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

Ribb"IT" Review

"What appears to be the end of the road may simply be a bend in the road."

-Robert H. Schuller

May 2019

Issue 4, 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

Amazon Echo is Always Listening

Amazon has admitted to employing thousands of people worldwide who are tasked with listening in on private conversations through its Echo line of speakers using the Alexa digital assistant, and the workers are revealing what they've heard.

What are the details?

Bloomberg reported that Amazon has teams of folks around the world tasked with transcribing recordings pulled from Echo customers' homes and offices. In one shift, the analysts will listen in on as many as 1,000 clips, which the firm says is minuscule considering the tens of millions of people who own the systems.

A company spokesman explained, "We only annotate an extremely small sample of Alexa voice recordings in order [to] improve the customer experience. For example, this information helps us train our speech recognition and natural language understanding system, so Alexa can better understand your requests, and ensure the service works well for everyone."

But the revelation confirms the fears of those who have warned against trading privacy for convenience. Two Amazon workers speaking on the condition of anonymity told Bloomberg that users frequently ask Alexa questions like, "Do you work for the NSA?" or "Is someone else listening to us?"

What else have they heard?

The Daily Mail noted that "concerns have been raised by some in the past that smart speaker systems could be used to [listen in on] user conversations, often with the aim of targeting users with advertising." But the analysts are hearing much more than just costumers' interests.

According to the Mail, Amazon workers have admitted to listening in on people singing in the shower, discussing bank account details, and conducting other intimate exchanges. Staffers have also raised the alarm when overhearing distressing situations like a child calling out for help, and instances where a sexual assault might have occurred.

It's only a matter of time, experts say, before law enforcement is granted access to listen in on what Alexa hears, too.

Security consultant Robert Graham told Gizmodo a few years ago, "It's likely that laws will be passed that will allow the police to remotely activate these devices and eavesdrop on suspects, pretty much as described in the book '1984.' "

(This article was obtained with permission by TheBlaze)

Windows Defender Security Comes To Mac Devices

If you're a Mac user and looking for next-level antivirus protection, we've got some potentially good news.

Microsoft recently announced that their enterprise security platform, (Windows Defender Advanced Threat Protection) is now available for macOS.

To reflect the product's move away from offering protection exclusively to Windows-based systems, the company tweaked the name of the product. It is now called simply "Microsoft Defender ATP."

The newly minted version of the software is currently available for Macs in limited preview form, and represents the latest in an ongoing expansion effort. Last month, the company rolled out a version that extended its impressive protection to both Windows 7 and Windows 8.1. Future plans will include a further expansion to also provide protection to Linux-based machines.

At this point, Admins can install Microsoft Defender ATP on the following macOS versions:

- Mojave
- High Sierra
- Sierra

Individual users will have the option to configure advanced settings in the software unless their admins specifically disable that functionality. The code also includes an auto-update feature that can be toggled by an Admin.

If you're an admin working in a Mac environment, you might not see a particular need for the new software. However, Microsoft pointed out in the bulletin they released with the announcement that Defender can detect KeRanger, which was the first ransomware strain to target the macOS.

In any case, more security options are generally better than fewer, and Microsoft has long been a favorite target of the hacking world. Love them or hate them, they do know a thing or two about security, especially at the enterprise level. Most insiders hail this move as a good one.

All that to say, if augmenting system security figures highly in your near term plans, and it probably does, this could be an excellent addition to your arsenal.

Phishing Attack Targets Amex And Netflix Users

If you do business with either American Express (AMEX) or Netflix, be on the alert. Windows Defender Security Intel has recently reported the detection of two major new phishing-style campaigns aimed at the customers of both businesses.

Recipients have been receiving emails that appear identical to official Netflix and American Express communications.

In both cases, the ultimate goal is to convince customers to hand over their credit or debit card information. Microsoft has sent a couple of different tweets out about the issue. One of them assures customers that "Machine learning and detonation-based protections in Office 365 ATP protect customers against both campaigns."

And another warned that "The Netflix campaign lures recipients into giving away credit card and SSN info using a 'Your account is on hold' email and a well-crafted payment form attached to the email."

The unfortunate truth is that emails like the ones currently in play are extremely easy to craft and very compelling. The hackers simply play on the fears of the customer, making it sound as though if they don't take

(Continued from page 2)

immediate action they'll lose access to a valued service they've come to rely on.

There's essentially no cost to the hacker for pushing out hundreds, or even thousands of emails like the ones currently being used. For each victim that falls prey to the tactic, the costs can be enormous.

As ever, the first best line of defense is education and awareness. In addition to that, if there's ever any question at all about the status of your account, the best thing you can do is to address the issue via another channel.

In other words, don't simply reply to the email you received. Open a new tab, look up the company's customer support number and call to verify. Doing so will tell you in short order whether the email you received was legitimate, or someone trying to separate you from your hard-earned money.

Toyota Customers Possibly Affected By Data Breach

In recent months, Japan is a nation under cyber-siege, with several high-profile attacks having been made against the country. The most recent attack targeted Toyota. If you own a Toyota or Lexus, it's possible that at least some of the information you gave to the company has been compromised.

Although an investigation into the matter is ongoing, Toyota wasted no time letting its massive customer base know.

