The Rising Threat from LockBit Ransomware

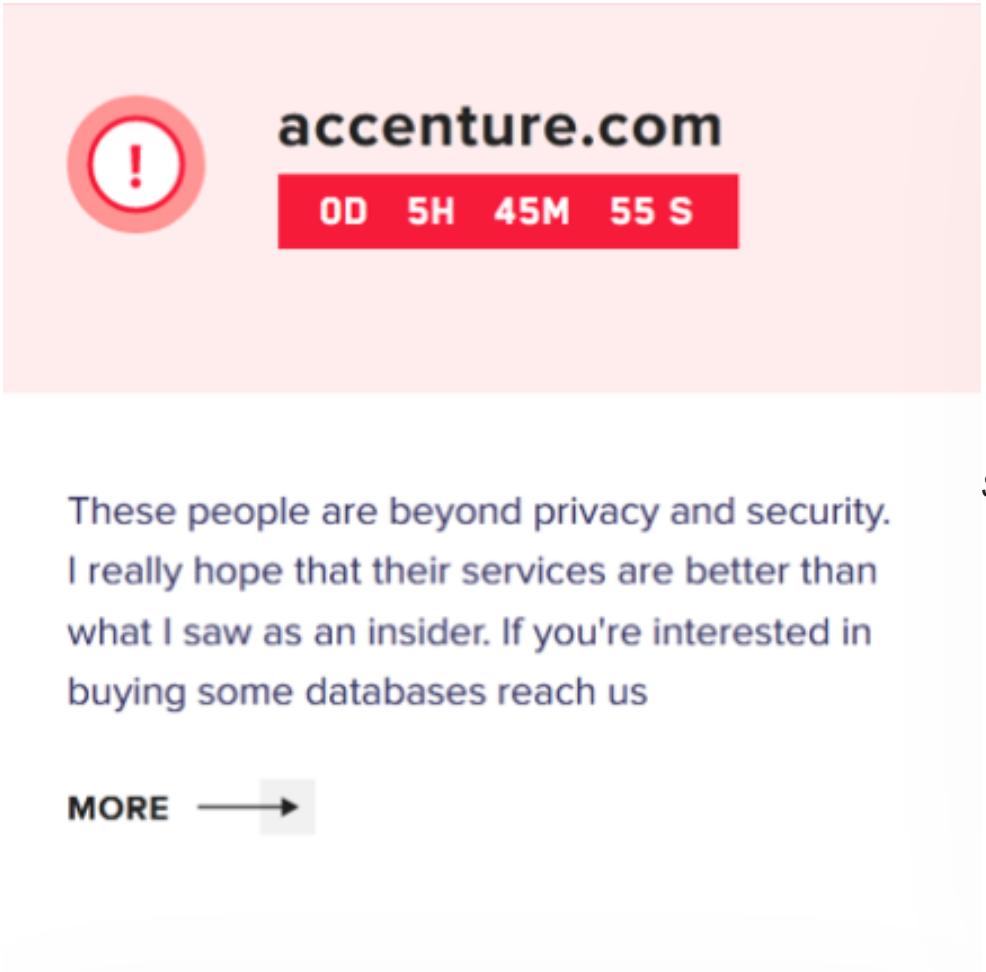
cybereason.com/blog/rising-threat-from-lockbit-ransomware

Written By
Tony Bradley

August 11, 2021 | 3 minute read

LockBit ransomware is the latest threat posing an increased risk for organizations. The ransomware gang has been making headlines recently. LockBit has also reportedly compromised Accenture.

The group reportedly revealed the attack on their site on the DarkWeb, noting: “These people are beyond privacy and security. I really hope that their services are better than what I saw as an insider. If you are interested in buying some databases, reach us.”



