LockBit ransomware encryptors found targeting Mac devices

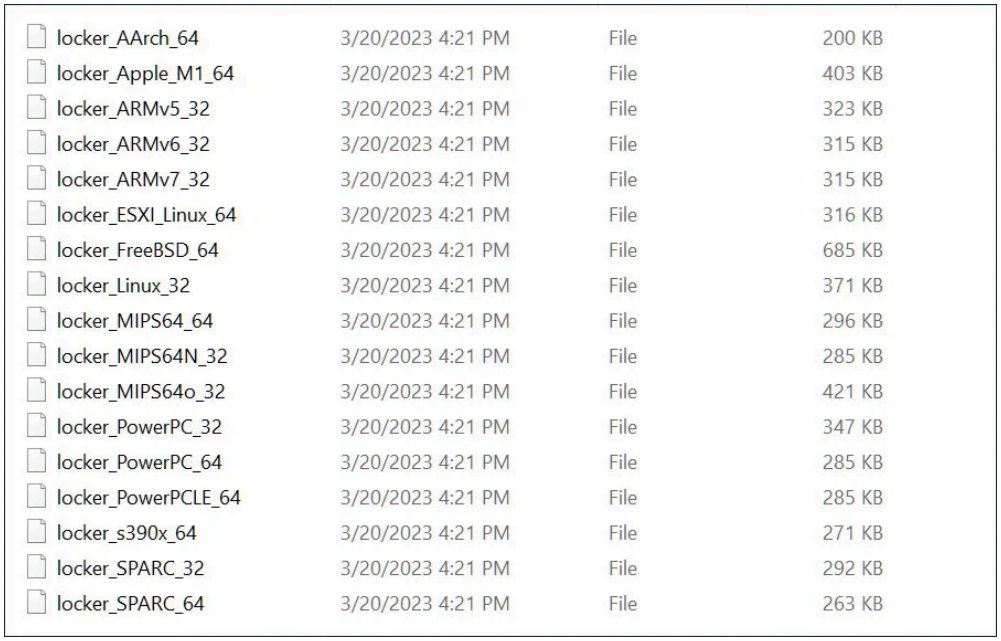
By Lawrence Abrams

Published: 2023-04-16 · Archived: 2026-04-05 15:32:41 UTC

The LockBit ransomware gang has created encryptors targeting Macs for the first time, likely becoming the first major ransomware operation to ever specifically target macOS.

The new ransomware encryptors were discovered by cybersecurity researcher MalwareHunterTeam who found a ZIP archive on VirusTotal that contained what appears to be most of the available LockBit encryptors.

Historically, the LockBit operation uses encryptors designed for attacks on Windows, Linux, and VMware ESXi servers. However, as shown below, this archive [VirusTotal] also contained previously unknown encryptors for macOS, ARM, FreeBSD, MIPS, and SPARC CPUs.

