Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

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.

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

1 February 2019

In The News This Week

How UAE used U.S. mercenaries and a cyber super-weapon to spy on iPhones of foes

A team of former U.S. government intelligence operatives working for the United Arab Emirates hacked into the iPhones of activists, diplomats and rival foreign leaders with the help of a sophisticated spying tool called Karma, in a campaign that shows how potent cyber-weapons are proliferating beyond the world's superpowers and into the hands of smaller nations. The cyber tool allowed the small Gulf country to monitor hundreds of targets beginning in 2016, from the Emir of Qatar and a senior Turkish official to a Nobel Peace laureate human-rights activist in Yemen, according to five former operatives and program documents reviewed by Reuters. The sources interviewed by Reuters were not Emirati citizens. Karma was used by an offensive cyber operations unit in Abu Dhabi comprised of Emirati security officials and former American intelligence operatives working as contractors for the UAE's intelligence services. The existence of Karma and of the hacking unit, code named Project Raven, haven't been previously reported. Raven's activities are detailed in a separate story published by Reuters. The ex-Raven operatives described Karma as a tool that could remotely grant access to iPhones simply by uploading phone numbers or email accounts into an automated targeting system. The tool has limits — it doesn't work on Android devices and doesn't intercept phone calls. But it was unusually potent because, unlike many exploits, Karma did not require a target to click on a link sent to an iPhone, they said. In 2016 and 2017, Karma was used to obtain photos, emails, text messages and location information from targets' iPhones. The technique also helped the hackers harvest saved passwords, which could be used for other intrusions. It isn't clear whether the Karma hack remains in use. The former operatives said that by the end of 2017, security updates to Apple Inc's iPhone software had made Karma far less effective. The disclosure of Karma and the Raven unit comes amid an escalating cyber arms race, with rivals such as Qatar, Saudi Arabia and the UAE competing for the most sophisticated hacking tools and personnel.. (Read the full Reuters article here: www.nbcnews.com)

Liquid Telecom – Big network refresh and a few unlucky breaks.

In South Africa, Liquid Telecom had some unlucky breaks. While the company's network refresh project is behind certain network disruptions experienced by clients, the company has also been hit by two big fibre breaks in recent months. The first was **caused by copper thieves** who cut through and broke all conduits along a 2-kilometre stretch. This was along a major route for Liquid Telecom, which had a ripple effect on the systems used to re-route traffic. To restore this route new infrastructure had to be built, which took much longer than fixing a simple break. The second incident, which took place in late December, was caused by a burst water pipe in Randburg, a suburb on the west side of Johannesburg. The utility provider dug up the pavement to install new pipes, which resulted in ripping up an important fibre route which connects two primary points-of-presence and took a several days to fix. (Read story here https://mybroadband.co.za/)

Data Breaches Dent Singapore's Image as a Tech Innovator.

Singapore takes pride in being a technology hub where municipal decisions are driven by cutting-edge data science. "Data is the new currency, and with open data, the possibilities are endless!" the government says on its "smart nation" portal. But that image has been dented by two embarrassing data breaches. Last year, a cyberattack on Singapore's public health system compromised data from **1.5 million** people. And on Monday, the Health Ministry said that medical records for **14,200 H.I.V**.-positive people in the city-state had been obtained by an American whose Singaporean partner worked at the ministry. The ministry said it learned on Jan. 22 that the records had been illegally disclosed online. (Read the full story here: www.nytimes.com)

Understanding Bluetooth Technology and Security concerns around it

What is Bluetooth? Bluetooth is a technology that allows devices to communicate with each other without cables or wires. It is an electronics "standard," which means that manufacturers that want to include this feature have to incorporate specific requirements into their electronic devices. These specifications ensure that the devices can recognize and interact with other devices that use the Bluetooth technology. Many popular manufacturers are making devices that use Bluetooth technology. These devices include mobile phones, computers, and personal digital assistants (PDAs). The Bluetooth technology relies on short-range radio frequency, and any device that incorporates the technology can communicate as long as it is within the required distance. The technology is often used to allow two different types of devices to communicate with each other. For example, you may be able to operate your computer with a wireless keyboard, use a wireless headset to talk on your mobile phone, or add an appointment to your friend's PDA calendar from your own PDA.

What are some security concerns? Depending upon how it is configured, Bluetooth technology can be fairly secure. You can take advantage of its use of key authentication (see Understanding Digital Signatures for more information) and encryption (see Understanding Encryption for more information). Unfortunately, many Bluetooth devices rely on short numeric PIN numbers instead of more secure passwords or passphrases (see Choosing and Protecting Passwords for more information). If someone can "discover" your Bluetooth device, he or she may be able to send you unsolicited messages or abuse your Bluetooth service, which could cause you to be charged extra fees. Worse, an attacker may be able to find a way to access or corrupt your data. One example of this type of activity is "bluesnarfing," which refers to attackers using a Bluetooth connection to steal information off of your Bluetooth device. Also, viruses or other malicious code can take advantage of Bluetooth technology to infect other devices. If you are infected, your data may be corrupted, compromised, stolen, or lost. You should also be aware of attempts to convince you to send information to someone you do not trust over a Bluetooth connection (see Avoiding Social Engineering and Phishing Attacks for more information).

