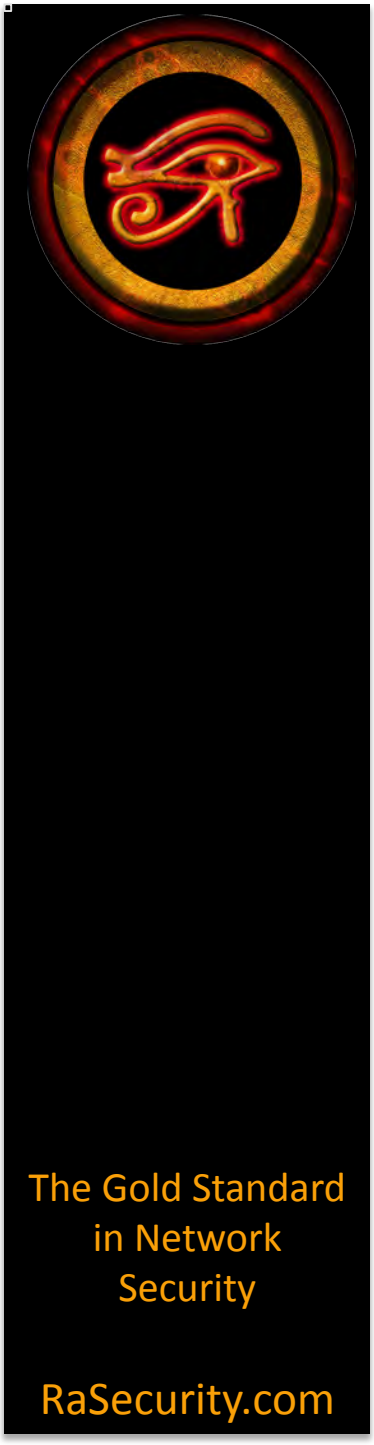
Mobile Computing in The Banking Environment

By

Gideon J. Lenkey CISSP

The Gold Standard in Network Security

RaSecurity.com



Shameless Plug

- Co-Founder of Ra Security Systems, Inc.
- Managed Security Services and Security Assessments
- Buy my book: Gray Hat Hacking 3rd ed.
- See me in a movie: Code 2600
- "Google" me or grab a brochure

What We'll Cover

- Risks associated with mobile devices
- Threat Trends and Projections
- What you can do to Cover Your Assets

The Gold Standard in Network Security

RaSecurity.com

Contemporary Mobile Devices

- More powerful than early PCs
- Always on Internet connectivity
- Text Messaging
- Email
- Personal Information Manager
- GPS
- Camera

A World of Information

- Contacts
- Email and Voicemail Communications
- Social Affiliations
- Where you are and have recently been
- Times and Places you will be in the future
- Where you live and work

The Gold Standard in Network Security

RaSecurity.com

Attack Vectors

- Physical Access
- Bluetooth
- Wifi
- SMS / MMS
- Voicemail
- Applications (Browser, Email, PDF etc.)

The Gold Standard in Network Security

RaSecurity.com

Physical Access

- Copy entire device for analysis
- Install Monitoring Software
  - Monitor ALL communications
  - Track location at all times
  - Activate microphone
  - Initiate Calls or SMS messages

The Gold Standard in Network Security

RaSecurity.com

INFORMATION

- Software Features
- Mobile Spy Uses
- Compatibility
- Online Demo
- How it Works
- Purchase Now

SUPPORT

- Help Center
- Software FAQ
- User Guide
- Affiliate Info
- Legal Info
- About Us

FEATURES MOBILE SPY

Reveal the Truth in Real Time!

Are your children or employees abusing the privileges of texting and calling? Are you worried they are using the phone for unallowed or inappropriate activities?

Mobile Spy will reveal the truth for any company or family. You will finally learn the truth about their call, mobile web, text message activities, photo, videos and GPS locations by logging into your Mobile Spy account from any web browser.

With the optional LIVE Control Panel, you can view the phone's screen and location **LIVE**, as well as remotely control the phone and retrieve up-to-the-minute information about the phone! This option also gives you the ability to have your logs delivered to your email address automatically.

Program Description

Mobile Spy is a hybrid software/service which allows you to monitor your smartphone in real time. This unique system records the activities of anyone who uses your iPhone, BlackBerry, Android, Windows Mobile or Symbian OS smartphone.

You install a small application **directly onto the phone you own and want to monitor**. It starts at every boot of the phone, remains stealth and does not show up in the running process list.

After the software is setup on the **monitored phone**, it will record an array of phone activities and then silently upload the data to your private Mobile Spy account using the Internet. When you want to view results, simply login from any web browser and enter your username and password.

Smartphone Interface (BlackBerry Version shown)

This program is loaded **directly onto the phone you want to monitor**. It stays


Locate...
Pinpoint device on map
Scream...
Sound alarm on device
Premium
Lock...
Prevent use of device
Premium
Wipe...
Delete data on device
Map
Satellite
Hybrid
06:49 PM Pacific Time (US & Canada)
Saturday, January 22, 2011
Accuracy: 8 meters
Google
Imagery ©2011 DigitalGlobe, USDA Farm Service Agency, IndianaMap Framework Data, GeoEye, U.S. Geological Survey – Terms of Use

