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

Ribb"IT" Review

In February there is everything to hope for and nothing to regret.

-Patience Strong

February 2020

Issue 2, 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

What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication works on the principle of using multiple pieces of secret information in order to verify identity. Standard usernames and passwords can be brute forced but using a separate piece (or more) of information makes this more and more impractical. Some MFA schemes will use secret questions (effectively extra passwords), or a onetime key from an authentication application (Google Authenticator for example.)

It used to take days to guess an 8-character password, now it can be done in minutes. Everything requires a password, and people can be lazy and recycle passwords. If a your password is compromised for a site, who knows what other accounts are now compromised? Using any multi-factor solution can reduce the impact substantially.

Knowledge
This can be an extra password, a security question, or some other type of challenge. By adding a separate password, an attacker must gain access to the password AND the additional layer (MFA), and avoid locking themselves out trying to do so.

Possession
Possession challenges rely on the physical possession of a device or some other item. This can be anything that generates a code. Most things people think of as 2FA are generally going to be password based on possession of an application which generates a one-time key.

Which Method Works Best?

Possession is the most practical at present. Having a physical device means that stealing a one-time key or password is near useless, and the device can be revoked if it is physically misplaced or stolen. We use the principle of possession (and a degree of knowledge for an added challenge). The important part is using a device someone will (almost) always have a way to authenticate without inconveniencing the user too much.

Why Is MFA So Important?

Phishing and social engineering are some of the biggest security threats to businesses. MFA helps neuter phishing and social engineering attacks by adding a layer that an end user will struggle to give away. It's easy to type your password into the wrong box, but how do you give your phone or a USB key out too? You also know almost instantly when one of these devices is missing.

MFA throws a wrench in the attackers gears for this. The username and password are only two of the three parts to the key. Without the third part, the whole exercise doesn't accomplish much for attackers direct target. Ask us about enabling multifactor authentication.

For more information about applying healthy MFA practices and keeping your business safe, schedule a FREE consult with us and we'll be happy to help you!

New Hacking Method Looks Like A Locked Computer

Scammers have breathed new life into an old scam.

For years, the old 'Law Enforcement Lock' trick has been used to cheat unsuspecting victims of their hard-earned money. The new wrinkle works like this:

Scammers will redirect users using the Chrome web browser to sites that host a full-screen image of a Windows 10 desktop with a notice that appears to come from local law enforcement agencies. This pages informs the user that their computer has been locked for some unspecified illegal activity.

The groups running this sort of scam make sure to display a legitimate government URL in order to make it look more convincing. Victims of this scam are informed that they can unlock their computer again by paying the fine via credit card, right then and there.

Of course, the computer actually isn't locked at all. However, this scam has taken in a surprising percentage of users who aren't paying close attention.

A typical lock screen from the scammers will bear a message that closely follows this script:

"Your browser has been locked due to viewing and dissemination of materials forbidden by law of (country name), namely pornography with pedophilia, rape and zoophilia. In order to unlocking you should (amount and currency type) fine with Visa or MasterCard. Your browser will be unlocked automatically after the fine payment.

Attention! In case of non-payment of the fine, or your attempts to unlock the device independently, case materials will be transferred to (name of local law enforcement agency) for the institution of criminal proceedings against you due to commitment of a crime."

As you can see from the grammatical errors in the script, this is by no means an official announcement, but it looks real enough that it sends people into a panic, causing them to enter credit card information without thinking.

Naturally, this information is harvested and resold on the Dark Web, putting money in the scammers' pockets. Make sure your employees are aware of it, and stay vigilant.

Message Recall Feature May Be Added To Office 365

For a while now, Microsoft Outlook users have enjoyed a highly popular addition to their email service. In a nutshell, it allows them to recall messages that have been sent using Outlook, which is an Exchange Online hosted cloud email service for business.

They can un-send the emails, provided that the recipient is using Outlook and the messages haven't been opened yet.

It's a good, well-implemented feature. Recently, Microsoft announced that it will be expanding its availability, adding it for all Office 365 environments during the fourth quarter of 2020.

The company had this to say on a recent blog post on the subject:

"The Outlook for Windows Message Recall feature is extremely popular with users, yet it doesn't always work so well. Part of the problem is that the recall is client-based and the recall can only happen if the recipient also uses Outlook.

With millions of users with mailboxes in Office 365, we're now able to improve upon that feature by performing the recall directly in the cloud in Office 365 mailboxes, so it doesn't matter which email client the recipient uses, the recall takes place in their Office 365 mailbox, and when their client syncs their mail, the message is gone."

As part of the Office 365 implementation of this feature, users will also have an aggregate message recall status report available to them that they'll be able to use to tell at a glance which messages were successfully recalled and which ones were not.

If you want more, you should know that Microsoft has recently announced it will be adding protections against Reply-All email storms. They have not-so-affectionately been referred to as 'Reply-allpocalypses' that are set off when people send emails with a large email distribution list. They can easily lead to accidental denial of service that can bring even the most robust email servers to their knees.

Both are welcome additions indeed. Kudos to Microsoft for the coming improvements.

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.