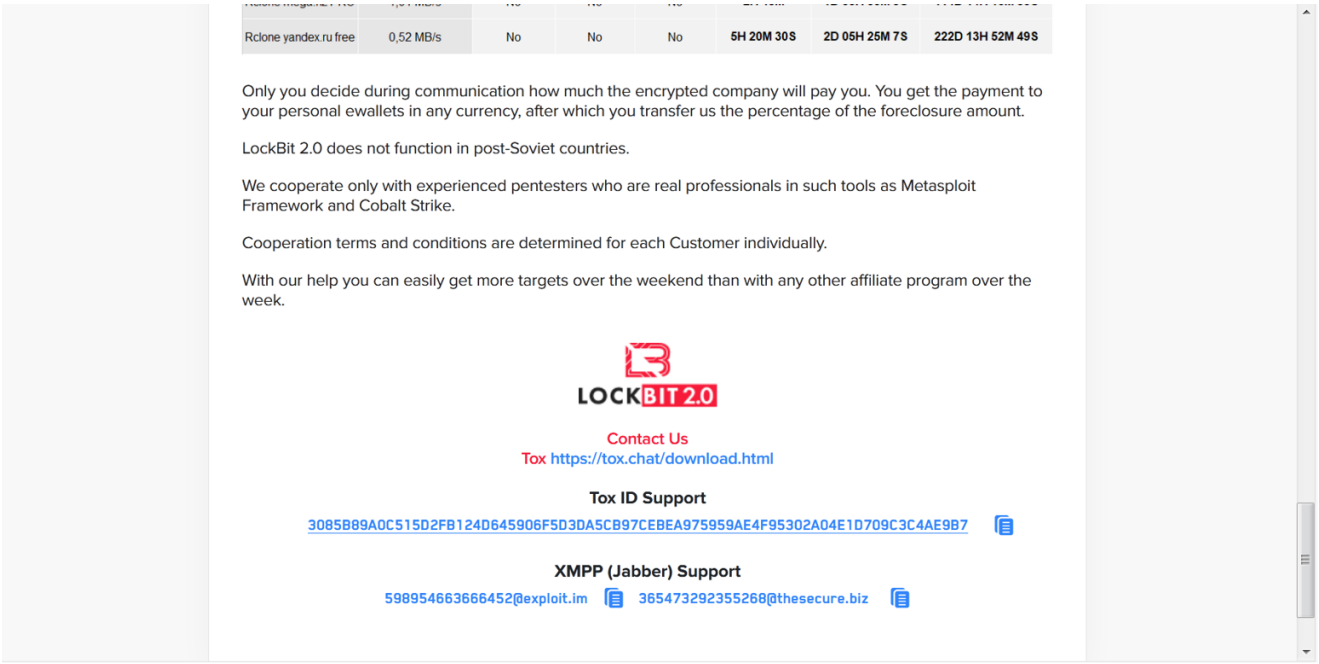
Screenshot from Lockbit site

What Is LockBit?

LockBit is a cybercriminal gang that operates using a ransomware-as-a-service (RaaS) model—similar to DarkSide and REvil. LockBit offers its ransomware platform for other entities or individuals to use based on an affiliate model. Any ransom payments received from using LockBit are divided between the customer directing the attack and the LockBit gang.

LockBit is believed to be related to the LockerGoga and MegaCortex malware families. It shares common tactics, techniques, and procedures (TTPs) with these malicious attacks—particularly the ability to propagate automatically to new targets, being used in targeted

attacks rather than just spamming or attacking organizations indiscriminately, and the underlying tools it relies on, such as Windows PowerShell and Server Message Block (SMB).



Screenshot from Lockbit site

Once a single host is compromised, LockBit can scan the network to locate and infect other accessible devices. It uses tools and protocols that are native to Windows systems—making it more difficult for endpoint security tools to detect or identify the activity as malicious.

The LockBit ransomware continues to adapt and evolve. More recent variants have adopted the double extortion model—locating and exfiltrating valuable data before encrypting systems. The stolen data provides additional incentive for victims to pay the ransom. Even if they can restore data from backups, refusing to pay the ransom may result in sensitive data being published publicly or sold to competitors.

