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

Ribb"IT" Review

"Spring is nature's way of saying, 'Let's Party!'"

-Robin Williams

April 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

Malware Stealing Usernames And Passwords At Alarming Rates

Much discussion has been had about the fact that hackers are becoming increasingly sophisticated, and their methods ever-increasing in their complexity. While that's certainly true, more complex isn't always better.

Take, for example, the malware called Separ, which is a credential-siphoning bit of code, first detected in late 2017.

Separ has benefitted from ongoing development by the hackers controlling it, but what sets it apart from other malware strains is that it's almost deceptively simple, and that simplicity is a big part of its success.

The program is surprisingly good at evading detection, thanks to clever use of a combination of short scripts and legitimate executable files that are commonly used for completely benign purposes. This allows them to blend in and be utterly overlooked by most detection routines.

The most recent iteration of the software is embedded in a PDF. When an unsuspecting user clicks to open the file, Separ runs a chain of other apps and file types commonly used by System Admins. The initial double click runs a simple Visual Basic Script (VBS), which in turn, executes a batch script.

The batch script sets up several directories and copies files to them. Then it launches a second batch script, which opens a decoy image to high command windows, lowers firewall protections, and saves the changes to an 'ipconfig' file.

Then, it gets down to its real work, again, relying on completely legitimate executables to collect passwords and move them to the hackers' command and control server.

According to Guy Propper, (the team lead of Deep Instinct's Threat Intelligence group):

"Although the attack mechanism used by this malware is very simple, and no attempt has been made by the attacker to evade analysis, the growth in the number of victims claimed by this malware shows that simple attacks can be very effective. The use of scripts and legitimate binaries, in a 'living off the land' scenario, means the attacker successfully evades detection, despite the simplicity of the attack."

Be sure your IT staff aware. It's not always the most complex forms of malware that can get you.

New Linux Security Flaw Could Give Hackers Full System Access

Linux users, beware of the security flaw known as "Dirty Sock" and identified as CVE-2019-7304.

This critical security flaw was discovered by security researcher Chris Moberly, who disclosed the details to the makers of the Ubuntu distribution last month. The flaw resides in the REST API for the Snapd service.

That is a universal Linux packaging system responsible for making applications compatible with Linux across multiple distributions, and with no modifications to the executable necessary. Unfortunately, that means that Ubuntu isn't the only build impacted by the flaw. Literally every flavor of Linux is at risk.

Moberly had this to say about the issue:

"Snapd versions 2.28 through 2.37 incorrectly validated and parsed the remote socket address when performing access controls on its UNIX socket. A local attacker could use this to access privileged socket APIs and obtain administrator privileges."

If there's a silver lining to be found in Moberly's discovery, it is the fact that the nature of the issue prevents a hacker from exploiting it remotely. They'd have to have physical access to the machine or somehow trick the user into doing something that would trigger a program to escalate privileges on behalf of the hackers. Even so, the fact that the exploit can be used to gain total access and control to a target system means it's not something that can be ignored.

The good news is that Canonical, the makers of Ubuntu, have moved quickly and have already issued an update that addresses this flaw, with other major Linux distributions having followed suit. Regardless of what build you're using, a fix is likely already available. So if it's been a while since you updated, now would be an excellent time to do so. Better to be safe than sorry.

New Malware Is Coming Through Messaging Apps

As if your stressed IT staff didn't have enough to deal with, there's a new threat to be on the lookout for.

Researchers at the antivirus company Avast have discovered a new strain of malware that can spread by way of Skype and Facebook Messenger spam messages. The malware, called "Rietspoof" is described as a multi-stage malware strain.

It was first discovered back in August of last year, and until recently, didn't raise any eyebrows because it was seldom used. That has now changed. There's been a notable uptick in the number of instances of Rietspoof detected on the web.

As malware goes, Rietspoof by itself isn't all that threatening. Its goal is merely to infect as many devices as possible, serving as a bridge between an infected device and a command and control server that allows other strains of malware to be systematically injected onto infected systems.

Rietspoof accomplishes this goal by placing a shortcut (LNK file) in the Windows Startup Folder. This is one of the critical folders that Avast and other major antivirus programs monitor rigorously. However, Rietspoof has

(Continued on page 3)

(Continued from page 2)

managed to slip through the cracks, bypassing security checks because it is signed with legitimate certificates.

The malware's infection cycle consists of four discrete steps. Three of them are dedicated to establishing a Rietspoof beachhead on a target system, and the fourth is reserved for the downloading of more intrusive and destructive malware strains.

According to the research team that discovered it, since they first began tracking the malware, it has undergone a number of incremental changes. That lead them to the conclusion that Rietspoof is a work in progress and currently undergoing testing and further development.

Although it may have limited functionality now, that could very easily change as the hackers behind the code continue to modify it. Be sure your IT staff is aware, and stay vigilant!

Adobe Shockwave Unavailable After April

It's the end of an era. Way back in 1995, a company called Macromedia released the iconic Shockwave player, which quickly became a mainstay on Windows-based machines.

A decade later, Adobe purchased Macromedia, taking ownership of the Shockwave player and the company's other products (like Flash), both of which continued under the Adobe brand.

