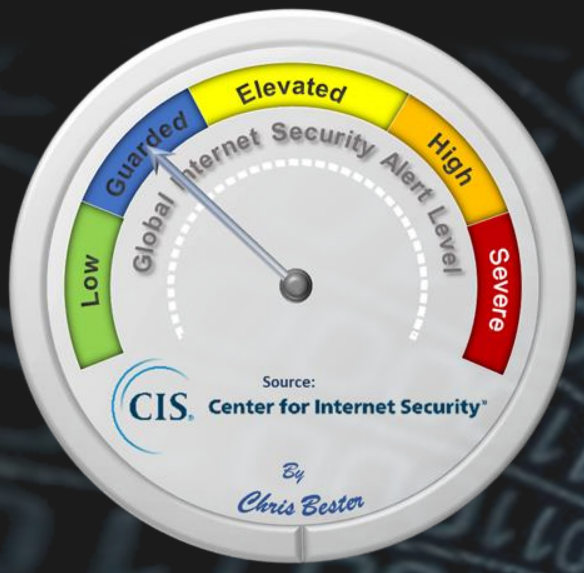

Low
Guarded
Elevated
High
Severe
Global Internet Security Alert Level
Source:
CIS. Center for Internet Security
By
Chris Bester

The last evaluation was done on May 29, 2019, and the Cyber Threat Alert Level is remaining at Blue (Guarded) due to a vulnerability affecting IBM and other 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

07 June 2019

In the News this week

NSA joins chorus urging Windows users to patch 'BlueKeep'.

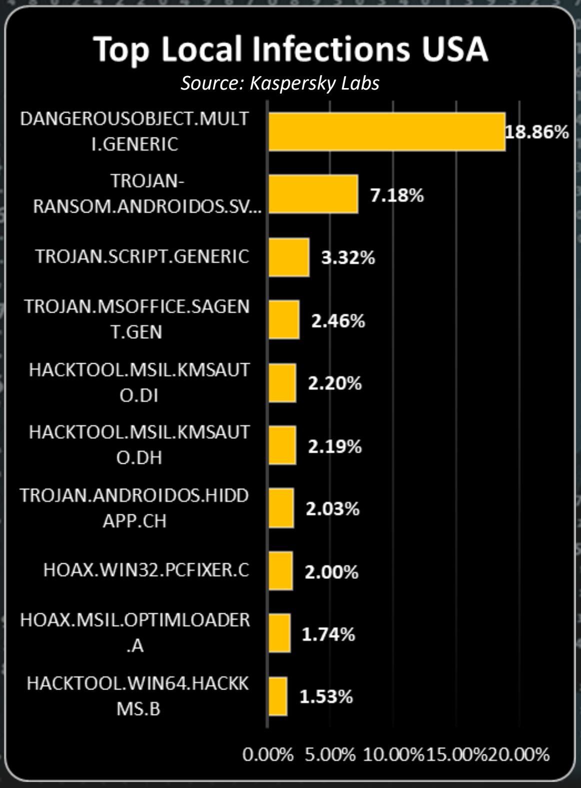
The United States' National Security Agency (NSA) has issued a rare alert urging Windows users and administrators to waste no time in patching the critical 'BlueKeep' security flaw in older Windows systems. "This is the type of vulnerability that malicious cyber actors frequently exploit using software code that specifically targets the vulnerability," reads the NSA's advisory. It also specifically highlights BlueKeep's 'wormable' nature and draws parallels between some major malware outbreaks in the past and the possible scenario now: "We have seen devastating computer worms inflict damage on unpatched systems with wide-ranging impact and are seeking to motivate increased protections against this flaw". Future exploits might use the flaw to propagate malware within or outside of networks in similar fashion to how, for instance, WannaCry spread a little more than two years ago. Tracked as CVE-2019-0708, BlueKeep is a Remote Code Execution (RCE) vulnerability in Remote Desktop Services of some older versions of Windows: Windows 7, Windows Server 2008 R2, Windows Server 2008, as well as out-of-support Windows XP and Windows Server 2003. Windows 8 and Windows 10 are not affected by the security hole. For those who don't know, Microsoft rolled out the patches for BlueKeep, along with the first patch-now alert, on Patch Tuesday on May 14. Late last month, the company issued a rare second warning, calling on the owners of affected systems to install the fix as soon as possible. Read the full story here: WeLiveSecurity

Cryptocurrency start-up hacks itself before hacker gets a chance to steal users funds.

