Darktrace: Investigation found no evidence of LockBit breach

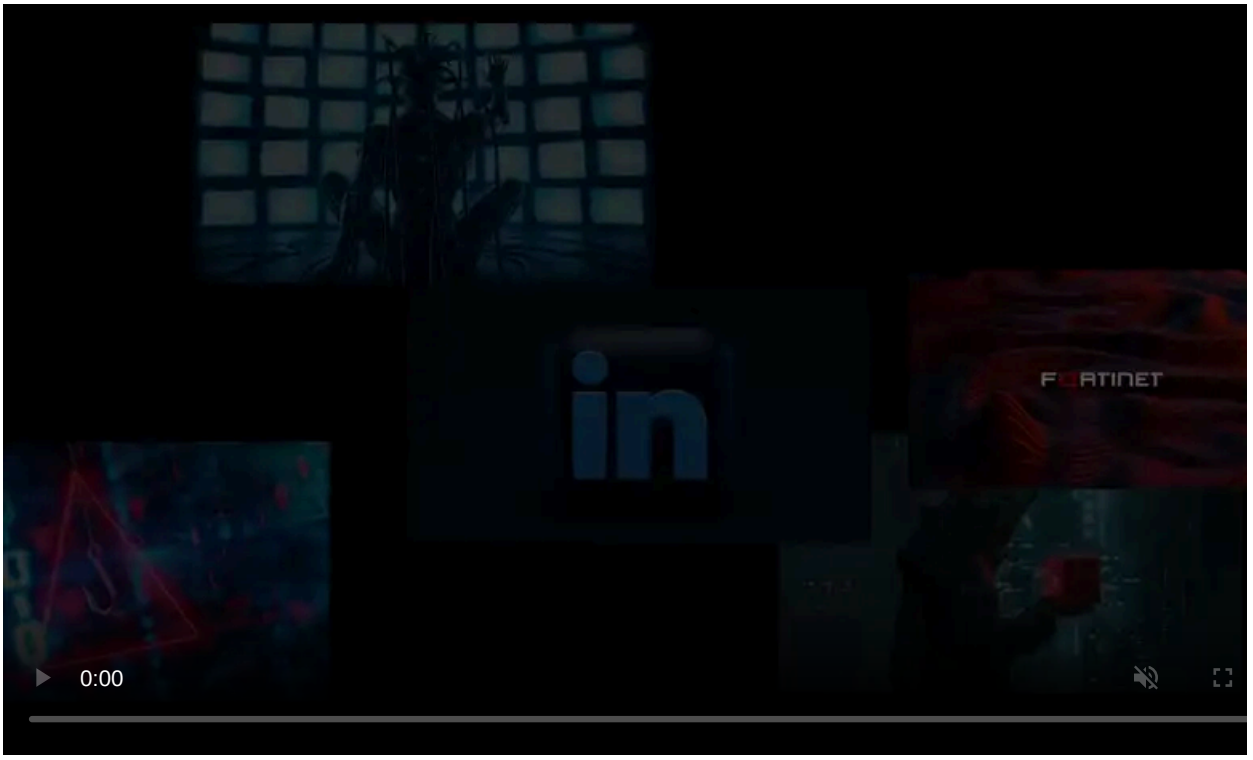
By Sergiu Gatlan

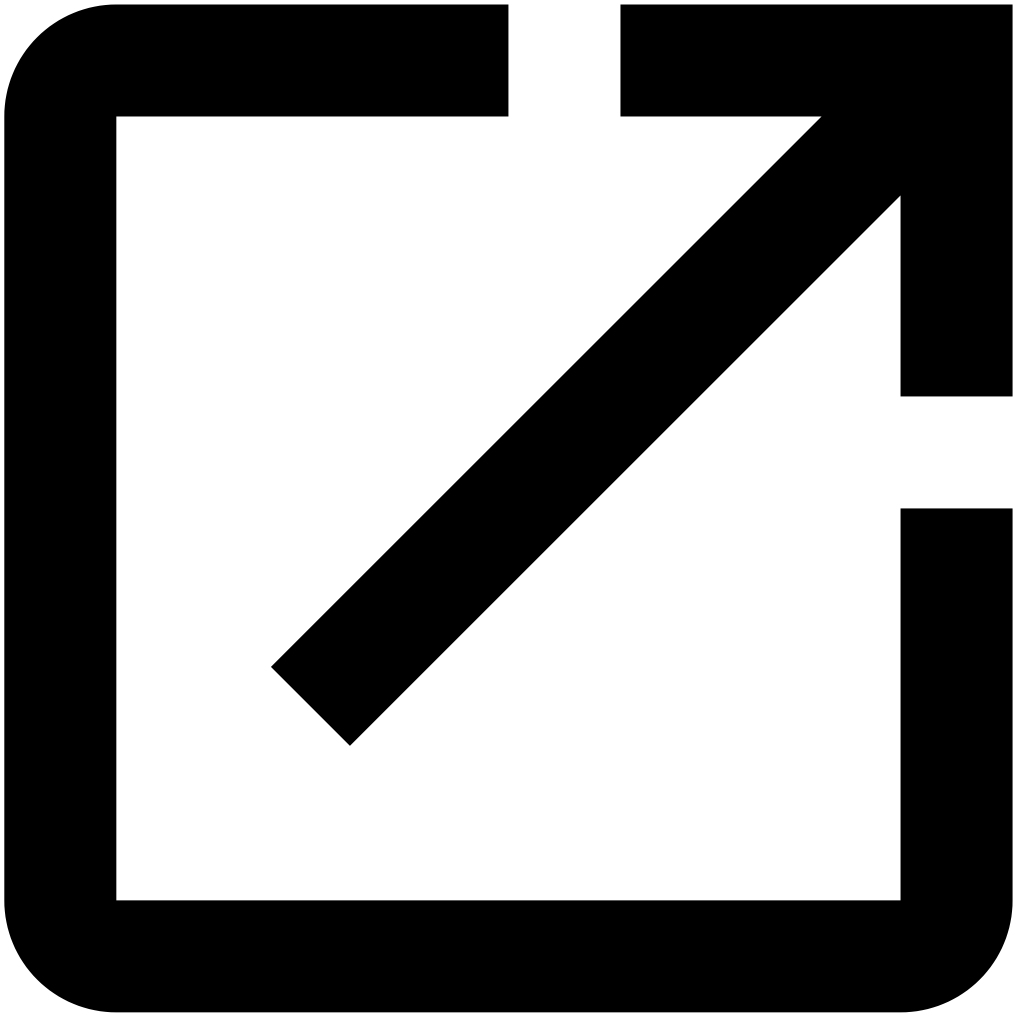
Published: 2023-04-14 · Archived: 2026-04-05 19:27:22 UTC

Cybersecurity firm Darktrace says it found no evidence that the LockBit ransomware gang breached its network after the group added an entry to their dark web leak platform, implying that they stole data from the company's systems.

Hours after the gang claimed DarkTrace as a victim on their data leak site, the company conducted an investigation and found no evidence of a breach of their systems.

