LockBit ransomware launches data leak site to double-extort victims

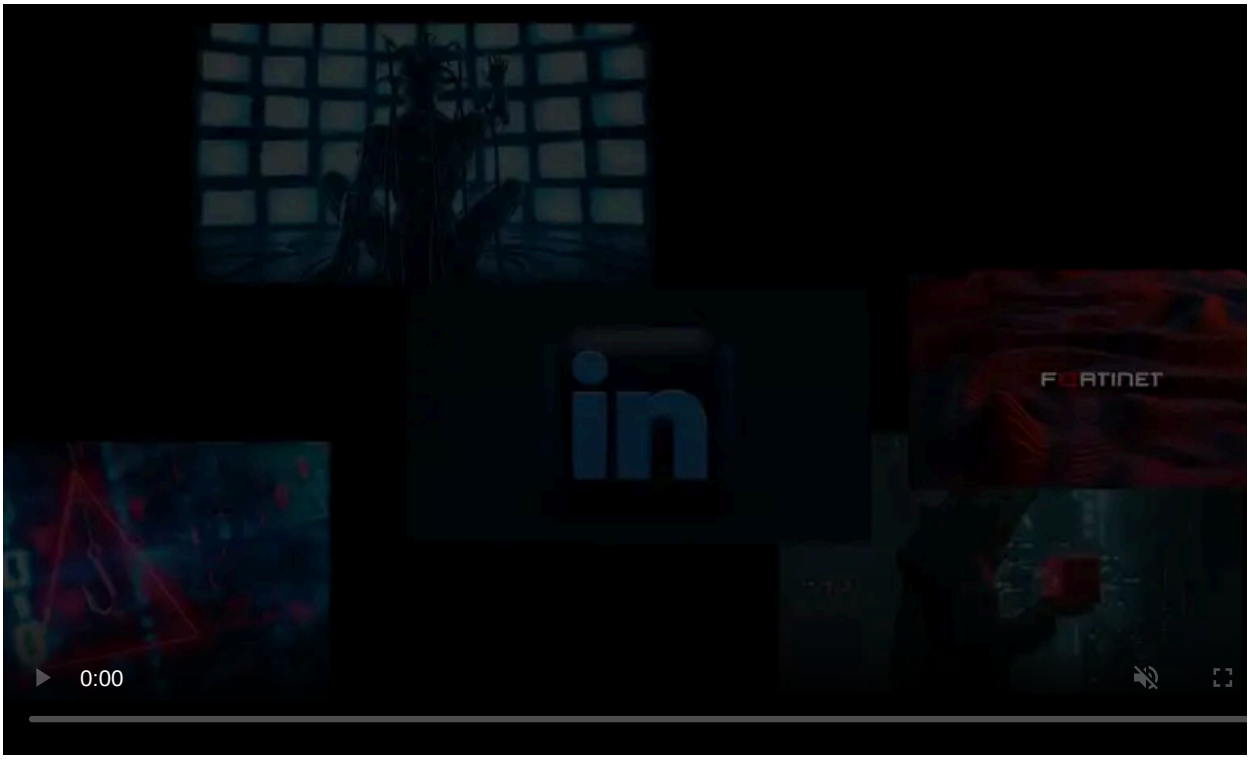
By Lawrence Abrams

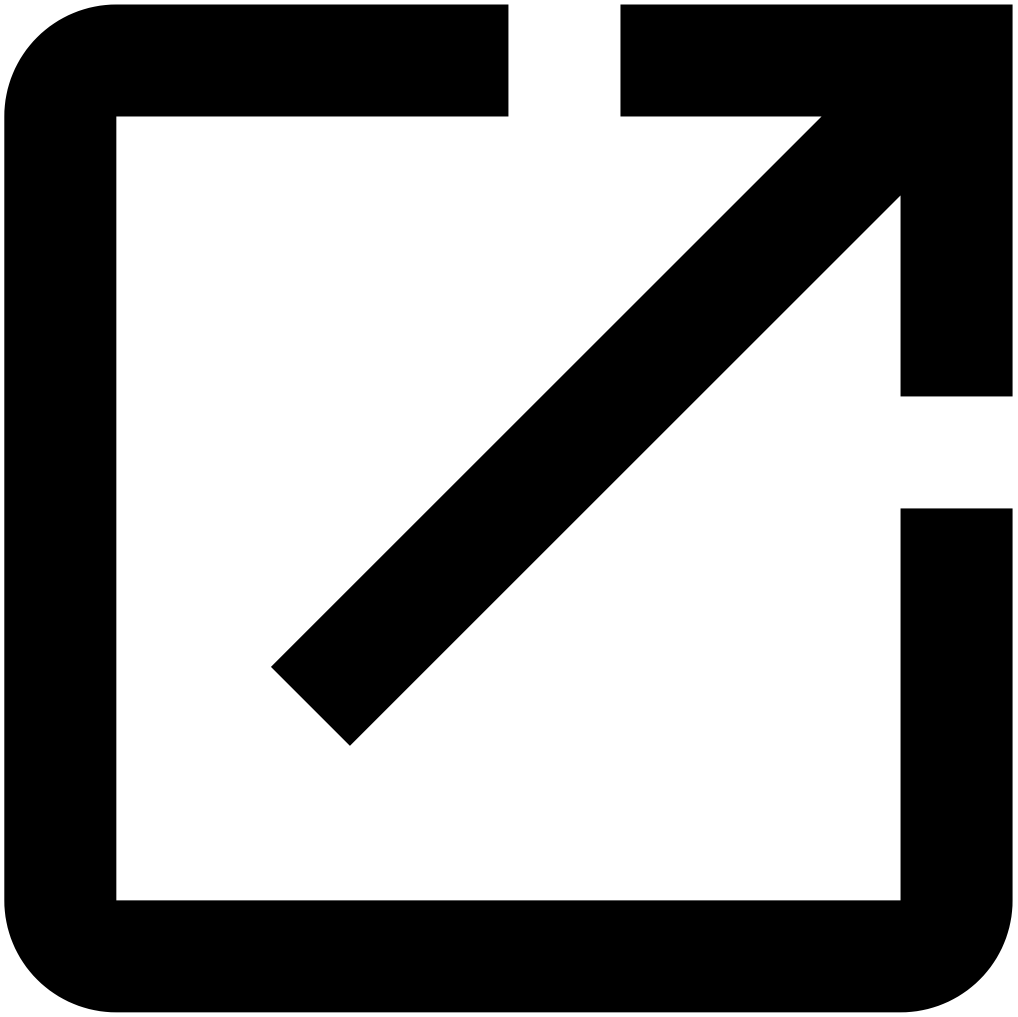
Published: 2020-09-16 · Archived: 2026-04-05 19:16:05 UTC

The LockBit ransomware gang has launched a new data leak site to be used as part of their double extortion strategy to scare victims into paying a ransom.

