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

Ribb"IT" Review

"There are far, far better things ahead than any we leave behind."

-C. S. Lewis

January 2019

Issue 1, Volume 9

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

No More Support For Microsoft Windows 7 and What This Means To You

Every few years this happens, Microsoft let's us know that they will no longer be supporting one of their older operating systems or Office versions. Sometimes, as is the case with Windows ME, Windows Vista, or Window 8, we don't care. We don't care because those were horrible operating systems anyhow. They were fraught with problems, security issues, never worked right, or no one really liked them at all – so they avoided buying them.

Then there are those, like Windows XP, which after 3rd party manufacturers built applications to be compatible with the then new operating system, people loved. It worked well, crashed less and was easy to use.

Windows 7, which Microsoft released on July 22, 2009 is of those that people loved and was well adopted. So, it is with much disappointment that Microsoft has set in stone that on January 14, 2020 it will no longer support the venerable, yet reliable Windows 7 operating system.

This means that the critical patches and security patches that protected your computers, network and data will be susceptible to attacks without Microsoft there to plug those holes. You may say, "Aren't you providing anti-virus so bad things don't happen?" The answer is, of course we are. But anti-virus is just *one* piece of a big jigsaw puzzle that protects your network.

Microsoft patches are another important piece of how we protect your business as they address specific bugs or flaws, improve the operating system with additional features or stability and also fix security vulnerabilities.

So, more that just patching your computer to improve them, if you don't replace your Windows 7 computers and your business has to meet HIPAA, Sarbanes Oxley, NIST or other compliancy guidelines, you will be out of compliance, typically due to Security Rules.

Well, for a while, Windows 10 was free until July of 2016, most applications were not ready for Windows 10 and frankly, Windows 10 (during that free period) was not ready either. Microsoft has spent a lot of time and effort toward improving Windows 10 – even causing more problems (see Windows Creator Update 1809), but all in all it has become a stable, even likeable operating system that will be around for some time.

It will also likely be the last Windows operating system that you do not have to pay a subscription

(Continued on page 2)

(Continued from page 1

charge for on a regular basis. Yes, that's right Microsoft is taking their operating systems to the same place as other things, like Office 365, Adobe Creative Cloud and store-bought anti-virus.

What is a business owner to do? Well, start with DON'T panic! You have a year to get there and we can help. Call us, we will take the time to meet with you to review your current situation. We will help you choose and implement the best and most efficient process for replacing those older machines that won't run Windows 10. We will evaluate machines that are three years older or newer that were purchased with Windows 7 to see if we can upgrade the memory or hard drive so that we can install Windows 10.

Officials Want To Know If Wireless Carriers Are Throttling Video

Remember earlier this year when net neutrality got killed off and everybody said it wouldn't matter? Well, it seems it might have mattered after all.

Recently, three US Senators sent letters of inquiry to four wireless carriers. They are investigating allegations that the carriers have been throttling (slowing down) video services or Skype video calls.

The allegations stem from recent research that utilizes the Wehe testing platform, which indicated that all four carriers had been doing exactly that.

As the Senators say in their letter:

"All online traffic should be treated equally, and Internet service providers should not discriminate against particular content or applications for competitive advantage purposes or otherwise."

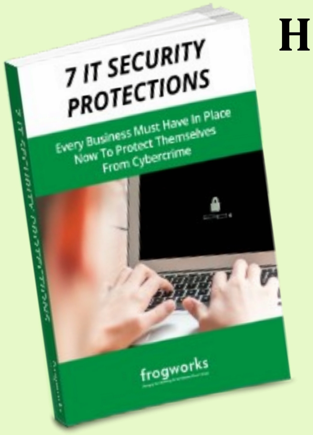
Here's a quick summary of what the Wehe tests revealed:

- Indications that AT&T has been throttling speeds of YouTube, Netflix, and NBC sports
- Indications that Verizon has been throttling speeds of Amazon Prime, YouTube and Netflix
- Indications that Sprint has been throttling YouTube, Netflix, Amazon Prime and Skype Video calls
- Indications that T-Mobile has been throttling Netflix, NBC Sports and Amazon Prime

It's likely true that much of the throttling can be explained by all four carriers' policies relating to limiting video throughput, especially where low-cost plans are concerned. However, it still raises disturbing questions, as these are exactly the types of issues the old net neutrality rules avoided.

