Severity

High

Analysis Summary

Phobos ransomware appeared at the beginning of 2019. It has been noted that this new strain of ransomware is strongly based on the previously known family: Dharma (a.k.a. Crysis), and probably distributed by the same group as Dharma. Phobos is one of the ransomware that is distributed via hacked Remote Desktop (RDP) connections. This isn't surprising, as hacked RDP servers are a cheap commodity on the underground market, and can make for an attractive and cost-efficient dissemination vector for threat groups. This ransomware does not deploy any techniques of UAC bypass. When we try to run it manually, the UAC confirmation pops up:

Impact

- File Encryption
- Data Exfiltration

Indicators of Compromise

MD5

- ab483b1bed135021a5c19725635a465f

SHA-256

- 82035c9ff5f0f3f2d3c75522e6773a46ebece35f9c15ad3f6c3c745b343dd8a6

SHA1

- b7654fa002a3f39bf06d85c100c349216092f641

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.