

Foxconn confirms ransomware attack disrupted production in Mexico

By Bill Toulas

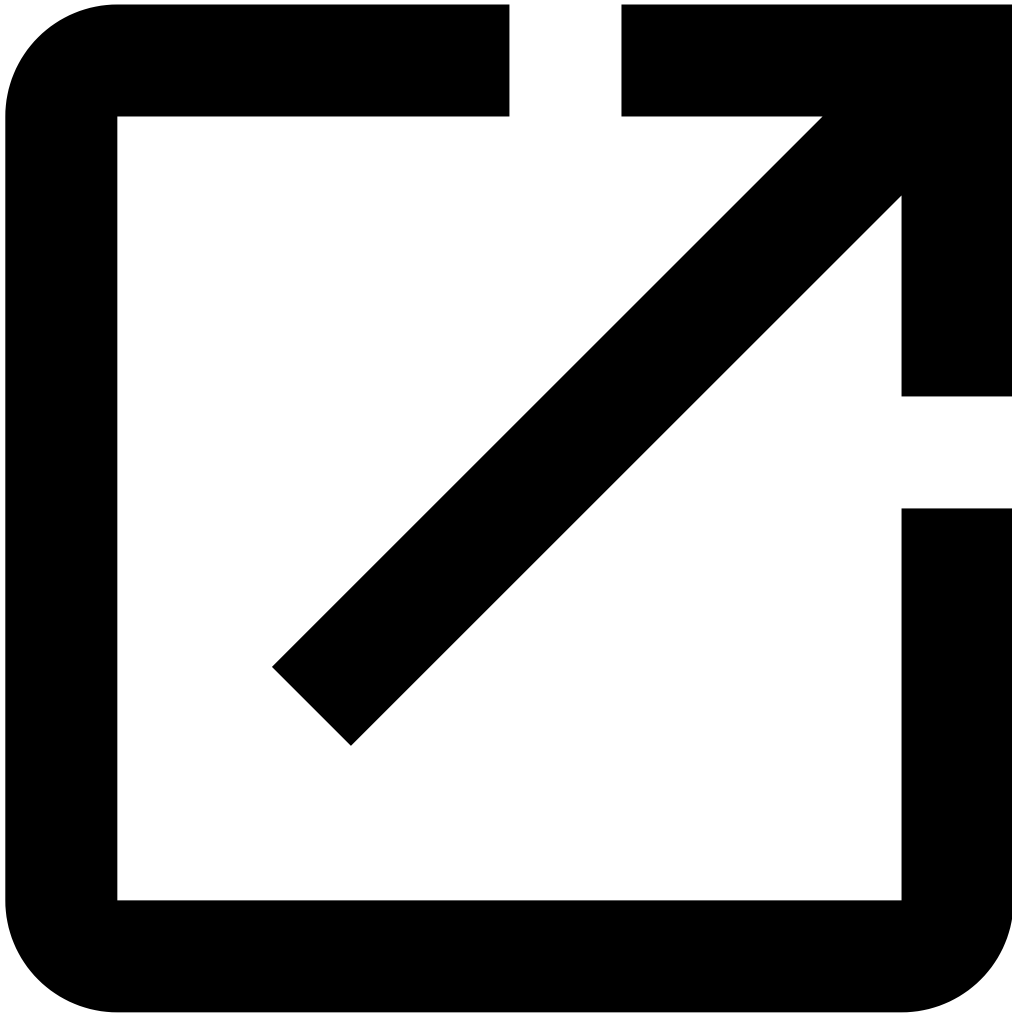
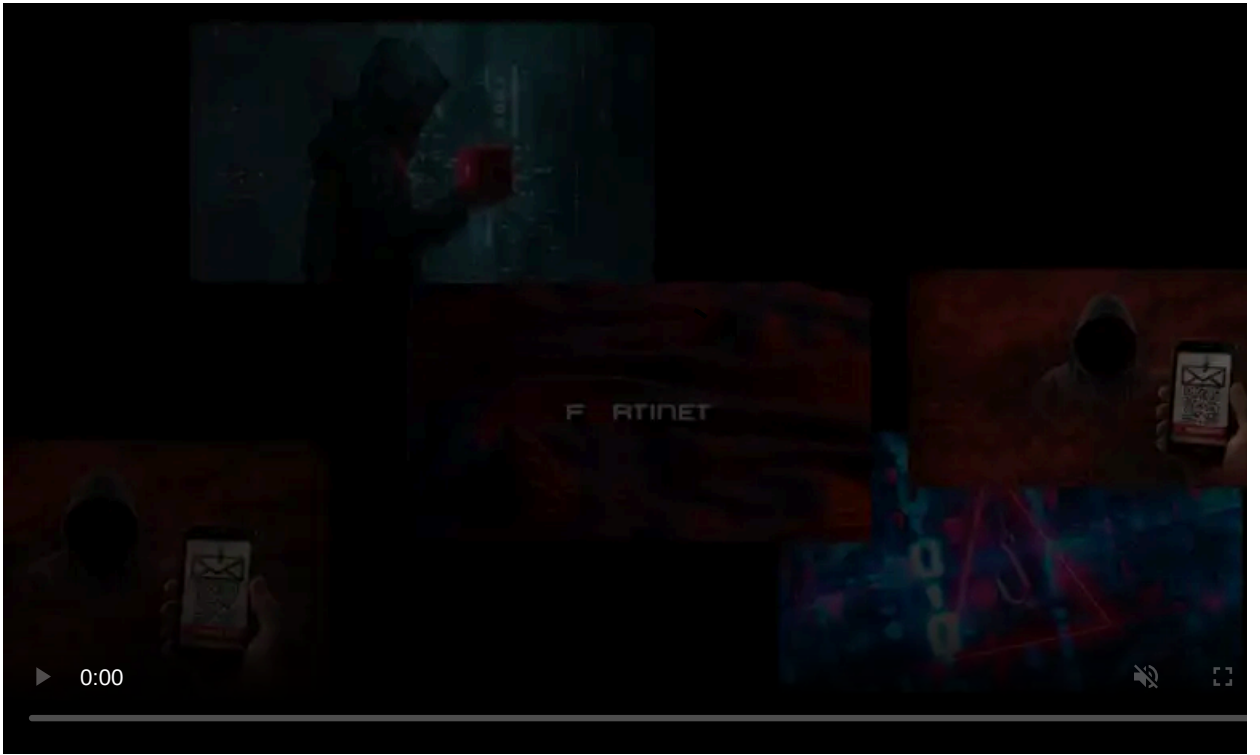
Published: 2022-06-02 · Archived: 2026-04-05 21:44:57 UTC



