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

Ribb"IT" Review

"Autumn shows us how beautiful it is to let things go."

October 2019

Issue 10, Volume 9

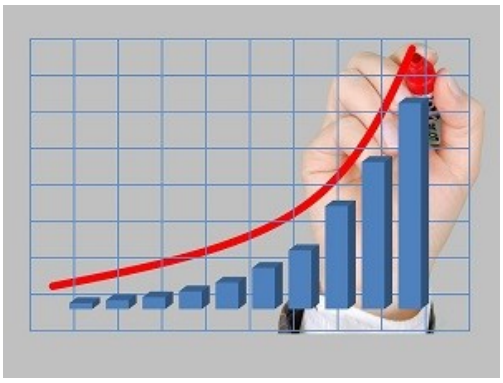
This monthly publication provided courtesy of Alex Bleam, Owner of Frogworks

We are excited and proud to announce that Frogworks has been recognized as one of the world's best MSPs by Channel

Channel Futures MSP 501 2018 WINNER

THE ULTIMATE GUIDE TO THE WORLD'S BEST MSPs

Report Shows 118 Percent Increase In Ransomware Attacks In 2019



Ransomware roared onto the global stage in 2017. Companies and government agencies around the world felt the impact with widespread campaigns like NotPetya and WannaCry.

By 2018, the number of ransomware attacks had begun to fall off while hackers found new tools to attack with, shifting toward cryptojacking, credential theft, and trojan malware.

Granted, ransomware attacks didn't fade completely from the picture in 2018, but they were overshadowed by the emergence of new attack vectors. Unfortunately, according to data collected by McAfee Labs, and published in their August 2019 Threat Report, Ransomware is back with a vengeance.

Christopher Beek, a lead scientist at McAfee had this to say about the report:

"After a periodic decrease in new families and developments at the end of 2018, the first quarter of 2019 was game on again for ransomware, with code innovations and a new, much more targeted approach."

The dramatic increase in ransomware attacks is being driven primarily by three families of ransomware: Ryuk, GrandCrab, and Dharma.

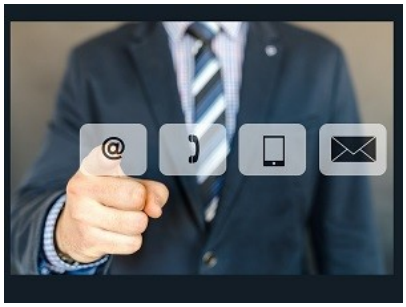
Ryuk is a scary bit of code that has been used to lock down entire large corporations and government agencies. It was originally credited to North Korea, but subsequent research points to the malware as being the work of a highly sophisticated cybercrime syndicate, rather than the product of a nation-state.

GrandCrab is a relatively new arrival on the ransomware scene, first emerging in 2018. Often described as one of the most aggressive families of ransomware, the original authors of the code have leased it out to other hackers around the world in exchange for a cut of the profits.

Dharma is the oldest family of the big three, first emerging on the scene in 2016. Originally, it was an offshoot of another, even older ransomware family known as Crysis. However, since branching off, it has become a potent threat in its own right, and the hackers who control the code regularly release new updates and continue to enhance its capabilities.

All that to say, it's too soon to breathe a sigh of relief where ransomware is concerned. It's back in 2019, and it's back with a vengeance.

Companies Are Losing Billions To Business Email Compromises



The FBI's statistics on BEC (Business Email Compromise) are alarming to say the least. Over the last twelve months, the law enforcement agency has witnessed a 100 percent increase in the identified global exposed business losses attributable to BEC. Between June 2016 and July 2019, there were a total of 166,349 BEC incidents reported to the FBI, which led to total losses in excess of twenty-six billion dollars.

Worse, the cyber criminals engaging in these types of attacks don't limit themselves to Fortune 500 companies. They're just as likely to target small to medium sized businesses as they are to target major international firms.

Typically, a BEC attack works something like this:

A fraudster will pose as either a high-ranking company official or a trusted business partner and begin email communication with a mid-level employee at your firm. Over the course of that conversation, a request will be made to the employee to transfer funds to what the employee believes to be an account belonging to a longstanding business partner.

Thinking that they're doing the bidding of their CEO or of a trusted business partner, these transfers are often made without a second thought. Of course, by the time it is discovered that the person the employee was communicating with was a fraud, the money is long gone and virtually impossible to recover. A BEC attack can take other forms too, however.

In fact, according to the FBI's Internet Crime Complaint Center:

"One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information or Wage and Tax Statement (W-2) forms. Payroll diversion schemes that include an intrusion event have been reported to the IC3 for several years. Only recently, however, have these schemes been directly connected to BEC actors through IC3 complaints."

The bottom line is that this type of issue is getting worse and increasingly common. Be sure your employees are aware and mindful of who they're releasing funds to.

Browsers Are Waging War On Third Party Cookies

Do you use Mozilla's Firefox browser? If so, then you should know that their most recent release, Firefox 69 has a new feature designed to help prevent companies from tracking you. If you update to Firefox 69, the new feature will be automatically enabled as part of the browser's Enhanced Tracking Protection feature. If you want to be tracked, you'll have to go into the browser's settings and choose to enable it.

The move is almost universally seen as a positive, and it's prompting other major browsers to take similar action. Google is a bit behind Mozilla in that regard, but in the company's most recent Chrome Canary build, Google has added a new experimental flag called "Enable Improved Cookie Controls UI."

If you choose to enable the flag, you'll see a new "Block Third-Party Cookies" option on the "Cookies and Site Data" screen. Once enabled, Chrome will automatically block all third-party tracking cookies sent by any site you visit.

