



Windows, OS X and Modern Malware How Different are the Issues?

David Harley
Research Author
ESET LLC



Whoami

- Security Analyst (et al), Imperial Cancer Research Fund 1989-2001
- NHS Threat Assessment Centre Manager/Anti-Malware Specialist 2001-2006
- Independent Author/Editor/Researcher Small Blue-Green World 2006-7
- Research Author, ESET LLC 2008-present



AMTSO & WildList WG

- Anti-Malware Testing Standards Organization
 - 40 or so people at present: mostly researchers from anti-malware vendors, a few testers and other stakeholders (VirusTotal eg).
 - Looking for input/independent validation
- WildList Working Group on WildCore, Testing and Certification
 - WildList members only, but focusing on resources to make testing and test evaluation easier.



AVIEN

- AVIEN (Anti-Virus Information Exchange Network)
 - 1500 or more users
 - Not security vendors
- AVIEWS (Anti-Virus Information & Early Warning System)



Blatantly Commercial Break

SYNGRESS®

4 FREE BOOKLETS
YOUR SOLUTIONS MEMBERSHIP

4 FREE E-BOOKLETS

AVIEN Malware Defense Guide

for the Enterprise

Stop the Stalkers on Your Desktop

- Complete Coverage of the Relationship Between Enterprise Security Professionals, Customers, Vendors, and Researchers
- In-depth Consideration of Key Areas of the 21st Century Threat Landscape
- Systems Security and DIY Defense Using a Range of Specialist Detection and Forensic Techniques and Tools

David Harley CISSP, Antivirus Researcher, former manager of the Threat Assessment Centre for the U.K.'s National Health Service

Ken Bechtel
Michael Blanchard
Henk K. Diemer

Andrew Lee
Igor Muttik
Bojan Zdrnja

FOREWORD BY
ROBERT S. VIBERT
AVIEN ADMINISTRATOR



A Brief History of Mac Malware

- Prehistory
 - Old Time File and System Viruses
 - HyperCard Viruses
 - Jokes and Trojans
- Mid-90s: Mac Users become macro Typhoid Mary and (some) learn to tolerate commercial AV
- Later 90s:
 - AutoStart
 - SevenDust et al



Into the 21st Century

- Malicious Script Trojans
- Simpson Worm
- OS X introduces a Unix-based security model
- Microsoft mitigates macro problem by rationalizing Office architecture
- Office 2008 loses VBA altogether



OS X & Security

- Stream of Vulnerabilities Found and Patched
- Occasional Proof of Concept Viruses
- Occasional High-Profile, Low Impact Non-Replicative-Malware (Trojans, Rootkits)



Equilibrium

- Security/AV Industry: “Macs are currently safer than Windows, but this could change.”
- Windows Users: “Macs? I don’t think about ‘em much.”
- Mac Fanboiz: “Windoze bad; Macs good. Windoze a mess; OS X safe as houses.”



Mac Users Smarter than Windoze Users?

- Some studies indicate that there's less of a support load for a Mac-using population.
- Is that:
 - Quality/Usability of Interface?
 - Intrinsic Stability?
 - Intellectual Superiority of Mac Users?



<http://www.macworld.co.uk/mac/news/index.cfm?newsid=20176>

- **Mac users are 'open, liberal, superior'**
- **A study of Mac users finds them open, liberal and a a little smug (Jonny Evans)**
- **I couldn't possibly comment...**



Case Study – OSX/RSPUG or OSX/PUPER (or whatever your vendor calls it)

Trojan originally reported October 31st 2007 by Intego,
makers of VirusBarrier at
<http://www.intego.com/news/ism0705.asp>.

Has links to the W32/PUPER or W32/ZLOB families of
Windows malware.

Up to variant “Trojan:OSX/DNSChanger.BK”
according to F-Secure.

(Variant identifiers go A-Z, AA-AZ, BA-BZ etc, so more
than 60 variants, but depends on how you count.)

The Rise of Troy

- This concentration of malware reflects the major shift in the Windows malware arena:
- ~~from~~ replicative malware (viruses, worms, some bots)
 - ~~to~~ out-and-out Trojans (non-replicative password stealers, keyloggers, some other bots, miscellaneous crimeware)



Viruses? Who cares?

- More Trojans seen than replicative malware
- More interest in ROI: the focus has shifted from hobbyist Proof of Concept (PoC) malware to crimeware and hacking for hire



OSX/Puper is *not*...

- Script Kiddie “Look, I wrote some Mac Malware!”
- Instant Bragging Rights
- Sophisticated PoC malware that will never be seen in the wild (either not injected, or doesn’t catch on).
- Spreading like wildfire (or AutoStart, for instance)
- A Vendor Hypefest (usually described as low-risk/low-impact: actually, the risk was originally understated by most vendors)



But it is Different/Significant...

- “Professional” Crimeware
- Using similar programmatic techniques and social engineering “hooks” to Windows crimeware (Zlob family, pushed out as fake codecs).



If This Catches On...

