

## Kmart nationwide retailer suffers a ransomware attack

By Lawrence Abrams

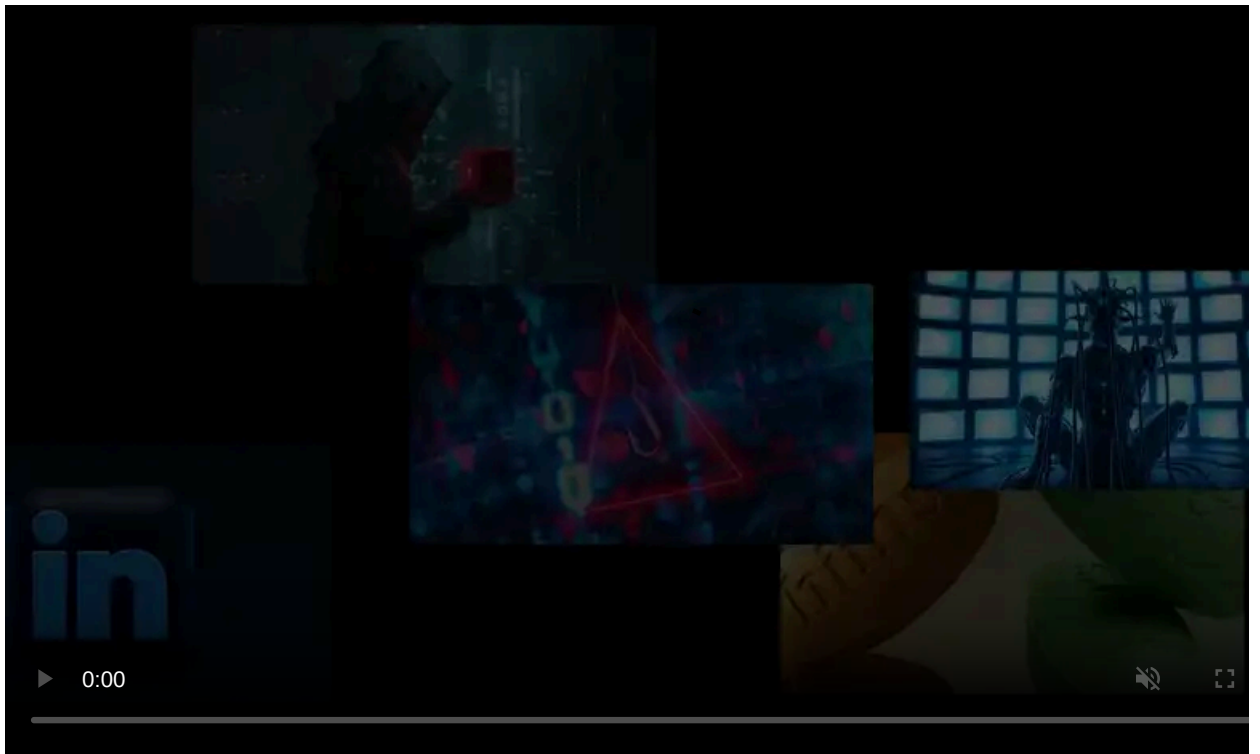
Published: 2020-12-03 · Archived: 2026-04-05 18:24:09 UTC



US department store Kmart has suffered a ransomware attack that impacts back-end services at the company, BleepingComputer has learned.

Sears Holding Corp originally owned both Kmart and Sears, but after the company filed for bankruptcy in 2018, it was purchased by Transform Holdco LLC (Transformco) in 2019.

While Kmart has been a household name in the USA, its number has dwindled over the past two years to only [35 stores remaining](#).