Their official statement reads in part, as follows:

"We have not confirmed the fact that customer information has been leaked at this time, but we will continue to conduct detailed surveys, placing top priority on customer safety and security."

Later in the statement the company stressed that if customer information was, in fact compromised, that information did not contain credit card or other payment numbers.

Early indications point to a well-organized hacking group calling themselves the OceanLotus Group. Although even this cannot be confirmed at this point.

The details surrounding the attack are murky at this point. What we do know with certainty is that on March 21st, the company detected an unauthorized intrusion into its corporate networks across a staggering 8 company divisions, marking it as an extremely well organized and sophisticated attack.

Considering the other attacks made against Japanese companies and government agencies, it seems that for reasons that are not yet clear, one or more big hacker organizations filled with top-tier talent has decided to put the nation under the virtual gun.

Only time will tell exactly who's behind the attacks and what their ultimate purpose might be. For now, the key thing to know is that if you own a Toyota or Lexus, it's possible that at least some of your personally identifiable information was compromised. Be on the lookout for additional information from Toyota as it becomes available.

Apple Developers Will Make Apps Usable On All Devices

Microsoft is slowly inching closer to a mainstream release of a new version of its Edge Browser for Windows 10, this one based around Chromium technology.

Recently, Microsoft released Canary, a developer build for the new browser.

Any member of the Windows Insiders group can get access to the early build if they want a sneak peek at what's to come.

The company has promised beta builds in the months ahead, along with builds that are Windows 7.8.1 and Mac OS compatible.

If you decide to take a look at the current state of the code, it's important to remember that the new Edge should still be considered in pre-Alpha state and is focused on the basics for the time being. That means there's not a lot in terms of functionality just yet. In fact, at present, the new Edge looks more or less like the old Edge, minus language support, PDF support, tab sweeps and smooth scrolling.

Consider it to be a scaled back version of the current Chrome browser with built in MSN news feeds. As such, these early builds may be of interest to enthusiasts, developers and early adopters who want to start getting a handle on the state of things to come. Honestly though, a casual user won't find much of interest here.

While Microsoft has had a poor track record where its browsers are concerned, the hope is that their new offering designed with Chromium at the core, will be more of a success. They hope to leverage the vast strengths of industry leader Google. That, however, remains to be seen. Even so, there is undeniable value to developers and a few other select groups to get in on the fun now so they can develop a better understanding of the shape and direction of the new Edge as its contours begin to emerge.

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.

Malware In Documents Is Latest Hacker Trend

There is a new Threat Spotlight released by Barracuda Networks.

One of the biggest trends in 2019 (where threats against businesses of all sizes are concerned) now takes the form of poisoned documents attached to emails.

The company analyzed more than 300,000 email samples collected over the past twelve months.

They discovered that the frequency of document-based malware attacks increased markedly during the first quarter of 2019, with nearly sixty percent of poisoned files taking the form of documents.

As Jonathan Tanner of Barracuda Networks put it:

"For the past couple of years, script files were a very popular attack method. The percentage of these sort of files declined drastically, however, and was a significant source of the increase of documents as an infection method...

Documents are a natural evolution from script files, since the languages used are also the ones used for documents - namely VBScript and JavaScript. The same attacks could be converted to the document-based ones with only slight modifications. The script authors had already become very adept at obfuscation techniques, so these could contribute greatly to document-based malware where scripting is already more common and thus deeper inspection of the script itself is required."

The good news is that most antivirus software is quite good at detecting malicious files. Of course, the weakest link in the equation isn't detection software, it's users. In light of the evolving threat, education is more important than ever. Although to date, the majority of employees have been stubbornly resistant to educational measures designed to reduce the rate at which employees will click on and open documents received from un-trusted or even unknown sources.

As a business owner, that will likely be one of your great challenges in the year ahead. The more wary you can make your employees about opening files from people they don't know, the safer your network is bound to be.

Millions Of Facebook Usernames And Passwords Stored By Accident

Are you a Facebook user? If you are, it may be time to change your password. KrebsOnSecurity recently reported that it found hundreds of millions of Facebook user account names and passwords stored in plain text and searchable by more than twenty-thousand Facebook employees. At present, there is no official count, but Facebook says the total number of records was between 200,000 and 600,000.

That's a big number, which makes this a serious incident, but in truth, it represents only a fraction of the company's massive user base.

Although there's no indication that any Facebook employee abused their access to the information, the fact remains that it was accessed regularly. The investigation to this point has revealed that no less than 2,000 engineers and developers made more than nine million internal queries to the file.

Facebook software engineer Scott Renfro, interviewed by KrebsOnSecurity, had this to say about the issue:

"We've not found any cases so far in our investigations where someone was looking intentionally for passwords, nor have we found signs of misuse of this data.

In this situation, what we've found is these passwords were inadvertently logged but that there was no actual risk that's come from this. We want to make sure we're reserving those steps and only force a password change in cases where there's definitely been signs of abuse."

This is just the latest in an ongoing series of security-related issues Facebook has found itself in the midst of. While the company is wrestling with making changes to prevent such incidents in the future, that's small comfort to the millions of users that have been adversely impacted over the last year.

According to the official company statement, unless you receive a notification from them, there's nothing you need to do and no need to change your password. But given the importance of data security, if you'd rather be safe than sorry, it certainly couldn't hurt.