

Blackberry Proof-of-Concept: Malicious Applications

Mayank Aggarwal, C|EH, SCJP
Junos Pulse Global Threat Center
maggarwal@juniper.net

Presented by Konstantin Yemelyanov, PhD
Junos Pulse Global Threat Center
kyemelyanov@juniper.net



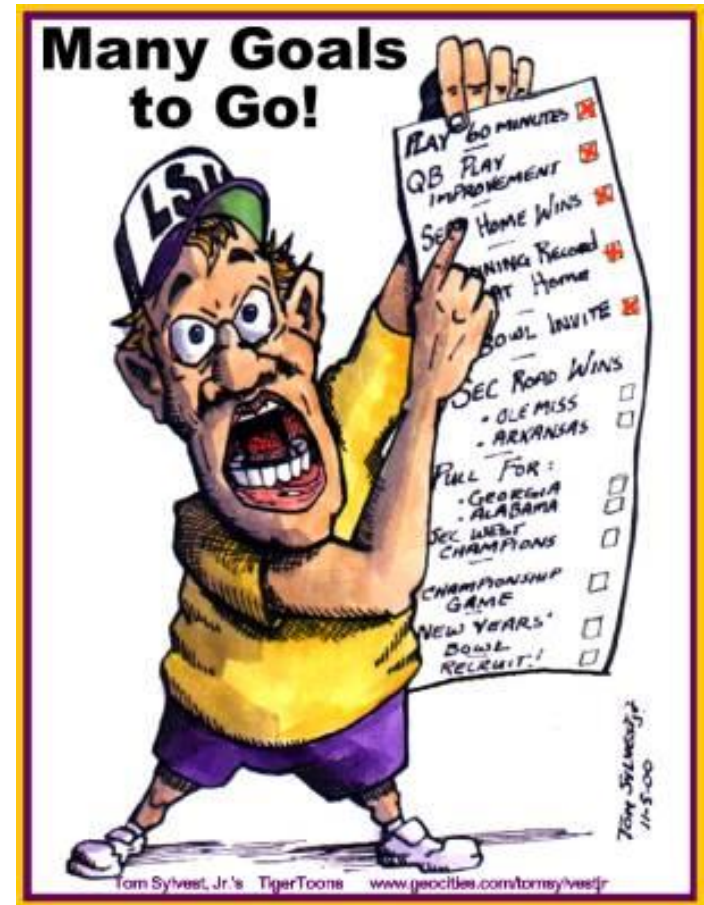
Overview

- ❑ Introduction
- ❑ BlackBerry Security Model
- ❑ Recent Threats
- ❑ Proof-of-Concept
- ❑ Demonstrations



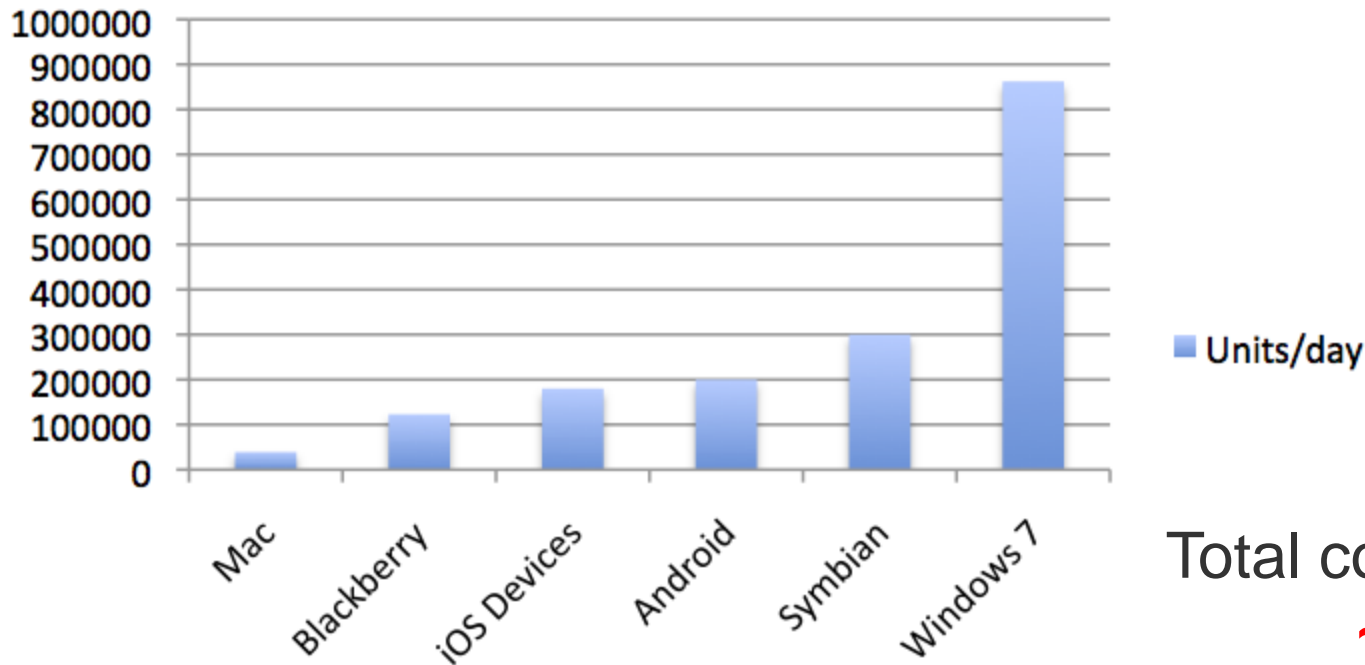
Goals

- ❑ Present the up-to-date state of the BlackBerry mobile security.
- ❑ Discuss commercial spyware & remote monitoring applications.
- ❑ Explore different malicious applications developed for BlackBerry phones.



Smartphone Market

Major OS Global units shipments/day



2010 Smartphone Market (Est. June 28)

Symbian 73 M

iPhone OS 35 M

Android 58 M

Windows Mobile 8.5 M

Blackberry 46 M

Total computer OS sold
~ 887,000

Total mobile OS sold
~ 713,000

Source: CNN Money (August 11, 2010)

BlackBerry Market

US smart phone market	
Leading vendors' share, Q2 2010	
Vendors	United States % share
Total	14.7m
RIM	32.1%
Apple	21.7%
HTC	14.4%
Others	31.8%
Source: Canalys estimates, © Canalys 2010	

