Issued 11/16/17

New Ransomware Attacks: LockCrypt Emerges From Satan's Shadow

Ransomware attacks are getting worse. New variants such as LockCrypt are now targeting unsecured enterprise servers with solid encryption and advanced obfuscation techniques. They are demanding between $3,500 and $7,000 per device for decryption keys, paid in bitcoin.

LockCrypt got its start under the umbrella of the Satan ransomware-as-a-service (RaaS), which lets would-be attackers piggyback on existing malware code to infect corporate systems. As noted by ZDNet, the Satan HTML file uses RSA-2048 and AES-256 cryptography, making it difficult — if not impossible — for victims to recover files unless they're willing to pay. Early versions of LockCrypt used email addresses associated with the Satan RaaS, but more recent attacks have ditched Satan infection vectors in favor of brute-force remote desktop protocol (RDP) attacks that compromise unsecured enterprise servers and then move laterally to as many devices as possible. While initial versions of LockCrypt weren't particularly complex, current attack vectors come with a number of features that make it a threat worth watching. First, the ransomware leverages strong encryption to prevent users and security firms from finding simple workarounds.

LockCrypt also gains boot persistence and deletes shadow volume copies, hampering the ability of users to remove infected code. Last but not least?

It kills all non-Windows core processes, effectively curtailing the ability of antivirus or antimalware tools to detect and eliminate the ransomware.