SPECIAL REPORT:
Enterprise Smartphone Security Solution – It’s Not Just for BlackBerrys

The smartphone is becoming the new Personal Computer.

Consumers and enterprises are demanding more and more functionality out of their devices; from just email, entertainment and gaming, to banking and remote Enterprise access. Attacks to such devices were limited in the past as there was no easy path to cash as there was with stealing identities and credit card details from PC users. This is what has changed.

Entirely new generations of powerful easy to use devices like the iPhone, iPad, Windows Mobile, Android and Symbian, among other smartphones are now hosting and providing more business, financial and personal information rich transactions. This simple yet profound evolution makes those devices not only a viable target, but a rather easy one as appropriate security measures have not been put in place.

Technical Impact Analysis:
The threat is real – and is here

The threats are more than just an annoyance like the days of pop-ups, but are a direct and immediate issue for financial, compliance-driven and personal identity information. “Bot nets” are used to harvest data and steal passwords, identities and in the end - real money. As with PCs, smartphones infected with malware and viruses first experience performance degradation. These infections are tools of the criminal element and organized crime, crafted by technical experts and explicitly designed with the intent to steal data for profit.

Finally, the spam and phishing attacks that we are all so familiar with are an immediate threat to smartphones and the networks they connect to. Unsuspecting users either purposely or mistakenly click on a link to a website embedded in an email that can then infect their smartphone, turning it into part of a botnet, ‘phoning home’ or being compromised in many other ways, depending upon the goals of the designer. Employees then connect to the enterprise network for updates, remote data access – use your imagination for the rest. Or, do you assume your current network security measures are sufficient to combat data breaches, network intrusions and become remote surveillance and tracking devices?

- The first mobile ‘bot net’ was discovered in July 2009 by researchers at security firm Trend Micro.
- By the first half of 2009, one in 63 smartphones was infected with mobile spyware and malware. - according to a July 2009 study of nearly 2,000 smartphone users.

- There have been multiple stories of spam being used to trick people into going to malicious web sites with their smart phone browsers, as well as to scam them directly from their phones[1].
- Increasing adoption of smartphones and access to 3G high speed networks has created a fertile environment for the acceleration of mobile banking illustrated by a study showing that 39% of respondents access their bank accounts on their smartphone rather than pc when they were at home.[2]
- The iPad has already been rooted (taken over by hostile code).[3]
- "Smartphones are essentially becoming regular computers," says Vinod Ganapathy, computing professor at Rutgers University in New Jersey. "They run the same class of operating systems as desktop and laptop computers, so they are just as vulnerable to attack by malware."[4]
- OSX and Android should be a bonanza for hackers and malicious software engineers.[5]
- An Australian student created an experimental worm that hopscotched across "jailbroken" iPhones, which are phones altered to run software Apple has not authorized.[6]
- Mobile phones will overtake PCs as the dominant web access device worldwide by 2013 according to a new forecast issued by research firm Gartner. Based on Gartner's PC installed base forecast, the total number of PCs in use should top 1.78 billion units in 2013--by that time, the combined installed base of smartphones and browser-equipped enhanced phones is expected to exceed 1.82 billion units,[7]
- Infecting a business network can be achieved when a user syncs an infected smartphone to their desktop or business laptop computer connected to an enterprise network. Such security breaches violate policy, compliance and regulatory guidelines and create the very real risk of data breaches through another path.

Market Impact Analysis:

Enterprise policy control, compliance and reporting – or perhaps not

Many enterprises have resigned themselves to permitting and authorizing users to only use BlackBerry phones on their networks given the nature of their security and moreover, policy control. However, with the functionality of the iPhone far above that of an average BlackBerry, many IT and IS directors are plagued with countless rogue devices on their enterprise, with no visibility, security measures or control and policies. In fact, in more cases then not, such enterprise directors would embrace the iPhone if it could give them the same breadth of control, reporting, security and compliance as the BlackBerry.

Surprising, however, are the countless organizations permitting 'personally liable' (or employee owned) smartphones on their network – often regardless of the kind of device or the potential liabilities involved. As reported by Aberdeen in a recent survey titled "Enterprise Mobility Strategies 2010: More Mobility, Same Budget." - more than two-thirds (73 percent) of respondents indicated that some or all employees were permitted to use personal-liable mobile devices for corporate use.[8]

[1] Fierce Mobile Content, Jan 2010

[2] ComScore Mobile Financial Services Market, July 2009

[3] http://www.theregister.co.uk/2010/02/23/smartphone_rootkits_demoed/

[4] http://www.theregister.co.uk/2010/02/24/mobile_network_security_threats/

[5] http://247wallst.com/?s=Hackers+To+Hit+Apple+iPhone%2C+Google+Android+Handsets+Next+Year

[6] http://www.emailsecuritymatters.com/site/blog/email-security/anti-spam-hacking-and-virus-security-how-will-smartphones-survive/

[7] http://www.fiercemobilecontent.com

[8] Aberdeen Group - *"Enterprise Mobility Strategies 2010: More Mobility, Same Budget."*

Regardless of company owned, or employee owned, the average employee has multiple email accounts on their smartphone of choice – most of which are not under corporate management, compliance control or accountability. Meanwhile, on average from 67-89% of emails are unwanted and potentially dangerous. Nonetheless, millions of mobile smartphone connect to corporate equipment and information, potentially exposing companies to threats like phishing, malware, SPAM, and viruses.

Operational Impact Analysis

So what if?

