PANDA SECURITY | *The Cloud Security Company*

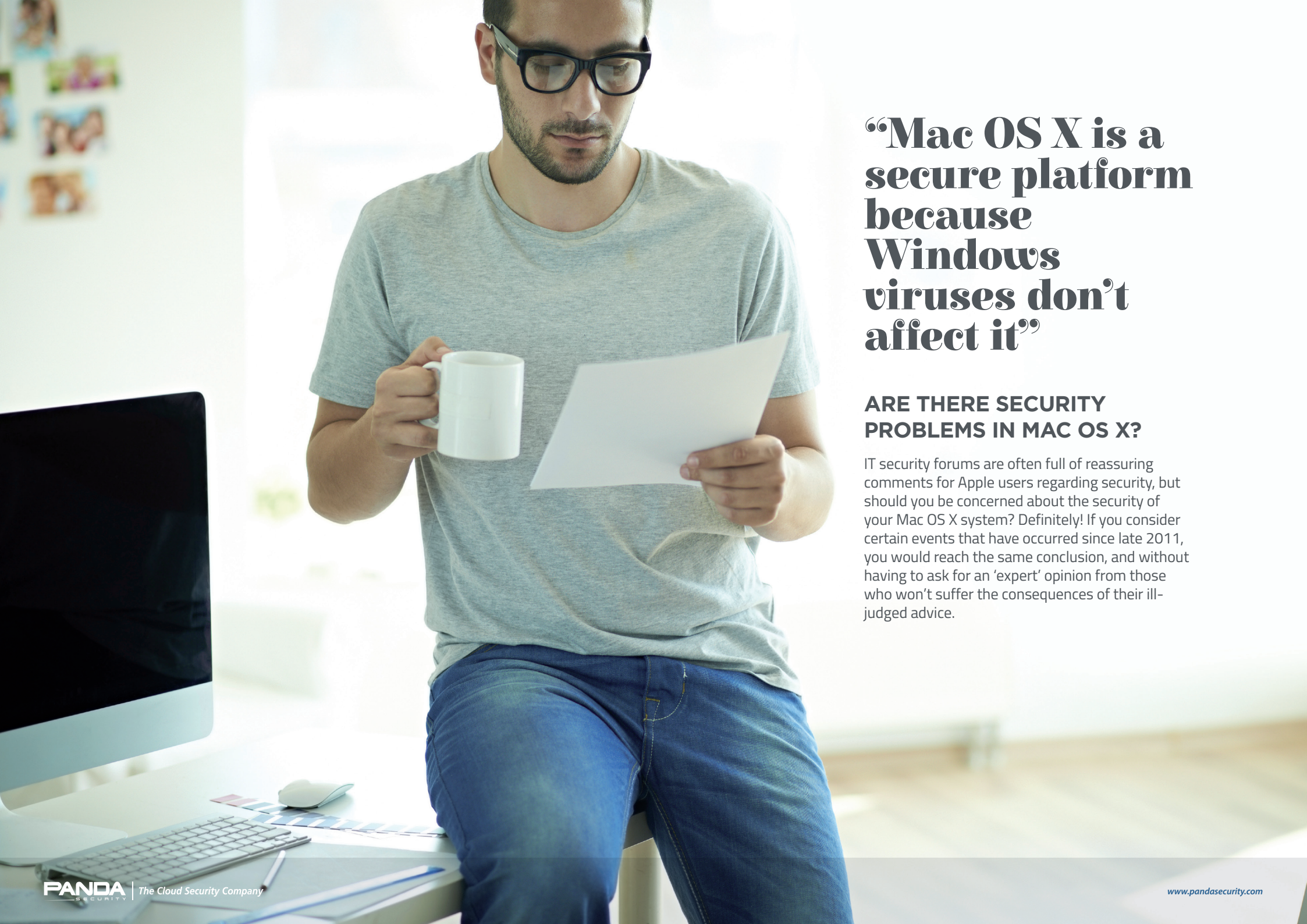
CONTENT

01
ARE THERE SECURITY PROBLEMS
IN MAC OS X?

02
IS IT TRUE THAT THERE ARE
NO VIRUSES FOR MAC?

03
WHAT IS APPLE DOING
TO PROTECT ITS USERS?

04
WHAT CAN BE DONE TO MINIMIZE
THE RISK OF INFECTION?



“Mac OS X is a secure platform because Windows viruses don’t affect it”

ARE THERE SECURITY PROBLEMS IN MAC OS X?

