

Home appliance giant Whirlpool hit in Nefilim ransomware attack

bleepingcomputer.com/news/security/home-appliance-giant-whirlpool-hit-in-nefilim-ransomware-attack/

Lawrence Abrams

By

[Lawrence Abrams](#)

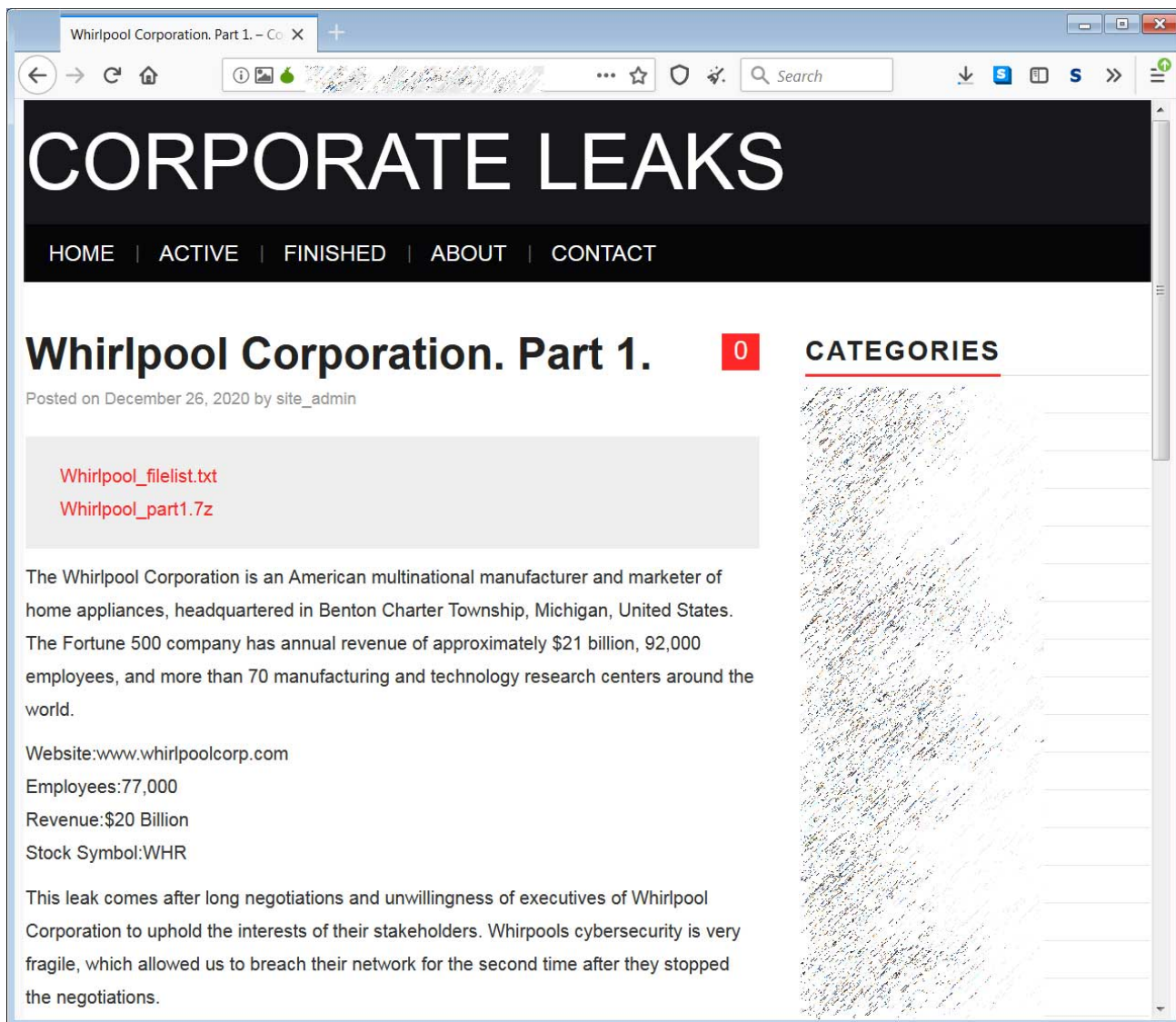
- December 28, 2020
- 12:12 PM
- 3



Home appliances giant Whirlpool suffered a ransomware attack by the Nefilim ransomware gang who stole data before encrypting devices.

Whirlpool is one of the world's largest home application makers with appliances under its name and KitchenAid, Maytag, Brastemp, Consul, Hotpoint, Indesit, and Bauknecht. Whirlpool employs 77,000 people at 59 manufacturing & technology research centers worldwide and generated approximately \$20 billion in revenue for 2019.

Over the weekend, the Nefilim ransomware gang published files stolen from Whirlpool during a ransomware attack. The leaked data included documents related to employee benefits, accommodation requests, medical information requests, background checks, and more.



Whirlpool data leak on Nefilim site

A source in the cybersecurity industry has told BleepingComputer that the Nefilim ransomware gang attacked Whirlpool in the first weekend of December.

```
1
2 Two things have happened to your company.
3 =====
4 Gigabytes of archived files that we deemed valuable or sensitive were downloaded from your network to a secure location.
5 When you contact us we will tell you how much data was downloaded and can provide extensive proof of the data extraction.
6 You can analyze the type of the data we download on our websites.
7 If you do not contact us we will start leaking the data periodically in parts.
8 =====
9 We have also encrypted files on your computers with military grade algorithms.
10 If you don't have extensive backups the only way to retrieve your data is with our software.
11 Restoration of your data with our software requires a private key which only we possess.
12 =====
13 To confirm that our decryption software works send 2 encrypted files from random computers to us via email.
14 You will receive further instructions after you send us the test files.
15 We will make sure you retrieve your data swiftly and securely and your data that we downloaded will be securely deleted
    when our demands are met.
16 If we do not come to an agreement your data will be leaked on this website.
17
18 Website: [REDACTED]
19 TOR link [REDACTED]
20
21 Contact us via email:
22 [REDACTED]@tutanota.com
23 [REDACTED]@tutanota.com
24 [REDACTED]@protonmail.com
```

Nefilim ransom note

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

In a statement to BleepingComputer, Whirlpool confirmed the attack and that their systems have been fully restored from the attack.

"We live in a time when illegal cyber crimes are all too prevalent across every industry. Data privacy is a top priority at Whirlpool Corporation and we invest in the technology and processes to help protect our people, our data and our operations."

"Last month Whirlpool Corporation discovered ransomware in our environment. The malware was detected and contained quickly. We are unaware of any consumer information that was exposed. There is no operational impact at this time," Whirlpool Corporation told BleepingComputer in an email.

Nefilim is not a particularly active ransomware operation but is known for attacks on other large and well-known victims in the past.

Other victims attacked by Nefilim include [Orange S.A.](#), [Dussman Group](#), [Luxottica](#), and [Toll Group](#).

Update 12/28/20: Whirlpool's systems are fully restored, not slowly recovering as initially stated.

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](#)
- [Data Leak](#)
- [Nefilim](#)
- [Ransomware](#)
- [Whirlpool](#)

[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](#)

Comments



[magic-luigi](#) - 1 year ago

-
-

Why do you publish shaming site Lawrence?



[Lawrence Abrams](#) - 1 year ago

-
-

Not intentional. Fixed



• Some-Other-Guy - 1 year ago

-
-

Wash, rinse, repeat

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
