WHITEPAPER

DRAGOS
SAFEGUARDING CIVILIZATION

Understanding LockBit 3.0 Ransomware

An Overview of Ransomware Capabilities and How to Respond to the Cyber Threat

STACEY COOK

CONCIERGE SENIOR THREAT ANALYST

MARCH 2023

TABLE OF CONTENTS

Executive Summary

There has been a significant uptick in LockBit ransomware attacks since 2021, impacting organizations closely aligned with critical infrastructure or within the critical infrastructure supply chain. This activity continued through 2022, with trends affecting manufacturing, electric, transportation, and logistics businesses.

LockBit operators capitalize on extortion tactics to increase the probability of the victim paying the ransom. One such tactic is stealing sensitive data, potentially including sensitive industrial control systems (ICS) and operational technology (OT) information, from victim organizations with StealBit, an information stealing tool created by the LockBit developers and typically deployed before LockBit encrypts compromised systems. If the victim doesn't pay the ransom, the stolen data is posted to the LockBit dark web resources (DWRs), which other adversaries can use for various reasons. Sensitive OT information in the hands of a capable adversary could lead to more severe consequences, such as a direct attack on an OT system, causing disruption, destruction or safety incidents. Recent public reporting suggests LockBit operators are also considering adding distributed denial of services (DDoS) capabilities as a third extortion method.

Although Dragos has not observed LockBit ransomware directly impacting or targeting ICS/OT technology, the fact remains that many organizations with industrial operations could be disrupted by a successful compromise of business-critical systems located in the information technology (IT)/Enterprise environment. Further, a significant number of LockBit operations over the past two years have impacted organizations with heavy reliance on ICS technology, suggesting an element of victim preference likely driven by the attacker's perspective of what drives organizations to be more likely to pay the ransom. Most industrial organizations rely on ICS technology and cannot afford disruption because of the critical functions they provide. Dragos assesses with moderate confidence that industrial organizations and associated supply chain companies will remain attractive victims for LockBit affiliates in 2023.

Key Takeaways

- LockBit Ransomware has similarities to other ransomware that have impacted industrial operations.
- LockBit 3.0 ransomware can infect Windows systems, Linux systems, VMware vSphere, and ESXi virtual environments.
- Criminals have used LockBit 3.0 in attacks against manufacturing, electric, transportation, and logistics organizations.
- A disgruntled LockBit developer released LockBit 3.0 builder code in September 2022 which researchers are using to identify detections for defenders.

Figure 1 below shows the Diamond Model diagram for LockBit 3.0.