Since the end of 2019, ransomware gangs have adopted a double extortion tactic of stealing unencrypted files before encrypting the computers on a network.

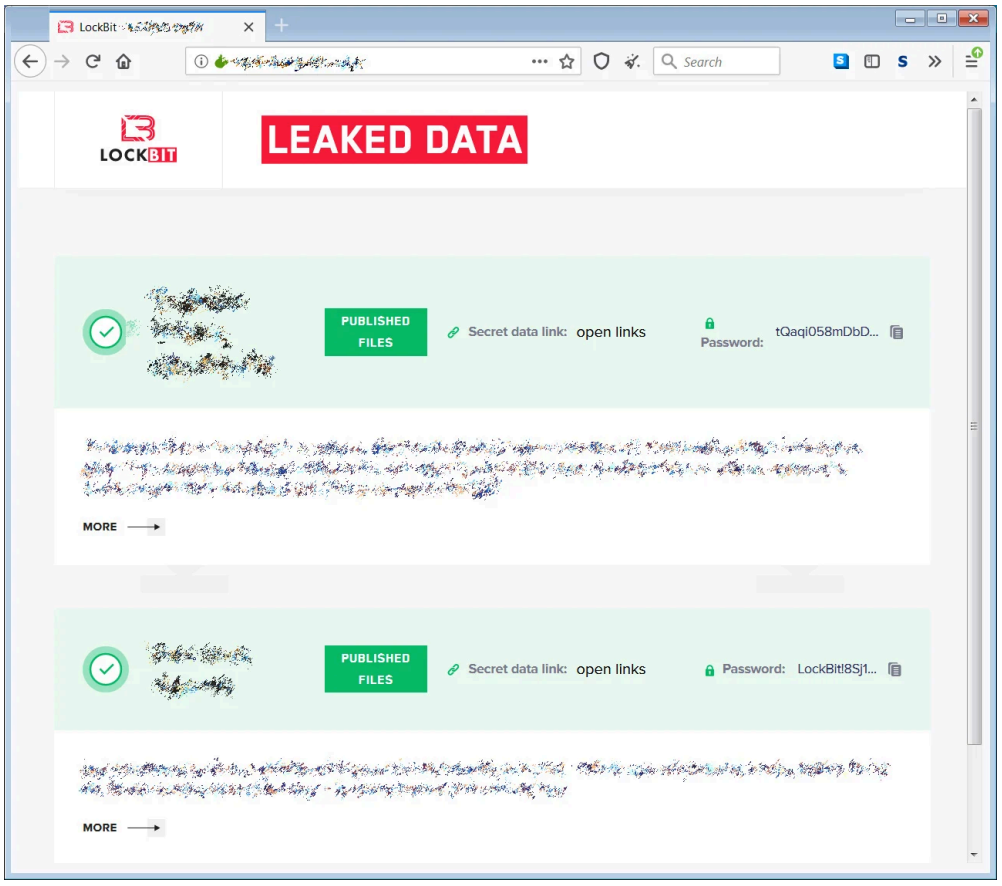
The ransomware gangs then use the stolen files and the threat that they will be publicly released on data leak sites as leverage to get victims to pay a ransom.


