

Evolving Threats

Paul A. Henry

MCP+I, MCSE, CCSA, CCSE, CISSP-ISSAP, CISM, CISA, CIFI, CCE, ACE, GCFA

Forensic & Security Analyst – CTO - Bayside Solutions Inc
Certified Instructor, SANS Institute



An Evolutionary Failure

- Malware has evolved dramatically and unfortunately our defenses have not
 - The use of Obfuscation has rendered traditional Signature Based Defenses effectively obsolete
 - Our Port Centric firewall policies are no longer effective when malware is designed to operate over any port or service



Today's Stealthy Malware

- Malware stealth techniques that can allow execution without touching the hard drive:
 - DLL Injection
 - Process Injection
 - Hook Injection
 - Library Injection
 - Direct Injection
 - Process Camouflage



No Longer A Theoretical Issue

- **Flux** is the name of a new pest spreading covertly through the internet. Flux is a Trojan that is making the life of most anti malware vendors much harder.
 - Flux is a reverse backdoor type of Trojan. Rather than the infected machine waiting for a connection to be made from outside, the infected machine makes the connection itself.

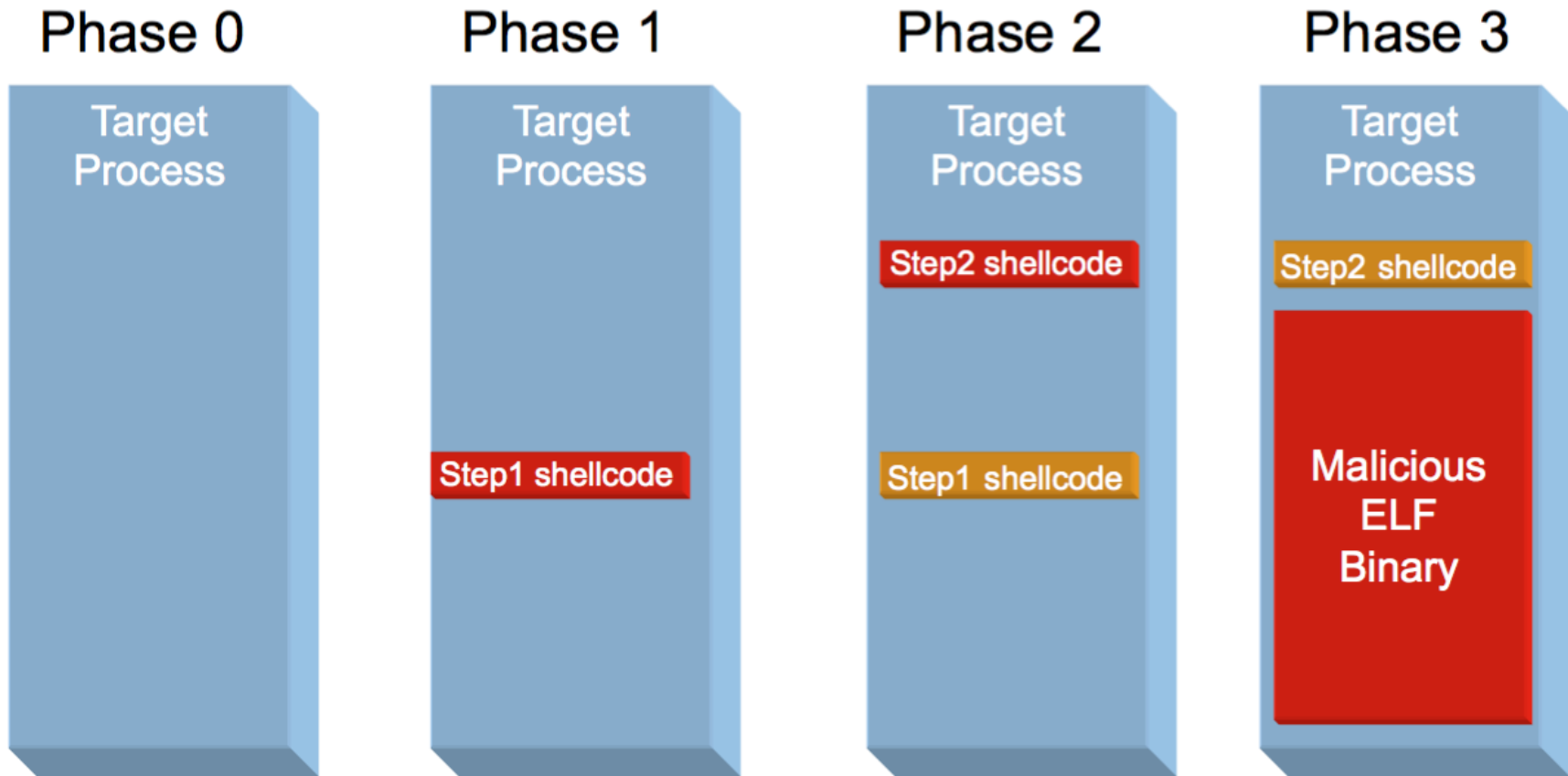
No Longer A Theoretical Issue

- Flux introduces a new technique of code injection. Flux doesn't use a DLL. Flux writes its connection code directly into a host process and executes it there.