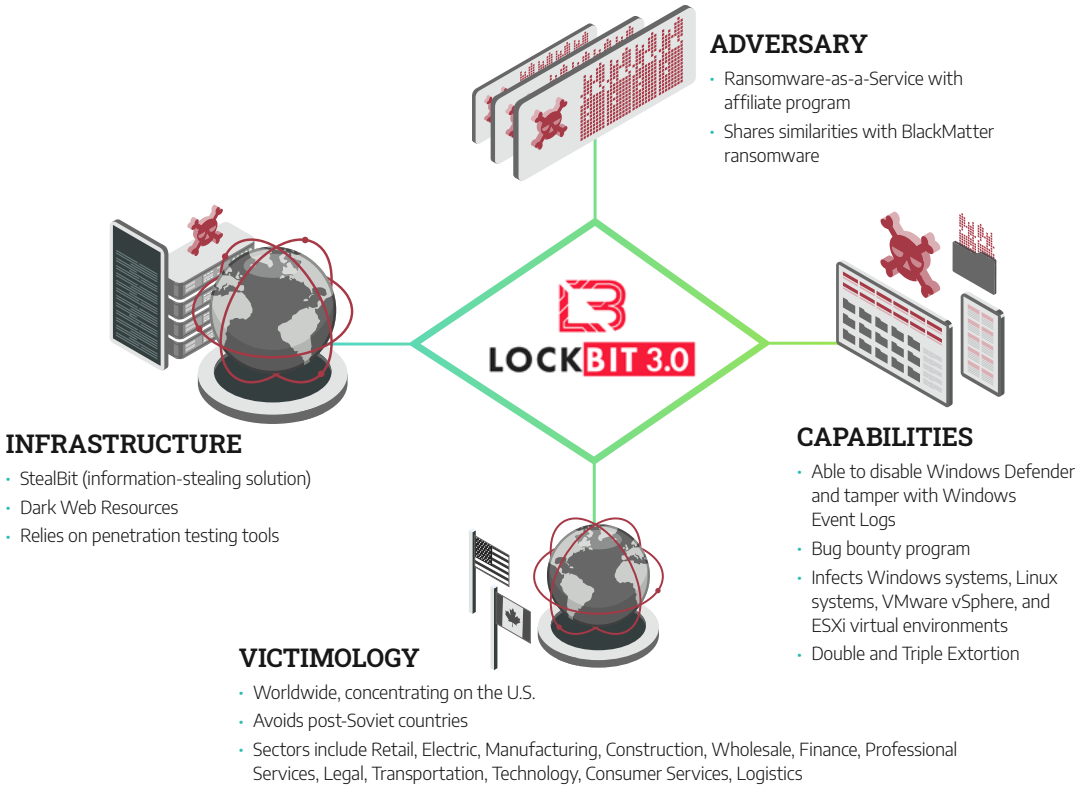

Figure 1: Lockbit Diamond Model

What Is LockBit?

LockBit is a ransomware-as-a-service (RaaS) provider that was first observed in September 2019. This means a controlling group develops the ransomware and then rents it to other adversaries for their respective criminal operations. Adversaries (commonly referred to as affiliates) that acquire LockBit get the ransomware and all the supporting infrastructure needed to conduct successful attacks. Profits generated from successful LockBit operations are split between the affiliates and the purveyors. LockBit affiliates are also encouraged to participate in a bug bounty program offering to pay anyone who finds bugs in the LockBit ransomware, vulnerabilities in their data leak site, and anyone who successfully doxes the "affiliate program boss."[1] These added affiliate perks increase the desirability of becoming a LockBit affiliate while improving the LockBit group's operational security.

The first iteration of LockBit was named the '.abcd virus,' referencing the file extensions used when encrypting files. The next iteration, LockBit 2.0, was released in June 2021, and a later release included a Linux version and a VMware ESXi hypervisor version. Additional features included self-spreading, clearing logs, and printing ransomware notes on network printers until the paper ran out.[2]

1 There has been a trend with cyber criminals to create new ways of attacking networks through crowdsourcing. Crowdsourcing ideas, also reduces the profits lost due to vulnerabilities in their own malware.

2 **LockBit 2.0: How This RaaS Operates and How to Protect Against It** – Palo Alto

LockBit 3.0 has ties to other ransomware groups that have impacted industrial operations, such as DarkSide and BlackMatter ransomware, which were responsible for the Colonial Pipeline incident in May 2021. LockBit 3.0 has also been called LockBit Black in some channels as a reference to their June 2022 release, which had significant code overlap with BlackMatter ransomware. Malware developers in the criminal ecosystem often move around, and, according to public reporting, it is highly likely that a developer associated with the BlackMatter ransomware operation joined the LockBit developers before the release of LockBit 3.0.[3,4] In addition to LockBit 3.0 being a derivative of BlackMatter's source code, LockBit 3.0 also includes the following features and capabilities:

- A new living-off-the-land (LOTL) technique to evade endpoint detection
- Ability to weaponize legitimate security tools on compromised networks
- Newly implemented an anti-analysis technique requiring a unique password for each LockBit binary
- Faster encryption rates that allow compromised hosts to be more fully encrypted before being detected
- A distributed denial of service (DDoS) capability as a third extortion technique[5]

The BlackMatter ransomware also shares similar features and configuration files with ALPHV,[6] aka Black Cat ransomware. In February 2022, members of the ALPHV ransomware group confirmed they were former members of the BlackMatter ransomware group. In July 2021, security researchers identified BlackMatter encryption algorithms[7] linking it to the DarkSide ransomware family. Further research revealed that DarkSide developers had rebranded the ransomware as BlackMatter after the Colonial Pipeline attack in May 2021. Although the DarkSide operators did not get into Colonial Pipeline's OT environment, the attack still had substantial impacts on their operations, including taking their critical business systems offline, which negatively impacted their ability to maintain their natural gas distribution pipeline. Shortly after this attack, DarkSide's operators lost access to their infrastructure.

Victimology

LockBit activity increased in 2022, and victims have compromised several global organizations, including manufacturing, transportation, and industrial businesses. As of December 2022, Dragos is unaware of any LockBit ransomware attacks that successfully penetrated the OT systems environment. However, like many ransomware attacks, LockBit operations can compromise an organization's critical business systems, often leading to service and supply chain disruptions in that organization's operational processes and systems. In fact, LockBit ransomware was considered one the most active in compromising industrial organizations in 2021 and 2022[8] Dragos' analysis of ransomware data shows Lockbit 3.0 was responsible for 21 percent of the total ransomware attacks, accounting for 40 incidents in Q4 of 2022. Black Basta and Royal came in second with only 12 percent each.[9] Multiple cyber threat intelligence practitioners have publicly assessed that LockBit will continue to be one of the top ransomware threats

