Marble Labs Mobile Threat Report, February 2015

US Publishers Are Responsible for Most Malicious and Risky Apps, Putting Everyone with a **Smartphone** at Risk

It's a common misconception that the risk of using mobile devices is limited to jailbroken or rooted devices in Asia, and apps that are downloaded from fly-by-night app stores other than the Apple App Store or Google Play. Nothing can be further from the truth.

Executive Summary

After analyzing more than one million apps available on the North American versions of the Apple App Store or Google Play, that *do not* require a jailbroken or rooted device, Marble Labs has determined that more than 40 percent of the world's dangerous mobile apps are developed and distributed by publishers based in the United States. This came as a bit of a surprise to Marble's analysts, who before examining the data would have bet that most malicious apps originated from publishers in Eastern Europe or Asia. While China, Korea, India and Taiwan generate a great number of malicious and risky apps, their combined total doesn't amount to that of the United States. This research further underscores that consumers and businesses need to pay close attention to what apps they download onto their mobile devices, and how those apps use or misuse personal data.

What is a Malicious or Highly Risky App?

For this study, Marble Labs examined apps that are malicious or highly risky. These are apps that:

- Send user's private data without their knowledge
- Copy contact databases and send them to untrusted locations on the Internet without the user's knowledge
- Send users' browser histories over the Internet
- Install helper apps to display unwanted advertising
- Communicate prohibited tracking information, including hardware identifiers
- Send premium rate SMS messages to defraud consumers
- Attempt to jailbreak or root mobile devices without a user's knowledge
- Lead users to malicious phishing websites
- Exfiltrate user data without a stated privacy policy
- Expose a user's contacts to spammers
- Have security vulnerabilities that expose user data

Apps with malicious behavior routinely skirt the security vetting of major app stores. For example, an app may request access to your contact database, but does not disclose the fact that it uploads your entire contact database to third party servers, perhaps insecurely, and that this data is sold or used to target your contacts who might be colleagues at work.

Another example is a mobile app that allows users to access images stored in their Dropbox account, and once given access, rifles through all the online data and sends files of interest to an outside server.

Some Android apps present users with a dizzying list of permissions, which must be granted, for the app to function. Among those permissions may be the app's ability to send the user's entire web browsing history along with detailed hardware identifying information over the Internet, allowing advertisers or attackers to target users or their employers.

Which Countries Publish The Greatest Number of Dangerous Apps?

It is a commonly held belief that Chinese or Russian app developers are responsible for the majority of malicious and highly risky apps. While that may be true for malware that targets jailbroken iPhones or rooted Android mobile devices, when we looked at apps that are available on legitimate app stores for non-tampered devices, the story is very different.

In fact, United States companies publish the largest number of malicious or highly risky apps in the world. More than 42 percent of global dangerous apps that target non-jailbroken and non-rooted devices originate with companies or publishers purportedly located in the United States.