- ... we'll have a significant problem, for Mac users and everyone else. In which case:
- Mac users need an attitude readjustment
 - Media need better information to work from
 - Anti-malware suppliers need an attitude readjustment



Back to the Future?

- Early 90s: “There are no Mac viruses.” (There were, but mostly low impact)
- Mid 90s spike: whole Mac-using populations became prime source of macro virus dissemination. Freeware AV (even Disinfectant) which had *never* been comprehensive became largely ineffective.
- Is there a parallel? (Mac users exposed to a risk they think of as Windows-specific; reliance on partially-effective freeware/open source)



The Misinformation Superhighway

- OS X is much more secure than (say) System 7 (but then Vista is much more secure than Windows 95)
- Mac and Windows users are more security aware nowadays, but that's not the same as security-literate.
- Copious conflicting (mis)information confuses the issue for both groups.
- Mac users with no or partially effective AV may miss that they're compromised until tagged by external sources or enterprise filters (eg gateway AV)



Paradox Lost – Some Mac Fanboiz Comments

- Mac users are more intelligent than Windows users and no Mac user will ever fall for a Trojan relying on a social engineering attack.
- If a Mac user -does- fall for a social engineering attack, he'll deserve everything he gets.



Mac users smarter than Windows users?

- At the moment, Mac users with no particular security knowledge may be *particularly* vulnerable to social engineering in that they believe that their systems are so secure out of the box that they don't need to know or to do anything about security. "If there's a problem, it will be patched automagically."



Apples are not the only fruit

- Security Threat \neq Technical Exploit (not always, anyway)
- Malware authors are not totally reliant on technical vulnerabilities
- Vulnerability number 1 is still wetware (social engineering)



Paradox Regained

- The Trojan is being hyped up by the anti-virus companies and the Mac-hating security community.
- Anti-virus companies are classifying this particular Trojan as low-risk, so it doesn't matter.
- (Yes, I have seen these positions taken in the same email...)

Besides...

- “Trojans don't matter because they don't replicate.”
- “Hardly any Windows malware requires user intervention, so social engineering isn't a factor at all.”



Fallacy 1: Only Viruses Matter

- In the world of Windows, where most malware lives at present, volumes of malware that doesn't (self-)replicate have exceeded volumes of replicative malware (worms and viruses, primarily) for a while, now.
- We can argue about comparative importance/impact of *specific* malware, but Trojans as a group are a serious problem.



What do we mean by Trojans?

- Working definition Non-replicative malware
 - Replicative malware that requires a response from its victim, usually programmed by some form of social engineering
 - Can include bots, keyloggers, banking Trojans, spyware, phish-related malware of all kinds, rootkits & stealthkits, yada-yada...



The New Polymorphics

- Fast spread less effective than polymorphism.
- Short spam runs, but the “shape” of the malware keeps changing (packers, compressors, obfuscators)

Packers?

- Tools used primarily (originally) to compress executables to save space
- Now more used malignantly to obfuscate code and confuse signature detection
- Can reduce the efficacy of reverse engineering under emulation/sandboxing
- Major PITA: subject of a two-day CARO workshop in May 2008.



Viruses worse than Trojans?

- Not so long ago, viruses and worms that spread far and fast were the main measure of success in malware distribution.
- Criminalization/Professionalization: how much you can steal or extort is more important than how many systems you compromise



Fallacy 2: Self-Launching vs. User-Launched

- The Mac myth is that Windows malware is usually self-launching (uses vulnerabilities and exploits, drive-by downloads, overflows, privilege escalation etc., without any action on the part of the victim).
- Some is (and much malware hedges its bets by including exploits as well as social engineering), but most malware *does* require user interaction.



User-Launched Threats

“86 percent of all announced vulnerabilities were client-side attacks requiring end-user interaction” (Roger Grimes)



What does that mean?

- Malware which works by “social engineering” — tricking the victim into running malicious software, in this case — is apparently more “successful” than malware that relies on exploiting software vulnerabilities.



Mitigation

- Malware that requires the victim to give it permission to install *may* be less effective where it's more difficult for them to run as an administrator or equivalent, or use an administrator level password to authorize the installation.



Mac Security Admin View

- Can't work because it takes so many steps and requires the user to enter their root password.
- Is it *that* difficult to trick a mark into taking those steps?



Mac Specialist View

- Most Mac specialist lists discussed the issue calmly and rationally, without the confused paranoia of the fallacies and self-contradictions listed above. Even lists where panic and abused initially ruled settled down to discuss relevant administrative issues rationally.



Media Attitudes

- “Established” Mac Information Sites mostly sober and responsible, *if* they reported it all.
- Published fixes before much AV info available.
- Little “it’s not a problem because there are no Mac viruses” issue avoidance
- Other security sources similarly responsive, e.g. bleedingsnort sigs



Non-Mac security view

- Some SchadenFreude: unsurprisingly, after years of Fanboi abuse.
- Premature prognostications: “Apple's day has finally come”; “This proves that Apple users are just as vulnerable to social engineering.”
- “..unpatched vulnerabilities are going to bite them in the behind.”
- “... the new Windows 98...”



