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

Ribb"IT" Review

"There is a powerful driving force inside every human being that, once unleashed, can make any vision, dream or desire a reality."

-Anthony Robbins

July 2020

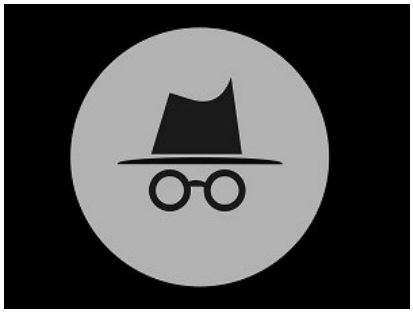
Issue 5 Volume 10

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

Lawsuit Claims Google Private Browsing Isn't Really Private



Google is in hot water with a complaint filed to the District Court of Northern California.

The complaint alleges that the tech giant tracks users' browsing data and a variety of other identifying information via Google Ad Manager, Google Analytics, and a variety of other applications. It tracks data even when users are accessing the web via Private Mode (Incognito).

According to the complaint filed, when an internet user visits a page or opens an app that makes use of Google's services (which covers some 70 percent of all online publishers), that data is tracked. In addition, it is collected and sent to the company's servers in California. In almost all cases, it is done without the user's knowledge or consent.

The complaint reads in part, as follows:

"*Google takes the data regardless of whether the user actually clicks on a Google-supported advertisement - or even knows of its existence. This means that billions of times a day, Google causes computers around the world to report the real-time internet communications of hundreds of millions of people to Google.*

Google's practices infringe upon users' privacy; intentionally deceive consumers; give Google and its employees power to learn intimate details about individuals' lives, interests and internet usage' and make Google 'one stop shopping' for any government, private, or criminal actor who wants to undermine individuals' privacy, security, or freedom."

The class action suit seeks to collect $5,000 in damages per user (or three times actual damages, whichever is greater). The money would be for anyone who accessed a page containing any service that relies on Google's services, and who did so using a non-Android device in private browsing mode.

It will no doubt be a long fight, but the plaintiffs may well win. In September of 2019, Google was forced to settle a case with the US Federal Trade Commission for $170 million for collecting the personal information of children via YouTube. So it's not completely outside the realm of possibility that the courts could decide against Google in this case.

Used with permission from Article Aggregator

Remote is the New Normal

by Jason Rivas, HR Char-tec

We're well into the COVID-19 pandemic and across the world, people are getting used to working from home.

If you're a business owner, ask yourself this, "Could I afford to pay my staff to not work for 30 days? Will I have to pay them and essentially forward their paychecks in faith, knowing I may not get it back?" Have that dialogue with your staff, talk to your CPA, talk to your spouse, talk to your business partners now. This is going to be a global financial impact so you're not alone.

Does anybody fear this setup? Is anybody grossly concerned about their employees working from home? If you do, I'd say, "If you're concerned about running your business with your employees working from home, you shouldn't have them on the payroll now."

Alex said to me a few years ago, "We don't really need this building. It's convenient for training, convenient for education, convenient for a lot of things, but we could run everything out of our homes if we needed to – because of our backup plan. If this building was destroyed by fire, our plan isn't to look for office space and move into another building, waiting for the insurance check. We plan to have our employees work from home, and keep the business running without interruption."

The challenge is that this pandemic hit us hard and fast without much warning. Now, a lot of you can't buy 30 laptops for your team members in seven days. I get that. But start asking your techs and your engineers, "What do we need to do if we had to package up our desktop PCs and send the workstations home with the employees? Is that a possibility? How do we do that? How do we get that done?"

For my marketing team, if we end up having to convert them into teleworkers, we're going to package up their computers, we're going to send them home with their Macs, and we're going to keep them working without missing a beat. We expect that we're going to allow people to work from home so we're already talking about it. Even if they're sick, work from home. We want people to be able to earn a living through this. Because I'm telling you, if you think life is hard now, try not having a paycheck because you're too sick to earn it. If that happens, you have compounding issues.

Think about how you would dispense your hardware, and how your software is set up. Is your software set up to allow working from home? Do you need a new IP popped into your software to allow that to work? Does your firewall work and does your network sync? Do you know the network minimum expectations for your home workers? Does your system work off of slow DSL? If it doesn't, you're not required to provide it. And right now, Spectrum has a seven-week wait for network installations for increasing bandwidth in homes here in Bakersfield. Everybody's scrambling to try to figure out how this works because it's touching every aspect of our lives.

And that's why when you think about network installation, that's going to be your possible weak link, even for your customer support. And so, one thing we'll want to talk about now is if one of our employees is working from home, how do we support that situation if a failure happens? Talk about it now, figure out what that looks like. Have a protocol in place now so you won't be caught off guard.

The other thing about this is, a lot of people have asked, "How do you stay connected and keep your culture strong if your staff is working from home?" Start buying a few webcams, if you can find them. Get Microsoft Teams installed on their smartphones. This becomes their webcam, their meeting platform for you to connect with them.

And a component of our plan is that managers have to meet with their team twice a day for five minutes, at least. Twice a day, we want to see their faces, see how they're doing. We need to see how they're taking it, get a temperature for how they're working in their environment because that will tell us a lot about how the process is working. Or not working.

