A **TrendLabs** Security in Context Paper

TREND MICRO™

Embracing BYOD

Are You Exposing Critical Data?

BYOD is a Reality

Increasing worker productivity is the top benefit achieved from deploying BYOD programs.

Source: Key Strategies to Capture and Measure the Value of Consumerization of IT, May 2012

While several factors can be cited for the strong consistent growth of consumer smartphone and mobile device use in recent years, reduced cost of device ownership is the primary reason. The bring-your-own device (BYOD) phenomenon continues to become more commonplace as Gartner predicts that half of employers will require their employees to supply their own devices by 2017.[1] This is clear evidence that BYOD is rapidly becoming embedded in employees' working life. This also, unfortunately, becomes a nightmare for security officers and IT staff.

Unlike company-issued devices, personally owned devices used in the workplace are not enabled with device and data management features. Given how enterprises now pursue consumerization in an attempt to increase productivity and reduce costs, compliance with previously existing IT policies may not always be their top priority.

Security in the enterprise environment is thus constantly changing due to consumerization. Security remains one of the biggest challenges in BYOD-enabled workplaces. A Gartner study on BYOD reports that over 60% of employees use a personal device for work. This suggests that the BYOD phenomenon isn't merely a trend, but a reality that will linger and grow.[2]

Mobile Device Use in the Cloud Computing Era

Mobile devices are ideal for accessing cloud service platforms, which several organizations increasingly use for their daily operations. The following cloud services are some examples:

- Note-taking apps
- Document-sharing services normally used to manage documents
- Cloud storage services that allow document hosting

Similar to other means of storing information, however, these can open up a different set of risks.

[1] Gartner, Inc. (May 1, 2013). *Newsroom*. "Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes." Last accessed February 13, 2014, http://www.gartner.com/newsroom/id/2466615.

[2] Gartner, Inc. (August 14, 2013). *Gartner Webinars*. "Bring Your Own Device Program Best Practices (BYOD)." Last accessed February 13, 2014, http://www.gartner.com/resId=2422315. *Note: Registration and login may be required

What kinds of smartphone data can be lost?

IT also faces a potential security tsunami if users are allowed to download whatever applications they wish from online app stores. While official iOS and Window Phone channels offer certain protections, Android's open ecosystem makes it easy for cyber criminals to upload malware-ridden apps masquerading as legitimate software.

Source: Bring Your Own Apps – Manage Risk to Reap the Rewards, January 2013

Broadly speaking, how "smart" a device is will affect the kind of data stored in it. At the most fundamental level, information such as contact lists, text messages, and call logs can be found in any device used for company purposes. In isolation, this kind of data may have relatively limited value to most businesses. However, attackers can use them for social engineering.

At present, smartphones connect to corporate networks to access data from email inboxes, calendars, and internal portals. Should confidential data like that be exposed to third parties, it can create severe enterprises risks. Leaked email conversations and attachments, for example, have caused major losses and much embarrassment for high-profile companies.

Attackers can use compromised or stolen mobile devices to access all kinds of information stored either in the device or in the networks these devices have access to. If an attacker is able to obtain the login credentials stored on an employee device, he can use it to infiltrate the organization's network and put its document databases at risk of unwanted exposure.

What are the risks to data on mobile devices?

Android™, the most dominant mobile OS in the market today[3], is plagued by a large number of malicious and high-risk or potentially unwanted apps. Since the discovery of the first Android Trojan in 2010 to the end of 2014, we have seen nearly 4.3 million of these bad apps emerge.

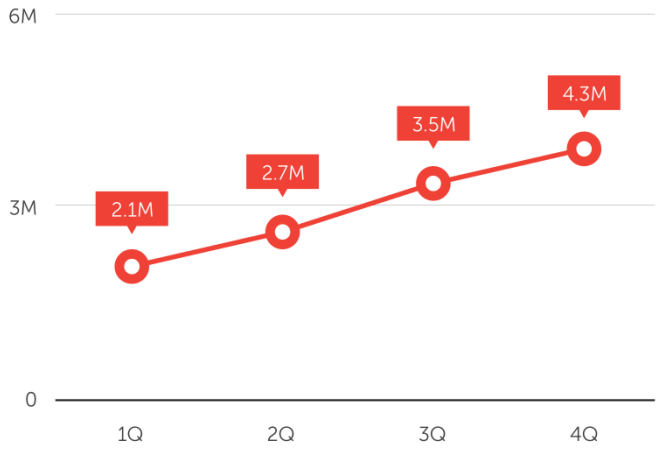

Figure 1. Malicious and High-Risk Mobile App Growth, 2014

[3] Jon Russell. (January 7, 2014). *The Next Web*. "Android will pass 1 billion users across all devices in 2014, according to Gartner." Last accessed February 13, 2014, http://thenextweb.com/google/2014/01/07/android-will-pass-1-billion-users-across-devices-2014-according-gartner/

