

## **BENJAMIN ROCKWELL**

COMPUTER TALK RADIO.COM  
TOLL FREE - 888-NERD-888

## **WRITTEN INTRODUCTION**

Hello! This was developed by myself, Benjamin Rockwell, for a computer seminar that I gave on computer security. It is not intended as an all-inclusive document, but merely covering a number of crucial items that you need to know to be secure. If you have any questions on this document, please contact me through the contact forms at ComputerTalkRadio.com or via my toll-free number.

This document is written in bullet form, as notes, but is far more granular than you might normally see, so that it might help you understand some of the major issues involved.

## **PERSONAL INTRODUCTION**

- Computer field for 21 years
- Computer Consultant for 18 years
- 12 years as a hands-on I.T. Director... being a jack of all trades, but working in small companies where I deal with the technology hands on, and working with a small staff.
- Started working with the Jeff Levy show almost 3 years ago, and have had my own show broadcast on radio for over 2 years.
- Computer Talk Radio is the show, and it covers the latest in news in the field, as well as answering your computer questions.

## **VIRUS BACKGROUND INTRODUCTION**

- I'm a subject matter expert on computer malware, having dealt with computer viruses since before I started in the tech side of the industry 20 years ago.
- Ran a Bulletin Board Service prior to becoming a field technician, and folks would upload malware to my BBS, a computer I left on 24/7 for other folks... this was before the internet became the web as we know it.
- Started as a field technician where within months, I became the sole contact for computer virus activity, dealing with early ones like Stoned, Michelangelo, and so forth.
- Later, I worked at Unocal for over 5 years, where for much of the time that I was there, I provided background information, alerts, diagnosis, and troubleshooting for our computer malware problems worldwide. If it was malware, I was either hands on, or at least heavily involved.

**Introduction - What is malware, best practices, antivirus and antispyware software, specialty tools and how firewalls and routers fit into the equation. Then a Q&A period at the end...**

## **WHAT IS MALWARE? (MALICIOUS SOFTWARE)**

- Types of malware, and how we get them?
  - Viruses - it infects good code, travels to other good programs, & attaches itself
  - Worms - Worm their way through various holes in the code to other computers... specifically uses specific programs versus random programs.
  - Trojan Horses - mythology - It's a standalone program that requires user interaction, comes from websites, spam, attachments to e-mails, and more.
  - Rootkits - Concealed versions that appear to be part of the actual system.
  - Spyware - Collects small bits of information about you...
  - Botnets - Computers that have been hacked, that work together to attack others.
    - 50-80% of all spam is believed to be sent by zombie computers
  - Keystroke loggers - track all of your activities and forwards them to the controller
  - Adware - Just puts up a lot of ads, pop-ups, and sometimes overwhelms your PC
  - Scareware - Similar to a spyware or adware, advises you that you have lots of malware
  - Ransomware - Hijacks your PC and holds the data ransom via encryption
- I could list hundreds of different programs that qualify as malware, but would you even know it, unless you had it before?
- When I started with computer malware, one could sit and memorize all 1000 active malware...
- For 2009, Sunbelt Software, the makers of Vipre noted some significant numbers... 30,000 new ones each day.... 15 million overall and it's almost doubling each year. Everyone's numbers are different, however... this was a conservative number. About one every 3 seconds.
- Now think... 30,000 per day... Facebook has 30,000 servers... McDonalds has 30,000 stores... and there are about 30,000 apps in the Google Android app store. It took Apple 9 months to get to 30,000 apps, and the malware authors do that each day.
- It used to be the game, the thrill, the excitement... but what is it now? Why do they do it? The fastest growing areas in malware... is where they make money.
- Imagine that scareware hitting you up for \$40 on your credit card, the money that they make from selling your card information to someone else, after they already ran a few scams, etc.
- So with a number this huge... how do we recognize it? Simply put, the average person notices very little until the machine is overrun with the disease. Slow downs, odd e-mail bounces, or friends confused by an e-mail that you sent them, but you didn't send it. Things like this will mount up quickly.
- This isn't a place to ignore the warning signs, as your vulnerability is huge at all points when you have malware. Your local information is compromised.... some items, like keyloggers, can share your passwords and credit card information, and more.
- I'm not here to scare you, and I'm not even here to sell you on anything, except to be prepared and cautious. You can take any or all of the information here, and apply it to yourself, but I'm going to give you information to make the best decisions.