3 **https://www.malwarebytes.com/blog/threat-intelligence/2022/10/ransomware-review-september-2022** – Malwarebytes
4 **LockBit Ransomware Group Augments Its Latest Variant, LockBit 3.0, With BlackMatter Capabilities** – Trend Micro
5 **LockBit ransomware mulls triple extortion following DDoS attack** – SC Media
6 **BlackCat (ALPHV) ransomware linked to BlackMatter, DarkSide gangs** – BleepingComputer
7 **DarkSide ransomware gang returns as new BlackMatter operation** – BleepingComputer
8 **LockBit, Conti most active ransomware targeting industrial sector** – BleepingComputer
9 **Dragos Industrial Ransomware Analysis: Q4 2022** – Dragos

in 2023 to organizations reliant on industrial infrastructure or providing critical services and, therefore more inclined to pay the ransom to avoid disruptions.

Dragos has identified trends[10] that could make an organization less defensible and more vulnerable to ransomware attacks. For example, many organizations lack visibility into critical OT environments, so it would be difficult to detect a ransomware attack occurring in the OT space. A lack of proper segmentation could allow a ransomware affiliate direct access to ICS devices for encryption. Ransomware affiliates will use stolen credentials to gain initial access, and Dragos found a large percentage of shared credentials between IT and OT systems in 2021. The most effective security measure, along with not sharing credentials, is enabling multi-factor authentication (MFA), but unfortunately, this isn't always feasible in an industrial setting. Dragos also found a significant increase in OT devices with external connections during 2021 engagements. Attackers will opportunistically use external connections as an easy access vector to a network.

Ransomware attacks on the industrial industry – in general - have remained steady over the last year. Based on Dragos analysis of ransomware attacks on ICS/OT, the manufacturing industry has been the most impacted, with 72% of the total industrial ransomware attacks in 2022. The food and beverage, oil and gas, energy, pharmaceutical, and transportation sectors received between 8 and 4 percent of the total ransomware attacks on industrial organizations.[11,12,13,14,15] This is shown in table 1 below.

	MANUFACTURING	FOOD & BEVERAGE	OIL & GAS	ENERGY	PHARMACEUTICAL	TRANSPORTATION
Q1 2022	75%	6%	3%	0%	4%	1%
Q2 2022	69%	8%	2%	8%	4%	5%
Q3 2022	68%	9%	6%	10%	10%	5%
Q4 2022	76%	8%	2%	7%	5%	1.80%
Average	72%	8%	4%	6%	6%	4%

Table 1: The Percentage Of Ransomware Attacks On Industrial Sectors By Quarter

10 **LockBit, Conti most active ransomware targeting industrial sector** – BleepingComputer
11 **Dragos Industrial Ransomware Analysis: Q3 2022** – Dragos
12 **Dragos Industrial Ransomware Analysis: Q2 2022** – Dragos
13 **Dragos ICS/OT Ransomware Analysis: Q1 2022** – Dragos
14 **Dragos ICS/OT Ransomware Analysis: Q4 2022** – Dragos
15 **Dragos Industrial Ransomware Analysis: Q4 2022** – Dragos

