JUNOS PULSE

TOP 10 THINGS

You Need to Know About Mobile Security Threats

If you ask today's C-level executives, IT directors and staff whether or not they're concerned about mobile security, chances are you'll be answered with a resounding "yes." However, ask what measures they've put in place to handle mobile security and you'll soon learn the difficulty organizations are having in identifying the growing range of threats and figuring out what to do about them. With this in mind, here are the top ten things about mobile security threats you need to be aware of:

1 BUSINESS HAS BECOME TOTALLY MOBILE—AND TOTALLY VULNERABLE.

According to a study of IT professionals conducted by ESG in late 2009, organizations are going through a rapid spending increase on mobile devices and a dramatic uptick in device use for business.[1] Data from the study indicates that most enterprises now regard mobile devices as critical business tools. Another respected study found that approximately 76% of mobile device users routinely access sensitive information on company networks.[2] Underlying this expansion has been a corresponding increase in the vulnerability of organizations to fraud and cyber-theft. If companies do not act quickly to put a strong mobile security platform in place, this vulnerability can be catastrophic for business.

2 WANT TO GET AT A COMPANY'S NETWORK? JUST INFECT A MOBILE DEVICE.

In the spring of 2010, thousands of malware-tainted microSD memory cards were found on Vodafone's HTC Magic smartphones. The malware was multifold, and included the nefarious Mariposa botnet, the dastardly Conficker worm, and a sneaky password stealer from the Lineage game. When the HTC Magic phones were connected to a computer, there was an immediate attempt to infect the machine, steal passwords, and generally wreak havoc. Luckily, the threat was identified and neutralized, but consider how the loss of just one key password could have compromised a company's data security. The takeaway? Now cyber-thieves have a whole new set of pathways into company networks—through mobile devices. [3]

1 ESG White Paper, page 2
2 KRC Research Paper, page 2
3 http://www.infoworld.com/d/security-central/malware-infected-memory-cards-3000-vodafone-mobile-phones-217
http://www.theregister.co.uk/2010/03/09/vodafone_mariposa/
http://www.securelist.com/en/analysis/204792100/Kaspersky_Security_Bulletin_2009_Malware_Evolution_2009

3 A VIRUS HAS JUMPED FROM A MOBILE DEVICE INTO OUR SYSTEMS! WE'LL DEAL WITH IT LATER.

Because employee use of mobile devices has had such a dramatic impact on productivity, many large organizations have begun making enterprise-wide investments in these devices. While this is an exciting business development, there has not been a widespread updating and integration of IT operations and security infrastructure for managing mobile devices.[4] As a result, much of an organization's mobile security ends up being conducted in a fragmented fashion, which makes it difficult for companies to perform real-time monitoring and neutralizing of mobile security threats. This not only leaves businesses increasingly vulnerable, but also drives up the cost and complexity of IT operations.

4 THE LINE BETWEEN BUSINESS AND PERSONAL IS GETTING BLURRY.

At this point in time, not only are users adopting mobile devices at a rapid rate, they are also using single devices for more than just personal activities. In a recent study conducted by KRC Research, 75% of respondents in China admitted to using their mobile devices for both business and personal purposes. Respondents in the U.S. indicated a combined business/personal device usage of nearly 40%.[5] This kind of multitasking may not seem like a big deal until you consider AdaptiveMobile's 2010 report that shows a near 33% increase in mobile malware over the previous year![6] All it takes is one infected device to compromise sensitive company information, which is argument enough for companies to adopt comprehensive mobile security solutions.

5 USERS AREN'T ALWAYS THE GREATEST AT PROTECTING THEIR DEVICES.

It would be great if companies could simply rely on the honor system or even the enlightened self-interest of users when it comes to completing basic security tasks such as creating and modifying device passwords. But a recent U.S. study unfortunately bursts this bubble, indicating that less than 50% of device users bother to take care of such simple security measures.[7] This means that if a device gets stolen or lost, it becomes exceptionally easy for a new "owner" to use the device to access sensitive data. Wouldn't it be nice if a company's IT department could protect that device remotely?