I have a teleworker agreement that is 50 state legal, including all the provinces in Canada, that allows you to be able to define the basic rules of the road for being a teleworker. It's not permanent. It's not a contract either. It says, "During this situation, we're going to approve working this way. You have to be available. Here are your rules of the road." Just have them sign it and we're done. If you need one, send me an email and I'll make sure you get it.Have the same conversation with your clients about their concerns over having a remote workforce. Right now, go talk to your clients. And then, reassure them, "Hey, we've got you handled. We'll be able to support you." It's what they need to hear from you, right now, in this time of crisis.

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 Set Their Sights On Cloud Services

Thanks to the pandemic, tens of millions of people are working from home.

Even before then, the Cloud was experiencing a tremendous amount of growth, but since shelter in place orders were issued by many governments around the world, growth has absolutely skyrocketed.

This has drawn the attention of a number of hacking groups, which have taken an increased interest in gaining access to Cloud resources, stealing login credentials and then making off with a wide range of sensitive data.

According to statistics gathered by McAfee, the number of attacks aimed squarely at Cloud services have increased by a whopping 630 percent between January and April of this year.

Broadly speaking, the attacks come in two basic flavors:

First, logins from anomalous locations that haven't previously been used and is not familiar to the organization.

Second, what researchers are calling 'suspicious superhuman' logins, which are defined by multiple login attempts in a short span of time from locations scattered across the globe. For instance, you might see one login attempt made in South America with another, a few seconds later, in Asia, and so on.

Rajiv Gupta, the Senior Vice President For Cloud Security at McAfee, had this to say about the company's findings:

"*The risk of threat actors targeting the cloud far outweighs the risk brought on by changes in employee behavior.*"

The good news is that there's a relatively simple way for organizations to reduce the risk to near-zero. Simply enable two-factor authentication and the vast majority of these types of attacks will be doomed to fail.

The bottom line is that the risks are increasing and that's not likely to change anytime soon. Stay on your guard and make sure your people are aware. Phishing scams are the most common means of gaining access to login credentials.

This New Malware Is Hitting Exchange Servers to Steal Info

In late 2019, a new strain of malware called "Valak" was detected. In the six months that followed its initial discovery in the wild, more than 30 variants of the code were detected.

Initially, Valak was classified as a simple loading program.

As various groups have tinkered with the code, it has morphed into a much more significant threat, and is now capable of stealing a wide range of user information. That is, in addition to retaining its original capabilities as a loader.

Researchers from Cybereason have cataloged the recent changes to the code. They found it to be capable of taking screenshots, installing other malicious payloads, and I infiltrating Microsoft Exchange servers, which seems to be what it excels at.

Most Valak campaigns begin with an email blast that delivers a Microsoft Word document to unwitting recipients. These documents contain malicious macro codes, which is an old, time-tested strategy.

If anyone clicks on the document and enables macros, that action will trigger the installation of the malware. Chief among the executables run is a file called "PluginHost.exe," which in turn, runs a number of files, depending on how the Valak software is configured. There are several possibilities here including: Systeminfo, IPGeo, Procinfo, Netrecon, Screencap, and Exchgrabber.

It is this last one that is used on Microsoft Exchange servers and is capable of infiltrating a company's email system and stealing credentials.

It is the extreme modularity of the malware's design that makes it a significant threat worth paying close attention to. Cybereason found more than 50 different command and control servers in the wild, each running a different strain of the software, and each with wildly different capabilities. However, they all share a common infrastructure and architecture.

Stay on the alert for this one. We'll almost certainly be hearing more about it in the weeks and months ahead.

Major WiFi Updates Came To Windows 10

Great news for the legions of Windows 10 users around the world. Version 2004 comes with a significant WiFi update that includes Wi-Fi6 and WPA3 support, which will give users better wireless performance and increased security.

That's great news, but of course, there's a catch. In order to make use of WiFi 6, you'll need a router with support for both WiFi6 and WPA3.

Although those do currently exist and are available for sale today, they are new, and therefore a bit on the expensive side. Even so, the new Windows 10 update gives you a compelling reason to upgrade your equipment.

If you recently purchased a new router, it may already support the latest standard. If so, that fact will be indicated either in the router's documentation or on the manufacturer's website.

You can check to see if you're currently connected to a WiFi6 network by following these steps:

- Connect to your network
- Select the WiFi network icon on the right side of the taskbar.
- Click on "Properties," which you'll find beneath the name of your network.
- When the properties screen loads, click the "Properties" tab and look at the information displayed next to "Protocol." If you're connected to a WiFi 6 network, you'll see "Wi-Fi 6 (802.11ax) in the Protocol box.

To see if you're connected using WPA3 security, follow these steps:

- Once you connect to your WiFi network, click the icon on the right side of the taskbar, then select Properties, located under your network's name.
- Once the screen loads, click the "Properties" tab and look at the information displayed next to "Security Type." If it says WPA3, you're all set.

To be sure you're using the latest Windows 10 update, just click your Start button, go to Settings, then Update & Security, and then Windows Update. Once there, you'll see a button labeled "Check for Updates." Click that, and if a new update is available, it will start downloading.
This is great news, and if you're looking for a simple way to boost your performance and productivity, this is it. Kudos to Microsoft for the inclusion.

Used with permission from Article Aggregator