Canadian retailer Home Hardware hit by ransomware

Archived: 2026-04-05 18:03:34 UTC

Skip to Content

- News
- Economy
- Energy
- Mining
- Real Estate
- Finance
- Work
- Wealth
- Investor
- FP Comment
- Executive Women
- Puzzmo
- Newsletters
- Financial Times
- Business Essentials

1. Home
2. Innovation
3. Information Technology

Canadian retailer Home Hardware hit by ransomware

Author of the article:

One of the country’s biggest privately-held dealer-owned hardware retailers has acknowledged it was hit by ransomware, with the threat group promising to start releasing copied data today, April 2.

Home Hardware Stores Ltd., with over 1,050 stores under the Home Hardware, Home Building Centre, and Home Furniture banners, acknowledged to *ITWorldCanada.com* an attack hit it in February.

“An unauthorized third-party was able to access parts of our corporate data,” Jessica Kuepfer, the company’s director of communications, said in an e-mail Friday.

“We immediately engaged our cybersecurity firm and quickly implemented countermeasures to isolate and contain the attack. We have maintained full business continuity.

“Each of the stores are independently owned and operated. Based on our investigation, it appears that attack has not impacted dealer retail systems or any consumer transaction or payment data.”

At press time Kuepfer didn’t reply to a query about how much money DarkSide has demanded and whether the company has talked to the attackers.

The attack against the Ont.-based Home Hardware comes after the DarkSide ransomware group began posting what it said was corporate data copied from the company and promising to publicly release data if it isn't paid for decryption keys.

A screenshot of the notice on the group's website says:

"We have downloaded a lot of your private data. You can see examples below. If you need proofs we are ready to provide you with it. The data is preloaded and will automatically be published in our blog if you do not contact us. After publication your data can be downloaded by anyone. It is stored on our tor for CDN and will be available for at least six months."

Screenshots of some of the documents seen by *ITWorldCanada.com* include what appears to be a December 2020 financial report and a November 2020 letter marked "Strictly Private and Confidential" dealing with an acquisition that was announced three months later.

The DarkSide website also includes countdown clocks for the automatic release of what are said to be copied documents for today, Saturday and Sunday.

Companies dealing with data exfiltration situations have no good options, commented Brett Callow, a British Columbia-based threat researcher for Emsisoft.

"They've been breached, and their data is in the hands of cybercriminals. If they refuse to pay the criminals, their data will be released online. If they do pay, they'll simply get a pinky-promise from a bad faith actor that the stolen data will be deleted – and, of course, there is ample evidence that that does not happen. Why would a criminal enterprise delete data that it may be able to use or further monetize?

"Unfortunately, data exfiltration is proving to be a strategy that works, with many organizations that were able to recover their systems using backups having still paid demands to stop their data being released. Since ransomware groups began exfiltrating data at the end of 2019, about 1,500 organizations have had their data stolen and posted online, while many others paid to prevent it being published."

According to a recent analysis by security vendor Varonis, DarkSide is a ransomware-as-a-service group that began operating last August. Like other RaaS services it offers, anyone who helps spread their malware gets 10 to 25 per cent of the payout.

Since starting they have become known for their "professional operations and large ransoms," the report said.

"They provide web chat support to victims, build intricate data leak storage systems with redundancy, and perform financial analysis of victims prior to attacking," it read. "Our reverse engineering revealed that Darkside's malware will check device language settings to ensure they don't attack Russia-based organizations. They have also answered questions on Q&A forums in Russian and are actively recruiting Russian-speaking partners."

DarkSide often uses compromised third-party contractor accounts to access Virtual Desktop Infrastructure (VDI) that had been put in place to facilitate remote access during the pandemic, says Varonis. It has also exploited servers, and then quickly deploys an additional remote access backdoor that would preserve access should the vulnerable server be patched.

“While neither of these vectors is novel, they should serve as a warning that sophisticated threat actors are easily bypassing perimeter defences,” according to the report. “They illustrate the need for multi-factor authentication on all internet-facing accounts and rapid patching of internet-facing systems.”

In January, Bitdefender released a decryptor for the version of the DarkSide encryption algorithm used at that time.

This section is powered by IT World Canada. ITWC covers the enterprise IT spectrum, providing news and information for IT professionals aiming to succeed in the Canadian market.

Source: https://financialpost.com/technology/tech-news/canadian-retailer-home-hardware-hit-by-ransomware