A **TrendLabs** Security in Context Paper

TREND MICRO™

Embracing the BYOD Era

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 consistent strong growth of consumer smartphone and other mobile device usage in recent years, reduced cost of device ownership is primary. This, along with other factors, led to a significant increase in the smartphone penetration rate. 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, which also spells out a nightmare for security officers and IT staff.

Unlike company-issued devices, personally owned devices do not come enabled with equipment device management features. Consumerization is now being pursued in an attempt to increase productivity and reduce costs. As a result, compliance with previously existing IT policies may not always be a 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 not only linger but grow. [2]

Mobile Device Usage in the Cloud Computing Era

Mobile devices are ideal for accessing cloud service platforms, which are increasingly being used by several organizations for their daily operations. Similar to other means of storing information, however, these can pose a different set of risks. The following are some of the cloud services smartphone owners and/or organizations use at present:

- Note-taking apps
- Document-sharing or -storage services, which are normally used to share and manage documents
- Some cloud storage services, which allow businesses to completely host documents in the cloud

[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, the kinds of smartphone data that can be lost vary depending on how "smart" a device is. At the most fundamental level, information such as contact lists, text messages, and call logs can be found in any kind of cellular device used for company purposes. In isolation, this information may have relatively limited value to most businesses. Note, however, that it can be used to launch social engineering attacks.

At present, smartphones are invariably used to connect to corporate networks in order to gain access to data from email inboxes, calendars, and internal portals, which all pose severe risks to enterprises should their contents be leaked to third parties. Leaked email and attachments, in particular, have caused numerous organizations, at the very least, embarrassment in the past.

Attackers can use compromised or stolen mobile devices to access all kinds of information stored in them or in the networks or databases they have access to. Compromising an organization's login credentials to any of the aforementioned services can also put its document databases at risk of unwanted exposure.

What are the risks to data on mobile devices?

Android™ as the most dominant mobile OS in the market today[3] also comes with a large number of malicious and high-risk or potentially unwanted apps. We have seen nearly 1.4 million of these bad apps in 2013, since the discovery of the first Android Trojan in 2010. This translates to potential threats on employees' devices, which puts their own data as well as company data at risk.

[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/

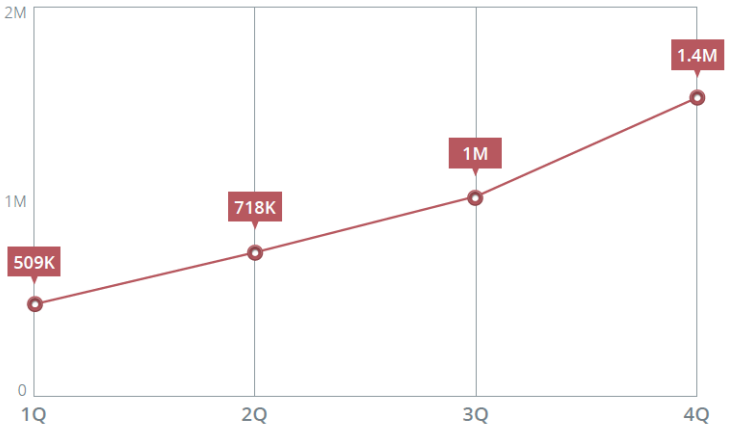

Figure 1. Malicious and High-Risk Mobile App Growth, 2013

The FAKEBANK malware seen in the second quarter of 2013 went after mobile banking users' account information, call logs, and text messages in the guise of a legitimate banking app.[4] The Perkele crimeware toolkit was designed to affect mobile apps and could be used for man-in-the-middle (MitM) attacks.[5] These threats may easily target employees' devices if businesses aren't BYOD-ready.

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 not securely communicating via mobile devices.

Device Loss or Theft

Smartphone loss is, unfortunately, an already-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

[4] Trend Micro Incorporated. (2013). *Threat Encyclopedia*. "A Look at Mobile Banking Threats." Last accessed February 13, 2014, http://about-threats.trendmicro.com/us/mobile/monthly-mobile-review/2013-08-mobile-banking-threats.

[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.

not properly configured for security, the possibility of losing data to malicious actors looms larger.

What mobile device security solutions are available?

Mobile device management (MDM) solutions such as *Enterprise Mobile Security* have the ability to minimize incidents of data loss or leakage. Installing data protection solutions in critical systems, along with MDM solution use, is also a great measure to minimize risks associated with data loss or leakage. Should users lose improperly secured mobile devices that have access to or contain sensitive information, data protection solutions installed on internal networks and systems that provide authentication, audit, and access control capabilities can continue to safeguard an organization's main data storage.

Additionally, a virtualized mobile infrastructure like Trend Micro™ Safe Mobile Workforce™ addresses the issue of maintaining a centralized and efficient BYOD workspace. With a virtualized solution, data is stored securely on corporate servers rather than on mobile devices so corporate data is easily separated from user personal apps and data.

Safe Mobile Workforce allows IT managers to host corporate apps and data within a secure mobile operating system on centralized servers. This client application is used to provide users with secure access to a remote, securely managed environment on their mobile device. It enables the clear separation of corporate and personal data, while users are able to access the same mobile environment across both iOS and Android platforms for smartphone and tablets.

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

- An advanced client-side rendering engine that provides an simple and familiar mobile user experience for accessing corporate workspace provided by the company
- Access to corporate email and files without needing to configure or install apps. Safe Mobile Workforce also 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