Visit Advertiser website [GO TO PAGE](#)

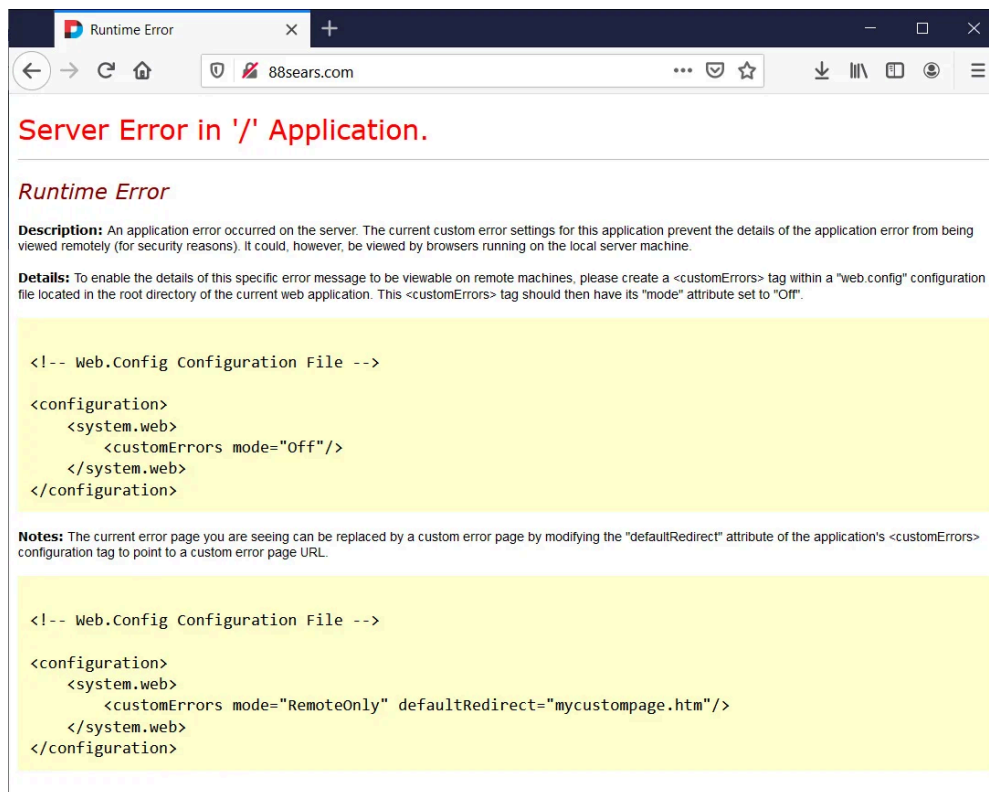
## Kmart Windows domain hit with ransomware

BleepingComputer has learned that Kmart suffered a cyberattack by the Egregor ransomware operation this week that encrypted devices and servers on the network.

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](https://twitter.com/lawrenceabrams-bc).

A ransom note shared with BleepingComputer shows that the 'KMART' Windows domain was compromised in the attack.

While online stores continue to operate, the 'Transformco Human Resources Site,' [88sears.com](http://88sears.com), is currently offline. Employees said that the outage is caused by the recent ransomware attack.



### 88sears.com suffering an outage

Egregor is known for stealing unencrypted files before deploying their ransomware. The ransomware operation then threatens to post the data on [ransomware data leak sites](#) if a ransom is not paid.

It is unknown if the attackers stole data, how many devices were encrypted, or the ransom amount demanded by the Egregor cybercrime group.

Egregor is a new ransomware operation that started encrypting victims in September 2020. BleepingComputer has been told by threat actors that after the [Maze Ransomware operation shut down](#), many of their partners switched over to the Egregor operation.

This migration of experienced threat actors has allowed Egregor to quickly amass many victims in a short period.

Other well-known companies recently attacked by Egregor include [Cencosud](#), [Crytek](#), [Ubisoft](#), and [Barnes and Noble](#).

BleepingComputer has reached out to Kmart and their parent company Transformco, but has not received a response yet.

*Update 12/6/20: There are 45 Kmart's operating.*



### [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/kmart-nationwide-retailer-suffers-a-ransomware-attack/>