frogworks
Managing Your Technology So Your Business Doesn't Croak.

Ribb"IT" Review

“With the new day comes new strength and new thoughts.”

-Eleanor Roosevelt

August 2018

Issue 8, Volume 8

This monthly publication provided courtesy of Alex Bleam, Owner of Frogworks

We are excited and proud to announce that Frogworks has been recognized as one of the world’s best MSPs by Channel Futures!

Channel Futures
MSP 501
2018 WINNER

THE ULTIMATE GUIDE TO THE WORLD'S BEST MSPs

USB Drive Security - Why You Should Be Worried About Your Team Using USB Drives

A serious design flaw in USB technology, identified by researchers at SR Labs, could mean that USB drives are a bigger security threat than was previously believed. But it isn't the content these devices might contain that should concern you. It's a fundamental flaw in the firmware that could spell serious trouble for your business's security.

If you or your employees use USB drives to store information or transfer files between computers, you'll want to read this!

What is USB?

USB stands for universal serial bus, a universal communication protocol that allows the connection of many different devices to a computer. Lots of hardware devices from keyboards and mice to charging cables, game controllers and Ethernet adapters connect to your computer via this universal port. In fact most computers have more than one port to accommodate multiple devices.

One of the most popular devices to connect via the USB port is the small, ultra-portable USB drive. Also known as flash drives, pen drives, thumb drives, memory sticks, USB keys or jump drives, USB drives are primarily used to store and transport files from one computer to another.

USB drives, like other devices connected to your computer, use a special type of software, known as firmware, to tell the computer what the device is and manage its functionality.

Typical firmware on a USB drive manages the transferring of files from the computer to the drive and vice versa. In a similar way, the firmware for a USB-connected keyboard converts key-presses on a keyboard to digital data that is sent over the computer's USB connection, enabling the keyboard to operate.

The key to USB technology's vulnerability lies in the fact that it was designed to work with a wide range of devices. The firmware identifies the device and the computer reacts accordingly.

But what if someone could alter the firmware of a USB drive to make it look like the device was actually a keyboard or an Ethernet adapter instead?

In 2014, researchers at SR Labs reverse-engineered the code of the basic firmware on many USB devices and found that the firmware could, in fact, be reprogrammed. This ability to reprogram the device's firmware, known as BadUSB, makes it possible for a USB drive to behave like a different device entirely, turning it into a potentially malicious device.

This is not the first time that the security of USB drives has been called into question. At one time users were warned never to connect a USB drive to their computer if they didn't know where the device originated. This was due to the frequent exploitation of the Windows Autorun function.

Created as a convenience for users, Windows computers (starting with the release of Windows 95) were programmed to recognize autorun.inf files on certain types of media, CDs and DVDs for example, and automatically play the music or movie, or run the program found on the device. This eliminated the need for consumers to figure out how to get the disk to work when it was inserted.

In 2005, Sony BMG took advantage of this feature, using it to install a subversive rootkit that circumvented a user's ability to rip content from their music CD's to their computer, effectively preventing unauthorized copies of music files.

But the AutoPlay feature wasn't limited to CD and DVD drives. The functionality also worked from USB drives. Since it was easy to install autorun.inf files on these portable drives, it wasn't long before hackers began using Microsoft's built-in Autorun function to launch malware and viruses to infect users' computers via USB drives.
Microsoft has since taken steps to limit or disable Autorun capabilities since the introduction of Windows Vista and subsequent operating systems.

The important thing to note here is that the Autorun vulnerability used the contents of the USB drive to infect a user's computer. The current threat creates the potential to circumvent the hardware itself, which is a much more serious concern.

What Could a Malicious USB Drive Do?

In theory, any vulnerable USB drive's firmware could be reprogrammed to:

Act as a keyboard and send key-presses to the computer as if the perpetrator were sitting in front of the computer

Could appear to function normally, then infect files as they leave the computer

Could work as a USB Ethernet adapter and route traffic from your computer to malicious servers

Modify or delete files on your computer

Relay information from your computer or other connected device to an attacker

Spread malware or viruses from the USB drive to your computer

Act as a boot device, which would load the computer's operating system while installing an invasive rootkit underneath

If none of that is scary enough, consider that the most dangerous aspect of all of this is the possibility that any infected computer could be programmed to infect the firmware of a clean USB drive. An infected drive could then become a malicious device that would later infect other computers.

Scarier still is the fact that much of this could happen in the background, without a user ever being aware that it was happening. This is because USB devices can use multiple profiles.

For example, a USB drive's firmware could tell the computer it is any type of USB device - a keyboard, Ethernet adapter, or game controller. But it can also function normally as a storage device, while reserving the ability to perform other operations, such as the functions of a keyboard or Ethernet device, at a later time.

This article continues online. To read more about how serious this problem is and how to protect your business, visit our website at: https://www.getfrogworks.com/usbsecurity

Have you ever lost an hour of work on your computer?

7 IT SECURITY PROTECTIONS
Every Business Must Have In Place Now To Protect Themselves From Cybercrime
frogworks

After working with dozens of small and mid-size businesses in the DC Metro area, we found that 6 out of 10 businesses will experience some type of major network or technology disaster that will end up costing them between $9,000 and $60,000 in repairs and restoration costs on average.

Gain Instant Access To Our Free Report, "7 IT Security Protections Every Business Must Have In Place Now To Protect Themselves From Cybercrime" TODAY! at https://www.getfrogworks.com/Cybercrime

Or call us today at (240) 880-1944

Is Your Website Search Engine Friendly?