Q1 2022 to Q4 2022

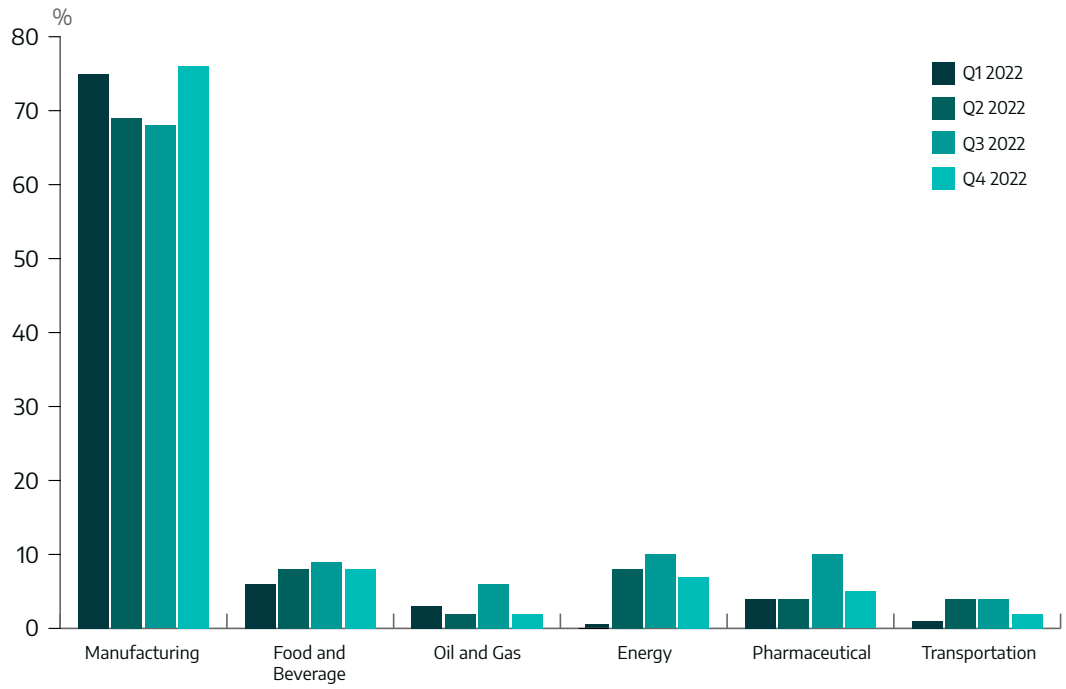

Figure 2: The Percentage Of Ransomware Attacks On Each Industrial Sector

Industrial Sectors Impacted by Ransomware Attacks (Q4 2021 to Q3 2022)

LockBit ransomware has been the most used ransomware against industrial targets since 2021, with an average of 31% of the total ransomware strains used against industrial sectors since the fourth quarter of 2021. Conti ransomware was the next highest used ransomware, with an average of 19% of the total ransomware attacks on industrial sectors. This average does not include the third quarter of 2022 because no attacks were recorded for the Conti ransomware since they officially announced they were shutting down their operations and rebranding in May 2022.[16]

Geographically, LockBit is a global threat, but it has largely impacted more industrial organizations within the United States compared to the rest of the world. Notably, LockBit ransomware will not execute on operating systems where the default language and keyboard layout are Cyrillic, a typical setting in the Commonwealth of Independent States (CIS) region. However, Kaspersky Labs has publicly reported that adversaries had used LockBit against organizations in Ukraine when LockBit was introduced in 2019.[17,18] The LockBit ransomware completes a language check, and if the current user's language settings match a list internal to the malware, it will terminate immediately.[19]

Figures 3 and *4* are a timeline of LockBit operations against industrial companies between August 2021 and September 2022.

16 **Conti ransomware shuts down operation, rebrands into smaller units** - BleepingComputer

