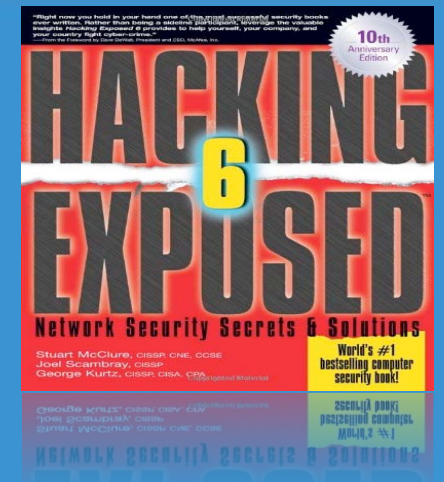




Hacking Exposed: Mobile RAT Edition

George Kurtz
President & CEO CrowdStrike
Co-Author: Hacking Exposed

Dmitri Alperovitch
Founder & CTO CrowdStrike



Session ID: HOT-203
Session Classification:

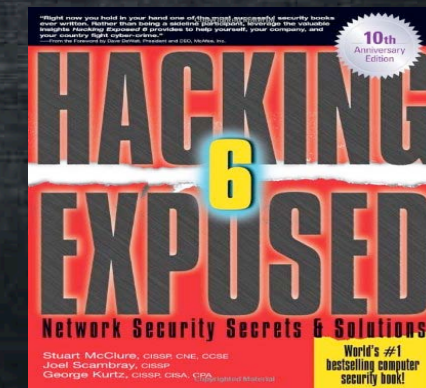
RSACONFERENCE2012

A Little About Us...

- George Kurtz
 - In security for ~20 years
 - President & CEO, CrowdStrike
 - Former CTO, McAfee
 - Former CEO, Foundstone
 - Co-Author, *Hacking Exposed*



Foundstone



A Little About Us...

- Dmitri Alperovitch
 - Co-Founder & CTO, CrowdStrike
 - Former VP Threat Research, McAfee
 - Operation Aurora
 - Night Dragon
 - Shady RAT



The Ninjas



Adam Meyers
Dir. Of Intel
CrowdStrike



Georg Wicherski
Sr. Research Scientist
CrowdStrike

Agenda

- RATs 101
- The Hack
- Bonus: Types of commercial RATs
- Countermeasures/Apply



RATs 101

What is a RAT?

- Remote Access Tools, better known as RATs
- Post-exploitation tool
- Allows administrative controls over the compromised system
- Adversaries have been targeting conventional computing platforms (PC) for many years

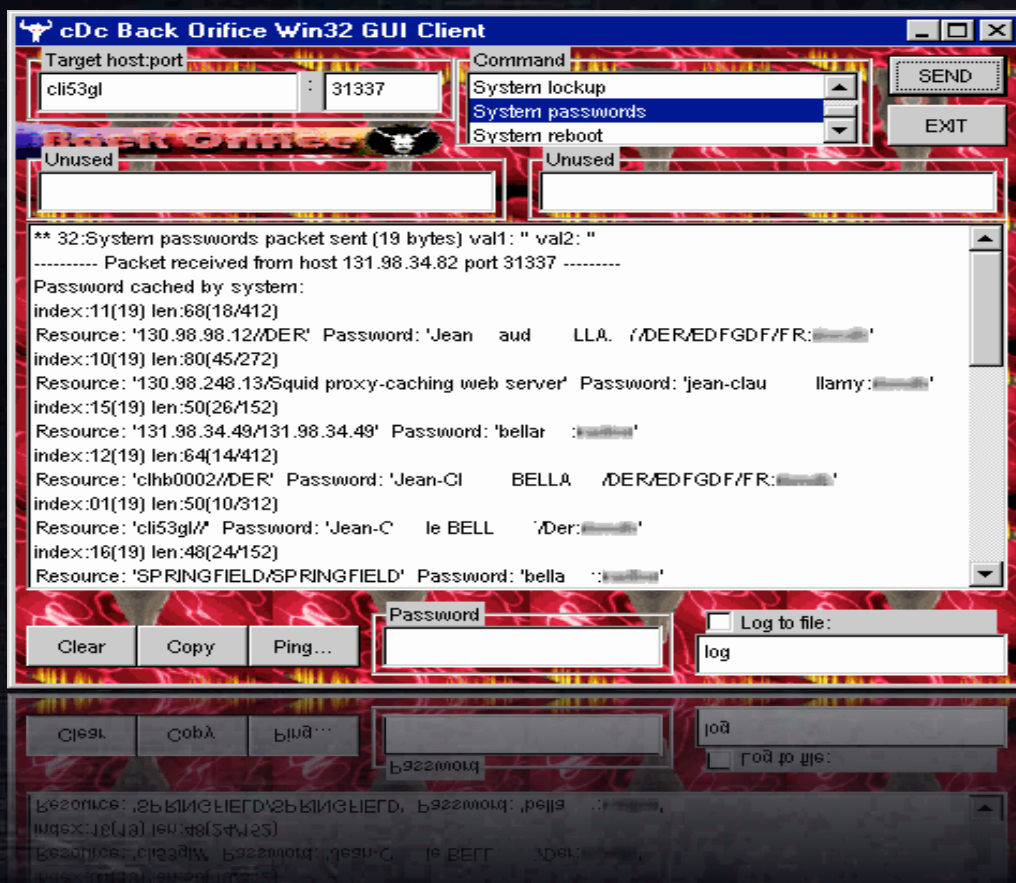
RAT Functionality

- Backdoor functionality and a host of other nefarious features
 - Activate video cameras and microphones
 - Take pictures of remote systems
 - Exfiltration - send back files
 - Run remote commands
 - Log keystrokes

