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

Ribb"IT" Review

"When everything seems to be going against you, remember that the airplane takes off against the wind, not with it."

Henry Ford

August 2020

Issue 6 Volume 10

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

We are excited and proud to announce that Frogworks has been accredited by the Better Business Bureau!

BBB ACCREDITED BUSINESS

New Powerful Malware Is Targeting Windows-Based Machines

Researchers have discovered a devilishly clever new stain of malware currently in use by hackers around the world. The new strain is appropriately called "Lucifer," and has been making life quite difficult for IT professionals managing Windows environments.

The malware exploits critical vulnerabilities in Windows-based systems to launch DDoS attacks and install cryptojacking code.

The latest version (2.0) of the code was discovered by researchers Durgesh Sangvikar, Zhibin Zhang, Chris Navarrete, and Ken Hsu, on May 29, 2020. They discovered it while investigating the exploit of CVE-2019-9081, which is a deserialization bug in Laravel Framework that can be used to conduct RCE (Remote Code Execution) attacks.

Their research revealed that CVE-2019-9081 is just one of many critical security flaws Lucifer exploits, including:

- CVE-2014-6287
- CVE-2018-1000861
- CVE-2017-10271
- CVE-2018-20062
- CVE-2018-7600
- CVE-2017-9791
- CVE-2019-9081
- CVE-2017-0144
- CVE-2017-0145
- CVE-2017-8464

Few malware strains incorporate code designed to exploit so many different security flaws, which makes Lucifer a serious threat indeed.

If there's a silver lining to be found, it is in the fact that all of these flaws have already been addressed via patches. So it comes down to making sure your software is up to date and running the latest and greatest security patches. The researchers who discovered it say that there are ongoing campaigns that are currently wreaking havoc on un-patched systems and urge all system admins to make sure the software they're running is patched as soon as possible.

In practice, Lucifer 2.0 works by scanning for open TCP ports 135 (RPC) and 1433 (MSSQL). When it finds a potential target, it will use credential-stuffing attacks to gain access to the targeted system. Once it gains a foothold, it installs XMRig, which is a program used to covertly mine Monero (XMR) cryptocurrency. Additionally, the malware connects to a command and control server where it can receive additional instructions.

As we said, it's a serious piece of work and not to be taken lightly.

Used with permission from Article Aggregator

If 123456 Is Your Password, Change It Immediately

You probably aren't familiar with the name Ata Hakcil. He's a computer engineering student who recently conducted one of the largest password security surveys currently available.

To conduct his research, he collected a number of username and password "data dumps" from the Dark Web and analyzed the passwords he found there. Hakcil was able to analyze a massive collection of more than a billion passwords, looking for trends and commonalities.

IT Security Professionals have long known that password security is an area of persistent weakness that leaves companies of all shapes and sizes exposed. Hakcil was able to measure and assess just how bad that problem is. What he found was depressing.

The most commonly used password in the collection he analyzed was simply '123456,' which appeared in his dataset more than seven million times. It is the most widely used password in the world. Put another way, a staggering 1 person in 142 was found to have used that simple password. As you might suspect, that is laughably easy for a hacker to guess using the simplest of techniques.

In addition to that, Hakcil discovered that the average password length is 9.48 characters, which isn't great. Given the password referenced above, is better than you might have guessed.

Other relevant and intriguing statistics culled from this study include things like:

- Only 12 percent of passwords include a special character
- 29 percent of the passwords reviewed used alphabet characters only
- 13 percent used numbers only
- Given the above, fully 42 percent of all the passwords in the dataset were vulnerable to quick "dictionary style" attacks that would allow a hacker to gain access with minimal effort.
- The most common 1000 passwords unearthed by this research accounted for 6.607 percent of the total, which gives hackers a long list of low hanging fruit to work with.
- With the most common 1 million passwords, the hit rate is 36.28 percent. With the most common 10 million passwords, the hit rate is 54 percent. This makes most networks incredibly easy to breach.

If you're wondering why we keep reading about so many high profile data breaches month after month, the results of this research go a long way toward explaining it, and that's unfortunate.

Used with permission from Article Aggregator

Google Meet Now Available On Gmail Using Mobile Devices

Google recently published a blog post that didn't get much attention, but that outlines a major change to the way the company's video collaboration tool "Meet" works.

