Foxconn electronics giant hit by ransomware, $34 million ransom

bleepingcomputer.com/news/security/foxconn-electronics-giant-hit-by-ransomware-34-million-ransom/

Lawrence Abrams

By
Lawrence Abrams

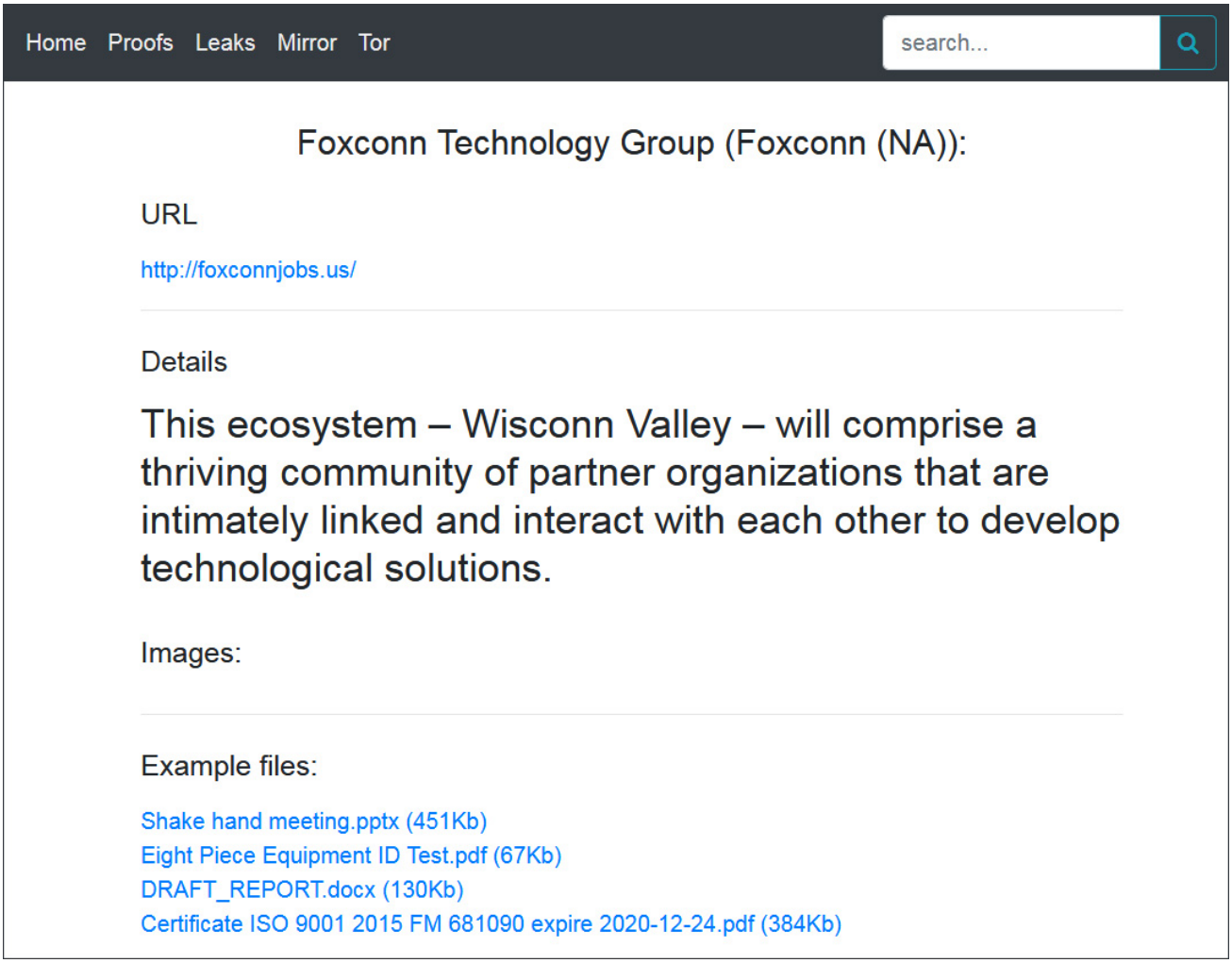
- December 7, 2020
- 01:01 PM
- 0

Foxconn electronics giant suffered a ransomware attack at a Mexican facility over the Thanksgiving weekend, where attackers stole unencrypted files before encrypting devices.

Foxconn is the largest electronics manufacturing company globally, with recorded revenue of $172 billion in 2019 and over 800,000 employees worldwide. Foxconn subsidiaries include Sharp Corporation, Innolux, FIH Mobile, and Belkin.