- Apart from the fact that this behavior would circumvent several Desktop Firewalls, it also makes Flux nearly invisible to current anti malware software
- Rootkits historically have used process hiding and Code Injection
 - HE4Hook, Vanquish, HackerDefender.

Injection Malware Examples

- A Process Injection was used and the malware never touched the hard drive?
- Malicious code was hidden in popular DLL files and time stamps were changed to match the original file date?
- Stealth Rootkit installed and logs overwritten?

Malware - Windows Scenario

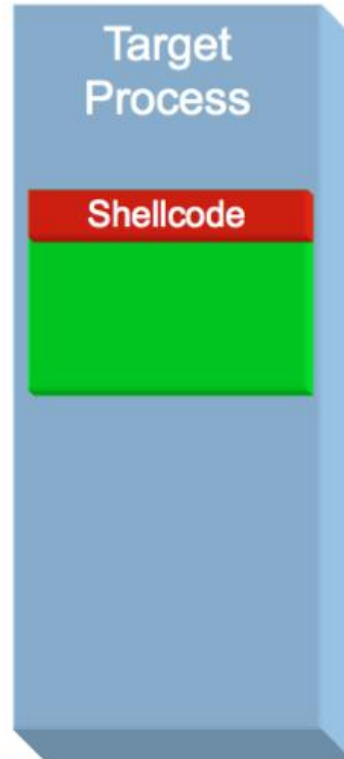


Malware - Unix/Linux Scenario

Phase 0



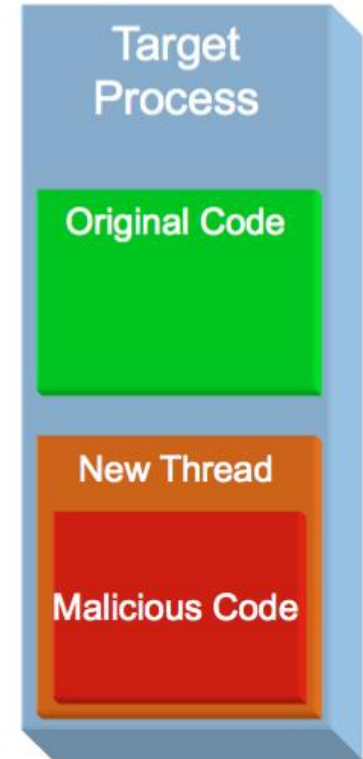
Phase 1



Phase 2



Phase 3



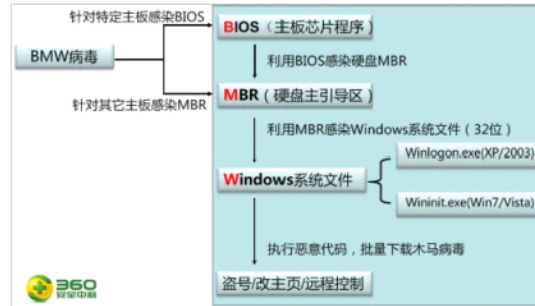
BIOS Based Rootkit

- Found in China by BMW 360 Security
- Works with popular Award BIOS
 - Once restarted
 - Infects MBR
 - Infects Winlogon.exe or Winnt.exe
 - Opens backdoor to download additional viruses and malware
 - Undetectable running a tool at the OS level!!!!

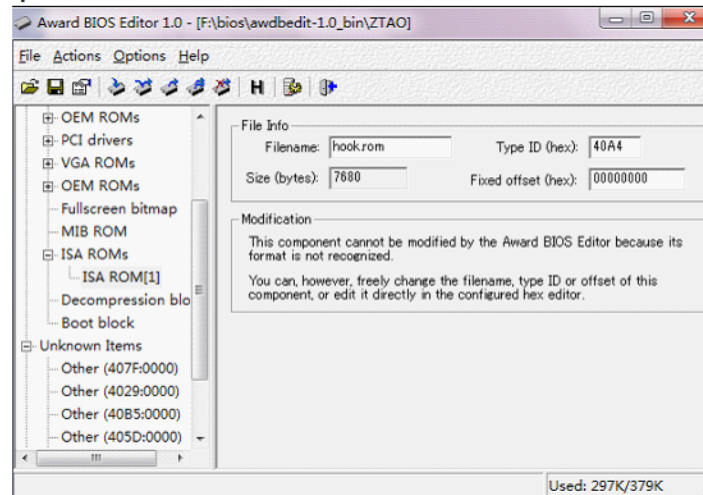
BIOS Based Rootkit

The following technical analysis for the BMW virus

BMW virus body is divided into BIOS, MBR and Windows of three parts, attack the process as shown below:



