macOS AND CYBERSECURITY

COMMON BELIEFS AND MISCONCEPTIONS

Data Security Guide

DO APPLE DEVICES NEED SECURITY SOFTWARE?

When it comes to cybersecurity, macOS is seen by many as a role model. Some Apple fans might even view their fruit-labelled computer as immune to attacks by cybercriminals, with Apple itself considering built-in macOS security measures adequate for the threats targeting it. However, there are macOS-specific cybersecurity and privacy threats, so even if you believe there is no overt malware threat to macOS devices, endpoint security software can certainly add value, especially for devices in a business network. ESET researchers take a closer look at five common beliefs associated with macOS cybersecurity.

The SolarWinds supply-chain attack, vulnerabilities in Microsoft Exchange and countless ransomware incidents are just some of the most prominent cyberattacks that made headlines in the early part of 2021... with new ones appearing almost daily. There is one thing all these attacks have in common: the security problems usually concern Microsoft systems. In comparison, Apple's macOS pops up only in a handful of cases each year.

This may be due to the fact that Windows remains the most used operating system on corporate endpoints and servers. Nevertheless, Apple has been slowly but steadily increasing its market share, and as the number of devices using Apple operating systems rises, so does interest from cybercriminals.

In business environments, Macs are popular amongst creative professionals such as graphic designers and video creators, and in desktop publishing. For personal use, MacBooks or iMacs may be preferred due to the intuitive

and user-friendly interface of the operating system and applications, and the devices' high-end design.

But how secure is macOS, and are the popular beliefs about its defences true? Let's look at some of them.

Belief #1:
"There's no malware for macOS"

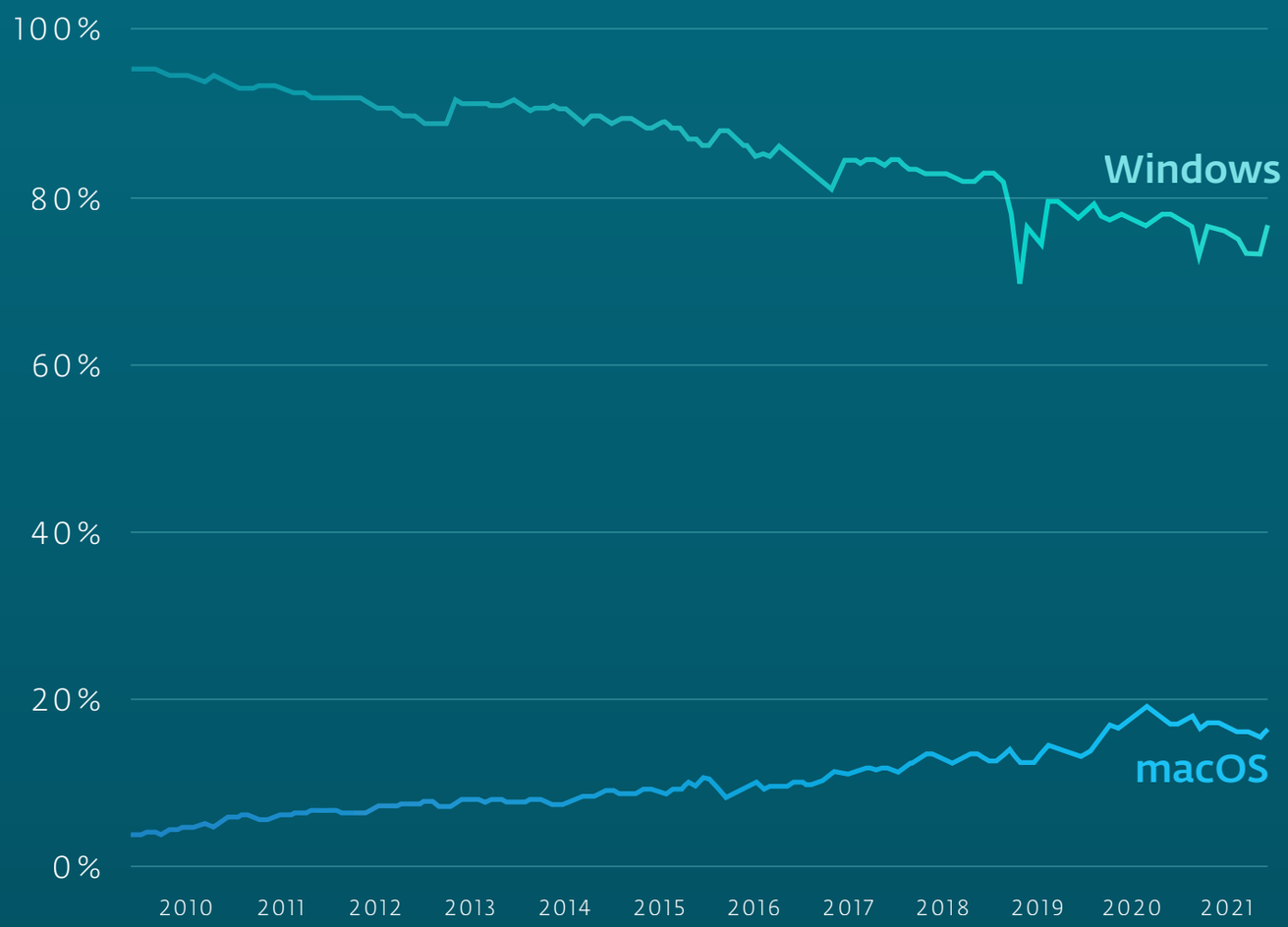
Belief #2:
"macOS is secure by design"

