As last reviewed On June 19, 2019, the Cyber Threat Alert Level was evaluated and is remaining at Blue (Guarded) due to multiple vulnerabilities in Mozilla Thunderbird and Firefox products. (Unchanged)

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

12 July 2019

In The News This Week

25 Million Android Users Infected with Powerful "Agent Smith" Malware.

Check Point Researchers recently discovered a new variant of mobile malware that quietly infected around 25 million devices, while the user remains completely unaware. Disguised as Google related app, the core part of malware exploits various known Android vulnerabilities and automatically replaces installed apps on the device with malicious versions without the user's interaction. This unique on-device, just-in-time (JIT) approach inspired researchers to dub this malware as "Agent Smith". It currently uses its broad access to the device's resources to show fraudulent ads for financial gain. This activity resembles previous campaigns such as Gooligan, HummingBad and CopyCat. The primary targets, so far, are based in India though other Asian countries such as Pakistan and Bangladesh are also affected. According to Neowin.net, "Agent Smith" is mainly distributed via the 9Apps app store commonly used in Asia but infected apps were also downloaded from Google's Play Store.

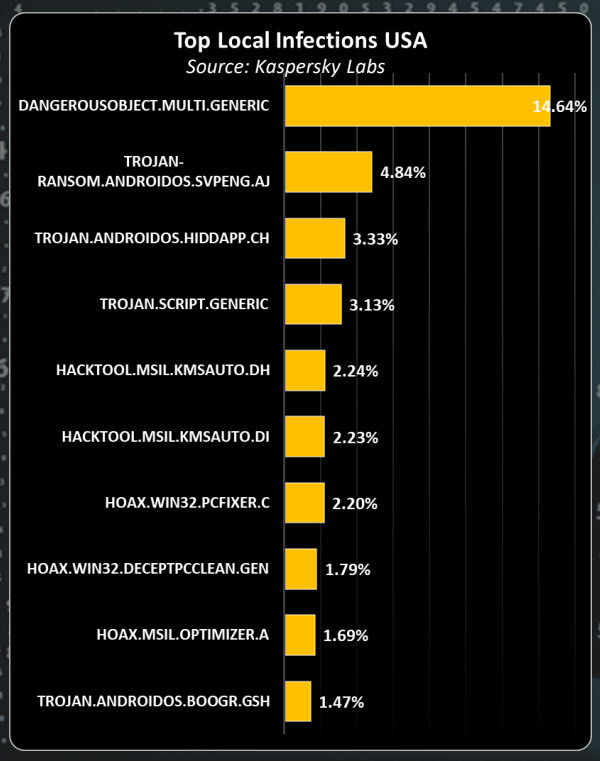
In a much-improved Android security environment, the actors behind Agent Smith seem to have moved into the more complex world of constantly searching for new loopholes, such as Janus, Bundle and Man-in-the-Disk, to achieve a 3-stage infection chain, in order to build a botnet of controlled devices to earn profit for the perpetrator. "Agent Smith" is possibly the first campaign seen that ingrates and weaponized all these loopholes and are described in detail the Check Point Research Report. In this case, "Agent Smith" is being used to for financial gain through the use of malicious advertisements. However, it could easily be used for far more intrusive and harmful purposes such as banking credential theft. Indeed, due to its ability to hide its icon from the launcher and impersonates any popular existing apps on a device, there are endless possibilities for this sort of malware to harm a user's device. Check Point Research has submitted data to Google and law enforcement units to facilitate further investigation. As a result, information related to the malicious actor is tentatively redacted in this publication. Check Point has worked closely with Google and at the time of publishing, no malicious apps remain on the Google Play Store.

Read the full story here: Check Point Research Report

Europe's huge privacy fines against Marriott and British Airways, a warning to others.

British Airways and Marriott received the largest-ever fines under the EU's new General Data Protection Regulation this past week. The U.K. Information Commissioner's Office (ICO) fined British Airways a proposed **$230 million** for an incident that took place from June to September 2018 and compromised the data of 500,000 customers. The ICO gave Marriott a **$123 million** proposed penalty for the loss of 339 million guest records, reported in November 2018. Both companies already indicated they will appeal the decision.

But the GDPR fines were important for reasons well beyond numbers. The GDPR is a very broad rule with little detail, and companies have had few insights into how regulators in the EU would interpret the law, particularly what they would consider "adequate" security measures. The maximum GDPR fine is 4% of a company's global turnover. The fines for BA and Marriott both represented 1.5% of their respective turnover, and the commission said both companies cooperated fully with their respective investigations. This makes the stakes particularly high for tech companies like Google and Facebook, which are either currently under investigation in the EU, and for whom the legislation essentially was tailor-made. Google could face a fine of up to $5 billion, and Facebook up to $2.2 billion, based on both companies' annual revenue in 2018. Read the full story here: CNBC



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

Available Apps in App stores as per Statista, May 2019

Google Play
2,100,000
Apple App Store
1,800,000
Windows Sore
669000
Amazon Appstore
475000

Third-Party vs Official APP Stores, how exposed am I?