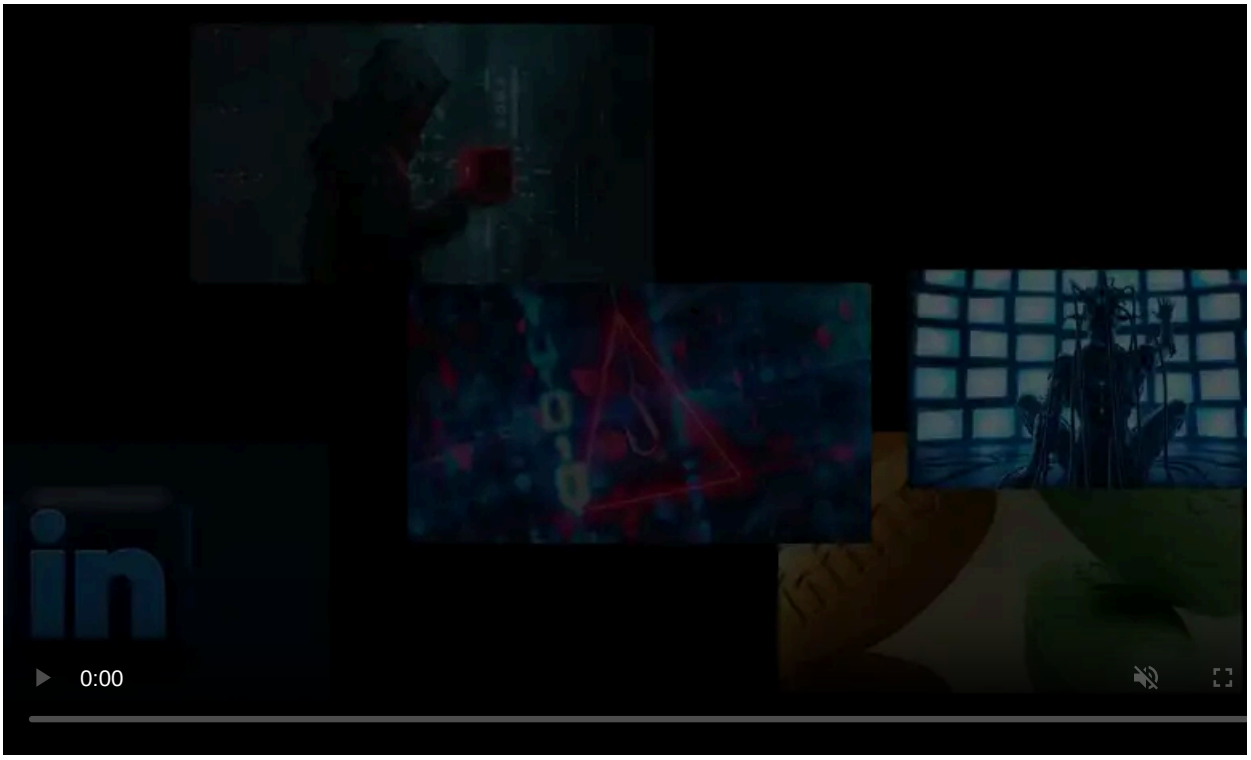


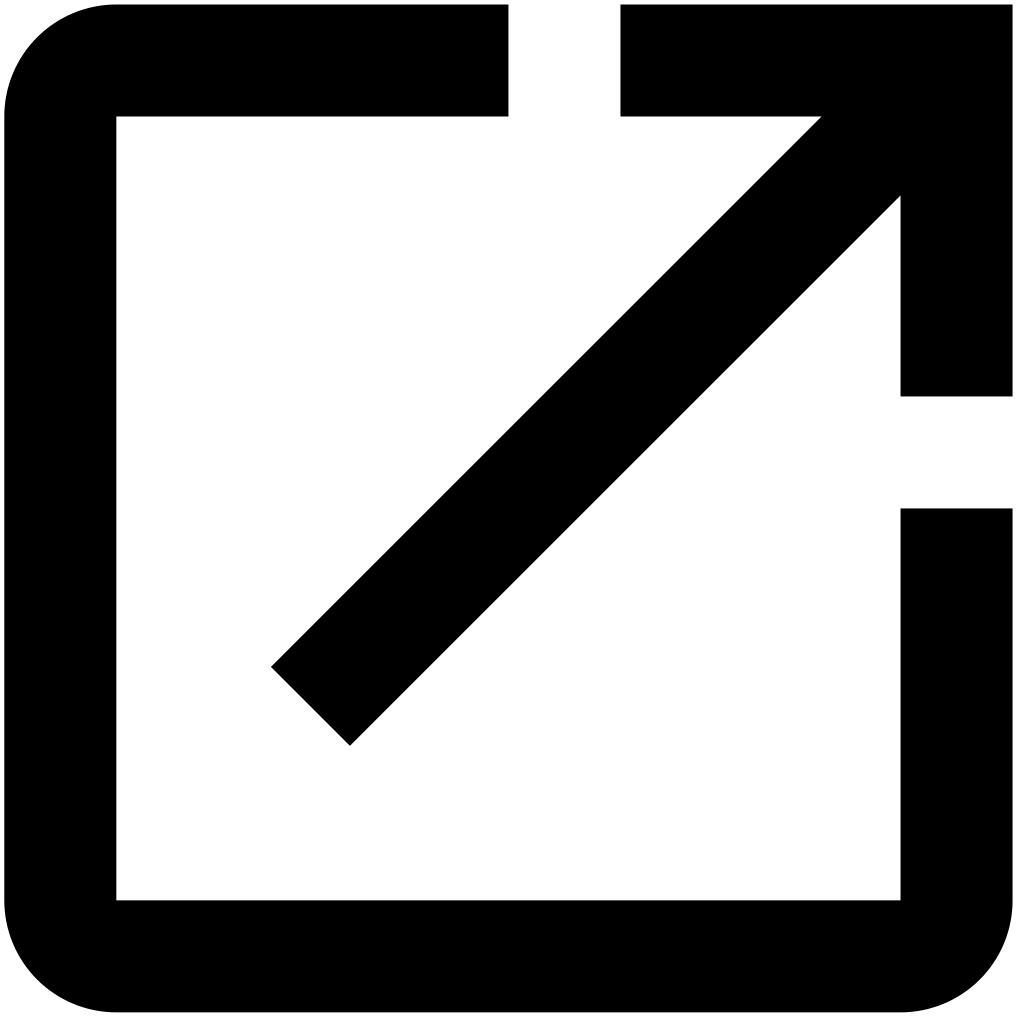
locker_AArch_64	3/20/2023 4:21 PM	File	200 KB
locker_Apple_M1_64	3/20/2023 4:21 PM	File	403 KB
locker_ARMv5_32	3/20/2023 4:21 PM	File	323 KB
locker_ARMv6_32	3/20/2023 4:21 PM	File	315 KB
locker_ARMv7_32	3/20/2023 4:21 PM	File	315 KB
locker_ESXI_Linux_64	3/20/2023 4:21 PM	File	316 KB
locker_FreeBSD_64	3/20/2023 4:21 PM	File	685 KB
locker_Linux_32	3/20/2023 4:21 PM	File	371 KB
locker_MIPS64_64	3/20/2023 4:21 PM	File	296 KB
locker_MIPS64N_32	3/20/2023 4:21 PM	File	285 KB
locker_MIPS64o_32	3/20/2023 4:21 PM	File	421 KB
locker_PowerPC_32	3/20/2023 4:21 PM	File	347 KB
locker_PowerPC_64	3/20/2023 4:21 PM	File	285 KB
locker_PowerPCLE_64	3/20/2023 4:21 PM	File	285 KB
locker_s390x_64	3/20/2023 4:21 PM	File	271 KB
locker_SPARC_32	3/20/2023 4:21 PM	File	292 KB
locker_SPARC_64	3/20/2023 4:21 PM	File	263 KB