Belief #3:
"Those few vulnerabilities don't mean anything"

Belief #4:
"Hackers are not interested in Apple"

Belief #5:
"Macs don't need a security solution"

Global market share of desktop operating systems



Source: StatCounter

Belief #1:

“There’s no malware for macOS”

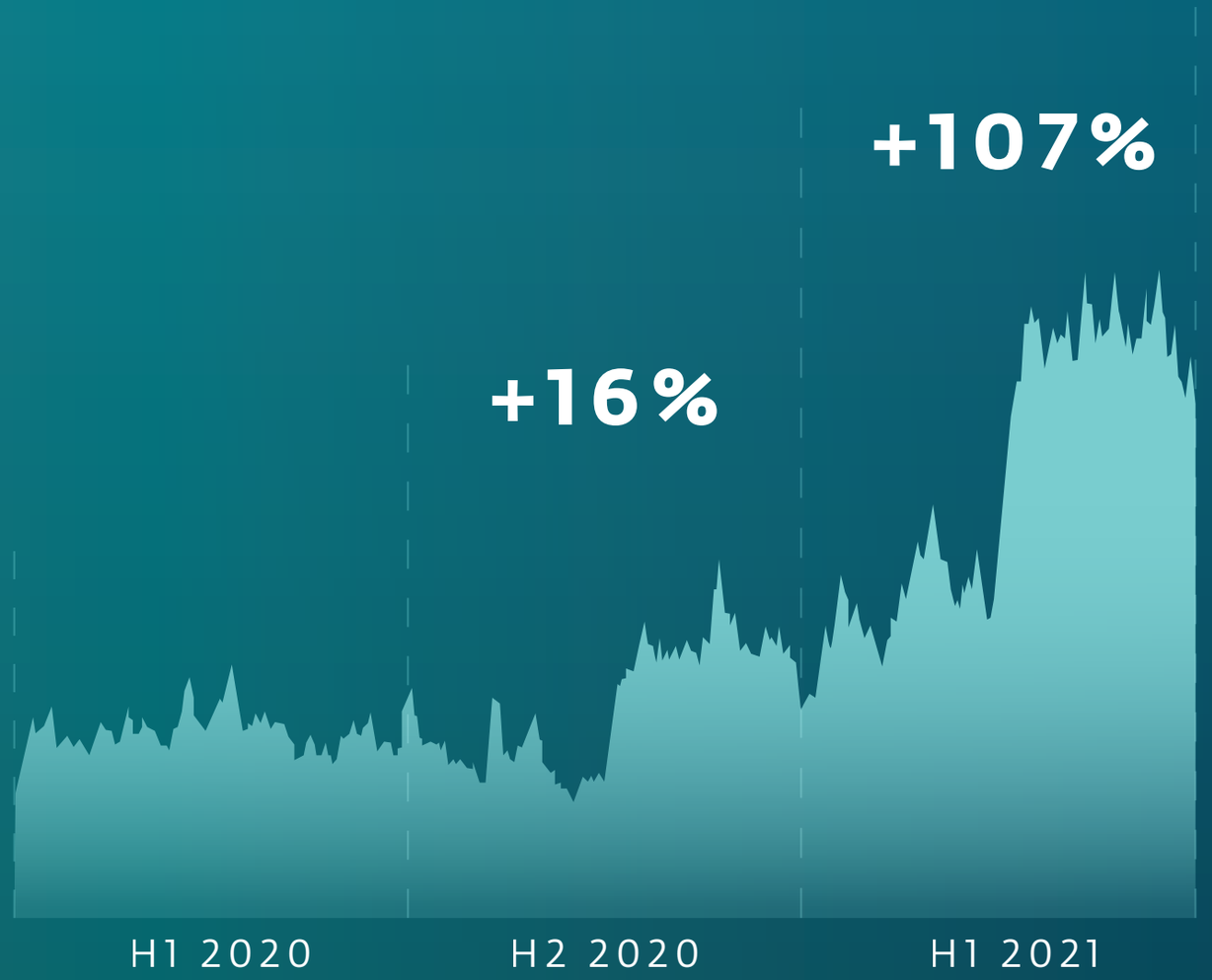
WRONG: There are thousands of malware families targeting macOS. ESET telemetry shows tens of thousands of trojan detection events globally throughout 2020, with a significant upturn in activity since the last quarter of 2020.

In November 2020, the Silicon Valley-based company introduced new Macs with Apple Silicon M1 chips. This news seemed to have caught the attention of cybercriminals too, who released new malware only weeks after the chips had been introduced. The GoSearch22 app is a variant of the Pirrit adware family, a common threat targeting Mac users. It typically displays fake coupons, banners and pop-up ads, and promotes dubious websites,

but there have been cases where it also collected browsing data and other sensitive information. The version targeting M1 chips installed itself as a Safari extension and achieved persistence as a launch agent.

The growing popularity of cryptocurrencies has also been mirrored in the variety of Mac threats. ESET detected a malware family that poses as crypto-trading software for macOS, yet stole browser cookies and crypto wallet credentials, and took screenshots of the victim's screen. To achieve their goal, malicious actors bundle a legitimate trading application with their malicious code, rebrand the "new versions" – using names such as Cointrazer, Cupatrade, Licatrade and Trezarus – and distribute it via a fake website mimicking the legitimate one.

macOS trojan detections



Source: ESET telemetry

Belief #2:

“macOS is secure by design”

LARGELY TRUE: Apple has been doing a lot to keep macOS safe from current cyberthreats, employing multiple layers of protection, including basic, signature-based malware protection, firewalls, built-in encryption and a backup solution. To further improve the security of some of its newer models, Apple even added a fingerprint scanner (“Touch ID”) as a means of multi-factor authentication.

To contain potential damage caused by compromised software, macOS employs App Sandbox. This technology limits any given app’s access to sensitive resources and user data to the bare minimum needed to get its job done. All apps distributed via Apple’s App Store are sent for notariation – a process which scans them for malicious activity. Additionally, before any of the approved apps can be launched, another built-in technology called Gatekeeper verifies their signature and ensures they have not been altered since being signed by Apple or by an “identified developer.”

eset

Despite these protective mechanisms, every now and then malware slips through the cracks. And even Apple itself sometimes slips up in terms of security:

#IAmRoot

To misuse the so-called #IAmRoot vulnerability, anyone with physical access to the device only needed to use “root” as the username and leave the password slot empty in any authorisation process and press return multiple times. Only the first attempt was rejected, but due to a bug, any of the following ones granted elevated rights.

