Severity

High

Analysis Summary

LockBit ransomware takes as little as five minutes to deploy the encryption routine on target systems once it lands on the victim network. LockBit attacks leave few traces for forensic analysis as the malware loads into the system memory, with logs and supporting files removed upon execution. In one case, they found that the attack began from a compromised Internet Information Server that launched a remote PowerShell script calling another script embedded in a remote Google Sheets document. This script connects to a command and control server to retrieve and install a PowerShell module for adding a backdoor and establish persistence. To evade monitoring and go unnoticed in the logs, the attacker renamed copies of PowerShell and the binary for running Microsoft HTML Applications (mshta.exe); this prompted Sophos to call this a “PS Rename“ attack. The backdoor is responsible for installing attack modules and executes a VBScript that downloads and executes a second backdoor on systems restart.

Impact

- Security Bypass
- Information Theft
- Files Encryption

Indicators of Compromise

MD5

- f35168aa5f285fc531b2a4858058537c

SHA-256

- f978a39f80fe81be9f9f98b00adf88a8b7300bd5d311597d00daa47da3676369

SHA-1

- 6035899426113a4584c6e4563c70d099e1d81d88

Remediation

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