Straight facts about **Mac® malware**

While remaining low comparatively to other major platforms, such as Windows® and Android™, the fact is Mac malware does exist. Last year we saw the largest ever infection on the OS X platform, in the form of the Flashback Trojan.

Does malware for Mac OS X pose a threat?

Yes. In the past two years, ESET Malware Research Lab has detected and identified many new malware families (1 family can contain multiple variants) specifically targeting the Mac OS X platform. For example, the Flashback Trojan that has infected hundreds of thousands of Mac machines.

Does my Mac need an antivirus?

No operating system is 100 % secure. While Mac OS X provides a host of security features, 3rd party applications and more complex modern malware create a need for a multi-layered protection.

Is Mac OS X malware a recent development?

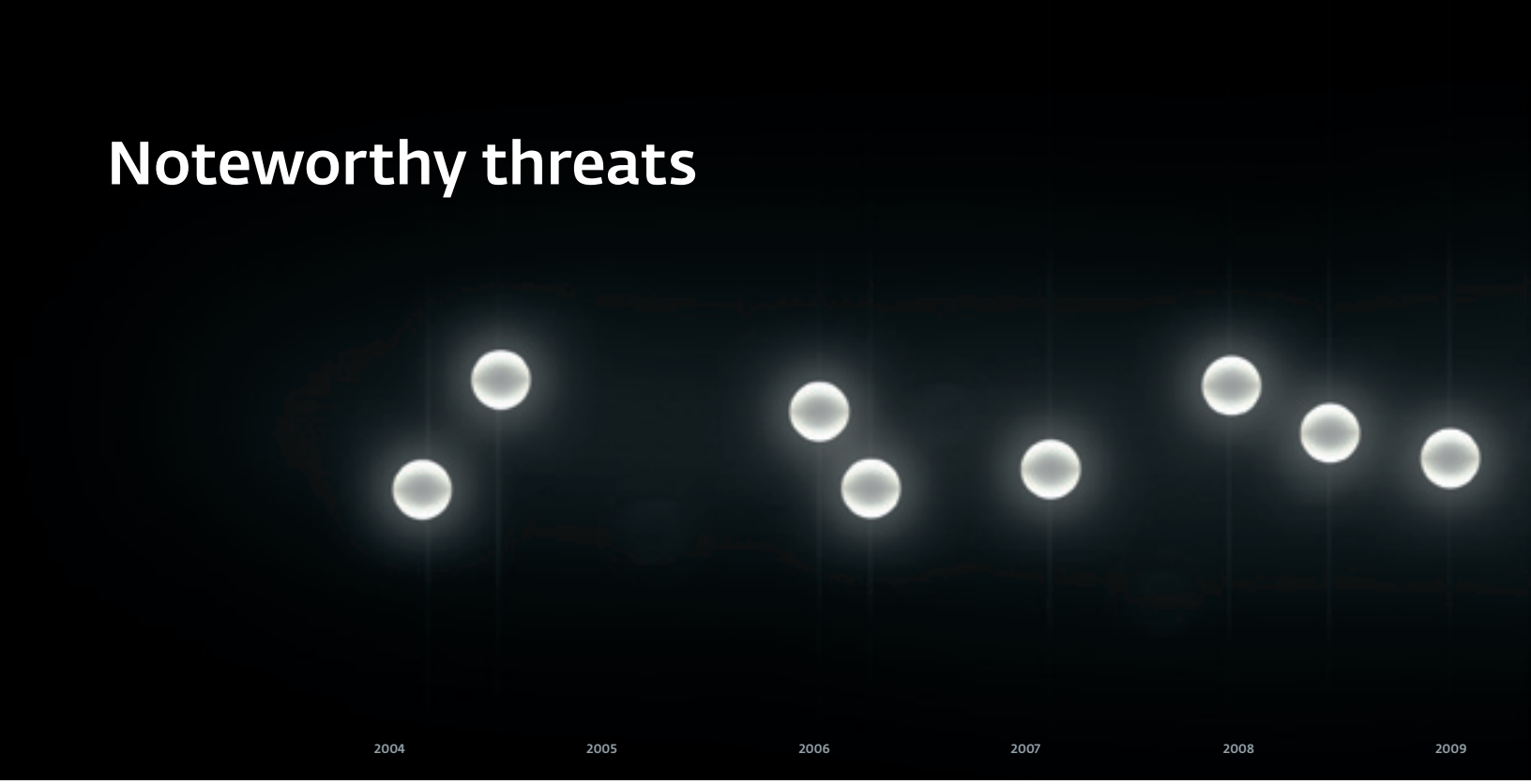
No. The first examples of Mac OS X malware date back to 2004 when OSX/Opener (Renepo) was detected. OSX/Leap.A, followed in 2006, and there have been other forms of threats developed against Mac OS X since then.