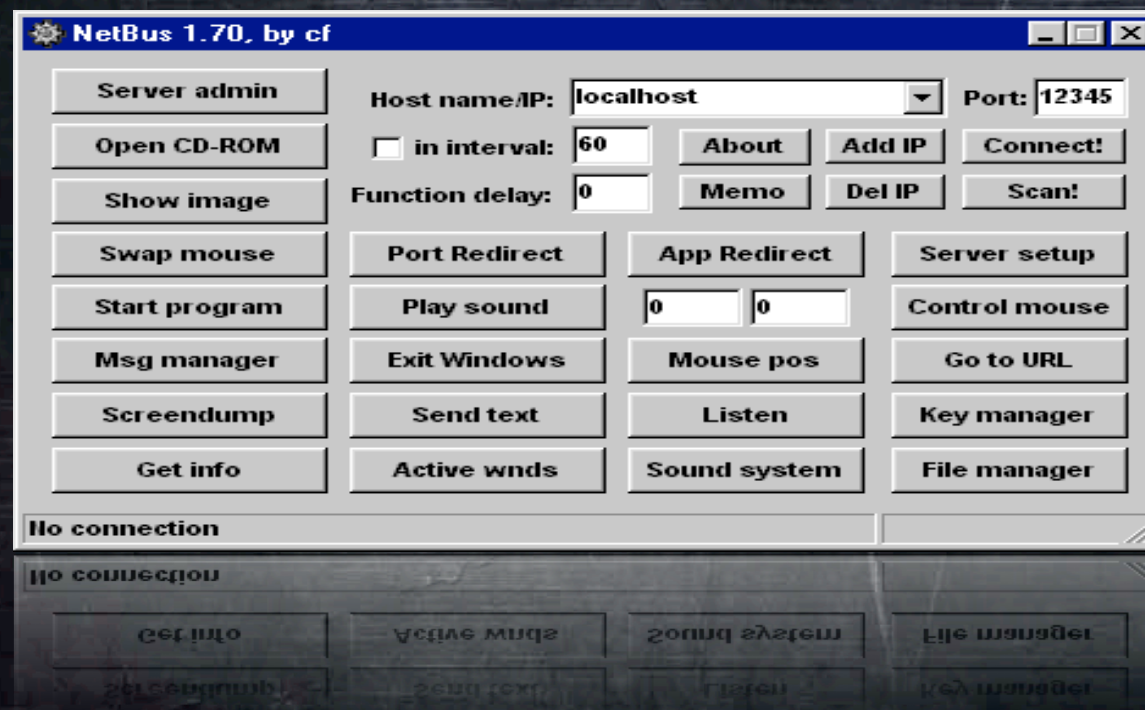


Granddaddy of RATs

Back Orifice



Netbus



Old-School RATs – Hacking Exposed Style

Netcat –
used to
shovel a
reverse shell



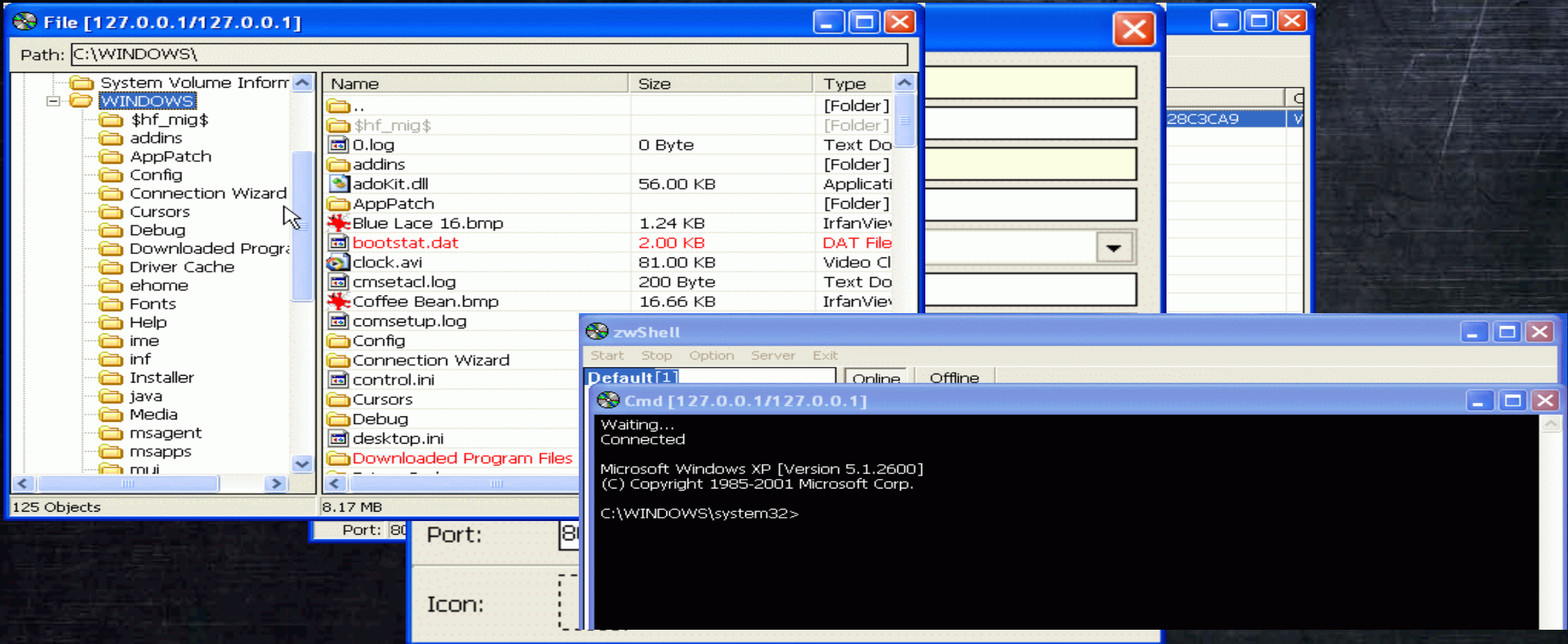
```
sh-3.2# nc -vv -l 80
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

Z:\crowdstrike>ver
ver

Microsoft Windows [Version 6.1.7601]

Z:\crowdstrike>
```


Current Generation: zwShell–Night Dragon



What is ubiquitous?



CrowdStrike

Has a camera?



CrowdStrike

Has a microphone?



CrowdStrike

Knows where you are?



CrowdStrike

Is always on?



CrowdStrike

...and stores your sensitive
information?



CrowdStrike



Dawn of a New Era—Mobile RATs

- Mobile RATs
- Smartphones are PCs that fit in the palm of your hand
- Perfect tool to:
 - Intercept calls
 - Intercept TXTs
 - Intercept emails
 - Capture remote video
 - Listen to sensitive conversations
 - Track location via GPS



In the News

[Cell Phone Spying Nightmare: 'You're Never the Same' - ABC News](#)

[abcnews.go.com](#) › GMA

Mar 8, 2010 – With **cell phone spying** software, your private life can be tracked through your **cell phone**. One woman says it led to years of cyberstalking.

[UAE spying on citizens through an Etisalat BlackBerry update ...](#)

[www.blackberrycool.com/.../uae-spying-on-citizens-through-an-etisa...](#)

Jul 13, 2009 – **Etisalat**, the carrier responsible for bringing the **BlackBerry** solution to the United Arab Emirates, released a very suspect official update.

[Etisalat BlackBerry update was indeed spyware, RIM provides a ...](#)

[www.engadget.com/.../etisalat-blackberry-update-was-indee...](#)



by Darren Murph · More by Darren Murph

Jul 21, 2009 – Um, yikes? An unexpected (and unwanted) surprise struck some 145000 **BlackBerry** users in the UAE this time last week, when an official ...

[Cell Phone Spying by Carrier IQ? Define Spying : Discovery News](#)

[news.discovery.com](#) › Tech News

Dec 2, 2011 – A tiny program that hides itself from your own scrutiny is probably monitoring how you use your **phone** on behalf of your wireless carrier.



CrowdStrike



The Hack

- 
- ✓ Mobile exploitation has been demonstrated before
 - ✓ Mobile malware has been demonstrated before
 - ✓ Rooting/Jailbreaking has been demonstrated before
 - **End-to-End malware delivery with a commandeered Chinese RAT has not!**



The Scenario

- RSA Conference: 22,000 security experts talking about stealth projects, M&A activity, and confidential compromises
- Lots of spies around eavesdropping on conversations and phone calls
- Adversary knows a VC partner who is in the midst of a number of hot deals
- Operation: To infect the VC's smartphone and eavesdrop on sensitive phone calls to gain inside intelligence on stealth deals



How Are We
Going to Do It?