Smart phone market grew by

64%

The RIM's BlackBerry market grew by

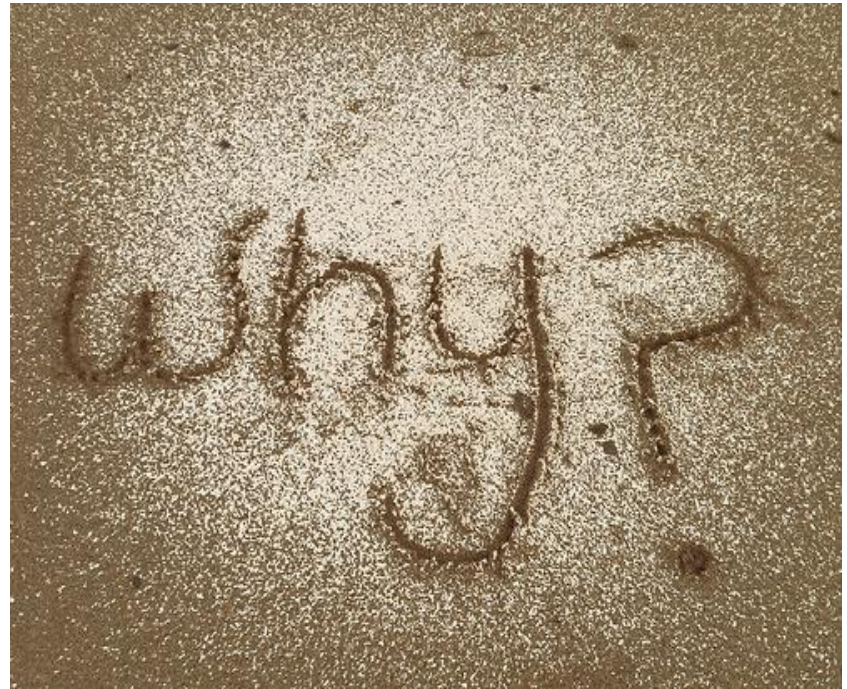
41%.

Why Does Smartphone Security Matter?

Smartphones are rapidly replacing regular phones: by 2012, 65% of all new cell phones will be smartphones.

Smartphones are used for the same activities and have the same capabilities as PCs.

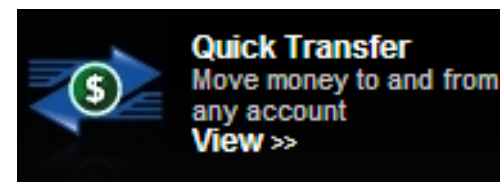
While most PCs have at least some security software in place, smartphones commonly do not have any security software installed.



Mobile Banking is on the Rise

One million mark achieved by Bank of America in active mobile banking customers

Thu. June 12, 2008; Posted: 01:07 PM



Why Does Smartphone Security Matter?

Would you conduct online banking and shopping on a PC without an antivirus software installed?

Are you willing to remove antivirus, firewall, encryption and VPN software on your enterprise workstation?



The Biggest Mobile Device Challenge for Enterprises

Which of the following would you consider to be the biggest mobile device challenges in your organization? (Percent of respondents, N=174, multiple responses accepted)



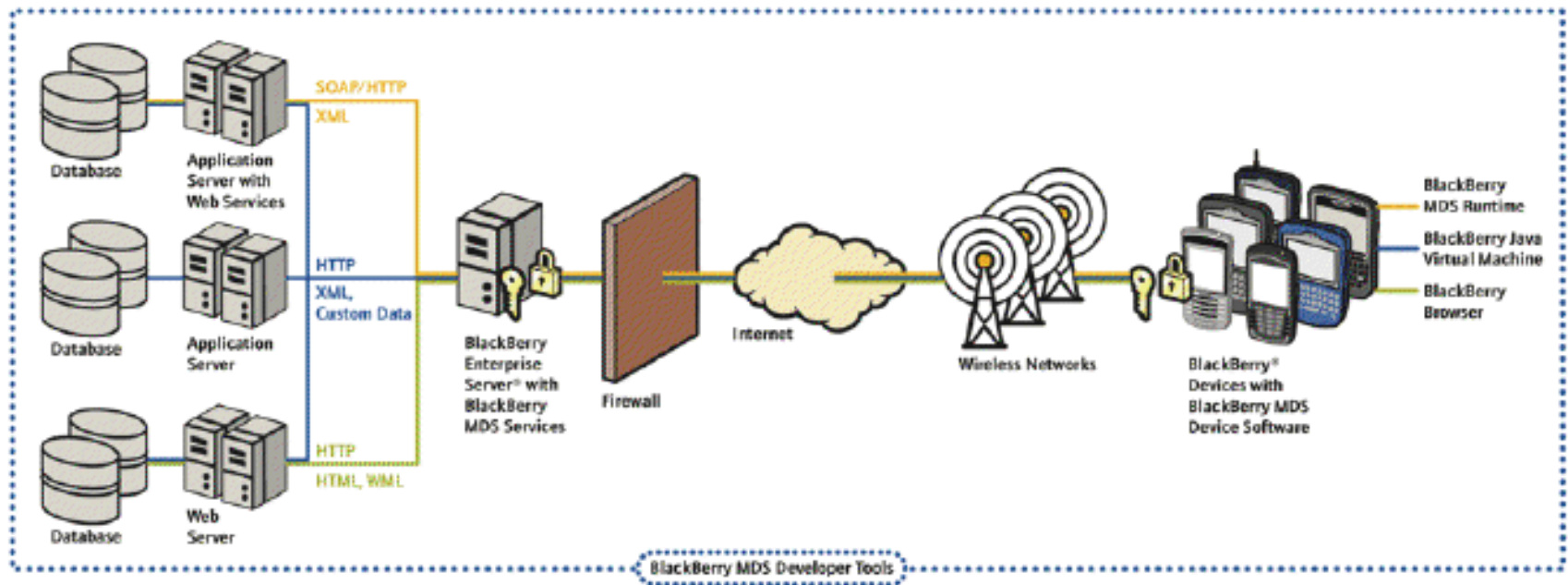
Source: Enterprise Strategy Group, 2010.

Attacker's Motivation

- Smartphone in its present state provides an easy access to the enterprise networks.
- Although smartphone market is growing, the users are unaware of threats to the devices.
- People think that smartphones cannot be hacked as easily as computers.
- Hacking smartphone is easy and quick way to make money.
- Easy to exploit user by social engineering.
- Corporate espionage.