Information security and information technology is always a delicate balancing act between ease of use, functionality, business need, risk and of course cost/benefit. So what if you could finally have your enterprise cake and eat it to?

- ***Scenario 1***
  - You are a BlackBerry shop, have rogue iPhones (and other smartphones) on your network but have no control or visibility of them or personal email use by employees on those devices
  - As a corporation, you want to be able to offer employees the option of using those devices secured, controlled and owned by the organization
  - Advantages are compliance through policy control, security and visibility

- **Scenario 2**
  - You allow employees to access company email from their own devices and as a result have little to no visibility of the devices or controls and security over their usage
  - As a corporation, for budgetary, privacy-related or other purposes, you want to keep your current policy of letting employees use their own smartphones, but recognize the need for policy control and security knowing those devices touch your network

- **Scenario 3**
  - You are primarily a BlackBerry shop, have rogue iPhones (and other smartphones) on your network and recognize you need some control over them but do not want to offer such company owned devices
  - This is the 'If you can't beat them, join them' scenario where you cannot stop the behavior but would like to control your risk

Financial Impact Analysis:

What is all of this really costing you now – total cost of ownership (TCO) and cost benefit

According to a recent Gartner study, managed mobile devices have significantly lower TCO (by 53% to 63%) than unmanaged devices.[9] This is because enterprise resources often end up supporting their users who are using unsanctioned mobile devices. The time, effort and costs associated with this 'out of band' assistance are significant as planning, procedures, training and tools are not in place to help a enterprise IT support team properly address issues. Conversely, when IT managers are able to provide mobile device management, they can predict what resources, skill sets and infrastructure is needed to

[9] Four TCO Profiles for Smartphones and PDAs: 2009 Update - 19 October 2009 Federica Troni, Ken Dulaney Gartner RAS Core Research Note G00171705

ensure proper service levels and security compliance are achieved within their budgets. Smartphones must be treated as another computing device or TCO will soar. As Strategy Analytics puts it “Mobility management in the enterprise must encompass a life-cycle approach, mimicking a traditional IT computing strategy.”[10]

Solutions Impact Analysis:

Now you can have your smartphone cake and eat it too

Recognizing the organizational need for BlackBerry-like enterprise control over iPhones and all other smartphones, Mobile Active Defense (MAD) has both created the cloud based technology for solving the phishing, malware, virus and SPAM problems while also providing organizations with the policy, compliance and device controls that are sorely needed.

Using MAD's patent pending cloud technology, all of your user's emails from all of their accounts (personal and business) are screened in the cloud before they ever reach the smartphone. This ensures that users are getting the best protection available even for accounts outside the corporate backbone lowering the risk of threat to your network. Because of the unique way MAD functions, it works with the existing smartphone email application making supporting the user simple, regardless of the scenario you are in as mentioned earlier.

Phone based solutions require constant updating of signatures to make sure the user's protection is current. This wastes time and bandwidth with each update having to be downloaded to their telephone limiting updates to a few times per week increasing the odds that a new threat could harm your resources. MAD performs over 100 updates every day without any intervention from the user or the need to download anything to their phone. This ensures that they always have the latest protection available against the newest threats.

Traditional PC/laptop security approaches require substantial resource utilization; processes, cycles, RAM and storage, straining performance and often creating operational conflicts. With MAD’s cloud, only a very thin client code (App) is installed on the smartphone – and all of the heavy work is done in the MAD cloud.

Finally, MAD provides protection, control and compliance when iPhones and other smartphones are connected to your network. With MAD’s Managed Security Service, small to medium enterprises can outsource the entire function, knowing that your risks are being mitigated constantly. Or, some organizations will prefer to use MAD’s upcoming Enterprise Management Console and operate their mobile security cloud within their own networks.

MAD can be up and running for your users in less than 5 minutes. Simply preinstall the MAD Controller Application to a user’s smartphone prior to them collecting it. For user-owned devices or corporate devices already in user possession, users merely download and install the software from your company’s network. MAD help videos make this is a simple process. The MAD application will import all of the

[10] Measuring the Value of Mobile Device Management – Philippe Winthrop, Strategy Analytics, 30, November 2009

user's existing email configurations so that they do not have to retype technical server information. Then they simply tell the MAD app on their smartphone which of their email accounts (unlimited number per phone) they want to protect.

MAD does the rest.

Key features of MAD:

- Combine and manage all smartphones with the MAD MSP or the Enterprise Console
- Filters all of a user's email accounts, not just the corporate one
- Filters emails for viruses, malware, and SPAM
- Prevents phishing attacks by removing them before they reach your users
- Deletes messages that are too large before being downloaded drastically lowering bandwidth usage
- Does NOT slow down the smartphone
- Works with existing smartphone email applications
- Includes online Security Awareness Training and Testing for your entire company – for free.
- MAD gets updated over 100 times a day to keep you safe from the newest threats
- Automatically imports all of existing email server configuration information from the phone with no need to retype complicated server information
- Supports POP3 and IMAP email accounts (Exchange 2Q2010)
- No limit to the number of email accounts that can be protected
- Works with all leading online email services including Gmail, Yahoo, and AOL
- Requires no technical background to install and configure. Grandma can do it!
- MAD is the first virus and SPAM protection available for the iPhone (MSRP $16.99 per seat available in the Apple Store Today!)
- MAD is also available for Microsoft Mobile, and NOKIA Symbian today!
- Call or email for more information and Enterprise pricing.

Christopher Breceda
760.613.4788
sales@mobileactivedefense.com

www.mobileactivedefense.com