One, BMW parts BIOS virus

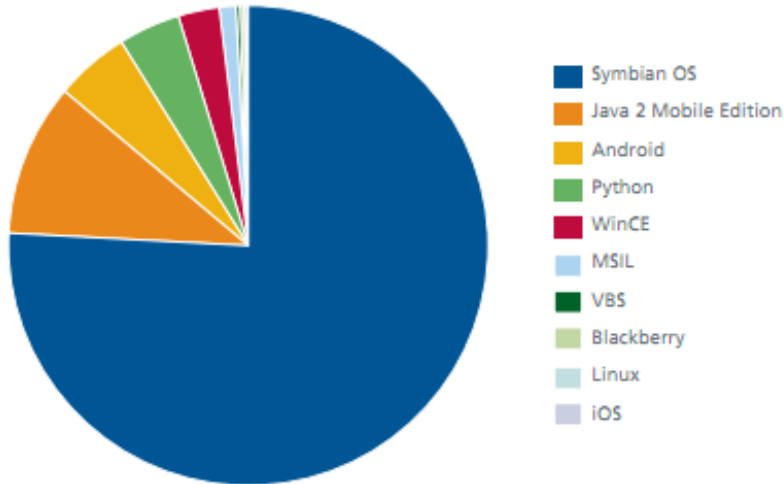


Mobile Device Threats

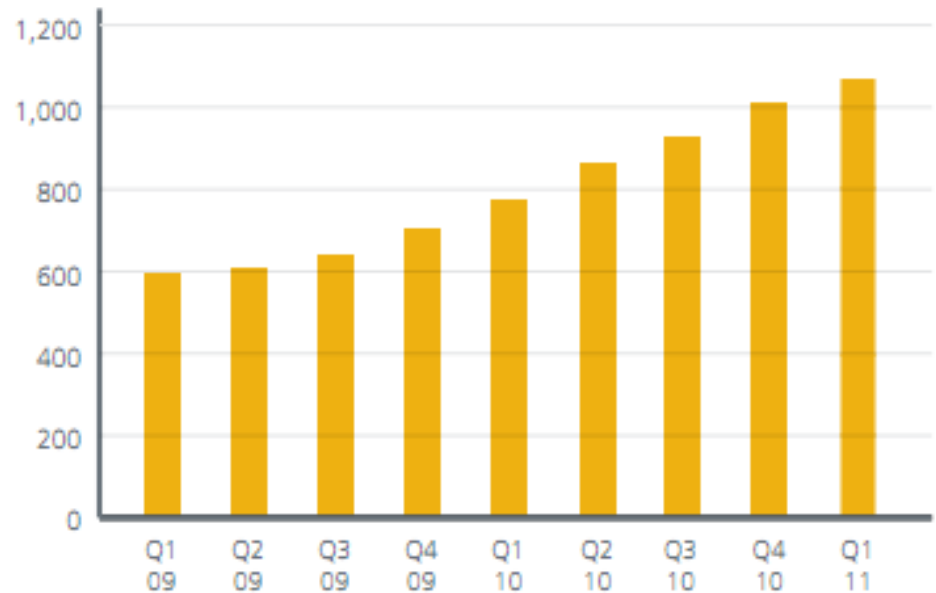
- Mobile devices are one of the most over looked threats we face today
- Many organizations with corporate issued mobile devices allow users to connect to the corporate network
 - Worse yet many allow employees to connect their personal mobile devices...
- If you fail to control mobile devices they will control you

