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

Ribb"IT" Review

December,

the month of

joy, happiness

and to finish

what you

started.

December 2019

Issue 12, 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

Hackers Are Imitating Government Agencies To Spread Malware

Researchers at Proofpoint have found evidence of a new threat actor who has been sending out convincing looking emails.

They are claiming to come from several government agencies.

These include the Italian Revenue Agency, the German Federal Ministry of Finance, and the United States Postal Service.

This is all part of a malicious campaign designed to infect targeted recipients with a variety of malware.

The bulletin Proofpoint released on matter reads, in part, as follows:

"Between October 16 and November 12, 2019, Proofpoint researchers observed the actor sending malicious email messages to organizations in Germany, Italy, and the United States, targeting no particular vertical but with recipients that were heavily weighted towards business and IT services, manufacturing, and healthcare.

These spoofs are notable for using convincing stolen branding and lookalike domains of European taxation agencies and other public-facing entities such as Internet service providers. Most recently, the actor has attacked US organizations spoofing the United States Postal Service. The increasing sophistication of these lures mirrors improved social engineering and a focus on effectiveness over quantity appearing in many campaigns globally across the email threat landscape."

In the US, emails claiming to be from the post office come with an attached Word Document called "USPS_Delivery.doc." If a recipient clicks on the document to open it, they'll receive a message that the file has been encrypted for additional security and in order to view it, they'll be required to "enable content."

Naturally, clicking on the "enable content" button does nothing of the sort. Instead, it installs whatever malware the senders have associated with the email in question.

The identity of the threat actor is not known at this time, but this is a serious issue that you should immediately alert all employees about in order to minimize the risk to your company.

Are Hackers Using Popular Assistant Devices To Listen To Users?

The utility of virtual assistants like Amazon's Alexa and Google Home are undeniable. They're just genuinely handy devices to have around.

Unfortunately, they're also prone to abuse and exploits by hackers and unsavory developers. They can be used to spy on and even steal sensitive information from unsuspecting users.

This is not new in and of itself. Security researchers around the world have, at various points over the last couple of years, sounded the alarm about weaknesses and exploits. To the credit of both companies, any time this has happened, both Amazon and Google have responded promptly, plugging gaps and shoring up the security of their devices.

Unfortunately, every few months or so, new exploits are discovered. The two companies are essentially playing Whack-A-Mole with security flaws, which appear to have no end.

Recently, security experts published two videos, one for Alexa and one for Google Home. Each demonstrated a simple back-end exploit that anyone with a DevKit could employ. The exploits revolve around inserting a question character (U+D801, dot, space) to various locations in the code. Then they introduce a long pause during which the assistant remains active and listening.

To give you an idea of how this could be exploited, one of the example videos shows a horoscope app triggering an error, but the presence of the special character introduces a long pause during which the app is still active.

During the long pause, the app asks the user for their Amazon/Google password while faking a convincing looking update message from Amazon or Google itself. Given the long pause, few users associate the poisoned horoscope app with the password request. It seems like it's coming from the device itself.

It's both sneaky and troublesome, and worst of all, even when both companies move to address this issue. By this time next month if history is a guide, there will be others. We're not saying not to use them, but when you do, be very mindful.

Netflix May Stop Allowing Users To Share Their Passwords

Do you have a Netflix account?

If so, you know how awesome the service is. Intuitive and easy to use, and of special interest, easy to share.

In fact, password sharing among family and friends is so common that it's even openly discussed on discussion forums around the web.

Unfortunately, it has become so commonplace that Netflix has begun making noises about finding ways of limiting the practice. Greg Peters, Netflix's Chief Product Officer, had this to say on the topic:

"We continue to monitor it. We'll continue to look at the situation and we'll see those consumer-friendly ways to push on the edge of that, but we've got no big plans at this point in time in terms of doing something different there."

As we said, this is not language that raises alarm bells. This is the earliest stages of rumbling from a company that's fundamentally dissatisfied with the idea that they're losing money at the margins. At least some of the people enjoying their content are borrowing a paying customer's password, and a portion of those would probably sign up for their own accounts if the company pressed the issue and they had to.

No doubt, based on the statement above, the day will eventually come when Netflix starts taking a harder look at the practice of sharing accounts and begins punishing users who break their password sharing rules. It seems clear that that day isn't upon us yet.