BlackBerry Security Model



BlackBerry Security Model

Q. How does BlackBerry's security system work?

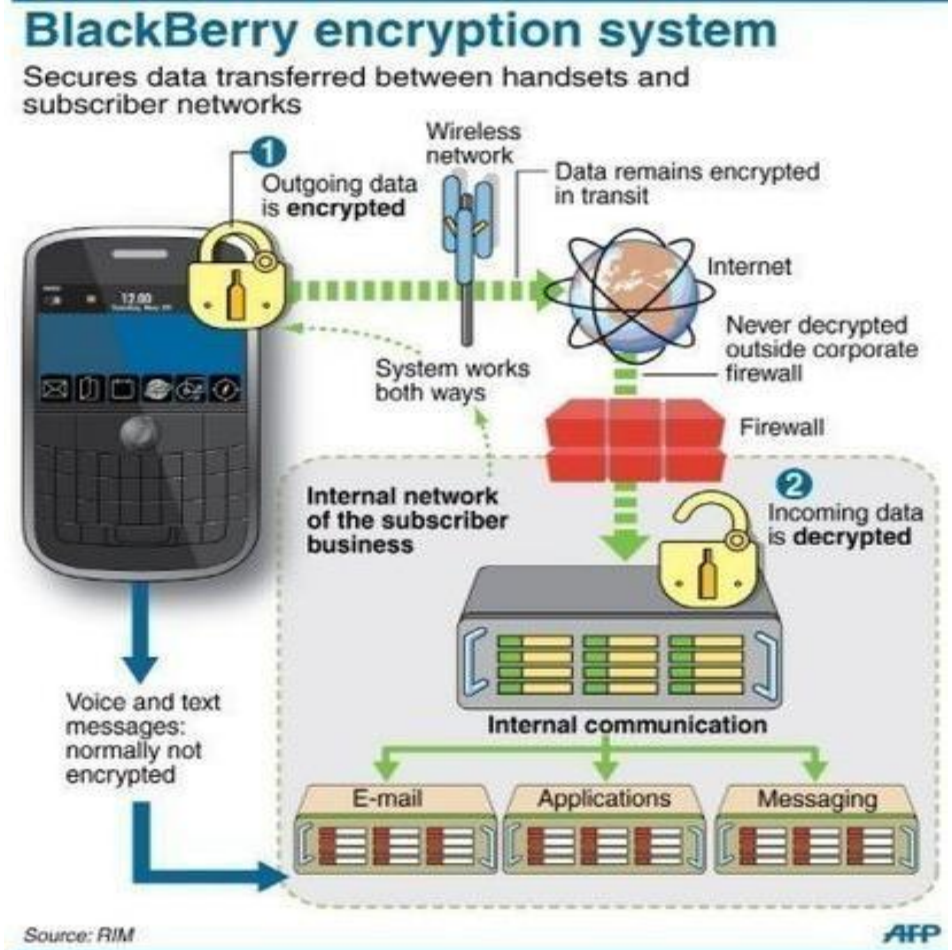
Q. Is BlackBerry's security unique?



Transport Level Security

End-to-end encryption – traffic is encrypted up to RIM servers in Canada.

No man-in-the-middle attack possible – all data traffic is tunneled.



Device Encryption

BlackBerry encrypts the data on both internal and external memory.

Without knowing the password, encrypted SD-card content cannot be accessed even on a different device.

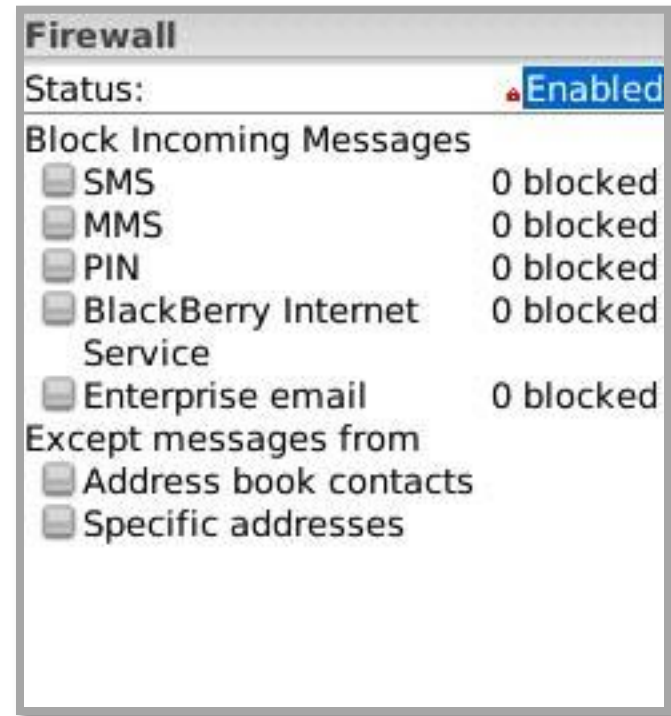
Lost or stolen encrypted devices are still safe.



Device Firewall

BlackBerry device is equipped with built-in firewall.

Option to block SMS, email, MMS and PIN.



Uniqueness of BlackBerry Security

RIM provides a device, a network and a service all bundled together.

Provides an overlay access network, called BIS (Blackberry Internet Service)

RIM network access as a gateway to the internet.

All the information transferred over RIM servers is encrypted with proprietary encryption.

Mobile operators cannot inspect the traffic between BlackBerry and RIM servers.



BlackBerry Security

RIM security chief sees smartphone attacks on horizon



By Wojtek Dabrowski and [Jim Finkle](#)
TORONTO/BOSTON | Tue Nov 17, 2009 4:32pm EST

(Reuters) - Hackers could one day turn ordinary smartphones into "rogue" devices to attack major wireless networks, Research In Motion's security chief warned.

Scott Tetzke, RIM's vice-president of BlackBerry security, said hackers could use smartphones to target wireless carriers using a technique similar to one used in assaults that slowed Internet traffic in the United States and [South Korea](#) in July.

"Smartphone could be used to cripple networks – RIM exec"

"Scott Tetzke, RIM's vice-president of BlackBerry security, said hackers could use smartphones to target wireless carriers."

"Criminals can use phone signals to order tens of thousands computers to contact a targeted site repeatedly, slowing it or eventually crashing it."

Facts & Fictions



Facts:

Very few known vulnerabilities –
no 0wned.

Transport data is encrypted –
no MITM.

No remote installation without user
permission.

Facts & Fictions



Facts:

Device can be lost or stolen.

Device can be controlled remotely .

Once the permission is provided, the full access to the device and it's resources is granted.

