macOS malware analysis: How can you stay safe online?

For decades, Apple strongly advocated that their MacBooks and iMacs are free from serious security threats. One should admit that the statement is overwhelmingly true up to a certain extent as Macs were a far less tempting target for cyber attacks. But those days are long gone. The prime reason for macOS being less prone to attacks as compared to Windows was the relatively lower number of systems running the macOS. But as Apple's operating system is becoming much more popular, threats targeting macOS is unfortunately far too common. Despite all the stringent security measures taken by Apple for macOS protection, the threat landscape for the platform is changing, malicious codes targeting Macs are more proliferating than ever, and the company may have to acknowledge that their highly regarded operating system is no longer resistant to malware attacks.

With the increase in market share, Mac has become an attractive target, and cybercriminals are toiling more to develop advanced full-fledged malware for the platform, mostly targeting business users than other individuals. To add, in-built defense mechanisms and security measures for Mac failed to come to fruition, leaving the doors open for these malicious actors to intrude. macOS malware has come a long way from isolated incidents to thousands of malware data breach cases reported in the past few years. What this sudden change is aiming to tell is that it is high time to come out of the presumption that macOS is invulnerable to security threats, have a long hard look at the different aspects of macOS malware, and think about what you can do to ensure the device safety.

What is macOS malware?

Malware, the short form for malicious software, is any code, script, computer program, or other kinds of software specifically designed with malign intent to damage, disrupt, or gain unauthorized access to a computer, server, or a network of computers. They can hide within the system and collect sensitive data that is being processed in the computer's chip or stored within the system. Mac system rarely shows symptoms that tip-off to being infected by malware. Many malware doesn't act suspiciously but run quietly in the background as cybercriminals are giving particular care to building sophisticated malware programs.

How does macOS malware work?

The installation process of most malware starts with users unknowingly downloading app installers or files from the web. Being unauthorized, the software will be blocked by the built-in security features on Mac, but the user will be provided with instructions to bypass the security restrictions to install the package. The intended software is then installed along with malware payloads, which are saved to any hidden folder so that

there is nothing suspicious.
Once the malicious software is installed within the system, it searches throughout the system for executable files. It then affixes malicious code at the beginning of the file, and when the file is finally executed, the malicious code will be the first thing to be executed. The code can copy file content to new invisible files and do other malicious actions.

Why did this happen?

Most of the data breaches and damaging malware attacks happen due to negligence, which opens up potential security holes that the malicious threats take advantage of to harm your Mac or your privacy. Users clicking on malicious links, downloading apps from unreliable or illegitimate sources, allowing unauthorized access to their systems, leaving sensitive data exposed, failing to update the software on time, etc. can welcome malware to their system. Any Mac user can fall victim to this.
One of the common ways cybercriminals use to distribute malware is to embed them in genuine-looking apps or maliciously modify genuine applications. The norm of installing apps outside the Mac App Store turns out to be a blessing for cybercriminals. Malware is also distributed with email as attachments and through the internet in the form of web downloads. Criminals provide fake data that make everything appear authentic.

Dark sides of macOS malware

Installation of malware on Mac causes many hardware and software vulnerabilities, totally wrecking the system and proving arduous to get rid of which includes:

- Slowing down the system and cooling fans started to run at high speed.
- Reduced battery life.
- More electricity usage.
- Hardware damages due to overheating.
- Compromise personal information.
- Emotional and financial distress.

Breaking down different types of malware that plagues Mac

Malware can range from annoying and relatively harmless popups to outright full-fledged damaging programs. A single malware program often includes multiple malicious functions with equal or varying threat levels. Many intend to take control of the user's Mac, host illegal content, collect sensitive information, and spread the infection to all other computers belonging to the same network. Some malware can be quite a nuisance than a danger. There are different types of malware with different malicious

codes contained in them and each of them behaves entirely differently once they get into the Mac system.

