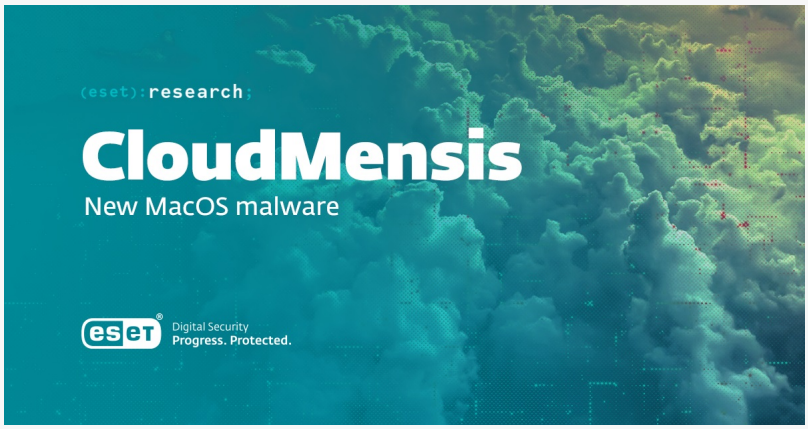
ESET Research discovers new threat to Mac users: CloudMensis spies on them in targeted operation



DUBAI, UNITED ARAB EMIRATES, July 20, 2022 /EINPresswire.com/ -- ESET researchers discovered a previously unknown macOS backdoor that spies on users of compromised Macs and exclusively uses public cloud storage services to communicate back and forth with its operators. Named CloudMensis by ESET, its capabilities clearly show that the intent of the operators is to gather information from the victims' Macs by exfiltrating documents and keystrokes, listing email messages and attachments, listing files from removable storage, and screen captures.

CloudMensis is a threat to Mac users, but its very limited distribution suggests that it is used as part of a targeted operation. From what ESET Research has seen, operators of this malware family deploy CloudMensis to specific targets that are of interest to them. The use of vulnerabilities to work around macOS mitigations shows that the malware operators are actively trying to maximize the success of their spying operations. At the same time, no undisclosed vulnerabilities (zero days) were found to be used by this group during our research. Thus, running an up-to-date Mac is recommended to avoid, at least, the mitigation bypasses.

"We still do not know how CloudMensis is initially distributed and who the targets are. The general quality of the code and lack of obfuscation shows the authors may not be very familiar with Mac development and are not so advanced. Nonetheless, a lot of resources were put into making CloudMensis a powerful spying tool and a menace to potential targets," explains ESET researcher Marc-Etienne Léveillé, who analyzed CloudMensis.

Once CloudMensis gains code execution and administrative privileges, it runs a first-stage malware that retrieves a more featureful second stage from a cloud storage service.

This second stage is a much larger component, packed with a number of features to collect

information from the compromised Mac. The intention of the attackers here is clearly to exfiltrate documents, screenshots, email attachments, and other sensitive data. Altogether, there are 39 commands currently available.

CloudMensis uses cloud storage both for receiving commands from its operators and for exfiltrating files. It supports three different providers: pCloud, Yandex Disk, and Dropbox. The configuration included in the analyzed sample contains authentication tokens for pCloud and Yandex Disk.

Metadata from the cloud storage services used reveal interesting details about the operation, for example that it started to transmit commands to the bots as of February 4, 2022.

Apple has recently acknowledged the presence of spyware targeting users of its products and is previewing Lockdown Mode on iOS, iPadOS, and macOS, which disables features frequently exploited to gain code execution and deploy malware.

For more technical information about CloudMensis, check out the blogpost “I see what you did there: a look at the CloudMensis macOS spyware” on WeLiveSecurity. Make sure to follow ESET Research on Twitter for the latest news from ESET Research.

About ESET
For more than 30 years, ESET® has been developing industry-leading IT security software and services to protect businesses, critical infrastructure, and consumers worldwide from increasingly sophisticated digital threats. From endpoint and mobile security to endpoint detection and response, as well as encryption and multifactor authentication, ESET’s high-performing, easy-to-use solutions unobtrusively protect and monitor 24/7, updating defenses in real time to keep users safe and businesses running without interruption. Evolving threats require an evolving IT security company that enables the safe use of technology. This is backed by ESET’s R&D centers worldwide, working in support of our shared future. For more information, visit www.eset.com or follow us on LinkedIn, Facebook, and Twitter.

Sanjeev Kant
Vistar Communications
+971 55 972 4623
email us here