LockBit ransomware moves quietly on the network, strikes fast

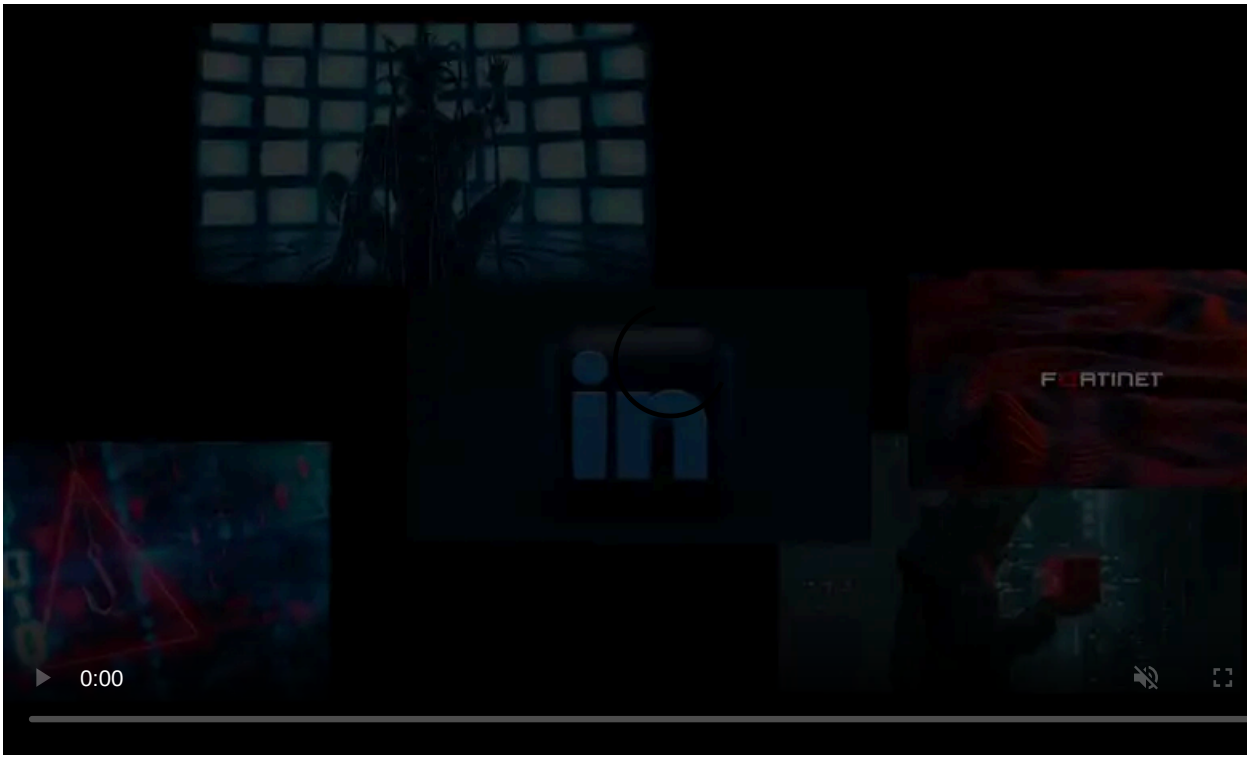
By Ionut Ilascu

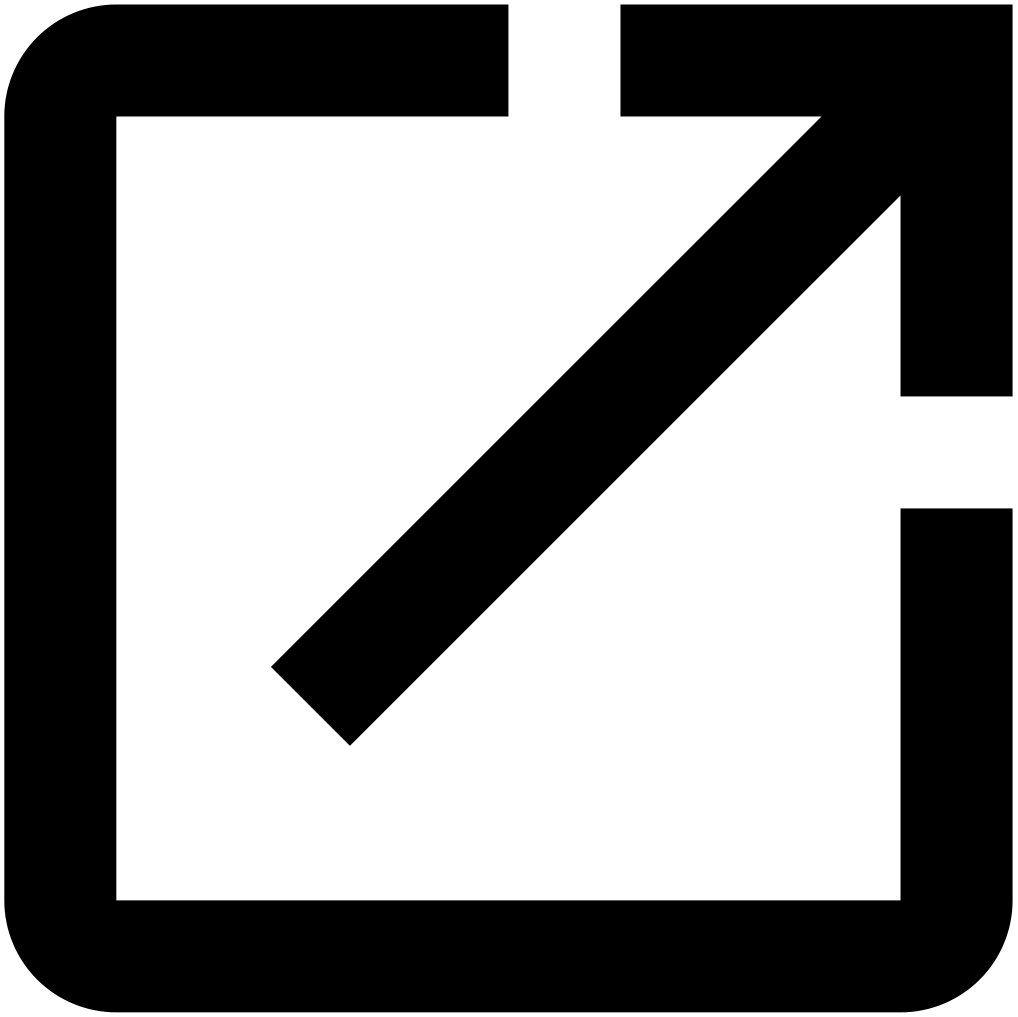
Published: 2020-10-21 · Archived: 2026-04-05 19:43:11 UTC