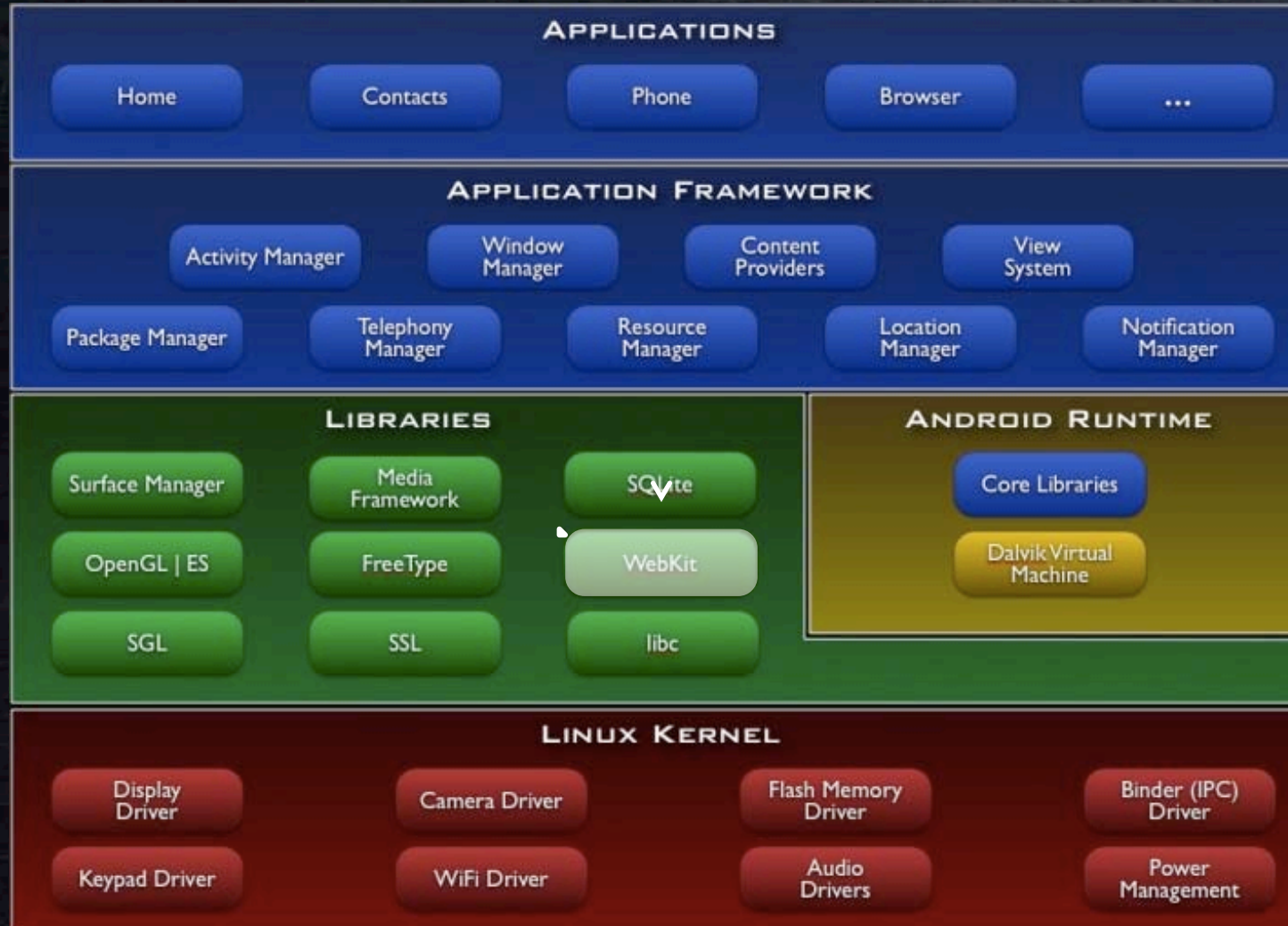
Target Selection



The WebKit Monoculture

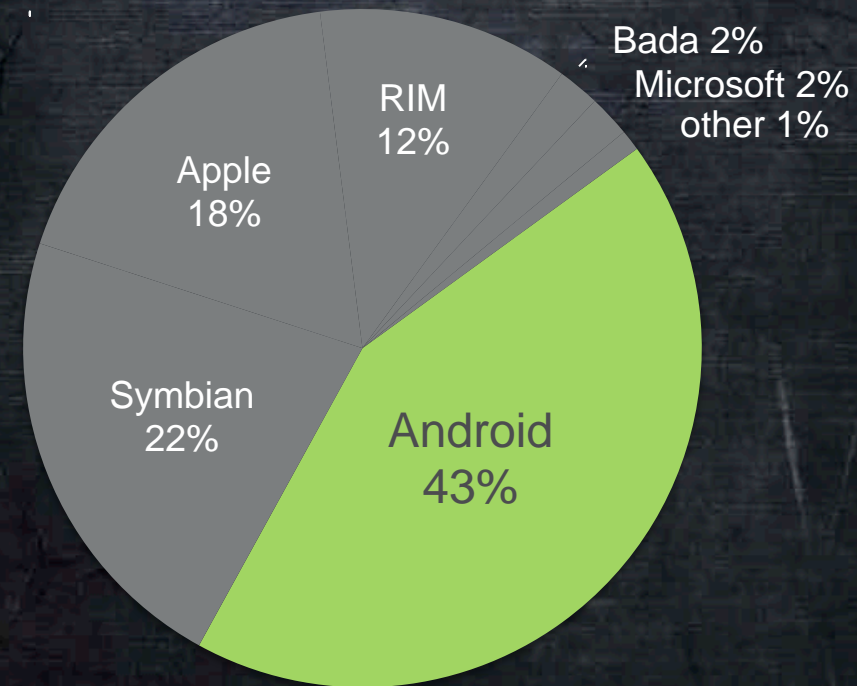
- The vulnerability demonstrated here is not Android specific
- It is in the underlying 'WebKit' library
- WebKit was derived by Apple from Konqueror
- It powers Safari & Chrome with a 36% market share
- It also powers iOS, Android, Blackberry Tablet OS & webOS

What is WebKit?



Android

Android is a popular mobile operating system which is featured on numerous devices and form factors



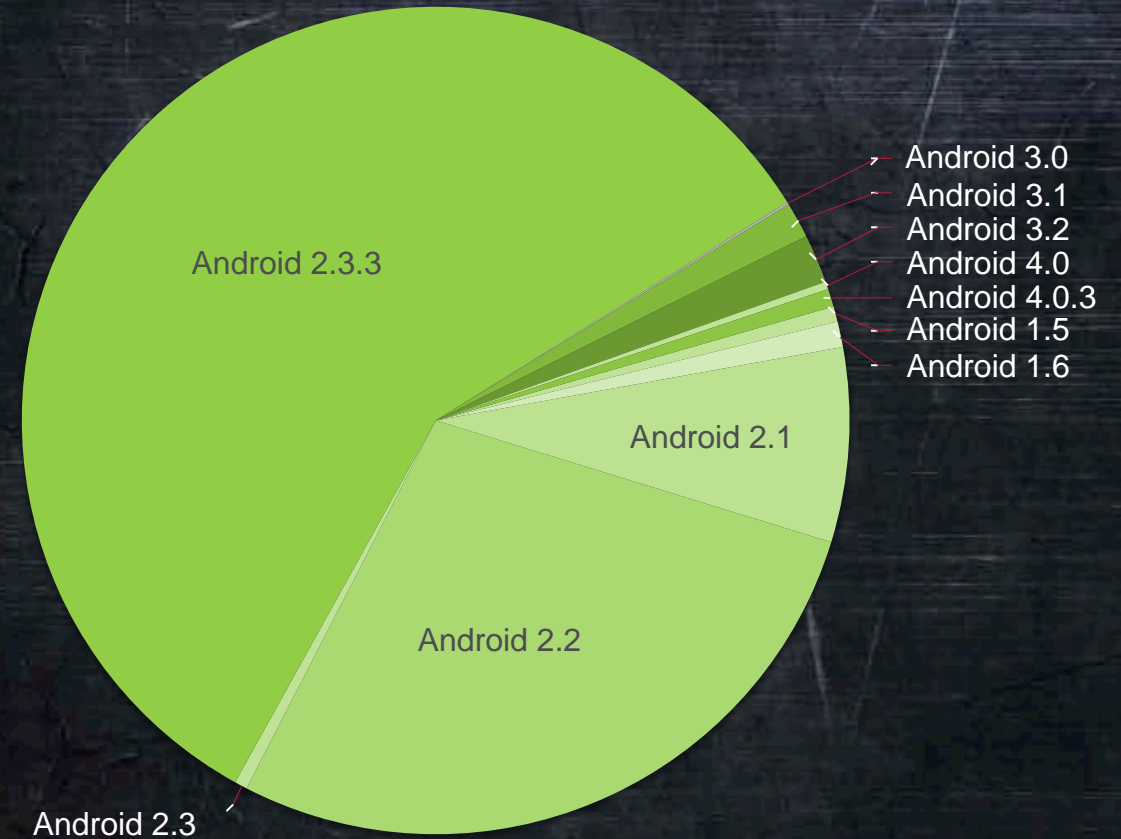
Android Versions

- Targeted version 2.2.x - Froyo
- Yes, not the latest version but still prevalent
 - Newer versions have additional security controls
 - 2.2.x was low-hanging fruit and a reliable exploit was easier to weaponize:
 - Feasible on 2.3.x
 - 2.3.x will require 1-2 weeks additional development time
 - 2.2.x is still common



Android Versions

PLATFORM	CODENAME	API LEVEL	DISTRIBUTION
Android 1.5	Cupcake	3	0.6%
Android 1.6	Donut	4	1.0%
Android 2.1	Eclair	7	7.6%
Android 2.2	Froyo	8	27.8%
Android 2.3 - Android 2.3.2	Gingerbread	9	0.5%
Android 2.3.3 - Android 2.3.7		10	58.1%
Android 3.0	Honeycomb	11	0.1%
Android 3.1		12	1.4%
Android 3.2		13	1.9%
Android 4.0 - Android 4.0.2	Ice cream sandwich	14	0.3%
Android 4.0.3		15	0.7%

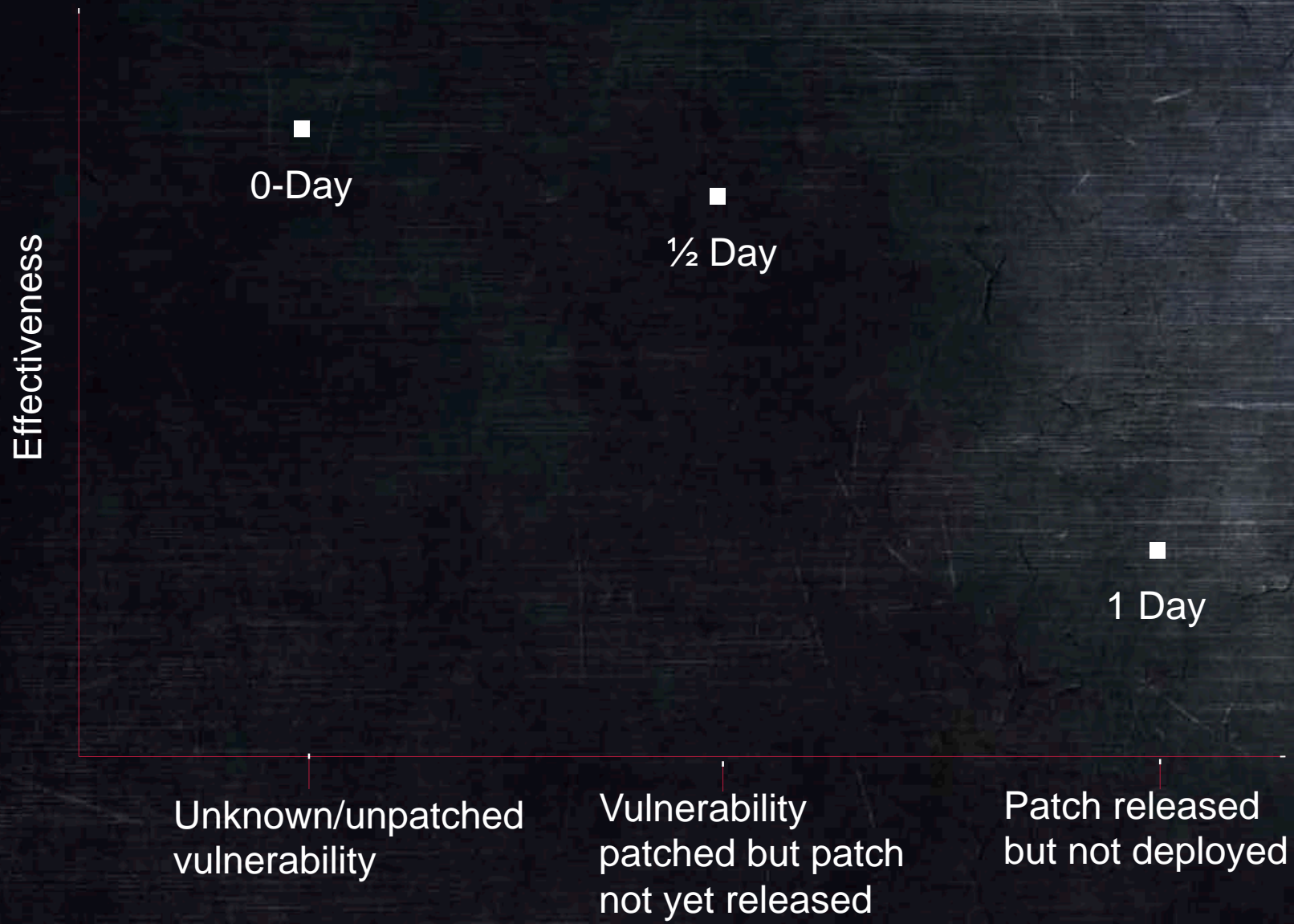


Source: <http://developer.android.com/resources/dashboard/platform-versions.html>