Is my Mac vulnerable to Windows malware?

Windows malware does not pose any danger to your Mac. However, your Mac can act as a carrier, which can result in it unwittingly passing along infected files from your Mac to other devices.

eset Internet Security

Noteworthy threats



2004

Amphimix (MP3Concept)

The first acknowledged OS X malware

Masqueraded as an MP3, the importance of this threat was in the timing — it was generally regarded as the first acknowledged OS X malware. However, it was never seen "in the wild".

Opener (Renepo)

Backdoor Trojan with spyware functionality

The installer, which launched during Startup, was designed to steal a host of personal items from the computer (including passwords and configuration files), as well as functionality to decrypt other password-protected items.

2006

Leap

The first true OS X worm

It appeared at the beginning of 2006 and attracted a great deal of media attention. It used a graphic icon to pass off a Unix executable as a JPG image, claimed to be the latest Leopard Mac OS X 10.5 screenshots, and was spread through the iChat messenger client.

Inqtana

Proof-of-Concept worm

The worm, written in Java®, spread by copying itself to other computers via a Bluetooth™ connection.

2007

Jahlav (RSPlug)

DNS Changer

Distributed mainly as a fake codec pack, Jahlav's purpose was to change DNS settings of an infected system — enabling the attacker to alter web content displayed in the browser.

2008

MacSweep

First OS X scareware

MacSweep was the first known OS X scareware, flagging legitimate applications as malware and trying to persuade users into buying the rogue MacSweep software.

iMunizator

Rogue AV application

iMunizator was essentially a retread of MacSweep. The "call to action" in this case was a screen saying "Get rid of compromising

files now," and claimed that the product was a "3-in-1 Internet cleaner, System cleaner, and Performance optimizer for your MAC."

2009

Tored

Worm spreading via email

Tored was a Proof of Concept worm that could spread through email and contact a command-and-control server, but it was never seen in the wild.

2010

Hovdy

Information-gathering spyware

The OS X/Hovdy family was a set of scripts designed to gather as much information as possible from a host to send it back to a potential attacker.

HellRTS (HellRaiser)

