Severity

High

Analysis Summary

Virlock is a file-infecting ransomware that was initially found in 2014 but reappeared in 2016 and 2017. Virlock revealed new abilities with each reappearance, showing that the threat actors are continually developing and updating the malware. It showed unique capabilities in 2016 that allowed it to expand through shared apps and cloud storage. During the initial stage of its attack, this ransomware drops three instances of itself, each with its own obfuscation and persistence techniques. By altering the functionality implemented by each instance, Virlock ensures that all three instances can evade a signature-based detection system. Virlock, like other ransomware, demands payment in Bitcoin from the victim in order to decrypt their machines.

Impact

- File Encryption

Indicators of Compromise

MD5

- 1c6b48545088dfb3829a3dd32b088964

SHA-256

- 1557867b4136ba567bcdf1624000e87df3fb4fac794f84bac296efabe17a9b8f

SHA-1

- 61a77948ccab1e6a86d15742d2d277def7890f0c

Remediation

- Never open attachments or links received by unknown senders.
- Look for IOCs in your surroundings.
- At your respective controls, disable all threat indicators.