Ransomware Spotlight: LockBit

Archived: 2026-04-02 11:37:19 UTC

The impact of LockBit and insights from Water Selkie

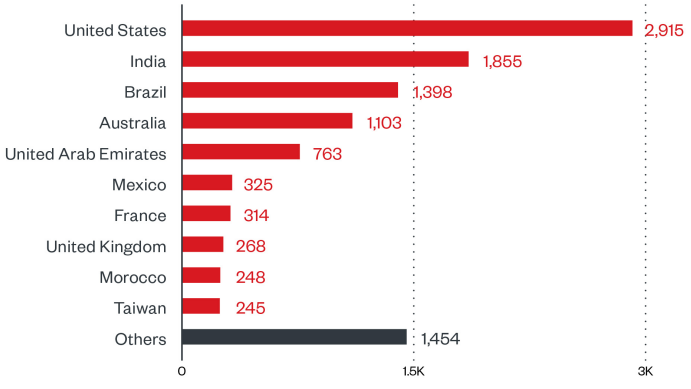
Our investigation into the intrusion set behind LockBit, which we track as Water Selkie, reveals the effectiveness and impact of the tactics we have discussed. The key takeaways are the following:

- **The malware's performance is a strong selling point.** The malware's speed and capabilities are widely known because the group uses them as selling points. The threat group's efforts to publicize their malware's capabilities have established it as the ransomware with one of the fastest and most efficient encryption methods.
- **It considers external pressures and issues faced by its potential targets.** Water Selkie's operators have indicated a preference for victims in Europe who fear breaching EU's General Data Protection Regulation (GDPR). They continue to also consider the US to have lucrative targets, but see that data privacy laws can affect their chances of getting a successful payout. In general, they are attuned to geopolitical issues that they can use to their advantage.
- **Banks on the strength of its affiliate program.** As mentioned earlier, a contributing factor in LockBit's success is how well it recruits trustworthy and capable affiliates. Evidence also suggests that several of its affiliates are involved in multiple RaaS operations, which helps Water Selkie innovate and keep up with its competition. In return, Water Selkie prides itself on its professional operation that can be trusted by affiliates.
- **It has more in store for the future.** Water Selkie clearly ramped up operations in the second half of 2021. We see that the intrusion set will either maintain or increase their level of activity in the first half of 2022. Organizations should also expect more supply chain attacks in the future according to an interviewopen on a new tab conducted with one of LockBit's operators.

With LockBit affiliates being likely involved in other RaaS operations, its tactics slipping into those of other ransomware groups isn't a far-fetched notion. Organizations would therefore benefit from recognizing LockBit's tactics, techniques, and procedures (TTPs) laid out in the next sections.

Top affected industries and countries

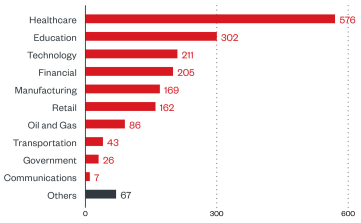
In this section, we discuss Trend Micro™ Smart Protection Network™ data, which are detections of LockBit attempts to compromise organizations. LockBit has been detected all over the globe, with the US seeing most of the attack attempts from June 2021 to January 20, 2022, followed by India and Brazil. Like many ransomware families LockBit avoids Commonwealth of Independent States (CIS) countries.



open on a new tab

Figure 2. Countries with the highest number of attack attempts per machine for LockBit ransomware (July 1, 2021 to January 20, 2022)
Source: Trend Micro™ Smart Protection Network™ infrastructure

