MINERVA

Ransomware Protection for Apple macOS

Given the financial motivation of most ransomware attacks, adversaries that develop ransomware are always looking for new money-making opportunities. So far, the majority of ransomware attacks have been targeting Windows users, due in part to the popularity of this OS. As the security architecture of Windows is continuing to mature, the attackers are looking to expand their reach to other operating systems, including macOS.

The Turn of the Mac

Adversaries have recognized that Apple macOS systems present a new lucrative market and revenue stream. They know that macOS systems hold sensitive files and often lack the sophisticated security controls that enterprises have had to deploy to Windows endpoints. Malicious activity trends indicate strong growth in the amount malware designed to run on macOS. For example, AV-TEST reported[1] an almost 400% increase in macOS malware in comparison to the previous year, while McAfee reported[2] a 7-fold increase in such occurrences. Not surprisingly, ransomware is among the types of malicious software finding its way onto macOS systems. Some examples of macOS ransomware include Filecoder and KeRanger.

It's a New Cat and Mouse Race

Antivirus products that form the baseline protection against macOS malware already exist. However, their efficacy against macOS ransomware is yet uncertain, in part because macOS is a relatively new and immature battlefield for malware. Minerva augments this protection by providing a critical safety net for potential ransomware incidents on macOS.

1: https://www.av-test.org/en/news/news-single-view/the-it-security-status-at-a-glance-the-av-test-security-report-20162017/
2: https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf

MINERVA

Your Data is Safe with Us

Minerva's Anti-Evasion Platform drastically lowers the risk associated with the threat of ransomware for macOS in enterprises. Our Ransomware Protection capability for macOS prevents the damage caused by destructive malware. Organizations can restore the encrypted files without relying on backup capabilities that can easily be disabled by the ransomware or might not even be enabled in the first place.

Never Pay the Ransom. Never Lose your Data

Minerva's Ransomware Protection for macOS ensures that just before the ransomware executes its mission to encrypt the data, a copy of the targeted file is automatically saved without any user involvement. Once users receive the ransomware note, they have the ability to easily restore the encrypted data, eliminating the need to pay the ransom.

Single Management Console for macOS and Windows

Through the Minerva Management Console, organizations can centrally manage the Minerva's agents on both Windows and macOS endpoints. Minerva Ransomware Protection uses a super-thin agent that requires no ongoing care and feeding to operate effectively.

Prevention Before Detection

Early detection tools are only good enough when you don't have a better solution. Minerva's patented solution prevents ransomware before detection, with no human intervention, eliminating the need to pay ransom while increasing the efficiency of your security team and tools.
This allows security professionals to mitigate on their own time, confident that the malware poses no threat, and to stop chasing after false-positive alerts, as there will only be an alert in a true event of unknown malware prevention.