Q-News

April 2019

A Word from Jack

It has been a little time since our last newsletter, but a lot of exciting things are happening at Quanexus. We have made a few internal organizational changes that have worked out very well and we added a few new team members. I'm excited to say that since making these changes we have been more responsive to our clients' needs and have become more efficient internally. In the world of technology, you have most likely seen a lot of hype about 5G and the promise of 5G. 5G has a lot to offer but there are some challenges that must be overcome before we see it fully rolled out. Have you ever wondered if your personal information has been stolen, well the answer is, most likely yes? With all the breaches over the last few years and the continued breaches it is highly likely that there is some personal information about you on the dark web. For those of you who really like Windows 7, and or are still running Windows 2008R2 servers in your organization, time is running short. These two products will be out of extended support on January 14, 2020. If you haven't upgraded yet, time is running out before your system becomes more vulnerable to cyber threats.

Windows 7, Windows Server 2008R2 and Office 2010 are Reaching End of Extended Support

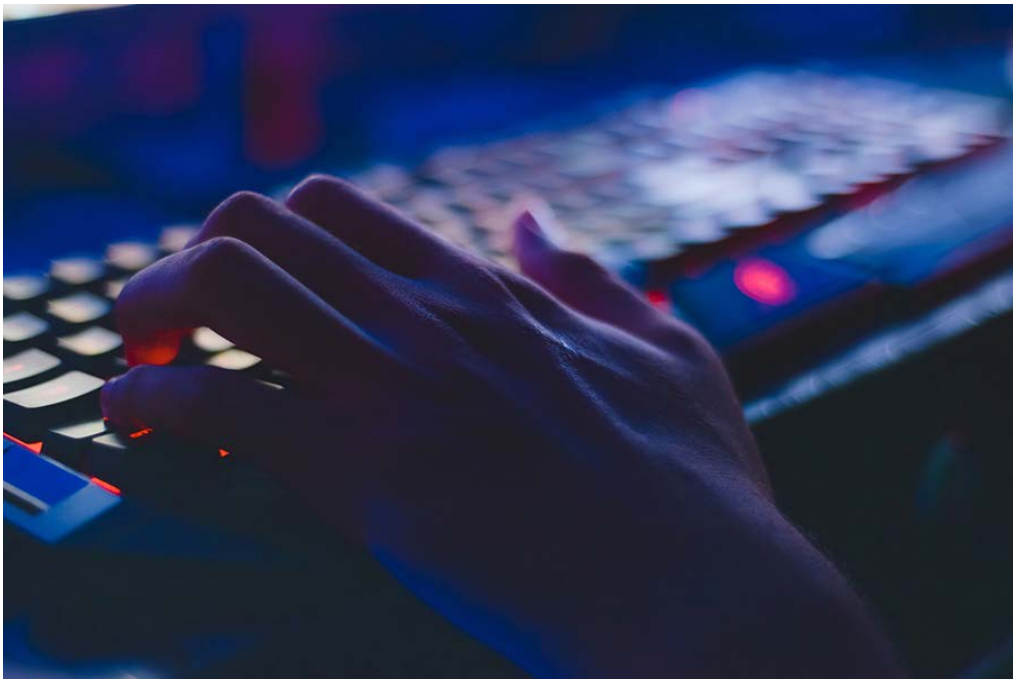
The time is quickly approaching when Windows 7, Windows Server 2008 and 2008R2 will no longer be supported. Technically these products are reaching the end of their extended support. Microsoft gradually ends support on their products. There is an official date for end of main stream support and another date for end of extended support. Extended support ends on January 13th, 2020 for Windows 7 and Server 2008. Extended support will end on October 13th, 2020 for Office 2010.

End of main stream support means that there will be no feature enhancements added to the product. Microsoft will continue to release patches that fix stability and vulnerability issues as they are found. End of extended support is defined as Microsoft will not issue stability or vulnerability updates.