Facts & Fictions

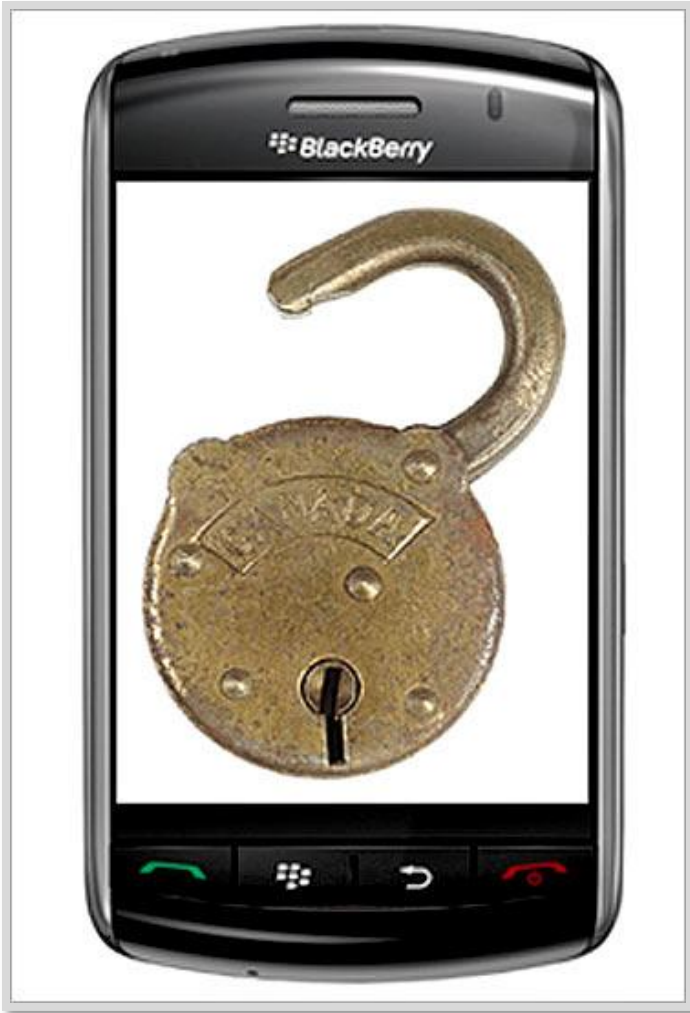
Fiction:
My BlackBerry is Secure.



Recent Threats



Blackjacking – Owning the Enterprise via the Blackberry



First BlackBerry Trojan.

Attack Enterprise Networks.

Allowed access to the internal network.

Use a BlackBerry for proxy connections.

Tool released called BBProxy.

Etisalat – BlackBerry Spyware

SECURITY

July 21, 2009 6:50 PM

RIM: UAE Carrier's Blackberry Update Was Spyware

By Robert McMillan, IDG News

A Blackberry firmware update pushed out by Etisalat contained spyware, Reser

PEOPLE WHO READ THIS ALSO READ:

- ▶ PlayBook Tablet OS Might Move to BlackBerry Phones
- ▶ Blackberry Torch 9800: Try Again, RIM
- ▶ RIM to Battle Apple With New Phone and Tablet, Say Reports
- ▶ RIM Posts Revenue Gains on BlackBerry Sales
- ▶ UAE Will Allow Blackberry Services Past Deadline

UAE Blackberry update was spyware

By Ben Thompson

BBC Middle East Bu

An update for Blackberry in the United Arab Emirates could allow unauthorized access to private data and e-mails.

The update was pushed out by Etisalat, suggesting it might improve performance.

Instead, the update caused the phone to crash or drain the battery life.

Blackberry maker RIM said in a statement that the update was not developed, or tested.

BlackBerry update bursting with spyware

Official snooping suspected in UAE

By Bill Ray • [Get more from this author](#)

Posted in Malware, 14th July 2009 18:31 GMT

[Free whitepaper – Protecting personally identifiable information](#)

An update pushed out to BlackBerry users on the Etisalat network in the United Arab Emirates appears to contain remotely-triggered spyware that allows the interception of messages and emails, as well as crippling battery life.

Sent out as a WAP Push message, the update installs a Java file that one curious customer decided to take a closer look at, only to discover an application intended to intercept both email and text messages, sending a copy to an Etisalat server without the user being aware of anything beyond a slightly excessive battery drain.

It was, it seems, the battery issue that alerted users to something being wrong. Closer examination (as reported by itp.net) seems to indicate that all instances of the application were expected to register with a central server, which couldn't cope with the traffic - thus forcing all the instances to repeatedly attempt to connect while draining the battery. A more phased reporting system might have escaped detection completely.

PCWorld

BBC News

The Register

How does it work?



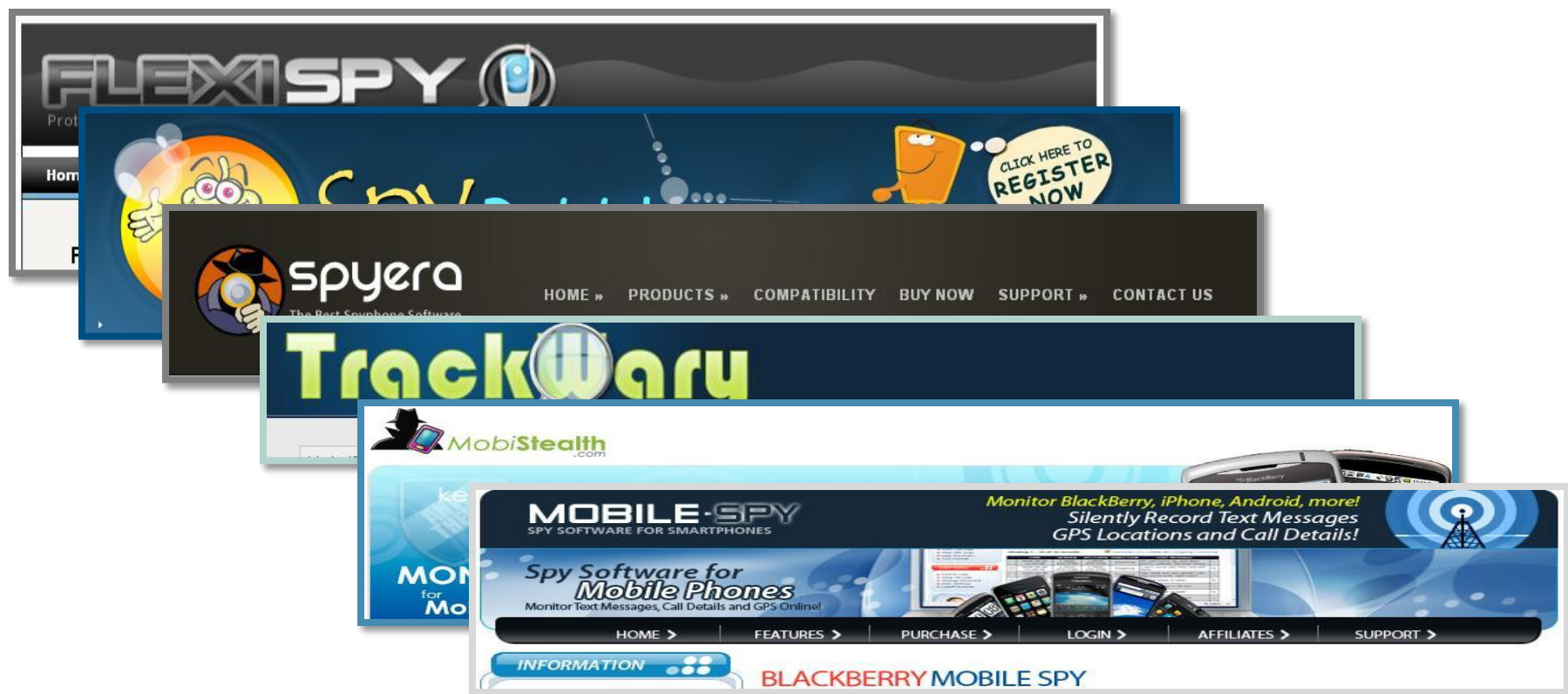
- Etisalat pushed out a network update to BlackBerry users.
- Such update, a remotely-triggered spyware, intercepted messages and e-mails.
- No visible icon and run at the background.
- Stays dormant until command message is received.
- Once activated, forwards all outgoing emails to a server.