SpectorSoft

Computer & Internet Monitoring Software

HOME PRODUCTS PURCHASE ABOUT US PRESS PARTNERS SUPPORT WEBINARS

CALL: 1-888-598-2788 -OR- 1-772-770-5670

eBLASTER® | mobile

Now available on Android™ and BlackBerry® Smartphones

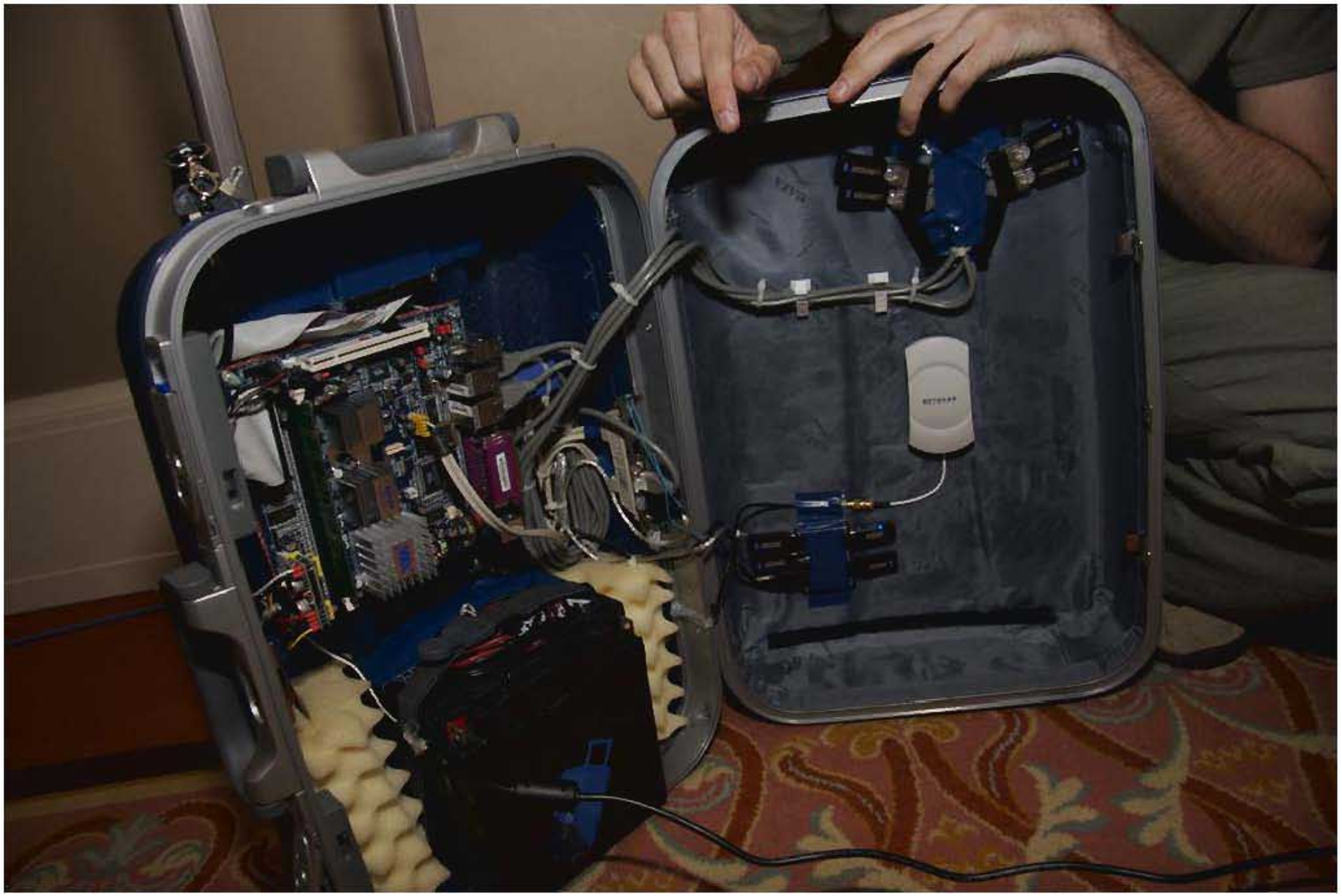
Monitor activity on Android or BlackBerry devices
from work, home, business trips, or vacations ... even if you are thousands of miles away!

Bluetooth

- iPhone remote code execution 2007
- Default security code 0000
- Headset Eavesdropping
- Audio Injection
- Attack range and be greatly extended

