KP Snacks giant hit by Conti ransomware, deliveries disrupted

By Ax Sharma

Published: 2022-02-02 · Archived: 2026-04-05 13:12:08 UTC

KP Snacks, a major producer of popular British snacks has been hit by the Conti ransomware group affecting distribution to leading supermarkets.

Kenyon Produce (KP) Snacks includes popular brands such as PopChips, Skips, Hula Hoops, Penn State pretzels, McCoy's, Wheat Crunchies, etc.

KP Snacks has more than 2,000 employees and estimates put the company's annual revenue at over $600 million, making them an attractive target for threat actors.


DIE LINKE.
0:00

Conti plans to leak sensitive documents

A cyber attack on British snack giant, KP Snacks has now escalated to supply chain disruption around the UK.

Because of the attack, deliveries from the company to leading superstores are reportedly being delayed or canceled altogether. According to discussions between KP Snacks and its partner supermarkets, the supply shortage issues can last until the end of March.

KP SNACKS

KP Snacks Limited
Fifth Floor
The Urban Building
3-9 Albert Street
Slough, SL1 2BE
t +44 (0)845 601 7583
w www.kpsnacks.com

Wednesday 2nd February, 2022

Dear Nisa Partner,

After the initial investigation of an IT outage and the communications on Friday 28th January, with regret, we are now able to confirm that we have been victims of a cyber-attack and our systems have been compromised by ransomware. Through the weekend our IT Team and third party experts have been assessing the scale of the intrusion and continue to do so. As a result, at this stage we cannot safely process orders or dispatch goods.

We have teams working through the resolution, but it is unknown when this will be resolved.

Thank you for your cooperation and patience while we manage the situation. We, KP Snacks, will keep you updated regularly.

If you have any questions, please do not hesitate to get in touch.

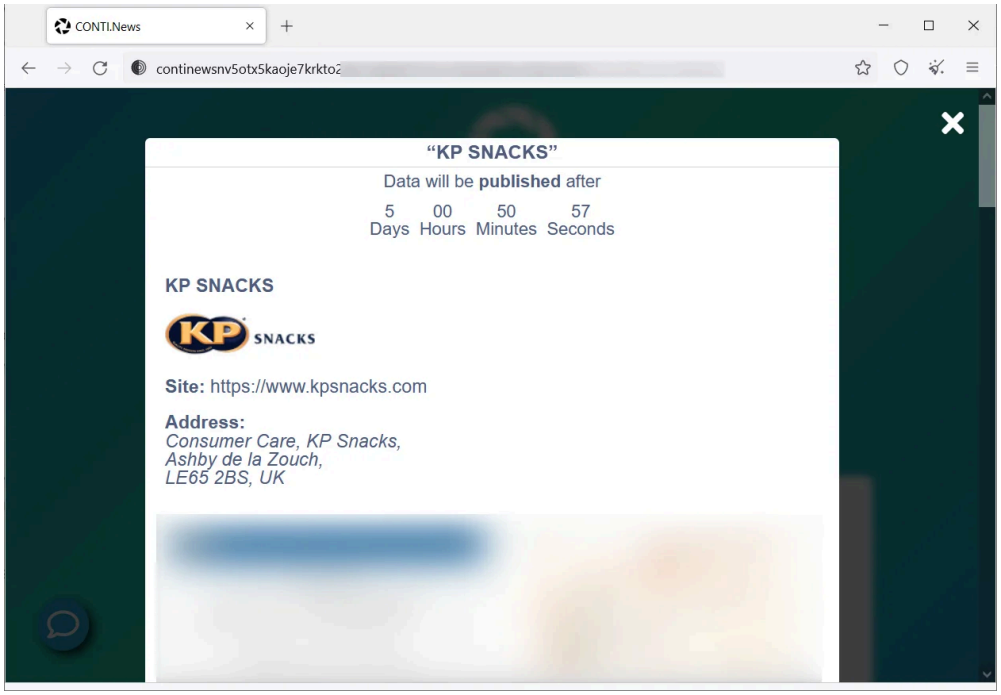
Kind Regards,

KP Snacks

Letter sent by KP Snacks to supermarkets like Nisa (betterRetailing)

A source informed BleepingComputer that the company's internal network had been breached with threat actors gaining access to and encrypting sensitive files, including employee records and financial documents.

Private leak pages seen by BleepingComputer show Conti ransomware group claiming responsibility for the attack:



KP Snacks listed on Conti's private data leak page (BleepingComputer)

On the private leak page, Conti shared samples of credit card statements, birth certificates, spreadsheets with employee addresses and phone numbers, confidential agreements, and other sensitive documents.

Darknet intel provider *DarkFeed* had also posted yesterday about Conti ransomware op giving the company **five days** before leaking even more proprietary data on their public blog.

It isn't clear if KP Snacks is currently negotiating with Conti or if it will pay a ransom.

"On Friday, 28 January we became aware that we were unfortunately victims of a ransomware incident," a KP Snacks spokesperson told BleepingComputer.

"As soon as we became aware of the incident, we enacted our cybersecurity response plan and engaged a leading forensic information technology firm and legal counsel to assist us in our investigation."

The company's internal IT teams are working with third party security experts to assess the situation.

"We have been continuing to keep our colleagues, customers, and suppliers informed of any developments and apologise for any disruption this may have caused," concluded the company in their statement to us.

Conti repeatedly hits high-profile organizations

Conti is a Ransomware-as-a-Service (RaaS) operation linked to the Wizard Spider Russian cybercrime group, also known for other notorious malware, including Ryuk, TrickBot, and BazarLoader.

The ransomware group's affiliates breach targets' networks after corporate devices get infected with BazarLoader or TrickBot malware, providing them remote access to the compromised system.

In recent weeks, Conti has rapidly climbed up the ranks among ransomware groups after repeatedly targeting prominent organizations.

Last month, Conti claimed responsibility for attacking Bank Indonesia, the country's central bank, and began leaking its data.

In December 2021, Conti had breached the systems of Nordic Choice hotel group, freezing the hotel properties' key cards.

The ransomware gang's former targets have included Ireland's Department of Health (DoH) and Health Service Executive (HSE), and marketing giant RR Donnelly (RRD).

Due to increased Conti activity, the FBI, CISA, and the NSA US have also recently issued an advisory warning of an increased number of Conti ransomware attacks.

Update Feb 3, 01:35 AM ET: Added a copy of the letter sent by KP Snacks to partner supermarkets.

Source: https://www.bleepingcomputer.com/news/security/kp-snacks-giant-hit-by-conti-ransomware-deliveries-disrupted/