Commercial Spyware



Copyright MAD Magazine

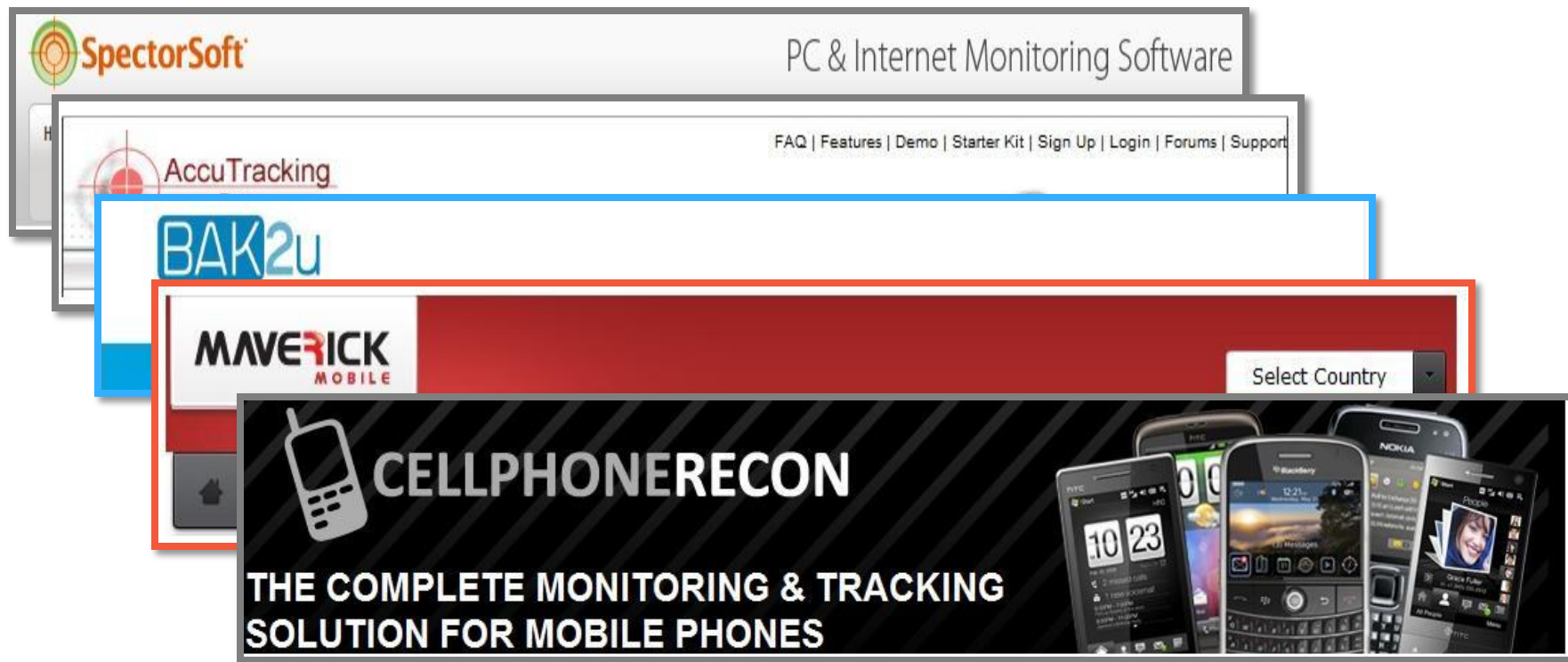
Commercial Spyware



“FlexiSpy offered the first commercial spyware for BlackBerry in 2006.”

“Eighty percent of commercial spyware applications have surfaced in less than a year.”

Commercial Spyware (cont'd)



“Above mentioned vendors sell their software as remote monitoring application.”

“However, due to the hidden and stealth nature of the application, it has a potential to be misused as a spyware.”

Commercial Spyware

Feature comparison

	FlexiSpy	MobileSpy	MobiStealth	SpyBubble	TrackWary	Spyera
Remote Monitoring	Yes	No	Yes	No	Yes	Yes
GPS tracking	Yes	Yes	Yes	Yes	Yes	Yes
View Photos	No	Yes	Yes	No	Yes	No
Read SMS	Yes	Yes	Yes	Yes	Yes	Yes
View call logs	Yes	Yes	Yes	Yes	Yes	Yes
Read Email	Yes	Yes	Yes	No	Yes	Yes
View Contacts	No	Yes	Yes	Yes	Yes	No
View Calendar	No	Yes	Yes	No	Yes	No
View Videos	No	Yes	Yes	No	Yes	No
BlackBerry Messenger Log	Yes	No	Yes	No	Yes	No

“Commercial spyware remotely monitors all the smartphone activity and invades into the user’s privacy”

“Price varies from \$50- \$400 depending on activation duration and types of features.

Remote Monitoring

SMobile Security Shield Parental Control dashboard

Home Reports Account Settings **Picture Viewer** Glossary

Welcome **epix@a.a**


Picture Viewer

Select Phone to View: 10

view 5 10 15 20 25

Total Pictures: 15

You have 0 Alerts
click to view alerts or configure notifications



MobileTracker
World Edition

[Features](#) | [Technical Details](#) | [Purchase](#)

Easily record tracklogs using your BlackBerry® Smartphone and view them in Google Earth™ or publish them with Google Maps™.

- Records a GPS tracklog.
- Elevation & time can be tracked.
- Easy one-click tracklog recording.
- Extensive statistical information and background tracking.

Guaranteed: **100% subscription free!**

BUY NOW - Only \$9.99

Get it at  **BlackBerry App World.**

Spyware or Remote Monitoring?

It's a **Spyware** if:

- Application's icon is hidden.
- User doesn't have information about application's activity.
- User did not provide a consent to install the application.



Spyware or Remote Monitoring ?

It's a **Remote Monitoring** if:

- The application has a visible icon.
- The user can control and monitor the operation.
- The users agree on certain invasion into their privacy ☺



Cut the Crap! Show me the Hack!



