Spy in Your Pocket – The Future of Android Malware

The exponential growth of the Android user base, coupled with the increasing sophistication of smartphone malware, has created a perfect digital threat storm for today's financial institutions, according to Michael Shalyt, malware researcher and corporate security 'White Hat'.

A featured speaker at FST Media's *Future of Security in Financial Services* conference, Shalyt delivered an uncompromising assessment of the risks posed by the next generation of Android malware and its growing band of criminal backers.

With a career in the Israeli Army's Military Intelligence, Shalyt offered a unique insight into the threats faced daily by the industry's digital defenders.

"For me, this is personal; this is my neighbourhood. You don't want mafia types moving in … blackmailing and attacking innocent people on the street. You want to fight back," said Shalyt.

With myriad platforms and operating systems available, why has Shalyt focused his attentions exclusively on Android, and why should the finance industry take notice?

For Shalyt, an understanding of the Android threatscape is critical to understanding the cybercriminal's motivations at large.

Android remains, far and away, the most popular operating system in the smartphone market, capturing more than 80 per cent of global market share. This overwhelming popularity (driven largely by consumer uptake of low-cost smartphones) has had the unfortunate effect of attracting a growing band of cyber-scammers ready and willing to exploit known vulnerabilities.

According to Shalyt, cybercriminals have no particular preference in targeting the Android platform; the lure is purely monetary.

"The mafia, or organised crime in general, don't care about technology, about the future of virtual worlds, or wearables … they care about money," said Shalyt.

"If they continue to exploit Android threats … it is cost-efficient for them."

The explosion of Android-specific malware in recent years has been unprecedented. From a standing start just five years ago, today over 16 million Android devices are infected with some form of malicious software.

However, the sheer number of infected devices is not the primary cause for concern; it is, Shalyt argues, the increasing sophistication of mobile malware, which is treading the same evolutionary path as PC malware.

"[Malware is] quickly closing the gap between the technological sophistication that we have all come to recognise on Windows, or desktops in general, and the mobile world," declared Shalyt.

The Financial Services Threatscape

Financial services organisations are, unsurprisingly, one of the chief targets for cybercriminal syndicates, accounting for 20 per cent of all data records stolen (roughly 206 million records last year).

Nearly half of all attacks (48.2 per cent) against Android devices utilised malware targeting financial data, with a three-fold increase in the number of financial attacks against Android users. "The growth," Shalyt observed, "is so exponential, it almost looks fake."

This threat is on the rise, with 75 per cent of mobile users more likely to experience an attack in 2014 than 2013, according to Checkpoint research, *The Myths of Mobile Security*. (http://www.checkpoint.com/campaigns/myths-of-mobile-security/index.html)

However, it is the growing complexity of malware that presents the greatest concern to the financial services industry. Indeed, today's criminal efforts have matured well beyond the notorious premium SMS scams, once the "go-to method" for monetising malware.

According to Shalyt, today's mobile malware exploits two primary attack vectors: "user innocence" (for example, tricking users into downloading malicious software), or attacks against the operating platform's back-end architecture.

"Exploiting user innocence," Shalyt confirmed, "accounts for more than 90 per cent of all cybercriminal scams." One successful strategy commonly utilised by criminal entities is the offer of zero-cost alternatives to popular Android apps, which, unbeknownst to the user, are laden with malicious code. Though far less common, the second primary attack type exploits Android's vulnerabilities and architecture design. One particularly dangerous mechanism is the Binder (Android's inter-process communication system).

Shalyt demonstrated what could prove the future of Android malware. With a

simple insertion of malicious code into the binder mechanism itself, the experimental hack (developed by Checkpoint) was able to instantly hijack a banking transaction during the authentication process, altering the transfer value and receiver, and tricking the bank server into processing these faked values.

While today's hackers have yet to reach this level of technical sophistication, according to Shalyt, it is only a matter of time.

With an incessant and increasingly sophisticated array of malware hacks, the question remains: does the financial services industry stand a chance of preventing cyber attacks? For Shalyt, the answer remains a resounding "no".

"I don't believe there is any system, no matter how sophisticated – not even the Pentagon – that could not be breached."

Nevertheless, despite his unequivocal stance, Shalyt is confident that banks and financial institutions have the wherewithal to frustrate and disincentivise criminal hackers to the point that any attack becomes financially untenable.

Thwarting Your Attackers

For Shalyt, the key to minimising the probability of criminal breaches is to reduce the economic viability of an attack. The more effort exerted, the costlier it is for cybercriminals to proceed with the attack.

"The only question is how much effort it takes. If it is incredibly difficult to penetrate your bank, either the [hackers] will simply [move on] to some other scams, or they will attack a competitor's bank."

To mitigate the persistent threat of criminal breaches, Shalyt offers four key pieces of advice for finance industry CISOs:

"I don't believe there is any system, no matter how sophisticated – not even the Pentagon – that could not be breached."
– Michael Shalyt, malware researcher and corporate security 'White Hat'

1. **Assume the worst – never trust the user's phone.** While a root exploit is not yet available on Andoid's latest update, all previous versions have been 'rooted', leaving them vulnerable to attack.
2. **Protect your app as much as you can.** Minimise the use of native services, which often provide inadequate security provisions. To reduce the risk of keyloggers, consider implementing a keyboard inside your app.
3. **Encrypt all sensitive data.** Try to keep everything that you really care about encrypted, even if it will not be transmitted via the internet.
4. **Do not rely on Android antivirus solutions.** The Android permissions structure prevents antivirus from interfering with applications as they run, reducing their effectiveness markedly.

While Shalyt concedes there is no such thing as a safe system, he offers prudent advice for IT security managers to reduce the economic and practical incentives for hackers to attack. "Throw everything at the problem: use VPN, go through a cloud firewall, [or] through a sandbox," said Shalyt.

"Every hurdle you add … will increase the cost of attacking your organisation – the cost of developing against you. Let's say you put 10 hurdles, each hurdle will block 50 per cent of attacks. This is [good] news, because the chance [the hacker] will actually get to the interesting part becomes very small."

In light of the government's Data Retention legislation, Shalyt concluded his presentation with a sobering message for attendees: "be scared."

"This is state-level information. [It is] a honeypot. Everyone is going to go after [this data]." *

To learn more about mobile security and how to protect your mobile users, visit Mobile Security – Check Point Capsule. http://www.checkpoint.com/products-solutions/mobile-security/check-point-capsule/index.html