The Gold Standard in Network Security

RaSecurity.com

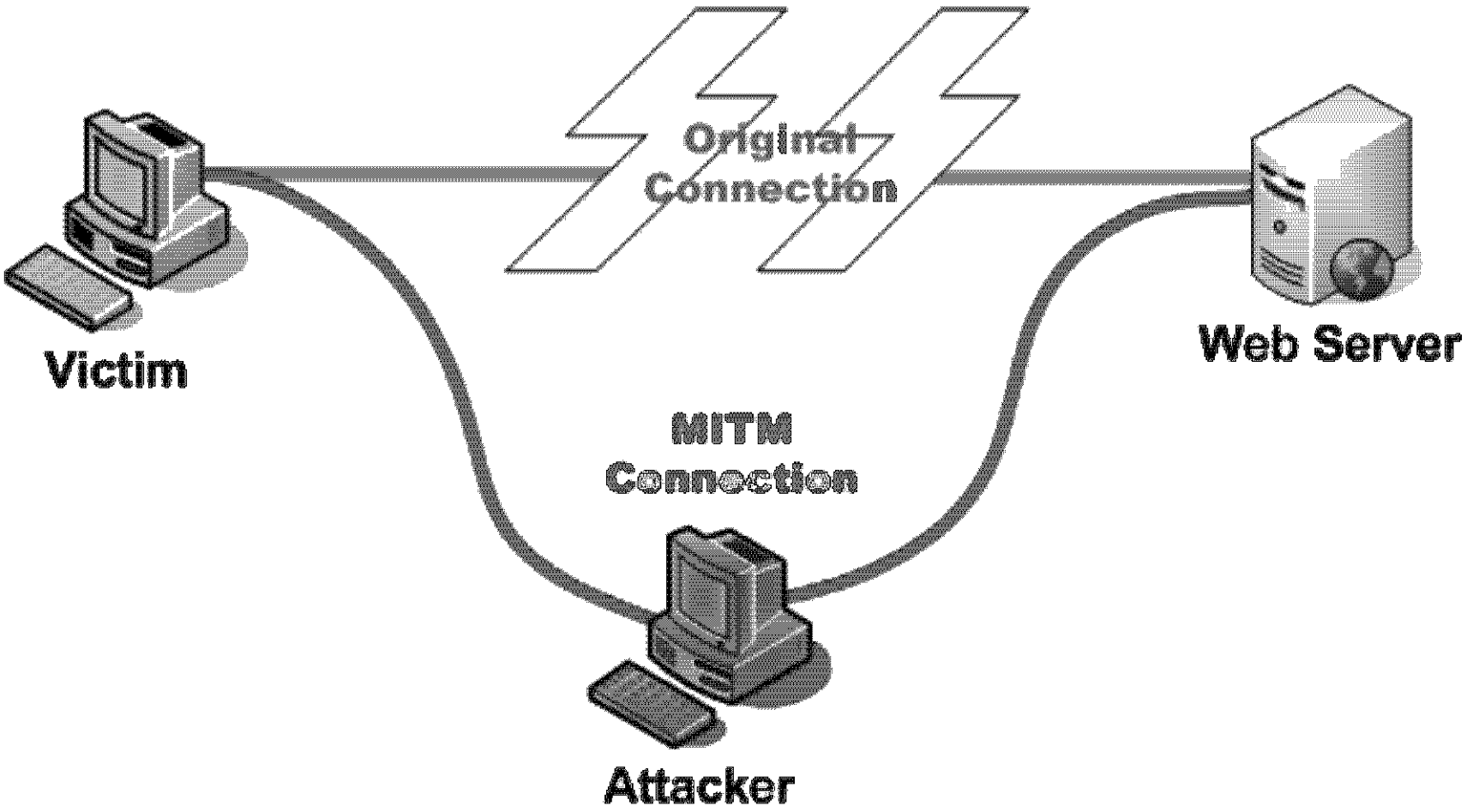


WiFi

- Man in the middle attack
  - Username and password
  - Fake Login Screens
  - Session Data
  - Traffic Analysis
  - Traffic Redirection
  - Potential Remote Exploit

The Gold Standard in Network Security

RaSecurity.com


Original
Connection
Victim
Web Server
MITM
Connection
Attacker

Karmetasploit

Covering MITM & Other Hacks

Jasager and BackTrack

February 7th, 2010

The beautiful part of using Jasager as opposed to airbase-ng for KARMA, is that by running karma as its own seperate module, we can keep the clutter out of BackTrack. So all the dhcp and karma stuff is taken care by Jasager running on fon, while BT can freely be used for sslstrip, hamster, middler and metasploit. The setup runs smooth and works great. So here is how you set it up:

Once you got Jasager running on fon, edit the /etc/config/dhcp and /etc/config/network files like this

dhcp:

```
config dnsmasq
option domainneeded     1
option boguspriv        1
option filterwin2k      '0'  #enable for dial on demand
option localise_queries 1
option local    'lan'
option domain   'lan'
option expandhosts      1
option nonegcache       0
option authoritative    1
option readethers       1
option leasefile        '/tmp/dhcp.leases'
option resolvfile       '/tmp/resolv.conf.auto'
```


Archives

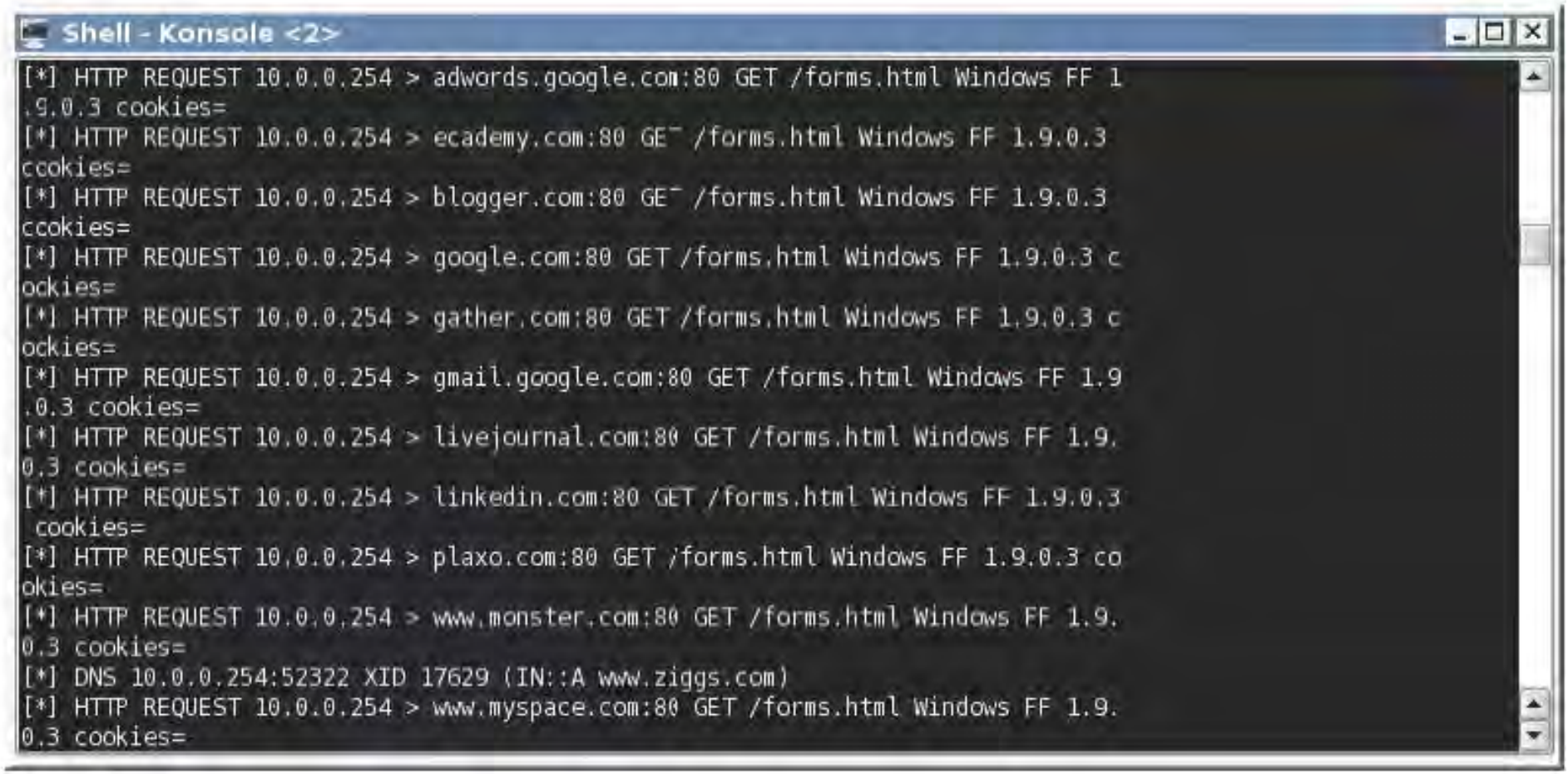
» February 2010
» December 2009
» March 2009