Rising Threat

The LockBit gang has been making headlines recently. In the wake of DarkSide and REvil both shutting down operations, it seems like LockBit may be working to fill the void.

Lawrence Abrams recently reported that the LockBit ransomware gang is actively recruiting insiders to help them breach and encrypt networks. According to Abrams, this may be a shift from the standard ransomware-as-a-service model to cut out the middleman and keep more of the ransom profit for themselves.

The wallpaper displayed on compromised systems now includes text inviting insiders to help compromise systems—promising payouts of millions of dollars.

Protecting against LockBit Ransomware

There is no good option for an organization once a ransomware attack has compromised systems and encrypted data. That is especially true in the case of a double extortion attack. Refusing to pay the ransom means going through a painful process of restoring data from backups and trying to regain control and functionality of your systems while also accepting that your data will likely be exposed.

Paying the ransom may allow the victim to be operational quicker and prevent having data published or sold, but research shows that 80% of companies that pay a ransom end up getting attacked again.

It is important to have effective protection in place to prevent the ransomware attack from getting that far in the first place. Organizations need to have an operation-centric view of the attack. The ability to view the entire malicious operation—or MalOp—and recognize indicators of behavior enables Cybereason to detect and block ransomware attacks and protect against threats like LockBit.

Defending Against Ransomware Attacks

The only way forward for organizations is to prevent an infection from occurring in the first place. To do that, they need to invest in an anti-ransomware solution that doesn't rely on Indicators of Compromise (IOCs), as not every ransomware attack chain is known to the security community. They need a multi-layered platform that uses Indicators of Behavior (IOBs) so that security teams can detect and shut down a ransomware attack chain regardless of whether anyone's seen it before.

The Cybereason Operation-Centric approach means no data filtering and the ability to detect attacks earlier based on rare or advantageous chains of (otherwise normal) behaviors. Cybereason is undefeated in the battle against ransomware thanks to our multi-layered prevention, detection and response, which includes:

- **Anti ransomware prevention and deception:** Cybereason uses a combination of behavioral detections and proprietary deception techniques surface the most complex ransomware threats and end the attack before any critical data can be encrypted.
- **Intelligence-Based Antivirus:** Cybereason blocks known ransomware variants leveraging an ever-growing pool of threat intelligence based on previously detected attacks.
- **NGAV:** Cybereason NGAV is powered by machine learning and recognizes malicious components in code to block unknown ransomware variants prior to execution.
- **Fileless Ransomware Protection:** Cybereason disrupts attacks utilizing fileless and MBR-based ransomware that traditional antivirus tools miss.
- **Endpoint Controls:** Cybereason hardens endpoints against attacks by managing security policies, maintaining device controls, implementing personal firewalls and enforcing whole-disk encryption across a range of device types, both fixed and mobile.
- **Behavioral Document Protection:** Cybereason detects and blocks ransomware hidden in the most common business document formats, including those that leverage malicious macros and other stealthy attack vectors.

Cybereason is dedicated to teaming with defenders to end cyber attacks from endpoints to the enterprise to everywhere - including modern ransomware. Learn more about ransomware defense here or schedule a demo today to learn how your organization can benefit from an operation-centric approach to security.

About the Author

Tony Bradley

Tony Bradley has a passion for technology and gadgets, and a desire to help others understand how technology can affect or improve their lives. In addition to writing and editing for Cybereason's Malicious Life, Tony is a regular contributor to Forbes, DevOps.com, and ContainerJournal. He is an experienced information security professional, speaker, author / co-author of 10 books and thousands of web and print articles. He was awarded the Microsoft MVP (Most Valuable Professional) award for 11 consecutive years, and I've been a CISSP (Certified Information Systems Security Professional) since 2002.

All Posts by Tony Bradley