On January 30, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Microsoft, Mozilla, and Google Products. *(No update from CIS by the time of publication, threat level unchanged)*

Threat Level's explained

- **GREEN or LOW** indicates a low risk.
- **BLUE or GUARDED** indicates a general risk of increased hacking, virus, or other malicious activity.
- **YELLOW or ELEVATED** indicates a significant risk due to increased hacking, virus, or other malicious activity that compromises systems or diminishes service.
- **ORANGE or HIGH** indicates a high risk of increased hacking, virus, or other malicious cyber activity that targets or compromises core infrastructure, causes multiple service outages, causes multiple system compromises, or compromises critical infrastructure.
- **RED or SEVERE** indicates a severe risk of hacking, virus, or other malicious activity resulting in widespread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors.

WEEKLY IT SECURITY BULLETIN

8 February 2019

In The News This Week

Several Photo Editing Apps Found Stealing User's Photos

Security researchers have discovered several photo editing apps in Google Play Store stealing user's photos. Researchers from Trend Micro labs have discovered at least 29 photo editing and beauty apps in the Google Play Store containing code capable of performing malicious activities on the user's phone. The malicious apps have been downloaded by approximately 4 million users before Google removed it from play store. "We discovered several beauty camera apps (detected as AndroidOS_BadCamera.HRX) on Google Play that are capable of accessing remote ad configuration servers that can be used for malicious purposes." said in the blog post published by Trend Micro researchers. The apps once installed will not show any suspicious behaviour until users try to delete the app. After installing, it creates a shortcut and hides its icon from the application list. The apps also use packers to prevent them from being analyzed. Some apps push full-screen ads on the user's device with fraudulent or pornographic content whenever they unlock their devices. Other apps redirect users to a phishing website and attempt to steal their personal information. Users are tricked by informing them they have won some contest and asks their personal information such as addresses and phone numbers. Researchers also discovered another set of photo filter or beautifying apps containing malicious codes which upload users photos to a remote server controlled by the attacker. (Find the list of Apps involved and Read the full article here: https://securereading.com/several-photo-editing-apps-found-stealing-users-photos/)

Android Phones Can Get Hacked Just by Looking at a PNG Image.

Using an Android device? Beware! You have to remain more caution while opening an image file on your smartphone—downloaded anywhere from the Internet or received through messaging or email apps. Yes, just viewing an innocuous-looking image could hack your Android smartphone—thanks to three newly-discovered critical vulnerabilities that affect millions of devices running recent versions of Google's mobile operating system, ranging from Android 7.0 Nougat to its current Android 9.0 Pie.
The vulnerabilities, identified as CVE-2019-1986, CVE-2019-1987, and CVE-2019-1988, have been patched in Android Open Source Project (AOSP) by Google as part of its February Android Security Updates. However, since not every handset manufacturer rolls out security patches every month, it's difficult to determine if your Android device will get these security patches anytime sooner.
. (Read story here https://thehackernews.com/)

Databases Collection Containing 2.2 billion records Discovered on Hacker Forums.

Security researchers have discovered a new collection of databases containing 2.2 billion unique usernames and passwords freely distributed in hacker forums and torrents. Earlier security researcher Troy Hunt discovered the first set of databases named collection #1 containing 773 million unique username and passwords Now researchers have discovered the remaining databases named Collections #2–5 containing 845 gigabytes of stolen data and 25 billion records in total. According to security researcher Chris Rouland, the collection has already circulated widely among hacker underground forums. The tracker file Rouland downloaded was being seeded by more than 130 people and has already been downloaded more than 1000 times. "It's an unprecedented amount of information and credentials that will eventually get out into the public domain," said Chris Rouland. Most of the stolen data appear to be from previous breaches like Yahoo, Dropbox and LinkedIn. *Thanks to Yazan Shapsugh who pointed me in the direction of this story*. (Read the full story here: https://secureread ing.com/)

Real-World Warnings Keep You Safe Online

Why are these warnings important?

Like the real world, technology and the Internet present dangers as well as benefits. Equipment fails, attackers may target you, and mistakes and poor judgment happen. Just as you take precautions to protect yourself in the real world, you need to take precautions to protect yourself online. For many users, computers and the Internet are unfamiliar and intimidating, so it is appropriate to approach them the same way we urge children to approach the real world.

What are some warnings to remember?