Spectre and Meltdown

These flaws – which affected Intel, AMD and ARM processors – allowed a rogue process to read all virtual memory without authorisation. The protected memory space can often store sensitive information, including drivers, passwords and cryptographic keys. Attackers could exploit the vulnerability to bypass important security measures – such as App Sandbox – and import malicious code into the targeted system.

Initial troubles with Big Sur

Transitioning to macOS Big Sur was not as seamless as Apple fans might have expected. The long download times and crashes were caused by Apple’s signature server, which is designed to detect and block malware. These issues also brought privacy-related problems, as Apple devices were returning unencrypted data on what software was opened, when and via which IP address, so anyone with access to the network was able to eavesdrop. Apple says it resolved the reported issues via updates.

Belief #3:

“Those few vulnerabilities don’t mean anything”

WRONG: In December 2020, Apple released important security patches for macOS Mojave and Catalina. The updates fixed more than 50 vulnerabilities, several of which were ranked ‘critical’ in their associated CVEs. Amongst the affected areas were graphics drivers for AMD and Intel; App Store; Audio; Bluetooth; CoreAudio; CoreText; FontParser; HomeKit; ImageIO; Kernel; System Settings; and WLAN. Some of these flaws enabled attackers to run malicious code with elevated rights, making these vulnerabilities exceptionally dangerous.

If this were an isolated incident, this belief would probably survive. However, one look at the statistics on the community-maintained vulnerability database VulDB.com shows that this is not the case. Latest data even suggests that the number of vulnerabilities reported for Apple software outpaces other popular vendors, including Oracle, Microsoft and Google.

Number of reported vulnerabilities

Source: VulDB.com, 25 June 2021

Belief #4:

“Hackers are not interested in Apple”

PARTIALLY TRUE: For a long time, macOS did not seem to be very lucrative for cybercriminals. A relatively small number of users and a relatively secure operating system meant a lot of work for minimal financial gain. Nevertheless, with the growing popularity of Apple devices, preferences of hackers may also start to change and Apple may become more of a target.

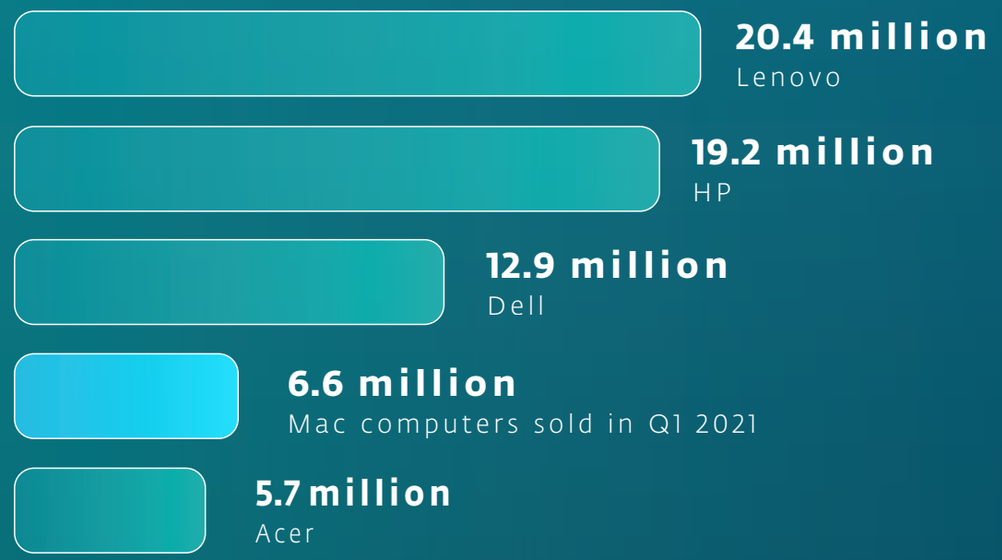
Once you buy an iPhone or an iPad and fall in love with it, it is also more probable that you turn to Mac computers instead of Windows PCs. This appears to be supported by the current sales figures published by Canalys, a company specialising in market analysis. Apple sold around 6.6 million Macs in the first quarter of 2021; compared to the same