Unfortunately, the new rules allow for a variety of abuses to go unchecked for months, years, or longer, and require significant oversight that simply didn't exist before.

Even more disheartening, there's an easy fix for it. Net neutrality matters because it allows the internet to be the ultimate level playing field. The sooner we can get back to that state of affairs, the better for everyone. Until that time, a cloud of suspicion is going to hang over all the major carriers every time evidence like this surfaces.


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

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

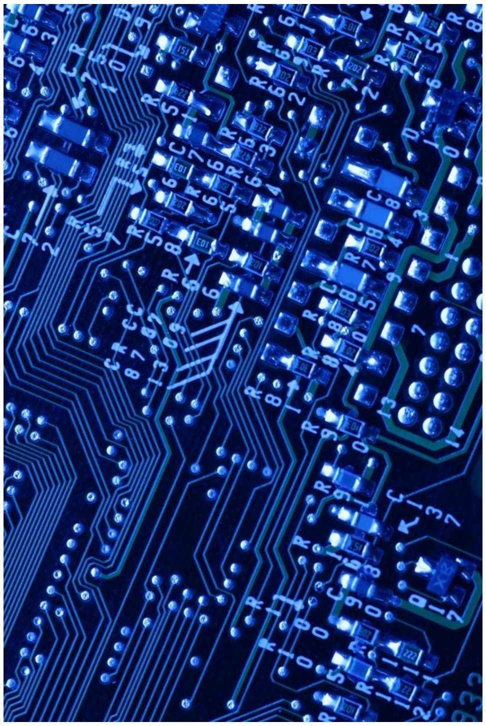
After working with dozens of small and mid-size businesses in the DC Metro area, we found that 6 out of 10 businesses will experience some type of major network or technology disaster that will end up costing them between $9,000 and $60,000 in repairs and restoration costs on average.

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

Are Graphics Processing Units Vulnerable To Hacker Attacks?



Bad news for computer users everywhere. Researchers at the University of California in Riverside have discovered that GPUs (Graphics Processing Units) are vulnerable to side-channel attacks like Spectre and Meltdown, which have been plaguing Intel CPU's for the better part of a year.

The team, (consisting of two computer science professors and two PhD students) reverse-engineered an Nvidia GPU and demonstrated three separate side-channel attacks. The attacks targeted both computational and graphics stacks, believing these to be the first ever side-channel attacks designed to work on GPUs.

All three of the newly discovered attacks exploit the user counter in the GPU, which is used for performance tracking and are available in user mode. This is significant because it means that literally anyone has access to them. All three also require the victim to download a piece of malware designed to spy on the user's system to provide information back to the hacker executing the attack.

The first of the three attacks tracks a user's internet activity and is made possible because GPUs are used to render graphics in web browsers. The attack is executed when a poisoned app utilizes OpenGL to infer browser behavior as it utilizes the resources of the GPU.

The second attack allows the hacker to glean password information, because GPU resources are used to render the login box on the user's screen. By monitoring memory allocations in the chip, a hacker can identify the specific keys pressed when entering a password.

The third attack targets computational applications and is designed to target neural network architecture. Its main purpose is to sniff out and steal neural network algorithms.

In terms of defending against these attacks, there's good news and bad news. Turning off user mode access to the counters is a viable defense, but unfortunately, many applications rely on that functionality. Turning it off will cause a number of programs (that you probably need) to stop working. Ultimately then, GPU manufacturers are going to need to engineer a fix in much the same way that Intel did for their impacted CPUs.

No instances of these types of attacks have been seen in the wild to this point, but now that the word is out, it's just a matter of time. 2019 stands to be a brutal year until and unless a fix is found and pushed out.

Uber Gets Hefty Fine From The EU For Data Breach

In recent years we've seen several companies suffer from hacks of various magnitudes. Over time, we've witnessed the growth of what could be described as best practices in terms of how to respond.

The typical arc goes something like this:

The hack is discovered. Immediately thereafter, the company discloses the pertinent details about the hack, including the number of users impacted, and specifics on what data was compromised. They apologize, tighten up their processes, and often pay for a year (or more) of free credit monitoring for users who were affected by the breach.