Demo Part I



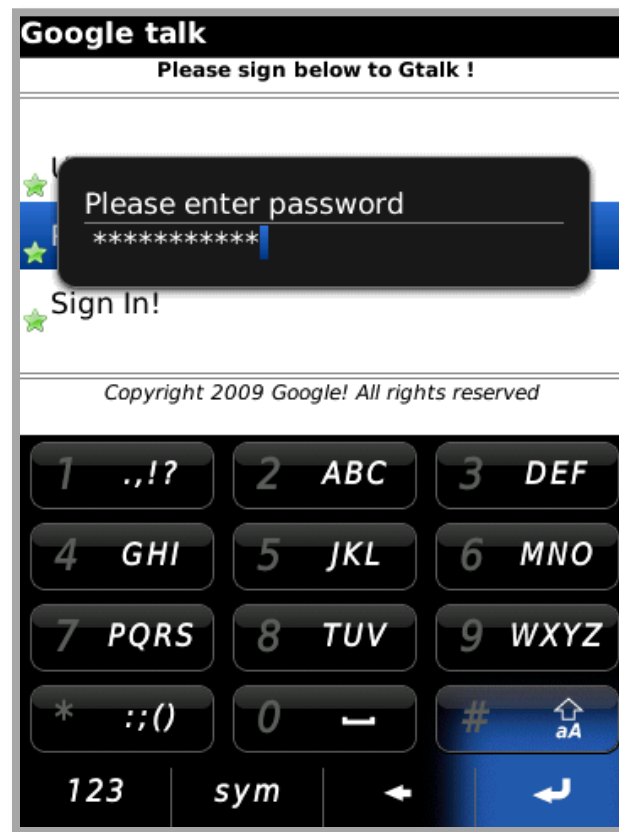
Hacker's at WORK 😊

Phishing Application

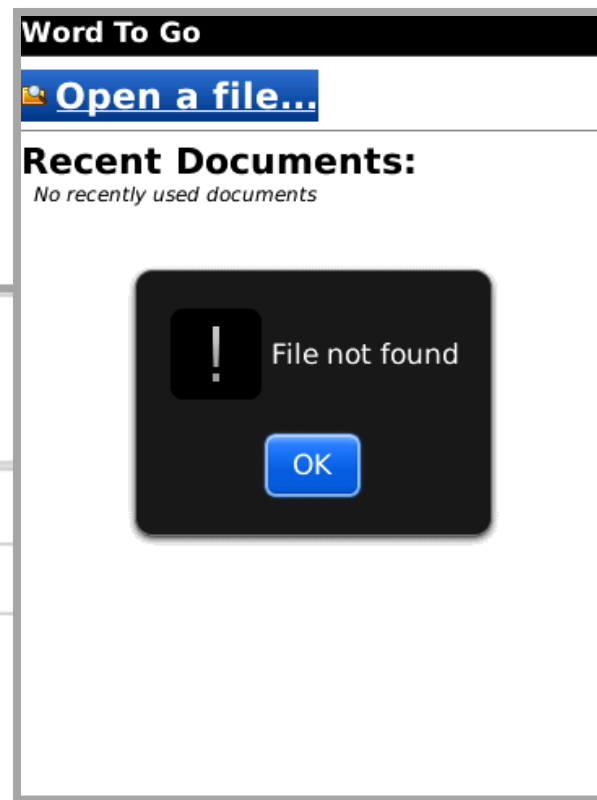
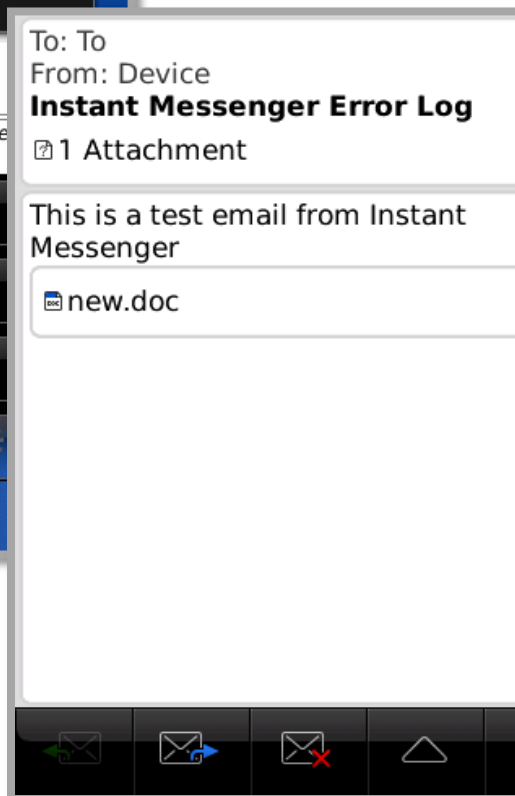
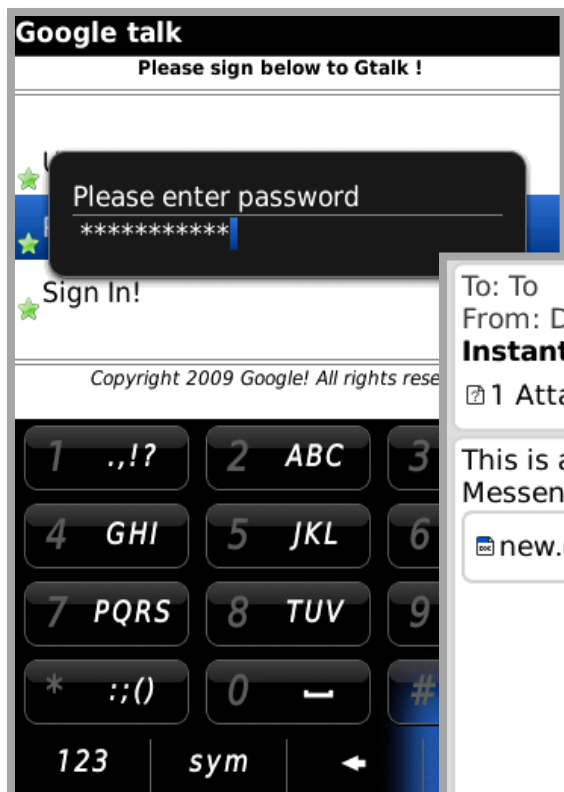
Acquire user's login and password.

Send login/password details to the attacker.