"Our security teams have run a full review of our internal systems and can see no evidence of compromise," Darktrace said.


0:00



On Friday, the company's Chief Information Security Officer Mike Beck reiterated the same conclusion after a thorough investigation of their systems.

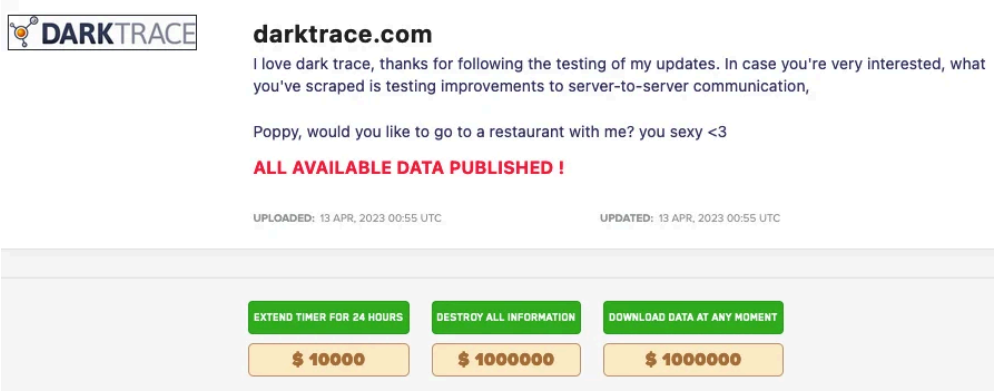
"We have completed a thorough security investigation following yesterday's tweets by LockBit claiming they had compromised Darktrace's internal systems," said Beck.