CrowdStrike

Vulnerability Spectrum



Vulnerability Spectrum



Bug Hunting Shopping

- We could hunt for the bug by fuzzing
- 0-day is overkill on mobile, plenty of unpatched bugs
- We bought 20 WebKit 1/2 day bugs for \$1,400 USD
- In-house weaponization, estimated cost ~\$14K USD
- Local privilege escalation (root) vulnerability publicly available
- Required two man-days to modify exploit to launch from browser context
- ***Does not require rooted/jailbroken phone!***



Weaponization

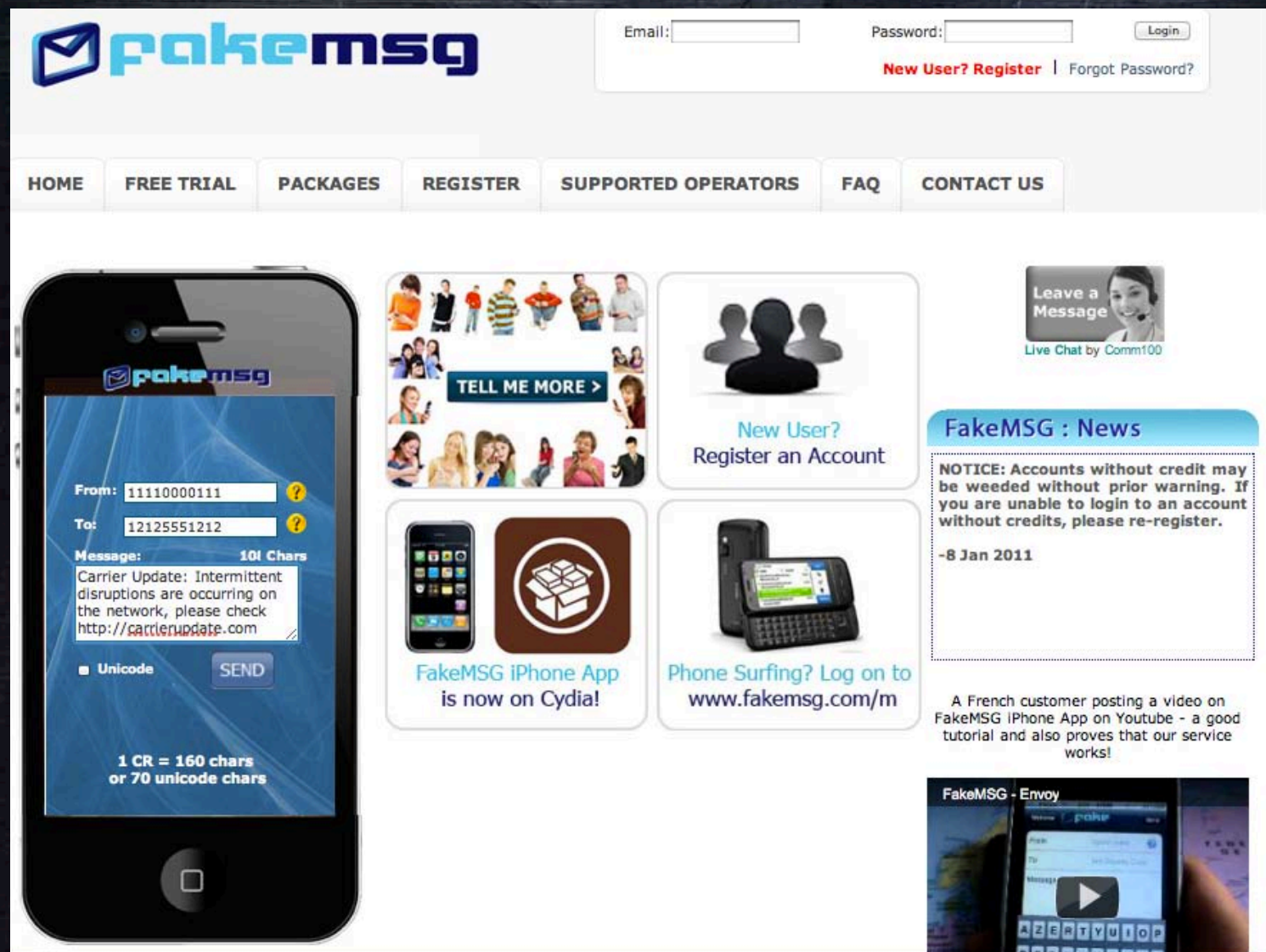
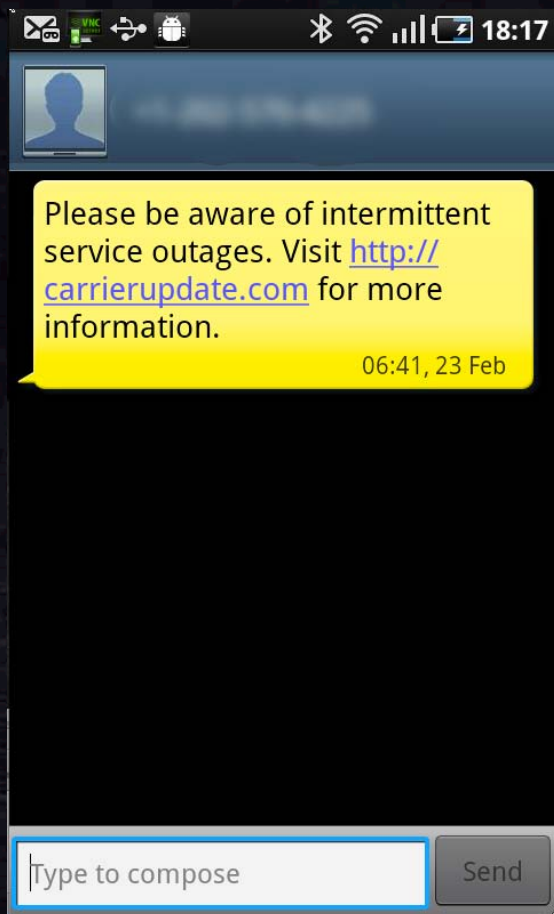
- Not as easy as initially thought
- Building tool chain for exploit development was very time consuming
 - Needed ARM tools, stable platform, debugger, etc.
- Once the tool chain was developed the next challenge was reliable control of PC (ARM program counter) to control execution
- Once we had a reliable PC control, the payload had to be placed
- Payload designed to use an egg hunter
- Reliability required some heap feng shui
- WebKit heaps abused to place payload

Putting it All Together

- ½ Day WebKit bug procured
- Bug weaponized with ROP chain and egg hunting payload
- Use root exploit to elevate privileges and install .apk
- APK is 'repurposed' Chinese RAT previously found in the wild
- Reboot the phone to activate the malware
- Win

