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

Ribb"IT" Review

The secret of getting ahead is getting started.

-Mark Twain

March 2020

Issue 3, 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

CoronaVirus Scare Is Being Used By Scammers To Trick People

There is no low that hackers and scammers won't stoop to.

The US Federal Trade Commission (FTC) has issued a warning about a worldwide scam in progress relating to fears surrounding the CoronaVirus. The FTC's announcement speaks for itself.

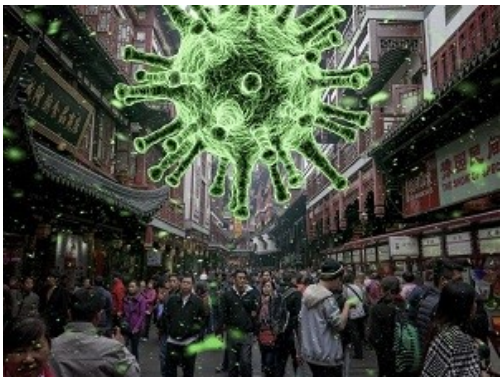
Their announcement reads, in part:

"Scammers are taking advantage of fears surrounding the Coronavirus. They're setting up websites to sell bogus products, and using fake emails, texts and social media posts as a ruse to take your money and get your personal information.

The emails and posts may be promoting awareness and prevention tips, and fake information about cases in your neighborhood. They also may be asking you to donate to victims, offering advice on unproven treatments, or contain malicious email attachments."

Even worse, it appears that there are multiple campaigns like this, running in tandem.

Francis Gaffney is the Director of Threat Intelligence for Minecast, which is one of several companies tracking the issue.



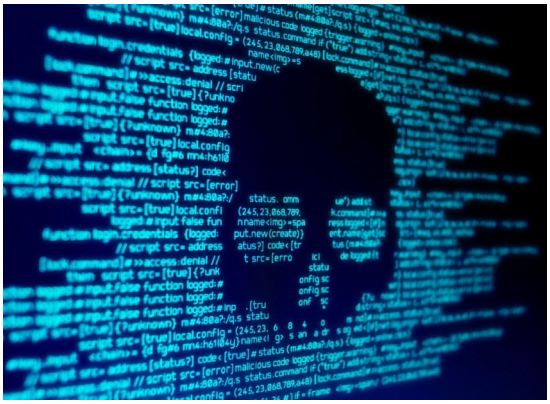
Francis added this:

"The sole intention of these threat actors is to play on the public's genuine fear to increase the likelihood of users clicking on an attachment or link delivered in a malicious communication to cause infection, or for monetary gain."

In short, this is about as despicable as it gets. Then again, hackers and scammers have been known to send emails targeting children, so it shouldn't come as a great surprise.

Even so, the standard precautions apply here. Unless you know and trust the sender of a communication, even if it's about something scary and important like the CoronaVirus, don't click on links or open attachments. You never know where it might take you or what type of malware might end up on your system. Better safe than sorry, and you can always get CoronaVirus information from official sources.

Old School Virus Called KBOT Is Hitting Networks



There was a day when worms were once common, terrifying threats on the internet. In the early days of the world wide web, there were a number of famous attacks that were considered highly advanced for their time.

Time and technology have moved on of course, and these days, modern malware is significantly more advanced.

Except for KBOT. KBOT is a blast from the past. Recently discovered by Kaspersky researchers, KBOT has been dubbed "the first living virus in recent years that we have spotted in the wild."

They describe the virus as follows:

"KBOT poses a serious threat because it is able to spread quickly in the system and on the local network by infecting executable files with no possibility of recovery. It significantly slows down the system through injects into system process, enables its handlers to control the compromised system through remote desktop sessions, steals personal data, and performs web injects for the purpose of stealing users' bank data."

As you can see from this brief description, this piece of malware might be old school, but it's a serious threat. By destroying the files it infects, it's not just a matter of getting rid of the infection. Invariably, you'll have to reinstall all the infected code on the PC.

In addition to being a highly destructive virus, it's also designed to steal vast quantities of data. Then it makes a priority of connecting to its command and control server once it establishes a hold so it can send back any data it's been coded to target.

If it's not already on your radar, it certainly deserves paying attention to. If you find yourself unfortunate enough to be on the receiving end of a KBOT infection, know that it will cause a tremendous amount of damage and bring your network to its knees before you get it under control.

Videos In Google Photos Accounts May Have Been Exposed

Security lapses can happen to any company, large or small. No one is immune. Not even Google. Recently, the company began sending out email notifications to some users explaining that a bug in their system caused their videos to be shared with other users.

Their email notification reads in part as follows:

"...some videos in Google Photos were incorrectly exported to unrelated users' archives. One or more videos in your Google Photos account was affected by this issue."

In particular, the issue is centered around the Google Takeout service, and occurred between November 21st, 2019 and November 25th, 2019. Any user who used Takeout during that period may have received videos that do not belong to them.

The company spotted and fixed the issue, so there's nothing to worry about going forward. However, if you used Google Takeout during the dates mentioned above, you'll want to do another import now to be sure you got everything.

This is a big deal for a few different reasons. Naturally, people who store their photos and videos on Google Photos expect them to remain private. Clearly in this case, that didn't happen. If you use the service to store videos that you don't want anyone to see, that could be a problem.

It also underscores the inherent risks involved in storing your data on the cloud. Yes, it's convenient. Yes, it saves space on your phone. Those are good things, but there's a trade off, and sometimes, that trade off is a painful one.

There are no perfect solutions here. Although such lapses in security are rare at Google, they do happen. They'll continue to happen. Each person using cloud-based storage solutions will have to come to find his or her own balance between privacy, security and convenience, which is no easy task.

