IMPLEMENTING BYOD PLANS
ARE YOU LETTING MALWARE IN?

A TrendLabs Cloud Security Primer
Employee-Liable Mobile Devices: Challenging IT Readiness

Enterprises cite security as their number 1 concern with regard to consumerization.¹ During the actual execution of a consumerization strategy, however, IT groups find that the increasing demand to use employee-owned devices for work is forcing security to compete with other equally important activities.

A number of factors contribute to the diminished regard for security:

- **Lack of awareness:** IT groups may not be aware how many mobile devices are connecting to their networks. A survey estimated that 69% of employees used smartphones for work while their respective IT groups said 34% did so.²

- **Increased workload:** Unlike company-issued laptops, employees’ smartphones require more from IT groups because IT administrators need to treat and configure each device and OS version differently.³ As a result, IT groups may only enforce minimal security.

- **Technical support prioritization:** Device-carrying employees demand that IT groups make their devices work.⁴ This forces IT groups to deprioritize security in favor of providing technical support.

- **Mobile OS updating difficulty:** IT groups’ jobs are not made easier by the open nature of the Android OS and mobile OS providers’ weak vulnerability handling and remediation processes. Waiting for patches can take weeks; fully deploying them takes even longer.

- **Knee-jerk mobile device management (MDM) solution purchases:** IT groups may be tempted to buy an MDM solution that may be inappropriate to their specific environments and can negatively impact their security.⁵

- **Informal adoption:** In some cases, enterprises may informally encourage the bring-your-own-device (BYOD) trend to please their employees. They may, however, not have written usage guidelines or implement best practices.

The introduction of employee-owned devices to workplaces has been acknowledged in order to increase employee productivity and satisfaction, business agility, and provable cost savings. Risks to security and data should, however, also be closely examined.

---

Security Threats Employee-Liable Devices Pose

According to a Trend Micro study, almost half of the total number of enterprises that allow BYOD experienced data breaches due to employee-liable devices that access their networks. As a result, 42% of enterprises have started installing security software on these devices and limiting employee access to data.

Malware and Employee-Liable Devices

Via Jail-Broken iPhones

IOS_IKEE.A is a worm that infects jail-broken iPhones with Secure Shell. It also targets other jail-broken iPhones connected to local networks. It does so by scanning for IP addresses then logging in and installing the malware package into target devices. This malware has the capability to receive commands from a remote user such as gathering information and sending it to a command-and-control (C&C) server.

Device Pre-Installation

Malware can enter systems and networks not only through jail-broken devices. They can also come pre-installed in devices prior to shipping. In 2010, Samsung’s S8500 Wave and Vodafone’s HTC Magic Android SD cards came pre-installed with malware. Plugging infected devices into systems spreads the infection to the systems along with any removable drive plugged into these.

Mobile Vulnerability Exploitation

- Vulnerabilities that affect Adobe Flash Player in earlier Android OS versions can potentially allow a remote user to take full control of affected devices.
- In 2010, a jail-breaking code for iPhone 4 used vulnerabilities in how Safari handles .PDF files. This exploit code could be modified by any remote attacker to create a far more damaging payload.

Potential Mobile Threat Vectors

While the scenarios above are based on documented malware behaviors, the following are other possible entry points for mobile threats:

- **Trojanized apps**: Cybercriminals can insert malicious code into apps that can infect devices.
- **SMS, social media, and email links**: Links embedded in SMS, social media posts, and emails can potentially redirect users to websites that host malicious files.
- **Third-party app stores**: Some third-party app stores may host malware that can potentially harm devices, systems, and networks.

For more information on how security threats enter networks via employee-liable devices, see Figure 3. These threats are not expected to disappear in the future as Trend Micro researchers predict a continuous increase in the Android malware volume as shown in Figure 2.

---

Risks to Corporate Data

In general, once a malware enters the network through an employee-liable device, it can perform a variety of damaging payloads, depending on its design. For instance, according to Trend Micro mobile malware researchers, a malware can launch a sniffer onto the network to collect data and send it via SMS or through the network. Data stored in shared folders and internal FTP sites can also be stolen.

Mobile Device Management with Security in Mind

The real objective of MDM is to enable an organization's security team to see and control each and every device that accesses the corporate network and uses corporate data. IT groups cannot hope to manage what they cannot see and prioritizing this is crucial.

A consumerization strategy that embraces instead of restricts is possible with the right amount of research on the current enterprise environment. This knowledge will allow IT groups to make informed decisions and purchase the right mobile security solution. The mobile security solution that is right for your organization should provide:

- Ample control in a centralized, scalable, single console
- Broad platform support to ensure that any and all types of devices are covered
- Mobile device security, including malware protection, malicious site access blocking, and firewall and intrusion detection system (IDS) protection
- MDM that allows visibility with regard to devices and their respective statuses
- Password employment and data encryption to limit the loss of corporate data aside from remotely wiping it in case a device gets lost or stolen
- Application management capabilities that manage personal and corporate apps as well as block the download of malicious ones onto the device

The scenarios that put security as less of a priority have dire implications. For instance, IT groups may have a bare-bones antivirus solution for mobile devices installed but neglected to orient employees about social engineering or corporate information sharing. In this example, employees may click a socially engineered link through their smartphone browsers that their organizations’ antivirus solution may not be able to catch.

Taking a proactive stance in managing mobile device consumerization ultimately reduces overall IT support costs. Solutions such as Trend Micro™ Mobile Security enables consumerization while reining control over employee-liable devices that access networks.
TREND MICRO™

Trend Micro Incorporated (TYO: 4704; TSE: 4704), a global cloud security leader, creates a world safe for exchanging digital information with its Internet content security and threat management solutions for businesses and consumers. A pioneer in server security with over 20 years' experience, we deliver top-ranked client, server and cloud-based security that fits our customers' and partners' needs, stops new threats faster, and protects data in physical, virtualized and cloud environments. Powered by the industry-leading Trend Micro™ Smart Protection Network™ cloud computing security infrastructure, our products and services stop threats where they emerge—from the Internet. They are supported by 1,000+ threat intelligence experts around the globe.

TRENDLABS™

TrendLabs is a multinational research, development, and support center with an extensive regional presence committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery. With more than 1,000 threat experts and support engineers deployed round-the-clock in labs located around the globe, TrendLabs enables Trend Micro to continuously monitor the threat landscape across the globe; deliver real-time data to detect, to preempt, and to eliminate threats; research on and analyze technologies to combat new threats; respond in real time to targeted threats; and help customers worldwide minimize damage, reduce costs, and ensure business continuity.