Running software that is no longer supported represents a great risk to organizations and the end user. When criminals know that security patches will no longer be developed, they begin to work very hard at finding new vulnerabilities and will continue to do so. The new exploits that are discovered, near the end of support date, won't likely be released immediately. The criminals will release them after the end of support date, because the vendor will no longer be supporting the product. These new exploits will be used to target Windows 7 systems, fully knowing that the systems are vulnerable.
Businesses, if you must run Windows 7 or Server 2008 after the end of extended support, there are a few things you can do to keep these older systems protected. If you already have a good security stack installed, like our Q-Stack, the likelihood of a successful attack is reduced, but that is still not good enough. An additional firewall will need to be installed to separate the Windows 7 and Server 2008 devices. This firewall will require very tight rules that limit the device's access to the internal network and the Internet. Depending on the type of firewall you have, it may be possible to create a virtual firewall on your existing device to create this additional layer of protection.

Quanexus™
571 Congress Park Dr.
Dayton, OH 45459
937.885.7272
quanexus.com

Hacked Website Databases for Sale on the Dark Web



There has been a rash of stolen databases being sold on the dark web. On February 11th, The Register's, Chris Williams reported that 620 million online account details were stolen from 16 hacked websites. Some of the more well-known sites were MyFitnessPal (owned by Under Armor), MyHeritage, Dubsmatch, and CoffeeMeetsBagel.

The hacker goes by the name Gnosticplayers and is allegedly in the US. She/he claims that the motives for stealing these databases are money and the downfall of American Pigs, as reported by ZDnet.com's Catalin Cimpanu.

In round 2, shortly after the release of the 620 million user's records, Gnosticplayers reportedly hacked another eight sites and acquired another 127 million user records. In round 3, they hacked another 96 million user records. In round 4, they were able to steal from another six companies, 26 million user records. The last two rounds they did not intend to hack, but did so because they believed that these companies did nothing to protect themselves.

Not all the companies hacked had their data offered for sale on the dark web. Some of the companies, especially start-ups, paid an extortion fee to protect their client lists.

The hacker claims the reason the attacks were successful was due to vulnerabilities found in the online web applications.

The databases vary in content, but they all have the individual's names, email addresses and hashed passwords. Users who chose poor passwords that were stored in databases, that were protected by simple MD5 encryption, are easily cracked.

Who is buying these hacked databases? There are two groups that buy user databases- those that are spammers and the other group is known as credential stuffers. The stuffers take the user IDs and cracked passwords and attempt to log into other websites, pretending to act as the real owner and steal information, money, or try to exploit the real account owner.

To prevent your organization from being a victim of an attack like these, there are security controls that need to be put in place. Quanexus always recommends a layered security approach and we have developed our Q-Security Stack to make it more challenging for attackers to get your data.

The best protection end-users can implement are:

- **Use of strong password/pass phrases of at least 13 characters**
- **Do not use the same password on multiple sites**
- **Implement 2-factor authentication if possible**
- **Keep your systems updated and patched, including 3rd party software, e.g. Adobe, Java, and your browsers**

5G Soon to be a Reality

Things are heating up and it looks like Verizon will be the first to rollout 5G. Verizon has officially announced that its first 5G FR platform will be turned on April 11th in select Chicago and Minneapolis areas. By the end of 2019, Verizon expects it to be rolled out in 30 markets. The cost to upgrade your current plan to 5G will be $10 per month. The first 5G enabled phone is the Motorola Moto Z3. The Moto Z3 will be available for pre-order on March 14th. The Samsung S10 5G will debut next month. AT&T is planning on rolling out 5G in Las Vegas, Los Angeles, San Diego, San Francisco, San Jose, Orlando, and Nashville by the end of June. Sprint's plan for rolling out 5G this year includes these cities: Atlanta, Chicago, Dallas, Houston, Kansas City, Los Angeles, New York City, Phoenix, and Washington DC.

Windows 10 to Uninstall Buggy Updates

For those of you who have been following the challenges with Microsoft's Windows 10 updates, there is help on the horizon. For those of you who weren't following the issues, simply put, some of the updates broke hardware drivers. The hardware driver issues only affected certain accessories in the computer. The range of problems created are from sound cards not working to computers not booting (fully turning on).

While the Microsoft updates created the issues, the problems were not entirely Microsoft's fault. Microsoft was supplied with updated drivers from major vendors, and it was these drivers that created the incompatibility issues.