SchadenFreude or Armageddon?

- This is an indicator, not Custer's Last Stand.
- So far, Mac users haven't fallen in droves for that particular social engineering ploy.
- Many OS X vulnerabilities do get patched, and Apple were slightly ahead on pushing system updates and patches by default.
- OS X isn't W98, any more than Vista is.



Nevertheless...

Some may see a parallel between the way OS X shook off most pre-X malware, and the way Windows after 3.x became less vulnerable to older malware



AV need to...

- Distinguish between low impact and low risk – i.e. consider the potential significance, not just the immediate effects
- Stop cowering before Mac Zealotry
- Pay more attention to cross-platform issues: different products from same vendor may not share detections.
- Gateway & External Scanners will *have* to detect across platforms



No Macs Land

- Some Mac AV doesn't detect Windows malware and vice versa.
- Some AV vendors with a Mac product don't detect across platforms, or don't do so by default
- Some gateway/external security software doesn't detect any Mac malware, though it often detects some other Unix threats.



VirusTotal et al.

- Widely used as tools for investigating/identifying malware. Useful, but not definitive.
 - Don't use all scanners (obviously) and only report what their scanners report.
 - In particular, don't at present use Mac-specific scanners (ClamAV isn't Mac-specific)
 - "Take it or leave it" as regards the settings used (heuristic level, current update status etc)



The Future

- Porn is not the only approach for social engineers.
- What forms of social engineering *will* work for Mac users, if RSPlug porn doesn't (and it doesn't seem to have, with a few exceptions)
 - Fake patches?
 - Standard bank/IRS/auction site etc phishing with a Mac binary lurking?
 - Free games and other recreational software?
 - Interesting "movies"?
 - Free antivirus/antispyware/other security programs?
- And what further measures can Apple take to maintain their lead over Microsoft NT-derived systems in security, if it exists?



Sea Change?

- January 2008:
 - The Register announced the MacBook Air as increasing risk, because would increase userbase
 - F-Secure commented on the MacSweeper scareware scam, as well as continuing to monitor OSX/DNSChanger
 - BlueCoat announced that they were extending their K9 Web Protection Internet filtering software to OS X
- Apple patched three vulnerabilities in iPhone and two in iPod Touch, plus four critical vulnerabilities in iTunes
- SecureMac's free tool for OS X/RSPlug.A
- Etc...



What does that tell us?

- Still interest in the platform both sides of the security divide: basically, awareness of profit potential. That doesn't mean all these alerts are equally important, or that the sky is falling: just that more of them are making the news (somewhere...)
- Kneejerk "stop being anti-Mac!" responses are less pronounced, and security vendors a little less diffident about flagging issues.
- Media, even Apple-loving journalists, more aware that the problem is more complicated than an evangelical issue?
- "The eyes of the world are watching now..."



Need to...

- Warn that about to make system wide change
- Educate about need to create and run as unprivileged user.
- Disable admin password for non-admin users (withhold, set as group policy, remove accounts from sudoers)
- “Harden” the admin group against wetware exploits
- “Stream” user groups, eg admin, local admin, power user, unprivileged user
- Mac enterprise admin solutions



Message to the User Community

- Macs get malware too.
- Malware doesn't have to be viral to be dangerous.
- Install and maintain competent security software. (Automate at admin level)
- Don't expect security software to give you 100% protection. E.g. don't assume AV will catch unknown malware
- Stay patched. (Should be automated)
- Keep listening to your IT/security team
- Accept that security is not always convenient, and not always a given.



Message to Apple (and Microsoft!)

- Learn tightrope walking (engineering vs marketing, security vs. convenience, QA versus PR, Complete Product versus Deadline).
- Take responsibility for customers:
 - Don't substitute marketing for information, certainly when it involves their future safety
 - If you prioritize a convenient configuration, make it clear that it could be safer and make hardening easy (some have suggested a "security wizard")
 - Accept responsibility for educating them and providing sound info on security practice and available utilities.
 - Provide sound security feature information, not "WonderOS makes you safer because it doesn't get viruses".
 - Build security awareness and expertise into your enterprise from board level down: not just security for the enterprise, but for your customers.



Wait and See, Watch and Learn

- It's not going to be altogether simple to measure the long term impact of this trend, not least because so many Mac users don't install security software at all, let alone AV.
- But we can learn something from the anti-malware community, simply in terms of their monitoring for new versions/variants/siblings.
- The rate of take-up and follow-up will be an indicator of "success" or "failure" in itself.
- Leave the bickering to the teen geeks. This is a time to be professional: observe and act accordingly.



Afterthought

- As OS X moves further from desktops/laptops/servers into the world of consumer technology (iPhones, iPods...) what are the implications for the further spread of malware and other security breaches?



The End...

- Any questions?
- (Don't feel obliged) ;-)

dharley@eset.com