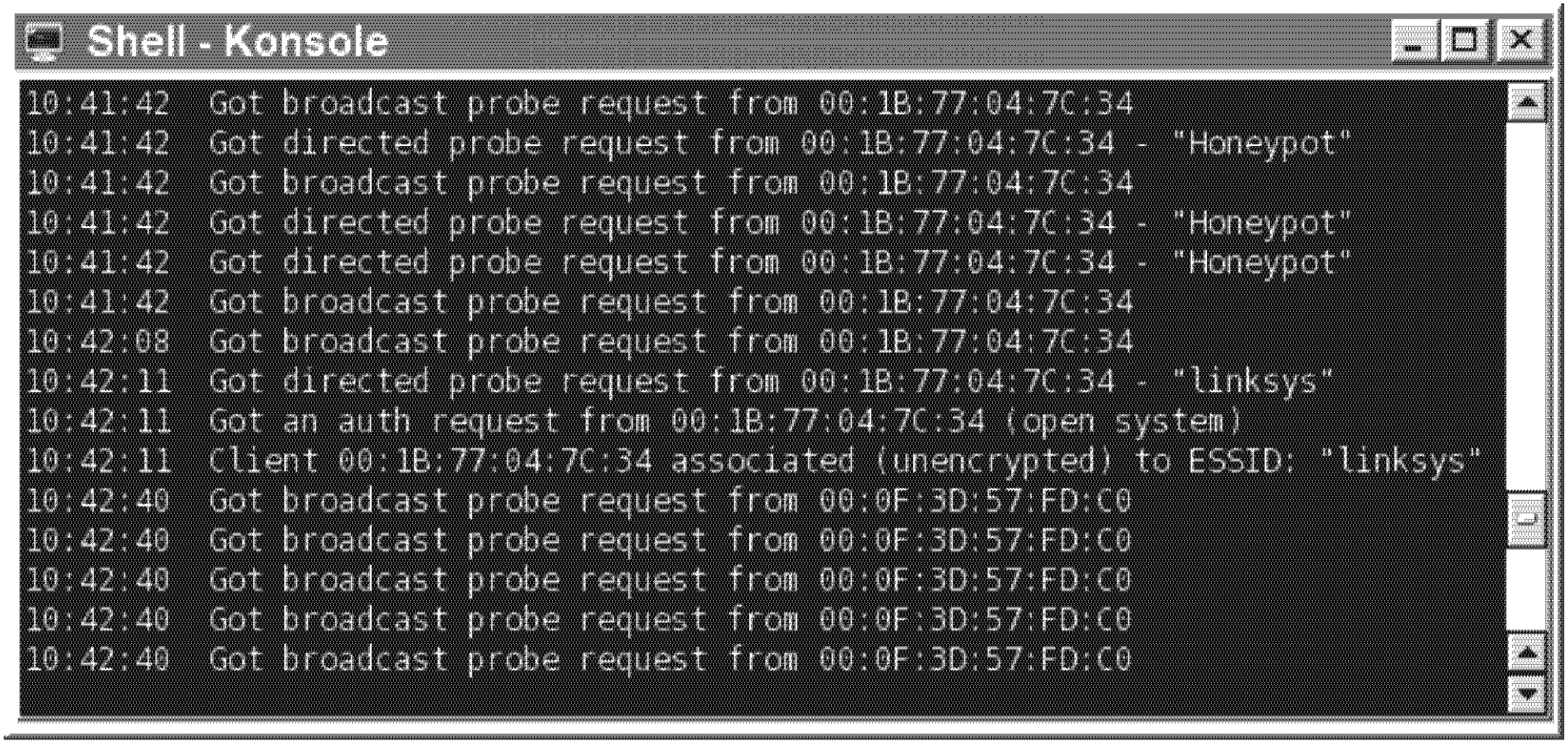
Karmetasploit

- Sets up fake AP
- Assigns DHCP Address
- Mimics authenticated services like POP3
- Collects credentials
- Identifies applications and launches exploits

The Gold Standard in Network Security

RaSecurity.com


Shell - Konsole <2>
[*] HTTP REQUEST 10.0.0.254 > adwords.google.com:80 GET /forms.html Windows FF 1
.9.0.3 cookies=
[*] HTTP REQUEST 10.0.0.254 > ecademy.com:80 GE¯ /forms.html Windows FF 1.9.0.3
ccokies=
[*] HTTP REQUEST 10.0.0.254 > blogger.com:80 GE¯ /forms.html Windows FF 1.9.0.3
ccokies=
[*] HTTP REQUEST 10.0.0.254 > google.com:80 GET /forms.html Windows FF 1.9.0.3 c
ockies=
[*] HTTP REQUEST 10.0.0.254 > gather.com:80 GET /forms.html Windows FF 1.9.0.3 c
ockies=
[*] HTTP REQUEST 10.0.0.254 > gmail.google.com:80 GET /forms.html Windows FF 1.9
.0.3 cookies=
[*] HTTP REQUEST 10.0.0.254 > livejournal.com:80 GET /forms.html Windows FF 1.9.
0.3 cookies=
[*] HTTP REQUEST 10.0.0.254 > linkedin.com:80 GET /forms.html Windows FF 1.9.0.3
cookies=
[*] HTTP REQUEST 10.0.0.254 > plaxo.com:80 GET /forms.html Windows FF 1.9.0.3 co
okies=
[*] HTTP REQUEST 10.0.0.254 > www.monster.com:80 GET /forms.html Windows FF 1.9.
0.3 cookies=
[*] DNS 10.0.0.254:52322 XID 17629 (IN::A www.ziggs.com)
[*] HTTP REQUEST 10.0.0.254 > www.myspace.com:80 GET /forms.html Windows FF 1.9.
0.3 cookies=