Foxconn electronics manufacturer has confirmed that one of its Mexico-based production plants has been impacted by a ransomware attack in late May.

The company did not provide any info on the group responsible for the attack but operators of the LockBit ransomware gang claimed responsibility.

Foxconn operates three facilities in Mexico, which produce computers, LCD TVs, mobile devices, and set-top boxes, formerly used by Sony, Motorola, and Cisco Systems.



Visit Advertiser website [GO TO PAGE](#)

The attacked Foxconn factory is located in Tijuana, Mexico, and is considered a strategic facility that acts a critical supply hub for the U.S. state of California, a significant electronics consumer.

In a statement to BleepingComputer, Foxconn has assured that the impact on its overall operations will be minimal, and the recovery will unfold according to a pre-determined plan. A company spokesperson provided the following comment:

"It is confirmed that one of our factories in Mexico experienced a ransomware cyberattack in late May. The company's cybersecurity team has been carrying out the recovery plan accordingly.

The factory is gradually returning to normal. The disruption caused to business operations will be handled through production capacity adjustment. The cybersecurity attack is estimated to have little impact on the Group's overall operations. Relevant information about the incident is also provided instantly to our management, clients, and suppliers." - Foxconn

LockBit strikes

LockBit ransomware operation claimed the attack on May 31 by publishing a threat to leak data stolen from Foxconn unless a ransom is paid by June 11.

