Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

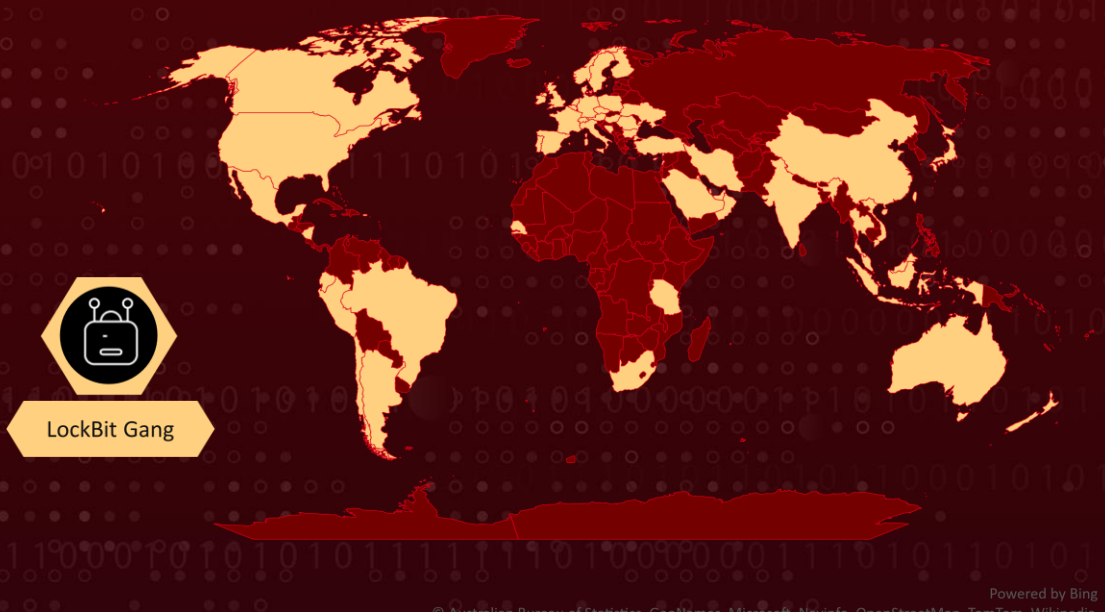
LockBit Ransomware Targets MacOS

Date of Publication	Admiralty Code	TA Number
April 19, 2023	A1	TA2023193

Summary

Attack began: November 2022
Threat Actor: LockBit Gang
Malware: LockBit Ransomware
Affected OS: macOS
Attack Countries: Argentina, Australia, Austria, Bahrain, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Canada, Cayman Islands, Chile, China, Cyprus, Czech Republic, Denmark, Ecuador, Finland, France, Germany, Hong Kong, Hungary, India, Indonesia, Iran, Ireland, Isle of Man, Italy, Japan, Kuwait, Lebanon, Malaysia, Mauritius, Mexico, Netherlands, New Zealand, Nicaragua, Norway, Oman, Peru, Poland, Portugal, Puerto Rico, Qatar, Romania, Saudi Arabia, Senegal, Singapore, South Africa, Spain, Sweden, Switzerland, Taiwan, Tanzania, Thailand, Turkey, United Arab Emirates, United Kingdom, United States, Vietnam, Ukraine
Attack Industry: Automotive, Aviation, Biotechnology, Chemicals, Construction & Engineering, Consumer, Defense, Distributors, Education, Electrical, Energy, Family Services, Financial, Food Products, Healthcare, Hotels, Insurance, IT, Machinery, Marine, Media, Metals & Mining, Oil and Gas, Pharmaceuticals, Professional Services, Real Estate, Retail, Telecommunication, Transportation, Utilities
Attack: LockBit ransomware, known as the oldest ransomware affiliate program, has been discovered on VirusTotal compiled for Apple's macOS arm64 architecture, raising concerns about the ransomware threat on Mac devices.

Attack Regions



Attack Details

#1 On April 16th, a sample of LockBit ransomware was discovered on VirusTotal compiled for Apple's macOS arm64 architecture. LockBit claims to be the oldest ransomware affiliate program, and news that one of the major cybercrime outfits in the ransomware landscape was targeting macOS devices has raised concerns about the ransomware threat on Mac devices. While no occurrences of LockBit for Mac have yet been reported in the wild, early claims that the sample was non-functional were incorrect. The ransomware functions as intended to encrypt targeted files, which are subsequently appended with the .lockbit extension.

