On May 29, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to a vulnerability affecting IBM 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

31 May 2019

In the News this week

Chinese military to replace Windows OS amid fears of US hacking.

Amidst an escalating trade war and political tensions with the US, Beijing officials have decided to develop a custom operating system that will replace the Windows OS on computers used by the Chinese military. The decision, while not made official through the government's normal press channels, was reported earlier this month by Canada-based military magazine Kanwa Asian Defence. Per the magazine, Chinese military officials won't be jumping ship from Windows to Linux but will develop a custom OS.

Thanks to the Snowden, Shadow Brokers, and Vault7 leaks, Beijing officials are well aware of the US' hefty arsenal of hacking tools, available for anything from smart TVs to Linux servers, and from routers to common desktop operating systems, such as Windows and Mac. Since these leaks have revealed that the US can hack into almost anything, the Chinese government's plan is to adopt a "security by obscurity" approach and run a custom operating system that will make it harder for foreign threat actors -- mainly the US -- to spy on Chinese military operations.

The task of developing the new OS and replacing Windows will fall to a new "Internet Security Information Leadership Group," as first reported by the Epoch Times, citing the May issue of the Kanwa Asian Defence magazine. Per the magazine, this new group answers directly to the Central Committee of the Chinese Communist Party (CCP), being separate from the rest of the military and intelligence apparatus.

This is similar to how the United States Cyber Command operates as a separate entity in the US Department of Defense, separate and independent from the other US military and intelligence agencies.

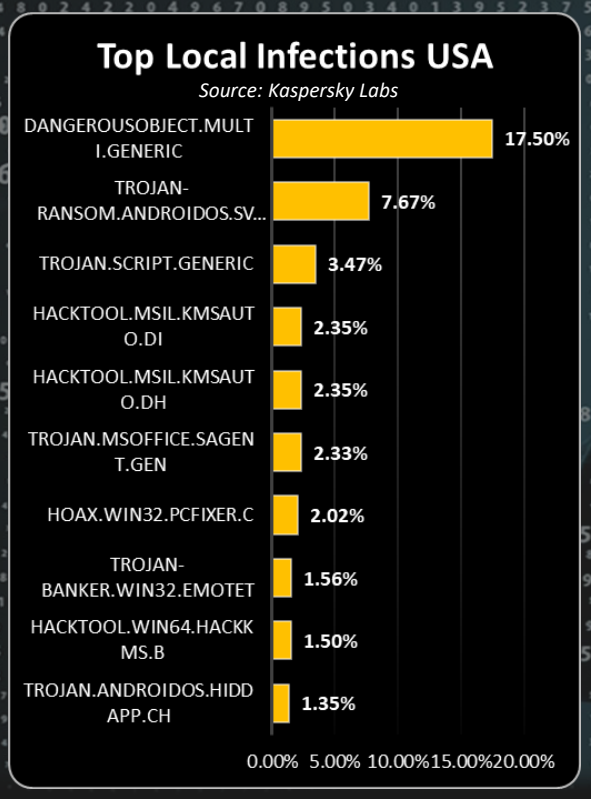
In the late 90s, North Korea also developed a custom operating system for use inside the country, called Red Star OS. The OS is still alive, it is a Linux distro, but it never became the "only" official OS for government agencies, which continued to use Windows, Mac, and Linux in parallel.

Read the full story by Catalin Cimpanu here: ZDNet Article

Chinese Hackers Infect Over 50,000 Windows MS-SQL and PHPMyAdmin Servers Worldwide with 20 Different Payloads.

A new China-based campaign dubbed Nansh0u targets Windows MS-SQL and PHPMyAdmin servers worldwide. The attack campaign primarily targets servers in the healthcare, telecommunications, media, and IT sectors. Guardicore Labs detected the campaign at the beginning of April but found that the attacks dated back to February 26. Throughout the campaign threat actors used 20 different payloads, and they keep on creating at least one payload a week and used them intermittently. "Hackers used a combined set of five attack servers, and six connect-back servers suggests an established process of continuous development which was well thought of by the attackers." More than 50,000 servers were breached in this campaign and once the targeted servers were compromised they were infected with a malicious payload, which in turn drops a crypto-miner that mines TurtleCoin and a sophisticated kernel-mode rootkit. Although crypto-mining is central, the Nansh0u campaign is not just a crypto-miner attack; hackers behind the campaign used advanced techniques followed by APTS groups such as fake certificates and privilege escalation exploits. In some instances the privilege escalation vulnerability CVE-2014-4113 was exploited to run the programs with SYSTEM privileges.