Archive of available LockBit encryptors

Source: BleepingComputer

These encryptors also include one named 'locker_Apple_M1_64' [VirusTotal] that targets the newer Macs running on Apple Silicon. The archive also contains lockers for PowerPC CPUs, which older Macs use.


0:00



Further research by cybersecurity researcher Florian Roth found an Apple M1 encryptor uploaded to VirusTotal in December 2022, indicating that these samples have been floating around for some time.

Likely test builds

BleepingComputer analyzed the strings in the LockBit encryptor for Apple M1 and found strings that are out of place in a macOS encryptor, indicating that these were likely haphazardly thrown together in a test.

For example, there are numerous references to VMware ESXi, which is out of place in an Apple M1 encryptor, as VMare announced they would not be supporting the CPU architecture.

```
 _check_esxi
esxi_
_Esxi
_kill_esxi_1
_kill_esxi_2
_kill_esxi_3
_kill_processes
_kill_processes_Esxi
_killed_force_vm_id
_listvms
_esxcfg_scsidevs1
_esxcfg_scsidevs2
_esxcfg_scsidevs3
_esxi_disable
_esxi_enable
```

Furthermore, the encryptor contains a list of sixty-five file extensions and filenames that will be excluded from encryption, all of them being Windows file extensions and folders.

A small snippet of the Windows files the Apple M1 encryptor will not encrypt is listed below, all out of place on a macOS device.

```
 .exe
.bat
.dll
msstyles
gadget
winmd
ntldr
ntuser.dat.log
bootsect.bak
autorun.inf
thumbs.db
iconcache.db
```

Almost all of the ESXi and Windows strings are also present in the MIPs and FreeBSD encryptors, indicating that they use a shared codebase.

The good news is that these encryptors are likely not ready for deployment in actual attacks against macOS devices.

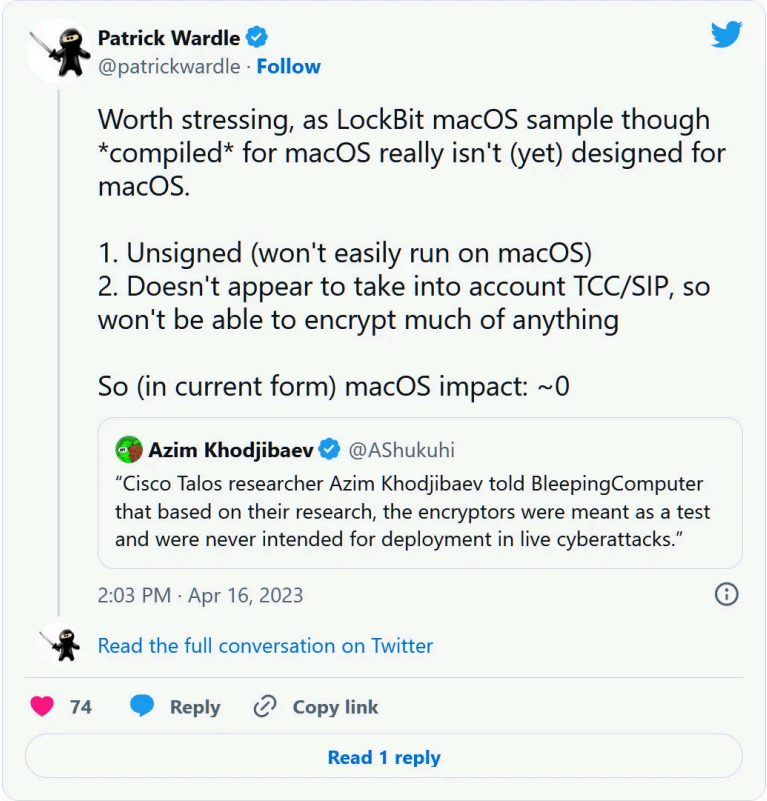
Cisco Talos researcher Azim Khodjibaev told BleepingComputer that based on their research, the encryptors were meant as a test and were never intended for deployment in live cyberattacks.