BleepingComputer has been tracking a rumored Foxconn ransomware attack that occurred over the Thanksgiving weekend.

Today, the DoppelPaymer ransomware published files belonging to Foxconn NA on their ransomware data leak site. The leaked data includes generic business documents and reports but does not contain any financial information or employee's personal details.



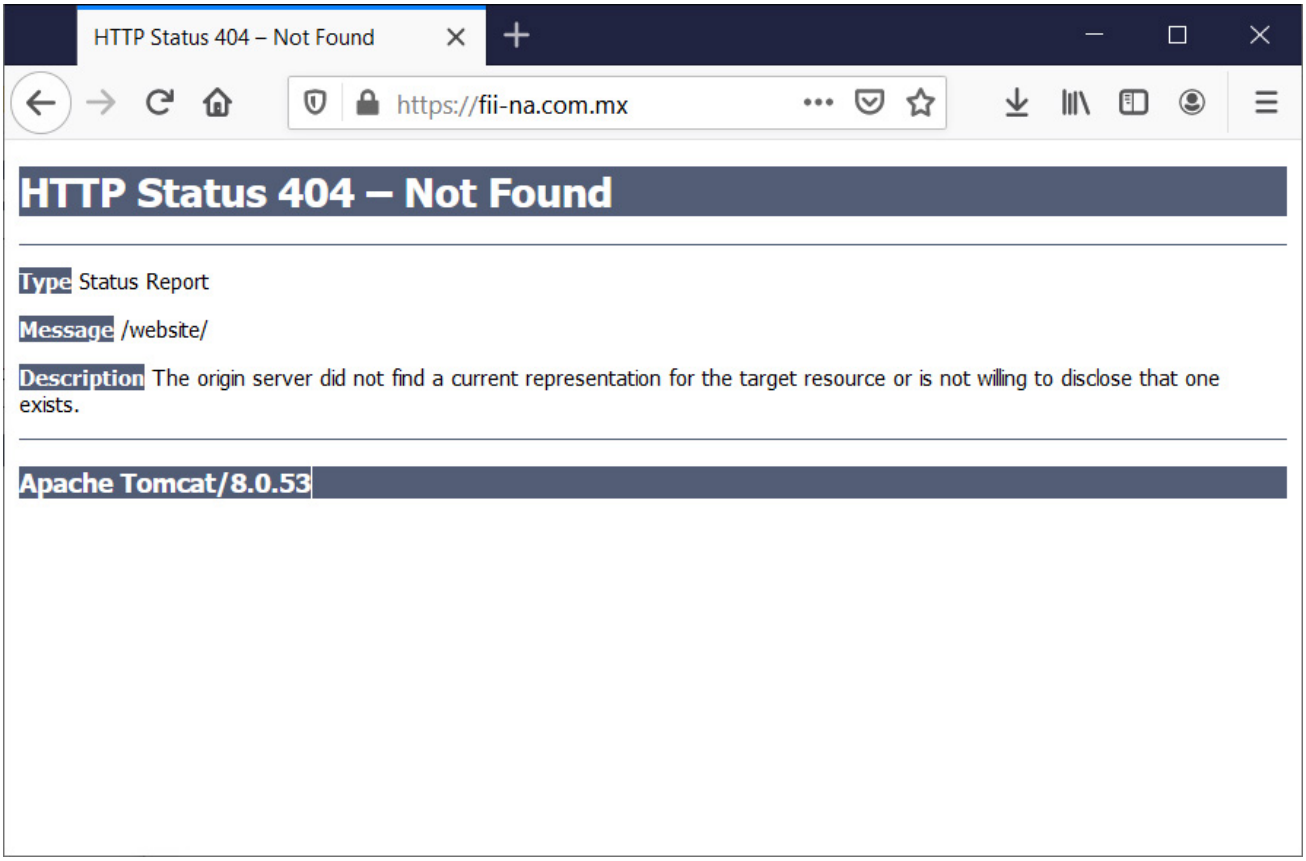
DoppelPaymer ransomware data leak site

Sources in the cybersecurity industry have confirmed that Foxconn suffered an attack around November 29th, 2020, at their Foxconn CTBG MX facility located in Ciudad Juárez, Mexico.

This facility opened in 2005 and is used by Foxconn for assembly and shipping of electronics equipment to all regions in South and North America.

"Our 682,000 square ft building was established back in 2005, and is located in Ciudad Juárez, Chihuahua, Mexico, just across the border from El Paso, Texas. [..] Foxconn CTBG MX is strategically located to support all Americas region," the Foxconn CTBG MX web page describes the facility.

Since the attack, the facility's web site has been down and currently shows an error to visitors.