IT security forums are often full of reassuring comments for Apple users regarding security, but should you be concerned about the security of your Mac OS X system? Definitely! If you consider certain events that have occurred since late 2011, you would reach the same conclusion, and without having to ask for an ‘expert’ opinion from those who won’t suffer the consequences of their ill-judged advice.

Any discussion of the concept of security in Apple systems is not straightforward. This is not something that arises from the manufacturer's clear concern to protect its products from external threats, but rather an undertaking of 'good practice' from the brand. And it's true that Apple has historically witnessed few security issues, primarily as a result of its lower sales compared to its direct competitor, Windows.

The truth is it would have been somewhat strange if hackers had developed malware for such a niche platform, and it would have been even stranger had Apple developed the necessary measures to prevent its customers from being compromised, if this had never occurred in the past.

With a global share of the desktop market of around 6% in 2012, it was hardly profitable to create malware for Mac nor was it viable to develop the means to defend against something that barely existed.

The security advice that appeared on Apple's website in the past was unequivocal.

> ***It doesn't get PC viruses***
>
> *"A Mac isn't susceptible to the thousands of viruses plaguing Windows-based computers. That's thanks to built-in defenses in Mac OS X that keep you safe, without any work on your part".*
>
> ***Safeguard your data. By doing nothing***
>
> *"With virtually no effort on your part, OS X defends against viruses and other malicious applications, or malware. For example, it thwarts hackers through a technique called "sandboxing" - restricting what actions programs can perform on your Mac, what files they can access, and what other programs they can launch".*

They describe PC viruses as the only potential problem and talk about defenses built into Apple's operating system as the means to keep the platform safe; a platform so secure that users were encouraged to do absolutely nothing to protect it. So the problem –supposedly– simply didn't exist.

Yet in June 2012, the message underwent a significant change.

> ***It's built to be safe***
>
> *"Built-in defenses in OS X keep you safe from unknowingly downloading malicious software on your Mac".*
>
> ***Safety. Built right in***
>
> *"OS X is designed with powerful, advanced technologies that work hard to keep your Mac safe. For example, it thwarts hackers through a technique called "sandboxing" - restricting what actions programs can perform on your Mac, what files they can access, and what other programs they can launch".*

Now there was no mention of PC viruses, and it's easy to imagine why. It was no longer possible to ignore the existence of specific malware for Mac.

To be on the safe side, they also withdrew the invitation to users to do nothing to protect their systems.

In June 2012, Apple first spoke about malware in a keynote speech at the Worldwide Developers Conference (WWDC) as part of the presentation of its Gatekeeper technology, which would "help keep the system malware-free."

All of this serves to show that Apple platforms have always been vulnerable to malware, just as its competitors systems have been.

This was finally demonstrated towards the end of 2011, when an Apple security provider -Intego- identified a Trojan, which it dubbed 'Flashback'.

This malware exploited a vulnerability in Java, which had been known for several weeks, to infect more than 600,000 Macs over several months. Moreover, 274 of these systems were in Cupertino, California, home of Apple's HQ.

Any advanced Windows user will know that many infections are quite visible and often result in changes to a system that may indicate the existence of malware on your computer.

On a Mac platform however, you could be infected for a fair while and yet be unaware, given that Mac OS X conveys a false sense of security which is, in the end, highly detrimental to your data security.

Apple platforms have always been vulnerable to malware, just as its competitors systems have been.