Over the years, we have seen attackers design mobile malware that target users' bank accounts. There are fake banking apps that mimic popular ones and are used to steal user credentials. There are also those that hijack mobile banking sessions, transmit information, and establish command-and-control communications.[4] We have likewise noted the development of the Perkele crimeware toolkit, which affects mobile apps and can be used for man-in-the-middle (MitM) attacks.[5]

Android malware has also evolved in terms of stealth and infiltration. In the fourth quarter of 2014, we discovered certain malware strains using SSL[6] and TOR[7] (The Onion Router) to hide their communications with their creators. HTML apps started getting repackaged into malware after the new standard was finalized. This gave rise not only to the infection of more Android devices, but also other platforms (iOS, Windows Phone). If businesses are not BYOD-ready, these threats may easily target employees' devices.

Apart from malicious and high-risk apps, two typical scenarios can also lead to the exposure of data stored in mobile devices—device loss or theft and unsecure communication via mobile devices.

Device Loss or Theft

Smartphone loss is, unfortunately, an all-too-common occurrence. Even though password and comparable lock features are part of all modern smartphone platforms, these still cannot be considered effective means of securing devices, especially those that contain sensitive information. Losing a smartphone comes with the expectation that malicious users can obtain access to all of the information stored in it.

Unsecure Mobile Access

Many mobile device users access the Internet via any available Wi-Fi network wherever they are. Accessing the web via open Wi-Fi networks, though free, may not be the best idea especially if confidential and sensitive information is stored in a mobile device. When mobile users access unsecure sites or make use of apps that are not properly configured for security, the possibility of losing data to malicious actors looms larger.

---

[4] Trend Micro Incorporated. (2015). *Trend Micro Security News*. "The South Korean Fake Banking App Scam." Last accessed February 26, 2015, http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/south-korean-fake-banking-app-scam

[5] Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "ANDROIDOS_PERKEL.A." Last accessed February 13, 2014, http://about-threats.trendmicro.com/us/malware/ANDROIDOS_PERKEL.A

[6] Trend Micro Incorporated. (2014). *Trend Micro Security Intelligence Blog.* Android Malware Use SSL for Evasion. Last accessed June 17, 2015. http://blog.trendmicro.com/trendlabs-security-intelligence/android-malware-use-ssl-for-evasion/

[7] Trend Micro Incorporated. (2014). *Trend Micro Security Intelligence Blog.* "Android Ransomware Uses TOR." Last accessed June 17, 2014. http://blog.trendmicro.com/trendlabs-security-intelligence/android-ransomware-uses-tor/

What mobile security solutions are available?

Enterprises can look into solutions that have device antivirus, application reputation, mobile device management (MDM), and mobile application management (MAM) capabilities. *Enterprise Mobile Security and Management* solutions, for example, cover all four. While device antivirus and application reputation services help prevent mobile malware from infiltrating employee-owned devices, MDM and MAM solutions have the ability to minimize incidents of data loss or leakage through remote wipe or lock options.

Another way of securing the enterprise data accessed via mobile devices is through virtual mobile infrastructure (VMI), like the *Trend Micro™ Safe Mobile Workforce™*. With VMI, data is stored securely on corporate servers rather than on employee mobile devices. This not only ensures that corporate data is easily separated from user personal apps and information; it also eliminates the chance of data leaks in case of device loss or improper device use.

Safe Mobile Workforce allows IT managers to host corporate apps and data within secure mobile operating systems stored on a centrally-managed company server. Employees can install a client application on any of their mobile devices. This will give them secure remote access to their company data without ever saving them on their devices.

Below are some of the features that Safe Mobile Workforce offers:

- An advanced client-side rendering engine that gives a simple and familiar mobile user experience for accessing a company-provided corporate workspace.
- Access to corporate email and files without needing to configure or install apps. Safe Mobile Workforce allows real-time access to company data on any device.
- Secured corporate data even if the mobile device is lost. The data is readily made available from the Safe Mobile Workforce server.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO

TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an “as is” condition.

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative security solutions for consumers, businesses and governments protect information on mobile devices, endpoints, gateways, servers and the cloud. For more information, visit www.trendmicro.com

TREND MICRO™

Securing Your Journey to the Cloud