10 Trickiest Mobile Security Threats

Mobile communications are an increasingly integral part of their everyday lives for people at work and at play. But as mobile access has grown, so have mobile threats. Such threats are lucrative for hackers and frustrating for companies trying to thwart their attacks.

We asked security experts for the most problematic mobile security issues. The 10 top mobile threats, in no particular order, are:

Legit Mobile Apps that Mine Corporate Information

"Enterprises face a far greater threat from the millions of generally available apps on their employees' devices than from mobile malware," said Dave Jevans, CEO and CTO of Marble Security. "Enterprise users casually give these riskware apps sweeping permissions, not realizing that their personal and corporate data may be sent to remote servers and advertising networks all over the world, where it can be mined by cybercriminals and hostile governments seeking access to corporate networks."

Through 2017, 75 percent of all mobile security breaches will be through apps, not through deep technical attacks on the OS, according to Gartner, Jevans noted.

Hostile Enterprise-Signed Mobile Apps

This class of malicious apps circumvents app store controls by leveraging enterprise application distribution capabilities in iOS and Android, Jevans explained. These apps may use private OS APIs to gain detailed device information or change settings, mine address books and profile enterprise networks and send that information to cybercriminals.

For example, the WireLurker family of more than 800 maliciously distributed iOS apps used an enterprise app signing certificate to allow users to download and install these apps from outside Apple's App Store, without requiring a jailbreak.

Sophisticated Mobile Attackers

"Attackers are continuing to become more and more savvy," said Roman Foeckl, CEO and founder of CoSoSys. "The WireLurker attack in 2014 was the malware to target non-jailbroken iOS devices. Enterprises need to be sure they have a comprehensive and up-to-date security solution in place."

Non-malicious but Clueless Insiders

According to a recent CoSoSys survey, 35 percent of enterprise employees think that data security is not their responsibility and 59 percent think that losing a mobile device or laptop with company data doesn't represent too much of a threat.

"The non-malicious insider has quickly become one of the largest threats to enterprises in terms of device security," Foeckl said. "Companies who do not have proper systems in place to educate employees about security risks leave themselves open to having sensitive data compromised by an employee leaving a mobile device at a restaurant and not reporting it lost or accessing files on their mobile on an unsecured coffee shop WiFi."

Android Fragmentation

While the fragmentation of the Android mobile operating system is well documented and discussed, the security

risks associated with Android are not generally highlighted in public forums, according to Morey Haber, vice president of technology for BeyondTrust.

"With so many variations, custom interfaces, and vendors incorporating the operating system in their products, critical items like security patches are often not a consideration until a full release is available. This includes the infrastructure necessary to deploy the update on a per-carrier basis and worldwide. Many devices are released with an OS and never see a patch or a full OS upgrade," Haber said.

Mobile Payment Security Sources

Facebook's new payment platform will use third-party sources for security, said Ozgur Gungor, general manager o mobile and EMV Solutions for Cardtek. If Facebook has a Trusted Service Manager platform in place and agreements with handset manufacturers for the management of secure elements, their payment solution would introduce Facebook into classical payment. However, this is quite hard – and Facebook may not evolve in that way.

Rootkits

"Due to the nature of rootkits, they are particularly difficult to trace but can give an attacker absolute control of a device," said Stephen Cobb, senior security researcher for ESET. "The Carrier IQ rootkit was installed by network operators on thousands of mobile devices and security analysts discovered that it was possible for the rootkit to harvest the personal information of any victim. This is especially worrying as we all rely increasingly on our mobile devices in our day-to-day activities. A malicious attack of this severity and scale would cause unprecedented damage, especially as security mechanisms put in place by manufacturers have proven to be potentially insecure."

Authentication Attacks

Authentication consolidation is likely to result in data-specific exploits, although not necessarily for stealing data on a mobile device, said Bob Hansmann, director of product security at Websense.

"Mobile devices will increasingly be targeted for broader credential stealing or authentication attacks to be used at a later date," he said. "To get a more complete understanding of the problem, we really have to think of mobile devices as conduits to the cloud. As the cloud gains more data, organizations facilitate the access of this data through various kinds of devices, whether desktop, tablet or mobile. Because of this, we will see criminals going after the mobile device – not to simply crack a phone code and steal data from the device itself – but as a vector into the growing data resources that the devices can freely access in the cloud."

Connection Hijacking

The man-in-the-middle attack is the most common example of connection hijacking, said Dennis Griffin, product manager of Vidder. "Your sales person sitting in a café is about to use a public Wi-Fi to access SharePoint behind the corporate firewalls. Unbeknownst to her, a nearby attacker has set up a rogue access point to conduct a man-in-the-middle attack. The sales person proceeds with the login. The attacker is able to watch and save the user's traffic in real time, exposing massive amounts of sensitive data," he said, adding that other forms of connection hijacking include certificate forgery and DNS poisoning.

Lack of Mobile Device Policy

A mobile security policy should include rules for authentication (including credential storage) and PII restrictions for email and for the device itself, as well as any restrictions or limitations for usage and passwords and PINs.

"A mobile device policy should be part of the onboarding process; it should be read and signed off on before new employees receive their company device or access company resources with their personal device," suggested Jeffrey Smith, IT security officer at Wombat Security Technologies.

Phillip J. Britt's work has appeared on technology, financial services and business websites and publications including BAI, Telephony, Connected Planet, Independent Banker, insideARM.com, Bank Systems & Technology, Mobile Marketing & Technology, Loyalty 360, CRM Magazine, KM World and Information Today.