



## BLACKBERRY EXPLOIT An Open Door to Your Corporate Network

RISK ADVISORY • TAX • FINANCE & ACCOUNTING

### THE EXPLOIT

Recently, an attack was identified that provides outsiders with direct access to corporate systems and network data through a linked Blackberry or other personal digital assistant (PDA), bypassing all implemented external access barriers. The attack uses Trojan code based on a Blackberry proxy attack (BBProxy).

Blackberry devices are typically connected to a corporate network through a “persistent tunnel” implemented via a protected VPN that prevents the communication from being inspected by an external process. This connection is terminated within the network at the corporate Blackberry server. The effect of this connection is to make the Blackberry essentially part of the internal network, regardless of the Blackberry’s connection point.

When the BBProxy Trojan is installed, it opens an additional encrypted tunnel between the Blackberry and the attacker’s server, establishing the Blackberry as a remote device on the attacker’s network. The attacker can then initiate a new link from the Blackberry through the already established VPN connection to the corporate network. Again, normal corporate security processes are ineffective because this tunnel is

encrypted. At the point the Blackberry is connected to both the corporate network and the attacker’s server, it acts as a proxy between the two.

Since the Trojan allows the attacker control of this proxy link, the corporate network is now open to the attacker via the unaware proxy device. Tools such as Metasploit, a full-function, menu-driven attack tool, now have exploits available to target this connection via transmission control protocol (TCP). The attacker is then able to use the Blackberry as a staging point to attack corporate systems, attempting to gain root/administrative access to internal servers or obtain and copy documents or data from those servers. Because the link is already established within the boundaries of the corporate network, such an attack avoids the organization’s IDS/IPS systems on its external boundaries. In addition, the attacker has access to all personal information and functions available through the Blackberry device.

This type of attack is equivalent to the old practice of implementing dial-up modems on user workstations, which was “outlawed” by IT a number of years ago, but this attack targets the newer remote technology.

Thankfully, an attack like the Blackberry exploit cannot be implemented against

Jefferson Wells delivers professional services in the areas of risk advisory, tax, and finance and accounting. We serve clients, including Fortune 500 and Global 1000 companies, through highly experienced professionals working from offices worldwide.

To learn more about our firm and our professional services, contact your local Business Development Manager or visit our Web site at [www.jeffersonwells.com](http://www.jeffersonwells.com).

## 10 WAYS TO PROTECT YOUR CORPORATE NETWORK

1. Bring PDAs into the scope of your local information protection program.
2. Enlist support of management by presenting it with the risks involved, along with a plan to address those risks in a consistent and cost-effective manner.
3. Formalize your corporate position on PDAs via a management-endorsed corporate policy.
4. If they will be used to link to the corporate network and process corporate data, documents or e-mail, determine the appropriate measures required to secure these devices.
5. Standardize the use of PDAs on a select subset of devices that are congruent with the protective measures to be employed and that support the implemented controls.
6. Segment the corporate PDA server to separate it from other corporate resources, just as with other remote-access servers.
7. Bar the PDA from downloading and installing an application from an unapproved Web site.
8. Enforce these measures through technical policies that require the device to be properly secured through an automated download to the device prior to connecting to the corporate network.
9. Implement an integrity management product at the corporate level to verify and disable a device that does not meet these security control requirements.
10. Require employees to work within these controls, and disable the connection of any device that has been altered so it deviates from the required baseline.

a PDA unless the owner in question visits a Web site housing the Trojan and specifically downloads and installs it. The Trojan is typically disguised as a game or popular utility. The exploit can, therefore, be prevented by implementing baseline security controls for all PDAs connected to the corporate network. (See *10 Ways to Protect Your Corporate Network*.) However, unprotected PDAs connected to the corporate network leave corporate data and systems open to this attack.

## PERSONAL DIGITAL ASSISTANT (PDA) SECURITY

PDA security is often overlooked by organizations' information protection programs. That's because these protection programs are typically IT-focused, and Blackberrys and other PDAs are frequently used within the network by senior executives and other corporate management and by other employees at all levels of the organization. They, therefore, fall outside the scope of a centralized IT information protection initiative even though PDAs can receive and process viruses and are subject to additional exploits that are often unaddressed.

After all, PDAs are computers. And their use on the corporate network subjects the corporate network to a number of threats that all computers share. These include:

- Viruses, Trojans and worms
- Theft of the physical PDA device
- Data theft
- Mobile code exploits
- Authentication theft
- Wireless exploits
- Denial-of-service attacks
- TCP session hijacking
- Bluetooth communications eavesdropping

PDAs are extremely popular with users because they are always on. So, while its more likely PDAs would be the recipient of malicious code than the subject of a direct attack, they are subject to identification through automated wireless scans, and can be targeted for direct attack. Because the newer generation of PDAs combines the

traditional digital assistant with a smart phone, this likelihood is even greater now than it has been in the past.

Basic protective measures that should be considered for PDAs include:

- Encryption of internal storage
- Password protection
- Automated wiping software that will erase internal storage during attempts to hack the password
- Cloaking software to prevent the PDA from connecting to non-approved wireless points
- Implementing wireless connections through a secure (encrypted) VPN
- Software to protect against malicious code, including viruses, worms and Trojan code
- Automatic software patch updates
- When directly (hard-wire) connected to the corporate network, disabling of the wireless port
- Enabling of security logging and reporting alerts to a corporate address
- Consider disabling Bluetooth communications (headsets) for the phone

Once you have PDAs covered by your protection program, be sure you perform a regular audit of the policies, procedures and control settings that implement the desired corporate policy.

## References

The following contain additional information on this exploit and measures that you can take to protect PDAs.

<http://www.pdastreet.com/articles/2006/8/2006-8-9-BBProxy-Hack-Exposes-print.html>

[http://na.blackberry.com/eng/deliverables/1835/Protecting\\_the\\_BlackBerry\\_device\\_platform\\_against\\_malware.pdf](http://na.blackberry.com/eng/deliverables/1835/Protecting_the_BlackBerry_device_platform_against_malware.pdf)

[http://na.blackberry.com/eng/deliverables/1460/Placing\\_the\\_BlackBerry\\_Enterprise\\_Solution\\_in\\_a\\_Segmented\\_Network.pdf](http://na.blackberry.com/eng/deliverables/1460/Placing_the_BlackBerry_Enterprise_Solution_in_a_Segmented_Network.pdf)

<http://www.blackberrytoday.com/articles/2003/4/2003-4-8-PDA-Security-101-print.html>

<http://www.blackberrytoday.com/articles/2004/6/2004-6-2-Learn-the-Basics-print.html>

<http://www.blackberrytoday.com/articles/2004/8/2004-8-5-Malicious-Code-Exploits-print.html>