quarter of the previous year, this represents a growth of 105%, notably outperforming the 55% market average. Apple's global market share grew as well, increasing year over year from 6% to 8% in Q1 2021.

Yet it's not just the increasing number of Mac fans that makes this operating system somewhat appealing to cybercriminals; for example, according to a US survey by RJI Online, Apple device owners seem to earn more than Android users. To malicious actors, this means a juicier and financially much more attractive target.

Thus, it is no wonder there is an increasing number of Apple security vulnerabilities that are actively sought out, exploited and only made public later. Thanks to these vulnerabilities, cybercriminals don't have to wait until the users make a mistake that would let them in and can find other ways to access victims' valuable data, or extort them by deploying ransomware.

Apple sales compared to other PC Brands



105 % Annual growth, compared to 55% market average

6 → 8% Increase of market share from Q1 2020 to Q1 2021

Source: Canalys PC Analysis, April 2021

Belief #5:

“Macs don’t need a security solution”

PARTIALLY TRUE: Many Mac users are not aware that their computers already run a built-in security solution, called XProtect, that is constantly on the lookout for malware. In contrast to many third-party alternatives, this solution uses signature-based detection only. To identify malicious code, the system uses regularly updated YARA signatures that are based on Apple’s threat landscape monitoring. To ensure that Mac users are protected from the latest threats as soon as possible, XProtect updates these signatures independently from other system updates.

Despite all of these protective measures, malware can still find its way onto Macs. For those cases, Apple offers another built-in tool called the Malware Removal Tool (MRT). This engine is designed to help with remediation, and removes malware upon receiving the latest updates. It also continues to monitor for compromises after restart and login.

In general, XProtect and MRT protect Mac users effectively. However, if the device is connected to a company or home network with Windows PCs, it can become a springboard for network-wide compromise. Therefore, if the Macs are not protected accordingly, malicious code can use them as a way to bypass the network firewall or sandboxing, and smuggle itself into an otherwise safe environment.

To avoid this scenario in mixed environments, a multilayered antimalware solution that protects both Macs and Windows computers against the latest cyberthreats is necessary and, for companies that follow the Zero Trust security model, even a must.

CONCLUSION

Apple's macOS currently belongs to the safer spectrum of the operating systems on the market. Regardless of the security shortfalls described, the manufacturer offers a very good security architecture that is constantly being updated and developed. The issues caused by Spectre and Meltdown should also be solved by employing the new "Apple Silicon" processors, which should also give Apple much greater control over its products. Upcoming operating systems should be optimally adapted to Apple's own chips, which can contribute to the security of the devices. With that being said, even macOS can become a target for cybercriminals, and some might even try to use it as an open door into otherwise safe environments.

Therefore, a reliable multilayered security solution that can protect Macs as well as other operating systems in the network is necessary for users and their devices to stay out of harm's way.

To start protecting your macOS devices right away and to discuss how ESET solutions can work for you, please reach out to us at sales@eset.com.

Data Security Guide

For over 30 years, ESET® has been developing industry-leading security software for businesses and consumers worldwide. With security solutions ranging from endpoint and mobile defence to encryption and two-factor authentication, ESET's high-performing, easy-to-use products give users and businesses the peace of mind to enjoy the full potential of their technology. ESET unobtrusively protects and monitors 24/7, updating defences in real time to keep users safe and businesses running uninterrupted.