LockBit ransomware - what you need to know

Archived: 2026-04-05 19:40:38 UTC

I keep hearing about LockBit ransomware attacks. What's going on?

It's no surprise if you have heard about LockBit. It is the world's most active ransomware group - responsible for an estimated 40% of all ransomware infections worldwide.

I guess LockBit does the usual bad stuff - encrypt your data, steal your files, dump a ransom note on your PC...

Yes. The first you might know that you've been hit by LockBit 3.0 (also known as LockBit Black) is when your desktop wallpaper is replaced with a message telling you that your files have been stolen, and pointing to instructions on how they can be recovered.

You are then encouraged to make contact via the dark web to negotiate your ransom payment.

Yuck. Are the LockBit attacks targeting any type of businesses in particular?

LockBit's victims are primarily small and medium-sized businesses, but sometimes much larger organisations have fallen foul.

LockBit's high profile targets have in the past included tech manufacturer Foxconn, NHS vendor Advanced, IT giant Accenture, and German autoparts company Continental.

Most recently the UK Royal Mail's deliveries overseas were disrupted following what is believed to have been a LockBit ransomware attack.

Yoinks. It sounds like any business could be a potential target...

Not quite. LockBit doesn't seem to have been launched against any Russian organisations, for instance.

Why no Russian victims?

Hmm... why do you think?

Ha, I get it. They don't want to get in trouble with the cops on their doorstep! I guess if they are hitting so many companies, these LockBit guys must be making a lot of money

When the US authorities charged a man in connection with the LockBit ransomware in November 2022, they claimed that it had been deployed against at least 1,000 victims in the United States and around the world, making at least $100 million worth of ransom demands.

Oh, so they've already nabbed someone for LockBit?

It's not as simple as that. It's not just one guy launching LockBit attacks from his back bedroom, surrounded by pizza boxes.

LockBit is a ransomware-as-a-service (RaaS) operation, meaning that other criminals pay to become an affiliate, launching attacks and sharing a percentage of their earnings with the original LockBit gang.

Identifying and charging one LockBit suspect does not necessarily mean the downfall of the entire criminal operation.

And so, different people could be responsible for different LockBit attacks...

Correct. For instance, the Royal Mail attack has been blamed by the gang on a LockBit affiliate.

It sounds like LockBit is quite a professional enterprise...

Yes, albeit a criminal enterprise.

The LockBit ransomware-as-service operation has certainly evolved over the last couple of years. One of the more unusual developments occurred last summer when the gang announced it was introducing a bug bounty program.

A bug bounty? You're kidding me...

In what was said to be the first ever bug bounty run by a ransomware gang, LockBit offered between $1000 and $1 million for anyone submitting bug reports. The gang cheekily announced that it was inviting "all security researchers, ethical and unethical hackers on the planet to participate."

In addition, the LockBit group said they would pay out for "brilliant ideas" that would improve their criminal operations.

Of course, helping cybercriminals might be frowned upon in your particular country, so think carefully before you get into bed with them.

Thanks. I wasn't planning to.

One other thing. LockBit also offers a way for you to earn "exactly one million dollars, no more and no less..." in cryptocurrency for doxxing the individual known as LockBitSupp, who provides support and administers the group's affiliates.

Perhaps they are hoping that any cybercriminal investigator who manages to uncover the identities of key individuals running LockBit will be tempted to tell the gang for a payout, rather than help the police.

So how can my company protect itself from the LockBit ransomware?

Once again, it comes down to following tried-and-trusted security practices:

- make secure offsite backups.
- run up-to-date security solutions. Ensure that your computers are configured properly, and protected with the latest security patches against vulnerabilities.

- use hard-to-crack, unique passwords to protect sensitive data and accounts, and enable multi-factor authentication.
- encrypt sensitive data wherever possible.
- educate and inform staff about the risks and methods used by cybercriminals to launch attacks and steal data.

Editor's Note: ***The opinions expressed in this guest author article are solely those of the contributor, and do not necessarily reflect those of Tripwire, Inc.***