0:00



Lockbit data leak site

According to cybersecurity intelligence firm Kela, the LockBit ransomware operation posted a link yesterday on a Russian-speaking hacker forum to their new data leak site.



LockBit data leak site

The data leak site currently contains two victims; an automation parts manufacturer and a shipping company.

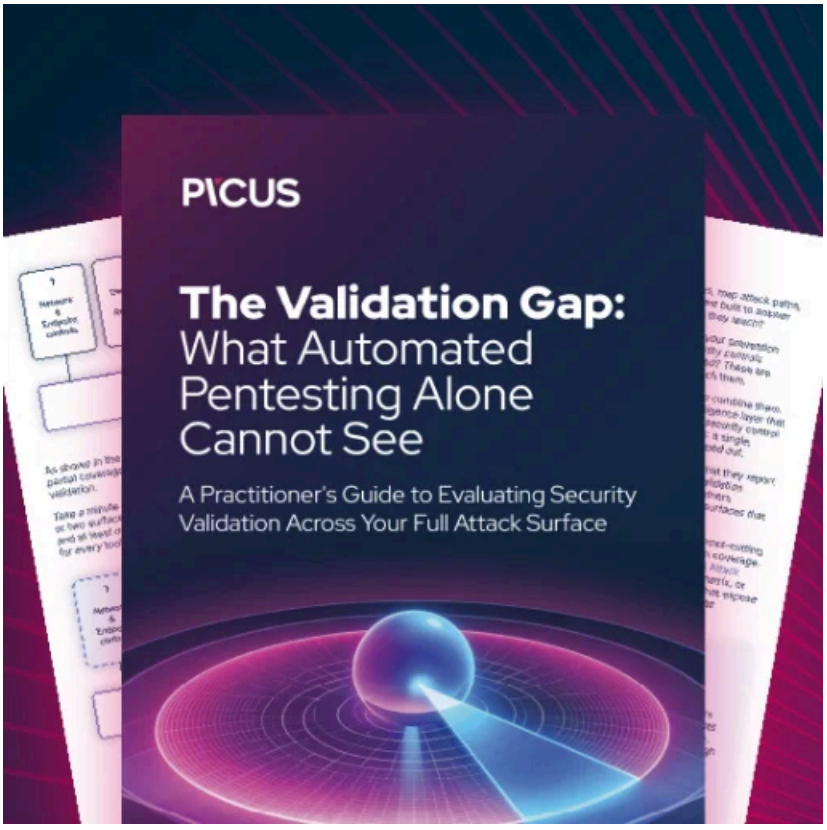
LockBit had previously launched a leak site but shut it down around the time they joined the 'Maze Cartel,' and started using Maze's site to publish stolen files

With the release of their data leak site, it is unknown if they are breaking away from this 'cartel' or just want a dedicated site under their control.

All ransomware attacks must be considered data breaches as the ransomware operators not only steal the data but also sift through documents to see what they contain.

Due to this, companies need to be transparent about attacks so that employees and customers can adequately protect themselves from the risk of exposed data.

With the release of LockBit's site, there are now a total of seventeen ransomware data leak sites used in the double extortion tactic.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/lockbit-ransomware-launches-data-leak-site-to-double-extort-victims/