On May 8, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to vulnerabilities in Cisco 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

17 May 2019

In the News this week

WhatsApp Hack, what really happened?

By now most of you have heard that Facebook-owned WhatsApp, revealed a security flaw allowing hackers to inject spyware on smartphones and it raised fresh concerns about the security of the mobile ecosystem. What happened? Hackers were able to remotely install surveillance software on phones and other devices using a major security hole or vulnerability in the app.

The attackers could inject malware to gain access to both Android or Apple smartphones.

How does the security flaw work?

Attackers used WhatsApp's voice calling function to ring a target's device. Even if the call was not picked up, the surveillance software could be installed. The call would often disappear from the device's call log depending on the phone. The perpetrators could then listen in on conversations, read messages posted and some say even access the phone's camera.

A fix was rolled out last Friday and on Monday, WhatsApp urged all of its 1.5 billion users to update their apps as an added precaution. "Journalists, lawyers, activists and human rights defenders" are most likely to have been targeted according to some sources.

WhatsApp promotes itself as a "secure" communications app because messages are end-to-end encrypted, meaning they should only be displayed in a legible form on the sender or recipient's device. However, the surveillance software would have let an attacker read the messages on the target's device.

Who is behind the software?

The NSO Group is an Israeli company that has been referred to in the past as a "cyber-arms dealer". The NSO Group is part-owned by the London-based private equity firm Novalpina Capital, which acquired a stake in February. NSO's flagship software, Pegasus, has the ability to collect intimate data from a target device, including capturing data through the microphone and camera, and gathering location data.

In a statement, the group said: "NSO's technology is licensed to authorised government agencies for the sole purpose of fighting crime and terror. "The company does not operate the system, and after a rigorous licensing and vetting process, intelligence and law enforcement determine how to use the technology to support their public safety missions. Under no circumstances would NSO be involved in the operating or identifying of targets of its technology, which is solely operated by intelligence and law enforcement agencies. NSO would not or could not use its technology in its own right to target any person or organisation."

The NSO also stated "We investigate any credible allegations of misuse and if necessary, we take action, including shutting down the system.

While the flaw was discovered in WhatsApp, security experts say any application could have been a "vehicle" for the spyware payload.

Although it is known what software were used, it is still uncertain who sits behind the attack but the consensus so far is that is state sponsored campaign, which state? Who knows? A WhatsApp spokesman said the attack was sophisticated and had all the hallmarks of a "private company working with governments on surveillance." - *Compiled from various sources*.

Smartphone Security (Part 1 of 5)

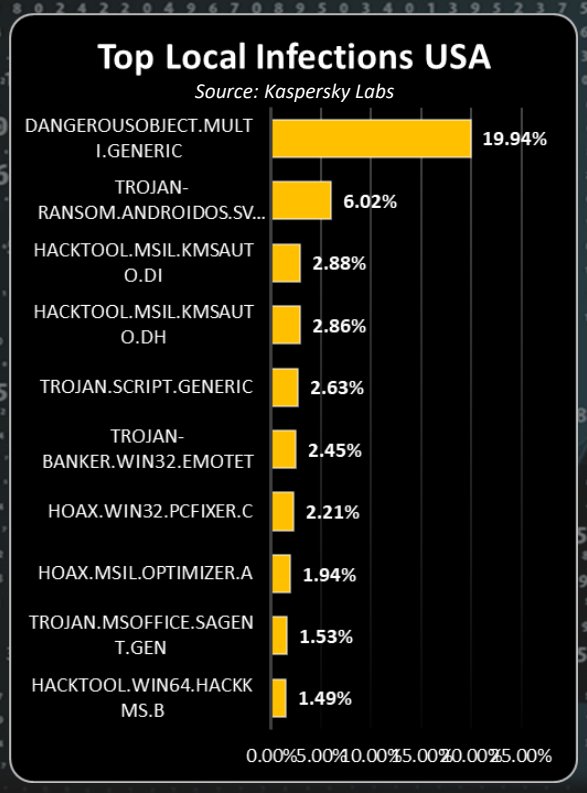
1. The first layer of protection: Activate a screen lock

Activate a screen lock after a short period of inactivity (30 seconds, for example), your phone should auto-lock itself. This is the most basic and essential security control. Most smartphones also give you the option to enforce automatic wiping of the device after 10 failed login attempts. The reason behind this is that you can never know where you'll accidentally forget your phone and who will end up accessing it. No matter how protective you are with it, there's no guarantee that it won't end up stolen one day. You can simply leave it on your table while in a bar or at work for a quick break, and someone will peek into it. Or, even worse, install a keylogger or screen recorder on it. And now, moving on to the details; if you can, don't use a PIN code for locking the screen. Instead, just like any other password, use a unique password that's long enough and mixes letters with digits and symbols. Some phones gives you the option to lock your screen using a pattern. Choose a complicated one and then deactivate the option that makes it visible when you enter it. You can also use your fingerprint to wake and unlock your phone in addition to the pattern. (if the option is available). Biometrics is one of the most secure ways of authenticating oneself, because it's so difficult to replicate the data. While we do leave our fingerprints everywhere, it's much easier for someone to spy on you from behind your shoulder while you enter your PIN than try to replicate your fingerprints. With the latest iPhone, Apple brings back facial technology that's been present on smartphones in the past but improves it tremendously. If in the past you could fool a phone into unlocking by holding a picture of its owner to the sensor, with Face ID things are different. iPhone X's Face ID uses a host of sensors to map your face in 3D. An infrared light illuminates your face and a projector maps it using an array of infrared dots, then an IR camera snaps an image of those dots and compares it to the image already stored in the phone. According to Apple, Face ID is so secure that it's a one in a million chance someone could spoof your image. I'm sure Android will follow suit.

