On February 13, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in PHP, Apple, Adobe, Microsoft, and Mozilla products.

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

15 February 2019

In The News This Week

2018 Was Second-Most Active Year for Data Breaches

Hacking by external actors caused most breaches, but Web intrusions and exposures compromised more records, according to Risk Based Security. More than 6,500 data breaches were reported in 2018, a new report from Risk Based Security shows. The breaches, both big and small, were reported through to Dec. 31, 2018 — marking a **3.2% decline** from the 6,728 breaches reported in 2017 and making it the second-most active year for data breaches on record. Some 5 billion records were exposed, or about 36% less than the nearly 8 billion records exposed in breaches in 2017. In addition, more records were compromised last year than in any previous year than 2017 and 2005. As has been the case previously, a handful of mega breaches accounted for a vast proportion of the compromised records. In 2018, the 10 largest breaches accounted for approximately 3.6 billion exposed records — or a startling 70% of the total. In all, 12 breaches in 2018 exposed at least 100 million records. Organizations that disclosed the largest breaches last year included Facebook, Under Armor, Starwood Hotels, and Quora. For a vast majority of breaches, however, the number of exposed records was 10,000 or less — as has been the case since at least 2012. (Read the full article here: https://www.darkreading.com/)

Hacker Breaches Dozens of Sites, Puts 127 Million New Records Up for Sale

A hacker who was selling details of nearly 620 million online accounts stolen from 16 popular websites has now put up a second batch of 127 million records originating from 8 other sites for sale on the dark web. Last week, The Hacker News received an email from a Pakistani hacker who claims to have hacked dozens of popular websites (listed below) and selling their stolen databases online. During an interview with The Hacker News, the hacker also claimed that many targeted companies have probably no idea that they have been compromised and that their customers' data have already been sold to multiple cyber-criminal groups and individuals. In the first round, the hacker who goes by online alias "gnosticplayers" was selling details of 744 million accounts in 2 batches belonging to 24 compromised websites for less than $20,000 in Bitcoin on dark web marketplace Dream MarketOut of these, the popular photo-sharing service 500px has confirmed that the company suffered a data breach in July last year and that personal data, including full names, usernames, email addresses, password hashes, location, birth date, and gender, for all the roughly 14.8 million users existed at the time was exposed online. Artsy, DataCamp, CoffeeMeetsBagel, MyFitnessPal, MyHeritage, Animoto, Dubsmash and Houzz also confirmed that they were victims of a breach last year and that personal and account details of their customers was stolen by an unauthorized attacker. These collections have since been removed from sale on the dark web. (Read the full story by Swati Khandelwal and find a list of the compromised websites on https://thehackernews.com)

South Africans at higher risk for harmful online behaviour

South Africans are among the most at risk for exposure to negative behaviour online according to Microsoft's 2019 Digital Civility Index (DCI) which was released on Safer Internet Day 5 February 2019. The annual study examines the online behaviour of internet users in 22 countries and its release coincided with international Safer Internet Day (5 February). South African millennials and teenagers – particularly teenage girls – are most affected by online risks such as receiving offensive or obscene content, internet hoaxes and fake news, and bullying and offensive name-calling. (Read or download the report from here: https://www.microsoft.com/en-us/digital-skills/digital-civility?activetab=dci_reports%3aprimaryr6)

Understanding Your Computer: Email Clients

How do email clients work?

Every email address has two basic parts: the user name and the domain name. When you are sending email to someone else, your domain's server has to communicate with your recipient's domain server. For example, let's assume that your email address is johndoe@example.com, and the person you are contacting is at janesmith@anotherexample.org. In very basic terms, after you hit send, the server hosting your domain (example.com) looks at the email address and then contacts the server hosting the recipient's domain (anotherexample.org) to let it know that it has a message for someone at that domain. Once the connection has been established, the server hosting the recipient's domain (anotherexample.org) then looks at the user name of the email address and routes the message to that account.

How many email clients are there?

There are many different email clients and services, each with its own interface. Some are web-based applications, some are stand-alone applications installed directly on your computer, and some are text-based applications. There are also variations of many of these email clients that have been designed specifically for mobile devices such as cell phones.

How do you choose an email client?

