Mandiant: “No evidence” we were hacked by LockBit ransomware

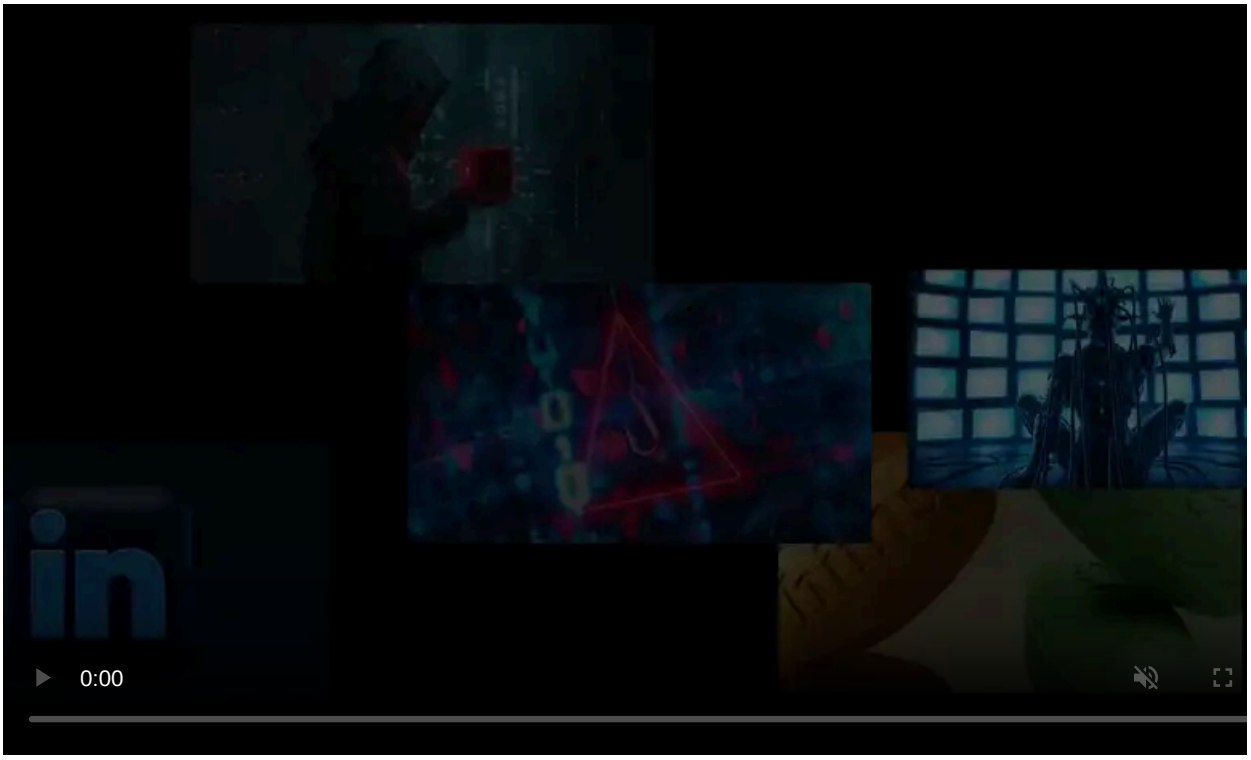
By Sergiu Gatlan

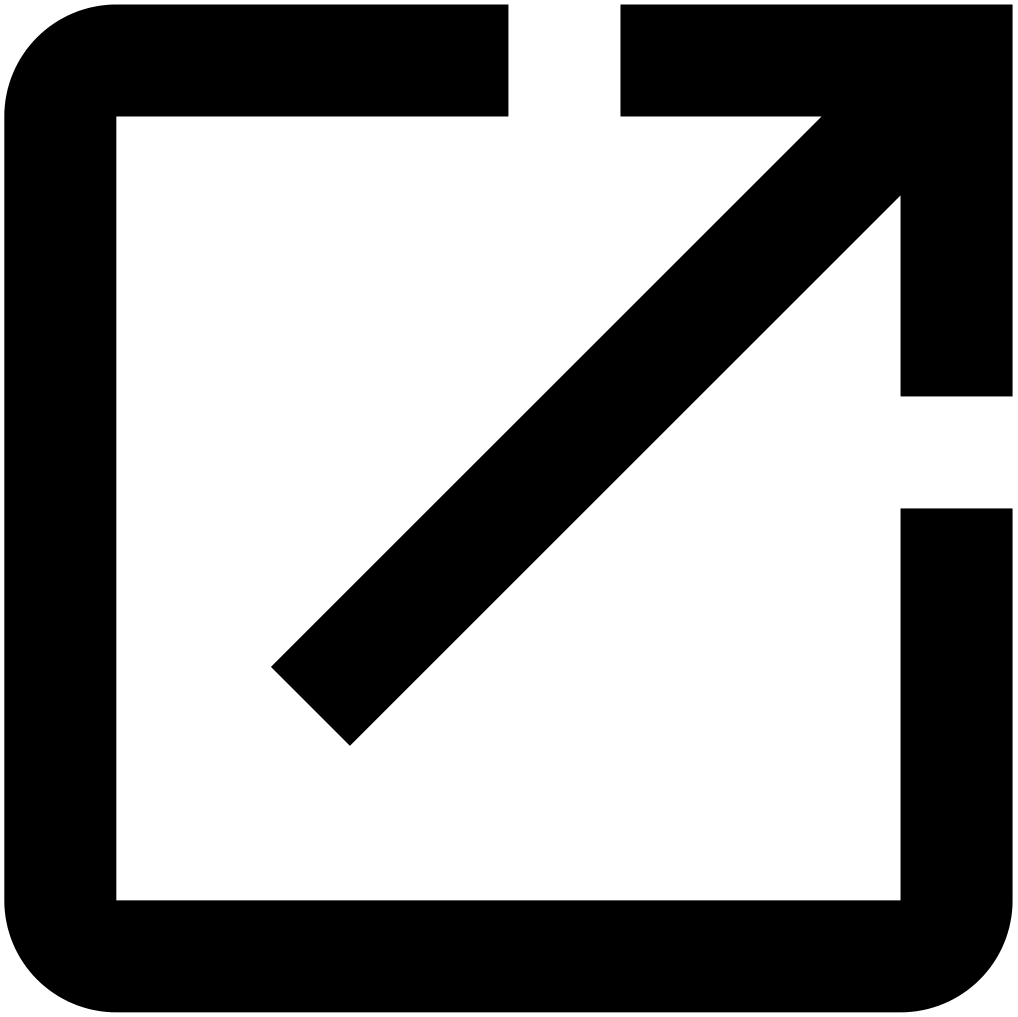
Published: 2022-06-06 · Archived: 2026-04-05 17:32:46 UTC