6 A LOT OF SENSITIVE DATA MAY BE HANGING OUT RIGHT ON THE MOBILE DEVICE.

For the sake of argument, let's forget about the fact that many users are currently accessing sensitive company data via their mobile devices. Instead, let's just consider that a high percentage of users already have sensitive company data sitting right on their mobile device. ESG discovered this fact in a recent study of 174 North American IT professionals.[8] This realization means that the loss of a single device, which may only be worth a few hundred dollars, could lead to a multi-million dollar data breach. Smart organizations may recognize that these types of security issues will only get worse unless they pursue a fully integrated approach to mobile security.

4 ESG White Paper, *Addressing Mobile Device Security and Management Requirements in the Enterprise*, page 3
5 KRC Research Report, slide 3
6 http://www.mobile88.com/news/read.asp?file=/2010/12/16/20101215212214&phone=mobile-_malware-_smartphone-_phone-_announces-
7 KRC Research, slide 6
8 ESG White Paper, *Addressing Mobile Device Security and Management Requirements in the Enterprise*, page 9

7 THIRD PARTY APPLICATION DEVELOPMENT MAKES DEVICES EVEN MORE VULNERABLE.

Downloading a variety of third party applications on mobile devices has created yet another way to be vulnerable to attacks and identity theft. Currently, the growing number of mobile Facebook applications has opened the door for hackers to grab User IDs and utilize them to misrepresent themselves and access sensitive data. Any employee who has used their work e-mail address as an anchor for their Facebook account, or simply hasn't maintained strong password protection, could be compromising important information that will ultimately impact their organization. [9]

8 HAVE YOU HEARD OF THE "IKEE.B WORM?" IT'S NASTY.

Sometimes called "Duh," the Ikee.B worm appeared in late 2009.[10] The worm proliferates by using an application's default password to compromise a mobile device (in this case, it was the iPhone). Once the device is cracked, the worm grabs text messages and searches for banking authorization codes. It's not that hard to see how such a worm can be applied to any number of codes that also pertain to sensitive company data. Without a comprehensive and integrated suite of mobile security solutions, many organizations will face increasingly higher risks of data theft.

9 TO INCREASE SECURITY, MANY COMPANIES ARE CUTTING OFF EMPLOYEE ACCESS.

With an increasing amount of employees accessing company networks via mobile devices, many organizations are opting to block employees' mobile access to their networks. While this may seem like a simple solution to a complex problem – especially for organizations that do not have well-developed mobile security procedures and protocols – the reduction in efficiency and employee productivity can be especially high. In a competitive marketplace in which most companies are taking advantage of the benefits of mobility, this loss of edge can really hurt the bottom line.

10 MOST IT DEPARTMENTS HAVE OUTDATED PROCEDURES FOR MANAGING MOBILE SECURITY.

ESG's recent study indicates that while mobile devices are making employees more productive from more places, management and security are lagging behind current practice. Since the growth in mobile has motivated large organizations to invest further in mobile devices and develop custom applications, it follows that security gaps will only grow over time. If device security continues to be managed on a purely ad-hoc basis, the cost and complexity of IT operations will continue to expand. To stave off this increasing insecurity, today's CIO's must move to establish a baseline of strong mobile device security.

[9] http://www.speedofcreativity.org/2010/04/07/cnbc8-com-facebook-hack-phishing-scam/
http://ipwatchdog.com/2010/10/19/beware-of-third-party-facebook-application-security-risks/id=12861/

[10] ESG White Paper: *Addressing Mobile Device Security and Management Requirements* in the Enterprise, page 9

Summary

If you want to tackle any and all of the issues raised here, consider the Junos Pulse Mobile Security Suite. It's a completely comprehensive mobile security and management solution that protects mobile devices—and the sensitive data they either access or contain—against a wide range of threats. Enterprises can use Junos Pulse to seamlessly manage a diverse mobile environment at scale, while mitigating the risk of losing sensitive, critical corporate or personal data on lost, stolen, or compromised devices. To read other whitepapers referenced in this piece or to get more information on the Junos Pulse Mobile Security Suite, visit: **http://www.sampleurl.com/**