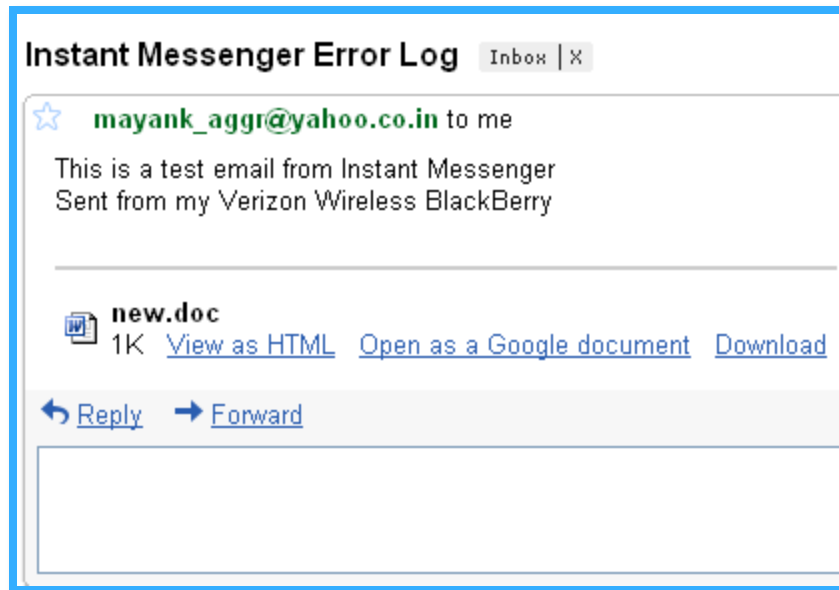
The victim has no way to identify the information sent to attacker's email.



Phishing Application- Victim's BlackBerry



Phishing Application (cont'd)



[Download the original attachment](#)

User:dave Password: columbus198



Demo Part II



Spyware Application

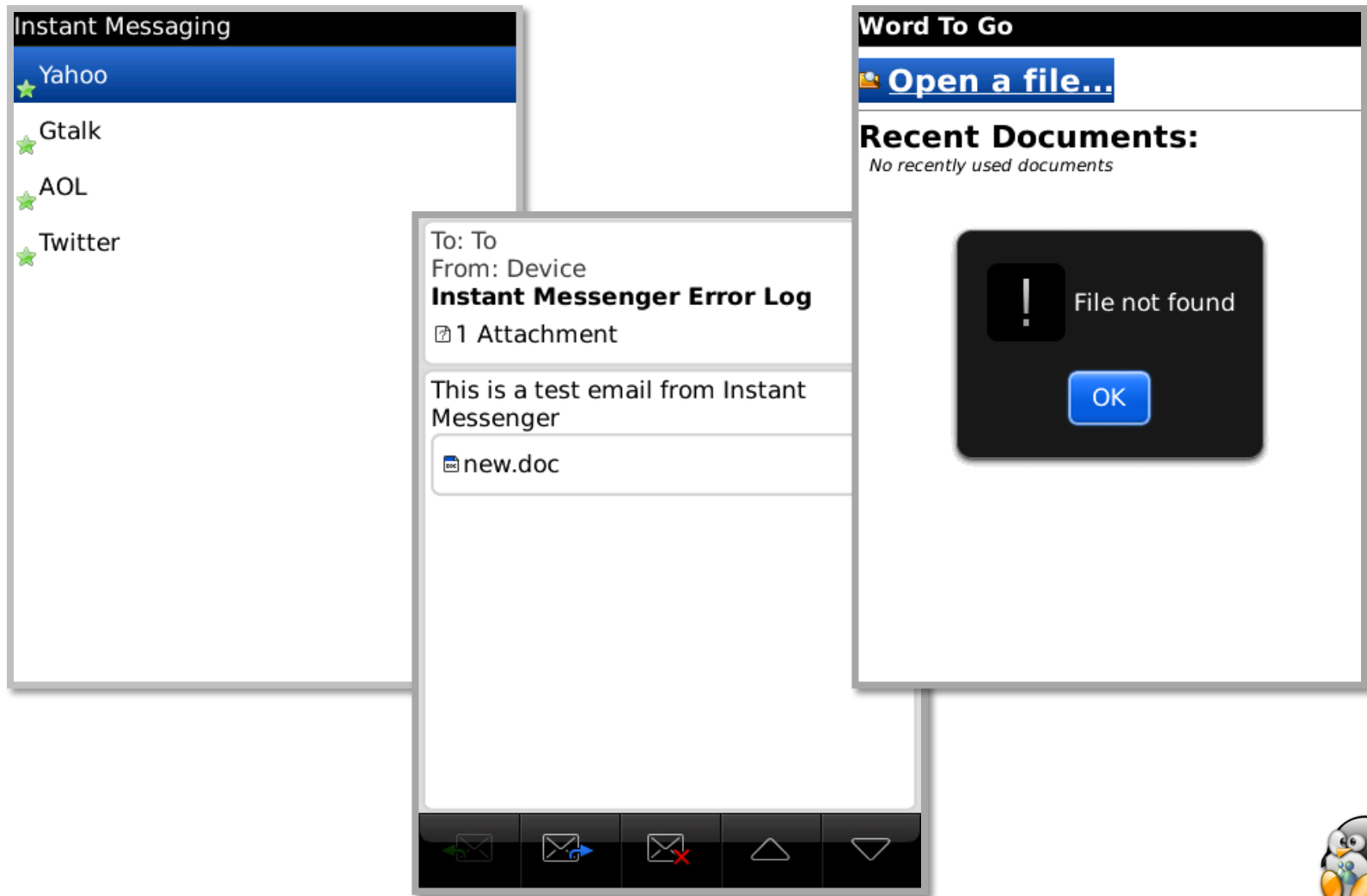
Captures data from the device's external memory and emails it to the attacker.

As of today: collects *.doc, *.pdf and images stored on SD card.

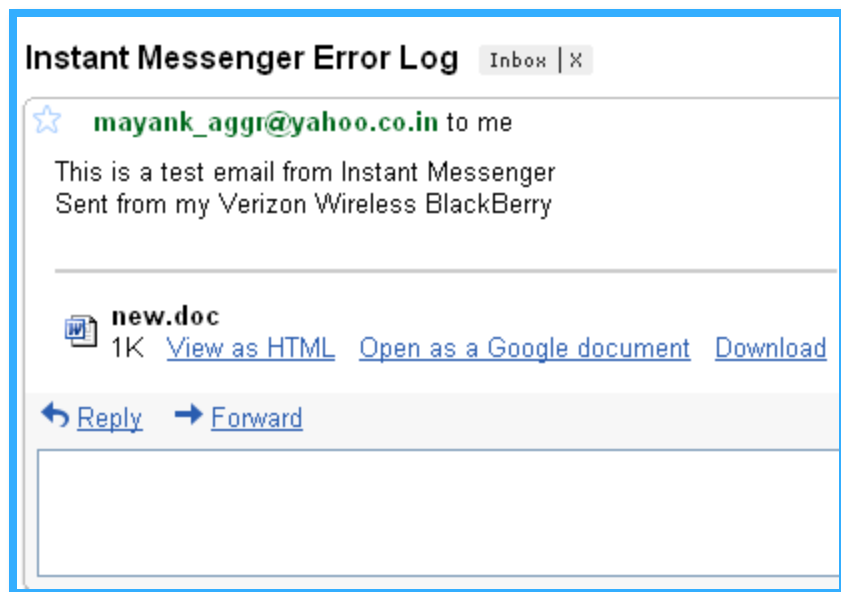
The victim can not identify the information sent in an email.