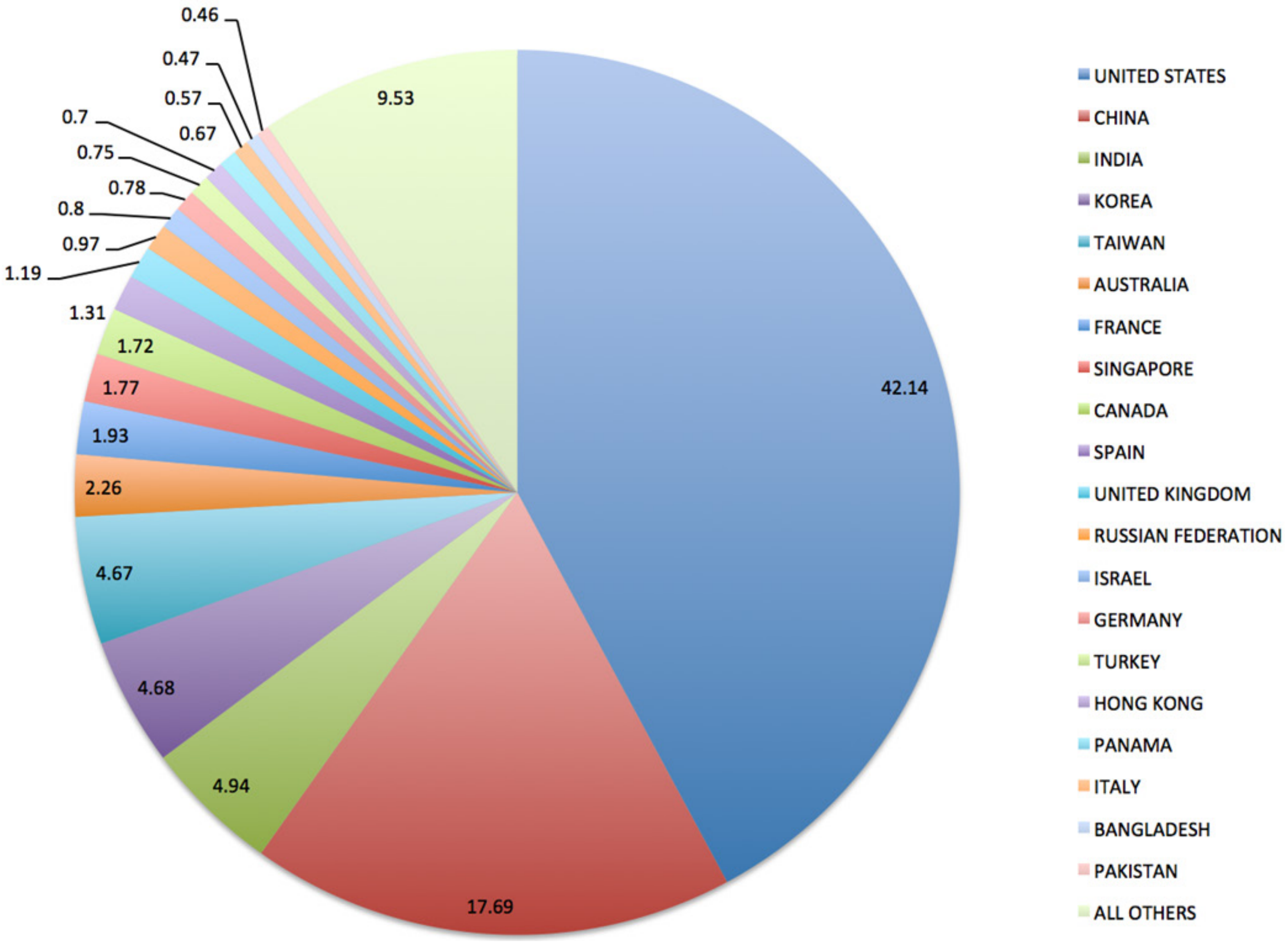
China is the second largest publisher of malicious and highly risky apps for standard iOS and Android devices, at almost 18 percent of the world's output. India, Korea and Taiwan follow, with approximately 4.5 percent of all published apps from those countries categorized as highly risky and malicious apps.

What Are The Chances That An App You Download is Malicious or Highly Risky?

Marble examined the risk that a downloaded app is malicious or highly risky and determined its country of origin. The graph below shows the top 10 countries that have published more than 100 highly risky or malicious apps on the Apple App Store or Google Play.

To clarify, the following graph only considers countries whose publishers have published more than 100 malicious or highly risky apps. For example, apps from countries such as Latvia, often associated with banking cyber crime, have a 6.5 percent chance of being malicious or highly risky. However, we have only analyzed 184 apps that originate from Latvia. While 12 of those apps are dangerous, it does not exceed our threshold of 100 risky apps. By contrast, we have detected more than 4,300 malicious or highly risky apps that originate in the United States and are available on the Apple App Store or Google Play.