Shell - Konsole
10:41:42 Got broadcast probe request from 00:1B:77:04:7C:34
10:41:42 Got directed probe request from 00:1B:77:04:7C:34 - "Honeypot"
10:41:42 Got broadcast probe request from 00:1B:77:04:7C:34
10:41:42 Got directed probe request from 00:1B:77:04:7C:34 - "Honeypot"
10:41:42 Got directed probe request from 00:1B:77:04:7C:34 - "Honeypot"
10:41:42 Got broadcast probe request from 00:1B:77:04:7C:34
10:42:08 Got broadcast probe request from 00:1B:77:04:7C:34
10:42:11 Got directed probe request from 00:1B:77:04:7C:34 - "linksys"
10:42:11 Got an auth request from 00:1B:77:04:7C:34 (open system)
10:42:11 Client 00:1B:77:04:7C:34 associated (unencrypted) to ESSID: "linksys"
10:42:40 Got broadcast probe request from 00:0F:3D:57:FD:C0
10:42:40 Got broadcast probe request from 00:0F:3D:57:FD:C0
10:42:40 Got broadcast probe request from 00:0F:3D:57:FD:C0
10:42:40 Got broadcast probe request from 00:0F:3D:57:FD:C0
10:42:40 Got broadcast probe request from 00:0F:3D:57:FD:C0

SMS / MMS

- Direct exploit so far rare
- Source address easily spoofed
- Tiny URLs easily hide true destination
- URL redirects exploit server
- Social Engineering Possibilities

Everything You Ever Wanted To Know About SMS Spoofing

What is SMS Spoofing?

SMS Spoofing allows you to change the name or number text messages appear to come from.

The Story Behind SMSspoofing.com

SMSspoofing.com initially was a service that launched in August 2005 allowing users to spoof SMS text messages. However, the service only lasted a few days due to legal threats from around the world. Pressure was put on us by our bulk text messaging provider because mobile carriers around the world were complaining that they were responsible for thousands of spoofed SMS messages. The plug was pulled and we were forced to stop offering our SMS spoofing service. In a matter of days over 250,000 people had visited this site and over 25,000 users from around the world, mostly in Europe (specifically the Czech Republic, where we were prominently featured by the media), had signed up for our service.

This website has pretty much been abandoned until we decided to turn this site into an information site in June 2008! Now we're back and ready to share some of our knowledge on SMS spoofing around the world.

About SMS Spoofing and How it's Done

More Resources

- Caller ID Spoofing
- Clickatell
- Wikipedia
- Fake My Text

Voicemail

- Often stored on phone
- Accessible from secondary number
- Protected by a PIN number
  - Date (01-12 : 19-20: 00-99)
  - Sequential 0000, 1234, 4321
- Weeks of messages often stored

Mobile Applications

- Cache Data
- Log Data
- Databases
- Username and Password
- Cookies
- Session Data

The Gold Standard in Network Security

RaSecurity.com

VIAFORENSICS
innovative digital forensics and security

Industries | Products | Services | Resources | Company

COMPANY

- Management Team
- Our Clients
- News

viaForensics » appWatchdog

APPWATCHDOG

APPWATCHDOG: IMPROVING MOBILE APP SECURITY FOR CONSUMERS

Using forensics to improve data security and protect users. Read our findings from objective analysis of various publicly available mobile apps.

Filter Apps | Show All

FINDINGS

App	Platform	Category	Latest	Prev	appSecure	Results
AIM	Android	Social Networking	✗			VIEW>
AIM	iPhone	Social Networking	✗			VIEW>
Amazon Mobile	Android	Retail	!			VIEW>
Amazon Mobile	iPhone	Retail	!			VIEW>
Android Banking	Android	Finance	✓			VIEW>

Read More

RELATED AREAS:

- **viaExtract** mobile forensic software
- **appSecure** mobile app security audit
- **Mobile Forensics** for iPhone and Android

viaForensics

- TD Ameritrade - plain text User IDs
- Wells Fargo Android - name, AN & PW
- Bank of America - clear text security question
- Chase – User ID cached

The Gold Standard in Network Security

RaSecurity.com

New type of financial malware hijacks online banking sessions

Posted on 22.02.2011

BOOKMARK

A new type of financial malware has the ability to hijack customers' online banking sessions in real time using their session ID tokens.

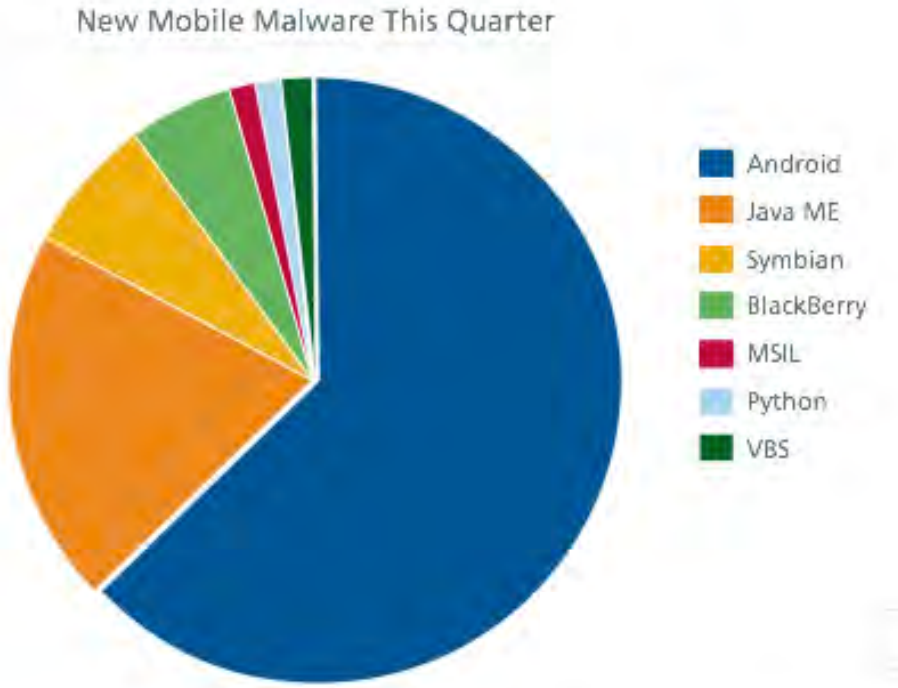
OddJob, which is the name Trusteer gave to this Trojan, keeps sessions open after customers think they have "logged off", enabling criminals to extract money and commit fraud unnoticed.

