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

Ribb"IT" Review

Happy New Year!

"You are never too old to set another goal or to dream a new dream."

– C. S. Lewis

January 2020

Issue 1, Volume 10

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

Ransomware Uses New Method To Get Past Antivirus Programs

Researchers at SophosLabs have discovered a new threat to be on the alert for. A variant of the Snatch ransomware has been spotted in the wild.

It features an innovative means of getting around whatever antivirus software you may be using to defend yourself.

Disguised as a backup utility, when the malware is installed, it forces the Windows PC it's being installed on to reboot in Safe Mode. This works because when the machine comes back up in Safe Mode, it's running with a limited set of drivers and capabilities that don't include antivirus software. Since it's not running, it obviously can't detect the infection. It is ransomware, so as soon as the installation is complete, the files on the infected system are encrypted and unusable.

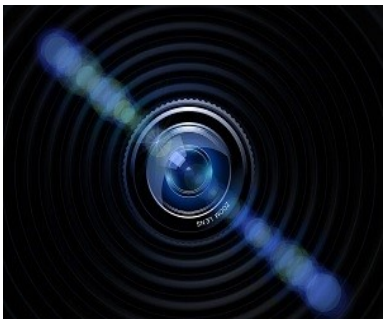
It gets worse. In addition to locking the infected system down, Snatch will also attempt to delete all the Volume Shadow Copies in order to prevent forensic recovery of the encrypted files. On top of that, Snatch does more than simply encrypt files. It also roots through the system and steals a wide range of data files, sending them off to a command and control server, even as it encrypts them.

The researchers report that Snatch can run on Windows versions 7 through 10, in both 32 and 64-bit versions. Of interest, it was written in Go, which is a programming language used by app developers to create cross-platform apps. Although Snatch is currently only known to impact Windows-based machines, given the programming language used, the developers would have an easy time creating variants that could infect just about any system, running any OS.

The hackers controlling the code seem to have big plans. They're advertising on underground forums on the Dark Web shopping for affiliates. They are hoping to partner with hackers or dissatisfied employees who have credentials that would enable the owners of the software to plant their malicious code inside large organizations.

Although there's no evidence yet of a widespread campaign using Snatch, that day seems inevitable, so make sure your staff knows to stay on the alert for it.

Update Amazon Blink Cameras To Fix Security Vulnerabilities



Do you have a home security system that incorporates Amazon's Blink XT2 cameras?

If so, be advised that researchers at Tenable Security recently identified several serious security flaws that would allow an attacker to take control of the cameras remotely and use them to spy on you and your family.

The security issues are centered in the cameras' Sync Module. It acts as a bridge between the camera itself and the cloud and allows users to divide their camera suite into discrete zones that cover different parts of the home. It also allows them to activate the cameras located in various zones at different times throughout the day and night.

Unfortunately, these vulnerabilities allow an attacker to selectively activate or deactivate cameras and view archived footage.

The researchers had this to say about the issue:

"When checking for updates, the device first obtains an update helper script (sm_update) from the web, and then immediately runs the content of this script with zero sanitation. If an attacker is able to MitM this request (either directly or indirectly - through some sort of DNS poisoning or hijacking) they can modify the contents of this response to suit their own needs or desires.

The most obvious attack scenario for this flaw would be some sort of insider threat - babysitters, house or pet sitters, Airbnb guests, or anyone else with somewhat privileged access to your home."

The good news is that Amazon has moved quickly to address the issue and has already issued a firmware update. All you need to do at this point is check your Blink XT2 cameras to be sure they're running firmware version 2.13.11 or later.

However, there's a caveat. If your camera has already been compromised, it won't automatically receive the firmware update. In that case, you'll likely need to hire an expert to manually force the update. Be sure to check the firmware version of your cameras as soon as possible. You don't want your security system to be used against you.

Instagram Adds AI To Warn You About Offensive Comments

Instagram has made a recent change you should be aware of. Any time you make a comment, you may get a popup warning that your comment may be "potentially offensive".

That is, if the service's AI-powered tools conclude that the warning is appropriate based on an analysis of other comments that have generated complaints.

Instagram isn't taking a hard-nosed approach here. If you get such a notification, you'll have the option to either edit it before posting or just post it as is.

In July 2019, the company introduced a similar tool for policing comments left on user posts, and this latest change builds on that toolset.

There's a method to the company's madness, and a broader purpose at work here. In October, Instagram added a "Restrict" feature that allows users to shadow ban bullies. Prior to that, it began rolling out AI bots that scanned content in an effort to proactively detect bullying in photos and captions, and other routines to filter offensive comments.

One thing that differentiates this latest feature from the others is that the company's latest change is only available in "select countries" for now. The rest have been rolled out globally. Eventually that's destined to change, but Instagram has not issued a statement for when that might happen.