17 **LockBit ransomware – What You Need to Know** – Kaspersky

18 **LockBit Ransomware: A Guide** – BlackBerry

19 **LockBit: Ransomware Puts Servers in the Crosshairs** – Symantec

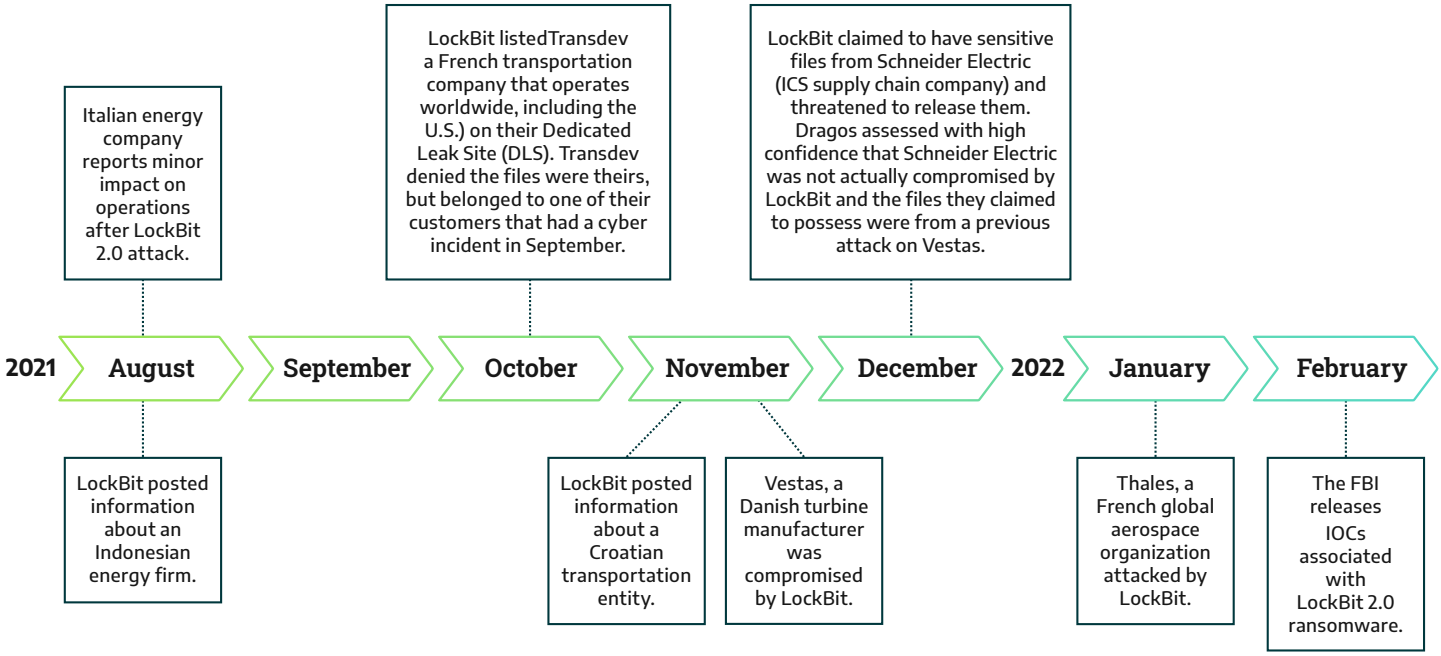

Figure 3: Timeline Of Transportation, Industrial, And Energy Companies Compromised By Lockbit From August 2021 To February 2022.

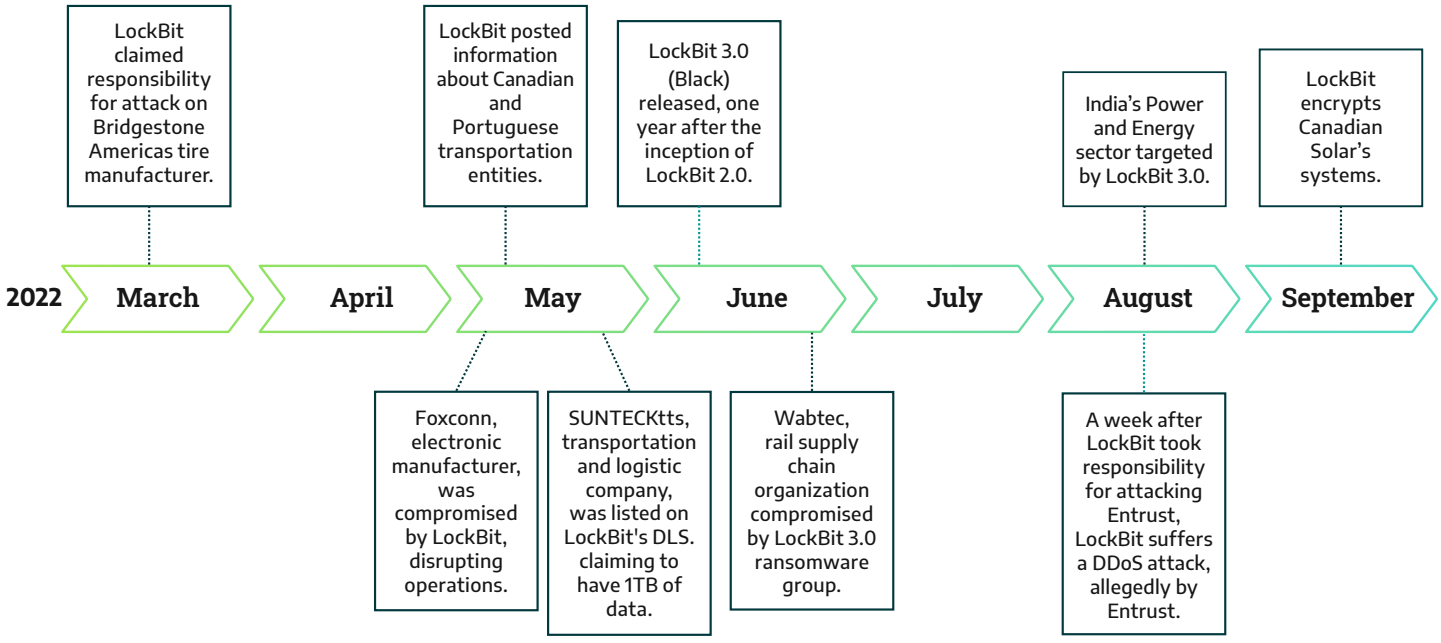

Figure 4: Timeline Of Transportation, Industrial, And Energy Companies Compromised By Lockbit From March To September 2022.

Early on in LockBit's existence, healthcare organizations were arguably the most impacted.[20,21,22] However, as LockBit gained more popularity, operators began expanding their use cases and ramped up attacks against manufacturing, transportation, aerospace, and food and beverage in 2022.[23]

Although LockBit developers have created rules stipulating that their ransomware will not be used against critical infrastructure, it is clear that LockBit affiliates largely disregard these rules and the LockBit developers do not appear to be overly concerned with holding their affiliates accountable. It is common for ransomware developers to have these ethical statements as part of their affiliate program because it provides an opportunity to distance themselves from their operators when their wares are used in an unethical fashion, which is often.

