Co-op confirms data theft after DragonForce ransomware claims attack

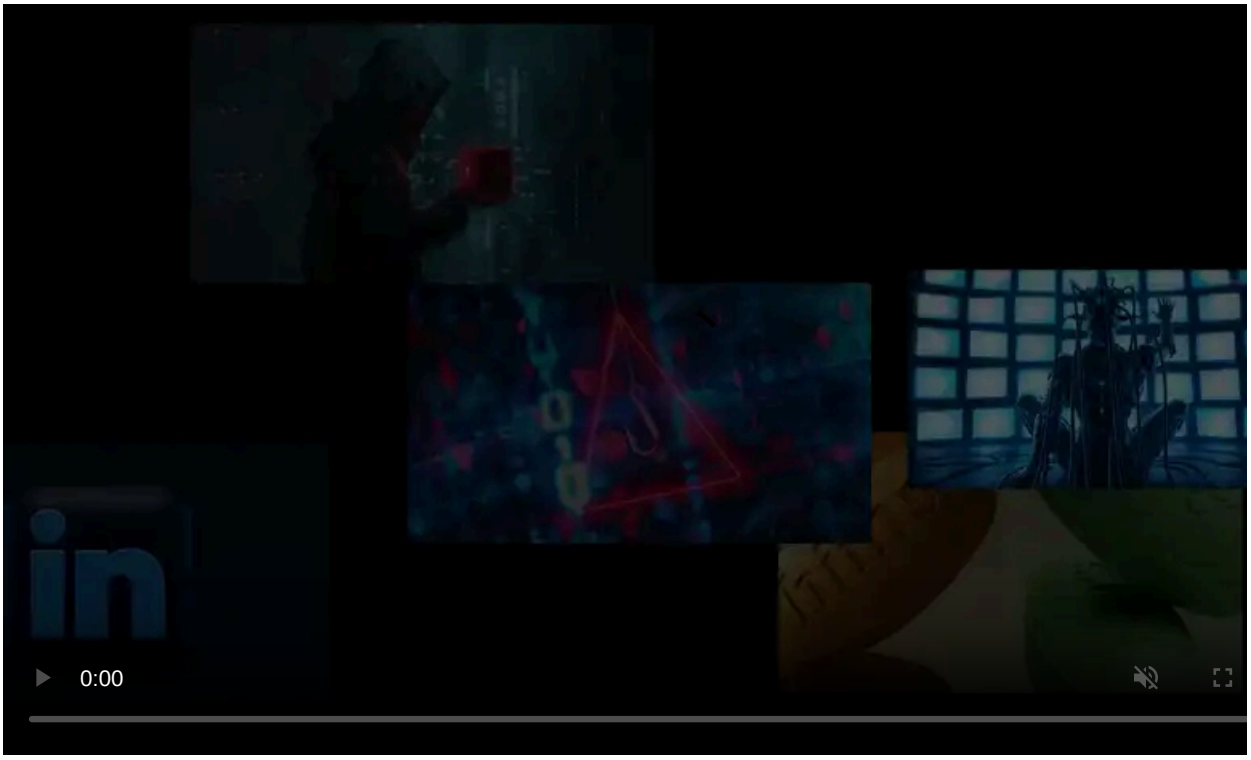
By Lawrence Abrams

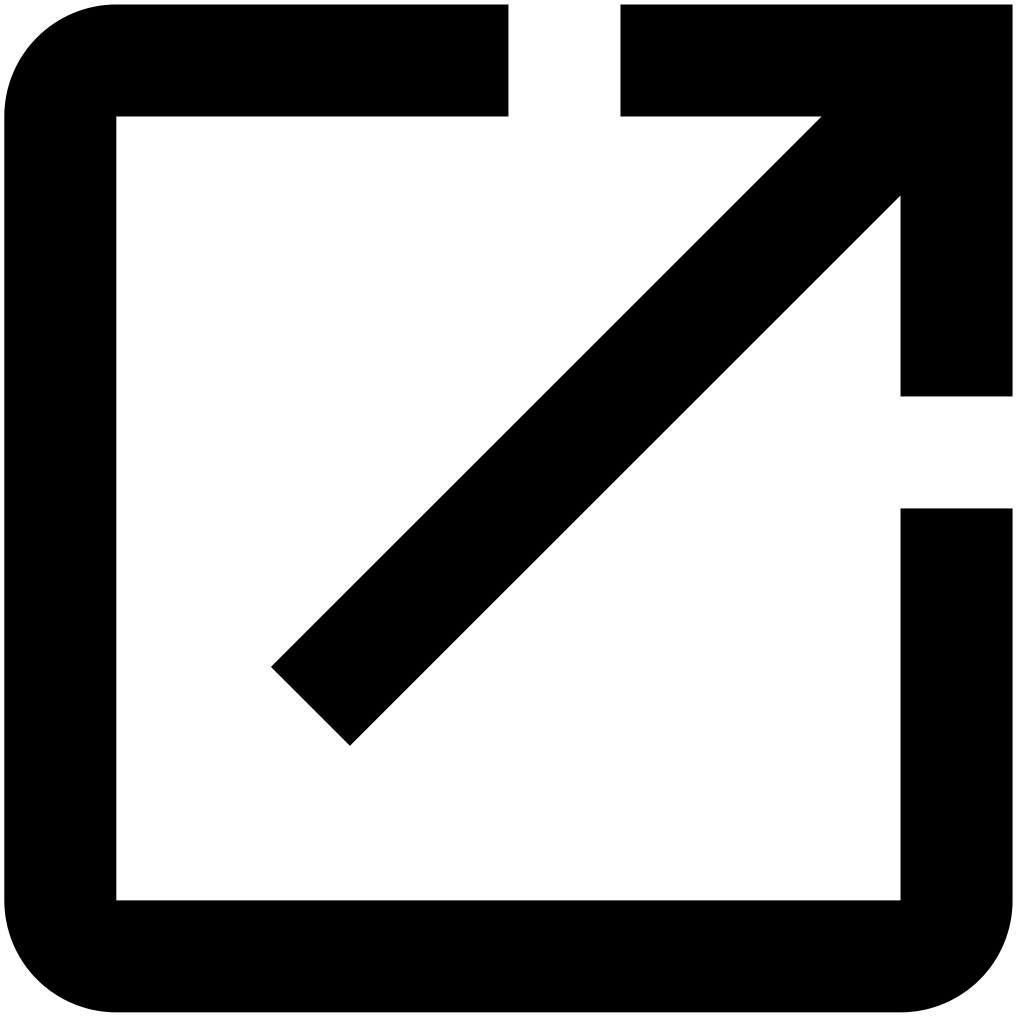
Published: 2025-05-02 · Archived: 2026-04-05 18:26:20 UTC