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.

Dangerous New Trojan Can Infect Systems Through Wifi

If you're not already familiar with the Emotet trojan, it deserves a special spot on your radar. It's one of the most dangerous forms of malware in the world today.

Their success is thanks to the fact that its creators have worked hard and diligently to keep it upgraded by bolting on a variety of modules that enhance its capabilities in new, and sometimes terrifying ways.

Recently, researchers at BinaryDefense have spotted a particularly nasty new module that allows the trojan to infect other devices nearby. Called a "WiFi Spreader," it allows the trojan to hop wirelessly from one device to another.

Granted, this capability does not guarantee a 100 percent infection success rate, because the nearby device may have protection protocols in place. It does, however, provide a new attack vector the malware can utilize to spread itself farther than it otherwise might.

The implications of this are staggering. If Emotet makes its way onto your system and the strain you have has the WiFi Spreader module, it poses many risks. It poses risks to your own network, to the personal devices your employees carry that aren't connected to your network, and also to any other networks in close proximity to yours. Whether the networks are one floor up, or down, right next door, they are also at risk.

Also, consider the implications of an Emotet infection in a shared work environment. For example, WeWork office space, or a constellation of small companies that share one floor of an office and work in close proximity to one another. These kinds of arrangements are increasingly common and will absolutely complicate forensic investigations of malware infections.

If there's a silver lining here, it is the fact that according to Binary Defense, the WiFi spreader doesn't work on Windows XP SP2 or Windows XP SP3. That is because it utilizes functions that are incompatible with those builds. In any case, stay vigilant and be on the lookout for Emotet. It's one of the most dangerous forms of malware out there.

Malware And Viruses On Apple/Mac Systems Are On The Rise

For most of Apple's history, the company has been able to cast itself as a safer alternative to Windows-based computers.Hackers tended to focus the bulk of their efforts on Wintel boxes (Windows processors), rather than Apple machines. That has been changing in recent months. According to research conducted by Malwarebytes, over the past twelve months, there has been a significant upsurge in the number of attacks made against Macs.

To give you a sense of the scope and scale of the increase, in prior years, the average number of detections per Mac clocked in at 4.8, while the number of detections per Windows-based PC was 5.8. In 2019, the average number of detections per Windows-based PC remained unchanged, while the average number of detections per Mac spiked to 11, more than doubling in a single year.

The researchers note, however, that the types of threats Mac users face are very different from the threats

(Continued on page 4)

(Continued from page 3)

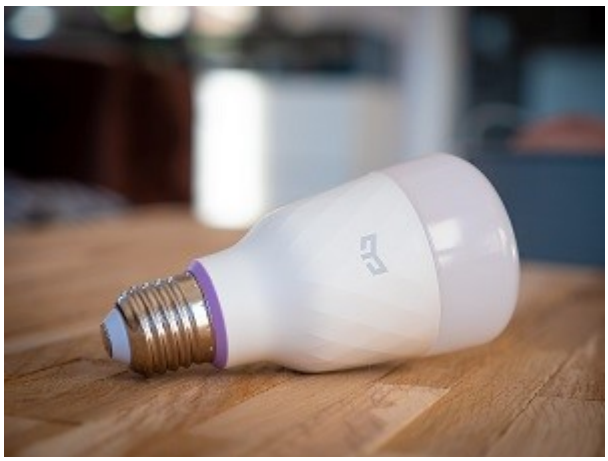
presented against Windows-based PCs, and are generally not dangerous. For instance, the most common infections Mac users suffer from are adware programs that display unwanted ads to infected recipients.

Naturally, there are cases of ransomware, keyloggers and banking trojans that target Macs. However, they are relatively less common than similar infections on Windows-based PCs.

If you're a Mac user, don't breathe a sigh of relief just yet though. The Malwarebytes research team concludes by warning us. They say although the attacks against Macs are currently less destructive than the attacks made against Windows-based PCs, that could change at any moment. There's nothing whatsoever keeping the hackers from swapping out adware in preference for a much more threatening piece of code.

All that to say, whatever type of computer you use day to day, it pays to keep your guard up. Nobody is truly safe.

Some Smart Light Bulbs Are Vulnerable To Hackers



Hackers will take any and every opportunity presented to them, even if it means hacking smart light bulbs. Recently, security researchers at Check Point discovered a bug in the Philips Hue smart bulb that makes it vulnerable.

The bug is being tracked as CVE-2020-6007 and scores an impressive 7.9 out of 10, making it the most serious security flaw in a light bulb we've ever seen.

It sounds funny. After all, who would want to hack a light bulb? But it's actually got serious implications. After all, the light bulb is just the beginning. Once hackers are 'in' the bulb, it gives them a beach head on the network that the bulb is attached to, and from there, they can jump to any other device they can see.

Fortunately, Philips has already published a fix for this, in the form of firmware version 1935144040. If you own one or more Philips Hue bulbs, you'll want to check the firmware version. If yours has not already been updated, take the time to do so.

This underscores the one glaring weakness of the Internet of Things. Very few of the smart products we're connecting to our networks have any security at all. The few devices that do boast some kind of security often have flaws like the one discovered here, which are severe enough to be considered crippling.

The net effect is to make any network that incorporates smart devices much less secure. After all, your network is only as secure as the weakest device on it, and smart devices have notoriously bad security.

That's changing, but it's changing at an incredibly slow rate. If you've got smart devices on your network, consider isolating them and minimizing the amount of contact they have with other devices on your network. That way, at least you can mitigate the impact until security improves.