LockBit 2.0

Archived: 2026-04-05 19:52:05 UTC

LockBit 2.0: In-Depth Analysis, Detection, Mitigation, and Removal

Summary of LockBit 2.0 Ransomware

LockBit 2.0 emerged in August 2021, and is the evolution of the original LockBit RaaS (Ransomware-as-a-service). Linux versions of LockBit 2.0 were first observed in early 2022. LockBit practices double extortion – demanding payment for a decryptor, as well as for the non-release of stolen data. LockBit touts their 'performance' (speed/rate of encryption) as a selling point for their services. The group is also known for using custom or specialized tools such as StealBIT for exfiltration.

What Does LockBit 2.0 Ransomware Target?

LockBit ransomware typically targets the healthcare, finance, legal, and insurance industries. Targeting may vary across affiliates. Campaigns within the CIS (Commonwealth of Independant States) are discouraged.

How Does LockBit 2.0 Ransomware Spread?

LockBit 2.0 is delivered in multiple ways: through Cobalt Strike or a similar framework, and through email phishing. Additionally, SMB spreading functionality is integrated into LockBit, and it can be turned on and off.

LockBit 2.0 Ransomware Technical Details

LockBit is an ongoing ransomware affiliate program. The second revision ‘LockBit 2.0’, has been operating since early 2020.

Encryption is implemented in parts via the completion port (I/O), encryption algorithm AES + ECC. So far, none have managed to decrypt it. LockBit is known for its encryption speed and self-spreading function.

Operators behind LockBit 2.0 attempt to utilize LOLBINS and COTS options where possible. Within LockBit campaigns, there is often heavy use of PowerShell. WMIC, and/or SMB for example.

LockBit 2.0 can encrypt files regardless of online status meaning the encryption works offline. Affiliates have complete control over their campaigns via an administrative panel hosted via TOR (.onion domain). LockBit 2.0 shares many features with other modern and successful ransomware families. These include:

- Network detection and spreading via DFS/SMB/WebDav
- Automatic termination of processes that may interfere with the encryption or extraction processed (backup software, security agents/scanners)
- Blocking the launch of processes that may lead to termination of the encryption
- Removal of Shadow Copies
- Clearing of logs, self-cleaning
- Options for hidden or visible runtime modes
- Spread to hosts with Wake-On-Lan
- Interaction with networked printers
- Support for “all” versions of Windows

In January of 2022, versions of LockBit targeting Linux were observed in the wild. These initial payloads primarily target Linux-based ESXi servers.

MITRE ATT&CK

Data Encrypted for Impact T1486

Network Share Discovery T1135

Remote Services: SMB/Windows Admin Shares T1021.002

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder T1547.001

Command and Scripting Interpreter T1059

Exploitation for Client Execution T1203

How to Detect LockBit 2.0 Ransomware

- The SentinelOne Singularity XDR Platform can identify and stop any malicious activities and items related to LockBit 2.0.

In case you do not have SentinelOne deployed, detecting this ransomware requires a combination of technical and operational measures, which are designed to identify and flag suspicious activity on the network. This allows the organization to take appropriate action, and to prevent or mitigate the impact of the ransomware attack.

1. Use antimalware software, or other security tools, which are capable of detecting and blocking known ransomware variants. These tools may use signatures, heuristics, or machine learning algorithms, to identify and block suspicious files or activities.
2. Monitor network traffic, and look for indicators of compromise, such as unusual network traffic patterns, or communication with known command-and-control servers.
3. Conduct regular security audits and assessments, to identify vulnerabilities in the network and the system, and to ensure that all security controls are in place and functioning properly.
4. Educate and train employees on cybersecurity best practices, including how to identify and report suspicious emails, or other threats.
5. Implement a robust backup and recovery plan, to ensure that the organization has a copy of its data, and can restore it in case of an attack.

How to Mitigate LockBit 2.0

- The SentinelOne Singularity XDR Platform detects and prevents malicious behaviors and artifacts associated with LockBit.

