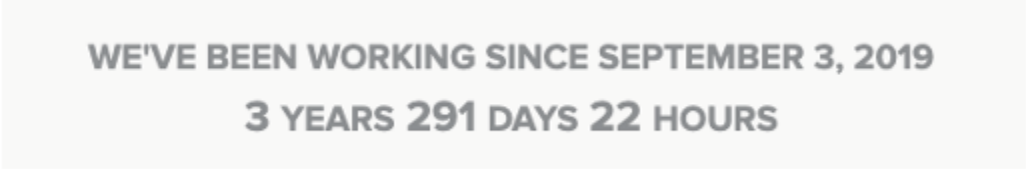
HISTORY OF LOCKBIT

LockBit is a ransomware group that has been active since early 2020 (the active period goes back to 2019 if its predecessor “ABCD ransomware” is included in the “LockBit” family) providing a Ransomware-as-a-Service (RaaS) service to for-hire online criminals known as affiliates. The affiliates’ job is to select and infiltrate victim organizations and deploy the ransomware provided by the LockBit developer.

The developer has consistently worked to improve the ransomware: LockBit 2.0 (also known as LockBit Red) was released in mid-2021, and LockBit 3.0 (also known as LockBit Black) became available in early-2022. The latest LockBit ransomware variant, “LockBit Green,” appeared in early 2023. While the LockBit ransomware initially only supported the Windows platform, the LockBit threat actor group added support for Linux/VMware/ESXi and macOS platforms in 2021 and 2023, respectively. The group also works with partners who want to sell exfiltrated data but do not want to encrypt victims' files.



LockBit uses a dual extortion tactic, demanding that victims pay a ransom to recover their files and not release the stolen information to the public. LockBit is also believed to threaten Distributed Denial of Service (DDoS) attacks against victims if the demanded ransom is not paid.

.As a RaaS, the LockBit operator offers its affiliates a variety of options for splitting the ransom fee. The ransom payment is typically split 1:4 between the LockBit operator and the affiliates.

Using the features provided by the LockBit operator, its affiliates can perform a variety of activities, including:

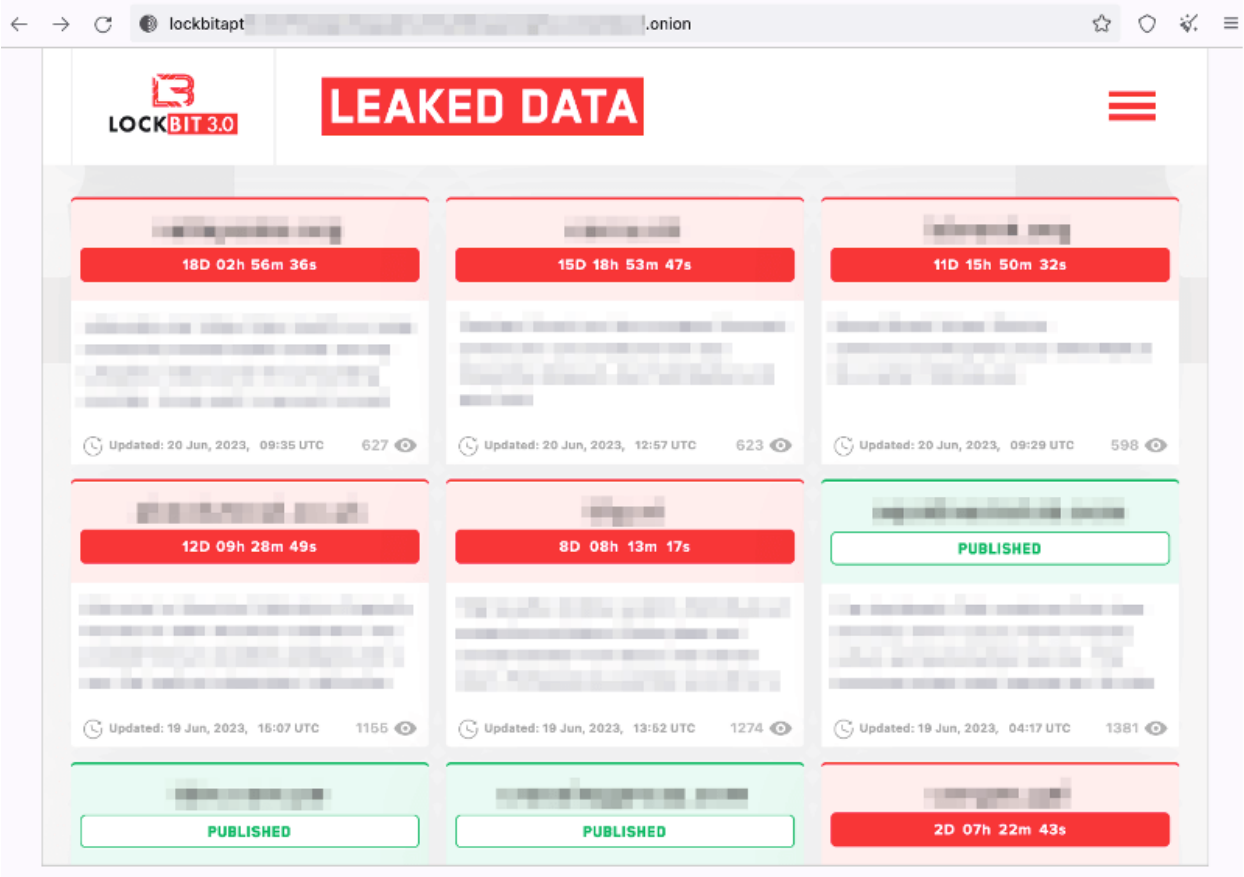
- Create private chat rooms to communicate with victim organizations
- Use of a custom “StealBit” stealer for data exfiltration
- Upload images, data, and communication history with victim organizations to the LockBit blog (data leak site)
- Set exceptions for computer names, file names, and file extensions that are not to be encrypted
- Shut down and remove Windows Defender
- Run the ransomware in SafeMode
- Delete shadow copies

It also has “do not target” and approved “target” industry lists for file encryption and data exfiltration.