Time has not been kind to the technology. Not only has the company struggled to keep them secure, but the web itself has moved on. While Flash and Shockwave were once instrumental to cutting edge web development, today's developers have migrated to WebGL and HTML5, leaving these products with a withering market share.

Although there's not much current demand for the products, there are a surprising number of legacy websites that still rely on the aging tech. That's why Adobe's recent end of life announcement for Shockwave is sending ripples of panic through the internet.

Adobe has begun sending out emails to their customers bearing the subject line "Adobe Shockwave Product Announcement" in a bid to give webmasters whose sites are built around the tech time to shift gears. The Shockwave Player will officially be retired as of April 8th, 2019, about a year before another iconic Adobe product called Flash Player is slated to retire.

According to the official announcement, business owners with existing Shockwave Enterprise licenses will continue to receive product support until the end of their current contract. There will be no renewals.

All that to say, the clock is ticking. If redesigning your company's website to migrate away from Shockwave and Flash is something you've had on the backburner for a while, it's time to move it to the front of the queue. Be sure your IT and web development staff are aware, and plan accordingly.

Apple Developers Will Make Apps Usable On All Devices

Apple recently announced an important strategic change in direction that's great news for developers. In their next SDK release, developers will be able to build a single app that will work on every iPhone, iPad, and Mac the company makes.

The benefits to developers are obvious, with the biggest being a general reduction of development time.

There will be no need to make three different variants of an app to cover the entire Apple ecosystem. It will also mean more potential customers if a development group has been focused on only one segment of that ecosystem.

The change will also give Apple a powerful advantage in that eventually, the company will be able to merge the Mac App Store and the App Store for iOS. That will reduce their digital footprint and make managing their vast holdings easier. In addition to that, it will streamline the approval process, allowing developers to submit a single binary for all Apple devices.

According to a statement recently published by the company, the new development kit could be pushed out by as early as June, which is generating a tremendous amount of excitement in the Apple development community.

Obviously, consumers will see a big win here as well. Once the changes are complete and the two app stores are merged, there will be a single official hub where Apple users can get all their favorite Apps. They won't even have to worry about cross-device compatibility, which will improve the overall user experience.

The bottom line is that it will make things easier for developers, make managing the process easier for Apple, simplify things, and improve the user experience for the legions of end users in Apple's ecosystem. Kudos to the company for making the move. Exciting changes are ahead!

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.

Google Releasing Chrome Extension To Detect Password Theft

Google has found itself in hot water for something they claim to be an honest mistake and oversight. Owners of the company's popular Nest Guard (the centerpiece to their Nest Secure home alarm system) have recently discovered a microphone hidden in the guts of the device. The microphone wasn't mentioned in the product's specification sheet, which has creeped out consumer groups around the country and the world.

Google claims that their intention from the beginning was to incorporate Google Assistant functionality into the design. This of course would necessitate the presence of a microphone, making their failure to mention it nothing more than an oversight. Unfortunately, consumer groups don't seem to be finding that explanation convincing, which explains the push back the company is suddenly getting.

To be fair, Google Assistant functionality would be a superb addition to Nest Secure, but people should be aware of what precisely they're getting when they open their wallets and buy a new product. Especially given the fact that there have been a number of high-profile instances where data captured by microphones embedded in a variety of consumer products has already been mishandled and misused.

It ultimately doesn't matter how many people would or wouldn't have made the purchase had they known about the presence of the microphone. The central issue is that they purchased a product without realizing it could be used to record them.

These days, privacy concerns are increasingly on everyone's mind and with good reason. Every day, what remains of our privacy seems increasingly under attack. Innocent oversight or not, this was an unnecessary invasion of that privacy, and advocacy groups are justified in calling the company out for it.

If you don't yet own a Nest Secure, but have been considering buying one, be aware. There's a microphone embedded in it.

Skype Video Calls Get Background Blur Feature

Skype is introducing a new feature to its video call service that users have been asking about for quite some time now. Background blur.

If you regularly make video calls, you've probably been in a situation where such a feature would have come in handy.

It could be anything, really. Maybe you're working from home and your place is a mess. Or people keep coming in and out. Or you've got a whiteboard behind you that contains sensitive information you'd rather not let everyone see.

Whatever the case, it's often true that people wish they could blur whatever's behind them when they activate their camera. It's also a feature that's been available on Microsoft Teams, so in this case, the Skype development team is playing a bit of catch up.

The new feature uses an AI routine that's been coded to recognize the human form. Even better, the AI routine is robust enough that it recognizes hair and hands, so if you tend to get somewhat animated when you talk, the camera will retain its focus on you while conveniently blurring whatever is behind you.

The new feature is available via the latest build of Skype, so if you don't currently see it on your desktop or laptop, the only thing you should have to do to start using it is to upgrade to the latest version and you'll be all set.

While it's certainly not the most critical new feature addition we've seen in recent months, it's certainly a welcome one. It's both useful and practical in a variety of situations. Everyone, from people working at home to independent contractors, to Enterprise users, can and will benefit from the new background blur. Kudos to the Skype development team for delivering the goods.