LockBit ransomware takes as little as five minutes to deploy the encryption routine on target systems once it lands on the victim network.

Joining the ransomware-as-a-service (RaaS) business in September 2019, LockBit is atypical in that it's driven by automated processes for quick spreading across the victim network, identifying valuable systems and locking them up.

LockBit attacks leave few traces for forensic analysis as the malware loads into the system memory, with logs and supporting files removed upon execution.

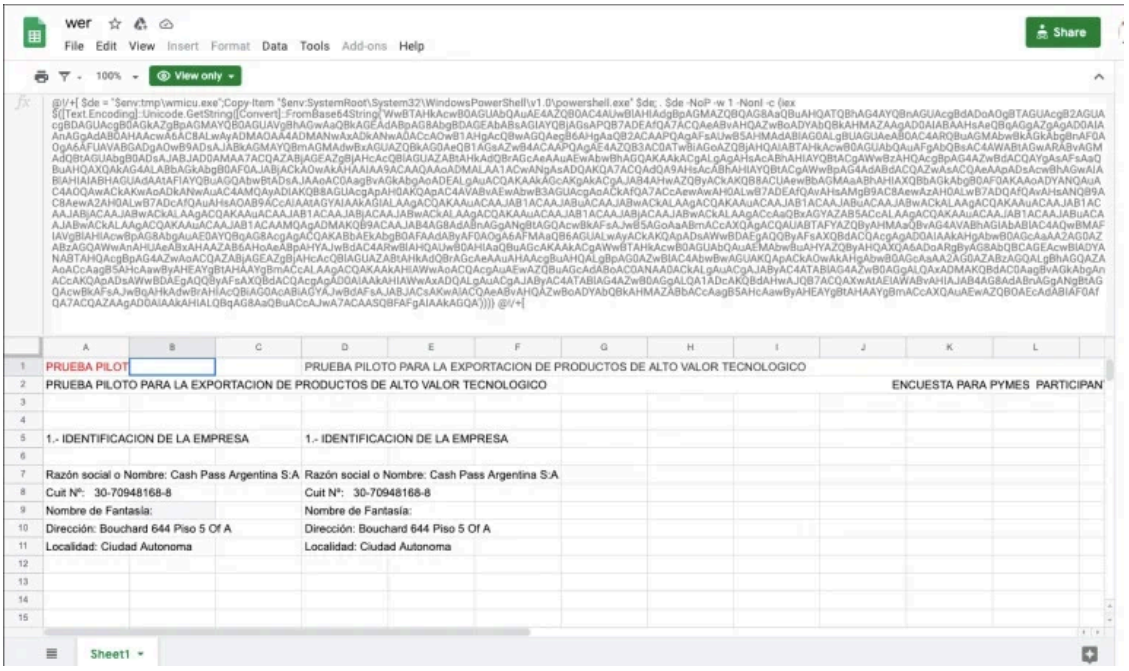

0:00



Scripts and backdoors

After investigating a series of eight incidents at smaller organizations, security researchers at Sophos were able to add more pieces to the puzzle that is LockBit.