Mobile Malware Stats

Mobile Malware, by Platform



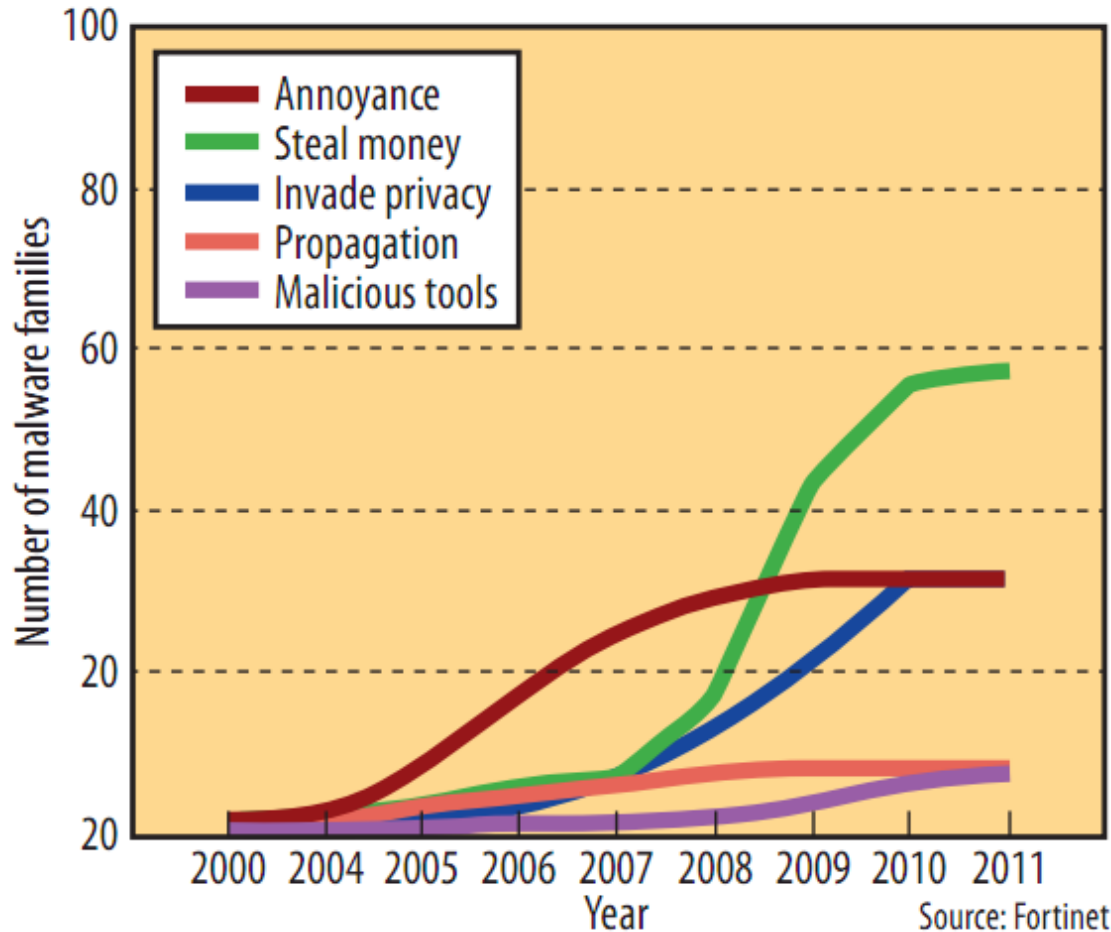
Total Mobile Malware Samples



Source: McAfee Threat Report



Same Old Song and Dance



Apple iPhone & iPad Risks (2)

- This seems to really upset some users - for the iPhone and iPad, Apple must review and approve each and every application
 - As for me I don't mind, as Apple is effectively keeping malware out by literally White Listing only approved applications being made available to their user community

Apple iPhone & iPad Risks (3)

- However many users don't like to be told what they can do with the product and have chosen to Jail Break it.
 - That is what hackers are taking advantage of – a Jail Broken Apple product faces formidable malware challenges



Apple iPhone & iPad Risks (4)

- Just like our desktops and servers, Mobile Malware across all platforms will only get worse
 - Incident Response plans must now include Mobile Devices

Worm author tells media he initially infected 100 iPhones

Hi there! If you're new here, you might want to [subscribe to the RSS feed](#) for updates.

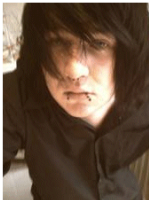
by [Graham Cluley](#) on November 9, 2009 | Comments Off
FILED UNDER: [Apple](#), [Malware](#), [Mobile](#)

The author of the world's first iPhone worm appears to be feeling pretty cocky about the whole incident.

Without a hint of apology, or the slightest acknowledgement that he may have done something wrong, Ashley Towns has been speaking to the media who have contacted him via his [Twitter account](#).

Towns, who goes by the online handle of "ikex", spread the Ikee worm which broke into jailbroken iPhones and installed a picture of Rick Astley before hunting for other vulnerable devices. In an [interview with ABC News](#), the 21-year-old student was asked if he knew how many iPhones had been affected:

"Due to the nature of it, it's kind of hard to tell, I know my phone hit about 100 alone but from there I have no idea," he said.