All they while, they're working with law enforcement to get to the bottom of who hacked them in order to bring the perpetrators to justice. That's not the path Uber chose to take when they were hacked two years ago.

Instead, when the hackers contacted Uber and demanded $100,000 to reveal how they compromised Uber's system, the company quietly paid up, and said the payment was a very large bug bounty. A year later, the company informed the users who had their data compromised.

Needless to say, that's fairly far removed from the established best practices. When the details came to light, the EU took action.

Recently, the UK's ICO (Information Commissioner's Office) and its data protection authority in the Netherlands both announced a decision to fine Uber for the disclosure delay. The UK fine amounted to £385,000 and the fine from the Netherlands amounted to €600.000.

In all, the breach impacted some 2.7 million users in the UK and nearly 200,000 in the Netherlands.

A spokesman from the Information Commissioner's Office had this to say about the matter: "The incident, a serious breach of principle seven of the Data Protection Act 1998 had the potential to expose the customers and drivers affected to increased risk of fraud."

Ultimately, the fines amount to little more than a slap on the wrist. Uber got off easy in that regard, but hopefully, the slap was hard enough that should another such incident occur, they'll choose to handle it very differently.

Google Continues To Battle With Malware In Play Store

In recent months, Google has taken steps to tighten up its processes so that fewer poisoned apps find their way into the Google Play Store. In addition to that, the company has stepped up its efforts to ruthlessly track down and remove malicious apps whenever and wherever they are found. By most accounts, that effort has been successful.

Sadly, it hasn't been completely successful, or as successful as they'd like it to be. Recently, independent security researcher Lukas Stefanko pointed the company to more than a dozen malicious apps still lurking on the Play Store. Worse, taken together, those apps had been downloaded more than half a million times.

Google acted swiftly and removed the offending apps, but based on the number of downloads, the damage has certainly been done.

What's worrisome is that these apps survived for quite a long time and managed to go undetected, even after Google strengthened their processes. Even worse, all the apps can be traced back to a single author, "Luiz Pinto," which is no doubt a pseudonym.

All of the apps were disguised as games and had interesting looking thumbnails to entice users to download them. None of them actually worked, and would crash when users would try to run them. Then the program would ask to install an additional APK (which would vary from instance to instance), but in no case was something benign installed.

All of the secondary APKs were malicious in their nature, designed to steal data in one form or another and send it back to the app's owner.

Clearly, Google has more work to do in this area, but the number of apps and downloads taken as a percentage of the Play Store as a whole are miniscule. Even so, it's a disturbing report, especially not long after Google made headlines for improving their processes.

Microsoft Is Bringing Augmented Reality To The Military

Microsoft just won a huge military contract worth $480 million to bring 100,000 customized AR (Augmented Reality) headsets, based on their HoloLens technology, to the US Army.

The army's plan is to integrate the headsets with their STES (Synthetic Training Environment Squad) system, which allows US forces to conduct hyper-realistic mock battles as practice before a live firefight, with an emphasis on improving close-combat capabilities, especially in subterranean and urban environments.

A spokesman for the Army had this to say:

"Soldier lethality will be vastly improved through cognitive training and advanced sensors, enabling squads to be first to detect, decide and engage. Accelerated development of these capabilities is necessary to recover and maintain over match."

A spokesman for Microsoft added:

"Augmented-reality technology will provide troops with more and better information to make decisions. This new work extends our longstanding, trusted relationship with the Department of Defense to this new area."

Obviously, the Army's version of the HoloLense headsets will be quite different from the consumer variants currently available. The Army will have wireless connectivity built in, and hooks that would allow other military gear like night vision goggles and sensors that provide real-time metrics on soldier performance. These metrics include basic health stats like heart rate, respiration rate to be fed into the HoloLens display.

Now that the ink is dry on this deal, the military is Microsoft's largest HoloLens customer, which isn't necessarily a bad thing. Already there's a long and growing wish list of new capabilities the army needs to make the headsets even more useful, some of which will eventually (and inevitably) filter back into the commercial market.

For one thing, the army is very interested in getting the overall weight of the headset down. Currently, the HoloLens headset weighs upwards of fifteen pounds. The army's goal is to see it reduced to just one pound.

A daunting challenge, like the rest of the items on the army's wish list, but these things will no doubt help push the technology forward.