2. The second layer of protection: Mind your APP's

Cases of smartphones that got infected with viruses and malware have been on a rise. Some of them ended up with annoying adware, while others were infected with ransomware. The Apple ecosystem is extremely targeted by cyber crooks, as iPhone owners are considered to be more wealthy and likely to pay a ransom. In general, devices with iOS are generally considered to be safer than Android because of two main reasons: (1) Market fragmentation: Google allowed every phone manufacturer to personalize its own Android version. While this is also a strength, it's also harder to control the security for every device that runs on Android, exposing users more to potential bugs. (2) Google is also more permissive with the apps that they allow in their official store. Unlike Apple, Google doesn't check as thoroughly the apps that they allow users to install. Of course, this is just a simplified view of the two biggest operating systems existent in the mobile market at this point. They both have their advantages and disadvantages when it comes to cybersecurity. What you should keep in mind is that bugs and vulnerabilities will always exist, no matter what operating system you use. Here's what you can do about apps to decrease your chances to be infected: (a) Always use official app stores to download and install an app. Disable the option to allow installation of third party apps. Third party apps usually carry malware that will harm your smartphone.? (b) Only install applications that you find in the official app store. That means no apps from third parties – no matter if those third parties are your online buddies, ads, blogs or torrents. (c) If you have Android, you can disable the option to allow installation of apps from sources other than the Play Store (from Settings -> Security). Fortunately, since Android Oreo, Google now asks you to give permission to download apps on each and every app – it's no longer a general setting, it's on a case by case basis. However, this doesn't mean that an app or game from the official store is 100% secure – sometimes, even popular apps, with more than 5 million downloads, has been infected in the past. (d) Check the permissions for installed apps. If anything looks out of order, then deny them access to what they're requesting. A flashlight app doesn't need permission to access your text messages or contacts, right? If you have Android, you can go to Settings -> Apps -> App permissions and check exactly what apps required permissions. (e) Do a spring clean-up of your apps. Look at all the installed apps and remove the ones you're not using anymore. Those are potential security risks and it's better to be safe than sorry. (f) Also check out the apps that consume the most battery, data or memory to see if there's anything suspicious around there. Look for significant changes – this way, you can detect if your smartphone has been compromised. (g) Update your apps. With each app that remains outdated, including commonplace browsers, your phone is more vulnerable to infections. All it takes is clicking on a link that will redirect you to an infected website – it can be a link from an ad, a spam email, or your friend's social account that got hacked. Outdated apps leave your data exposed to attacks.

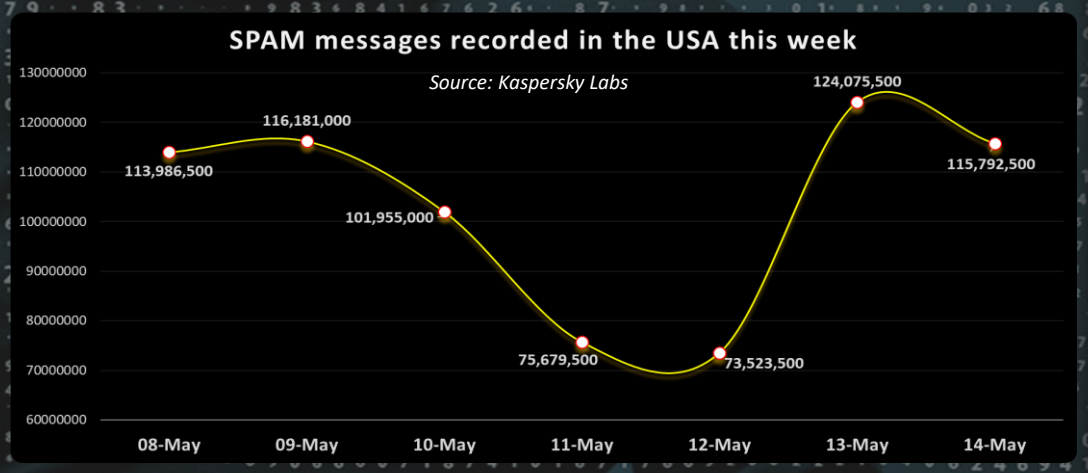
Adapted from an article by Cristina Chipurici, which you can find here - HEIMDAL SECURITY



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

According to the Identity Theft Resource Center

Hackers stole nearly **447 million** consumer records containing sensitive personal information last year



AUTHOR: CHRIS BESTER