With Microsoft's next update (1903), which should be released in the next few months, they have included a roll-back feature. At this point, the roll-back feature is limited to systems that won't complete their boot cycle. If the operating system determines that there is an issue and the boot cycle terminates, it will automatically roll back the last update making the computer usable again. This new feature will also stop the automated update process for 30 days to protect itself from re-downloading the same update.

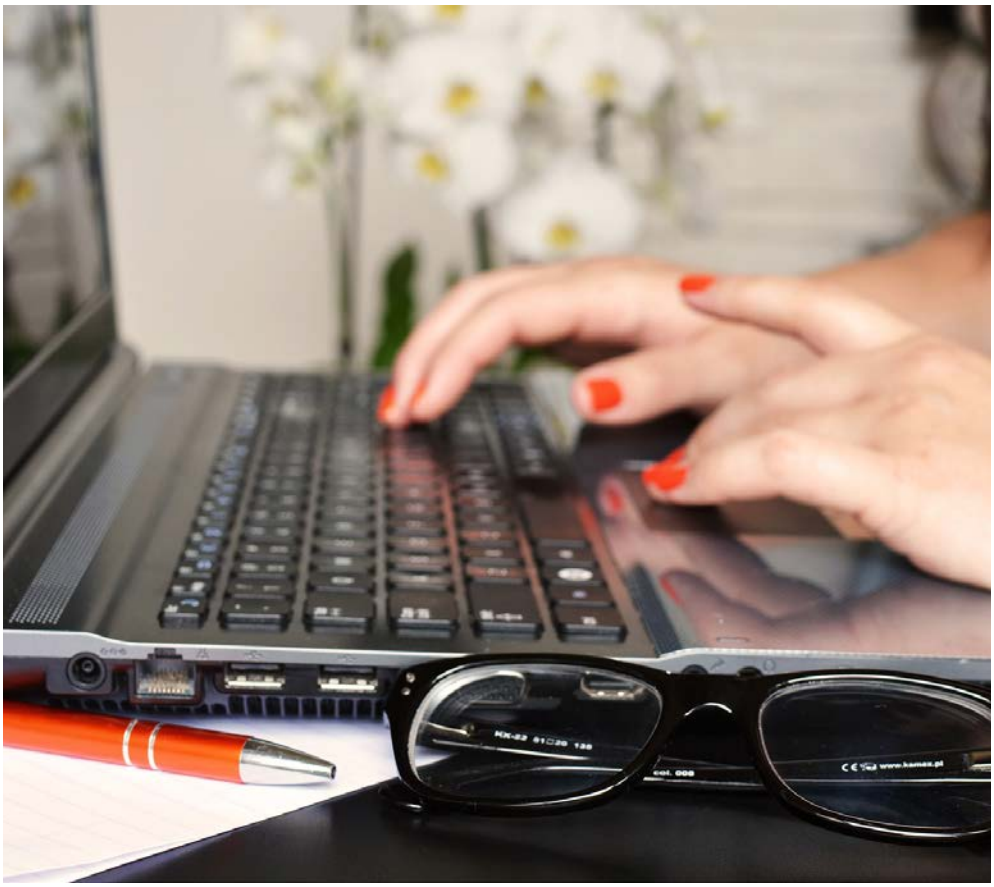
USB Charging

A question that I have been asked many times, is how do USB chargers work. This question typically comes from semi-technical people that have a basic understanding about battery chargers. The problem is the word we use to define the things we plug into the wall, aka wall warts, a charger. The device that plugs directly into the wall, is not a charger, but rather a power supply. More specifically, it is a switch mode power supply (SMPS), which is very efficient. The actual charging circuit (charger) is built into your device (phone, iPad, notebook, etc.). To clear up the confusion, we are incorrectly calling the power supply a charger.

Patch Management and Notebook Issues

For our clients that are on our Q-Works platform, notebooks are becoming more challenging to keep updated. On your monthly status reports, there is a section that shows patch status of each computer and an overall score that indicates how successful the patch management solution is.

