LockBit Ransomware Group Developing Malware to Encrypt Files on macOS

The notorious LockBit ransomware group is apparently developing a piece of malware that can encrypt files on devices running Apple's macOS operating system. Researchers have analyzed the malware to determine how much of a threat it actually poses.

MalwareHunterTeam reported on Sunday that they had come across what appeared to be the first macOS malware sample developed by a major ransomware group.

Shortly after, Vx-Underground, which collects malware samples, found evidence that the malware has been around since at least November 2022.

The malware appears to be real and, when the first sample was discovered, none of the antimalware engines on VirusTotal were detecting it.

Apple security expert Patrick Wardle has conducted an analysis of the macOS version of LockBit and found that while it can run on Macs and it is capable of encrypting files, it currently doesn't pose any real risk.

First of all, the analyzed malware sample was signed, but not with a trusted certificate, which means macOS prevents it from running. Wardle also pointed out that even if such ransomware finds a way to run on a macOS device, file system protections implemented by Apple, such as TCC (Transparency, Consent, and Control), are likely to significantly limit its impact.

The researcher also found that the malware has bugs that can cause it to suddenly terminate when running on macOS.

During his analysis, Wardle found strings suggesting that at least some of the malware code was taken from a version designed to target Windows systems. There is also indication that much of it is Linux code that was recompiled for macOS.

“While this may be the first time a large ransomware group created ransomware capable of running on macOS, it’s worth noting that this sample is far from ready for prime time. From its lack of a valid code-signing signature to its ignorance of TCC and other macOS file-system protections as it stands it poses no threat to macOS users,” Wardle said.

Emsisoft threat analyst Brett Callow pointed out that there is no evidence the malware has been deployed in the wild. “It is, however, an indication that LockBit is, or at least was, thinking about Macs,” Callow noted.

Related: Microsoft Flags Ransomware Problems on Apple’s macOS Platform

Related: User Documents Overwritten With Malicious Code in Recent Dridex Attacks on macOS

LockBit Ransomware Group Developing Malware to Encrypt Files on macOS