

Snap-on discloses data breach claimed by Conti ransomware gang

By Lawrence Abrams

Published: 2022-04-08 · Archived: 2026-04-05 17:49:18 UTC



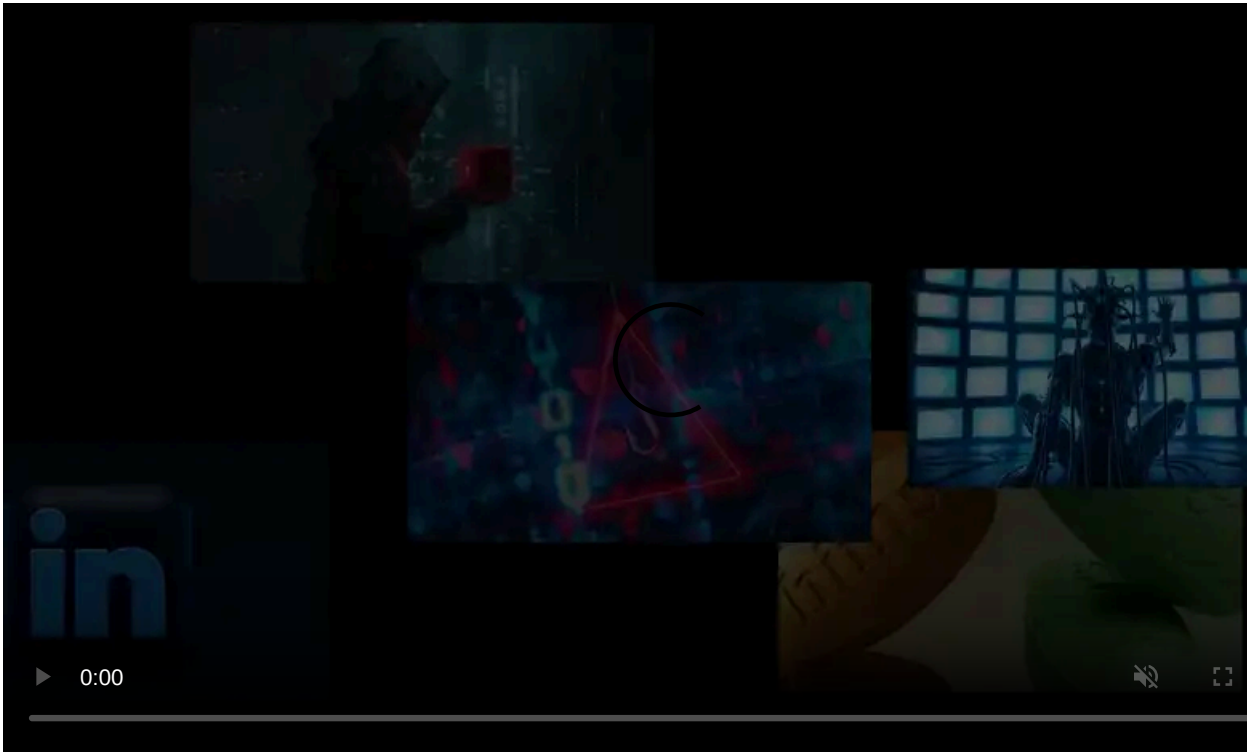
Source: [snapon.com](https://www.snapon.com)

American automotive tools manufacturer Snap-on announced a data breach exposing associate and franchisee data after the Conti ransomware gang began leaking the company's data in March.

Snap-on is a leading manufacturer and designer of tools, software, and diagnostic services used by the transportation industry through various brands, including Mitchell1, Norbar, Blue-Point, Blackhawk, and Williams.

Yesterday, Snap-on disclosed a data breach after they detected suspicious activity in their network, which led to them shutting down all of their systems.

"In early March, Snap-on detected unusual activity in some areas of its information technology environment. We quickly took down our network connections as part of our defense protocols, particularly appropriate given heightened warnings from various agencies," reads a notice on the Snap-on website.



Visit Advertiser website [GO TO PAGE](#)

"We launched a comprehensive analysis assisted by a leading external forensics firm, identified the event as a security incident, and notified law enforcement of the incursion."

After conducting an investigation, Snap-on discovered that threat actors stole personal data belonging to employees between March 1st and March 3rd, 2022.