Preventing cyberbullying doesn't get as much attention as it should. Cyber bullying a real thing that leads to a tragic handful of deaths every year, and causes no end of pain and suffering to the targets of such behavior. So far, most companies haven't been paying much more than lip service to doing something about it, so kudos to Instagram for taking this series of steps. While it remains to be seen how effective these efforts will be, the fact that the company is doing something is praiseworthy.

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.

About Half A Million Credit Cards Found On Dark Web

Researchers from Group-IB monitor the Dark Web and have recently reported the appearance of nearly half a million credit card records available for sale.

Each record is valued at more than half a million dollars. The records were rolled out in staggered fashion, with the first file containing some 30,000 records.

They included credit card numbers, CVV codes, expiration dates, email addresses, owner's names, addresses and phone numbers.

Much of the information contained in the database can't be found on the card's magnetic stripe. That's a clear indication that the cards being offered for sale were not gathered from infected point of sale terminals or ATMs but rather, collected via online attacks.

Although there's no definitive proof, MageCart seems to be the most likely source of the card records in this collection. That is because there have been a number of high profile, successful MageCart attacks in recent months.

Just a month after the initial database of 30,000 records was offered for sale, two additional databases appeared in the same corner of the Dark Web. One of them contained 190,000 records, and another containing some 205,000 offered by the same hacker.

Initially, the card records were being sold at $3 each. When the two larger databases appeared, the seller lowered the price to $1 per record. In all three cases, the hacker offering the cards assured purchasers that 85 to 90 percent of the records were valid and came with full information.

Most of the records in all three databases were collected in Turkey and based on Group-IB's analysis of the data. The researchers were able to confirm that most of the card numbers could be traced back to the top 10 Turkish banks.

In light of this, if you're living or doing business in Turkey, or have a payment card issued by one of the big Turkish banks, it pays to take steps to protect yourself.

New Trojan Malware Steals Passwords From Chrome

If you use Google's Chrome web browser, there's a new threat you should be aware of. A new trojan targeting Windows-based machines will attempt to steal passwords stored in the Chrome browser.

Dubbed CStealer, it was discovered by the Malware Hunter Team. They found some points of interest that make this threat more notable than others in its class.

If infected by this malware, the code will connect to a MongoDB database where it will upload stolen credentials at periodic intervals. There are hardcoded MongoDB credentials embedded in the code that facilitate the connection, with the goal being to create a convenient password repository for the owners of the malware.

Unfortunately, the same hooks used to create this database connection can easily be modified to redirect to a command and control server. So once infected, the hacker who controls the malware could easily use it to infect the compromised machine with other types of malware that is capable of causing whatever mayhem the hacker felt like inflicting.

(Continued on page 4)

(Continued from page 3)

The other point that's worth mentioning here is this: Potentially anyone could gain access to the password repository. Again, the MongoDB credentials are hardcoded into the malware, so anyone who takes the time to analyze the code can connect to the server and retrieve whatever happens to be stored there.

Given that hackers aren't known for their altruism, this is almost certainly an unintended consequence of the design of the code. So, it's likely that this method of execution will be corrected in some future build of the trojan. For now though, if you are infected with CStealer, know that your stored passwords can easily be accessed by any number of hackers.

As ever, awareness and vigilance are the keys to keeping these sorts of things from happening. Stay alert, and make sure your employees are aware of this latest threat.

New Gmail Attachment Feature Makes Forwarding Easier

Google has a solid reputation when it comes to making a steady stream of improvements to its large and growing base of products and services. They have a demonstrated a track record when it comes to enhancing user experience. Recently, they've proved that once again by adding a new feature to Gmail that allows you to forward one or more emails you've received as attachments.

This enhancement allows the recipients of your forwarded message to open the attached email and view it in its original form with its headers intact. While it's useful for individual Gmail users, it's incredibly useful to security professionals, network admins and server admins who often need to examine email headers.

There are two different ways you can use the new feature. First, create a new blank email message and drag and drop one or more emails into the message you're composing. Second, you can select the emails you want to forward, click on the hamburger menu running across the top of your inbox and select "Forward as attachment."

Whichever method you choose, the emails you attach will be sent as an EML file, which is supported by most of the email clients in use today. Even better, there's no upper limit to the number of emails you can send as attachments.

On the receiving end, when you receive an attached EML message, clicking on it will open it in a new window.

Note that the new feature is currently rolling out and is not available universally at this point. You'll know when you have the functionality when you click on the three-dot More menu and see a new option: "Forward as attachment."

Even if you don't personally have much cause to use this new feature, it's big news and will be a huge boon to admins. Kudos to Google for the addition.