2016 Security Predictions from Zscaler™ CISO Michael Sutton

Android finally cleans up its act

Android is well on its way to becoming the Windows of the mobile malware world. With 99% of mobile infections targeting the platform, Android is the only game in town when it comes to infected tablets and smartphones.

Love it or hate it, Apple's walled garden and refusal to allow downloads from third-party app stores has paid security dividends. Sure, Google Play has Bouncer, and it's done a fine job of keeping the miscreants out, but that's of limited value when users are willing to go to shady Chinese app stores to save a buck on Candy Crush. Google clearly knows that this will hurt it in the long run, and while the company is taking steps to increase security, it needs to be much more aggressive going forward, by:

- Cracking down on third-party app stores
- Taking more drastic steps and restricting the permissions available to apps not vetted through the Google Play submission process
- Expecting side-loaded apps that request Administrator permissions to become a thing of the past
- Mandating acceptable timeframes for patches and firmware upgrades from Android licensees

Some developers and partners will push back, but Google will have little choice but to implement these changes if it wants to get malware under control. These steps won't eliminate Android malware, especially with Android's slow O/S upgrade cycle, but they will raise the bar for third-party app stores, just as Bouncer is doing for Google Play.

Terrorists target critical infrastructure

This prediction is one that saddens me to write, but I feel this threat is inevitable and one that can't be ignored. We know that terror organizations are continually searching for new avenues to instill fear, but we also know that they require significant funding to further their hateful agendas. Unfortunately, skilled hackers can aid on both fronts. Cyber-attacks can clearly be used by terrorists to obtain intelligence, and we're already seeing early signs of cyber-attacks being used to cause physical damage through targeting critical infrastructure. Last year, hackers caused significant damage to a German steel mill when they disabled systems responsible for controlling a blast furnace.

This wasn't just kids playing around either, as the attacks reportedly required substantial knowledge of industrial control systems in order to succeed. With almost all industries reliant on computerized systems, the

potential attack surface for critical infrastructure is enormous. Hacking is also extremely lucrative and, sadly, terrorists won't necessarily need to acquire the necessary skills themselves to carry out cyber-attacks, as there is no shortage of cyber criminals willing to rent their skills out to the highest bidder and look the other way.

Password reuse attacks decline

And now for some good news. Password reuse attacks will begin to decline. Attackers are quite happy to compromise virtually any site, even if it's not the endgame, as they can generally recover information and resources that will aid in other attacks. Most people use a handful of passwords at best. (Think of your favorite password that you've used over the years. How many sites have you used it on? You lost count, didn't you?) Fortunately, this is starting to change, thanks in large part to the smartphone.

Smartphones can be many things, but they make for a handy, secure, and always-with-you data repository. As such, people are starting to adopt password managers such as 1Password, LastPass, etc., as they offer user-friendly smartphone apps that present a convenient option for always having sensitive data, such as passwords, within easy reach.

Advancements in biometrics are also helping the cause with consumer-grade fingerprint scanners now becoming a standard feature on modern smartphones. This not only makes accessing that password repository quicker and more user friendly, but also makes it an option—finally—to do away with passwords altogether. While less user friendly, most major web properties are also adding two-factor authentication as a standard option. At last, the average user has realistic authentication options that don't involve sticky notes.

The encryption showdown

Encrypted communications have long been the bane of law enforcement and those in the intelligence communities. As privacy concerns mount, thanks in part to the Snowden revelations, leveraging strong encryption for messaging and data storage is no longer the realm of geek speak. It is, in fact, an expected and differentiating feature. iOS now encrypts data by default and Android, while lagging, is fighting to get there. Popular chat applications like WhatsApp tout encryption as a key feature, and Apple's iMessage app, which features end-to-end encryption and no central key store, is often referenced by law enforcement when arguing for a "backdoor." In 2016, this battle will come to a head.

While politicians used to dance gingerly around the topic given the privacy abuses exposed by the Snowden revelations, recent terrorist attacks have brought this issue front and center. Multiple pieces of legislation are sure to be introduced that will propose weakened encryption protocols or procedures to grant law enforcement access to decrypted communications as needed. Weakening encryption to benefit law enforcement will also reduce security for everyone, and if the U.S. government mandates a "backdoor," you can rest assured that China, Russia, and [pick a country] will be demanding the same for their citizens. This is one battle that will have serious repercussions for years to come. Here's to hoping that Apple, Google, Microsoft, Yahoo!, and the like manage to prevail.

PII is the new hotness

In 2015, the trend of major retail data breaches resulting in bulk debit and credit card theft continued, but the year also marked a shift that will accelerate in 2016. In the coming year, expect attackers to move away from targeting financial

©2017 Zscaler, Inc. All rights reserved.

information and instead begin to target personally identifiable information (PII). The quest for PII is being driven by two separate groups of attackers.

While nation states desire PII for espionage, criminals are also shifting to PII, as it is generally more valuable than credit and debit cards, which are getting more challenging to harvest in bulk due to greater awareness of the problem and new technology. PII is highly sought after in the underground as it can be leveraged to commit financial fraud on several fronts, such as applying for credit, submitting false medical/insurance claims, or filing for fraudulent tax refunds. Whereas credit cards can be easily canceled, it's not generally an option to change one's name, address, and social security number, so the stolen data remains valuable for a longer period of time. In 2016, attackers will increasingly target sectors known to store bulk PII, including finance, healthcare, and government entities, to harvest valuable PII.

About Zscaler

By 2008, Zscaler founders could see that business was transforming, moving away from the corporate network and into the cloud. Believing that the only way to deliver security for the cloud would be in the cloud, we set out to build a global, multi-tenant platform with comprehensive, integrated security services and access controls to protect organizations from cyberattacks and prevent data loss. Today, Zscaler operates the world's largest 100% cloud-delivered security platform, helping thousands of leading organizations make the secure transformation to the cloud. Learn more at **www.zscaler.com**.

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

facebook.com/zscaler
linkedin.com/company/zscaler
twitter.com/zscaler
youtube.com/zscaler
blog.zscaler.com

Zscaler™, SHIFT™, Direct-to-Cloud™ and ZPA™ are trademarks or registered trademarks of Zscaler, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners. This product may be subject to one or more U.S. or non-U.S. patents listed at www.zscaler.com/patents

©2017 Zscaler, Inc. All rights reserved. Z170329