- Don't trust candy from strangers – Finding something on the Internet does not guarantee that it is true. Anyone can publish information online, so before accepting a statement as fact or taking action, verify that the source is reliable. It is also easy for attackers to "spoof" email addresses, so verify that an email is legitimate before opening an unexpected email attachment or responding to a request for personal information. (See Using Caution with Email Attachments and Avoiding Social Engineering and Phishing Attacks for more information.)
- If it sounds too good to be true, it probably is – You have probably seen many emails promising fantastic rewards or monetary gifts. However, regardless of what the email claims, there are not any wealthy strangers desperate to send you money. Beware of grand promises—they are most likely spam, hoaxes, or phishing schemes. (See Reducing Spam and Identifying Hoaxes and Urban Legends.) Also be wary of pop-up windows and advertisements for free downloadable software—they may be disguising spyware. (See Recognizing and Avoiding Spyware.)
- Don't advertise that you are away from home – Some email accounts, especially within an organization, offer a feature (called an autoresponder) that allows you to create an "away" message if you are going to be away from your email for an extended period of time. The message is automatically sent to anyone who emails you while the autoresponder is enabled. While this is a helpful feature for letting your contacts know that you will not be able to respond right away, be careful how you phrase your message. You do not want to let potential attackers know that you are not home, or, worse, give specific details about your location and itinerary. Safer options include phrases such as "I will not have access to email between [date] and [date]." If possible, also restrict the recipients of the message to people within your organization or in your address book. If your away message replies to spam, it only confirms that your email account is active. This practice may increase the amount of spam you receive.
- Lock up your valuables – If an attacker is able to access your personal data, he or she may be able to compromise or steal the information. Take steps to protect this information by following good security practices. (See the Tips index page for a list of relevant documents.) Some of the most basic precautions include locking your computer when you step away; using firewalls, anti-virus software, and strong passwords; installing appropriate software updates; and taking precautions when browsing or using email.
- Have a backup plan – Since your information could be lost or compromised (due to an equipment malfunction, an error, or an attack), make regular backups of your information so that you still have clean, complete copies. (See Good Security Habits.) Backups also help you identify what has been changed or lost. If your computer has been infected, it is important to remove the infection before resuming your work. (See Recovering from Viruses, Worms, and Trojan Horses.) Keep in mind that if you did not realize that your computer was infected, your backups may also be compromised.

Read the full article here : https://www.us-cert.gov/ncas/tips/ST05-014

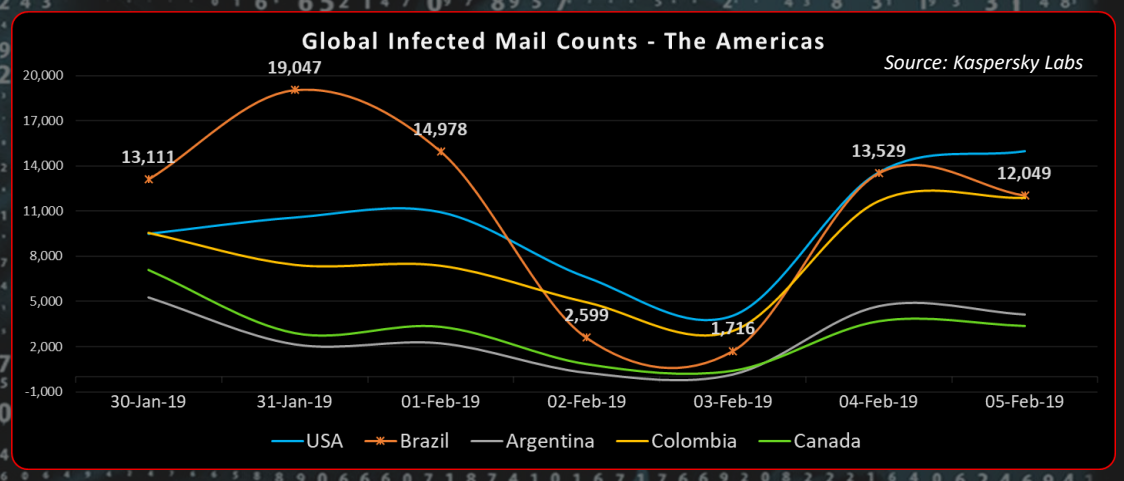
TOP Mail Infections for last week in the USA

#	KNOWN AS	(%)
1	Trojan-Downloader.Script.Generic	25.81%
2	DangerousObject.Multi.Generic	16.73%
3	Trojan.PDF.Badur.gen	5.16%
4	Exploit.MSOffice.CVE-2017-11882.gen	4.27%
5	Trojan-Downloader.MSOffice.SLoad.gen	4.27%
6	Backdoor.Win32.Androm.gen	3.44%
7	Worm.Win32.WBVB.vam	3.31%
8	Trojan.MSOffice.SAgent.gen	1.80%
9	Trojan.Script.Generic	1.59%
10	Exploit.MSOffice.CVE-2018-0802.gen	1.15%

Source: Kaspersky Labs

For Reporting Cyber Crime go to the Internet Crime Complaint Center (IC3) www.ic3.gov

According to Cybersecurity Ventures:
There may be **3.5** million unfilled cybersecurity jobs by 2021



Author: Chris Bester