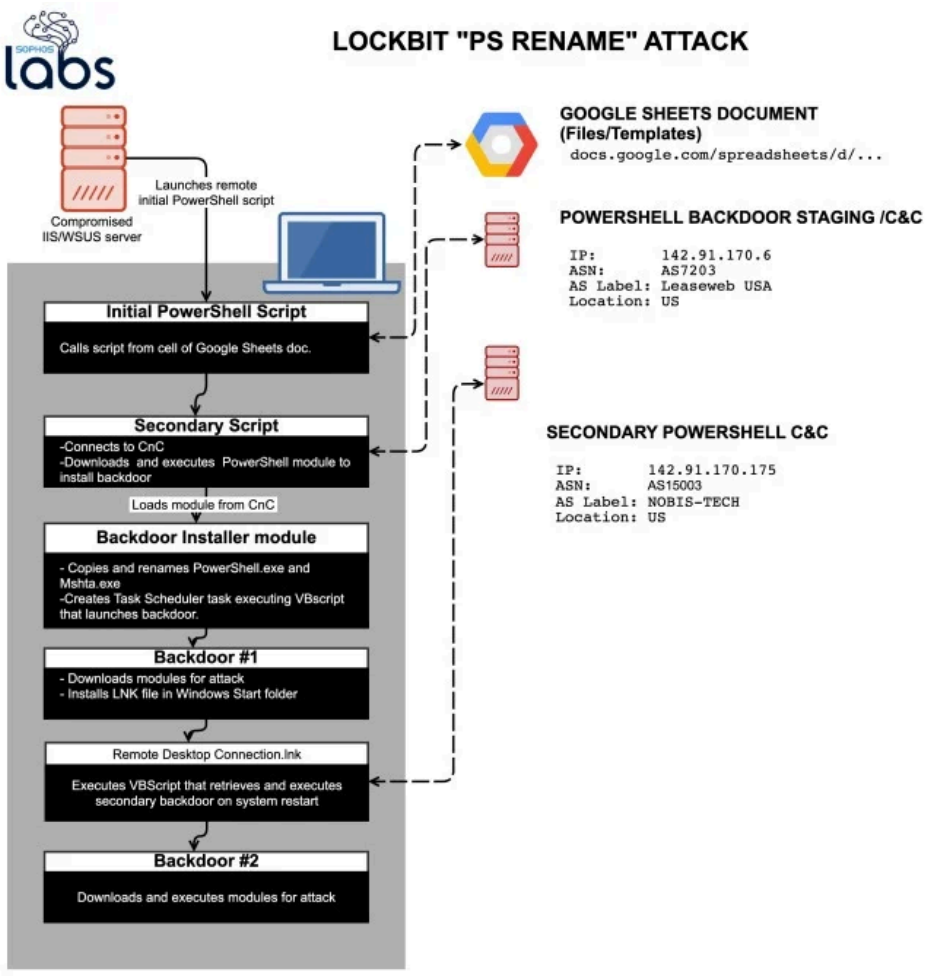
In one case, they found that the attack began from a compromised Internet Information Server that launched a remote PowerShell script calling another script embedded in a remote Google Sheets document.



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. An overview of the attack is available below:



“The attack scripts also attempt to bypass Windows 10’s built-in anti-malware interface [AMSI], directly applying patches to it in memory,” says Sean Gallagher, Senior Threat Researcher at Sophos

Artifacts found on attacked systems suggest the use of scripts based on the PowerShell Empire post-exploitation framework. Their purpose was to collect details about the victim network, identify valuable systems, and check for available defense solutions.

Gallagher says that these scripts also used regular expressions to search Windows Registry for “very specific types of business software” used for point-of-sale systems or accounting.

Below is a list of with keywords of interest included in the search:

Keyword	Target
Opera	Opera browser
Firefox	Mozilla Firefox browser
Chrome	Google Chrome browser
Tax	Search for any tax-related software process
OLT	OLT Pro desktop tax software
LACERTE	Intuit Lacerte tax software for accountants
PROSERIES	Intuit ProSeries tax software
Point of Sale	Search for point-of-sale (retail) software
POS	Search for point-of-sale (retail) software
Virus	Search for anti-malware processes
Defender	Microsoft Windows Defender
Secury	
Anti	Search for anti-malware processes
Comodo	Search for Comodo antivirus or firewall
Kasper	Kaspersky anti-malware software
Protect	Search for anti-malware processes
Firewall	Search for firewall processes

The malicious code would deploy LockBit ransomware only if the targets matched a fingerprint indicating an attractive target, the researcher notes in a report today.

Quick strike

After picking the valuable targets, LockBit ransomware would execute in memory within five minutes using a Windows Management Instrumentation (WMI) command.

“All of the targets were hit within five minutes over WMI. The server-side file used to distribute the ransomware, along with most of the event logs on the targeted systems and the server itself, were wiped in the course of the ransomware deployment” - Sean Gallagher

The researcher says that WMI commands could pass from a server to a system because the attack modules modified firewall rules to allow it.

In these attacks, the initial compromise method remains unknown. In a report from May, McAfee Labs and cybersecurity firm Northwave detail how LockBit ransomware gained access to the victim network by brute-forcing an admin's logins for an outdated VPN service.

In three hours, the malware encrypted about 25 servers and 225 computer systems.

Source: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-moves-quietly-on-the-network-strikes-fast/