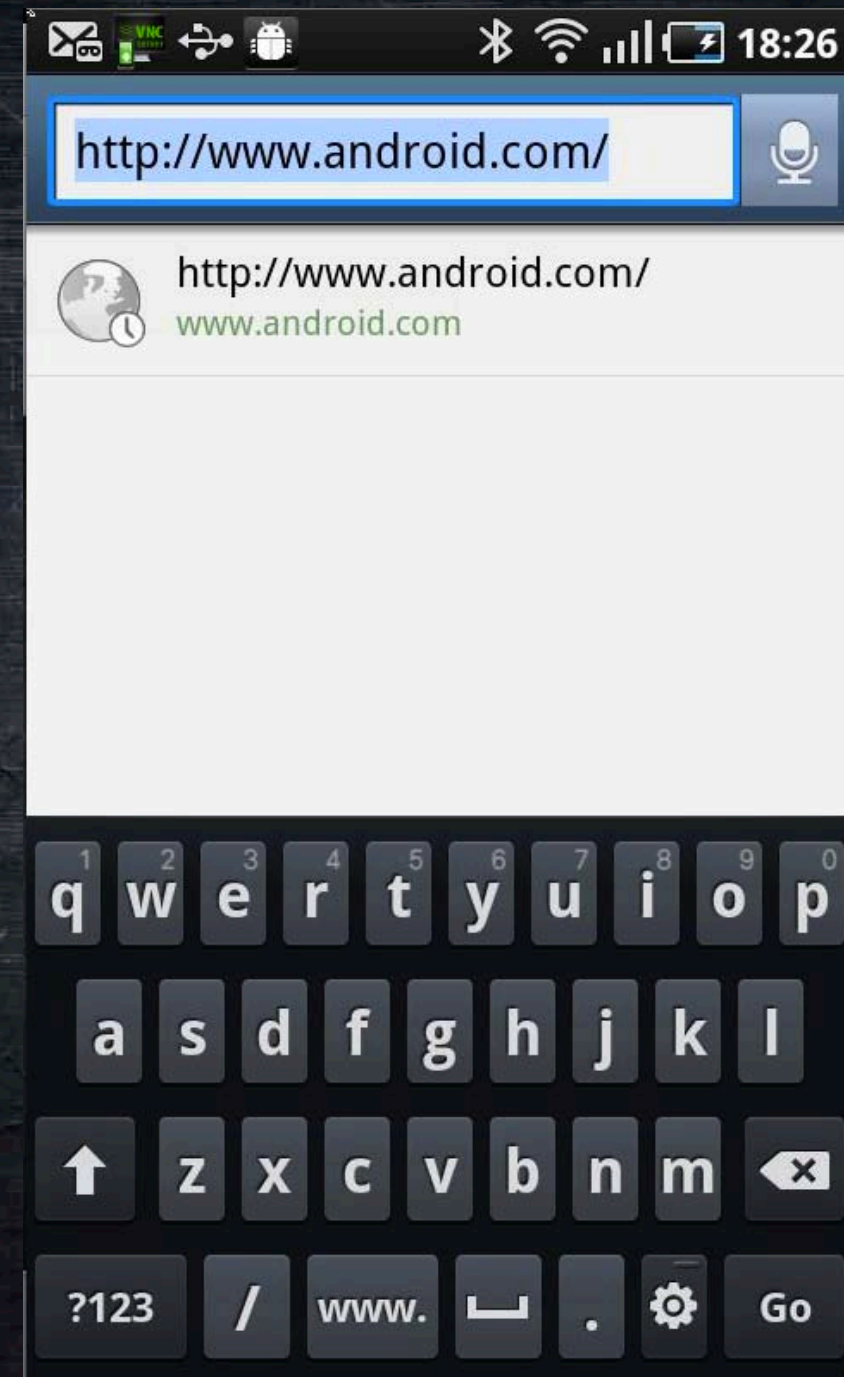
Step 1: The Phish Is Sent

■ SMS/MMS (spoofable)



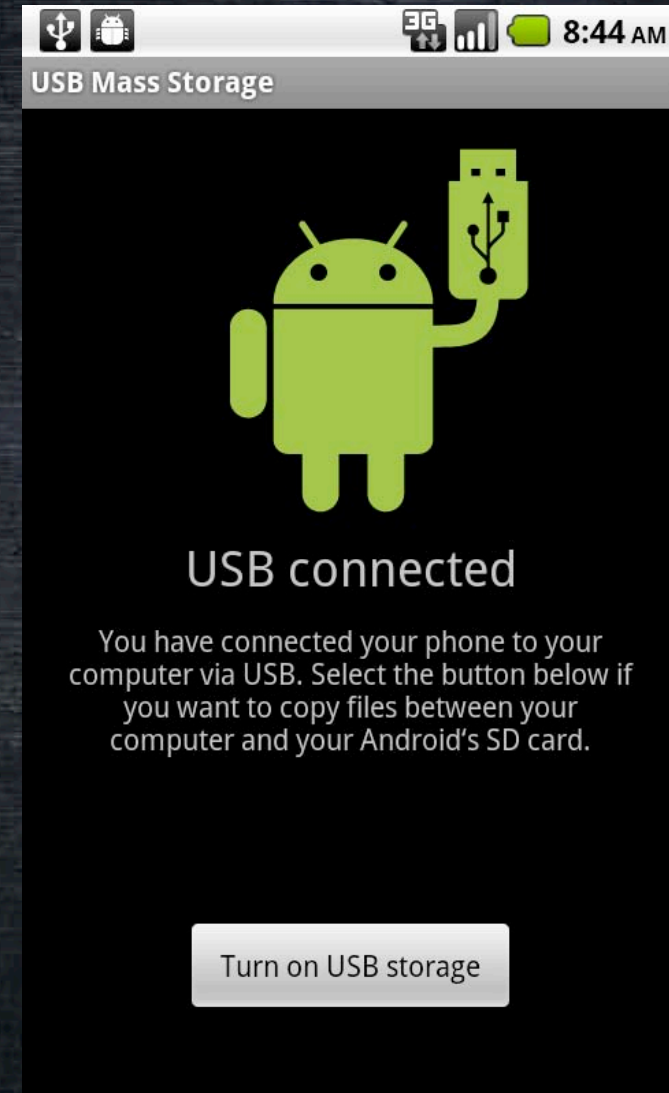
Step 2: Browser Exploited

- WebKit exploit is delivered
- Run under the context of the browser process, not root



Step 3: Privilege Escalation

- *vold* exploit used
- *vold* is used to mount removable media like SD cards
- Exploit good up through 2.3.3
- After exploit is run, we now have root privileges









Step 4: RAT installation

- *Nickispy* installed as part of the payload
- Phone reboots

Running services

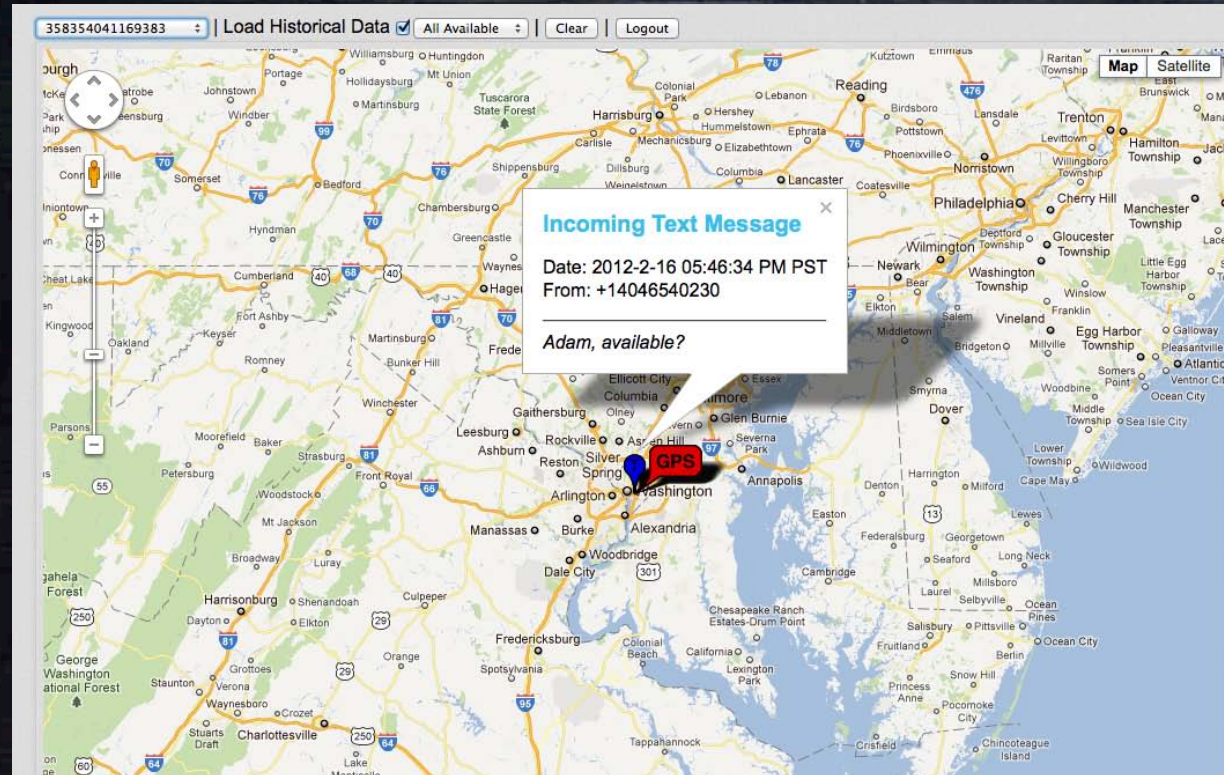
Android System Message 3.1MB
Process: com.nicky.lyyws.xmall

	XM_CallListener 01:17 Started by application: Tap to stop
	MainService 01:17 Started by application: Tap to stop
	XM_CallRecordService 01:17 Started by application: Tap to stop
	SocketService 01:17 Started by application: Tap to stop
	XM_SmsListener 01:17 Started by application: Tap to stop
	GpsService 01:17 Started by application: Tap to stop