Global Percentage of Malicious and Highly Risky Apps by Country

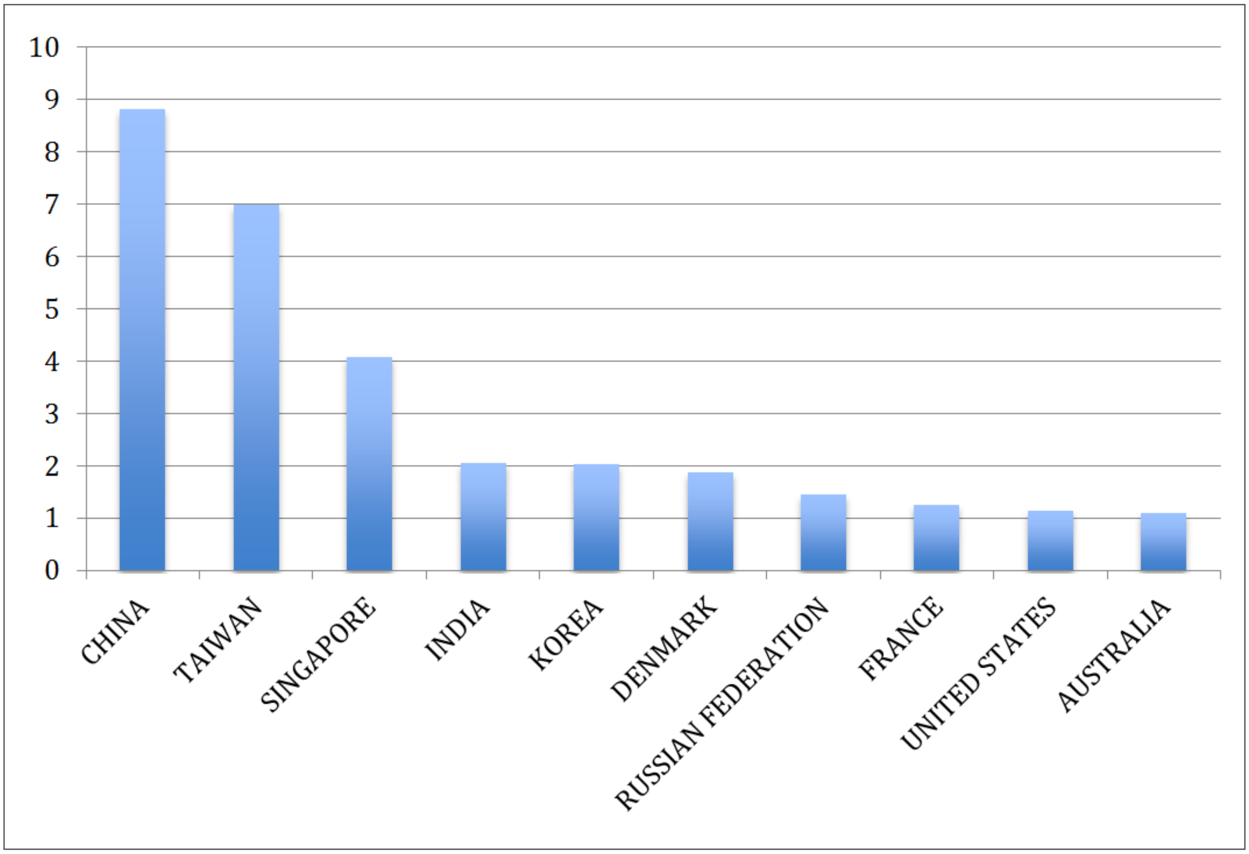


There is an 8.8 percent chance that an app that was written by a publisher based in China is highly risky or malicious. Apps from Taiwan have a 7 percent chance of being highly risky or malicious, while apps from India have only a 2 percent chance of such dangers. About 1.1 percent of apps originating from the US are malicious or highly risky.

Summary

A common misconception is that only mobile users with jailbroken iPhones or rooted Android devices are at risk from malicious apps. Many also believe that all dangerous apps originate from China or Russia.

Likelihood that an app from these countries is malicious or highly risky



Our research indicates that all mobile users with standard iPhones, iPads and Android devices are at risk from malicious and highly risky apps. These apps are widely available on the Apple App Store and Google Play, and users needn't download apps from illegitimate locations to acquire them. In fact, most users do not know where their apps were written.

The overwhelming majority of malicious and highly risky apps originate from companies located in the United States.

However, it is true that one of every 10 apps developed by Chinese developers are malicious or highly risky. Note that this analysis considers apps that are published on the Apple App Store and Google Play that are available to North American consumers and business users.

Therefore, consumers and businesses need to pay close attention to what apps they download on their mobile devices, even if those devices are not jailbroken or rooted. Malicious and highly risky apps can come from companies, individuals and criminals from all over the world.

MARBLE
SECURITY

Marble Security, Inc.
68 Willow Road
Menlo Park, CA 94025

T: 855.737.4370
sales@marblesecurity.com

www.marblesecurity.com