The importance of mobile threat defence

By Rick Rogers

11 Oct 2016

LAGOS, Nigeria - Mobile malware and vulnerabilities have been making headlines well over the past year, and attacks are becoming a more common way for cybercriminals to steal sensitive data. We believe this trend - one that our research team encounters daily - is illustrated in the Gartner Market Guide for Mobile Threat Defense solutions.

Image by 123RF

This rise in the sophistication and volume of mobile malware and continued exposure to unknown vulnerabilities demonstrates how Android and iOS devices simply aren't secure on their own.

According to the Check Point 2016 Security Report, mobile devices pose massive risks for organisations. Some of the key takeaways include:

- Employees mix business with personal use and one in five mobile devices are infected.
- One in five employees will be the cause of a company network breach through either malware or malicious Wi-Fi.
- Mobile security lags behind mobile adoption as users discover new ways of engaging while on the go.
- Cybercriminals can easily set up a fake hotspot, or hijack an existing one.
- The mobile threat defence market is growing rapidly.
- Mobile malware and vulnerabilities aren't all that different than their cousins in the PC world. We've seen how today's mobile malware imitates techniques introduced by PC malware. According to the 2016 Security Report the five major categories of attacks and vulnerabilities challenging the mobile device space are: System Vulnerabilities; Root Access and Configuration Changes; Repackaged or Fake Apps; Trojans and Malware; Man-in-the-Middle Attacks.

As mobile threats develop, more companies should adopt mobile security solutions designed to keep pace with this evolution.

According to Gartner: “By 2018, fewer than 15% of organisations will have mobile threat defence (MTD) in place, which is an increase from fewer than 5% today”.

We believe if the number of organisations implementing MTD solutions triples by 2018, it becomes that much harder for cybercriminals to infiltrate and exploit mobile devices, and gives them even less motivation to do so.

The time to act is now. If organisations don’t do something soon to stop mobile malware in its tracks, we’ll soon face a problem on a much wider scale, like the one we encounter already for PCs today. Organisations need across-the-board protection. Cybercriminals focus on three main vectors to conduct attacks on mobile devices:

1. **Networks:** Network attacks allow cybercriminals to handpick their targets, minimising the potential risk of discovery and focusing their efforts only on the specific objective. Cybercriminals can easily set up a fake hotspot, or hijack an existing one.
2. **Apps:** App-based attacks provide cybercriminals with the greatest capabilities, enabling them to compromise virtually any target. Both the Apple App Store and Google Play have been contaminated with malware. The situation is even worse in third-party app stores which have even less control over the apps they host.
3. **Device:** Both iOS and Android are riddled with exploits developers constantly struggle to patch. These exploits exist everywhere, from the kernel through the chipsets to the OS. From the moment an exploit is discovered to the moment it is patched, cybercriminals can use it to attack defenceless users.

Accordingly, Gartner says “MTD solutions provide security at one or more of these four levels:

- **Device behavioural anomalies —**MTD tools provide behavioural anomaly detection by tracking expected and acceptable use patterns.
- **Vulnerability assessments —**MTD tools inspect devices for configuration weaknesses that will lead to malware execution.
- **Network security —**MTD tools monitor network traffic and disable suspicious connections to and from mobile devices.
- **App scans —**MTD tools identify “leaky” apps (meaning apps that can put enterprise data at risk) and malicious apps, through reputation scanning and code analysis.”

With billions of new connections formed every minute, the world is more globally linked than ever. Innovations like cloud, mobility and IoT are changing the way we deploy, the way we consume, and the way we secure technology.

More and more malware is being put into our ecosystem that traditional security techniques are powerless to prevent. Given this, staying a leader requires being one step ahead of things you cannot see, know or control – and preventing attacks before they happen. Organisations need to do everything in their power to ensure that they are as secure as possible. Some of the best practices to protect your mobile business are:

- Educate your workforce.
- Define your risk tolerance.
- Enforce basic hygiene.
- Separate work and personal data.
- Invest for an uncertain future.

For the modern enterprise advanced threat prevention, mobile device protection and segmenting a network are all critical

components in order to secure themselves.

ABOUT THE AUTHOR

Rick Rogers is Area Manager for East and West Africa at Check Point Software Technologies.