American cybersecurity firm Mandiant is investigating LockBit ransomware gang's claims that they hacked the company's network and stole data.

The ransomware group published a new page on its data leak website earlier today, saying that the 356,841 files they allegedly stole from Mandiant will be leaked online.

"All available data will be published!" the gang's dark web leak site threatens under a timer showing just under three hours left until the countdown ends.


0:00



LockBit has yet to reveal what files it claims to have stolen from Mandiant's systems since the file listing on the leak page is empty.

However, the page displays a 0-byte file named 'mandiantyellowpress.com.7z' that appears to be related to a mandiantyellowpress[.]com domain (registered today). Visiting this page redirects to the ninjaflex[.]com site.

When BleepingComputer reached out for more details on LockBit's claims, the threat intel firm said it hadn't yet found evidence of a breach.

"Mandiant is aware of these LockBit-associated claims. At this point, we do not have any evidence to support their claims. We will continue to monitor the situation as it develops," Mark Karayan, Mandiant's Senior Manager for Marketing Communications, told BleepingComputer.

These claims come after Mandiant revealed in a report published last week that the Russian Evil Corp cybercrime group has now switched to deploying LockBit ransomware on targets' networks to evade U.S. sanctions.

Mandiant announced in March that it entered into a definitive agreement to be acquired by Google in an all-cash transaction valued at roughly $5.4 billion.

The LockBit ransomware gang has been active since September 2019 as a ransomware-as-a-service (RaaS) and relaunched as the LockBit 2.0 RaaS in June 2021 after ransomware actors were banned from posting on cybercrime forums [1, 2].

Accenture, a Fortune 500 company and one of LockBit's victims, confirmed to BleepingComputer in August 2021 that it was breached after the gang asked for a $50 million ransom not to leak data stolen from its network.

In February, the FBI released a flash alert with technical details and indicators of compromise associated with LockBit ransomware attacks, asking companies targeted by this RaaS' affiliates to urgently report incidents to their local FBI Cyber Squad.

As cybersecurity company Sophos reported in April, a LockBit affiliate lurked around the network of a U.S. local government agency for months before deploying the ransomware payload.

Update: After LockBit published the files, it looks like this wasn't about files stolen from Mandiant's network but, instead, about the ransomware group trying to distance itself from the Evil Corp cybercrime gang.

This was likely prompted by LockBit fearing the lost revenue because their victims will stop paying ransoms as Evil Corp is sanctioned by the U.S. government.

> I was very surprised to read the news on Twitter from the yellow press. mandiant.com are not professional. Any scripts and tools for attacks, are publicly available and can be used by any hacker on the planet, most of the attack methods are on the forums, github and google, the fact that someone uses similar tools can not be proof that the attack is done by the same person.
>
> Our group has nothing to do with Evil Corp. We are real underground darknet hackers, we have nothing to do with politics or special services like FSB, FBI and so on.

mandiant.com

Mandiant is on a mission to make every organization secure from cyber threats and confident in their readiness. We deliver dynamic cyber defense solutions powered by industry-leading expertise, intelligence and innovative technology. Get Started arrow_forward EVENT Mandiant Worldwide Information Security Exchange (mWISE)

ALL AVAILABLE DATA PUBLISHED !

RETURN BACK

NAME	DATE	SIZE
foxconfortwitter.7z	6.Jun.2022	2.34MB
mandiantyellowpress.com.txt	6.Jun.2022	1.45kB

"Mandiant has reviewed the data disclosed in the initial LockBit release. Based on the data that has been released, there are no indications that Mandiant data has been disclosed but rather the actor appears to be trying to disprove Mandiant's June 2nd, 2022 research blog on UNC2165 and LockBit," Mandiant's Karayan told BleepingComputer.

Source: https://www.bleepingcomputer.com/news/security/mandiant-no-evidence-we-were-hacked-by-lockbit-ransomware/