If you're a cryptocurrency start-up, would you face a huge backlash by hacking your own customers to keep their funds safe if you know that a hacker is about to launch an attack and steal their funds? This is exactly what happened yesterday when the Komodo Platform learned about a backdoor in one of its older wallet apps named Agama. Knowing they had little time to act, the Komodo team said it used the same backdoor to extract users' funds from all impacted wallets and move them to a safe location, out of the hacker's reach. The tactic paid off, and 8 million Komodo coins and 96 bitcoins, worth nearly $13 million, were taken from users' vulnerable accounts before the hacker could get a chance to abuse the backdoor and steal users' funds. The backdoor in the Agama wallet app was discovered during an audit by the security team of the npm JavaScript package repository. Npm staff said they identified a malicious update for the electron-native-notify (version 1.1.6) JavaScript library, which contained code designed to steal cryptocurrency wallet seeds and other login passphrases specific to cryptocurrency apps. While initially, it did not make any sense for a library with a very limited feature-set to contain such an advanced functionality, after investigating the issue, npm staffers realized they were dealing with a supply-chain attack aimed at another app downstream, which was using the now-backdoored library. Read the full story here: ZDNet Article

U.K. Cybersecurity Official Says 5G Market Is 'Fundamentally Broken'

Ian Levy, technical director of the U.K.'s National Cyber Security Centre, said the providers of 5G equipment have little incentive to invest in security. Levy said on Thursday 6 June 2019 at the WSJ Pro Cybersecurity Executive Forum, the concentration of the 5G market in a handful of companies is "insane" and will increase security risks as the superfast networks are installed globally. Just five telecom-equipment manufacturers; Huawei Technologies Co., ZTE Corp., Nokia Corp., Ericsson AB and Samsung Electronics Co., supply 5G radio hardware and systems to carriers. Read the full story here: The Wall Street Journal



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

According to the US Federal Budget document

$15 billion

are set aside for Cyber Security for 2019

See it here:

Federal Cyber Security Budget

Smartphone Security (Part 4 of 5)

7. The seventh layer of protection: activate two-factor authentication on the accounts you use.

No matter if you have an Apple, Google, Microsoft or any other online account, activating two-factor authentication **(2FA)** is highly recommended. This will act as a second layer of security. Every time you'll want to sign in on a new device or from a new location, it will require you to verify your identity through a unique, time-sensitive code, that you'll receive via text message, voice call, mobile app or other means.

It's getting increasingly risky to use online services. You store a lot of your personal data in the cloud, and your credit cards are linked to accounts on retail websites. Hackers would love to get at your data, to empty your bank account, or to access your email account, using it for spam and phishing. And if someone can pretend they are you (steal your identity) they can cause innumerable problems to you and your finances. We also hear of an increasing number of data breaches (as often reported in this bulletin), where major websites, stores, or services have entire databases of user names and passwords hacked. These databases are then traded on the hacker underground, allowing anyone willing to pay a few cents per name to access your accounts. More and more websites and services are using two-step or two-factor authentication to provide an additional layer of security. This security technique verifies your identity when you log into a website or an online account by requiring you to both know something and have something (2 Factors). The thing you need to know is a user name and a password or a PIN; the thing you need to have is a mobile phone, or another device that can generate one-time codes. (Like an RSA Token). Most of the mainstream services you use offer two-factor authentication nowadays, and these include: Apple (iCloud and other services), Google (Gmail and other services), Microsoft Office 365, Yahoo!, PayPal (limited to certain countries), Dropbox, Facebook, Twitter, Instagram, LinkedIn, SnapChat, Tumblr, Most major banks and many more.