All that to say, if you're currently in the practice of letting your brother in law or girlfriend borrow your account access to watch movies, you can continue to do that, at least for the foreseeable future. Even when the day comes that the company clamps down on that kind of thing, there are already several tools, like the Netflix Party Chrome Extension that allow sharing in a different form.

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.

Fake Voicemail Messages Tricking People Into Opening Malicious Content

Office 365 has been the target of an increasing number of ongoing phishing scams.

The latest scam involves using fake voicemail messages to convince targets that they need to log in to hear the full recording.

Researchers at McAfee Labs had this to say about the matter:

"Over the past few weeks McAfee Labs has been observing a new phishing campaign using a fake voicemail message to lure victims into entering their Office 365 email credentials. At first, we believed that only one phishing kit was being used to harvest the user's credentials. However, during our investigation, we found three different malicious kits and evidence of several high-profile companies being targeted."

Recipients will receive an email message informing them that they missed a call. A partial recording is available andembedded in the email, but the recipient gets little more than hello, so there's no real indication of what the message might be about.

Then, if the recipient clicks the link provided to "log in and hear the message" they will, of course, be sent to a page that looks like an Office 365 login screen. All they're really doing at that point is handing their credentials over to whomever sent the message.

As we said at the start, Office 365 has become an increasingly popular target. There's another scam making the rounds that tries to get a user's login credentials by making it seem as though the message was sent by the recipient's employer's HR department and talks about an upcoming raise.

Both are powerful approaches that have been yielding better results than usual for the scammers. Be sure your IT staff and all of your employees are aware of and on their guard against these scams.

Non-Updated Android Phones Vulnerable To NFC Beaming Hacks

Has it been more than a month since you upgraded your Android OS?

If so, you should make upgrading a priority.

Just over a month ago, Google patched a critical flaw in the Android OS that allowed hackers to "beam" malware to any unpatched devices via a process called 'NFC Beaming'.

It relies on a service called Android Beam that allows an Android device to send videos, apps, images, or other files to a nearby device using Near-Field Communication (NFC) radio waves as an alternative to Bluetooth or WiFi. It's a great technology and a handy capability but sadly, its implementation was flawed.

Fortunately, the flaw was unearthed by an independent security researcher who alerted Google to the problem. Even worse, when files are sent in this manner, the user would not get a prompt warning

(Continued on page 4)

(Continued from page 3)

them that an app was attempting to be installed from an "unknown source."

If there's a silver lining in all of this, it is the fact that NFC connections are only initiated when two devices are sitting close to each other. By 'close' we mean really close. The range is limited to 4 centimeters (about an inch and a half). This limits the attack vector's utility quite sharply.

Even so, it's something to be aware of, especially if you travel frequently. It's well worth grabbing Google's latest update for Android Oreo if you haven't already done so. The alternative to this course of action is to go into your Android settings and disable Android Beam and NFC if it's a feature you seldom use anyway.

Kudos to the sharp-eyed researcher who caught the bug, and to Google, who responded swiftly and issued a fix for the issue.

New Office 365 Feature May Prevent Questionable Emails

Microsoft continues their war against spam and phishing emails with the rollout of a new feature in Office 365 called 'Unverified Sender'.

It is designed to help Outlook users identify emails that may contain poisoned files or requests for personal or sensitive information that could be used to steal a user's identity.

The company had this to say about the new feature:

"Unverified Sender is a new Office 365 feature that helps end-users identify suspicious messages in their inbox...we've added an indicator that demonstrates Office 365 spoof intelligence was unable to verify the sender."

When you toggle the new feature on, any email in your inbox that the AI is unable to identify or verify will be marked. It will have the sender's initials or photo replaced with a question mark in the People Card. That will make it easy for any Office 365 user to spot potential phishing or sender spoofing attempts.

In tandem with the Unverified Sender feature, Microsoft is also increasing the size of its DKIM keys from 1024-bit to 2048-bit for all Office 365 customers during the month of October. They are doing this in order to enhance security in all environments.

About this, the company published the following:

"If you already have your default or custom domain DKIM enabled in Office 365, it will automatically be upgraded from 1024-bit to 2048-bit at your next DKIM configuration rotation date...This new 2048-bit key takes effect on the RotateOnDate and will send emails with the 1024-bit key in the interim. After four days, you can test again with the 2048-bit key (that is, once the rotation takes effect to the second selector)."

Finally, Microsoft is rolling out a feature they announced in late July of this year (2019), which is their improved Malicious Email Analysis. Collectively, these new features should provide a much safer environment for all Office 365 users. Kudos to Microsoft for that!