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

- 931979a25c286c3d0c83fa6481d4f9f0

SHA-256

- 7cc0c4d1f3bc3c5e486077bd69c1aeedba27a085c5e6f67d7309f2aa79a0e5b9

SHA-1

- 4d043df23e55088bfc04c14dfb9ddb329a703cc1

Remediation

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