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

Ribb"IT" Review

"Freedom lies in being bold."

-Robert Frost

July 2019

Issue 7, 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

Your Company's Data was Hacked – Are You Legally Responsible?

So, who should be held responsible when a company's data system gets breached? Historically, the CIO, the CISO, or both have shouldered the lion's share of data breach responsibility; well over half of security decision-makers expect to lose their jobs if a hack happens at their organizations. However, breaches don't happen in vacuums, and CIOs and CISOs don't operate in them, either. Many CIOs report directly to the CEO, and some security experts feel that CISOs should be elevated to the same reporting level.

Whatever an organization's reporting structure, the bottom line is the same: the responsibility for everything that happens within the organization, positive or negative, ultimately falls on the CEO and the board of directors. This includes data breach responsibility. This has been reflected in the numerous CEO firings (or resignations) that have followed bad breaches over the past few years, including those at Target, Sony Pictures, and the Democratic National Committee.

Apparently, Yahoo didn't get the memo about this a couple of years ago. After years of poor cybersecurity practices caught up with them, resulting in multiple breaches affecting over a billion user accounts, putting its acquisition by Verizon into question, and making the Yahoo brand name synonymous with the phrase "data breach," the company decided to fire its General Counsel, Ron Bell. Shockingly, CEO Marissa Mayer remained in place, albeit with a pay cut (she then went on to leave Yahoo after the Verizon acquisition, however, but it was of her own choosing).

In Yahoo's case, the CISO and the rest of the security staff couldn't be fired. Fearing that a major security incident would eventually happen, they'd already run for the hills. The New York Times reported that former CISO Alex Stamos and his team had spent years warning Mayer of potential security issues, but Mayer insisted on putting "the user experience" ahead of cybersecurity and even cut the team's budget.

Preventing Breaches Is Everyone's Responsibility

Cybersecurity isn't just an IT issue. It impacts every individual and department in an organization — from the board of directors all the way down to minimum-wage clerical and retail employees. The overwhelming majority of data breaches originate inside an organization, either because a

negligent or untrained employee makes a mistake or a malicious insider decides to strike back against the company. No cybersecurity policy is complete unless it addresses the human factor behind data breaches by promoting a culture of cybersecurity awareness. This culture must start at the top of the organization; if the board, the CEO, and the rest of the C-suite do not take security seriously, front-line employees certainly won't.

Yahoo's firing of Ron Bell certainly shook up the legal community and caused much debate over where data breach responsibility ultimately lies. While this may have served to light a fire under organizations with questionable cybersecurity practices, the focus should not have been on whose heads would roll if a breach happened; it should have been on implementing proactive cybersecurity and compliance measures to prevent hacks from happening in the first place.

As for Yahoo, they settled in September a worldwide class-action lawsuit that alleged security issues dating back as far as 2003. Yahoo's attorney and lead plaintiffs' counsel told the U.S. District Judge in federal court that both sides had reached an "agreement in principle" — $47 million to be exact.

New Security Vulnerabilities Found In Intel Processors

Remember the Spectre and Meltdown CPU vulnerabilities discovered early last year? Well, hold onto your hat, because they've got company.

Recently, researchers discovered a new class of side-channel vulnerabilities in Intel processors that impact every modern chipset the company makes, including those used in Apple devices.

The new vulnerabilities exploit weaknesses in something called 'speculative execution' which is a core design feature of modern processors. This feature allows them to speculatively execute instructions based on conditions the system has 'learned' are likely to be true. If those assumptions are proved to be valid, then the execution continues. If not, it is discarded. The net effect of this design is to increase overall system performance speed, but it also opens up the door for additional risk.

The researchers had this to say about their latest discoveries:

"The new vulnerabilities can be used by motivated hackers to lead privileged information data from an area of the memory that hardware safeguards deem off-limits. It can be weaponized in highly targeted attacks that would normally require system-wide privileges or deep subversion of the operating system."

Collectively, these new vulnerabilities are being referred to as 'MDS speculative execution' flaws, and have been identified as follows:

- CVE-2019-11091 - Microarchitectural Data Sampling Uncacheable Memory (MDSUM), part of the RIDL class of attacks.

- CVE-2018-12127 - Microarchitectural Load Port Data Sampling (MLPDS), also part of the RIDL class of attacks.

- CVE-2018-12130 - Microarchitectural Fill Buffer Data Sampling (MFBDS), also called 'Zombieload' or RIDL (Rogue In-Flight Data Load).

- CVE-2018-12126 - Microarchitectural Store Buffer Data Sampling (MSBDS), also known as a Fallout

(Continued on page 3)

(Continued from page 2)

Of these, the ZombieLoad attacks seem to be the most worrisome of the lot. They impact the largest number of chips, encompassing everything Intel has produced from 2011 onwards, but all of these are considered serious security flaws. Worse, there are no fixes yet, and no word yet on when a fix might be forthcoming.

Malware Focused On Mobile Banking Greatly Increased In 2019

Researchers at Kaspersky Lab have been tracking a disturbing new trend.

In the first quarter of 2019, the company has noted a massive 58 percent increase in modifications of various banking Trojan families that have been used in attacks against more than a quarter of a million users around the world.

This increase is troubling in that it paints a picture of hackers taking much more interest in and developing tools that are specifically designed to target users who access banking services from mobile devices, which is a target rich environment indeed.