Apple iPhone & iPad Risks (5)

- Remote monitoring of an iPhone is getting more common
 - In my forensics practice I see Spyware installed on iPhones that is typically installed by a spouse but occasionally is installed by a coworker, disgruntled employee, or a competitor

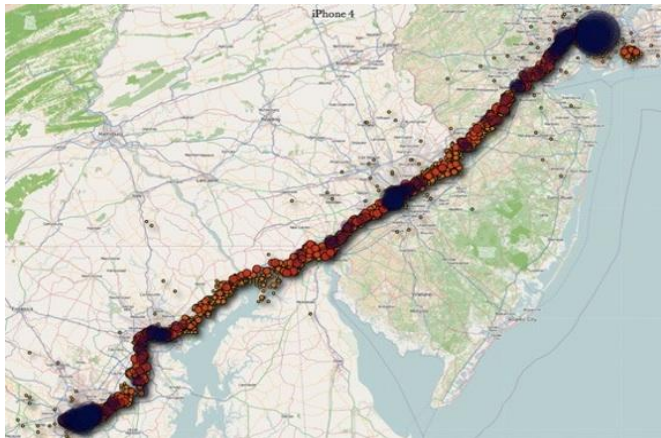
Apple iPhone & iPad Risks (6)

- State laws vary but in many, all parties using the device must be notified if they are being monitored. Some actually collect data on the wire and may be considered to be wire tap issues....



Apple iPhone & iPad?

- Where has the iPhone (and the suspect) been – location data
 - Yes Apple patched it but the patch simply encrypts the data and limits it to 7 days of data stored on the phone



Android OS Based Devices

- Fastest growing mobile OS
- Over 300,000 Android activations a day
- Android overtook iOS as the dominant OS in US during 2H 2010
- First phone launched - HTC G1 in 2008
- Currently an OS of choice for Motorola, HTC, Samsung, Sony Ericsson, among others

Android Device Risks

- With all of the news about malicious Droid Apps downloaded from the Droid Marketplace it is clearly apparent that testing apps is not a high priority before turning them loose on users



Android Device Risks

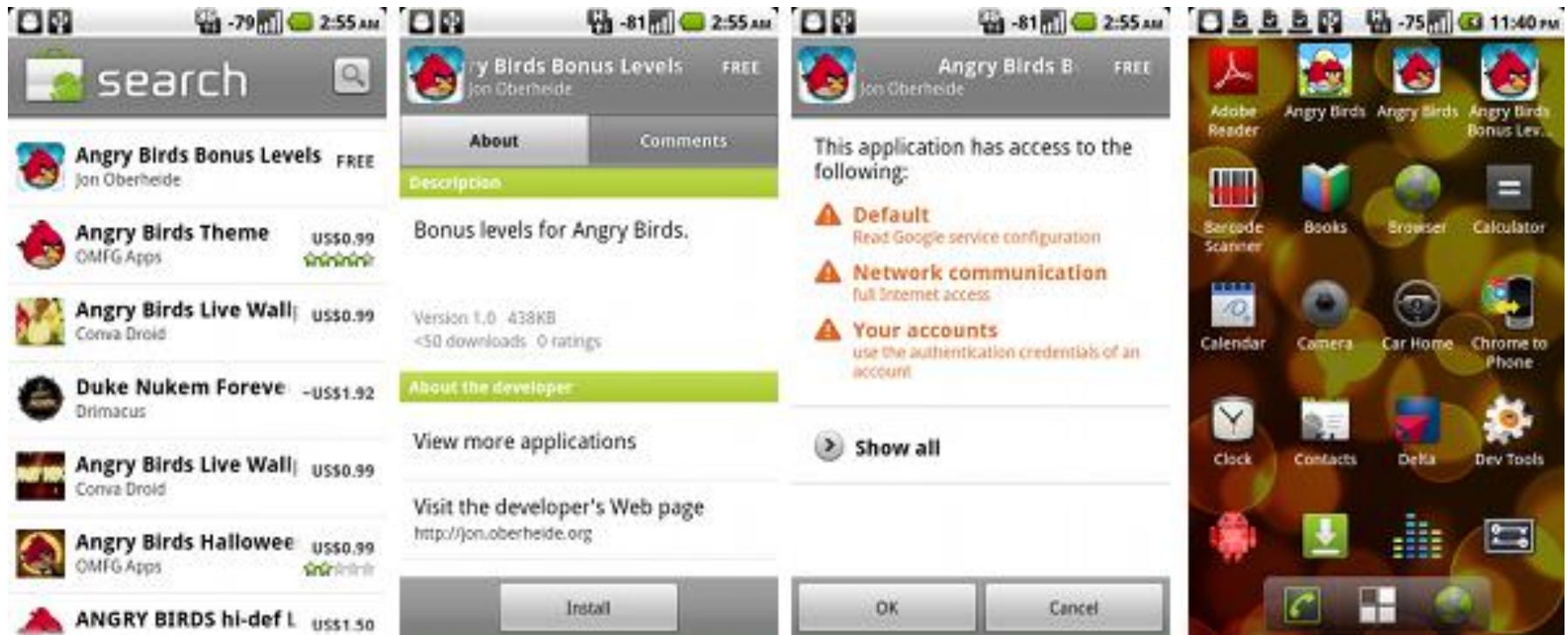
- A good example of Android security issues was highlighted with Angry Birds. Duo Security showed us that it was possible to install an app that allowed the unprompted installation of arbitrary applications with arbitrary permissions on a victim's device.