The challenge with notebooks is, when they are turned off, they are not receiving updates. If you have notebooks in your environment, your users need to have these notebooks turned on after hours so they are successfully updated. Any unpatched system represents a potential vulnerability to your network environment. The notebooks do not need to be in the office to receive updates, they only need to be turned on and have access to the Internet. If your notebooks are scheduled to go into sleep mode, this needs to be turned off. For more information or help with your notebook environment, please contact our support desk.



What is 5G All About

There are many benefits that will come from the new 5G infrastructure that is being created today.

Initially, we will see Internet speeds increased by a factor of 100x. Speed is one thing, but low latency is just as important. Today's 4G has relatively high latency, which makes watching HD media a challenge. With low latency, HD streaming video will become a reality. Other benefits of 5G are:

- **It will greatly enhance the ability of self-driving cars**
- **Municipality traffic control**
- **IoT device enhancement of sensors**
- **Assist with the increase of farm yields**
- **Medical procedures and remote surgery**

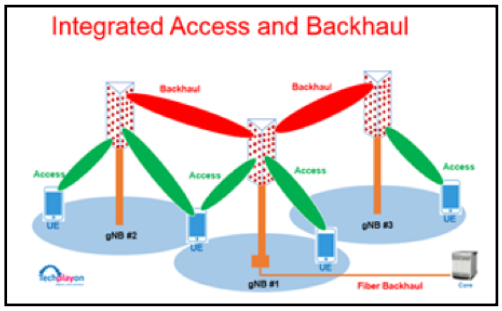
With the new millimeter band spectrum, we will see small 5G cell sites densely distributed throughout the country. As 5G rolls out, the ability to connect with many IoT devices/sensors will provide invaluable information to increase the efficiency of everything. A few examples of industries that will quickly take advantage of this new technology are: medical, agricultural, and automotive/traffic control. Imagine having sensors in the field to monitor crop yields and check the health and status of livestock. In the medical field, 5G will increase the ability for augmented technology to assist with complicated surgeries. In the automotive world, autonomous cars will be better able to communicate with each other and will be one of the major technologies used to prevent collisions. Cities will be able to control traffic patterns based on real time information transmitted from vehicles. The possibilities are endless.

Back in the days of 2G and early 3G, the definition of what these terms meant were not as clearly defined as they are today. All the major telecommunication standards organizations got together and created the 3rd Generation Partnership Project (3GPP). This group defined the 3G standard and would define the specifications of future G technology. The difference in technology between 2G, 3G, and 4G is based on modulation techniques. Using different modulation techniques, we were able to transmit more data in the same spectrum space. Moving to 5G is a major technological paradigm shift from 4G. Basically, 5G is a list of approved/agreed specifications, standards and protocols. Depending on the infrastructure where the small cell sites are installed, power lines or fiber can be used to back haul the data.

The 5G standard includes many technologies, which offers the cell carriers options for implementation. The long-term implementation goal that most carriers will implement, includes small cell sites that have coverage ranges of 200 yards. These small cell sites will connect directly to cell phones or IoT devices. The small cell sites will back haul (connect) wirelessly to a data center for distribution.

3GPP has defined what the specific technologies that are 5G and what is not 5G. A few years ago, several of the big companies put up enhanced 4G services that they were marketing as 5G-like service, but the services they were selling were not real 5G as defined by the standard.

While the promise of 5G looks good and the major carriers are all set to start rolling out the technology, there are still some very big technological issues that need to be worked out. Many initial 5G roll-outs will be based on 5G FR1 (frequency range 1), with a migration plan to move to 5G NR (new radio, frequency range 2). It is estimated that it will be another year before some advanced features of 5G will be rolled out. There are some industry experts that are questioning the economics of 5G and are concerned whether 5G will be a profitable model for the carriers.



Follow Quanexus on Social Media!

Find Quanexus on Facebook, Twitter, LinkedIn and Instagram! We share blog posts, useful articles, and pose questions to our followers. We also like to share pictures of our team to give you a glimpse of what's going on in the office!

Also, subscribe to our email list to regularly receive tech news, cybersecurity alerts, and information on upcoming events. **Visit Quanexus.com to sign up!**

@Quanexus571 **@Quanexus** **@Quanexus** **@Quanexus571**