FBI Sheds New Light On Ransomware Tactics

According to a recent FBI alert marked "TLP: AMBER," businesses should be on high alert for ransomware attacks.

The alert reads, in part, as follows:

"Since January 2019, LockerGoga ransomware has targeted large corporations and organizations in the United States, United Kingdom, France, Norway, and the Netherlands. The MegaCortex ransomware, first identified in May 2019, exhibits Indicators of Compromise (IOCs), command and control (C2) infrastructure, and targeting similar to LockerGoga.

The actors behind LockerGoga and MegaCortex will gain a foothold on a corporate network using exploits, phishing attacks, SQL injections and stolen login credentials."

The alert also states that the attackers behind these two ransomware strains often wield Cobalt Strike tools, including Cobalt beacons to gain remote access.

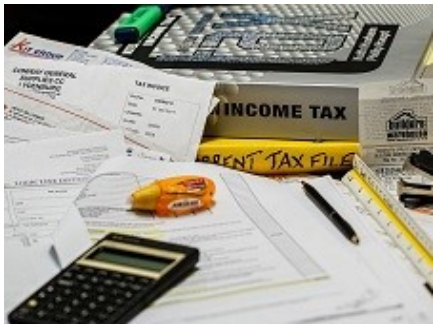
Once the attackers gain a toehold inside a target network, they'll carefully explore and map the target network, seeking out the most sensitive information including proprietary company data, payment card information and other customer details and the like.

The goal here is to identify the highest value information that can be exfiltrated to the command and control server for sale on the black market. Finally, when all of the most valuable information has been siphoned from the network, the hackers will trigger the ransomware itself, which they'll use to gain an additional payment, extorting the affected organization.

The FBI also reports that hacking operations carried out by nation-states often deploy ransomware to make it appear that the attack is the work of traditional cybercriminals, throwing forensic investigators off of their trail.

The process of network mapping and exfiltrating valuable data can take weeks or even months, depending on the size of the network. So, organizations may be infected long before the visible signs of the attack become evident. Given that, it's more important than ever to have robust security system in place. You should have remote backups taken at regular intervals and a rapid response plan in place in the event of a breach.

New IRS Tax Scammers Use Personal Data For Big Returns



Recently, the Department of Justice brought charges against Babatunde Olusegun Taiwo for using personal information acquired on the Dark Web. He used the information from data breaches to file fraudulent tax returns with the IRS.

He was able to gain enough information to file more than two thousand income tax returns that attempted to claim more than $12 million. The IRS paid out nearly $900,000 before the authorities caught wind of the scam and shut it down, arresting the St. Louis man and sentencing him to four years in prison.

The Special Agent in charge of the investigation, Thomas Holloman, had this to say about the matter:

"We will continue to pursue criminals who prey on innocent victims and we will continue to enforce our nation's tax laws. Today's sentencing should send a clear message to would-be criminals - you will be caught and you will be punished."

(Continued on page 4)

(Continued from page 3)

Taiwo isn't the only criminal to have recently been caught by the Department of Justice's drag net. In a separate announcement, the DOJ released details of the case against Hitesh Madhubhai Patel, an Indian national. Between 2013 and 2016, he leveraged call centers to scam victims out of millions of dollars by impersonating the IRS and USCIS. He was threatening victims with deportation, arrest, and jail time unless they paid bogus fines over the phone to his employees.

Patel is due to be sentenced on April 3rd of this year and could face up to twenty years of prison time, in addition to fines of up to a quarter million dollars.

Kudos to the Department of Justice for bringing these crooks to justice. One has to wonder though, for every criminal caught and jailed for activities like these, how many more remain uncaught? Too many, but progress is progress!

New Malware Sends Offensive Texts From Your Phone

Malware tends to be at its most effective when it exists in secret. Under the radar. This is what allows malicious code to burrow deep into an infected system and capture a wide range of data. It's what allows cryptojacking software to quietly siphon off computer power to mine for various forms of cryptocurrency. That makes money for the malicious code's owners. Secrecy is typically seen as a very big deal.

Then there's the malware called Faketoken, which has recently been upgraded with enhanced capabilities that throws all that out the window. The latest version of the malware adds insult to injury by sending out offensive, expensive, or overseas text messages after milking as much money out of an infected system as it can. It's such a departure from hacking norms that it caught researchers at Kaspersky Lab by surprise when they saw it.

Researchers have been tracking Faketoken's ongoing development since it first made the "Top 20 Most Dangerous Banking Trojans" list in 2014.

Since that time, the code's owners have added a raft of capabilities to the malware, including:

- The ability to steal funds directly, rather than relying on other Trojans bundled with it to do the heavy lifting
- Using phishing login screens and overlaid windows designed to dupe mobile users into entering their account credentials, handing them straight to the hackers
- The ability to act as ransomware, encrypting files and demanding payment

Sending out offensive texts is an oddly amusing addition to malicious code like this. However, there may be a method to the apparent madness of the people behind the code. It is, after all, a fantastic way to advertise the code's effectiveness.

Ultimately, the only people who know the true purpose behind this new functionality are the hackers themselves, but we may well be looking at the leading edge of a new trend in malware.