The company had this to say about their findings:

"As is customary, first place in the Top 20 for Q1 went to the DangerousObject.Multi.Generic verdict (54.26 percent) which we use for malware detected using cloud technologies.

Cloud technologies are deployed when the antivirus databases lack data for detecting a piece of malware, but the company's cloud already contains information about the object. This is basically how the latest malicious programs are detected.

The rapid rise of mobile financial malware is a troubling sign, especially since we see how criminals are perfecting their distribution mechanisms. For example, a recent tendency is to hide the banking Trojan in a dropper - the shell that is supposed to fly to the device under the security radar, releasing the malicious part only upon arrival."

The bottom line is that if you use your mobile device to access banking services of any kind, be aware that you are increasingly seen as a target. In fact, given the latest findings, you're rapidly becoming the preferred target of a growing body of hackers.

As ever, your best defense is vigilance. Don't install apps from untrustworthy sources. Before adding any new app to your phone, do some due diligence to minimize your risk of inadvertently installing something not just unwanted, but incredibly dangerous.

Instagram User Information May Have Been Available To Hackers

Do you have an Instagram account?

If so, be advised that David Stier (a business consultant and researcher for CNET) has recently discovered a flaw in Instagram's website that exposed thousands of users' email addresses and phone numbers for a period of more than a month.

Mr. Stier provided screen shots and other details to Instagram demonstrating that when the source code for some users' profiles were displayed in a web browser, supposedly confidential information was plainly visible.

The exposed information ran the gamut and included the contact and personal information of individual adult users, some businesses, and an unknown number of minors. The company responded promptly and issued a patch that corrected the problem not long after they were made aware, but at this point, the damage may have already been done.

From a user's perspective, the best thing you can do is to change your Instagram password immediately and be on the alert that if a hacker made a copy of the information, you may be on the receiving end of phishing emails in a bid to collect even more information from you in the months ahead.

At this point, it is unknown whether any group or individual other than Mr. Stier found and made use of the exposed information. Instagram faced a similar issue several months ago, in which the company improperly protected a database containing the contact information of millions of their users, including several influencers and celebrities. This database was initially uploaded and shared by a Mumbai-based marketing firm called Chtrbox, and the information it contained is unquestionably in the wild at this point.

Instagram's parent company, Facebook, issued a brief statement to the effect that they were working with Chtrbox to understand exactly how they came to posses the data and how it became publicly available. At this time, however, no additional information is available.

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 Using WhatsApp To Install Malware On Phones

If you're among the masses of people using WhatsApp, for either Android or iOS, be advised that the Israeli hacking consortium known as the NSO Group may have installed spyware on the device you use WhatsApp on.

A massive security flaw identified as CVE-2019-3568 has been discovered and weaponized by the NSO Group.

This allows them to install spyware and steal a variety of data from impacted devices. Worse, the group is installing their Pegasus spyware, which is among the most advanced on the planet. It's very good at hiding itself, deleting incoming calls, and other log information in order to remain hidden.

The good news is that Facebook, which owns WhatsApp, has patched the flaw with an update. As long as you're using the latest version, you're protected. Unfortunately, not everyone keeps their apps up to date. Prior to the patch being released, all 1.5 billion of the app's users were considered vulnerable.

According to the official company statement:

"The issue affects WhatsApp for Android prior to v2.19.134, WhatsApp Business for Android prior to v2.19.44, WhatsApp for iOS prior to v2.19.51, WhatsApp Business for iOS prior to v2.19.51, WhatsApp for Windows Phone prior to v2.18.348, and WhatsApp for Tizen prior to 2.18.15."

Although millions of users have already updated their software, the sad reality is that for most people, keeping apps up to date generally ranks quite low on their list of priorities. That means there are still untold millions of users who are vulnerable.

If you use the app or if you know anyone who does, the best thing you can do is to update to the latest version right away and have your phone thoroughly scanned to be sure you don't have the Pegasus Spyware already embedded in your system.

Unexpected Support Updates For Older Systems Released By Microsoft

Users of Windows XP, Windows 2003, Windows 7 and Server 2008 got an unexpected benefit from Microsoft recently.

All of the OS's mentioned above have reached the end of their support lives and the company hasn't been issuing new security updates for them. However, they made a rare exception in the case of patching CVE-2019-0708.

CVE-2019-0708 is a critical security flaw that allows hackers to exploit the Remote Desktop Service and gain access to a target system without any authentication.

Windows 8 and later versions are unaffected by this flaw, but there are millions of vulnerable users still on the older operating systems we named above who are vulnerable. Microsoft threw them a lifeline releasing the patch that addressed this issue, along with 79 other security flaws.

Last year, the malware strain known as Wannacry swept across the globe, infecting hundreds of thousands of systems, most of which were running older OS's. Fearing that something similar could happen this year, the company took the extraordinary step of issuing an unexpected security patch.

While the smart money says that you should already be well into making plans to migrate away from these older operating systems with little to no support, that may not be possible for everyone. At the very least then, be sure you grab the latest security patch from Microsoft, which will undoubtedly buy you at least a bit more time.

Honestly though, at this point, the only safe move is to migrate to a more modern OS with all possible speed, even if it means some short-term discomfort. Wannacry devastated thousands of businesses of all shapes and sizes. Microsoft isn't going to continue making heroic efforts to save a user base unwilling to migrate forever.