<http://blog.duosecurity.com>



When Angry Birds Attack (1)

- Hmm...



When Angry Birds Attack (2)

- Ouch...



The Droid Dream Fiasco

- There are serious issues over at Google's Android Market

Over 50 "DroidDream" Malware Apps Removed from Android Market

By [Sarah Perez](#) / March 2, 2011 7:20 AM / [6 Comments](#)

 Tweet 273

 Recommend 67

 Hacker News

 Share & Save



Over 50 applications found to contain malware were removed from the Android Market yesterday, after being downloaded approximately 50,000 times. The apps contained a type of malware called "DroidDream," which was able to use exploit code to root (take administrative control over) the phones where it was installed and steal sensitive data from the devices. In addition, a second APK (an Android application file) was also found hidden inside the code, which could steal additional data.

It Is Poised To Get Worse...

- If you use an Android smartphone, you are now 2.5 times more likely to encounter malware (malicious software) than you were six months ago.
- This year, 30% of Android users are likely to encounter a Web-based threat such as phishing scams, "drive by downloads" and browser exploits.

<http://www.cnn.com/2011/TECH/mobile/08/04/lookout.threat.report.gahran/>

Is the Droid Enterprise Ready?

- This raises concerns that Google's mechanisms for protecting Android users from threats simply aren't good enough at the present time
- While it's commendable that Google jumped quickly when a researcher notified them of the threat, that is simply not enough
- My personal opinion: With the risk of malicious apps “unchecked” in the Android Market, I feel that the Droid may be a high risk if used within the enterprise...

Is Apple Enterprise Ready?

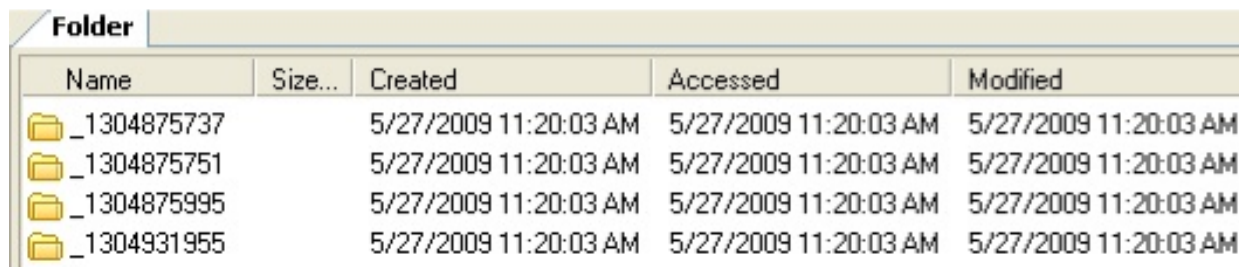
- The DigiNotar issue raises the question as to the enterprise readiness of Apple mobile devices. While Apple clearly lagged other vendors in responding to the threat on their desktop and laptops as of the date of writing this slide, we still do not have a solution for iPads and iPhones
- The recent Apple issue with AD integration and authentication of users without looking at the password does not help bolster confidence in Apple's enterprise readiness either...





Bad Guys Learn Quickly...

- They learned what tools were used to uncover their activities
 - Traditional computer forensics involves examining the contents of computer media for evidence of a crime
 - A suspect system is powered off, the storage media is duplicated then analyzed in a controlled environment
- Then the bad guys simply evolved....