- Affiliates are NOT allowed to encrypt files belonging to critical infrastructure, such as nuclear/thermal/hydroelectric power plants, gas and oil pipelines, oil production stations, and refineries. However, affiliates are allowed to steal data from such organizations without encrypting files.
- Affiliates are NOT allowed to attack post-Soviet countries: Armenia, Belarus, Georgia, Kazakhstan, Kyrgyzstan, Latvia, Lithuania, Moldova, Russia, Tajikistan, Turkmenistan, Uzbekistan, Ukraine, and Estonia.
- Affiliates ARE allowed to target non-profit organizations
- Affiliates ARE allowed to target private and for-profit educational institutions
- Affiliates ARE allowed to attack medical and pharmaceutical institutions/companies, as long as the attack does not result in death. Affiliates are free to steal data without encrypting files.
- Affiliates ARE allowed to attack government agencies (as long as they make a profit)
- Affiliates ARE ENCOURAGED to attack police stations and law enforcement agencies

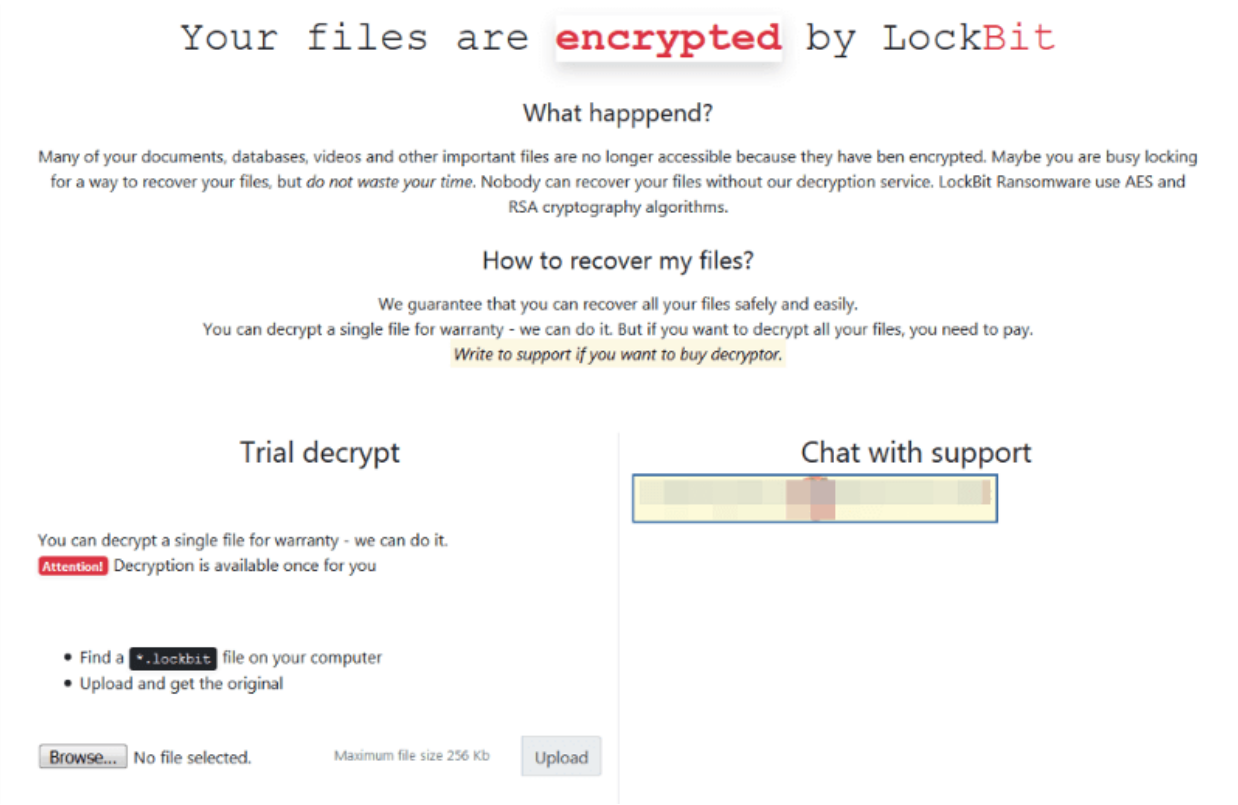
LockBit Data Leak Site

LockBit has a data leak site on TOR where LockBit affiliates can post information about victims and their stolen data.



Each victim has their own page with a countdown timer and examples of stolen information. In some cases, LockBit threat actors offer to extend the ransom deadline, download stolen information, and destroy all copies for a fee.

The LockBit group also offers a file-sharing service that supports files up to 2GB. The service also has options to automatically remove uploaded files after 24 hours, seven days, or on the first download, as well as a password setting.
The LockBit leak site was initially not as sophisticated as it is today—proof that the LockBit developer has put much effort into improving the site along with improvements to the ransomware code over the years. The below figure of the LockBit Data Leak site is courtesty of id-ransomware.



The LockBit Group has worked hard to improve its services to those who work with them. These efforts have enabled LockBit to remain at the forefront of the ransomware realm in terms of popularity and prevalence.

https://www.fortinet.com/blog/threat-research/lockbit-most-prevalent-ransomware#:~:text=The%20developer%20has%20consistently%20worked,%2C%E2%80%9D%20appeared%20in%20early%202023.