Other: 60... Available: 143MB+88MB in 16 services

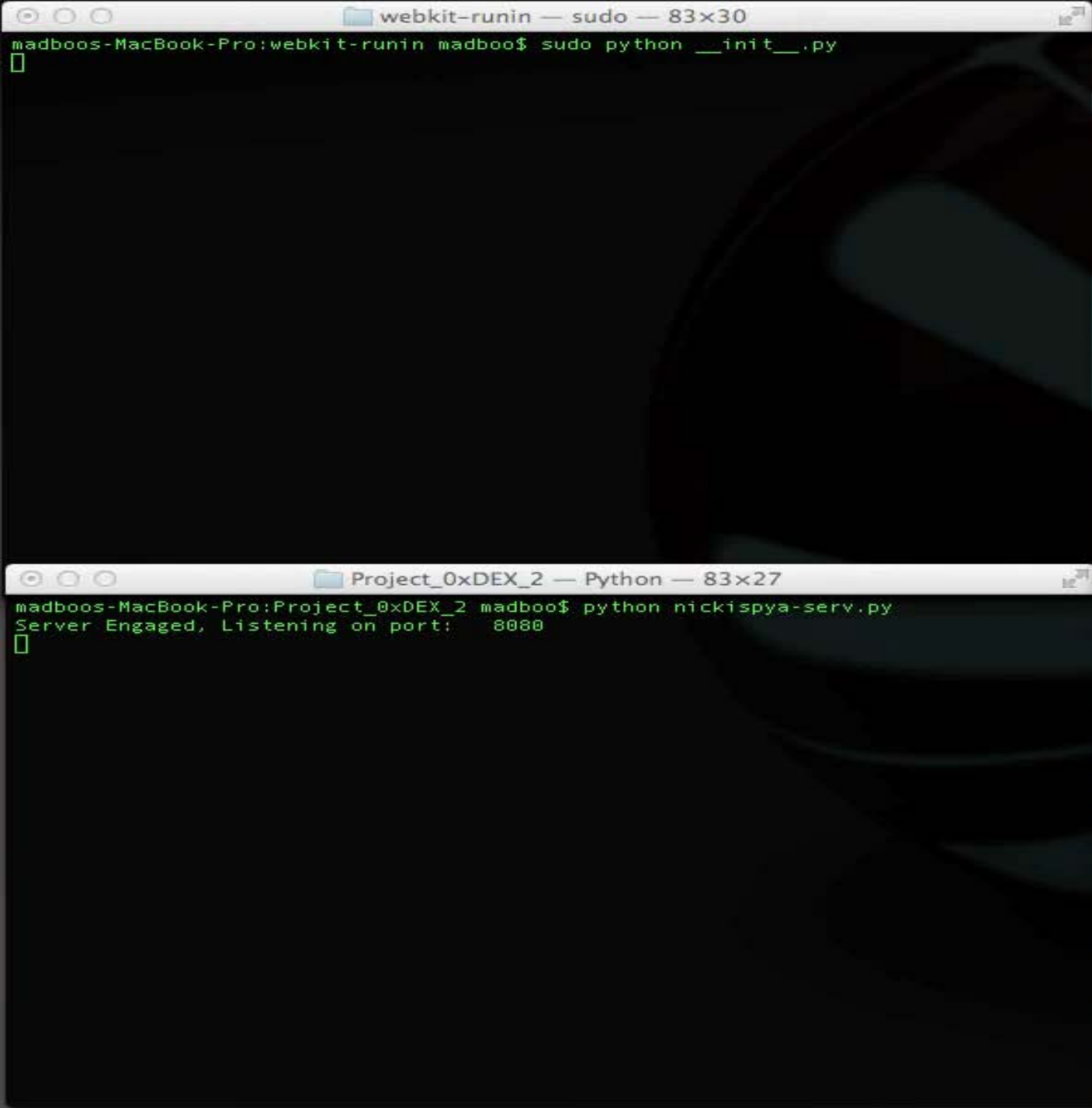
Step 5: Winning...

- Only the malware was available with no C2 server...
- So we built our own
- Custom C2 Server is used to:
 - Intercept voice calls
 - Intercept inbound/outbound SMS
 - Log Missed/Aborted Calls
 - Get Geolocation information





ATTACK DEMO





Commercial Mobile RATs


Commercial RATs

- Generally marketed towards jealous and/or suspicious lovers

**SINCE 2005, WE'VE HELPED
CATCH THOUSANDS OF
CHEATING PARTNERS**

Let Us Help You Catch Yours

**CATCH YOUR CHEATER
WITH THEIR PHONE**



Uncover them in 5 minutes by reading everything on their cellphone

FlexiSPY Is The Original And Most Powerful Spyphone Software Since 2005

Marketing Mobile Spying

How Does Your Partner Act Around Their Cell Phone?

Of course, your partner may be innocent, but its the '**not knowing**' that is the **problem**. Its the 'not knowing' that creates **nagging suspicions** - its the **uncertainty** which creates the heartache **that ruins your mind and your relationship** .

There is no any need to suffer any longer. Just install FlexiSPY on your partners phone and you will **know for sure** what your **partner is really feeling, saying and doing behind your back**

"wrong number"

(right number, wrong time)

"he's just a friend"

(new boyfriend)

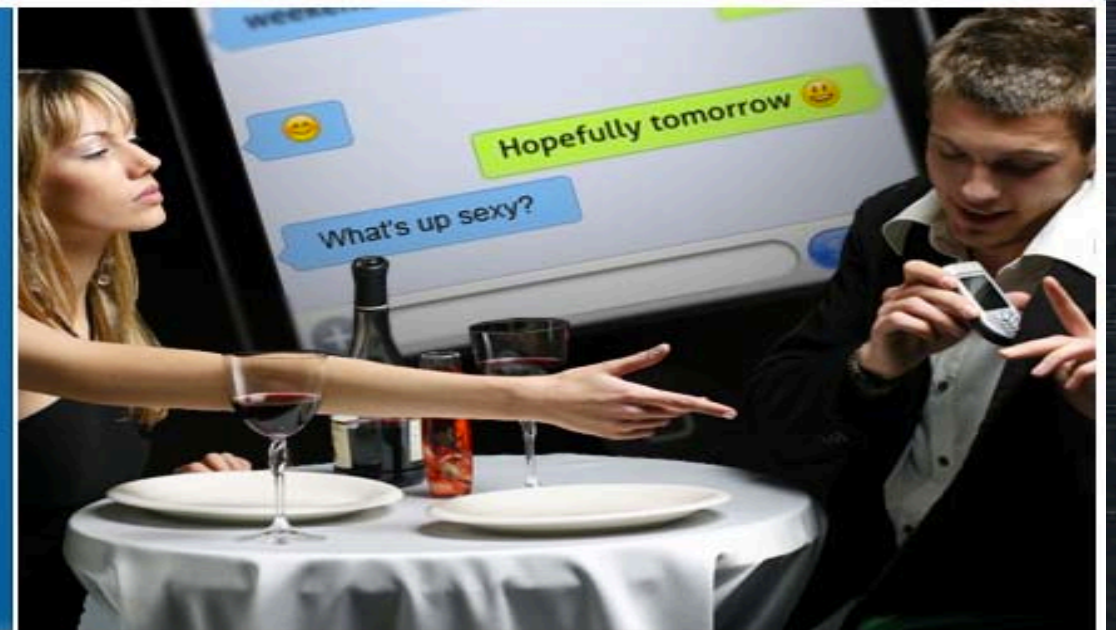
- ▣ Are they unusually jumpy when their phone rings.
- ▣ Do they immediately delete their SMS messages.
- ▣ Do they always keep their phone close to them at all times.
- ▣ Always keep their cellphone on silent or vibration mode.
- ▣ Take great pains to keep their phone locked with a password.
- ▣ Religiously places their cellphone face down so you cant see the display
- ▣ Often leaves the room to take a phone call.



Marketing Mobile Spying

**Many People Cheat.
They All Use Cell
Phones.**

***THEIR CELLPHONE WILL TELL YOU
WHAT THEY WONT***



CrowdStrike

Commercial RATs

- <http://www.easy-cellphone.info/tracker.php>
- <http://www.cell-watch.com/>
- <http://www.mobile-spy.com/>
- <http://utilities.flexispy.com/checkphones.jsp?p=4>
 - One of the best
- <http://www.howtocellphonespy.com/spybubble-review-does-spybubble-really-work>
- <http://www.bomgar.com/micro/try/index.htm>
- <http://www.brickhousesecurity.com/iphone-spy-data-recovery-stick.html>

Commercial RAT Delivery

- Most commercial RATs require physical access to the target's mobile device
- The attacker must know the target's password or the device must be unlocked
- The attacker browses to an installation page, or is instructed to install the app via a third-party market
- iOS devices require a jail break in order to complete the install

Commercial RAT Collection

- Commercial RATs generally provide a management portal to facilitate collection of information
- Typical data collected:
 - GPS
 - Audio recordings
 - Pictures
 - SMS/email traffic
 - Call logs
 - Hot mic capabilities
 - Keyword alerting

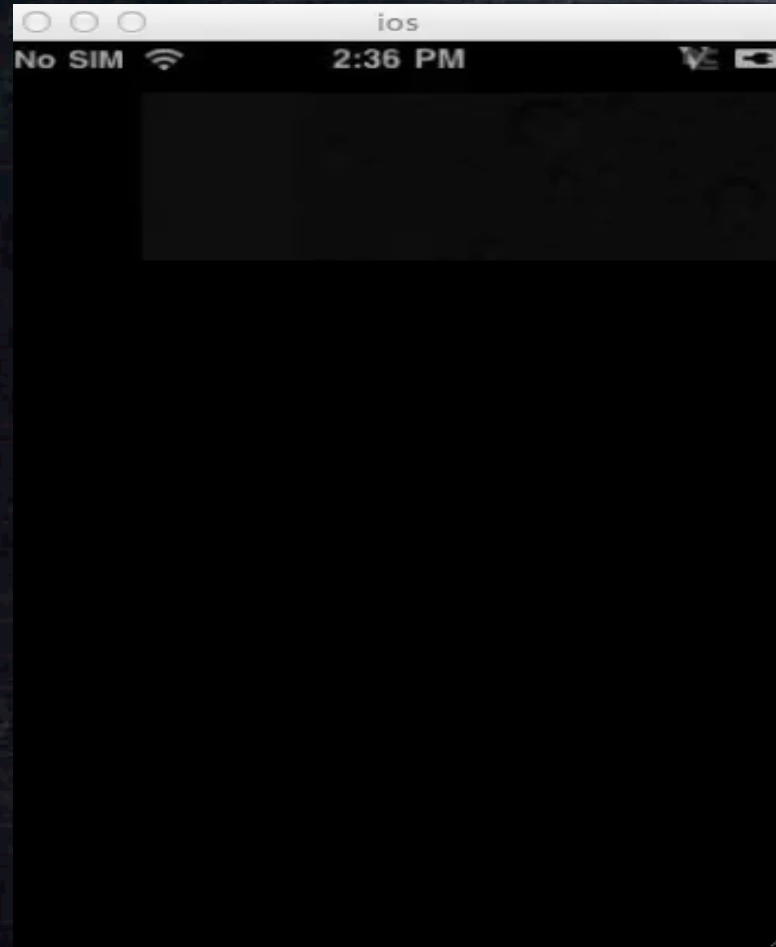
Command and Control

- Commercial mobile RATs typically use HTTP for C2
- Some use encryption using onboard packages, such as AES
- Most do not encrypt C2 communications
- Device registration almost always in the clear