Capabilities

LockBit's attack methodology is like other ransomware variants. Figure 4 summarizes the high-level stages of a LockBit attack collected from open-source research.

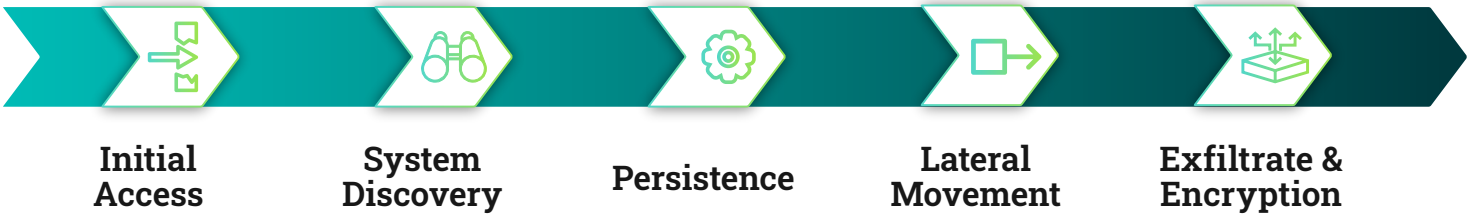

Figure 5: Stages Of A Lockbit Attack

The capabilities of LockBit ransomware are defined as the tools and techniques used throughout an attack. Each stage from Figure 4 is broken down into the tools, techniques, and associated MITRE tactics and techniques as documented from incident response and code analysis.

Initial Access

LockBit operators, like many other ransomware operations, gain initial access through well-known and established means including phishing/spearphishing, vulnerability and zero-day exploitation, capitalizing on compromised employee credentials, or acquiring unauthorized access through one of the many initial access traffickers that exist within the Darknet ecosystem. The following diagram lays out LockBit's Initial Access and System Discovery processes.

20 **An interview with LockBit: The risk of being hacked ourselves is always present** – The Record
21 **Ransomware Spotlight LockBit** – Trend Micro
22 **The State of Ransomware in Healthcare 2022** – Sophos
23 **Dragos Industrial Ransomware Analysis: Q2 2022** – Dragos

The following table details the initial access techniques and tools observed in LockBit attacks.

OPERATION CATEGORY	ADVERSARY PROCEDURE	MITRE ATT&CK MAPPING
Initial Access	SocGholish (a.k.a. FakeUpdate) downloads Cobalt Strike onto the victim's device.	• T1189 Drive-by Compromise • T0822 External Remote Services • T1190 Exploit Public-Facing Application • T1406.002 Obfuscated Files or Information: Software Packing

Table 2: Initial Access Techniques And Tools

System Discovery

Once initial access is gained, the LockBit ransomware leverages tools and techniques to discover vulnerable aspects of a network that would enable the ransomware to spread throughout a victim's network. Tools such as PC Hunter, Process Hacker, and GMER are used to terminate antimalware solutions. The ransomware also does system language checks to ensure the victim network is not a CIS country, which LockBit affiliates avoid attacking.

The following table details the system discovery techniques and tools observed in LockBit attacks.

OPERATION CATEGORY	ADVERSARY PROCEDURE	MITRE ATT&CK MAPPING
Discovery	The system's default language is checked against a LockBit-derived list of Cyrillic languages and terminates the ransomware if a match is found.	T1614 System Location Discovery
Defense Evasion	Exploit Process Hacker, PC Hunter, and GMER to terminate antimalware solutions on a victim network.	T1489 Service Stop
Discovery	Network and advanced port scanners are used to identify network structure and discover open ports and domain controllers.	• T1082 System Information Discovery • T1083 File and Directory Discovery • T1078.002 Valid Accounts: Domain Accounts
Discovery	Mimikatz is used to find authentication credentials.	T1003 OS Credential Dumping
Discovery	AdFind and Bloodhound find Active Directory and shared resources on a network.	T1482 Domain Trust Discovery
Discovery	Leverage PowerShell to execute additional SocGholish "sniffing" attributes against victim's device and network.	• T1059.003 Command and Scripting Interpreter: Windows Command Shell • T1059.001 Command and Scripting Interpreter: PowerShell
Discovery	Escalation of privileges by capitalizing on vulnerabilities like Microsoft Exchange Server vulnerability CVE-2021—34523 and using Windows Background Intelligent Transfer Service (BITS) vulnerability CVE-2020-0787.	T1218.003 System Binary Proxy Execution: CMSTP

Table 3: System Discovery Techniques And Tools

Persistence

Persistence is established by techniques to avoid detection, like anti-debugging and disabling services and tools that could identify and disable the ransomware. An adversary can use a Cobalt Strike beacon as a communication and remote execution tool.