Mobile Malware

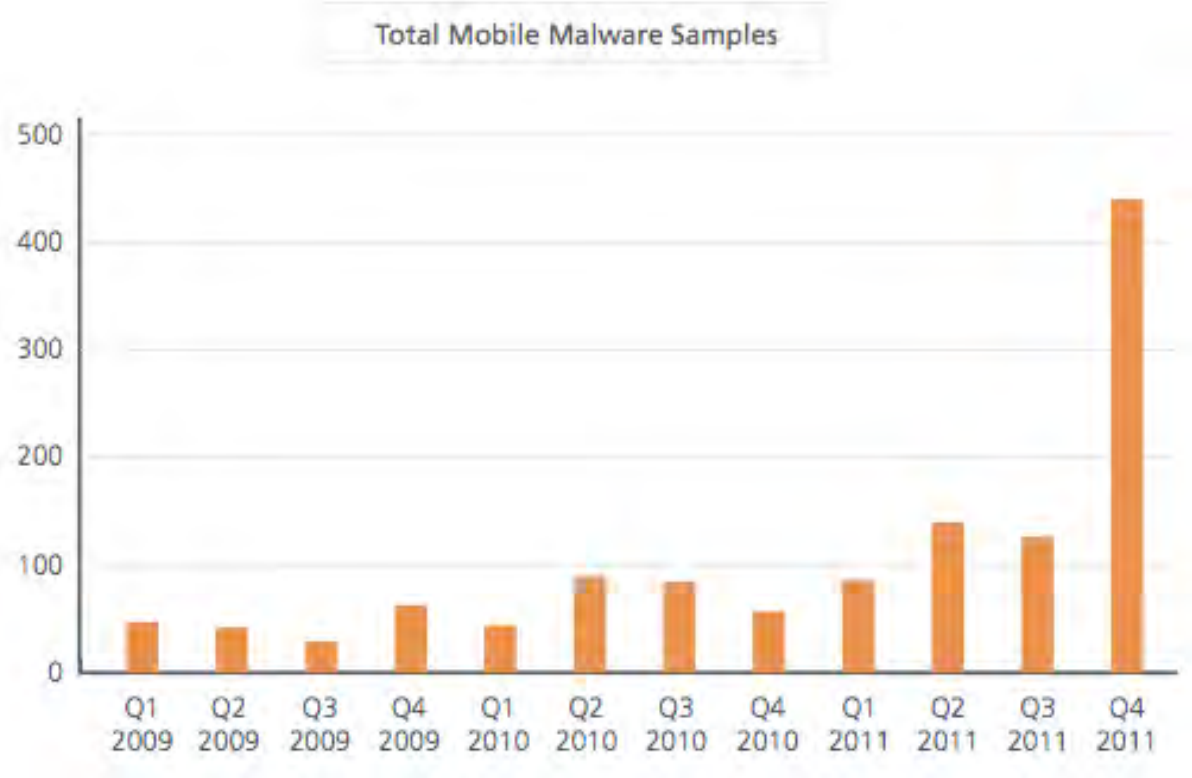
- Current Trends
- Apple IOS vs Andriod
- How they get on your device
- What they can do

