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

Ribb"IT" Review

“Success is not final;

Failure is not fatal;

it is the courage to continue that counts.”

– Winston Churchill

September 2020

Issue 7 Volume 10

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

WE'RE MOVING!

Beginning September 11, our new mailing address will be:

2670 Crain Highway, Suite 304
Waldorf, MD 20601

Latest Microsoft Update Provides Some Needed Fixes

If you aren't normally in the habit of installing updates when companies release them, you'll probably want to make an exception for KB4484439.

It is a non-security update for Windows Installer editions of Office 2013 and 2016 products.

If you use Office 2016, and frequently edit Word documents that feature custom XML values, these will cause Office 2016 to hang or create serious delays when opening. The recent patch fixes that issue.

In a similar vein, if you use Skype for Business 2016 and the device you're using is awakened from sleep mode, it could cause Skype to hang, forcing you to end task and restart the program. The most recent patch addresses that issue as well.

Finally, there's a bug in Excel that causes it to become unresponsive after using Control+Shift+Arrow keys for scrolling when the user is sharing Excel in a window via Microsoft Teams. As with the others we've mentioned so far, the most recent patch fixes that.

As the name of this patch indicates, none of the items mentioned above are security flaws, but depending on what software you use and how you use it, this patch could solve some serious problems for you.

You can grab the patch from the Microsoft Download Center or via

the Microsoft Update Catalog and install manually, or by using the Microsoft Update Service, which will install the update automatically.

Note that you'll probably need to restart your computer after applying this patch. The best approach is to simply plan for it and reboot when the installation is complete. If that's impractical, just keep an eye out for any odd behavior from your Office products (2013 or 2016), or Skype, post patch installation and definitely reboot if you start seeing any unusual behavior.

Used with permission from Article Aggregator

2020 – The Year Everything Changed

As we know, during this pandemic phishing and hacking attempts are on the rise. Hackers never sleep. They've started to use these times of unrest as good opportunities to breach security while everyone is distracted. Even if our business includes security, we can even fall prey to some of the tricks. For example, one of our employees recently received a text message from Amazon saying that she could claim a reward and it would be shipped and delivered to her within two days. Since she shares the Amazon account with her husband, she asked him, "Hey, did we get an Amazon reward?" And he said, "No, nothing. No reward. They don't have a reward system." Which of course they don't. She was lucky. Too many people fall for these types of scams every day.

During this pandemic, these attacks are on the rise. We don't anticipate any slowdowns to this nefarious activity anytime soon.

Hackers prey on times like these. They're posing as large consumer companies, and they're preying on people who may not be paying attention to what's going on. Phishing attempts across the board are on the rise. Maybe a text message won't be relevant to your company, but they'll try anything to get a foot in your door and steal some company information. Tell your clients, if some of their employees use shared passwords and a hacker finds a way into their system, they could be wide open for data loss or a ransomware attack.

There is also a new criminal enterprise in cyber-hacking taking place. Some of you may have applied for PPP, the payroll protection loans from the government during all this craziness. Well, these cyber hackers are using that process for Phishing attacks, and they're stealing information with fictitious emails and using it to gain bank account access. Some businesses have received emails like this: "Your PPP has been approved for X amount of dollars, please submit your information here and it will be transferred within the next 10 business days." They're following the government templates and it's crippling businesses. We have to be very cautious, not only for ourselves from a security standpoint, but we have to educate our employees and clients on these threats and how to prevent them.

Let's turn a little bit and talk about the current state of the workforce. Before all this started, a small percentage of the workforce worked remotely, and within about 14 days, it went from 30% working remote to about 62% of the workforce going remote. We don't anticipate that's going to change anytime soon. There's no going back. The state of the workforce is now more adaptable. Moving forward, it seems small businesses have three choices on how they can handle their workforce: Force everyone to come back into the office, let employees who work remotely to continue to do so, and lastly, have a hybrid of in-office and remote staff.

