone engage in the activity described here, but small business owners beware — Those PC's in your home or office that seem very busy doing something in the background may already be under the control of a zombie botnet army.

"...PC's in your home or office that seem very busy doing something may be under the control of a zombie botnet army..."

QUESTIONS FROM THE INBOX

Q– “How can I tell if there is a hidden program running on my computer and communicating with someone out on the Internet?”

A– “Short of hiring a professional IT consultant like myself to do a security sweep and analyze the results, you can use some of the free software tools available on the Net if you’re a savvy do-it-yourselfer.

One of the easiest to use is a free download available from the “Cliff’s Pick’s” page of my website. Scroll to the bottom and select the “Free Port Activity Revealer”. It links to the download page for “Active Ports 1.4”. Download and run it. This tiny program will present you with a list of currently running processes, the IP address and port numbers they are using, and whether they are actively communicating with those IP’s or just listening to them.

The easy part is revealing all this information. The hard part is knowing which ones are normal, and which ones are suspicious. If you are the brave sort, you can terminate each process one-at-a time to see what happens. It’s a fun kind of Russian Roulette, and a learning experience. Just don’t be surprised if your PC crashes when you terminate something critical. No need to panic though. Simply re-boot and they all start back up again.

Q– “I know you are a big fan of Kaspersky AntiVirus, but can you recommend something very basic and preferably free for my kid’s PC?”

A– No problem. The free versions I can recommend are:

[Avast! Home Edition 4.8](#), and [Avira AntiVir Personal 9.0](#).

AVG also has a free antivirus product that many like, but in my experience it created too much of a drain on the system resources. The 8.5 version slowed the PC down so much I had to remove it and try something else.

You can find download links to all these on CNET’s website: www.download.com.

Q– “I’m sure all of our office systems are old and outdated, but I still remember what a nightmare it was the last time we upgraded something. Sooner or later, I’m going to have to make some changes, but how can we avoid going through a disruption like that again?”

A– Change can be difficult. Especially when you’re used to doing something a certain way for a long time. If your last transition was that disruptive, it may be that it was poorly planned, poorly implemented, or your people were poorly trained.

First, I look at the cost (in

terms of time *and* money) versus the benefit to your business. If you can’t see how the benefits outweigh the cost, you shouldn’t go through with it.

Second, I plan a phased approach whenever possible. One step at a time. The strategy for going forward is just as important as the strategy for backing out if it doesn’t work the way you want.

Third, I do all the training myself once I know everything is working properly. It’s my job to simplify the process so your people can pick up on it quickly. If they can’t, it’s my fault—not theirs. I don’t allow nightmares in my business. My work is not done until everyone can say it works like a dream.

Q– “When are you going to make some new videos for your website?”

A– Frankly, I just haven’t had any good ideas for another video lately. One suggestion was to show a Vista PC being violently destroyed. Another one was to show my latest custom PC creation (shown here at right). What would you like to see? Send me some suggestions.

“The strategy for going forward is just as important as the strategy for backing out if it doesn’t work the way you want..”



E-mail your questions to:
questions@rhodenizer.com

AMAZON TURNS BIG BROTHER

Amazon.com recently sold many copies of the books "1984" and "Animal Farm" to its e-book customers who downloaded them in electronic format to read on their Kindle devices. However, when Amazon discovered that the source they had originally purchased these from did not legally own the copyrights to the material, they did something extraordinary. In a move unprecedented in America, this corporation remotely accessed each customer's electronic device and deleted content

without the owner's permission. The next time owners went to open the e-book, they discovered an empty space.

While Amazon maintains that the owners were refunded the price they paid, this begs some interesting legal questions. If the books had been on printed paper, could Amazon have sent representatives to enter the homes of customers unannounced and taken the books from their bookshelves?

We know that governments like Iran and China commonly

block Internet sites and try to control the flow of information to the people, so an incident like this would not be surprising there. But who would dare attempt such a thing in America? It's ironic that one of the e-books seized was George Orwell's "1984", a story about the long reaching arm of "Big Brother".

Granted, our government had nothing to do with this, it was the act of one corporation. But, if they can get away with this unchallenged, what might be next? - C. R.



ABOUT RHODENIZER IT

We are a different kind of IT service provider. We don't resell any hardware or software. We find the best deals on what you need and pass the savings along to you.

Our mission is to help small businesses reduce expenses, increase productivity, and safeguard private information.

It's about more than just fixing computers. We also

provide IT consulting and services that include finding the best solutions to your business problems.

We work with clients to prepare disaster recovery plans that ensure their critical data remains safe, yet easily accessible. Additional benefits include money-saving ideas for managing your computer resources and planning for future business expansion.

We have the training, experience, and know-how to provide the right solutions for your needs, and your budget.

Just call to schedule your **free initial consultation with no risk, and no obligation.**

Tell me about your computer needs or IT issues. I'll recommend a course of action that makes sense for your situation at no cost to you. What have you got to lose?

Rhodenizer IT
Information Technology Services

P. O. Box 768122
Roswell, Georgia 30076

(404) 202-8657

www.rhodenizer.com

The Rhodenizer Report is published and distributed by Rhodenizer IT, Inc. © Copyright 2009. All Rights Reserved.

DISCLAIMER: The information, opinions, and recommendations expressed within are for general knowledge and are not intended to be a substitute for personal consultation. Furthermore, some information may be based upon other information provided by third parties. Unless specifically stated, no form of independent verification is undertaken. The author is not responsible for any errors, omissions, or inaccuracies. This information is provided free of charge and is without warranty, neither explicit nor implied. The reader assumes all risk when performing any computer modifications without the direct supervision of a qualified IT professional.