## BEST PRACTICES FOR SAFETY TO PREVENT PROBLEMS

- Already described why you don't want malware, and the various types. Let's look at what I did, as a test example, in preparation for this seminar today.
- I took a computer and exposed it online for 30 minutes without a firewall, without patches, without virus software, and the like. It received 2 infections in that time. BOOM...
- I took another computer and spent time doing something I've taught against... using a major search engine, and looking for inappropriate material on the Internet. 10 minutes later... boom.
- I decided to click on ads on websites, turning off my pop-up blocker, and simply chasing after random twitter links from folks I don't know.
- Some of these issues stem from vulnerabilities within Windows. So what do we do? Abandon Windows and go to the Mac? Nope, Apple patched 88 vulnerabilities to OS 10.6.3 in March... and a few thousand Mac-only malware packages exist out there, and they are growing!
- The truth is, our behaviors indicate our chances of infection.
- In the past 3 years, I haven't had a single computer virus on my computers, except when I intentionally did so to battle the nasty little bugs. In a span of a day, using three different methods, I managed to rack up enough garbage to crash 2 machines.
- So, we'll talk about software in a minute, but let's talk about your activities first...
- **Don't play in the underground** of the Internet, where people promise something for free, or you're going to get burned. Some of the biggest problems these days stem from adult websites, file sharing, and messing around with attempts to get copyright software for free.
- **Don't assume a link is safe because it came from a friend.** E-mail, IM apps, twitter, myspace, and facebook items have all been methods to attack at everyone.
- Oh, and yeah, twitter is scanning for malware, but that's not foolproof...
- **Bit.ly links, and other TinyURL type links are not safe, as you can't see ahead.**
- **Be aware of social engineering.** The tactics used to get you to click a link promising easy money, or free items, or even the latest news in regards to the latest tragedy... it's all calculated
- **Use an recent browser...** the idea of IE 6 users, or folks running an old version of Firefox, is bad. Chrome is a good option, but you can stick with IE8 or Firefox 3.6, as long as you keep updating.
- **Update your operating system.** Most of the packages out there are looking for vulnerabilities within your computer, usually ones that have been patched for a while. (0-day vulnerabilities are rare, but combined with your best practices, things should be good.)
- **Be suspicious of free offers** for scans... or even what looks like your computer antivirus program, or even Windows, telling you there is a problem. It's not always the case.
- **Know which AV you have,** and understand that if it doesn't look right, don't click it.
- If you have administrator access, that's also a vulnerability... as the code gets in and uses your access to the system to change things, and to further make you vulnerable.
- There are active tools that you can use... Antivirus, Firewalls and Routers, and cleanup tools