The following table details the persistence techniques and tools observed in LockBit attacks.

OPERATION CATEGORY	ADVERSARY PROCEDURE	MITRE ATT&CK MAPPING
Persistence and Defense Evasion	Adding a file path to the registry run key to execute when the user logs in. This technique has the capability to persist even after a reboot.[24]	• T1547.001 Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder • T1112 Modify Registry
Defense Evasion	Anti-debugging techniques to hinder dynamic analysis.	T1622 Debugger Evasion
Persistence	Cobalt Strike beacon acts as a C2 tool and execution of remote commands.	• T1543.003 Create or Modify System Process: Windows Service • T1055 Process Injection
Persistence and Defense Evasion	Disabling of select processes, services, and tools to avoid detection.	• T1562.001 Impair Defenses: Disable or Modify Tools • T1489 Service Stop

Table 4: Persistence Techniques And Tools

Lateral Movement

The lateral movement of LockBit into a victim network is done by taking advantage of the access and inherent connections of a network's Domain Controllers and Active Directory. The attacker uses acquired credentials, either purchased through the darknet or found through penetration tools, to establish remote access and then infiltrate a victim's network.

The following table details the lateral movement techniques and tools observed in LockBit attacks.

OPERATION CATEGORY	ADVERSARY PROCEDURE	MITRE ATT&CK MAPPING
Privilege Escalation	PsExec is used to remotely execute processes on other systems.	• T1021.002 SMB/Admin Windows Shares • T1570 Lateral Tool Transfer
Lateral Movement	CrakMapExec is a penetration tool that collects Active Directory information.	• T1087 Account Discovery: Domain Account • T1083 File and Directory Discovery
Privilege Escalation	Group Policy modifications are made on the Domain Controller and then pushed to all machines on the Windows Domain.	T1548.002 Abuse Elevation Control Mechanism: Bypass User Account Control

Table 5: Lateral Movement Techniques And Tools

24 **LockBit ransomware borrows tricks to keep up with REvil and Maze** – Sophos

Privilege Escalation	Self-propagation via SMB connection using acquired credentials	T1021.002 SMB/Admin Windows Shares
Lateral Movement	RDP sessions are established using acquired credentials.	• T1021.001 Remote Services: Remote Desktop Protocol • T1078.001 Valid Accounts: Default Accounts

Table 5: Lateral Movement Techniques And Tools – Continued

Exfiltration and Encryption

The LockBit developers have demonstrated the ability and willingness to create more custom tools, such as StealBit. The StealBit information stealer was an addition to the LockBit 2.0 service offering and is a data exfiltration tool and the primary vector for their double-extortion capability. One of the main features of StealBit is that it has high rates of data exfiltration because it can steal multiple files in parallel and it uses interprocess communication (ICP) between multiple StealBit processes that are running on a compromised system.[25]

A highly enticing component of LockBit 3.0 is its encryption speeds. There are two schools of thought about ransomware encryption speeds:

1) Slow encryption is designed to not be "noisy" within the victim's network and thereby avoid detection.
2) Fast encryption is often "noisier" and more noticeable for network defenders, but because of the rate of encryption, defenders may not realize what is happening until it's too late.

LockBit can maintain high encryption rates because it only encrypts the first 4KB of a file and adds an "HLJkNskOq" extension. Once executed, LockBit encrypts victims' files with advanced encryption standard (AES) and the AES key is then further encrypted using the RSA algorithm. Finally, the victim's background is changed after the encryption process, and the ransom note begins printing on locally networked printers.

The following table details the exfiltration and encryption procedures observed in LockBit attacks.

OPERATION CATEGORY	ADVERSARY PROCEDURE	MITRE ATT&CK MAPPING
Exfiltration	StealBit is information-stealing malware developed by the LockBit group.	• T1106 Native API • T1559 Inter-process communications • T1070.004 Indicator Removal on Host: File Deletion • T1027 Obfuscated Files or Information • T1564.003 Hide artifacts: hidden window • T1614 System location Discovery • T1030 Data transfer size limits • T1041 Exfiltration Over C2 Channel
Exfiltration and Collection	Rclone, FreeFileSync, FileZilla, MegaSync, and MEGA are solutions for synchronization and file-sharing for the exfiltration of data.	• T1567.002 Exfiltration Over Web Service: Exfiltration to Cloud Storage • T1560.001 Archive Collected Data: Archive via Utility

Table 6: Exfiltration And Encryption Techniques And Tools

25 **THREAT ANALYSIS REPORT: Inside the LockBit Arsenal - The StealBit Exfiltration Tool** – Cybereason

