Mobile Malware Skyrockets in 2016

Published April 3, 2017

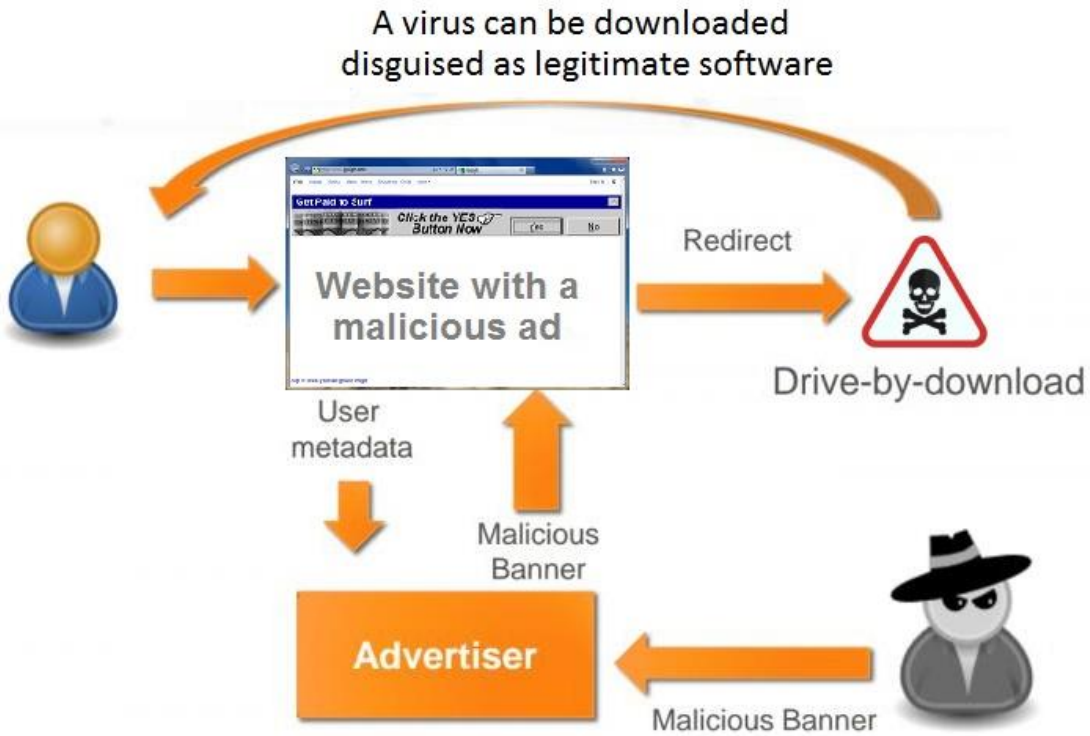
It was a productive year for those who like to spread mobile malware. Kaspersky researchers wrote in the company's annual Mobile Virusology report that mobile malware detections increased 3.5 times over the last year to 8.5 million.

There were three primary culprits contributing to the numbers:

- Malvertising
- Mobile Banking Trojans
- Ransomware

Malvertising

This type of malware increased 8.5 times in 2016. It targeted over 153,000 unique users too. Sr. malware analyst, Roman Unuchek of Kaspersky noted that these advertising trojans were the top threat. It is believed that they are taking advantage of unpatched devices and those that are not updated for various reasons. One is that users just don't apply the updates and patches when they are made available. The other is that manufacturers of mobile devices don't release them in a timely enough manner and the cybercriminals get to them first.

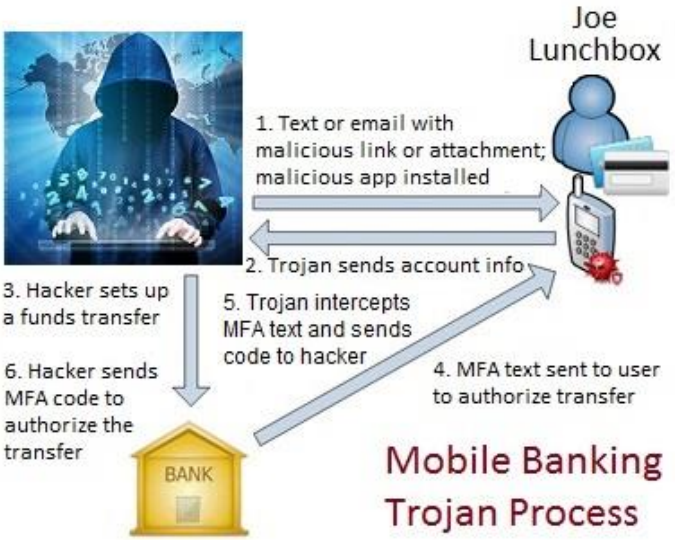


These are dangerous trojans and can wreak a lot of havoc if they do infect a device. They can potentially gain root or administrator access, which will allow them to perform all kinds of tasks such as display unwanted ads that may merely be annoying, change settings so that they cannot be restored to factory defaults, or hold a device for ransom. They can also exploit other vulnerabilities that have not been patched.

Users can thwart these tasks by always updating their devices right away when that little indicator pops up on the screen. Additionally, it may help to notify the various cellular service providers that you would like to have these updates as soon as the manufacturers release them. Some companies have been accused of holding them back in hopes that users will choose to upgrade their devices rather than patch their current ones. If you suspect your carrier is doing this, make sure it knows that's not acceptable to you.

Mobile Banking Trojans

These increased 1.6 times over 2015. The Marcher family of banking trojans was found to be particularly troublesome. It added additional "features" that allowed it to bypass security mechanisms to steal user information, overlay legitimate banking apps and redirect users to phishing sites where credentials and other sensitive information could be gathered.



Phishing will likely be around for the foreseeable future. It continues to work, partly because users will always be vulnerable to it, but also because the phishers are getting very crafty in creating realistic looking messages, websites, and apps. While the basics of detecting phishing are, and will likely remain the same for a very long time, email messages that try to trick users are becoming far more difficult to filter out using technology and human intervention. They can appear to come from someone familiar and can include attachments that execute malware when opened.

That is why you should always assume that <u>any</u> attachment that arrives *unexpectedly* is suspect. Verify that it is safe to open with the sender before doing so. If any doubt remains, just don't take the risk.

Ransomware

This can be particularly nasty. Years ago, ransomware cybercriminals went after individuals who, they hoped, just could not do without their precious photos or documents. As it happened, they became very successful at accumulating significant wealth $100-200 at a time by holding this information hostage. Of course they quickly determined that it's likely they could get far more out of businesses and organizations by holding their data hostage. And they have indeed been successful at getting paid by law enforcement agencies, hospitals, and others to the tune of $10,000 or more per instance.

Backing up devices is one way to make sure you don't feel the need to pay a criminal for your own data. Get into the habit of doing this regularly and make sure the backup copy is kept in a separate location from the device you're backing up. External hard drives are relatively inexpensive these days, are very easy to use, and can save you a lot of headache should your device get locked up with ransomware. If you have just a few files that you can't live without, you can use a USB drive just as well.

One particularly popular bit of malware that Kaspersky noted causing problems in 2016 was an app that made it into the Google Play store loaded with malware. It was supposedly a Pokémon Go Guide and was downloaded approximately 500,000 times. However, the only way to get the Pokémon Go game on Android, was to sideload it from other sites. While obviously getting apps exclusively from the official stores does not guarantee safe apps, it does mitigate the risk significantly. Therefore, it remains important to avoid getting apps from third party sites.

Unuchek surmises that in the future, we may see attacks launched toward the Internet of Things (IoT) components from mobile devices. This is because the traditional malware space appears to be getting quite crowded.