## ANTIVIRUS SOFTWARE SELECTION

- **Antivirus software** is a large industry, largely due to the great amount of threats before us.
- Opinions and favorites... I have interviewed reps from each of the Big 3 on my radio show... none are sponsors, and while I have product from many vendors, it's as a courtesy to you.
- Norton - Long known as bloatware, is distinctly working to overcome their past. New methods may allow for exploits (no proof of concept yet), otherwise good, except that they are a target.
- McAfee - Has been everywhere from bloated, unresponsive, false negative rate, etc... the biggest target of virus authors...
- Trend Micro - Business oriented, with dramatically low false positive rate, but a delayed response, and insufficient response on ultra-rare malware threats.
- **Other vendors worth mention in the game...**
- Kaspersky - Good product, but built in Russia, home to many malware authors (China is 1st place), but Kaspersky also overreacts, hypes to the extent of scareware...
- Nod32 - Frequently gets favorable reviews, but they go all over the place.
- AVG - great product, if a little quirky. Their free product is great for those unable to pay.
- Avast! - Does OK, but frequently misses the biggest threats early on... more reactive than not.
- Vipre - Does a great job at speed, and reliability, but sometimes misses key threats.
- Microsoft Security Essentials - Microsoft has bad history with Live OneCare, and before that, Windows Defender... and in 1993, MicrosoftAV... Sounds great, is free, but...
- **Paid vs. Free** is a tricky aspect, as we all like free items, right? It's the pocketbook, right?
- When you pay for something, you pay for a service, reliability, the insurance that you will be able to recover, and that folks will stand with you battling the problems.
- As I mentioned earlier, if you don't have software, you're already in deep potential trouble, and probably have malware on it. If you let it expire, you're vulnerable, if you don't patch, etc...
- The problem is that what used to be pranks, like the Stoned Virus, are now distinctly deadly to your PC, your credit report, and really, your entire identity for years to come.
- You have car insurance, right? Home insurance? Do you have fire extinguishers and smoke alarms? Malware protection is absolutely key in this same way, protecting you from the threats.
- Which do you want, the free seatbelt, or the car that comes with a seatbelt and an airbag?
- Free = Self-supported, or the provider disappears, and you had no idea you were unprotected.
- Only you can make a decision on which product to go with... This is like car buying... I can't tell you to go out and only buy my particular car, Pontiac (out of business).
- I suggest one of the big three, after you weigh out the differences in your book. Choose a big name in the supplemental ones, like Kaspersky or Nod32. This is for the paid software.
- A Security Suite is good if you're on a laptop, but it'll take up resources for the firewall product, and other bells and whistles that may be overkill on a desktop.
- I personally use Trend Micro in the business environment, Norton on my wife's computer, and McAfee on one of my laptops. Each setting is different, and covers different things.
- On my lab computers, I frequently use AVG Free, as it's not protecting production.

## REACTING TO INFECTION

- So what do you do if you see something dangerous? What do you do if you've already got a computer infection? Addressing each malware program is difficult. There are tools out there for just about every infection possible, just as we use Penicillin for some viral strains, Tamiflu for others, and simple bedrest for even more.
- Now, is there such a thing as simple bedrest for our computers? No. Once infected, it's over.
- Specialty tools abound in the computer world, and these tools are different than the scanners.
- Norton, McAfee, Trend, etc, all work on the prevention measure, and will clean many problems.
- Specific infections require different tactics that will clean things up for you. There is no magic bullet that covers all of the fixes, but usually someone focusing on a specific variety of infection.
- Step 1 - Before you even venture down the road, make sure that your backups are secure. Please tell me that you have a backup of everything on hand, right?
- Step 2 - Identify your infection by what it's acting like... what the screens that are associated with it say, and so forth.
- For instance, Antivirus 2010, or Windows Security Center, or Spy Sheriff or whatever.
- Step 3 - Research the approaches for that infection and apply.
- The problem is that you might have multiple infections....
- Recently did the following... Used program from Microsoft called Process Explorer to kill all active applications, used ComboFix (available at BleepingComputer.com) to attack Antivirus 2009, used MalwareBytes (available at MalwareBytes.org) to kill off some of the other downloads that Antivirus 2009 brought with it, and then I installed an antivirus software.
- Tools that are generally safe include MalwareBytes, Spybot Search & Destroy, Lavasoft's Ad-Aware, and so forth.
- The top tools out there for the most recent threats are available at FileHippo.com, and a few of them are dangerous if you just act randomly, like ComboFix. The legitimate ones that are dangerous will warn you before you start working with them...
- Oh, and there is no reason to pay for any of these one time usage tools... if you have to pay for a tool, it's likely one of the scammers. AntiVirus 2009 was known for a number of scam tools to "fix it", which were presumably from the authors of Antivirus 2009. Not real tools for all threats.
- These don't fix everything, but I'll review the big specific tools and websites again...
- MalwareBytes (MalwareBytes.org) - catches a number of the bad guys, especially ones that fit in that gray area, or are hiding from other software packages.
- Spybot Search & Destroy - Quality goes all over the place, and same with the releases, sometimes great, sometimes not. It's still a tool used to address infections after the fact.
- Lavasoft's Ad-Aware - Download it from FileHippo.com, and it eliminates a number of the pop-ups and more. Recent moves into competition with the AV companies, but may not be ready yet.
- Combofix - Available at BleepingComputer.com, and that website is a great place for resources specifically dealing with removing your infections. A whole group of folks work together to ensure your computer safety, and I rely on their website for a number of infections