LOCKBIT 2.0 **LEAKED DATA** **CONDITIONS FOR PARTNERS AND CONTACTS**

UNTIL FILES
10D 07:19:03
PUBLICATION

11 Jun, 2022 18:01:00

foxconnbc.com
foxconnbc.com Foxconn Baja California is located in the city of Tijuana, on the border with San Diego, California, this being a strategic geographical point in the reception and distribution of materials, as well as a commercial relationship between both countries

ALL AVAILABLE DATA WILL BE PUBLISHED !

LockBit claiming Foxconn as victim (KELA)

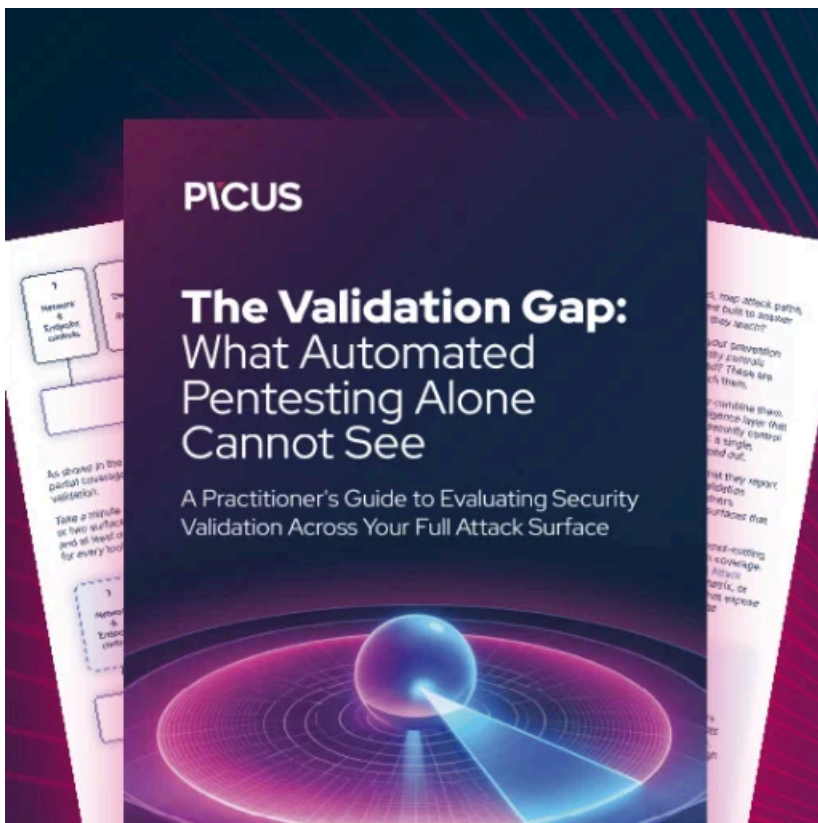
This means that negotiations may not be completely over and the cybercriminals still hope to come to an agreement with the company. LockBit's demands remain unknown at the moment but they are likely to be quite large, given that the gang typically targets successful companies that can pay larger ransoms.

The attacker has not given any hint about the data they hold but they usually look to exfiltrate valuable information that could be used as leverage for the victim to pay.

Since Foxconn produces various consumer electronic products for many brands, LockBit might hold valuable schematics and technical drawings that constitute intellectual property shared under non-disclosure agreements.

Foxconn's factory in Tijuana is the second one hit by a ransomware attack in less than two years. In December 2020, the DoppelPaymer ransomware group announced that it hit the company's CTBG MX facility in Ciudad Juárez.

The attackers asked for a [\\$34 million ransom](#) and claimed to have stolen 100GB of data, encrypted between 1,200 and 1,400 servers and destroyed 20 to 30TB of backup data.



[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/foxconn-confirms-ransomware-attack-disrupted-production-in-mexico/>