SEO is incredibly complicated in some ways – but that doesn’t mean you can’t master some basic techniques to help you rise in rank on a search engine. Usually, you want your website to be three things to a search engine: crawlable, findable, and understandable. Though these terms may initially sound strange, they represent essential factors in any website’s SEO tactics.

Can Search Engine Spiders Crawl Your Website?

Spiders – also called bots or crawlers – are programs that most search engines use to index your content. Since you want your website to be indexed, you want to fight these spiders as little as possible. One of the easiest ways to make your website crawler-friendly is to give “directions” to spiders in your robots.txt file. You can tell the robot.txt which pages the crawlers should ignore and which you wish to be indexed.

Spiders also “speak” HTML and don’t understand pictures, Java, or Flash. So if your website is all pictures, a spider will have absolutely no idea what to do with it. Everything should be in text, and if you have videos, make sure you include a transcript.

Can You Be Found on the Web?

An easy way to determine whether or not your Internet presence is sufficient is to search for your services in your area. For example, if you do dog grooming in Orlando, search for “dog grooming in Orlando”. If you can find yourself pretty easily, it’s likely a crawler can as well – but if you have trouble, then so will a bot.

To win the popularity contest of the Internet, make sure you’re tracking your reach via something like Google Analytics – or Vertical Axion’s SiteSpy – and that you’re responding appropriately to the information gathered. If your ranking is low, make sure your content is crawler-friendly and unique. If your ranking is high, then you likely don’t have much to worry about.

One of the best things you can do for your website is to create a comprehensive back-linking system. Having links on any site is good, but the more powerful the website, the more valuable the back-link is. Stay away from “spammy” link-building activities. Google has taken extra measures as of late to make sure that any site that is categorized as spam and links to your site will drag your ranking down.

Is Your Content Human Friendly?

It is true that humans read while bots crawl, but good content on a page will make both parties happy. All you need is an exceptional format and structure.

(Continued on page 4)

The ONLY Way to Run Your Business

A lot of these tips come from the book *Anything You Want* by Derek Sivers, but they’re simply too good not to take a second look at. Think about them, and see if you can apply them to your business.

Business is Not About the Cash

A business can’t run without the cash, this is true. However, that doesn’t mean it’s all *about* making the cash. If your heart isn’t in it, and you’re not focused on making your dreams and someone else’s dreams come true as well, then you shouldn’t be running your business. Never do anything just for the cash – you’ll often regret it.

Focus on Improvement

Starting a company is a great way to bring improvement to your own life as well as to the world. You’re bringing jobs, necessary services or products, and experience to yourself and those who work for you.

Know Where Success Comes From

Success doesn’t come from forcing your product on other people. It also doesn’t come from promoting an idea that just isn’t working for you. Instead, it comes from finding something that does work and then constantly improving and reinventing it so it’s bigger and better than the last version.

You Don’t Need Money to Start a Company

Time and time again, we hear businesses that started on less than five or ten thousand dollars and have become something huge today. People turn a couple of hundred dollars into products that everyone loves. This is particularly true with the Internet companies of today – it doesn’t take a lot of cash to start a website and get your product out there so you can start helping other people.

Don’t Be Everyone’s Everything

You can’t please everyone, even if you offered every single option for every single service you have (some people would complain about having too much choice). So don’t try to. Focus on what you’re good at and offer it to those who will be pleased with it.

(Continued from page 3)

When you're writing page titles, make sure to add description and title tags for the bots, but design unique and interesting titles for the people. A unique title for every page will not only help visitors understand what you're all about, but bots will be able to distinguish between your pages so each one is indexed.

The body of your website should be both professional and pleasing to the eye. It should be free of grammatical and spelling errors, and the flow should be flawless. This may mean quite a bit of editing, but it's nothing a good writer or two can't handle.

What to Do with Unfavorable Customer Reviews

You're not really in business unless you have customers complaining about what you do. The internet is an asset to many, many small and medium business owners, and the kind of exposure you can get from simply being online is astronomical. If your business is particularly wonderful, you may experience a ton of positive business coming your way when you launch your website. But just because you do good business and do your absolute best to make sure everyone is satisfied doesn't necessarily mean that everyone is going to give you a positive review, and when these bad reviews pop up, they can be seen by anyone who is shopping with you when they Google your business.

But like everything, there is a way to combat negative reviews and make sure they don't hurt your business.

Is the Review Legit?

Some companies have stooped really low and have started battering their competitors with reviews that are untruthful. If you can collect evidence proving that another company is being obnoxious like this to you – say, you find the job posting that brings people to say negative things against you for a little cash – then you can e-mail the review sites and have such negative comments taken down.

However, if the review is legitimate, then sometimes the only way to make it better is to make sure your next few reviews are stellar.

Encourage your Customers to Leave Happy Reviews

One of the best ways to get people to leave good reviews is to run a contest that encourages them to do so. You can't pay anyone to leave a good review for you, and you can't even offer them any sort of compensation – but you can still encourage them if it's part of the process of being able to enter a contest, or a prerequisite for a special website offer. Even then, you can only encourage people to leave honest reviews for you, not just good ones.

Plus, most customers are happy to leave reviews when there's a little something in it for them and they have a reason to take ten minutes out of their busy days.

Deal Politely with Those Who Leave Negative Reviews

People know they wield a lot of power with their reviews, and thus will sometimes try to procure free services or product when they didn't have a good experience in order for you to receive good feedback. Make sure you have an established way of dealing with this kind of thing so when someone does approach you with a complaint, all involved know exactly what to do so everyone's on the same page. That way, no matter what, you have always done the exact same service to all customers and leaving feedback that is negative or positive at that point is completely up to them.

If you do get some negative feedback, don't sweat it too much – just keep up the good work and you'll see more positive feedback then not in no time.