#2 However, the Mac sample does not appear to implement any functionality for exfiltrating the data it locks, nor does it have any method of persistence. These are clear signs that this is a work in progress and not a genuine payload intended for use in the wild. It is important to note that there is no publicly recorded case of any business ever paying a ransom demand as a result of macOS ransomware.

Recommendations

- Ensure that your Mac is updated with the latest security patches and software updates, as vulnerabilities in software can be exploited by attackers. Use a reputable anti-virus software that includes ransomware protection and regularly scan your Mac for malware.
- Backup your important files regularly to an external hard drive or cloud storage, so that you can restore them in case of a ransomware attack. Block the indicators of compromise related to the attack campaign.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion	TA0011 Command and Control
TA0009 Collection	TA0040 Impact	T1486 Data Encrypted for Impact	T1059 Command and Scripting Interpreter
T1195 Supply Chain Compromise	T1553 Subvert Trust Controls	T1553.002 Code Signing	T1566 Phishing
T1566.001 Spearphishing Attachment	T1219 Remote Access Software	T1560 Archive Collected Data	T1027 Obfuscated Files or Information
T1204 User Execution			

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	2d15286d25f0e0938823dcd742bc928e78199b3d, 864f56b25a34e9532a1175d469715d2f61c56f7f, ef958f3cf201f9323ceae9663d86464021f8e10d

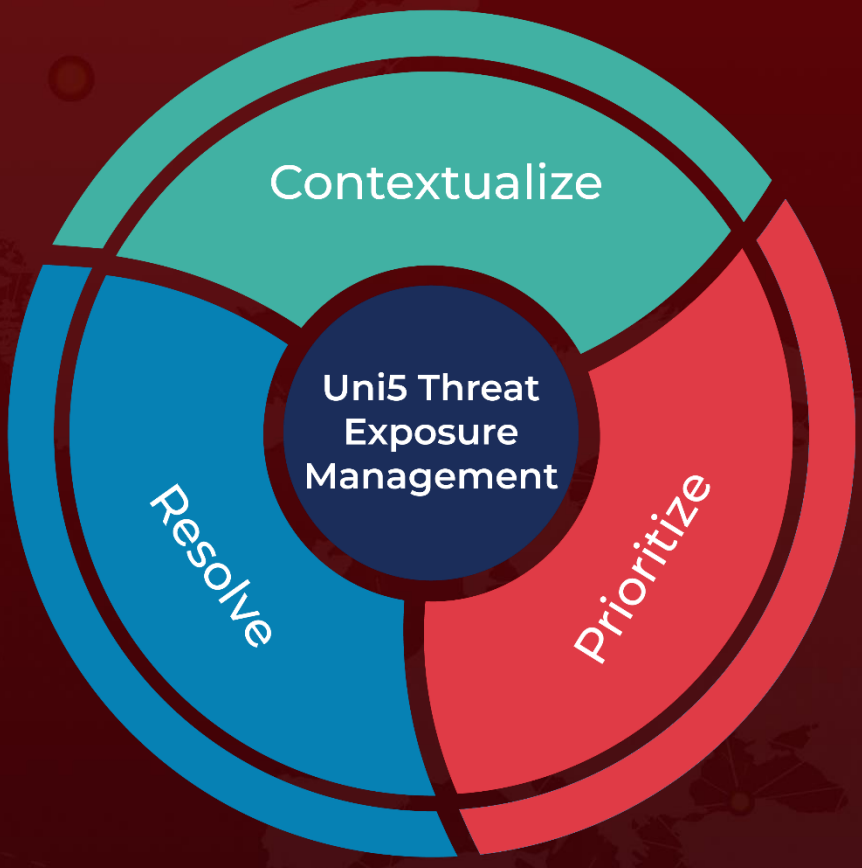
References

https://www.sentinelone.com/blog/lockbit-for-mac-how-real-is-the-risk-of-macos-ransomware/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 19, 2023 • 12:30 AM

More at www.hivepro.com