The Co-op cyberattack is far worse than initially reported, with the company now confirming that data was stolen for a significant number of current and past customers.

"As a result of ongoing forensic investigations, we now know that the hackers were able to access and extract data from one of our systems," Co-op told BleepingComputer.

"The accessed data included information relating to a significant number of our current and past members."


0:00



"This data includes Co-op Group members' personal data such as names and contact details, and did not include members' passwords, bank or credit card details, transactions or information relating to any members' or customers' products or services with the Co-op Group."

On Wednesday, UK retail giant Co-op downplayed the cyberattack, stating that it had shut down portions of its IT systems after detecting an attempted intrusion into its network.

However, soon after the news broke, BleepingComputer learned that the company did indeed suffer a breach utilizing tactics associated with Scattered Spider/Octo Temptest, but their defenses prevented the threat actors from performing significant damage to the network.

Sources told BleepingComputer that it is believed the attack occurred on April 22, with the threat actors utilizing tactics similar to the attack on Marks and Spencer. The threat actors reportedly conducted a social engineering attack that allowed them to reset an employee's password, which was then used to breach the network.

Once they gained access to the network, they stole the Windows NTDS.dit file, a database for Windows Active Directory Services that contains password hashes for Windows accounts.

Co-op is now in the process of rebuilding all of its Windows domain controllers and hardening Entra ID with the help of Microsoft DART. KPMG is assisting with AWS support.

When sharing these details with Co-op yesterday, the company said it had nothing further to share and sent us its original statement.

Do you have information about this or another cyberattack? If you want to share the information, you can contact us securely and confidentially on Signal at LawrenceA.11, via email at lawrence.abrams@bleepingcomputer.com, or by using our tips form.

DragonForce ransomware behind attack

Today, the BBC first reported that affiliates for the DragonForce ransomware operation are behind the attack on Co-op. As first reported by BleepingComputer, these are the same hackers who breached Marks and Spencer last week.

BBC correspondent Joe Tidy spoke to the DragonForce operator, who confirmed they were behind the attack and shared samples of corporate and customer data stolen during the attack. The threat actors claim to have data from 20 million people who registered for Co-op's membership reward program.

The threat actors stated they contacted Co-op's head of cyber security and other executives using Microsoft Teams messages, sharing screenshots of the extortion messages with the BBC.

After the attack, Co-op sent an internal email to employees warning them to be vigilant when using Microsoft Teams and not to share any sensitive data, likely out of concern that the hackers still had access to the platform.

The threat actors also claimed to the BBC that they were behind the attempted cyberattack on Harrods.

DragonForce is a ransomware-as-a-service operation where other cyber criminals can join as affiliates to use their ransomware encryptors and negotiation sites. In exchange, the DragonForce operators receive 20-30% of any ransoms paid by extorted victims.

In attacks, the affiliates will breach a network, steal data, and ultimately deploy malware that encrypts the files on all of the servers and workstations. The threat actors then demand a ransom payment to retrieve a decryptor and promise that stolen data will be deleted.

If a ransom is not paid, the ransomware operation typically publishes the stolen data on their dark web data leak site.

DragonForce is a relatively new operation but is gearing up to be one of the more prominent ones in the ransomware space.

They are believed to be working with English-speaking threat actors that fit a specific set of tactics associated with the name "Scattered Spider" or "Octo Tempest."

These threat actors are experts at using social engineering attacks, SIM Swapping, and MFA fatigue attacks to breach networks and then steal data or deploy ransomware. The threat actors are known to aggressively extort their victims.

To be clear, Scatted Spider is not a gang or group with specific members. Instead, they are an amorphous community of financially motivated threat actors who congregate on the same Telegram channels, Discord servers, and hacking forums.

As they are "scattered" throughout the cybercrime landscape, it is more difficult for law enforcement to track individual people who are associated with an attack.

The original threat actors associated with the Scattered Spider classification were behind a string of attacks, including those on MGM and Reddit.

Some, if not all, of these original hackers have now been arrested by the US, United Kingdom, and Spain.

However, previously unknown hackers or copycats are now utilizing the same methods to escalate attacks.

Cybersecurity researcher Will Thomas has put together a recommended guide on defending against Scattered Spider attacks.

Source: https://www.bleepingcomputer.com/news/security/co-op-confirms-data-theft-after-dragonforce-ransomware-claims-attack/