The blog post reads in part, as follows:

"*In the coming weeks, you'll soon notice a new Meet tab on your phone's Gmail app where you can see upcoming meetings scheduled in Google Calendar, and easily join them with a single tap....If you don't want Meet to appear as a tab in the Gmail app, access the Settings from the hamburger menu in the top left corner of your inbox, tap on your account, scroll down and uncheck Meet.*"

This is a small change, but it represents a huge improvement in the way Meet works. The change makes it much more streamlined and efficient, which dramatically improves the quality of the user experience.

The change builds on Google's decision earlier this year to make Google Meet free for all users, which arose from the changes the global pandemic wrought in how the world works. Demand is spiking for video conferencing services due to worldwide lockdowns. Popular video conferencing service Zoom is stumbling over security concerns. Google and other tech giants moved quickly to take advantage of the surge in demand. This represents the latest manifestation of those changes.

Google has made a number of tweaks and improvements to Meet since the surge in demand began. Although they're playing it close to the vest in terms of the future changes they have planned, one thing that seems clear is the fact that more changes and improvements are coming.

Kudos to Google for rising to the challenge and making their video conferencing service more accessible and more user friendly. It is rapidly becoming the default choice for a growing number of organizations. If you're not currently using it and you're not 100 percent satisfied with the video conferencing service you are using, it's well worth checking out.

Used with permission from Article Aggregator

Hackers Used Favicon Website To Steal Credit Card Information

Hackers are constantly on the lookout for new ways of causing mayhem and stealing data.

Recently, researchers have unearthed a new technique to be on guard against. A few hackers have begun embedding credit card stealing scripts inside favicon meta data.

If you're not familiar with the term, you definitely know what a favicon is.

It's a custom icon used by websites for branding, associated with a specific URL. Although not universal, they are ubiquitous on the web and most companies have them.

While the idea of embedding malicious scripts on websites to steal credit card information is not new, the notion of hiding those scripts in the EXIF files of a company's favicon to avoid detection is both new and innovative. The new technique was spotted by researchers at Malwarebytes. They discovered the script embedded as described above, and designed to steal credit card data from sites making use of a popular WordPress ecommerce plugin called WooCommerce.

Of course, the script could be modified to attack any other ecommerce platform, so this isn't a threat that's unique to those making use of WooCommerce. If you do use that plugin, you should have your IT staff perform a careful check of your system to ensure that you haven't been compromised. The value of embedding the script here is that most scans don't include favicon meta data by default. Fortunately, that's easily fixed. So going forward, as long as you be sure to include it, then your risks should be minimal.

This is by no means the first time hackers have found an unusual point of insertion for the scripts they rely on to cause harm, and it certainly won't be the last. Just be sure that your IT staff is aware of the issue and stay vigilant.

Used with permission from Article Aggregator

Survey Shows How Employees Working Remotely Affects Business

Tens of millions of workers have been forced to work from home as the COVID-19 virus rampages around the globe. That has naturally increased reliance on internet connectivity and disrupted a number of longstanding, well-established working routines. Some of the changes have been for the better, including not having to fight traffic during the daily commute, for example.

However, other changes have made it difficult to work effectively and efficiently. Until recently, no one has been able to study or precisely measure how those changes are impacting the legions of people currently working from home.

That is beginning to change. Recently a California-based tech firm called Fluxon published the results of a survey they conducted to get a better handle on how work behaviors have changed with so many people now working remotely. The results of the survey contain a number of surprises.

Here's a quick overview of the company's findings:

- Nearly one quarter (23.3 percent) of survey respondents reported feeling more disciplined and almost a third (29.6 percent) report that they are more creative working from home than they were in the office.

- Nearly three quarters (72.4 percent) of respondents reported that there have been challenges and difficulties with the transition, with the top ten problems survey respondents encountered being:

- Technology/connectivity issues (50.6 percent)
- Communication issues (39.6 percent)
- Virtual Meeting issues (34.4 percent)
- Lack of social interaction (32.5 percent)
- Boredom (31 percent)
- Difficulty collaborating with colleagues (29.9 percent)
- Not enough face to face time with team members (26.3 percent)
- Loneliness (25.1 percent)
- Difficulty accessing company resources (19.1 percent)
- Difficulty balancing work and home life responsibilities (18.6 percent)

Other issues included things like unproductive meetings, difficulty stopping or stepping away from work, insufficient workspace, and colleagues contacting workers outside of normal business hours. In addition to that, fully a third of survey respondents said they felt less disciplined and efficient since working from home.

The survey results are fascinating and clearly illuminate the challenges, opportunities and areas where working from home can be improved. Wise is the manager who takes these statistics to heart and uses them to make incremental improvements.

Used with permission from Article Aggregator