From what we can tell, there needs to be some level of adaptability. People need to be able to move in and out of the office and work remotely when they are able to. To get this to work, we have to do away with the perfect attendance mindset. So many people come to work sick because they have to, because they need the paycheck. After all, they need to get their jobs done, and they need to feel like they're integral to the team. For various reasons, too many people go to work sick.

Businesses need to change the culture and say it's okay to stay home and maybe it's okay to stay home and rest if you have to, but we'd prefer you stay home and work if you can. You have to figure out where that fine line is. But the workforce structure needs to change. It's got to adapt. Sometimes life gets in the way and we can use some flexibility.

Adapting is what all of us need to do right now. And that could open the doors to unforeseen opportunities. For example, we were in the middle of planning our quarterly Academy event in May when the pandemic hit and people didn't want to travel. Instead of cancelling it, we took on the challenge of streaming our training sessions live, every day, for five days in a row! If you were lucky enough to view some of it, well, you could say that maybe we bit off more than we could chew. But we committed to it, we integrated new technology, and we made it happen. And it was so well received that we're doing it again in September.

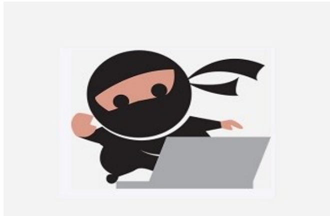
As Managed Service Providers, we cannot be afraid of technology. We need to be brave enough to try new things and learn from them, even if we fail. Especially if we fail. We need to learn new things and show our clients that we are keeping up with the times. Stopping cyberattacks and helping employees work remotely didn't happen a few years ago. Is there a problem one of your clients is having that you can't find a solution for? Invent something to fix it! Try thinking differently. Be a leader in our industry. Adapt, grow, and succeed. Because if you don't, someone else will.

Article by Chartec

We now have an E–newsletter!

… but we might not have your email address! If you would like to receive our newsletter though email please visit us at **www.getfrogworks.com/newsletter** and sign up.

Android Users Beware Of BlackRock Malware Credential Stealer



Do you have an Android phone? If so, be advised that there's a new threat to be on the lookout for.

The threat takes the form of a malware strain that's being called BlackRock. It is a banking trojan that specializes in pilfering login and credit card information, which means that if you get infected, it's likely to hit you hard.

The new variant was discovered by security researchers and analysts operating out of ThreatFabric. Based on an analysis of the code, it is a derivative of the Xerxes banking malware, which traces its roots back to the LokiBot trojan.

The key difference between this malware strain and the strains it was derived from is this: LokiBot and Xerxes focused their attention exclusively on banking and payment card information. BlackRock is equally interested in social media and dating site logins.

It's a fairly stealthy piece of code, too, disguising itself as a Google Update, which requests Accessibility Services privileges and hiding its icon when it is launched. Even worse, once a victim grants the malware access to Accessibility Services, it will begin granting itself additional permissions out of the sight of the victim.

In addition to banking apps, BlackRock also targets a number of cryptocurrency wallet apps, including Coinbase, BitPay, and Binance, as well as popular apps like Microsoft Outlook, Gmail, Uber, Amazon, Netflix, and Google Play.

The researchers at ThreatFabric had this to say about their discovery:

"*The second half of 2020 will come with its surprises, after Alien, Eventbot and BlackRock, we can expect that financially motivated threat actors will build new banking Trojans and continue improving the existing ones.*

With the changes that we expect to be made to mobile banking Trojans, the line between banking malware and spyware becomes thinner, banking malware will pose a threat for more organizations and their infrastructure, an organic change that we observed on Windows banking malware years ago."

All that to say, it's a serious threat, so be on the alert for it.

Used with permission from Article Aggregator

Billions Of Breached User Credentials Are Available For Purchase

On a regular basis, we see headlines talking about how this or that company got hacked and X number of employee or customer logins got exposed. However, since those headlines happen in isolation, it's easy to lose sight of the bigger picture. A trip to the Dark Web will reveal just how big of a problem the world faces. If you dare venture into those waters, you'll find literally billions of user accounts for sale.