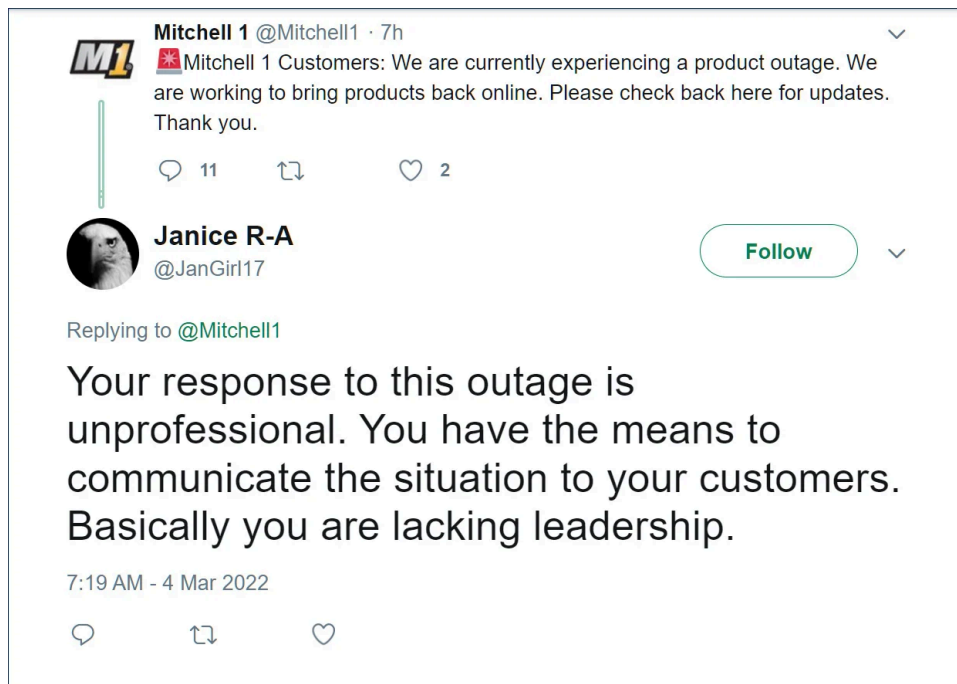
"We believe the incident involved associate and franchisee data including information such as: names, Social Security Numbers, dates of birth, and employee identification numbers," discloses a Snap-on [data breach notification](#) submitted to the California Attorney General's office.

Snap-on is offering a free one-year subscription to the IDX identity theft protection service for those affected.

Conti claimed an attack on Snap-on

While Snap-on's data breach notification did not shed much light on its attack, BleepingComputer received an anonymous tip in early March stating that one of Snap-on's subsidiaries, Mitchell1, was suffering an outage caused by a ransomware attack.

Mitchell1 had initially tweeted about the outage but soon deleted the notices from Twitter and Facebook.



Deleted Mitchell1 tweet about the outage

Source: [Archive.org](#)

 **Mike Smith**
@MikeSmi91056416

Replying to @Snapon_Tools

Can you explain why the tweets and Facebook posts related to the Mitchell1 outage March 4-6 were DELETED? Mitchell1 employees stated that Snap on controls their social media.


1:50 PM · Mar 24, 2022

♡ Reply ↗ Share

[Explore what's happening on Twitter](#)

However, another source told BleepingComputer that it was not Mitchell1 who had suffered an attack but their parent company Snap-on.

Soon after, threat intelligence researcher [Ido Cohen spotted](#) that the Conti ransomware gang claimed to have attacked Snap-on and had begun to leak almost 1 GB of documents that were allegedly stolen during the attack.

 **Ensar Seker**
@cyberguideme

Replying to @barricadecyber @ido_cohen2 and @Snapon_Tools

"SNAP-ON INCORPORATED"

<https://www.snapon.com/>

2801 80th Street Kenosha, Wisconsin 53143, USA
Phone: 877-762-7664
Email: crystallakeweb@snapon.com

Snap-on makes work easier for professionals performing critical tasks. Rooted in the dignity of work, guided with insight shaped from experience. Snap-on provides a broad array of unique productivity solutions. Precision. Performance. Pride. Snap-on supports a wide range of serious professionals in critical industries.