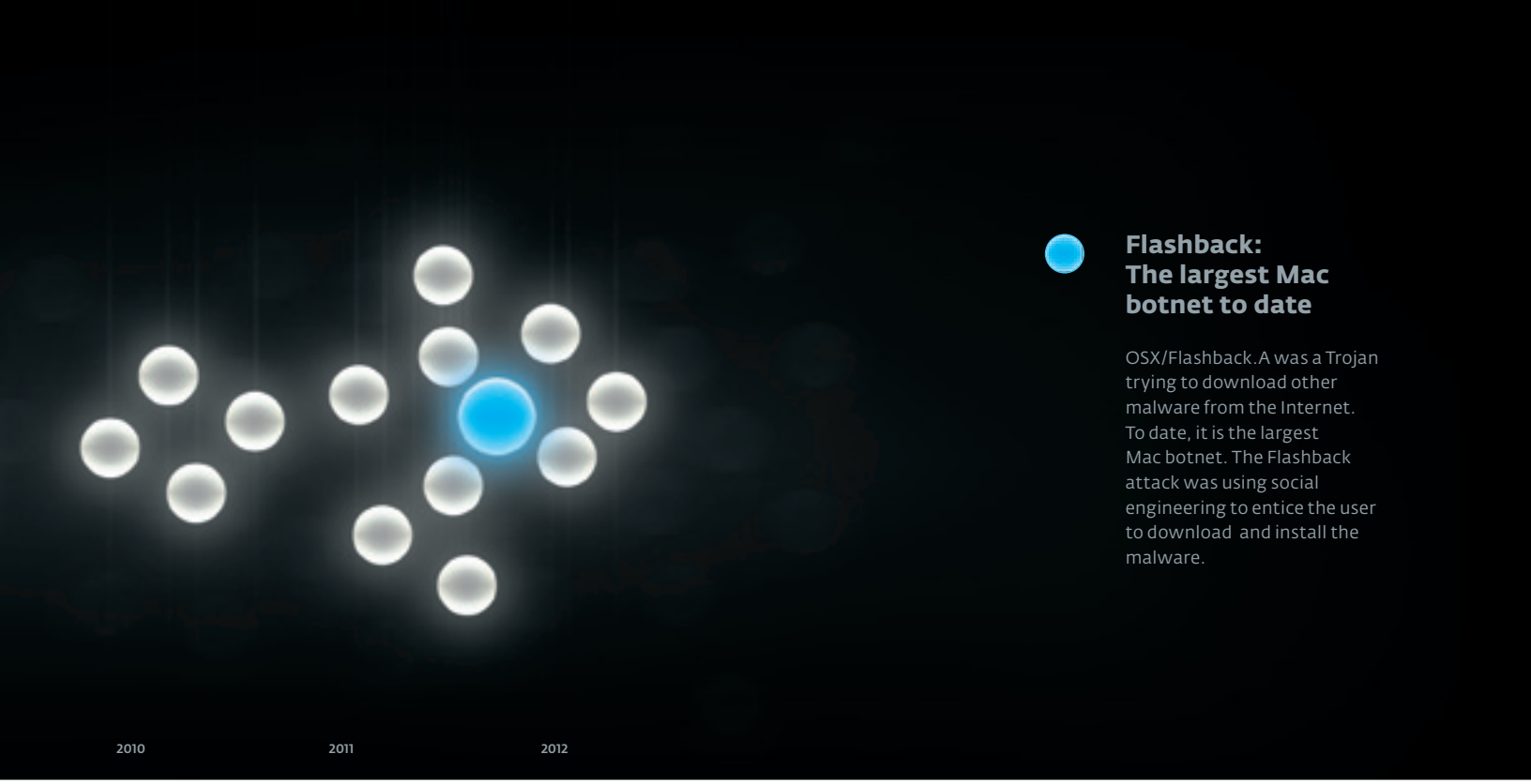
Information-stealing backdoor Trojan with remote control capability

This was a backdoor Trojan that could be controlled remotely. It was attempting to send captured information (including files and screenshots) to a remote machine, using HTTP, FTP and SMTP.
In order to get sensitive information it was displaying the dialog box below, duping users by masquerading as a typical Mac OS X permission window.

OpinionSpy

Spyware with backdoor and remote control capability

This spyware masking itself as a market research utility was offered as part of the installation process for a number of screensavers. It also acted as a backdoor and could be controlled remotely.



Flashback: The largest Mac botnet to date

OSX/Flashback.A was a Trojan trying to download other malware from the Internet. To date, it is the largest Mac botnet. The Flashback attack was using social engineering to entice the user to download and install the malware.