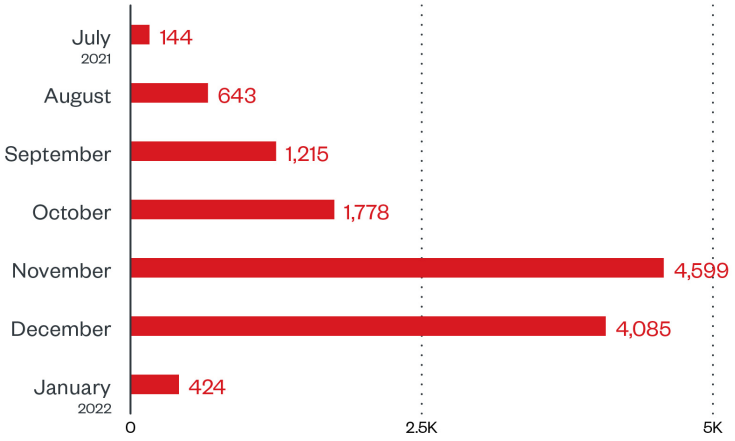
We saw the most LockBit-related detections in the healthcare industry followed by the education sector. LockBit threat actors have claimedopen on a new tab that they do not attack healthcare, educational, and charity institutions. This "contradictory code of ethics," has been notedopen on a new tab by the US Department of Health Services (HHS) who warns the public not to rely on such statements as these tend to dissolve in the face of easy targets.



open on a new tab

Figure 3. Industries with the highest number of attack attempts per machine for LockBit ransomware (July 1, 2021 to January 20, 2022)
Source: Trend Micro Smart Protection Network infrastructure

Overall, we saw increased LockBit-related activity following the release of LockBit 2.0, peaking in November 2021.



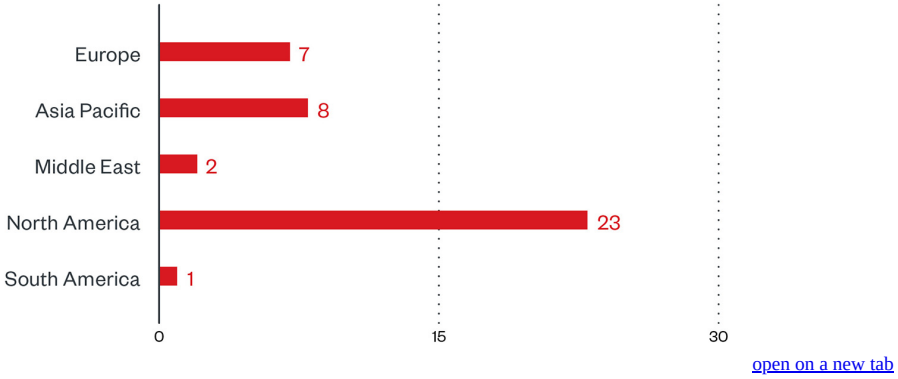
open on a new tab

Figure 4. LockBit monthly detections per machine (July 1, 2021 to January 20, 2022)
Source: Trend Micro Smart Protection Network infrastructure

Targeted regions and sectors according to LockBit leak site

In this section, we examine the number of attacks recorded on LockBit's leak site, which represents successfully compromised organizations who, as of writing, have refused to pay ransom. In our foray into the leak site of LockBit operators from December 16, 2021 to January 15, 2022, we observed that they had the highest number of recorded victims among active ransomware groups at 41, followed by Continews article at 29. Do note, however, that LockBit has been accusedopen on a new tab of artificially inflating the number of their victims.

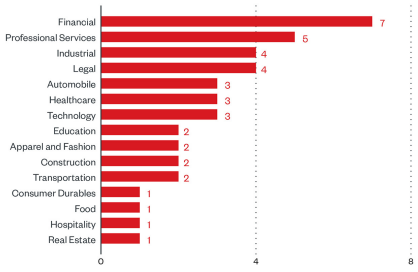
Looking into the list of their victims, it appears that more than half of the organizations are based in North America, followed by Europe and Asia Pacific.



open on a new tab

Figure 5. Regional distribution of LockBit victims according to the group's leak site (December 16, 2021 to January 15, 2022)

LockBit targets organizations indiscriminately, in that their victims come from many different sectors compared to other groups. In the abovementioned time period, they have victims coming from financial, professional services, manufacturing, and construction sectors, just to name a few. The majority of LockBit's victims have been either small or small and medium-size businesses (SMBs) – 65.9% and 14.6% respectively, with enterprises only comprising 19.5%. That's at odds with a group like Conti who victimized 44.8% of enterprises and 34.5% SMBs, and only victimized 20.7% of small businesses.