## FIREWALLS AND ROUTERS

- I mentioned firewalls and routers earlier, and this is one of the other major defenses.
- When a computer has a public IP address, they are out on the Internet exposed to everyone.
- Their operating system stands as the last line of defense, but most OS's have vulnerabilities.
- Best practices say to use a firewall, a way to protect us from the outside. It sits between our computer and the internet and controls all activity, preventing the bad guys from getting to us.
- This is because Active programs, like worms and viruses, look for vulnerable locations without our public access point, much like a burglar scouts around the house before breaking in.
- A software firewall merely shuts down all activity on all ports, and then opens up the ports that you tell it are acceptable, or specific ports that you are actively using. ZoneAlarm is a common firewall, that folks have been using for ages, and is available at FileHippo.com
- Windows has a built-in firewall, which is better than nothing, but honestly... do we wish to trust our security to the folks that made the mistakes the first time around in their programming?
- A hardware firewall serves as the public viewing point, and hides your computer behind it.
- This occurs through NAT. Think of your Public IP address as your phone number on the Internet. NAT gives you an extension within your own network, but then prevents inbound calls. Great if you're dialing out only, which in most cases, is all we ever do.
- Hardware routers, known as broadband routers are used frequently to allow you to have multiple computers within your house all sharing your DSL, Cable, or FIOS internet connections.
- Linksys (owned by Cisco) is my personal preference, but they are available from other companies as well. Belkin, Netgear, D-Link, and for security preferences, it doesn't matter whose unit, so long as you make sure that you assign an administrator password to it.
- Advanced routers with firewall features will also allow for forensic examination, inspection of the data to ensure that you aren't going anywhere bad, or even block you from certain websites.
- As a consultant, I have recommended SonicWall routers for businesses for over 5 years now, and while they lack the Cisco name, they are distinctly prepared for the Small-to-Medium Sized business, even one run out of your own home.
- When do you use what?
- **Software firewall** - Laptops that are being used outside of the home. If you're working wirelessly, accessing through Starbucks, the airport, or anyplace public, turn on ZoneAlarm...
  - protection is designed for network connection, but impacts computer performance.
- **Hardware Firewall** - If your computer is a desktop, or you never leave the house, this is the better route. Your computer is protected at the router, so you can increase performance and turn off Zone Alarm.
- **Advanced Firewall** - This is ideal in a business environment where you might have to handle professional levels of protection. The router monitors all kinds of traffic, and you can set reports to advise you if you're under an advanced threat. Additionally, it'll monitor traffic going out, protect your company from folks who might go to non-business websites, etc.

## SUMMARY OF KEY POINTS

- I'm going to do these in a different order now... it's in order of importance.
- The largest vulnerability first... it's you. It's your level of trust. I distrust a number of the different things on the Internet, and honestly, you should too. Social engineering is about circumventing your distrust and leveraging that newfound level of trust against you to do you distinct harm.
- Don't play in the underground of the Internet... if you play with fire, gasoline, and explosives...
- Use an Anti-Virus program (misnamed, because they really handle everything today), probably from the Big 3, or one that I mentioned here today.
- Make sure that you have a firewall (hardware or otherwise).. ZoneAlarm for the laptop, and get a hardware firewall for the house. Adds wireless access, but lock that firewall down.
- Keep your system patched and updated.
  - That means turning on Microsoft Update... not just Windows Update. If you aren't sure if you have Microsoft Update on, go to Windows Update, and they're good about offering the Microsoft Update as an add-on.
  - Mac users need to do the same thing...
- Back to that social engineering, if you see something that tells you about your computer problems, assume that it's lying to you. As part of that, know which AV you have, and make sure that you know what the screens look like.
- Finally... if you do run into a problem, there are plenty of folks that are willing to help you for free on the Internet. Bleeping Computer.com is a great resource, and I want you to consider checking them out for more information.
- Caution folks... if you're not sure about it, contact a professional with experience. That's not the Geek Squad, but someone who is interested in dealing with the problems head-on, not in selling you a new computer.