Boonana

Multi-platform social engineering Trojan

This Java-based Trojan that attacks Mac, Linux and Windows systems spread through social networking sites, passing itself off as a video and using the "Is this you in this video?" trick, reminiscent of Windows malware. It was used to enroll the infected machine in a botnet, a network of remotely controlled computers used for malicious purposes, without the permission or knowledge of their owners.

2011

BlackHole (darkComet, MusMinim)

Multi-function backdoor Trojan

This RAT (Remote Access Tool) came to light early in 2011. It was described as a "beta version," intended to be more stable in due course. Its abilities included executing shell commands remotely, creating text files, redirecting the browser to another website and many others.

MacDefender

The first major Mac malware

This fake AV has also been reported as calling itself MacProtector, MacDetector, MacSecurity, Apple Security Center, MacGuard and MacShield. Appearing in May 2011, it is probably the most widespread rogue antivirus on the Mac to date. The infection was spread via poisoned search engine results on image searches. When a bad link was followed in a search, the user was presented with an alert that Trojans or other threats had been detected on the system.

Olyx

A malware-downloading backdoor

A backdoor that allowed the infected machine to be controlled remotely. Its purpose was to download from/send files to a remote computer, execute shell commands, create and send out a list of files on a specific drive, etc.

Flashback

The largest Mac botnet to date

OSX/Flashback.A was a Trojan that tried to download other malware from the Internet. To date, it is the largest Mac botnet. It was using social engineering to entice the user to download and install the malware, presenting a standard and professional looking installer screen to create a backdoor. Once installed, it initiated a communication with a remote server, transmitting data such as the MAC address, OS version, UUID and more. This threat could also potentially be used to allow an attacker to inject malicious code into the targeted Mac. A later variant was even more dangerous because it was able to infect host computers without user interaction.

Revir and Imuler

Dropper/downloader backdoor with spyware capabilities

These two pieces of malware worked together to compromise the victims' computers, making their contents visible to the attacker. The malicious application was served as a PDF file displaying some politically contentious Chinese text while the app was extracting a downloader fetching and installing a backdoor Trojan (Imuler). The backdoor was intended to communicate with a C&C (Command and Control) server.

Devilrobber (Miner)

Bitcoin-generating spyware using Torrents to spread

The program has spread hidden inside copies of GraphicConverter, which is a legitimate image editor.

SEE NEXT PAGE ▶

Devilrobber was listening to command-and-control servers, creating Bitcoins – a form of electronic currency, and stealing usernames and passwords. It could also be looking for files containing child abuse material.

Tsunami (Kaiten)

IRC-controlled backdoor

This was an IRC controlled backdoor that enabled the infected machine to become a bot – part of a botnet. This botnet could be used to take down a legitimate website with an overwhelming amount of traffic, an attack known as a Distributed Denial of Service (DDoS).

2012

Lamadai

A Backdoor targeting Tibetan NGOs

This was a malware attack targeting Tibetan NGOs (Non-Governmental Organizations). The attack consisted of luring the victim into visiting a malicious website, which then would drop a malicious payload – set of instructions, on the target's computer using Java CVE-2011-3544 vulnerability and then would execute it.

Sabpab

Backdoor Trojan with remote control capability

This Trojan served as a backdoor. It could be controlled remotely to acquire data and commands from a remote computer or the Internet, using HTTP to contact a URL in its own body. This malware, like the highly prevalent Flashback variant, was exploiting the CVE-2012-0507 vulnerability. Later attacks have used Word documents exploiting a buffer overflow vulnerability in Microsoft® Office.

Morcut (Crisis)

Multi-platform spyware Trojan

Morcut was an OS X Trojan specific to Snow Leopard and Lion. It installed without any action on the part of the user and was extremely persistent, even surviving reboot. Morcut also had rootkit capabilities that could be activated if the infected system was running under root. The sensitive data it could compromise included IM transactions, location, keystrokes and mouse movement, contents of the clipboard, running processes and an assortment of other device and environment information. It hasn't been seen in the wild to date.