If you do not have SentinelOne deployed, there are several steps that organizations can take to mitigate the risk of AtomSilo ransomware attacks.

Educate Employees

Employees should be educated on the risks of ransomware, and on how to identify and avoid phishing emails, malicious attachments, and other threats. They should be encouraged to report suspicious emails or attachments, and to avoid opening them, or clicking on links or buttons in them.

Implement Strong Passwords

Organizations should implement strong, unique passwords for all user accounts, and should regularly update and rotate these passwords. Passwords should be at least 8 characters long, and should include a combination of uppercase and lowercase letters, numbers, and special characters.

Enable Multi-factor Authentication

Organizations should enable multi-factor authentication (MFA) for all user accounts, to provide an additional layer of security. This can be done through the use of mobile apps, such as Google Authenticator or Microsoft Authenticator, or through the use of physical tokens or smart cards.

Update and Patch Systems

Organizations should regularly update and patch their systems, to fix any known vulnerabilities, and to prevent attackers from exploiting them. This includes updating the operating system, applications, and firmware on all devices, as well as disabling any unnecessary or unused services or protocols.

Implement Backup and Disaster Recovery

Organizations should implement regular backup and disaster recovery (BDR) processes, to ensure that they can recover from ransomware attacks, or other disasters. This includes creating regular backups of all data and systems, and storing these backups in a secure, offsite location.

The backups should be tested regularly, to ensure that they are working, and that they can be restored quickly and easily.

LockBit 2.0 Ransomware FAQs

What is LockBit 2.0 Ransomware?

LockBit 2.0 is a dangerous program that locks up your files and demands money to get them back. It spreads through bad links, fake emails, or hidden downloads. Once inside, it scrambles everything, leaving only a ransom note behind. Companies and individuals have both been hit. You can lower your risk by avoiding suspicious attachments, updating security software, and backing up important files in a safe place.

What happens when LockBit 2.0 Ransomware infects a system?

Once LockBit 2.0 gets into a computer, it scans for important files and locks them with powerful encryption. Then, it leaves a ransom note demanding payment for a secret key to unlock the files. Sometimes, it even spreads to other computers on the same network. You can fight back by backing up your data in secure locations and responding quickly if something unusual starts happening on your system.

What types of files does LockBit 2.0 encrypt?

LockBit 2.0 locks a wide range of files, including documents, spreadsheets, videos, and databases. Anything valuable or important is a target. After encryption, the files can’t be opened without a special key that attackers sell for ransom. You can prevent losing access to your data by making regular backups and storing them somewhere safe, like an external hard drive or a protected cloud service.

Does LockBit 2.0 steal data before encryption?

Yes, LockBit 2.0 doesn’t just lock files—it also steals data before encrypting it. Hackers can then threaten to leak sensitive information if the ransom isn’t paid. This makes attacks even more dangerous. You can limit the damage by protecting sensitive data with strong security measures, using encrypted backups, and monitoring networks for suspicious file transfers that might signal a ransomware attack.

Which industries are most targeted by LockBit 2.0 Ransomware?

LockBit 2.0 attacks businesses that rely on important data, such as healthcare, finance, and manufacturing. These industries can’t afford long shutdowns, making them more likely to pay the ransom. Hackers look for weak spots, like outdated security or employees who fall for phishing scams. You can lower your risk by keeping security patches updated, training staff, and using strong security software.

How can businesses protect themselves from LockBit 2.0 Ransomware?

Companies can fight LockBit 2.0 by training employees to recognize phishing emails, limiting who can access important files, and using strong antivirus programs. You can also block untrusted websites, keep your software updated, and back up files regularly. Hackers look for weak spots, so closing security gaps and watching for unusual activity on your network can help keep them out.

What security best practices help prevent a LockBit 2.0 infection?

Good security habits make a big difference. You can use strong passwords, set up multi-factor authentication, and scan for strange behavior on your network. Teach employees how to spot suspicious emails and avoid risky links. Back up your data often and keep backups separate from your main system. The harder you make it for hackers, the less likely you are to become a victim.