The Gold Standard in Network Security

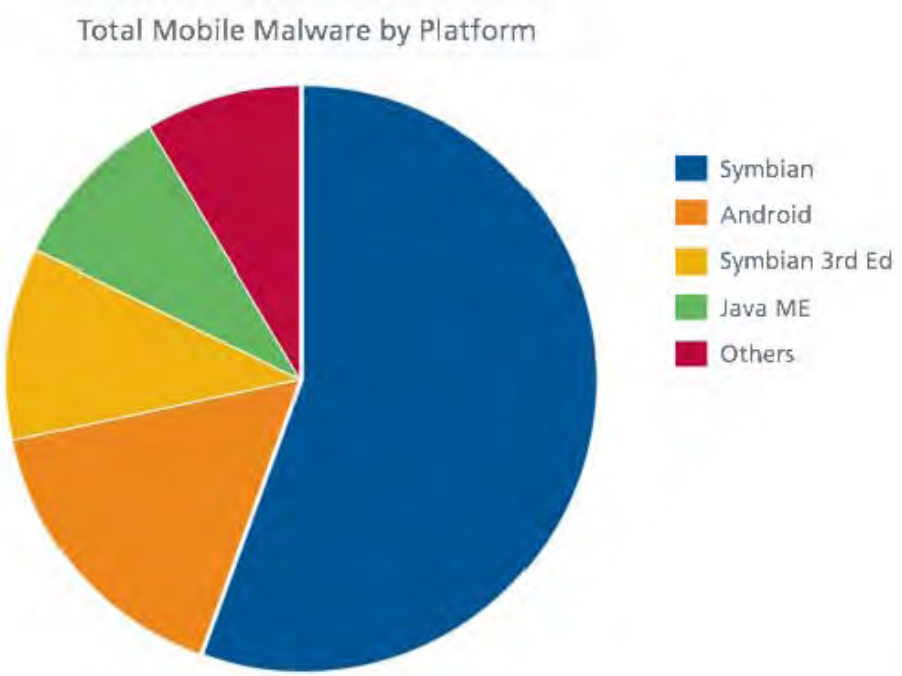
RaSecurity.com

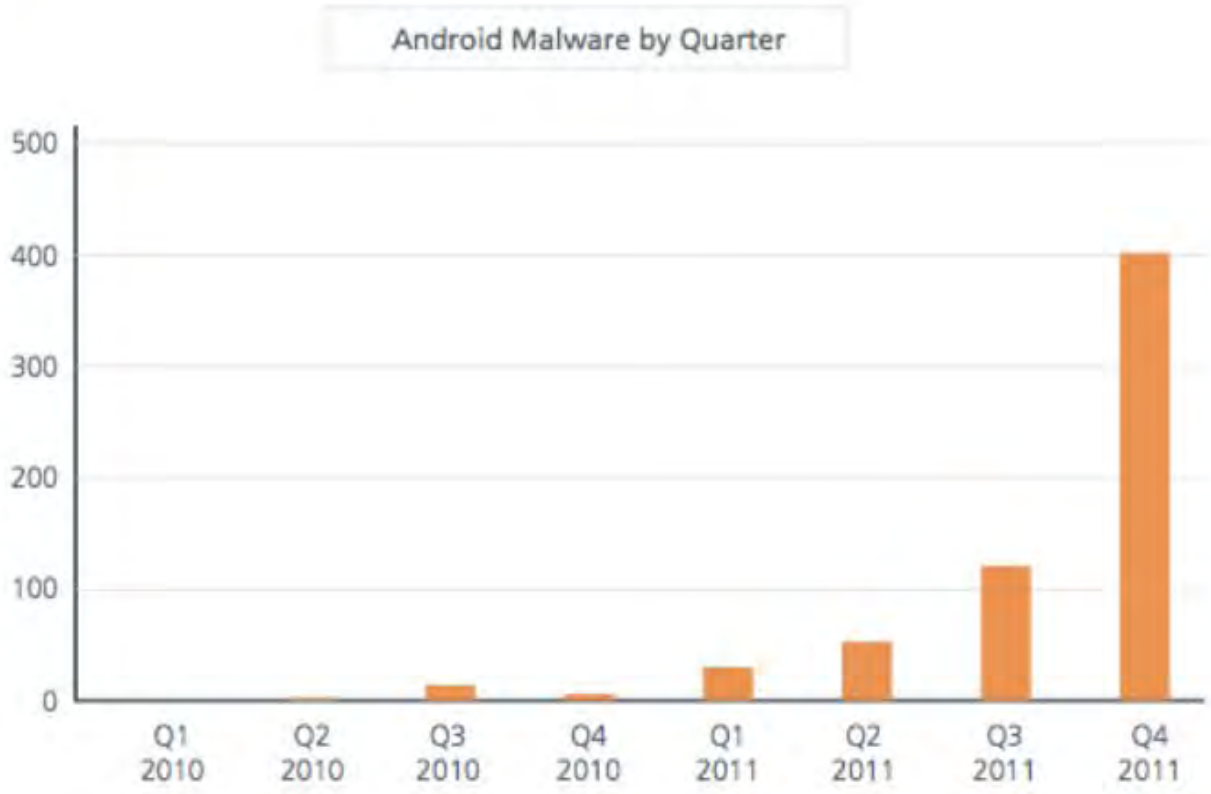


Q2 2011



Source: McAfee





Source: McAfee

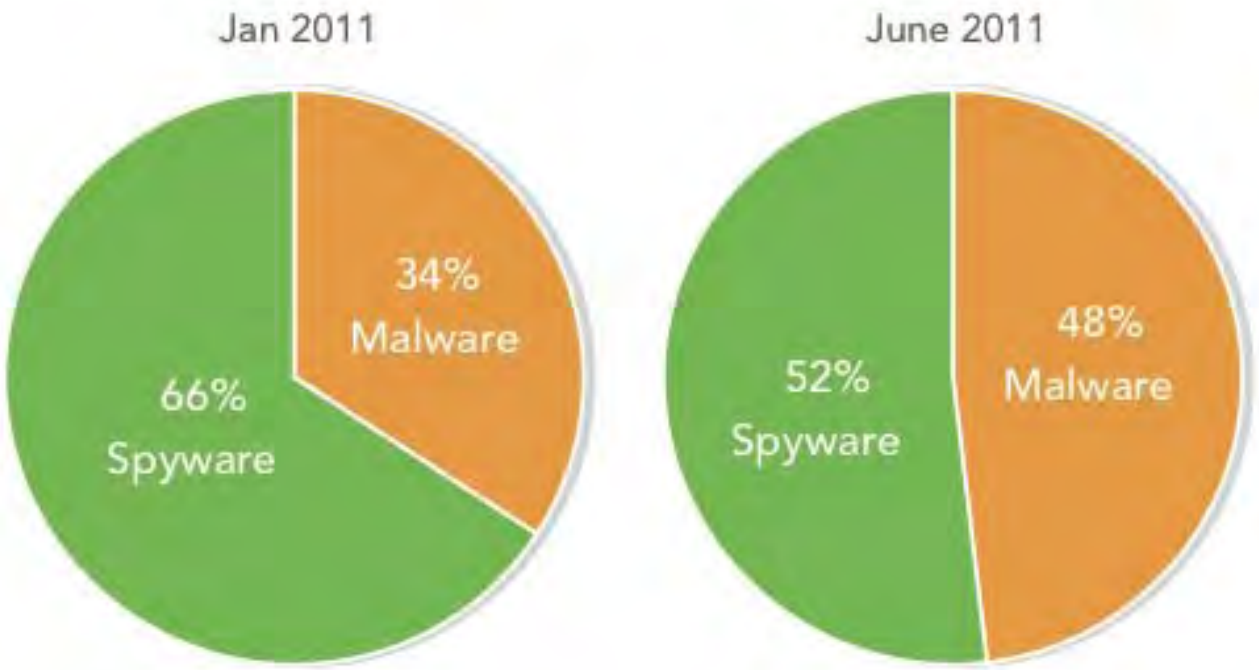
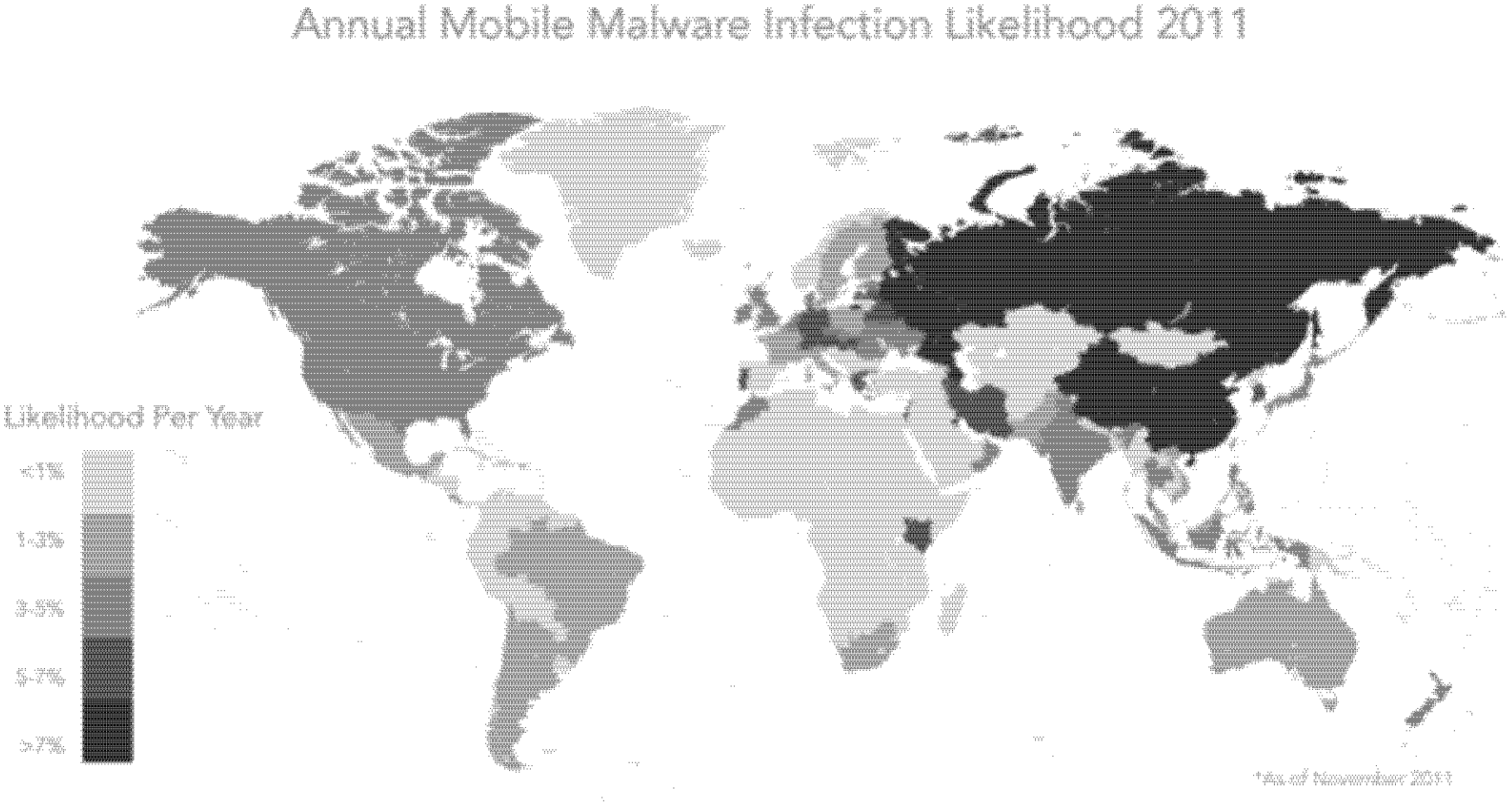


DIAGRAM 2

Application-based Threats Breakdown

Jan 2011 vs. June 2011

Source: Lookout



Source: Lookout

Source: Lookout

IOS vs Andriod

- IOS app run in a predefined restricted environment
- Android uses gated permissions
- IOS has one Application Source
- Android has multiple

The Gold Standard in Network Security

RaSecurity.com

Gaming Apps

BubbleBuster, repackaged with DroidDream Light

Chess, repackaged with DroidDream

Spiderman, repackaged with DroidDream

Utility Apps

Battery Saver app, repackaged with GGTracker

Scientific Calculator app, repackaged with DroidDreamLight

Porn Apps

Porn app, repackaged with GGTracker

DIAGRAM 5

Source: Lookout

Source: Lookout

Current Capabilities

- Send SMS usually to premium service
- Copy SMS messages off device
- Place calls from device
- Copy contact list
- Install and Remove Applications
- Open web pages
- Change C&C server location

The Gold Standard in Network Security

RaSecurity.com

So What Can I Do?

The Gold Standard in Network Security

RaSecurity.com

So What Can I Do?

Not Much!

We're All Doomed

Good Luck!

The Gold Standard in Network Security

RaSecurity.com

So What Can I Do?

- Keep user owned equipment off your network
- Alternatively provide separate WiFi
- Create an approved application policy
- Make users aware of the threats
- Password protect devices by policy
- Utilize remote lock and erase software
- Use Security Software

The Gold Standard in Network Security

RaSecurity.com

Protective Measures

- Change Bluetooth security codes
- Power off Bluetooth when not needed
- Bluetooth notify on connect
- Initiate Upgrades
- Centrally Manage Devices
- Ability to detect jailbroken devices
- Ability to remove user apps
- Ability to detect tethering

When Traveling

- Sync/Backup your device
- Turn WiFi off
- Configure device to ask before joining a WiFi network
- Sign out of apps
- Rotate passwords after your trip
- Don’t download apps from public WiFi

The Gold Standard in Network Security

RaSecurity.com

Further Reading

- NIST SP800-124
- Is My Cell Phone Bugged? By Kevin D. Murray

Fin

Gideon J. Lenkey, CISSP

glenkey@rasecurity.com

(908) 246-0634

The Gold Standard in Network Security

RaSecurity.com