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

Ribb"IT" Review

November is the month to remind us to be thankful for the many positive things happening in our life.

November 2019

Issue 11, 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

Ransomware is Everywhere

Ransomware keeps appearing in headlines; attacking hospitals, banks, school districts, state and local governments, law enforcement agencies, as well as businesses of all sizes.

Holy moly. This isn't good.

It's reaching an epidemic level. The number of people targeted by ransomware is staggering: in the U.S. alone, 4.1% of the population (13.1 million). Back in 2016, cybercriminals collected $209 million in just the first 3 months from ransomware!

What is ransomware?

So what is it? What is this software wreaking havoc all over the globe?

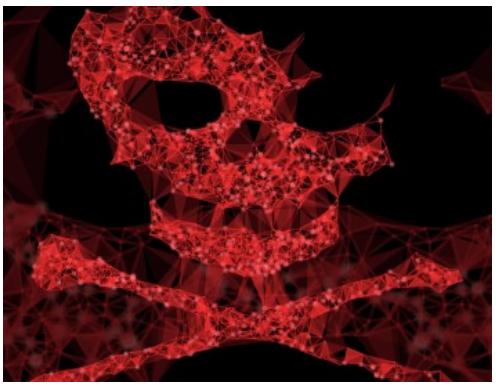
Ransomware is a form of malicious software (or malware) that, once it's taken over your computer, threatens you with great harm, usually by denying you access to your data. The attacker demands a ransom from the victim, then promises — though not always telling the truth of course — to restore access to the data upon payment. Users are then shown instructions for how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals typically in Bitcoin.

Ransomware has come to be viewed as an epidemic, expanding to more attacks from PCs to mobile devices and IoT. It is typically delivered through phishing emails, drive-by downloads or malvertising.

There are a few types of ransomware:

Crypto Ransomware

Locker/Lock-Screen Ransomware



Rogue Security Software: Fake AVs

Crypto Ransomware are variants that encrypt data on an infected host, and demand ransom in exchange for decrypting it. This is currently the most common ransomware type in the wild. Locker/Lock-Screen Ransomware are variants that deny access to the infected host and extort the victim for money in exchange for "releasing" it. Such variants are particularly popular among mobile ransomware. And finally, Rogue Security Software: Fake AVs are programs that "warn" the user against malware, which has already allegedly infected the host and can only be removed by purchasing the malicious "security software."

There are several different ways attackers choose the organizations they target with ransomware. Sometimes it's a matter of opportunity: for instance, attackers might target universities because they tend to have smaller security teams and a disparate user base that does a lot of file sharing, making it easier to penetrate their defenses.

On the other hand, some organizations are tempting targets because they seem more likely to pay a ransom quickly. For instance, government agencies or medical facilities often need immediate

access to their files. Law firms and other organizations with sensitive data may be willing to pay to keep news of a compromise quiet — and these organizations may be uniquely sensitive to leakware attacks.

But don't feel like you're safe if you don't fit these categories: some ransomware spreads automatically and indiscriminately across the internet.

Defensive steps to prevent ransomware infection:

There are a number of defensive steps you can take to prevent ransomware infection:

Keep your operating system patched and up-to-date to ensure you have fewer vulnerabilities to exploit.

Don't install software or give it administrative privileges unless you know exactly what it is and what it does.

Install antivirus software, which detects malicious programs like ransomware as they arrive, and whitelisting software, which prevents unauthorized applications from executing in the first place.

And, of course, back up your files, frequently and automatically! That won't stop a malware attack, but it can make the damage caused by one much less significant.

Several New Issues Being Seen With Apple's Latest iOS

Apple is the largest tech company in the world.

Their iPhones are in the hands of legions of loyal, faithful users all across the globe.

Unfortunately, the latest build of the iPhone's operating system, iOS 13.1.2, has been plagued with serious issues that render their vaunted smartphones virtually useless.

Even more problematic, the company seems to be their own worst enemy in recent weeks. For every bug they fix with their latest update, they've been introducing at least two more and they can't seem to get out of their own way.

In the wake of the company's most recent update, 13.1.2, users around the world are complaining that their phones will inexplicably drop calls after about a minute of being placed. In addition, although reports are not widespread, there are reports in Apple's support forum with more complaints. The users state that the new update is causing (or contributing to) rapid battery drain and even some cases of batteries overheating.

Screen Protectors Circumvent Fingerprint Security On Samsung Devices

Do you own a Samsung Galaxy S10? If so, one of the reasons you bought it may be because of its cutting-edge biometric technology. It utilizes ultrasounds to create a detailed 3D map of your fingerprint and thus, provides a greater level of security.

Earlier in the year, the company warned its customers against using tempered glass screen protectors with their phones.

This was due to the fact that those products tended to create a small gap of air when used on the phone that interfered with the creation of a good fingerprint map.

Now, it seems, a new problem has emerged. A couple in the UK accidentally discovered that if an inexpensive silicone case was put on the phone, it interfered with the operation of the fingerprint scanner and allowed literally any fingerprint to unlock the phone. The couple did some experimentation on this front and worked with Samsung customer support to reach their conclusion. Sure enough, when the silicone case was on the phone, the owner's husband and sister could unlock it with their fingerprints, even though neither of their fingerprints had been registered on the phone.

