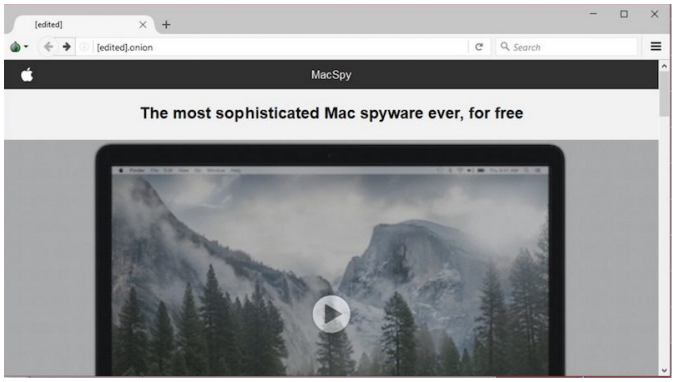
Security news site Bleeping Computer discovers a pair of Mac malware strains on the Dark Web-- a piece of spyware dubbed MacSpy and MacRansom, an example of Mac ransomware.



The two pieces of malware are the work of the same developer (or cybercriminal group), and are found on almost identical Dark Web portals. Both websites run on a "closed" manner, meaning interested parties have to contact the malware creator for demo packages and the price negotiations.

Following the initial Bleeping Computer report, security researchers at Fortinet and AlienVault managed to get samples of the Mac malware. The two companies believe MacSpy and MacRansom are the work of an inexperienced coder, since MacRansom is not a digitally signed file (meaning it triggers security alerts if executed as a standard macOS installation) and MacSpy is built from code copy-pasted from Stack Overflow.

That said, MacRansom appears to be the more dangerous of the two malware, since it can permanently wreck user files if deployed in live campaigns. However none of the two appear to be currently in active use, probably since getting the ransomware involves a lengthy email back-to-forth with the creator, defeating the purpose of "malware-as-a-service."

Either way, it is clear malware is an increasingly pressing issue with Apple products-- as the number of Macs grow, so will malware targeting Macs and iDevices. Bleeping Computer even has reports of a developer working on a cross-OS ransomware, and as such moving forward customers have to be more cautious than ever.

Go MacRansom and MacSpy Malware-as-a-Service Portals Put Mac Users on Alert (Bleeping Computer)

Go MacRansom: Offered as Ransomware as a Service

Go MacSpy: OS X RAT as a Service