“Mac OS X viruses don’t exist”

IS IT TRUE THAT THERE ARE NO VIRUSES FOR MAC?

It is also difficult to talk about security in Mac environments because it involves talking about flaws and bugs, which enters the terrain of techie talk and also of brand loyalties. Security experts claim that “the greatest vulnerability of Macintosh is the belief among devotees that the Apple operating system is superior and that this makes them immune to malware”.

Strictly speaking, a virus is a malicious program embedded in another program or file that can spread itself to other computers. However, Flashback was not a virus, but a Trojan which once installed, would download software specifically designed to steal bank account details, browser passwords and other confidential information from the user's computer. The point here is that we should be talking about malware and security in general, not just viruses.

To say that there are no viruses that affect Mac systems is highly dangerous: it leads to confusion, and in terms of security, confusion leads to financial losses.

Apart from Flashback, other malware for Mac that have had some kind of impact include:

Pintsized

It is a malware that exploits vulnerabilities in Java to open a backdoor on a computer and allow a hacker to take remote control of the system.

CoinThief

It is a malware that appears to be a legitimate application for making payments on the Internet but which really steals Bitcoins.

Icefog

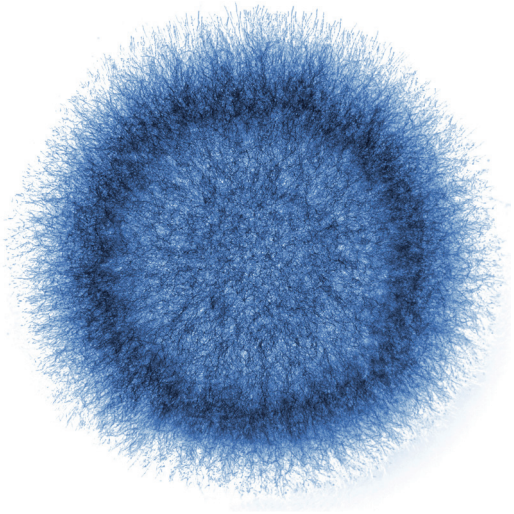
It is a cross-platform malware used in cyber-espionage in Japan, South Korea and other parts of Asia.

Mac Defender

It is a fake anti-virus that gets users to register the program and pay for 'protection'.

The consequences of malware are always the same, regardless of whether they are viruses, Trojans, rootkits or ransomware, there's no need to know all the technical jargon. **What you need to know is that there is malware out there that CAN affect your Mac OS X and that it's your finances that are at stake.**

To say that there are no viruses that affect Mac systems is highly dangerous:
the greatest vulnerability of Macintosh is the belief among devotees that the Apple operating system is superior and that this makes them immune to malware.



“You don’t need to worry about security in Mac”

WHAT IS APPLE DOING TO PROTECT ITS USERS?

Even though some users still deny it, there is a war on and this is evident by the way attacks and defenses are continuously developed. There is a community whose financial motivation to develop malware grows in parallel with sales of Mac OS X, and consequently, Apple develops protection and defenses to keep its users safe... or so it might seem.

The main problem is that Apple has arrived very late on the scene; a scene in which Microsoft is now battle-hardened having suffered greatly some years ago. The arrival of the Internet saw the beginning of an exponential growth in malware, and Windows 95, 2000 and XP were the platforms with which Microsoft had to cope -practically on its own- with the situation. There had never been a similar situation before and the company had to react quickly under the pressure of millions of infected systems.

The result of such a steep learning curve is a company now strongly committed to security, with a clear schedule for releasing security bulletins and the capacity to react swiftly when it comes to releasing patches and updates for its operating systems.

Apple's case is quite the opposite: It only releases updates when it considers it necessary, and in the case of Flashback, **it took six weeks to release the fixes to the flaws that led to the infection**, even though the patches had already been developed and released by Oracle.