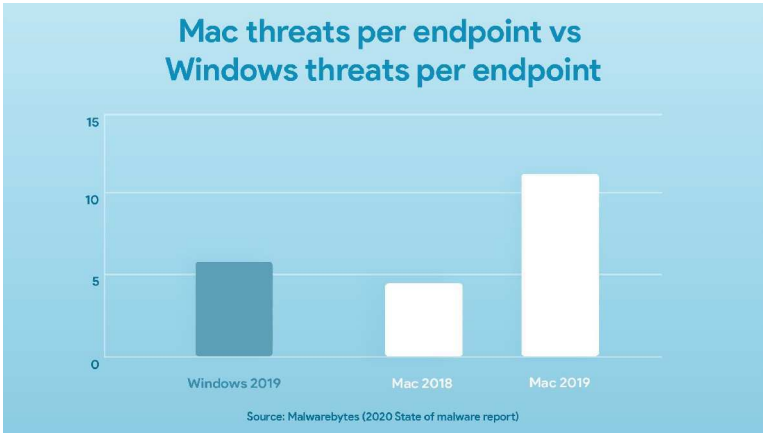
- Worms – Worms are a kind of viral program that spread through ways other than coming attached to any files. It is quite difficult to find their source and the worst thing is that they are self-replicating. So, once they intrude into a system, their goal is two-fold. They cause all possible damage to the infected system and start cloning themselves. Then, they seek to spread over networks as far as they can and carry out malicious actions on new hosts.
- Macro viruses – Macro viruses are cross-platform viruses that are often embedded with data files. They can take screenshots, corrupt data, move text, format hard drive, modify menus or commands, and alter application functions. They get active the instant a user opens the infected file. Macro viruses are capable of copying themselves into other files inside the same application. That way, they get spread when you open other files and share those files with other systems.
- Trojan horse – Trojan horse disguises itself as something desirable in order to penetrate the Mac system. Once they are downloaded or installed onto the system, they carry out malicious activities that can compromise the system. The trojan horse can affect the system security in different ways, from paving the way for the installation of other malware to handing over the remote control over the entire system to the hacker.
- Ransomware – Ransomware is a type of malware attack that denies the user access to their data forcefully encrypting the files on a system that could be of any value to the user and make a ransom demand in order to get them decrypted. They sometimes hold the file hostage, delete critical files, and keep deleting important files until the user pays the demanded ransom. Ransomware is more prevalent on Windows computers than on Mac laptops and desktops.
- Spyware – Spyware is a form of malicious software that gets installed on Macs without the knowledge and permission of the users. They monitor the system activities, including browsing activity, application activities, call, and message logs. It invades the system, steals data, and relies it to external users, advertisers, or data firms. They often sell your network data, payment information, and other personal information including login and password details.
- Scareware – As the name suggests, they scare the users by merely displaying a fake warning that their system is heavily infected with worms, viruses, and malware. The attackers persuade users to buy protective software. The phony alert stays until the user register for what is shown in the alert, and the user ends up paying for a worthless program. Scareware may sometimes manipulate users to call a provided premium-rated number for tech support. The attacker can earn money in this manner too.

- Worms – Worms are a kind of viral program that spread through ways other than coming attached to any files. It is quite difficult to find their source and the worst thing is that they are self-replicating. So, once they intrude into a system, their goal is two-fold. They cause all possible damage to the infected system and start cloning themselves. Then, they seek to spread over networks as far as they can and carry out malicious actions on new hosts.
- Botnet – Botnet refers to a network of hijacked computers that are normally used by cybercriminals for malicious attacks and scams. Botnet gains access to a system employing malicious coding and forces the system to join the army of connected computers bent on destruction. Each of the malware-infected devices that are added to the system is called a zombie computer or bot. This network of computers is meant to collectively attack other systems or launch threats to websites, usually for monetary gains.

Malware is always evolving to become more potent. Here is a quick list of some recently reported Mac malware:

- XCSSET malware – This is a family of worms found spreading through the Xcode projects in Github. They collected sensitive personal information, including passwords and payment details via the Safari browser.
- Shlayer – This newly updated Shlayer malware comes in the form of a Trojan horse appearing like an Adobe flash player installer. After the user downloads the installer, it shows on-screen steps for installing. As the user follows the on-screen instructions, a bash shell script is instantly opened and executed using the Terminal app. Running the script extracts a zip archive file, and the Mac app will be installed in a hidden temporary folder. When the app is launched in order to appear genuine it wi/ll download an Adobe flash player installer. However, the Mac app in the hidden folder is designed to introduce other malware packages to the system.
- TheifQuest – This malware combined the properties of ransomware and spyware to cause more devasting harms to the infected systems. The ransomware part of this malware is considered incomplete as the ransom note simply shows the Bitcoin address to which the ransom payment is to be sent. The attacker won't get the details of who all made the payment, and also, there is no email id attached for the user to contact the attacker for the decryption key. The spyware capabilities of ThiefQuest include stealing personal information, including passwords and credit card credentials. They exfiltrate files from infected devices and serves as a backdoor for secondary attacks.