There is usually an email client included with the installation of your operating system, but many other alternatives are available. Be wary of "home-brewed" software, because it may not be as secure or reliable as software that is tested and actively maintained. Some of the factors to consider when deciding which email client best suits your needs include: (1) security - Do you feel that your email program offers you the level of security you want for sending, receiving, and reading email messages? How does it handle attachments? If you are dealing with sensitive information, do you have the option of sending and receiving signed and/or encrypted? (2) privacy - If you are using a web-based service, have you read its privacy policy? Do you know what information is being collected and who has access to it? Are there options for filtering spam? (3) functionality - Does the software send, receive, and interpret email messages appropriately? (4) reliability - For web-based services, is the server reliable, or is your email frequently unavailable due to maintenance, security problems, a high volume of users, or other reasons? (5) availability - Do you need to be able to access your account from any computer? (6) ease of use - Are the menus and options easy to understand and use? (7) visual appeal - Do you find the interface appealing?

Each email client may have a different way of organizing drafted, sent, saved, and deleted mail. Familiarize yourself with the software so that you can find and store messages easily, and so that you don't unintentionally lose messages. Once you have chosen the software you want to use for your email, protect yourself and your contacts by following good security practices (see US-CERT Tips for more information).

Can you have use more than one email client?

You can have more than one email client, although you may have issues with compatibility. Some email accounts, such as those issued through your internet service provider (ISP) or place of employment, are only accessible from a computer that has appropriate privileges and settings for you to access that account. You can use any stand-alone email client to read those messages, but if you have more than one client installed on your machine, you should choose one as your default. When you click an email link in a browser or email message, your computer will open that default email client that you chose.

Most vendors give you the option to download their email software directly from their websites. Make sure to verify the authenticity of the site before downloading any files, and follow other good security practices, like using a firewall and keeping anti-virus software up to date, to further minimize risk.

You can also maintain free email accounts through browser-based email clients (e.g., Yahoo!, Hotmail, Gmail) that you can access from any computer. Because these accounts are maintained directly on the vendors' servers, they don't interfere with other email accounts.

Read the full article by Mindi McDowell here : **https://www.us-cert.gov/ncas/tips/ST04-023**

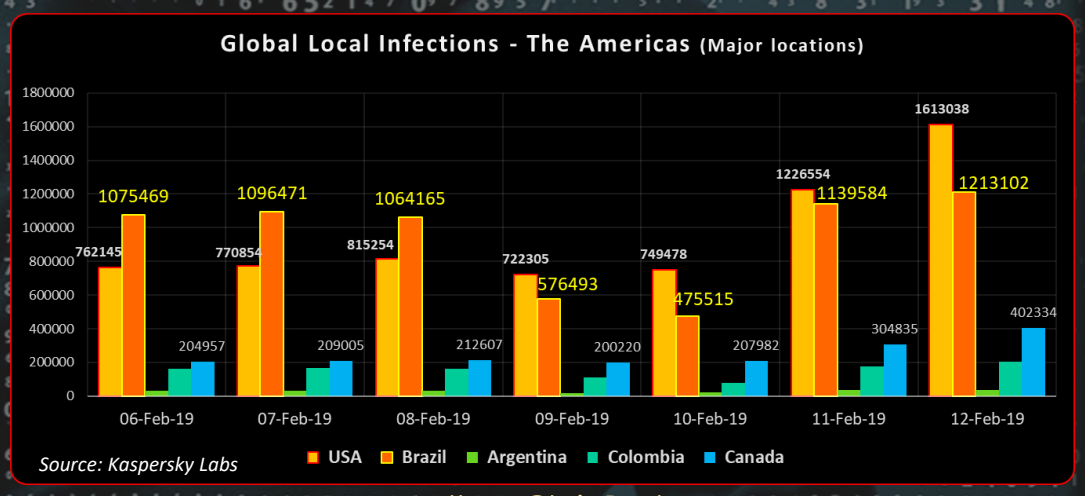
TOP Local Infections for last week in the USA

#	KNOWN AS	(%)
1	DangerousObject.Multi.Generic	15.75%
2	Hoax.Win32.PCFixer.c	6.21%
3	Trojan.Script.Generic	6.03%
4	Trojan-Ransom.AndroidOS.Svpeng.ah	3.64%
5	Hoax.MSIL.Optimizer.a	2.92%
6	Trojan.PDF.Alien.gen	2.62%
7	Net-Worm.Win32.Kido.ih	2.12%
8	Trojan.Win32.Runner.amo	1.95%
9	Trojan.MSOffice.SAgent.gen	1.71%
10	Trojan.Win32.Alien	1.68%

Source: Kaspersky Labs

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

According to Gartner, Security Spending Growth will Outpace IT Spending Growth in **2019**
Worldwide IT Security spending growth will jump by 8.7% this year, up to $124 billion.
IT spending growth will only see a 3.2% bump this year.



Author: Chris Bester