How Two-Factor Authentication Works: When you activate two-factor authentication for a website or a service, you generally provide your mobile phone number. (You can also use an app, but the phone is the most common method of using two-factor authentication.) Most forms of two-factor authentication ask you to sign in with your user name and password, and then enter a code that is sent to you via SMS. This method not only proves that you know something (the user name and password), but also that you have something (the mobile phone), which you have "registered" as a device to receive these codes. Generally, once you've used two-factor authentication on a specific device, you won't be asked to do so again on that device. Some services may only trust your device for 30 days or one year, and others may give you the option of trusting a device permanently. Some services will ask for 2FA if the detect that you are logging in from a new location or obviously if you are using a different device. The short of it though, **2FA** is a good thing)

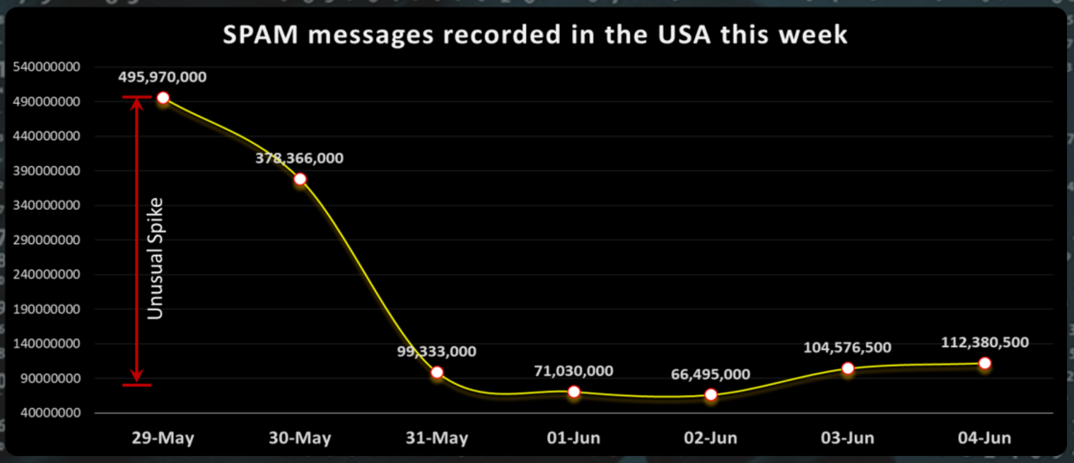
8. The eighth layer of protection: turn on encryption.

If your smartphone offers the option to encrypt the data on it, enable it. Once you encrypt it, the phone will ask you to set a password to unlock it and decrypt the data on it. Caution: If you forget your encryption password or pin, only a complete factory reset will get access back into the system. Unfortunately, the option to encrypt your data is only available for a limited number of operating systems, such as the latest Android versions and Apple's iOS . How to encrypt an iPhone or iPad: Enabling encryption on Apple's iPhone and iPad devices is relatively simple. The moment you set a passcode or enable Touch ID on the device running iOS 8 and above, the full device encryption is turned on automatically without you having to do anything. Here's how to go about doing this: (1) Launch the Settings app on your iPhone or iPad. (2) Select Touch ID & Passcode from the list of available options. (3) Now simply tap Turn Passcode On and enter in a passcode of your choice. A longer alphanumeric passcode is recommended but a six-digit PIN code will do as well. Avoid four-digit PINs as your passcode.

How to encrypt an Android device: As you might expect, the fragmented nature of the Android platform means that things can be a little more complex. The general rule of thumb with Android devices seems to be that the newer the software and hardware, the easier it is to enable encryption. If you have a relatively new Android device running Marshmallow and up, then like the iPhone, it's a case of invoking the Settings app and then heading to Security > Screen lock and adding a passcode for the lock screen. This instantly provides the device with a layer of security, and therefore enables encryption. Now to confirm if the encryption is enabled or not, head into Settings > Security > Encryption > Encrypt phone and make sure it reads "Encrypted". Caution! - Encryption invoked on an Android device that is not encrypted by default through the means of a lock code (as mentioned above) will erase all data on the phone.

To set up encryption on a Windows phone, please follow this link for instructions Windows Phone Encryption

Adapted from various sources and an article by Cristina Chipurici, which you can find here - HEIMDAL SECURITY



Author: Chris Bester