For their part, Samsung has reported that they are opening an investigation into the matter. For now, they warn consumers to only use Samsung approved accessories with their Galaxy S10 and S10+ phones. That's good advice, but here's the danger: If a hacker physically steals your phone, they may be able to unlock it and conduct financial transactions from it by doing nothing more than buying a cheap silicone case and slipping it on.

Needless to say, this is a potentially serious issue. If you own a Samsung Galaxy S10 or S10+ you can experiment with it for yourself, but be prepared to be dismayed by the res.

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.

RobbinHood Ransomware Another Reason To Back Up Your Systems

The creators of the dreaded 'Robbinhood' ransomware strain are putting their reputation to work for them. The hackers have recently modified their ransom note in a couple of important ways.

First and foremost, they stress that there's no public decryption tool currently available to recover files encrypted by RobbinHood and that they are monitoring the situation to make sure that the company impacted by the malware does not contact law enforcement. Any attempt to do so "will damage your files," the warning reads.

Those two recent additions are bad enough on their own, but the hackers took an additional step. They are now directing victims to a web search highlighting an incident that occurred in Greenville North Carolina and another that impacted servers in the city of Baltimore.

Robbinhood was used in both attacks, and while the ransoms demanded in both cases weren't excessive (less than $100,000 initially demanded), the aftershocks arising from those attacks wound up costing the city millions. In fact, according to CBS Baltimore, the city "put more than $18 million into the attack."

Clearly, the recent changes to the ransom note used by the attackers is aimed at convincing those impacted by their malware to pay up and keep quiet. How well that will ultimately work remains to be seen, but at this point, the hackers are correct. There is no public decryption tool.

What they don't mention, of course, is the fact paying the ransom isn't the only way to recover encrypted files. If your company is in the habit of making good, complete backups at regular intervals, then a ransomware attack doesn't have to be devastating. With a proper, timely response, it could be little more than an inconvenience. Naturally, the hackers don't want to draw attention to this, but it is something you and your IT staff should keep very much in mind.

Malicious Apps Continue Getting Past Google On Play Store

Say what you want about Google, but the company has a solid track record of doing all they can to keep the Google Play Store relatively free of malicious apps. By most accounts, they have been wildly successful at that.

Unfortunately, given the sheer number of apps available on the Play Store, statistics invariably catch up with them.

A small number of poisoned apps, trojans and the like still find their way onto the store. They blend in with legitimate apps until some enterprising researcher discovers them, at which point, Google promptly brings the hammer down.

The question is, why does it keep happening? It's a fair question, but it's important to put it in proper context. After all, more than 99 percent of the apps on the Play Store right now are perfectly fine, so Google's

(Continued on page 4)

(Continued from page 3)

robust system of checks and strict guidelines are certainly working.

The problem is, nobody ever reports on the fact that the majority of the time, the system works as advertised. We only tend to hear about the instances where something goes off the rails and an unsavory developer temporarily pulls the wool over Google's eyes.

At the end of the day, the answer is simply this: No system, no matter how robust, is perfect. Google generally does a good job of policing its Play Store, which is why it's seen as one of the safe havens on the internet.

Having said that, there's always room for improvement. To the company's credit, Google is in the habit of regularly and methodically improving its own processes. Even so, a certain amount of due diligence is required on the part of the user, even when downloading apps from a supposedly safe source. We can't fault Google for the actions of careless users. We can't blame them for the actions of determined, unsavory developers who occasionally find ways to temporarily circumvent the company's safeguards.

Support For Microsoft Office 2010 Ending Soon Upgrade Recommended

Are you still using Microsoft Office 2010?

If so, Microsoft recently issued a reminder you're not going to like hearing.

Extended Support for Office 2010 expires on October 13th, 2020, so time is running out to upgrade. The company's official recommendation is to upgrade to either Office 365 ProPlus, or Office 2019.

In addition to that, "We also recommend business and enterprise customers use the deployment benefits provided by Microsoft and Microsoft Certified Partners, including Microsoft FastTrack for cloud migrations and Software Assurance Planning Services for on-premises upgrades." This, according to the Office 2010 End of Support Roadmap, published by Microsoft.

Elsewhere on Microsoft's site, the company seems to be pushing hard for Enterprise users to upgrade to Office 365 ProPlus. In particular, they added the following information:

"Upgrade to Office 365 ProPlus, a product built for today's challenges and literally getting better all the time, as we continue innovating across--and investing in--the experience. Consider just a few benefits: AI and machine learning to advance creativity and innovation, real time collaboration across apps, and Microsoft Teams as the hub for teamwork."

All of that is well and good, and certainly true. However, for some Enterprise users, office 2019 might simply be the better fit, even if the company isn't pushing it as hard. In any case, the takeaway is simply this: Support is ending for Office 2010. If you're still using it, you need to be making migration plans now and begin using one of the two aforementioned products before the support period ends. You'll find detailed instructions on how to migrate on the company's website if you don't already have a clear understanding of the process.

In a related vein, note that the Windows 10 Creators Update (version 1703) has now reached end of service and will no longer receive any quality or security updates.