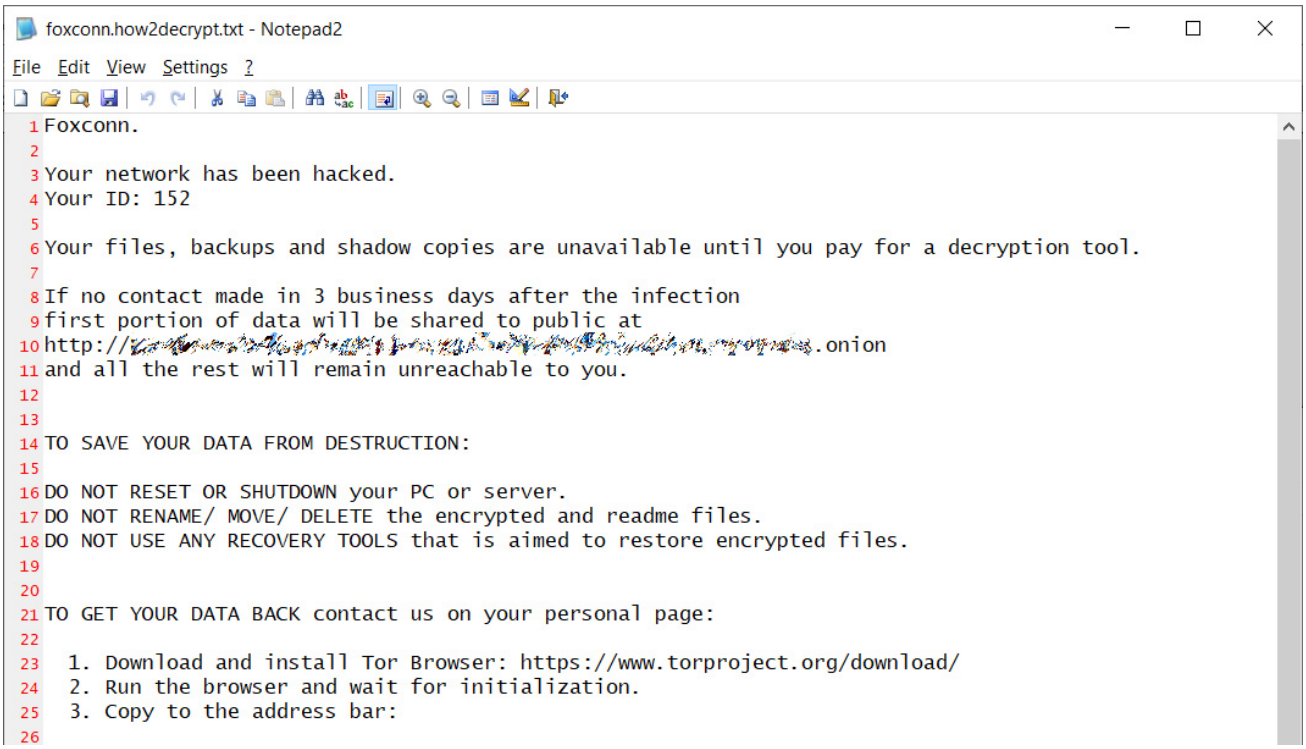


Foxconn CTBG MX facility website

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731 or on Wire at @lawrenceabrams-bc.