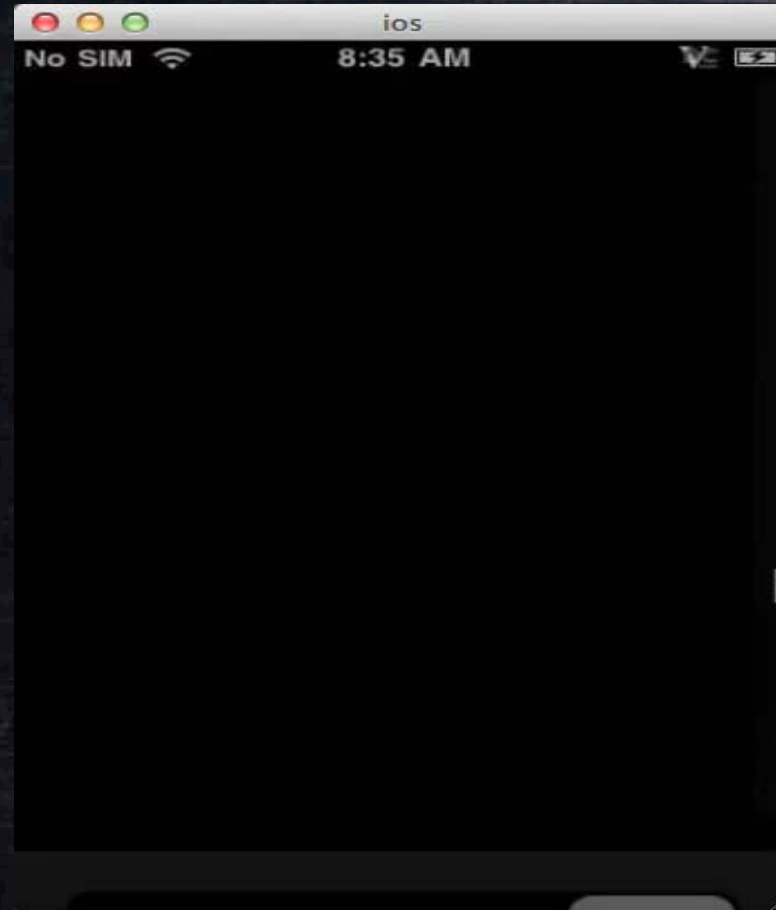
FlexiSPY

- Emerged in 2006 timeframe as a consumer- marketed cell phone spying software
- Capabilities include:
 - Monitoring email
 - Monitoring SMS/MMS
 - Monitoring chat/Facebook/WhatsApp
 - Number flagging
 - Call intercept (only live calls)
 - Hot mic
 - SMS C2

FlexiSPY Installs the App



Installing FlexiSPY



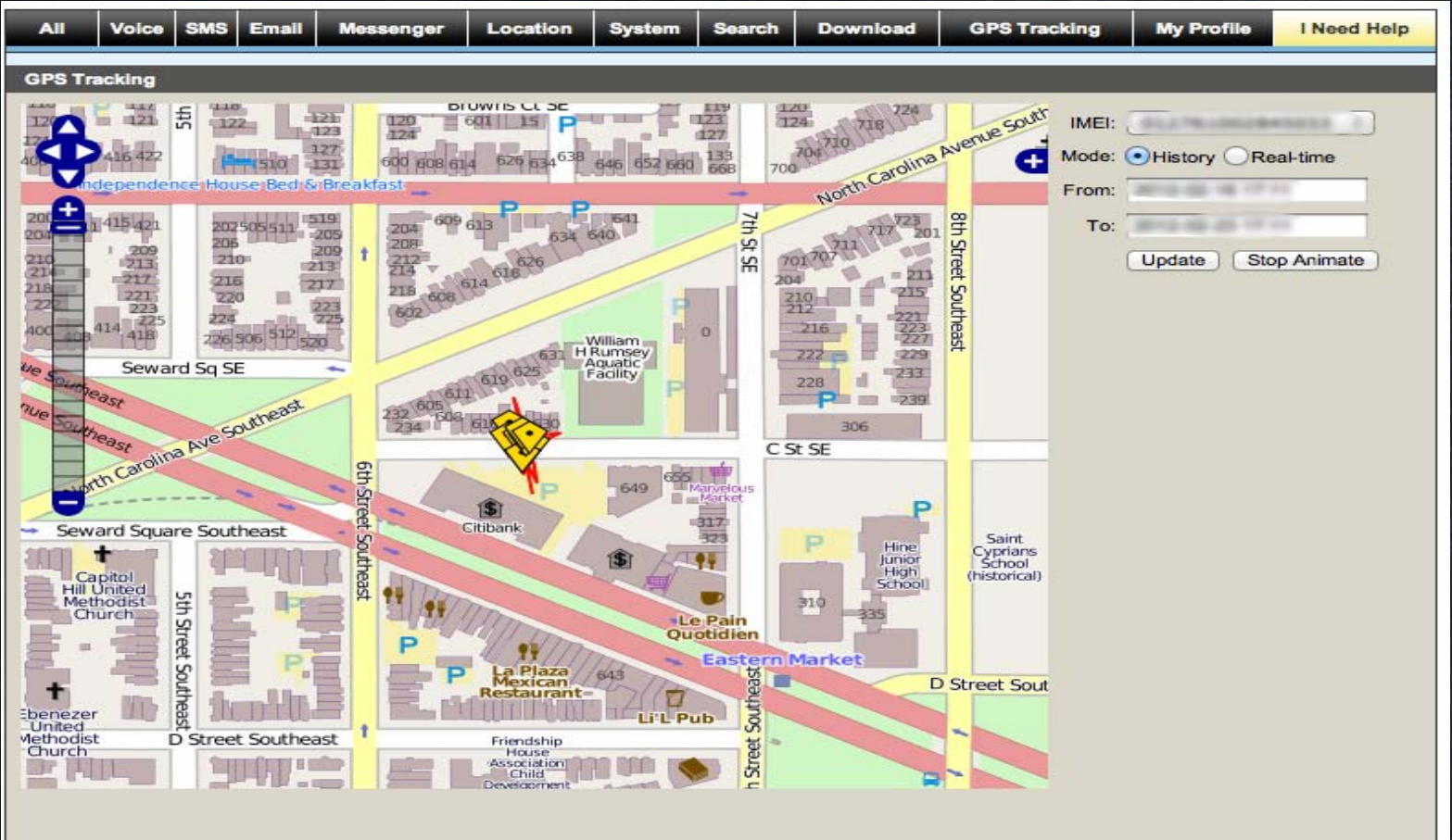
FlexiSPY Logs

All	Voice	SMS	Email	Messenger	Location	System	Search	Download	GPS Tracking	My Profile	I Need Help	
ALL EVENTS 1 - 10 of 70 records										Row Per Page	10	Print
#	<input type="checkbox"/>	Type	Direction	Duration	Contact Name	Mobile Time	Server Time					
1	<input type="checkbox"/>	VOICE		0:00:14		23/02/12 15:00:00	23/02/12 15:00:00					
2	<input type="checkbox"/>	LOC	Map			23/02/12 15:00:00	23/02/12 15:00:00					
3	<input type="checkbox"/>	LOC	Map			23/02/12 15:00:00	23/02/12 15:00:00					
4	<input type="checkbox"/>	LOC	Map			23/02/12 15:00:00	23/02/12 15:00:00					
5	<input type="checkbox"/>	LOC	Map			23/02/12 15:00:00	23/02/12 15:00:00					
6	<input type="checkbox"/>	LOC	Map			23/02/12 15:00:00	23/02/12 15:00:00					
7	<input type="checkbox"/>	LOC	Map			23/02/12 15:00:00	23/02/12 15:00:00					
8	<input type="checkbox"/>	LOC	Map			23/02/12 15:00:00	23/02/12 15:00:00					
9	<input type="checkbox"/>	LOC	Map			23/02/12 15:00:00	23/02/12 15:00:00					
10	<input type="checkbox"/>	LOC	Map			23/02/12 15:00:00	23/02/12 15:00:00					
<div> Delete Refresh Report Setting</div> <div>First Previous 1 2 3 4 5 Next Last</div>												