Adapted from an article in GBHackers – To read the full story and how the campaign works, go to GBHackers



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

Cybersecurity Ventures estimates that there are **111 billion** lines of new software code being produced each year

Smartphone Security (Part 3 of 5)

5. The fifth layer of protection: activate remote device locator.

In case your smartphone is ever lost or stolen, the easiest way to remotely locate it is by installing a dedicated app and making sure that the option to track its location is always turned on. For Apple's iOS there's the tracking solution called "Find my iPhone", Microsoft has "Find my device", and Android has "Android Device Manager"
Here is how you set it up:

On your iPhone, tap on the "Setting" icon, as shown on the left, and click on the "Apple ID, iCloud, iTunes & App Store" option right on top, this is the one that normally has your photo or picture that is associated with your Apple ID on. Now scroll down until you see the "**Find my iPhone**" tab and turn it on.

On Windows phones, sign in to your Microsoft account on your Windows device. Select the Start button, then tap on the "Settings" icon (see picture on the left), now select "Update & Security", tap on the "**Find My Device**" option and tap "Change" and then turn the setting to "On" if not on already.

For Android phones, tap on your device's "Settings" icon and tap on "Security & location" (If you don't see "Security & location", tap Google Security). Now tap on "**Find My Device**" and make sure it is turned on.

If this feature is activated on your phone, you can also remotely wipe or delete everything on your phone if it is lost or stolen. In today's world, you don't want those private pictures or any other data stored on you phone to get into the wrong hands. Click on one of the following links to find out more on how that works:

1.) Android 2.) iPhone or iPad 3.) Windows Phone

6. The sixth layer of protection: activate automatic backup

Have automatic backups in the cloud. This option is available on all operating systems, you just have to enable it (or don't disable it, in case it's already set as default). In case that your phone is lost, destroyed or stolen, you won't have to worry about the fact that you didn't get the chance to backup all your data on it. All apps and data will be automatically synchronized in the cloud.

Here's how you activate backup in Android if not set up already: Tap on the "Settings" icon that looks something like the picture on the left, now select "Backup & Reset", and select the option to have your data stored on their Google Drive. Now activate "Back up my data" and "Automictic restore" (to back up your Photos in Android, you'll have to go in the Photos app and configure it separately – you can choose what folders to backup and at what size to upload the photos)

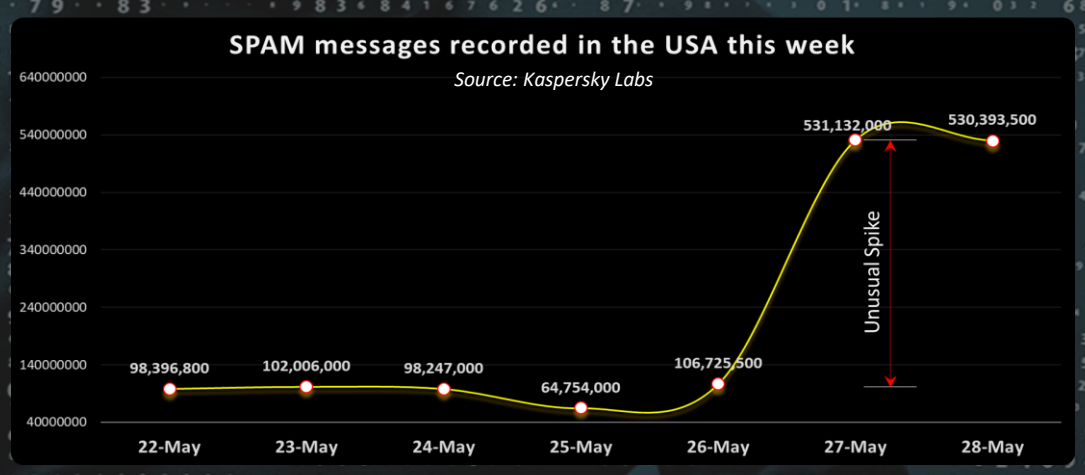
On your iPhone, tap on the "Setting" icon, as shown on the left, and then tap on the "Apple ID, iCloud, iTunes & App Store" option right on top, this is the one that normally has your photo or picture that is associated with your Apple ID on. Now scroll down until you see the "iCloud Backup" tab and turn it on.

On your Windows phone, from the Start screen, slide left and select the "Settings" icon then find and select "Backup". Now tap "App list + settings" and then tap on the "App backup" switch to turn it on. If necessary, sign in to your Microsoft account.

When you set up a new device, you will just have to enter the credentials for your Apple, Google or Microsoft account, and all apps, settings, and data will be automatically restored. You can also set up your data to automatically backup in other accounts, such as Dropbox.

Note: If you don't want to quickly exhaust the internet traffic allocation included in your data plan, set it up to backup only when it connects to wi-fi.

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



Author: Chris Bester