In fact, by scouring various forums on the Dark Web, you can find more than fifteen billion credentials for sale, and more than five billion of them are unique.

Typically, hackers sell login credentials by company, but some larger collections are aggregated by industry. Of those, user accounts and passwords from non-financial service companies including VPN, the adult industry, the video game industry, and social media tend to be the least expensive. They tend to be sold for less than twenty dollars. Contrast that with user accounts and passwords from the financial services sector average about $70 each.

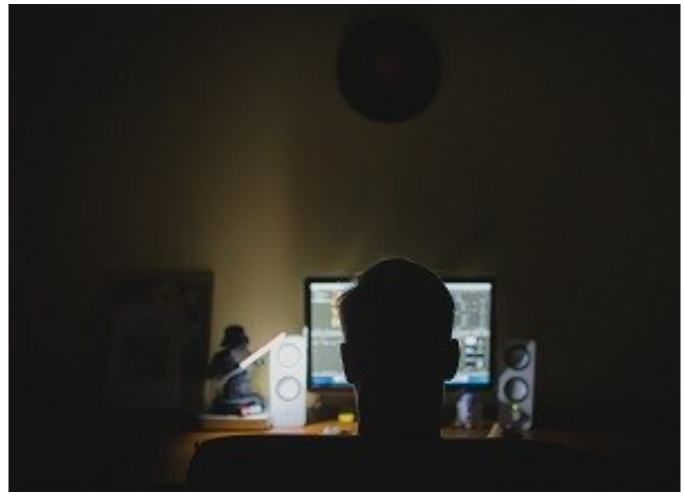
The real money though, is in accounts where a hacker can confirm a bank balance for an online bank account. In those instances, depending on the confirmed balance, the credentials can go for $500 or even more.

The most expensive login credentials on the web are those with confirmed domain admin access. These are not sold at a fixed price, but rather, auctioned to the highest bidder. They average more than $3,000 per account, but in one instance, sold for a staggering $120,000.

The bottom line here is simply this: Your information is valuable, and there's a largely invisible market for your login information. Guard it closely and make sure your passwords aren't easily guessed. When a company you do business with is hacked, don't take any chances. Change your password immediately. Don't become a statistic.

Used with permission from Article Aggregator

Remote Workers Are Getting Hit By Ransomware



According to the 2020 Vulnerability and Treat Trends Report, the number of new samples of ransomware increased by a staggering 72 percent during the first half of this year.

Hackers around the world have come to increasingly view it as their go-to attack option.

As with a great many things in recent months, this trend can be traced back to the COVID-19 pandemic. In response to the virus, untold millions of employees began working from home, which allowed them to stay productive, but at a terrible cost to network security. Few companies can afford to provide the same level of security and protection to their remote employees as they can when everyone is in the office.

Unfortunately, the moment a remote employee is infected and connects to the corporate network, the malware in question spreads like wildfire. Worse, since IT staffs are running thin these days and many security professionals themselves working from home, they're relatively less able to deal with the rising threat.

The biggest and best way to protect against a ransomware attack now and at some point in the future, when the pandemic has finally run its course, comes down to visibility. Specially, the IT security people who have watching your network need full visibility and the means of analyzing how critical network assets could potentially be accessed by an agent moving laterally within the network, with or without proper credentials.

Additionally, this full and transparent view of things gives your security professionals the means of telling, at a glance if VPN's, firewalls and related systems are properly configured and have all the latest security patches installed.

While that certainly doesn't provide bullet-proof protection, that kind of visibility goes a long way toward minimizing your risk. If you don't have something very like that in place right now, you need it as soon as possibly.

Used with permission from Article Aggregator

Labor Day 2020 will occur on Monday, September 7. Labor Day pays tribute to the contributions and achievements of American workers and is traditionally observed on the first Monday in September. It was created by the labor movement in the late 19th century and became a federal holiday in 1894. Labor Day weekend also symbolizes the end of summer for many Americans.

We hope you enjoy this Labor Day, which falls during such unprecedented times!