There have been other similar cases, such as Icefog, where **Apple took two weeks**, to include the signature file in its Xprotect anti-virus. During this time, Icefog continued to infect the computers of users who were unaware of the problem. **Compare this with cloud security providers who deliver updates in a question of minutes!**

Neither does Apple have a clear policy when it comes to announcing the end of product support: with the release of versions 10.9 and 10.9.1, for example, several of the fixes included were not available for earlier versions (Lion and Mountain Lion). Yet with the release of version 10.9.2, the company did publish security fixes to protect users of Lion and Mountain Lion from malware. But in this case, Snow Leopard (10.6) was overlooked.

If you have a 10.6 system, update it as soon as possible!

The consequence of all of this is that **users don't know when or if solutions will be released if they don't have the latest version of the operating system**. Apple's commitment to security is simply not up to the task. Keeping users in the dark is its main strategy and perhaps the reason for this is that **it is not finding it easy to let go of its image of the 'invulnerable platform' that was so beneficial to it in the past**.

Mac OS X 'antibodies' are beginning to appear, and although this is a major improvement with respect to the security of the platform, but as Apple's security provision is part of the basic installation of the operating system, malware creators are already aware of its existence.

On the other hand, since2009 Apple has been progressively including substantial changes to its operating systems in order to bolster security. A short summary could include:

- **Leopard (10.5)**
  SandBox, file quarantine and application firewall.
- **Snow Leopard (10.6)**
  Xprotect anti-virus.
- **Mountain Lion (10.7)**
  Gatekeeper.

Apple has been progressively including substantial changes to its operating systems in order to bolster security

Mac OS X 'antibodies' are beginning to appear as if it were a biological organism, and although this is a major improvement with respect to the security of the platform, it has the same effect as Security Essentials in Windows: as Apple's security provision is part of the basic installation of the operating system, malware creators are already aware of its existence and therefore concentrate their efforts on developing counter-measures to beat the protection.

That's why users need to complement Apple's basic security provision with a good third-party anti-virus.

WHAT CAN BE DONE TO MINIMIZE THE RISK OF INFECTION?

Common sense and prudence are key to avoiding malware infections. Being aware that your system is vulnerable, using caution when handling the information available on your devices, installing a good antivirus and keeping it up-to-date, and avoiding suspicious-looking files and websites are the first steps in protecting your computer from cyber-attacks.

Going back to 2011, Apple was proud to announce on its website that its system was immune to PC viruses. And that was more or less true: in general, a virus written for a Windows system won't work on Mac OS X.

With the emergence of specific malware for Mac OS X, threats for Windows were still a potential source of problems in mixed environments or even with respect to corporate image. Imagine sending an offer to a customer with an attachment infected with PC viruses; third-party statistics suggest that 43% of malware on Mac OS X is native Windows malware.

Whether it is to protect your own systems, the Windows computers around you or your corporate image, you can give your Mac OS X system a decent level of security with just a few simple measures.

Facebook and other social networks are, very often, a spreading gate for malware.

Handle only files that come from a reliable source.

---

1. Your Mac system is not invulnerable

Keep in mind the following unequivocal truth: Your Mac system is not invulnerable. Your computer could be infected and your systems, instead of helping you detect it, could be working against you, making you think simply that viruses 'don't work' on Mac.

2. Get a good third-party antivirus

Whatever your Mac OS version ,you will benefit greatly in terms of protection. The malware in circulation at the moment aims to overcome Apple's own protection, and the more antivirus solutions there are on the market, the more the efforts of hackers will be diluted and consequently the chances of infection will be much lower than if there is a de-facto monopoly on security.

3. Install all updates

Install all updates as soon as they are released for your operating system and for any third-party applications you have installed.

4. Take care which files you run

Sites like Facebook and others are a typical source of malware from so-called 'friends'. The same applies to email attachments from unknown senders and files downloaded from P2P programs: only download and run files from reliable sources.

5. Disable problematic software

Java and Flash are both technologies with a long history of bugs and exploits. Go to the Security panel of your Safari browser and disable the Java module or click 'Manage website settings' depending on the browser version.