Encryption	LockBit ransomware focuses on the encryption of VMware vSphere and ESXi virtual platforms.	• T1497 Virtualization/Sandbox Evasion • T1486 Data Encrypted for Impact
Defense Evasion	LockBit deletes shadow copies and recycle bins of every drive to prevent system recovery.	• T1485 Data Destruction • T1047 Windows Management Instrumentation • T1490 Inhibit System Recovery
Defense Evasion	LockBit deletes itself using a dropped .tmp file and any group policy updates to remove indicators that defenders can use.	• T1070.001 Indicator Removal on Host: Clear Windows Event Logs • T1070 Indicator Removal on Host

Table 6: Exfiltration And Encryption Techniques And Tools – Continued

Infrastructure

LockBit maintains DWRs on TOR where stolen documents and information are published from victims that refused to pay the ransom. They accept multiple forms of payment on their DWRs, such as Monero, bitcoin, and Zcash. Other third-party criminals can purchase the stolen data from their DWRs, as well, however, this feature does not appear to be fully operational at the time of this report. Third-party criminals interested in buying stolen information advertised on their DWRs could just as easily connect with the LockBit purveyors directly through peer-2-peer channels.

Detection and Mitigations

In late September 2022, LockBit's builder was released, supposedly by one of their own disgruntled developers.[26] Security vendors, including Dragos Detection and Vulnerability teams, continue to analyze the code to provide detections to network defenders. Dragos is actively developing detections for the LockBit 3.0 builder and has made detections available in its latest Knowledge Packs (KP).

The following signatures from open source research are still under development, and Dragos has not evaluated them for accuracy.

- Florian Roth is actively developing working Yara signatures:
- MAL_RANSOM_Lockbit_3_Jul22_1[27]
- MAL_RANSOM_Lockbit_Embedded_Jul22_2[28]
- Malpedia Yara rule detects win.lockbit[29]

26 **LockBit ransomware builder leaked online by "angry developer"** – BleepingComputer

27 **MAL_RANSOM_Lockbit_3_Jul22_1** – Valhalla

28 **MAL_RANSOM_Lockbit_Embedded_Jul22_2** – Valhalla

29 **Win.lockbit** – Malpedia

Mitigations Against LockBit:

Dragos recommends that asset owners and operators undertake the following mitigations against Lockbit:

- Monitor for abnormal legitimate Windows command line tools such as net.exe, taskkill.exe, vssadmin.exe, and wmic.exe.[30]
- Segmentation of IT and OT and additionally different processes.
- Stay up to date on patches for VMware.
- Protect the virtualization platform by enabling strict lockdown mode and restricting unsigned scripts by enabling the 'execInstalledOnly' flag.[31]
- Back up virtual machines and save snapshots offsite.
- Only allow traffic from designated hosts on ports 445 (Server Message Block (SMB)), 135 (Remote Procedure Call (RPC)), 598505986 (Windows Remote Management (WinRM)), and 22 (Secure Shell protocol (SSH)). This can be accomplished through host-based firewalls, proper network segmentation, or modern micro-segmentation technologies.
- Limit remote user permissions and audit user group membership regularly.
- Disable Remote Desktop Protocol (RDP) if unnecessary.
- Set firewall rules to block RDP traffic between network zones and do not leave RDP accessible to the internet.
- Use remote desktop gateways
- Use multi-factor authentication for remote logins.
- Harden the Active Directory environment and apply least privileges.
- Implement robust credential and password hygiene practices.
- Implement Privileged Identity and Access solutions.
- Use anti-malware solutions to detect ransomware attacks and the ability to roll back infections.
- Deploy endpoint detection and response (EDR) solution.

Conclusion

LockBit RaaS remains a threat to critical infrastructure, both directly and indirectly. An attack on supply chain manufacturing companies easily leads to a disruption of services or products that critical infrastructure relies upon. Additionally, LockBit shares code with BlackMatter and, subsequently, DarkSide, which is arguably a watershed moment for how true ransomware attacks can impact a critical infrastructure organization's operational processes and systems as well as causing significant financial and reputational loss.

Finally, one of the most pertinent observations of LockBit operations is that there is a more thoughtful process to victim selection. It isn't simply attacking as many organizations as possible – there is an observable method and if the Colonial Pipeline incident taught ransomware operators anything it's that critical infrastructure organizations may be more willing to pay the ransom if their operations are impacted.

30 **LockBit Ransomware** – HHS Cybersecurity Program

31 **Revealing Emperor Dragonfly: Night Sky and Cheerscrypt** – A Single Ransomware Group – Sygnia

About Dragos, Inc.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about our technology, services, and threat intelligence offerings, visit **dragos.com** or connect with us at **sales@dragos.com**.

Copyright ©2023 Dragos, Inc. | All Rights Reserved. | Last updated March, 2023