If you're surfing in Incognito Mode, you'll see a new button on the Omnibar that will display a new dialogue informing you that third-party cookie blocking is on. It will give you a running count of the number of sites Chrome is blocking from. Also present on the dialogue box will be the option to turn the feature off for the site you're presently visiting, giving you one touch control and convenience.

No matter what browser mode you're in, you can always access the list of cookies being blocked by clicking on the shield icon next to the URL and clicking "Cookies" on the dialogue box that appears.

Eventually, this feature is likely to make its way into all versions of Chrome. For now, if you want to give the feature a test drive, you'll need to download and install Chrome Canary. It's a good idea, and a long time coming. Kudos to both Mozilla and Google.

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.

Hackers Are Using Resumes To Deliver Malicious Software

Hackers have used poisoned documents to deliver malware payloads for years. Recently though, researchers at the security company Cofense have spotted a new twist to the ploy, aimed squarely at HR departments. The recently detected campaign uses fake resume attachments to deliver Quasar Remote Administration Tool. It is affectionately known as RAT to any unsuspecting Windows user who can be tricked into jumping through a few hoops.

Here's how it works:

An email containing a document that appears to be a resume is sent to someone in a given company. The document is password protected, but the password is politely included in the body of the email, and is usually something simple like '123.' If the user enters the password, a popup box will appear, asking the user if he/she wants to enable macros.

Up to this point, the attack is fairly standard, but here's where it gets interesting:

If the macros are allowed to run, they'll display a series of images and a message announcing that content is loading. What it's actually doing is throwing out garbage code that's designed to crash analysis and detection tools while RAT is installed quietly in the background.

At that point, the system is compromised. RAT's capabilities give the hackers the ability to open remote desktop connections, log keystrokes and steal passwords, record any webcams in use, download files, and capture screenshots of the infected machine.

Worst of all, the first part of the infection process knocks out most detection programs. So, the hackers generally have a large window of time to take advantage of the newly created beach head. That can cause all manner of havoc in your network or simply choose to quietly siphon proprietary data from your systems.

Be on the alert and make sure your HR staff is aware. This is a nasty campaign and it's just hitting stride.

Watch Out For Old Hacking Technique Offering Free Downloads

An old hacking technique is getting new attention from hackers around the world, and it underscores the fact that people must exercise extreme caution when it comes to deciding who to trust and where to download files from.

Hackers have long been in the business of spoofing legitimate sites; making exact replicas of popular websites offering a variety of free downloads.

Of course, instead of getting genuinely useful code, you find yourself on the poisoned domain. Rather than the legitimate site, what you download will be malware of one type or another.

The most recently discovered instance of this involves the Smart Game Booster site. It's a legitimate piece of code that helps to improve the performance of the games you play, and it has become popular enough that it's caught the attention of at least one hacking group. That group cloned the site and pretends to offer the same product.

In this case though, the malware the hackers deploy is one of the more insidious we've seen. Unlike many malware attacks which latch onto a system with a persistent presence, this one runs only once and then deletes itself. Even more alarming is that it leaves no trace that it was ever there.

When it runs, it scans the infected device for passwords, your browser history, any cryptocurrency wallets you may have, and a wide range of other critical files. It collects these and sends all the data to its command and control server, and then self-destructs.

With no outward sign, many users will be completely unaware that there's a problem until they start seeing suspicious charges on credit cards, noticing funds being removed from bank accounts and the like. By then of course, it's far too late.

The bottom line here is simple: Be mindful about where you download files from. Check your URLs, and unless you can avoid it, never stray far from the big, well-respected sites like the Apple Store, Microsoft Store, or Google Play Store. It's just not worth the risk.

Malware Now Hiding Inside Fake Copies Of Online Books

Kaspersky Lab has recently issued a warning that should alarm and dismay students around the world. Based on the findings of some of the company's researchers, they've discovered a new surge in malware masquerading as legitimate digital textbooks. Given the staggering price of physical textbooks, many students have changed to acquiring digital copies of the books they need.

While the price difference is considerable between the digital and physical copies, penny-pinching students often shop for the best deals possible on the digital copies of the books they're buying. Unfortunately, a disturbing percentage of bargain-priced texts are poisoned and used to infect the devices of the students downloading them with a variety of malicious payloads.

Based on Kaspersky's research, there were in excess of 365,000 attacks last year that relied on malicious documents with educational-related filenames. Of those, 233,000 of the cases involved poisoned documents downloaded by more than 74,000 people and blocked by the company's software.

According to a Kaspersky spokesperson, about a third of those files were malware disguised as textbooks, and more than 30,000 users attempted to open them.

The company was able to block an impressive percentage of those types of attacks. However, based on their own numbers, that still means that more than 132,000 infection attempts were successful. While the attacks were made using a staggering array of malware, the most commonly employed were identified as:

- MediaGet
- Agent.gen & Win32.Agent.ifdx
- The Stalk worm

Of the 'Big Three,' the MediaGet downloader is the least harmful, designed to simply download an unnecessary torrent client. Unfortunately, the other two downloaders, WinLNK.Agent.gen and Win32.Agent.ifdx are capable of dropping all manner of nasty malware onto an infected device.

Stalk is different from these others, being classified as a worm. Its main goal in life is to spread itself to as many machines as it can and will merrily mail and text itself to the entire contacts list on any infected machine.

The bottom line from Kaspersky is simply this: Bargain priced digital texts very often have a high hidden cost. It pays to be wary.