open on a new tab

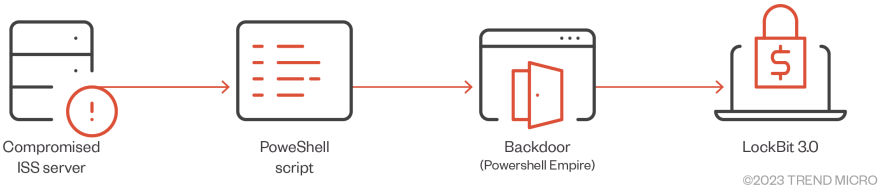
Figure 6. Sector distribution of LockBit victims according to the group's leak site (December 16, 2021 to January 15, 2022)

In our observation of the activities within the LockBit leak site for the same time period, majority of attacks took place during weekdays, approximately 78% of the total, while 22% happened during the weekend.

Infection chain and techniques

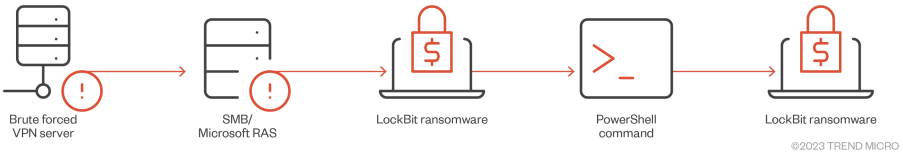
Operating as a RaaS, LockBit infection chains show a variety of tactics and tools employed, depending on the affiliates involved in the attack. Affiliates typically buy access to targets from other threat actors, who typically obtain it via phishing, exploiting vulnerable apps, or brute forcing remote desktop protocol (RDP) accounts.

Here are some of the observed infection flows of LockBit variants:



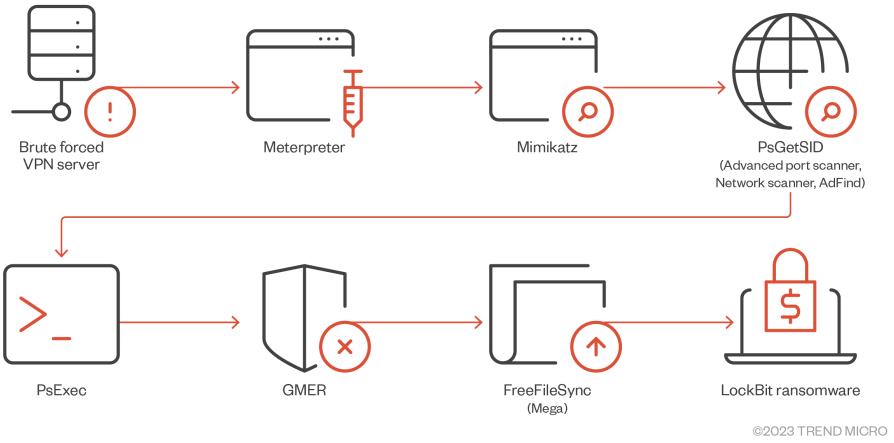
open on a new tab

Figure 7. A LockBit 1.0 campaign that used PowerShell Empire to perform command and control after gaining access to the system