Without A Trace

- Hackers today routinely cover their tracks after an intrusion
 - Log entries scrubbed or wiped not simply deleted
 - Anti-Forensics tools used to alter file time stamps
 - Malware MAC times set to match OS library files



Folder		Name	Size...	Created	Accessed	Modified
	_1304875737			5/27/2009 11:20:03 AM	5/27/2009 11:20:03 AM	5/27/2009 11:20:03 AM
	_1304875751			5/27/2009 11:20:03 AM	5/27/2009 11:20:03 AM	5/27/2009 11:20:03 AM
	_1304875995			5/27/2009 11:20:03 AM	5/27/2009 11:20:03 AM	5/27/2009 11:20:03 AM
	_1304931955			5/27/2009 11:20:03 AM	5/27/2009 11:20:03 AM	5/27/2009 11:20:03 AM

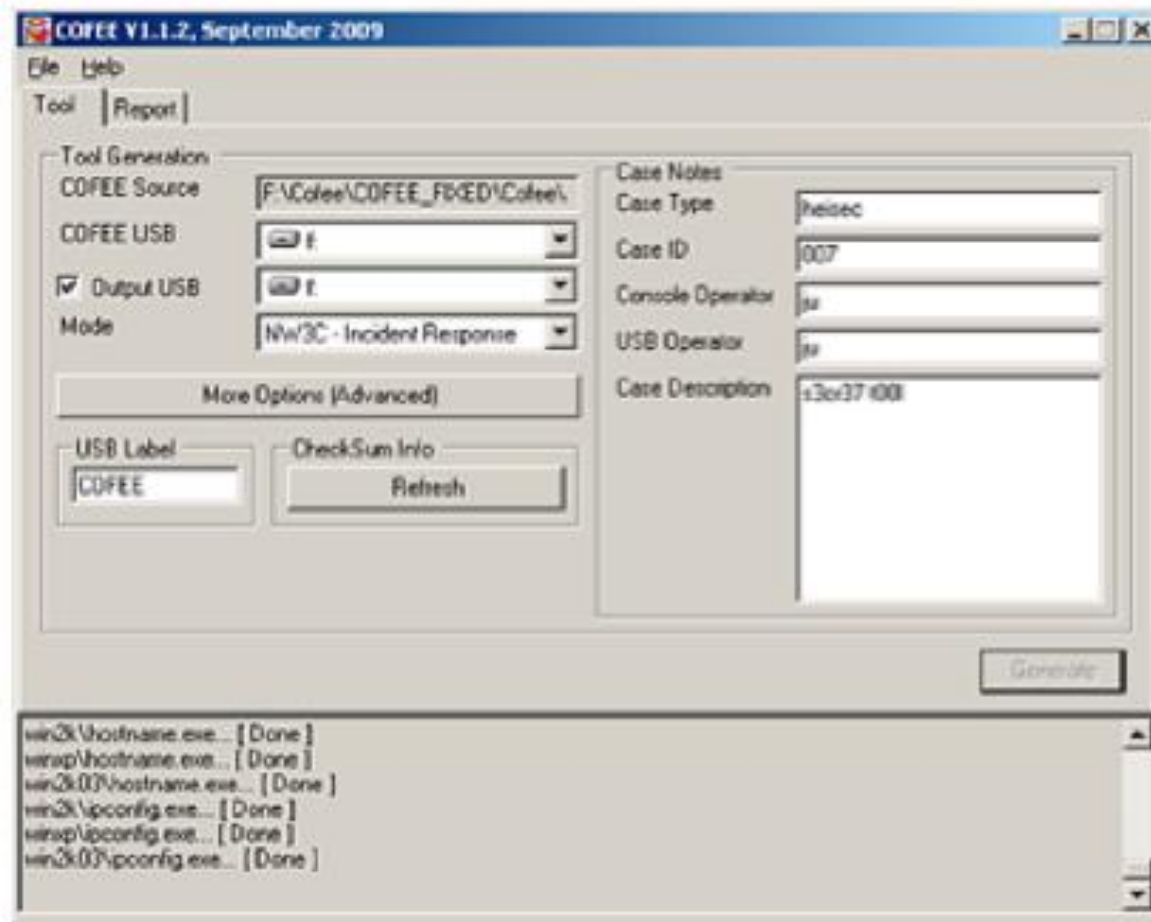
Anti Forensics Is Nothing New

- I started researching Anti-Forensics in early 2000 and presented on it at the LayerOne Event in LA in 2006