Spyware Application - Victim's BlackBerry



Spyware Application - Attacker's machine



[Download the original attachment](#)

How to crack wireless network

Tools Needed

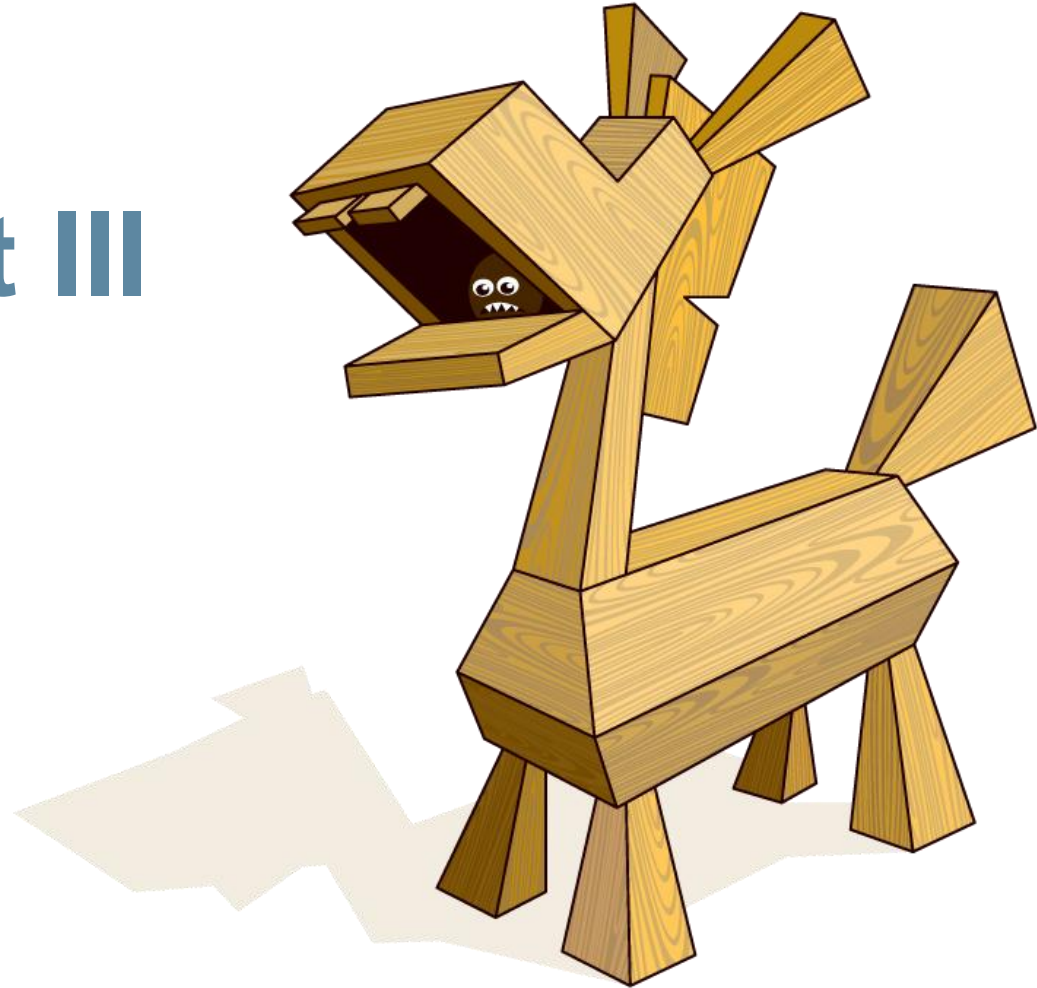
1. Air-crack suite

Steps to be followed:

1. `sudo airmon-ng start wlan0`
2. `sudo airodump-ng - testfile wlan0`
 - a. Note BSSID, Channel #, ESSID



Demo Part III



Trojan Application

Acts as a messenger application.

Deletes all the information from the SD card.



Trojan Application - Victim's BlackBerry

Twitter
Please sign below to Twitter!

★ User Name
★ Password
★ Sign In!

© 2010 Twitter! All rights reserved

...ia Card/BlackBerry/documents/

...ia Card/BlackBerry/doc

Android_Packages.txt	
Android_permissions.txt	21KB
bbdevicesim.txt	27KB
device-state.txt	738KB
log.txt	55KB
virusdb.txt	36KB
viruses.txt	32KB



Reality Bites

- No spyware is as stealthy as claimed.
- User can identify application even if an application icon is hidden.
- Once the application is installed and requested permissions are approved, the complete access to the device is granted.

What if your application leaks server information?

A well-known remote monitoring / commercial spyware leaks it's server login information.

Application features:

- Remote Listening
- C&C Over SMS
- Pictures, Video & Audio Logging
- SMS & Email Logging
- Call History Logging
- Location Tracking
- Call Interception
- GPS Tracking

What if your application leaks server information?

```
[EmailCDRProcessor]: Printing number of calls in the call log folders
[EmailDebugManager]: return Stored Command is LOCATION_LOG_STOP
[EmailCMM]: EmailClient3(4754) no sig from 0x33
[EmailSettingGetter]: going to process settings if available
[EmailDownloadManager]: inside areCommandsAvailable
[EmailCMM]: EmailClient3-1(4798) no sig from 0x33
[EmailFTPClient]: File to upload: 432984540532109-stealth-20101008172122.sys
[EmailJVM]: bklt @1137770: timer
[EmailJVM]: bklt @1137770: idle 15
[EmailDownloadManager]: inside sendHttpRequest
[EmailConfigurations]: initUser: [REDACTED].com
[EmailConfigurations]: initPassword: KWwL[REDACTED]
[EmailDownloadManager]: url: http://[REDACTED].php?imei=432
[EmailCMM]: EmailClient3(4754) no sig from 0x33
[EmailConfigurations]: serverIP: [REDACTED]
[EmailEncryptionDecryption]: inside encryptData
[EmailEncryptionDecryption]: data is encrypted 176
[EmailFTPClient]: FTP try 0
[EmailCMM]: EmailClient3-1(4798) no sig from 0x33
[EmailHTTPUpload]: response is SUCCESS
```



Where do we go from here?

Conclusion

- ❑ Unlike iPhone, BlackBerry applications can be obtained from anywhere.
- ❑ Once installed, the application can gain complete access to the device.
- ❑ Lack of real time detection and eradication.
- ❑ Free apps are not always free.
- ❑ Enable firewall and device encryption.
- ❑ Set the device password.
- ❑ Finally, don't let others use your phone.

“

Regardless of any sort of filtering, scanning, firewall, protection or analyzing software you may have, there is no substitute for common sense and a healthy dose of skepticism.

”

Questions?



Thank You for Coming!



maggarwal@juniper.net



[@unsecuremobile](https://twitter.com/unsecuremobile)