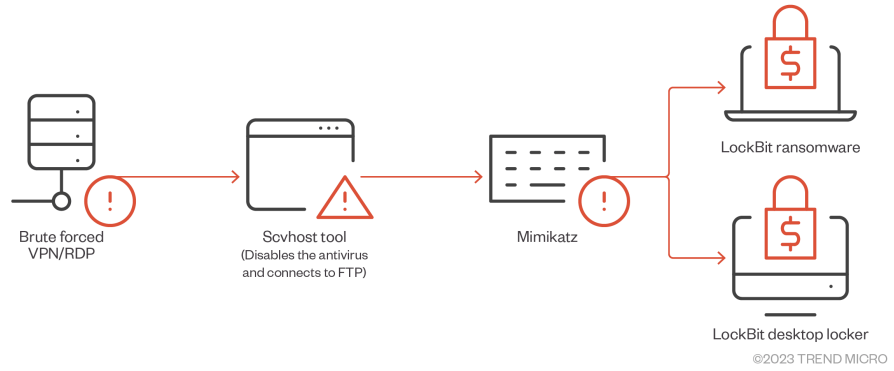
open on a new tab

Figure 8. A LockBit 1.0 campaign that used Microsoft RAS to access other systems



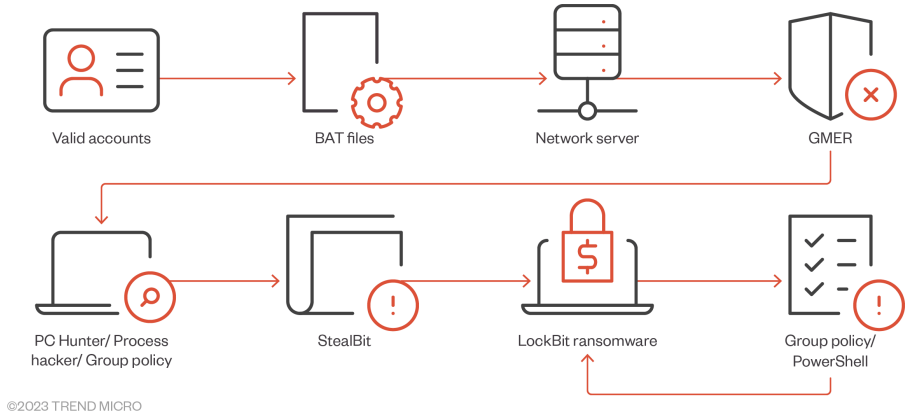
open on a new tab

Figure 9. A LockBit 1.0 campaign that used Meterpreter to perform command and control after gaining access to the system



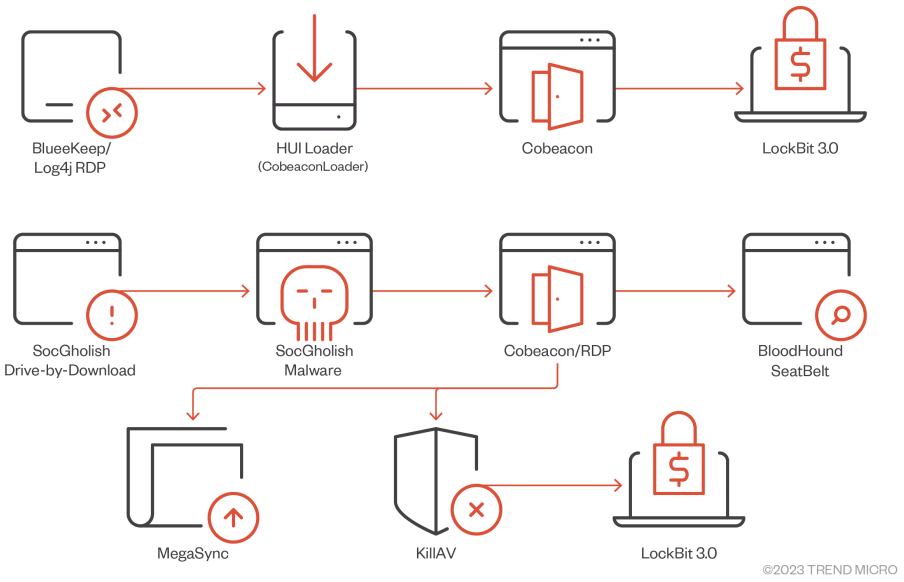
open on a new tab

Figure 10. A LockBit 1.0 campaign that did not involve any network scanning as it directly deployed the payload after gaining access to the system



open on a new tab

Figure 11. LockBit 2.0 infection chain that uses StealBit for automated data exfiltration



open on a new tab

Figure 12. LockBit 3.0 infection chain that uses Cobeacon and KillAV

Initial Access

- LockBit operators mostly gain access via compromised servers or RDP accounts that are usually bought or obtained from affiliates.
- In some instances, it arrived via spam email or by brute forcing insecure RDP or VPN credentials.
- It can also arrive via exploiting Fortinet VPN's CVE-2018-13379open on a new tab vulnerability.