macOS cybersecurity expert Patrick Wardle further confirmed BleepingComputer's and Cisco's theory that these are in-development/test builds, stating that the encryptor is far from complete as it is missing the required functionality to encrypt

Macs properly.

Instead, Wardle told BleepingComputer that he believes the macOS encryptor is based on the Linux version and compiled for macOS with some basic configuration settings.

Furthermore, Wardle told us that when the macOS encryptor is launched, it crashes due to a buffer overflow bug in its code.



"It seems that macOS is now on their radar ... but other than compiling it for macOS, and adding a basic config (which are just basic flags ...not specific to macOS per se) this is far from ready for deployment," Wardle told BleepingComputer.

Wardle further shared that the LockBit developer must first "figure out how to bypass TCC, get notarized" before becoming a functional encryptor.

A detailed technical analysis conducted by Wardle on the new Mac encryptor can be found on Objective See.

While Windows has been the most targeted operating system in ransomware attacks, nothing prevents developers from creating ransomware that targets Macs.

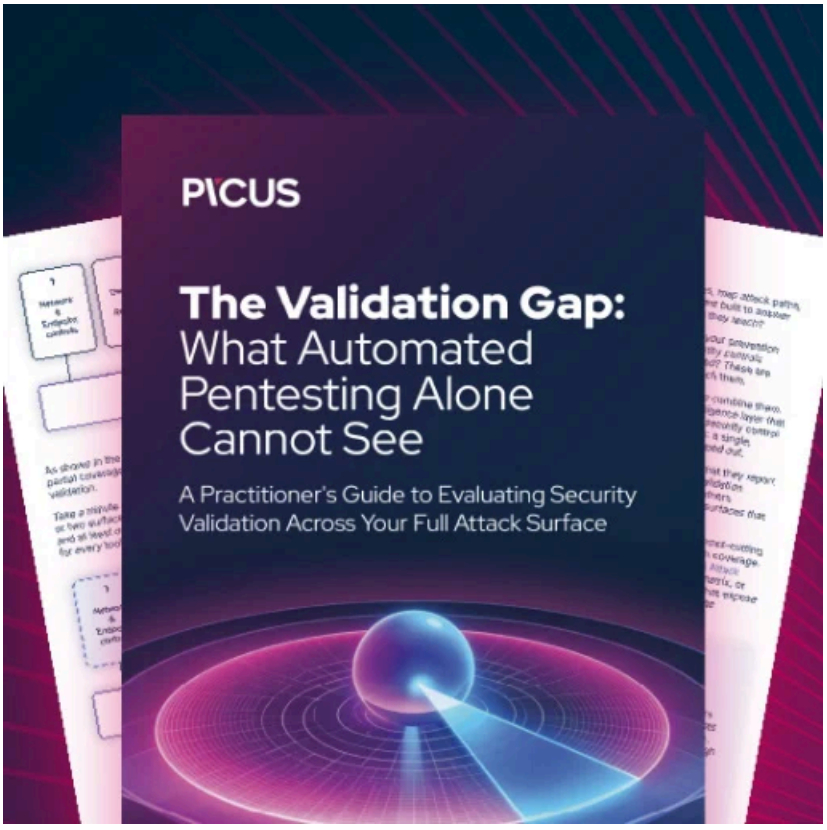
However, as the LockBit operation is known for pushing the envelope in ransomware development, it would not be surprising to see more advanced and optimized encryptors for these CPU architectures released in the future.

Therefore, all computer users, including Mac owners, should practice good online safety habits, including keeping the operating system updated, avoiding opening unknown attachments and executables, generate offline backups, and using strong and unique passwords at every site you visit.

Update 4/16/23: In response to questions from BleepingComputer, the public-facing representative of LockBit, known as LockBitSupp, said that the Mac encryptor is "actively being developed."

While LockBit has a history of toying with security researchers and the media, if true, we will likely see more production-quality versions in the future.

Furthermore, while it's not clear how useful a macOS encryptor would be in the enterprise, some LockBit affiliates target consumers and small businesses, where an encryptor like this could be more useful.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-encryptors-found-targeting-mac-devices/