Are Macs outpacing Windows to become the primary target for Malware?



Some recent statistics
In the last decade, the cyber threat landscape is clearly showing an inclination towards businesses with increasing business-focused threats and more sophisticated attack vectors. Initially, Macs were less susceptible as they were less in number for enterprise use.

But as the enterprise share of the Mac platform suddenly shoot up, there's a sudden uptick in the threats targeting Macs.
The 2020 State of malware report by Malwarebytes shows that Macs have surpassed Windows with more threats per endpoint in the period of 2018 – 2019.

How efficient are the built-in security tools in fighting macOS malware?

In order to prevent malicious attacks, Apple has in hand some of the strictest security strategies, though, on occasions, some effectual malicious software slips out of the net to enter the Mac system. There are stringent security checks for all the apps distributed via the Mac App Store. In addition to this, there are some other security mechanisms and examinations a Mac software should pass through.

Gatekeeper

Gatekeeper has been an inevitable part of Apple's security mechanism for years since macOS Mountain Lion and is often referred to as OS X's defense against malware. Gatekeeper's duty is to check the downloaded to make sure that only trusted software runs on Macs. Gatekeeper checks code signing and ensures that the app is verified by Apple before allowing the application to run on the system in order to minimize the likelihood of inadvertently executing malware.

App notarization

App notarization is one of the toughest security measures taken by Apple for software distributed outside the Mac App Store. Notarization is the process of getting a stamp of

approval from Apple after an app downloaded from a third-party server passes through the notarizing security process by the Apple notary service, which scans the software for malicious content. Gatekeeper allows only notarized software to run on Mac.

Browser safety

The default Mac internet browser, Safari, has the capability to identify websites containing malware. Safari is a full-featured browser with many more security features, including ad-blocking, blocking unwanted popups, private session browsing, intelligent tracking prevention, warning before connecting to unencrypted sites, and prompts of approval before downloading files.

All the above-mentioned security mechanisms are helpful but can't be considered universal. History shows that much-advanced malware can easily bypass them. With this in the mind, it's better to complement the Apple security mechanism with additional security measures. Businesses themselves have to reconsider their security strategy and take steps to tie over the ever-rising tide of malware attacking macOS.

A security action plan for macOS

As macOS cannot be considered totally bullet-proof, an average Mac user should exercise cautious online behavior to take malware off their system. Understanding the different ways by which Macs can be infected is the prime step to keeping your Macs and files safe and secure. Some of the major malware attacks can be prevented by simply taking the proper security measures while using the device and the internet. As malware is always evolving, there is a constant need to update the security practices to inhibit the latest mode of attacks.

Here are a few guidelines to ensure that Mac systems are less susceptible to malware:

- Be cautious with links and attachments coming with emails and messages.
- Avoid using pirated and questionable software.
- Keep all software up to date. Regularly update the OS.
- Enforce the use of a VPN and an encrypted connection tunnel while working on the internet.
- Exercise good password hygiene.
- Pay close attention to the files downloaded from the internet.
- Always read the installation terms carefully while installing any third-party applications.
- Add apps only from the Mac App Store and identified developers. Be careful while permitting third-party extensions and packages to run on the device.
- Adopting a UEM solution is a cutting-edge technique to fight malware. Organizations can create a list of safe applications that are allowed to run on

employee devices and enforce encryption and other security practices using UEM policies, which acts as an extra layer for the security outfit.
- Be cautious of websites urging you to take any actions or payments.
- Avoid sharing any sensitive information online.
- Be cautious of any odd details in emails, popups, and messages. Pay attention to oddly spelled email addresses.

If the system is found infected with macOS malware:

- Immediately back up vital files and remove the physical drive to which the data is backed up.
- Disconnect the infected device from the network by turning off Wi-Fi and ethernet.
- Wipe the OS and reinstall.