Delete Refresh Report Setting											
First Previous 1 2 3 4 5 Next Last											
10	<input type="checkbox"/>	LOC	Map			23/02/12 15:00:00	23/02/12 15:00:00				
11	<input type="checkbox"/>	LOC	Map			23/02/12 15:00:00	23/02/12 15:00:00				




FlexiSPY Geolocation



FlexiSPY SMS

All	Voice	SMS	Email	Messenger	Location	System	Search	Download	GPS Tracking	My Profile	I Need Help	
SMS EVENTS 1 - 4 of 4 records										Row Per Page	10	Print
#	<input type="checkbox"/>	Type	Direction	Duration	Contact Name	Mobile Time	Server Time					
1	<input type="checkbox"/>	sms				22/02/12 15:00:00	23/02/12 15:00:00					
2	<input type="checkbox"/>	sms				22/02/12 15:00:00	22/02/12 15:00:00					
3	<input type="checkbox"/>	sms				22/02/12 15:00:00	22/02/12 15:00:00					
4	<input type="checkbox"/>	sms				22/02/12 15:00:00	22/02/12 15:00:00					
Delete Refresh Report Setting										First Previous 1 Next Last		

Support Forums



Protect Your Children | Catch Cheating Spouses

[Home](#) [Features](#) [Phones](#) [Demo](#) [Community](#) [Reseller](#) [About Us](#) [Cart](#)


[Support Home](#) [Register](#) [Knowledgebase](#) [News](#) [Downloads](#) [Troubleshooter](#) English (U.S.)

[Login](#) [Subscribe](#)

☐ Remember me

[Knowledgebase](#)

- General Information (61)
- Downloads (33)
- Technical Support (6)

 **Live Support**
AWAY
Live Chat by Kayako

Or call us for
Pre-Sales Only at:

USA 1-646-240-4063
UK 44-207-979-7126


[Register](#) [Register \(Login to Submit a Ticket\)](#) [Knowledgebase](#) [News](#)
[Downloads](#) [Troubleshooter](#)

Latest Updates

Feb 23

New FlexiSPY Products and Promotions!

Posted by Christian . on 23 February 2012 12:39 PM



We're shaking things up – check us out!

Sometimes, it's just time for a change. It's a new year and we've launched a fresh new web site, complete with a new product line as well! Don't worry, all existing customers are still fully supported, and new features are fast on their way.

If you haven't seen us lately, come check out the new <http://www.flexispy.com> and tell us what you think! Our new pages are not only slicker and more

If you haven't seen us lately, come check out the new <http://www.flexispy.com> and tell us what you think! Our new pages are not only slicker and more

all existing customers are still fully supported, and new features are fast on their way.

Sometimes, it's just time for a change. It's a new year and we've launched a fresh new web site, complete with a new product line as well! Don't worry,

We're shaking things up – check us out!

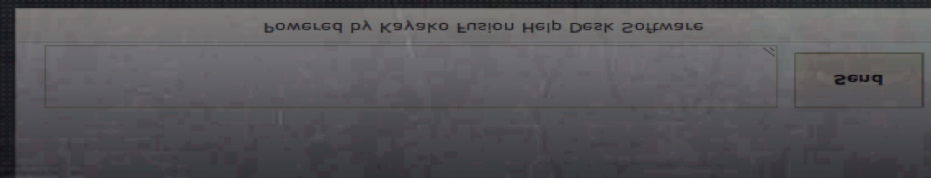
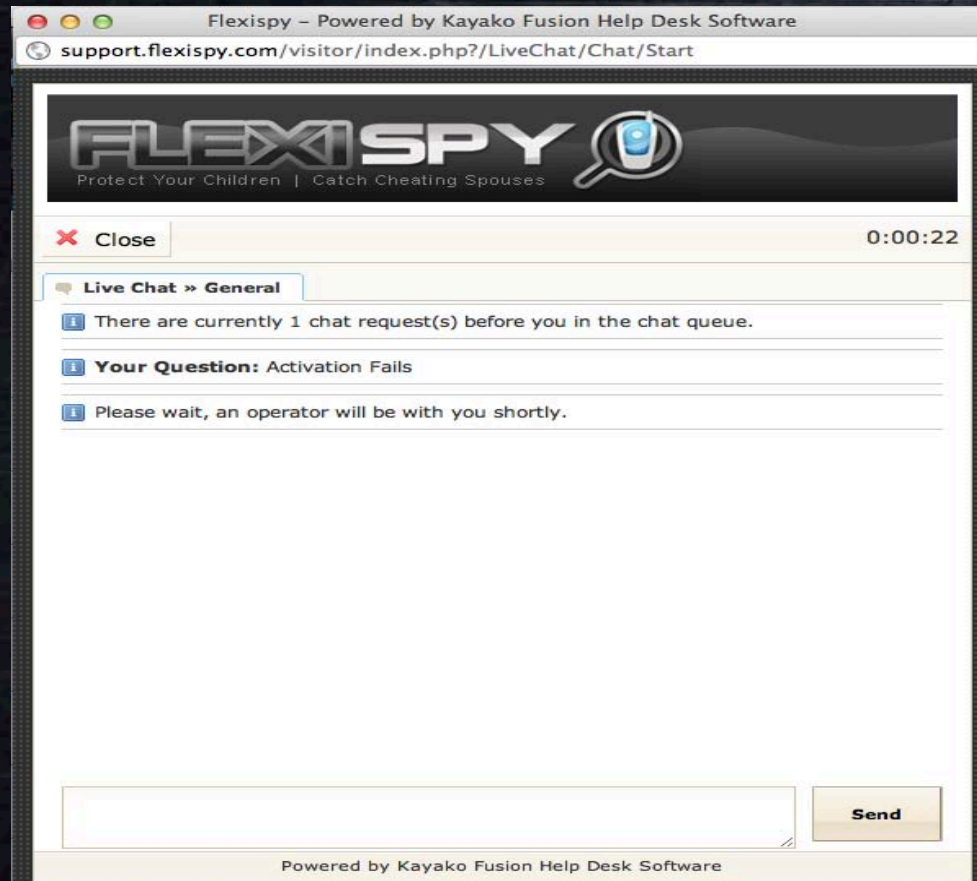
UK 44-207-979-7126
USA 1-646-240-4063

Pre-Sales Only at:
Or call us for



CrowdStrike

Live Support





Countermeasures / Apply

Pontifications

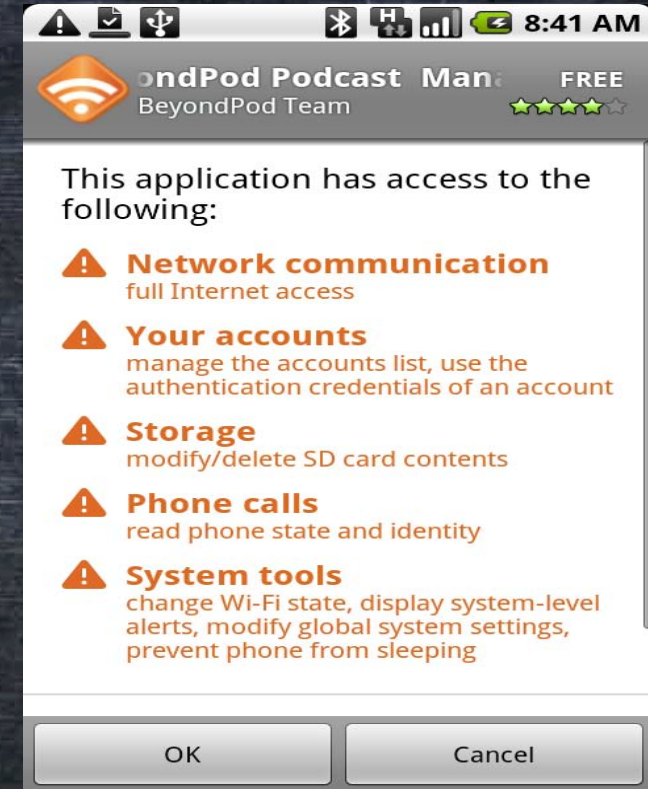
- Device manufactures and vendors are working to enhance security
- The mobile platform is a very attractive target, especially to get unparalleled close access to a victim
- Mobile users behavior is different than on conventional platforms
 - Waiting for train or going into meeting, it is easy to target the victim at a time when they may be distracted
- Users are not patching nearly as frequently as they should
 - Complex eco-system

Apply Slide / Countermeasure

- **Patch!** Not only do bugs get patched, but new security features are often added
- Treat mobile computing with the same degree of paranoia as conventional computers
 - Be alert for spear phishing/smishing/crashing applications
- Understand new risks and concerns
 - Battery drain/GPS polling/weird SMS
- Tough problem; leverage existing technologies at enterprise level to identify exploitation and C2 activity
 - Tunnel traffic through corporate networks
 - Look for C2 and exploit indicators

Mobile Conundrum...

- Is Sandboxing the answer?
 - Nickispy.A uses permissions that should require user authorization
 - We are installing as root so this is not required
- Weaponization will get harder but will always be doable
- 3rd party Security software runs in sandbox, adversaries have root – security software does not
- *When you ban root, only the adversary will have root!*





CrowdStrike