Execution

- LockBit is usually executed via command line as it accepts parameters of file path or directories if desired to only encrypt specific paths.
- It may also be executed via created scheduled tasks. This is usually the case if it is propagated in other machines.
- There are also reports of it being executed using PowerShell Empire, a pure PowerShell post-exploitation agent.

Credential Access

- Aside from using credentials obtained from affiliates. LockBit attacks were also observed using Mimikatz to further gather credentials.

Defense Evasion

- Some infections were observed to have GMER, PC Hunter, and/or Process Hacker. These are tools that are usually used to disable security products.
- In some observed attacks, a Group Policy was created to disable Windows Defender.

Discovery

- Network Scanner, Advanced Port Scanner, and AdFind were also used to enumerate connected machines in the network. Probably to locate the Domain Controller or Active Directory server as these are usually the best targets for deploying ransomware with network encryption or propagation.

Lateral Movement

- LockBit can self-propagate via SMB connection using obtained credentials.
- Some samples can self-propagate and execute via Group Policy.
- In some instances, PsExec or Cobalt Strike were used to move laterally within the network.

Exfiltration

- Uploads stolen files via cloud storage tools like MEGA or FreeFileSync.
- Sometimes, the StealBit malware (also sold by the threat actors) was used instead to exfiltrate stolen files.

Impact

- The ransomware payload will proceed with encryption routine upon execution. Encryption includes both local and network encryption.
- It encrypts files using AES and encrypts AES key with RSA encryption. The AES Key is generated using BCryptGenRandom.
- For faster encryption, it only encrypts the first 4KB of a file and appends it to ".lockbit."
- It will also replace the desktop wallpaper with a note that includes a statement where it tries to recruit insiders or affiliates within companies.

Figure 12. Sample wallpaper used by LockBit

- LockBit also sends a WoL packet to ensure that network drives are active for its network encryption; this behavior was first observed on the Ryuk ransomwarenews- cybercrime-and-digital-threats.
- LockBit also has the capability to print its ransom note using connected printers using WinSpool APIs, which is probably inspired by Egregor ransomware.

MITRE tactics and techniques

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Exfiltrati
T1566 - Phishing *Arrives via phishing emails* **T1190** - Exploit public-facing application *Arrives via any the following exploits:• CVE-2018-13379* **T1078** - Valid accounts	**T1059** - Command and scripting interpreter *Uses various scripting interpreters like PowerShell and Windows command shell* **T1204** - User execution	**T1547** - Boot or logon autostart execution *Creates registry run entries*	**T1134** - Access token manipulation *Use AdjustTokenPrivilege API to modify token attribute to SE_PRIVILEGE_ENABLED* **T1548** - Abuse Elevation Control Mechanism *Makes use of ucmDccwCOMMethod in UACME, a github collection of UAC bypass techniques*	**T1140** - Deobfuscate/Decode Files or Information *Strings to be used throughout the routine are encrypted using XOR or Subtraction.* **T1562** - Impair defenses *Disables security related services via terminating them. May include using tools like PC Hunter, Process Hacker, KillAV/KillProc*	**T1083** - File and directory discovery *Searches for specific files and directory related to its encryption* **T1135** - Network Share Discovery *Enumerate network share for*	**T1570** - Lateral tool transfer *Can make use of RDP, SMB admin shares, or PsExec to transfer the ransomware or tools within the network*	**T1567** - Exfiltratic over web service *Syncs files a specifie cloud storage, s as MegaS or FreeFileS* **T1041** - Exfiltrati Over C2 Channel *Exfiltratic using StealBit to*

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Exfiltrati
Has been reported to make use of compromised accounts to access victims via RDP or VPN **T1106** - Execution through API *Uses native API to execute various commands/ routines*	*User execution is needed to carry out the payload from the spear phishing link or attachments*			**T1574** - Hijack execution flow *DLL side-loading can also be used as a form of defense evasion* **T1218** - Signed Binary Proxy Execution *Executes mshta to open the ransom note* **T1484** - Domain Policy Modification *It releases group policy update that will be able to terminate AV tools and create scheduled tasks to execute the propagated copies via SMB* **T1070** - Indicator Removal on Host *It is capable of deleting Windows event logs and its executable file to remove traces*	*its network encryption* **T1018** - Remote system discovery *Makes use of tools for network scans* **T1057** - Process discovery *Discovers certain processes for process termination*		