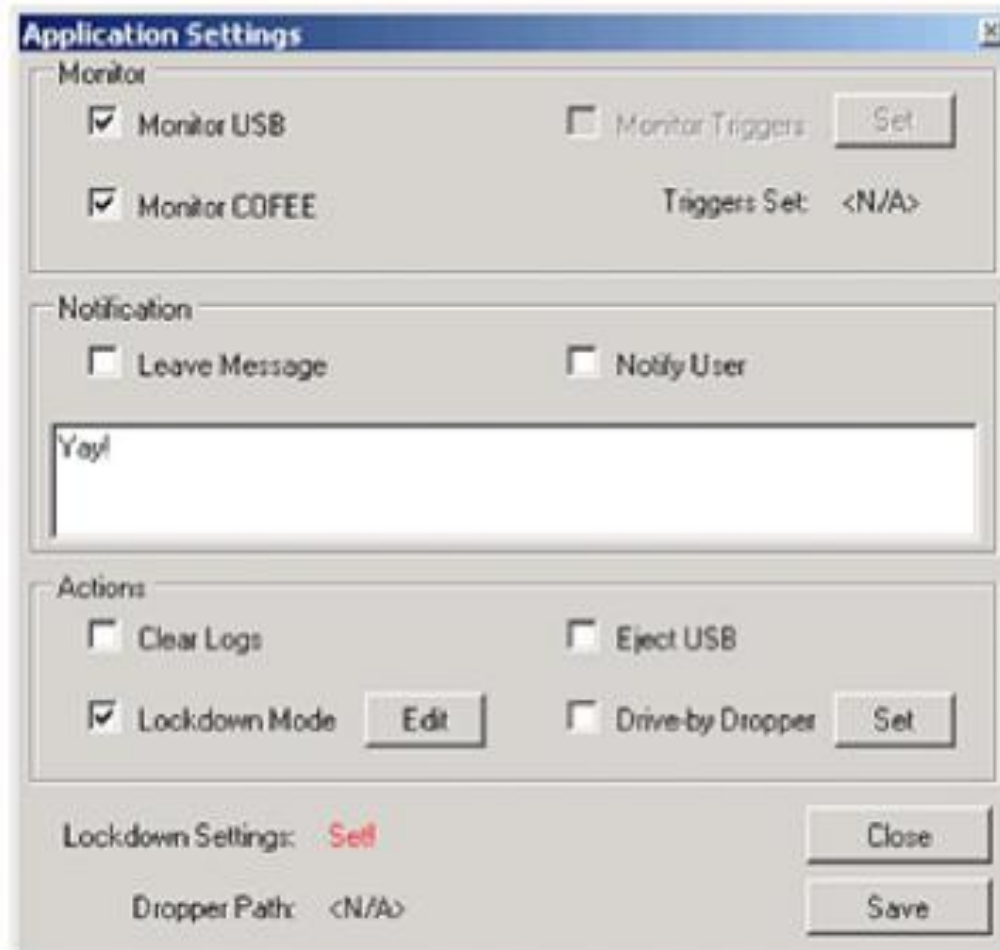
<http://www.youtube.com/watch?v=q9VUbiFdx7w>



Someone Spilled The Coffee



....Coffee Meets Decaf



Ok.... But What Can We Do?

- The Bad Guys have adapted methodologies that blow through our defenses, compromise our PC's in a manner that is effectively undetectable and hide anything that would be found with traditional media based forensics
- The time for defenders to also adapt is long over due

Revisiting The Basics

- There is no Holy Grail solution
- Make sure you have the basics covered
 - Harden exposed servers
 - Enforce the rule of least privilege
 - Review flaw remediation
 - Revisit user awareness training to include Social Media

Assume Your Already Pwned

- Your only indication that you have been breached will likely come from detective controls NOT preventive controls
- Containing a breach is just as important as preventing a breach in the current environment

Network Forensics (1)

- Even if an attacker is smart enough to clean up tracks on the victim system, remnants remain in router logs, firewall logs, web proxy caches, and other sources
- In the simplest of terms, Network Forensics follows the attacker's footprints and analyzes evidence across the network environment

Network Forensics (2)

- Network equipment such as web proxies, firewalls, IDS, routers and even switches contain evidence that can make or break a case.
- Forensic investigators must be savvy enough to find network-based evidence, preserve it and extract the evidence.

Network Forensics (3)

- Network Forensics is quickly moving from an advanced discipline to a necessity
- Traditional Digital Forensic skill sets must be updated to keep pace with the rapidly evolving threat environment
- Where does Network Forensics “Fit” within the SANS Curriculum?

Summary

- Examined the current “State of Insecurity”
- Examined Malware Capability and Methods Used to Evade Detection from our Defenses
- Examined the use of Anti-Forensic Tools to avoid detection in a Traditional Analysis

Thank You

Paul A. Henry

MCP+I, MCSE, CCSA, CCSE, CISSP-ISSAP, CISM, CISA, CIFI, CCE, ACE, GCFA, VCP - vExpert

vNet Security, LLC

www.vnetsecurity.com

phenry@vnetsecurity.com

(954) 854-9143