PUBLISHED 5%

3/16/2022 71 2 [928.71 MB]

/ ROOT

DETRW23FILE1.part1.rar	750.00 MB
DETRW23FILE1.part2.rar	178.71 MB

1:10 AM · Mar 18, 2022

♡ 2 Reply ↗ Share

[Read 1 reply](#)

The Conti gang quickly removed the data leak, and Snap-on has not reappeared on their data leak site, leading security researchers to tell BleepingComputer that they believe Snap-on paid a ransom for the data not to be leaked.

BleepingComputer has contacted Snap-on to confirm if the disclosed data breach is linked to the alleged Conti ransomware attack, and we will update this story if we hear back.

Who is Conti Ransomware?

[Conti](#) is a ransomware operation operated by a Russian hacking group known for other malware infections, such as Ryuk, TrickBot, and BazarLoader.

Conti commonly breaches a network after corporate devices become infected with the [BazarLoader or TrickBot malware infections](#), which provide remote access to the hacking group.

Once they gain access to an internal system, they spread through the network, steal data, and deploy the ransomware.

The Conti gang recently suffered their own data breach after siding with Russia over the invasion of Ukraine, leading to a Ukrainian researcher publishing almost [170,000 internal chat conversations](#) between the Conti ransomware gang members and the [Conti ransomware source code](#).

“WARNING”

🗨 The Conti Team is officially announcing a full support of Russian government. If any body will decide to organize a cyberattack or any war activities against Russia, we are going to use our all possible resources to strike back at the critical infrastructures of an enemy.

📅 2/25/2022

👁 55

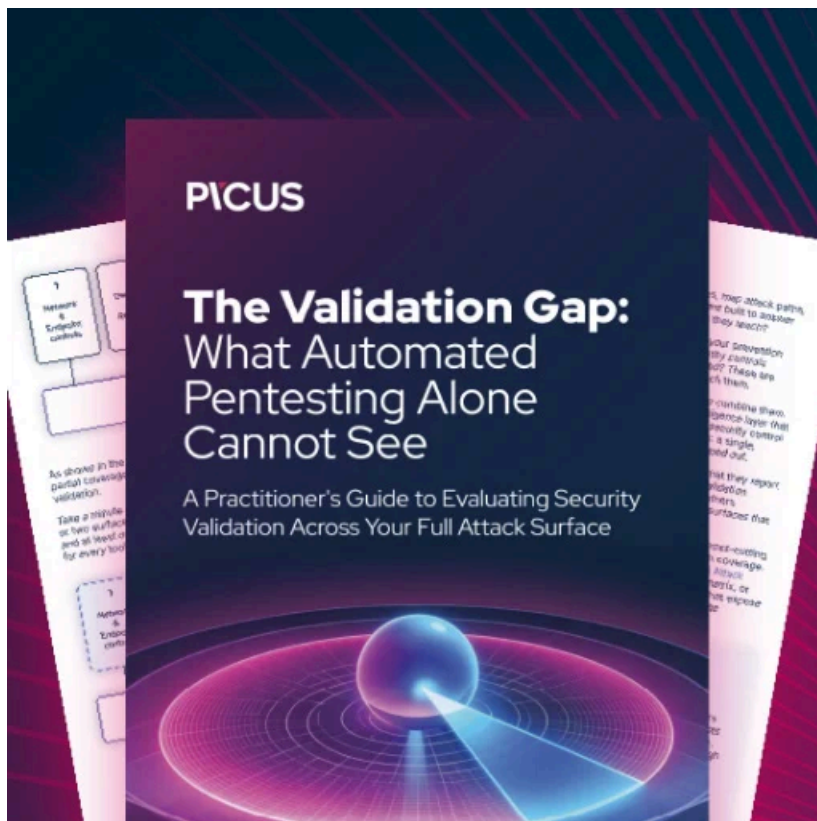
📄 0 [0.00 B]

Conti siding with Russia on the invasion of Ukraine

Source: [BleepingComputer](#)

Conti is known for past attacks on high-profile organizations, including Ireland's [Health Service Executive \(HSE\)](#) and [Department of Health \(DoH\)](#), the [City of Tulsa, Broward County Public Schools](#), and [Advantech](#).

Due to the cybercrime gang's ongoing activity, the US government issued an [advisory on Conti ransomware attacks](#).



[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/snap-on-discloses-data-breach-claimed-by-conti-ransomware-gang/>