Following the news story this week of "Agent Smith" and many similar cases reported, we ask the question of how big is my exposure from a security perspective if I download and use third-part apps or apps from third-party app stores.

First lets see what is a third-party application?

A third-party app is a software application made by someone other than the manufacturer of a mobile device or its operating system. For instance, app development companies or individual developers create a lot of applications for Apple's or Google's operating systems. Those manufacturers also create applications for their own devices. In that case, it's called a first-party or "native" app. But the vast majority of available applications are third-party apps.

Here's how it works. An email application that comes with your mobile device, likely with the manufacturer's name on it, would be a native app. If your roommate develops an app that dispenses advice from "mom" for any life situation, that's a third-party app.

Official app stores vs. third-party app stores

Apple® AppStore and Google Play™ are the two biggest official app stores. You can go there to download mobile applications for your iPhone or Android device. Each distribution platform includes native applications, the apps Apple built for its iOS operating system and Google built for Android devices. Both platforms also include third-party apps, millions of them. Developers or companies (third parties) not Apple or Google, create the apps to work on iOS, Windows or Android devices.

Are they safe?

Third-party apps in the official app stores usually follow strict development criteria. The stores also vet the applications for bad stuff like malware. Third-party app stores may not apply the same level of scrutiny toward the apps they allow to be listed in their app stores. Still, it can get tricky, third-party app stores might offer mostly safe applications, but there's a higher chance that they might offer malicious or dangerous apps. And those apps can include malicious code, viruses, trojans, ransomware, etc. Triggered advertisements or code can be "injected" into some of the most popular apps that you might consider buying or to download through these so-called third-party stores. These stores might offer popular apps for cheaper prices, which may sound appealing, but can put privacy at risk and can ultimately make you a target for financial fraud. For example, third-party apps bought or downloaded from third-party app stores may harvest sensitive information like Phone numbers, Banking details, Device information, Email addresses, Physical address and current location, etc. (if they know where you live and your current location is at some popular resort, they know you are not at home and your house might be unguarded)

Are third-party APP stores all the same?

It's important to keep in mind that not every third-party app store poses the same level of risk and is in some cases the user's only option. For instance, Google Play is not available in all countries and many users in those countries would rely on apps that may be legitimate from another app store. Also, some apps are not available in official app stores for specific countries and the same applies for those. The one thing third-party app stores have in common; they are not restricted, meaning, the operating systems' owners don't control them. App developers often find that lack of restriction attractive for mainly 2 reasons; (1) They might be able to target their audiences in ways they can't through official app stores, and (2) They may get more exposure for their apps in a "niche" market. For this reason, you might be tempted to download an app from these third-party stores, but you can't be sure how secure they are. At least you know that Google and Apple are large organisations with very public and transparent security policies and they stand much to loose if they breach governing laws.

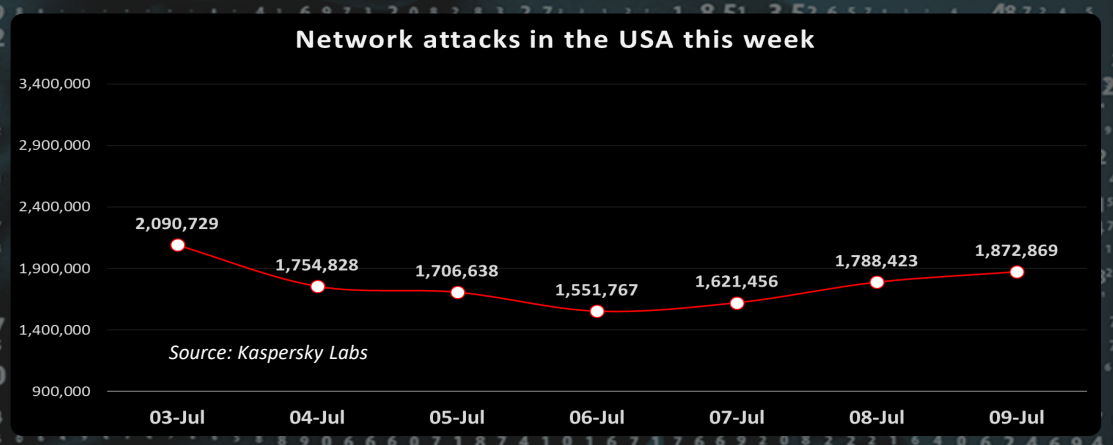
What can you do to help stay safe when buying from third-party app stores?

The obvious way to minimize danger from third-party APP stores is to avoid them. But, even if you do, it's also possible to download an app from one of the official app stores and have your device subject to malware.

So how do you keep your device and your personal information safe? It's part common sense, and it's part protection. For instance, it's a good idea to do some research before downloading an app, Google it and see if anyone posted something that could pose a question on how secure or genuine the app may be. Also, never trust apps offered via unsolicited emails, more often than not they are not exactly what they claim to be.

Protect yourself by installing security products to safeguard your device and private data. Many security products offer malware protection and has features that scans and removes apps with viruses, spyware, and other threats.

Adapted from an article by Symantec that you can find here: Norton Article



AUTHOR: CHRIS BESTER
chris.bester@yahoo.com