How can you protect yourself?

- ❖ Disable Bluetooth when you are not using it - Unless you are actively transferring information from one device to another, disable the technology to prevent unauthorized people from accessing it.
- ❖ Use Bluetooth in "hidden" mode - When you do have Bluetooth enabled, make sure it is "hidden," not "discoverable." The hidden mode prevents other Bluetooth devices from recognizing your device. This does not prevent you from using your Bluetooth devices together. You can "pair" devices so that they can find each other even if they are in hidden mode. Although the devices (for example, a mobile phone and a headset) will need to be in discoverable mode to initially locate each other, once they are "paired" they will always recognize each other without needing to rediscover the connection.
- ❖ Be careful where you use Bluetooth - Be aware of your environment when pairing devices or operating in discoverable mode. For example, if you are in a public wireless "hotspot," there is a greater risk that someone else may be able to intercept the connection (see Securing Wireless Networks for more information) than if you are in your home or your car.
- ❖ Evaluate your security settings - Most devices offer a variety of features that you can tailor to meet your needs and requirements. However, enabling certain features may leave you more vulnerable to being attacked, so disable any unnecessary features or Bluetooth connections. Examine your settings, particularly the security settings, and select options that meet your needs without putting you at increased risk. Make sure that all of your Bluetooth connections are configured to require a secure connection.
- ❖ Take advantage of security options - Learn what security options your Bluetooth device offers, and take advantage of features like authentication and encryption.

Read the full article by Mindi McDowell and Matt Lytle here : https://www.us-cert.gov/ncas/tips/ST05-015

TOP vulnerabilities registered for last week in the USA

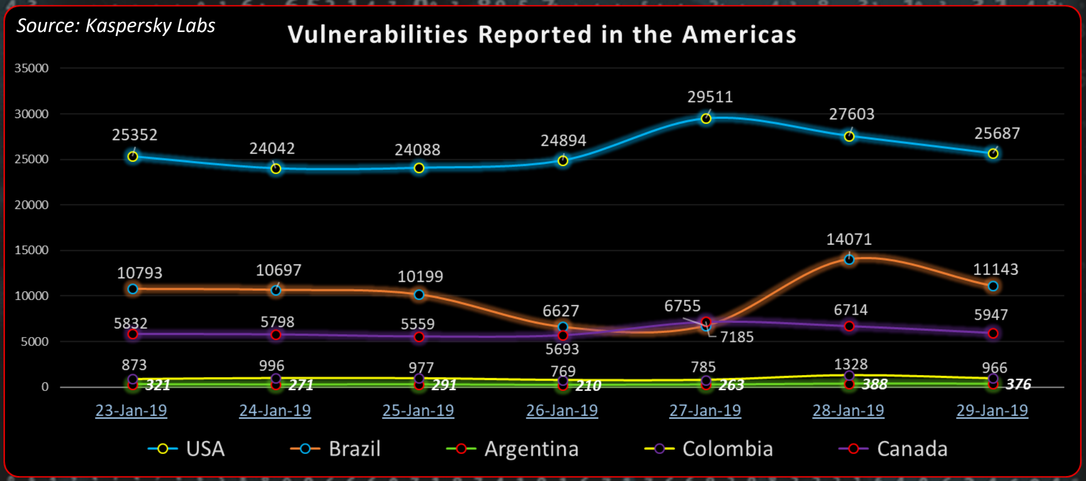
#	KNOWN AS	(%)
1	Exploit.MSOffice.CVE-2017-11882.gen	56.68%
2	Exploit.Script.Generic	20.61%
3	Exploit.Win32.CVE-2017-11882.gen	5.85%
4	Exploit.MSOffice.CVE-2017-11882.b	5.80%
5	Exploit.MSOffice.CVE-2017-8570.gen	3.31%
6	Exploit.MSOffice.Pederr.gen	0.90%
7	Exploit.MSOffice.CVE-2018-0802.gen	0.88%
8	Exploit.AndroidOS.Lotoor.a	0.61%
9	Exploit.OLE2.Wahel.a	0.43%
10	Exploit.PDF.Generic	0.40%

Source: Kaspersky Labs

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

According to Cyren's 2018 Email Security Gap Analysis Report:
(Out of 2.7 million sample emails inspected)
92.8% Were clean
6.9% Were SPAM
0.26% Were Phishing
0.04% Had Malware

Source: Kaspersky Labs



Author: Chris Bester