

Kmart nationwide retailer suffers a ransomware attack

bleepingcomputer.com/news/security/kmart-nationwide-retailer-suffers-a-ransomware-attack/

Lawrence Abrams

By

[Lawrence Abrams](#)

- December 3, 2020
- 01:08 PM
- 0



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.

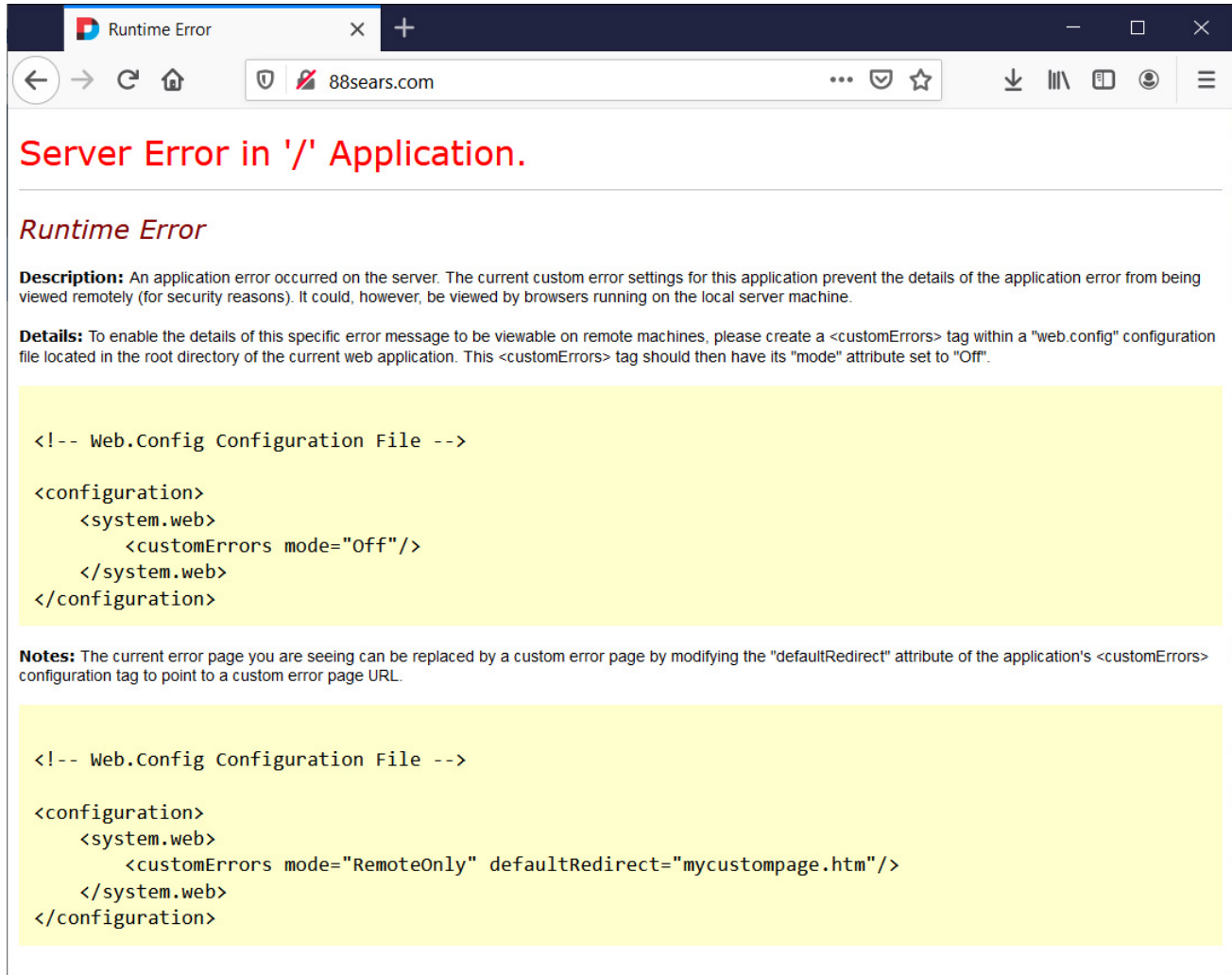
Kmart Windows domain hit with ransomware

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 or on Wire at @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, is currently offline. Employees said that the outage is caused by the recent ransomware attack.



Server Error in '/' Application.

Runtime Error

Description: An application error occurred on the server. The current custom error settings for this application prevent the details of the application error from being viewed remotely (for security reasons). It could, however, be viewed by browsers running on the local server machine.

Details: To enable the details of this specific error message to be viewable on remote machines, please create a <customErrors> tag within a "web.config" configuration file located in the root directory of the current web application. This <customErrors> tag should then have its "mode" attribute set to "Off".

```
<!-- Web.Config Configuration File -->

<configuration>
  <system.web>
    <customErrors mode="Off"/>
  </system.web>
</configuration>
```

Notes: The current error page you are seeing can be replaced by a custom error page by modifying the "defaultRedirect" attribute of the application's <customErrors> configuration tag to point to a custom error page URL.

```
<!-- Web.Config Configuration File -->

<configuration>
  <system.web>
    <customErrors mode="RemoteOnly" defaultRedirect="mycustompage.htm"/>
  </system.web>
</configuration>
```

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 Kmarts operating.

Related Articles:

[Windows 11 KB5014019 breaks Trend Micro ransomware protection](#)

[Industrial Spy data extortion market gets into the ransomware game](#)

[New 'Cheers' Linux ransomware targets VMware ESXi servers](#)

[SpiceJet airline passengers stranded after ransomware attack](#)

[US Senate: Govt's ransomware fight hindered by limited reporting](#)

- [Egregor](#)
- [Kmart](#)
- [Ransomware](#)
- [Sears](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- [Previous Article](#)
- [Next Article](#)

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