"We can confirm that there has been no compromise of our systems or any of our affiliate systems. Our service to our customers remains uninterrupted and is operating as normal and no further action is required."

It is now apparent that LockBit messed up, confusing Darktrace with threat intelligence company DarkTracer which tweeted about the gang's leak site being flooded with fake victims.

"The reliability of the RaaS service operated by LockBit ransomware gang seems to have declined," DarkTracer said.

"They appear to have become negligent in managing the service, as fake victims and meaningless data have begun to fill the list, which is being left unattended."



LockBit Darktrace fake leak (BleepingComputer)

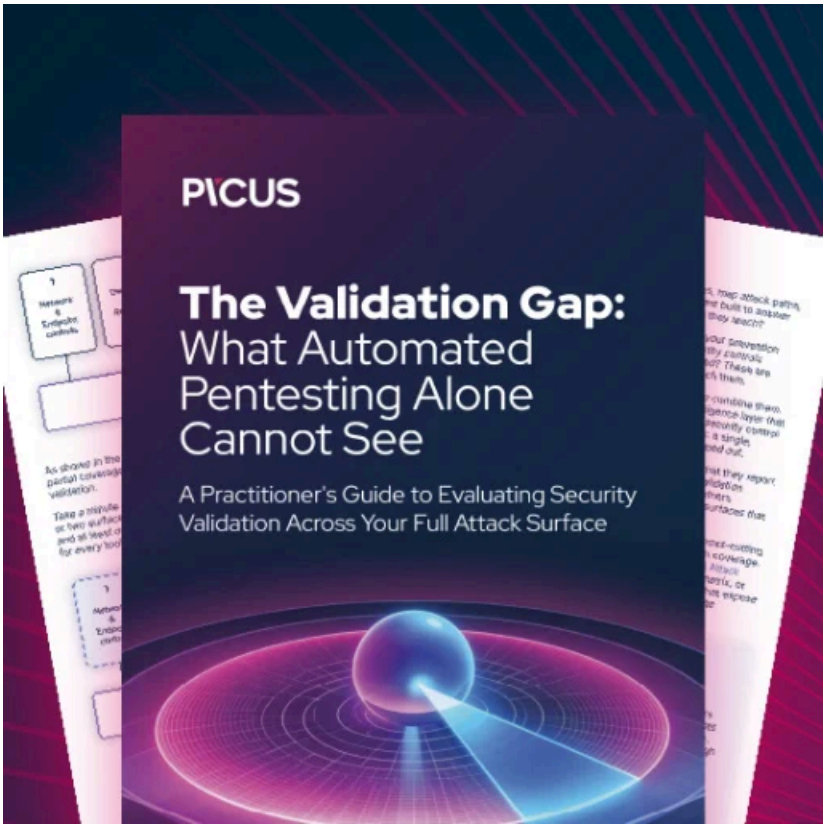
This is not the first time LockBit claimed they'd breached a cybersecurity company's systems by mistake or intentionally.

Last year, in June, the ransomware gang also added Mandiant to their leak website, saying that more than 350,000 files they had allegedly stolen would be published.

However, as it happened with Darktrace, Mandiant told BleepingComputer that it hadn't found any evidence of a breach.

In the end, LockBit's claims that they hacked Mandiant proved to be nothing more than a feeble attempt to distance the operation from the Evil Corp cybercrime gang following a Mandiant report linking the two after Evil Corp switched to deploying LockBit ransomware in their attacks to evade U.S. sanctions.

Unlike this week, when Darktrace was listed as a victim because of confusion, Mandiant being tagged as a victim was prompted by LockBit's fears of lost revenue if victims stopped paying ransoms since the U.S. government sanctioned Evil Corp in December 2019.



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/darktrace-investigation-found-no-evidence-of-lockbit-breach/