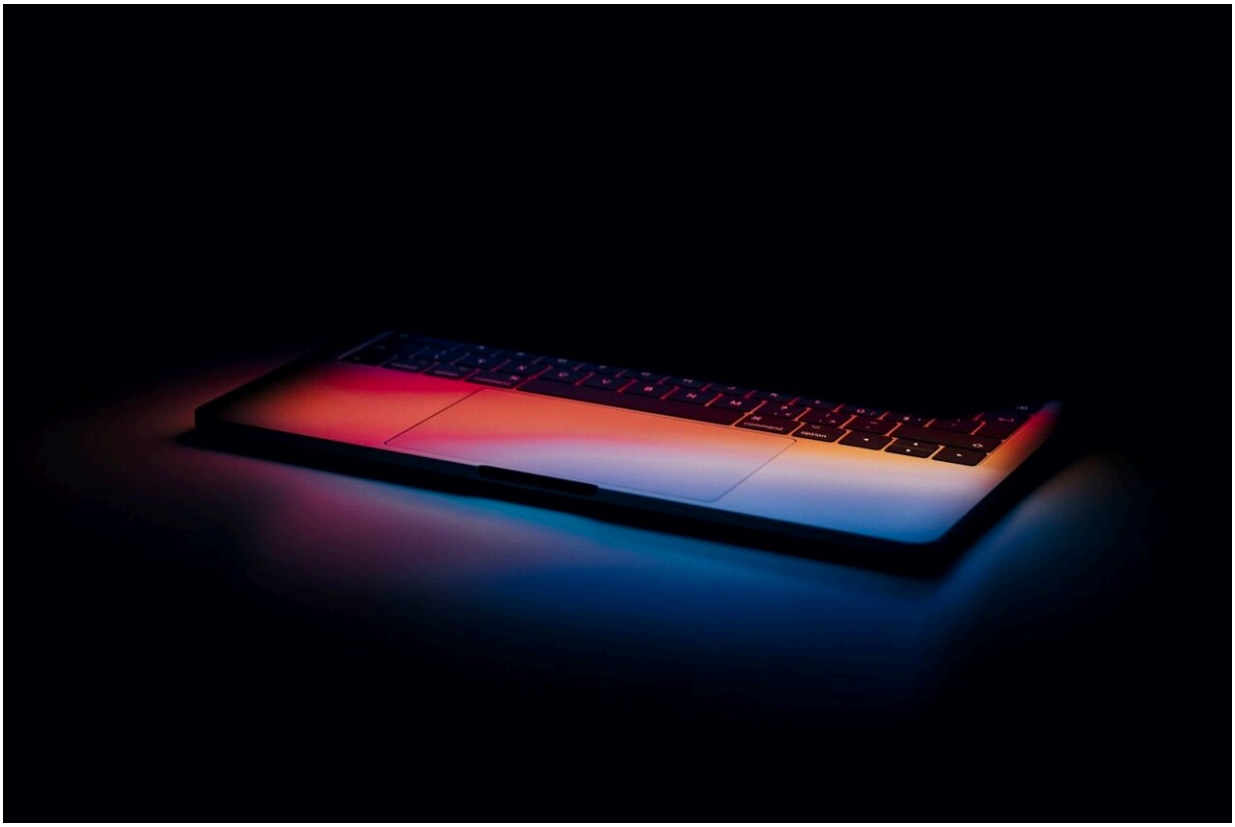
Hackers use a bug to evade macOS defenses

April 27 2021, by Sarah Katz



MacOS keyboard. Credit: Unsplash.com

Lauded for years as the system able to best prevent malware infection, macOS recently fell victim to an operating system vulnerability that hackers used to circumvent all of Apple's system defenses.

Security researcher Cedric Owens discovered this bug in March 2021

while assessing Apple's Gatekeeper mechanism, a safeguard that will only allow developers to run their software on Macs after registering with Apple and paying a fee. Moreover, the company requires that all applications undergo an automated vetting process to further protect against malicious software.

Unfortunately, Owens uncovered a logic flaw in the macOS itself, rather than the defense systems. The bug allowed attackers to develop malware able to deceive the operating system into running their malware regardless of whether they passed Apple's safety checks. Indeed, this flaw resembles a door that has been securely locked and bolted but still has a small pet door at the bottom through which you can break in or insert a bomb.

Owens found that the bug worked by exploiting Apple's assumption regarding all applications allegedly including a standard metadata file called "info.plist." He soon realized he could easily craft malware that ran as a simple script, thus avoiding the multiple layers that trigger Apple's Gatekeeper and enabling evil software to fly under the radar. In fact, he discovered that this evil code could run so stealthily that macOS wouldn't even prompt the user for permission to download the app from the Internet.

Further analysis showed that macOS does run a check to see whether the new application is notarized. However, if the system finds that the software bundle doesn't include an "info.plist" file, the software passes the checkpoint. Once the researchers had confirmed the bug with Apple, they learned that the Apple-focused device management firm Jamf had, in fact, detected script-based malware that fit the criteria of this threat, soon finding that a version of Shlayer adware had already actively exploited the vulnerability.

With the introduction of Gatekeeper in February 2020, cybercriminals

have faced a significant obstacle due to the massive decrease in at-risk users, thanks to Apple's enhanced defenses. However, groups like the attackers who developed Shlayer have had some luck tricking Apple into notarizing their malware. Using this method, hackers don't even have to worry about macOS notifying users of a new application in the first place.

In response, Apple has patched the bug in the macOS Big Sur 11.3 version. Additionally, the company has upgraded its XProtect system monitoring tool to identify and notify users regarding any software potentially trying to exploit this flaw.

More information: macOS Gatekeeper Bypass (2021 Edition): cedowens.medium.com/macos-gate … edition-5256a2955508

About the security content of macOS Big Sur 11.3: support.apple.com/en-us/HT212325