Summary of malware, tools, and exploits used

Security teams can watch out for the presence of the following malware tools and exploits that are typically used in LockBit attacks:

Initial Entry	Execution	Discovery	Lateral Movement	Defense Evasion	Exfiltration
• Phishing emails • RDP/Valid accounts • Exploit: ◦ CVE-2018-13379	• Scheduled tasks • Windows command-line	• Network Scanner	• Group Policy • SMB • PsExec	• KillAV/KillProc • PC Hunter • Process Hacker	• StealBit • FreeFileSync • MegaSync

Recommendations

As mentioned earlier, we expect the LockBit to continue its level of activity, if not increase it in the coming months. From our discussion, LockBit also demonstrates both consistent and versatile operations that adapt to current trends that affect the threat landscape. Organizations therefore should also keep abreast of the latest shifts that could influence their own security measures.

To help defend systems against similar threats, organizations can establish security frameworks that can allocate resources systematically for establishing a solid defense against ransomware.

Here are some best practices that can be included in these frameworks:

Audit and inventory

- Take an inventory of assets and data
- Identify authorized and unauthorized devices and software
- Make an audit of event and incident logs

Configure and monitor

- Manage hardware and software configurations
- Grant admin privileges and access only when necessary to an employee's role
- Monitor network ports, protocols, and services
- Activate security configurations on network infrastructure devices such as firewalls and routers
- Establish a software allow list that only executes legitimate applications

Patch and update

- Conduct regular vulnerability assessments
- Perform patching or virtual patching for operating systems and applications
- Update software and applications to their latest versions

Protect and recover

- Implement data protection, backup, and recovery measures
- Enable multifactor authentication (MFA)

Secure and defend

- Employ sandbox analysis to block malicious emails
- Deploy the latest versions of security solutions to all layers of the system, including email, endpoint, web, and network
- Detect early signs of an attack such as the presence of suspicious tools in the system
- Use advanced detection technologies such as those powered by AI and machine learning

Train and test

- Regularly train and assess employees on security skills
- Conduct red-team exercises and penetration tests

A multilayered approach can help organizations guard the possible entry points into the system (endpoint, email, web, and network). Security solutions can detect malicious components and suspicious behavior could help protect enterprises.

- Trend Micro Vision One™products provides multilayered protection and behavior detection, which helps block questionable behavior and tools early on before the ransomware can do irreversible damage to the system.
- Trend Micro Cloud One™ Workload Securityproducts protects systems against both known and unknown threats that exploit vulnerabilities. This protection is made possible through techniques such as virtual patching and machine learning.
- Trend Micro™ Deep Discovery™ Email Inspectorproducts employs custom sandboxing and advanced analysis techniques to effectively block malicious emails, including phishing emails that can serve as entry points for ransomware.
- Trend Micro Apex One™products offers next-level automated threat detection and response against advanced concerns such as fileless threats and ransomware, ensuring the protection of endpoints.

Indicators of Compromise (IOCs)

HIDE

Like it? Add this infographic to your site:
1. Click on the box below. 2. Press Ctrl+A to select all. 3. Press Ctrl+C to copy. 4. Paste the code into your page (Ctrl+V).

Image will appear the same size as you see above.

We Recommend

-
-
-
-

- The Industrialization of Botnets: Automation and Scale as a New Threat Infrastructurenews article
- Complexity and Visibility Gaps in Power Automatenews article
- Azure Control Plane Threat Detection With TrendAI Vision One™news article
- AI Security Starts Here: The Essentials for Every Organizationnews article
- The AI-fication of Cyberthreats: Trend Micro Security Predictions for 2026predictions
- Ransomware Spotlight: DragonForcenews article
- Stay Ahead of AI Threats: Secure LLM Applications With Trend Vision Onenews article
- The Road to Agentic AI: Navigating Architecture, Threats, and Solutionsnews article

---