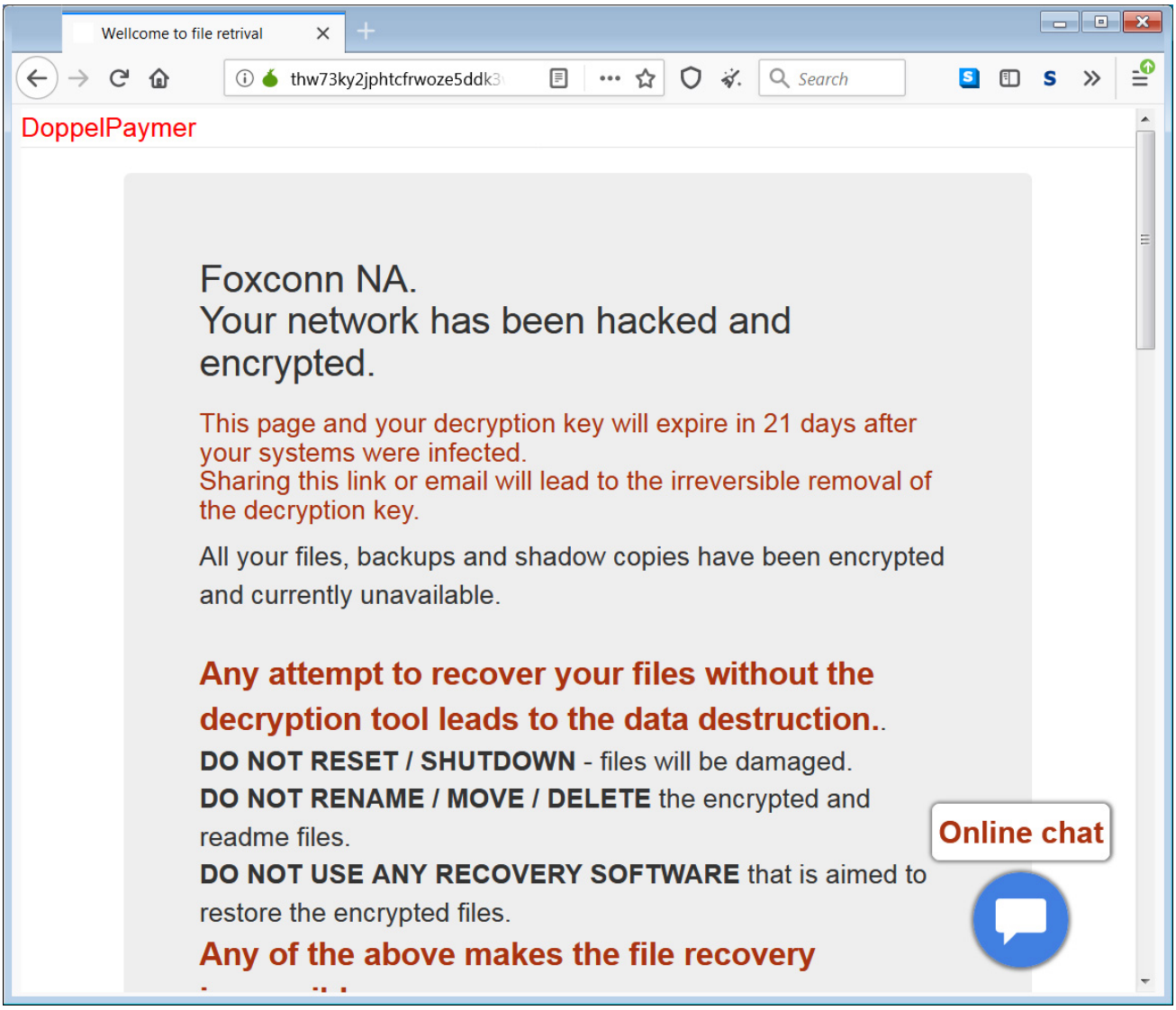
Attackers demand $34 million ransom

Sources have also shared the ransom note created on Foxconn servers during the ransomware attack, as can be seen below.



Foxconn ransom note

Included in the ransom note is a link to Foxconn's victim page on DoppelPaymer's Tor payment site where the threat actors are demanding a 1804.0955 BTC ransom, or approximately $34,686,000 at today's bitcoin prices.



Foxconn victim page on DoppelPaymer's website

In an interview with DoppelPaymer, the ransomware gang confirmed that they attacked Foxconn's North America facility on November 29th but did not attack the whole company.

As part of this attack, the threat actors claim to have encrypted about 1,200 servers, stole 100 GB of unencrypted files, and deleted 20-30 TB Of backups.

"We encrypted NA segment, not whole foxconn, it's about 1200-1400 servers, and not focused on workstations. They also had about 75TB's of misc backups, what we were able to - we destroyed (approx 20-30TB)," DoppelPayment told us about the attack.

In a statement to BleepingComputer, Foxconn confirmed the attack and said they are slowly bringing their systems back into service.

"We can confirm that an information system in the US that supports some of our operations in the Americas was the focus of a cybersecurity attack on November 29. We are working with technical experts and law enforcement agencies to carry out an investigation to

determine the full impact of this illegal action and to identify those responsible and bring them to justice."

"The system that was affected by this incident is being thoroughly inspected and being brought back into service in phases," Foxconn told BleepingComputer.

Other victims attacked by DoppelPaymer in the past include Compal, PEMEX (Petróleos Mexicanos), the City of Torrance in California, Newcastle University, Hall County in Georgia, Banijay Group SAS, and Bretagne Télécom.

Update 12/8/20: Added statement from Foxconn.

Related Articles:

Industrial Spy data extortion market gets into the ransomware game

Costa Rica declares national emergency after Conti ransomware attacks

Quantum ransomware seen deployed in rapid network attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

- Cyberattack
- Data Exfiltration
- DoppelPaymer
- Foxconn
- Ransomware

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: