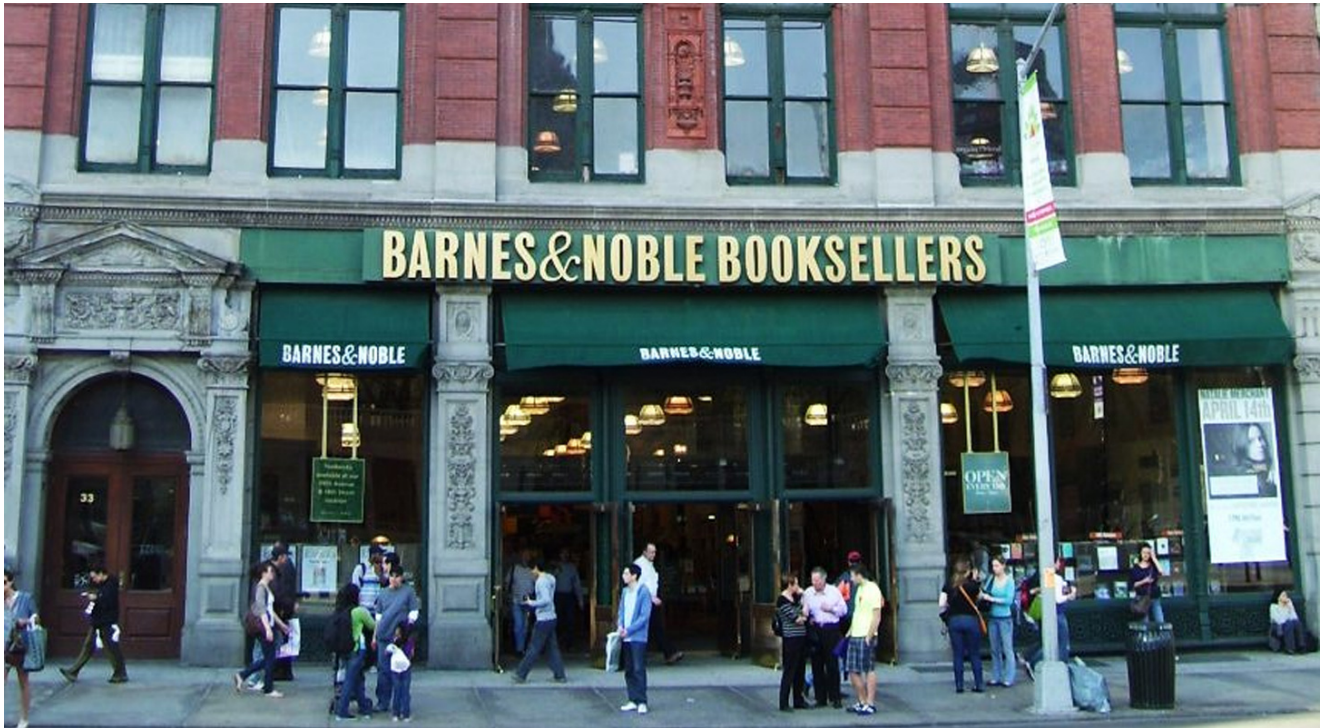


# Barnes & Noble hit by Egregor ransomware, strange data leaked

[bleepingcomputer.com/news/security/barnes-and-noble-hit-by-egregor-ransomware-strange-data-leaked/](https://bleepingcomputer.com/news/security/barnes-and-noble-hit-by-egregor-ransomware-strange-data-leaked/)

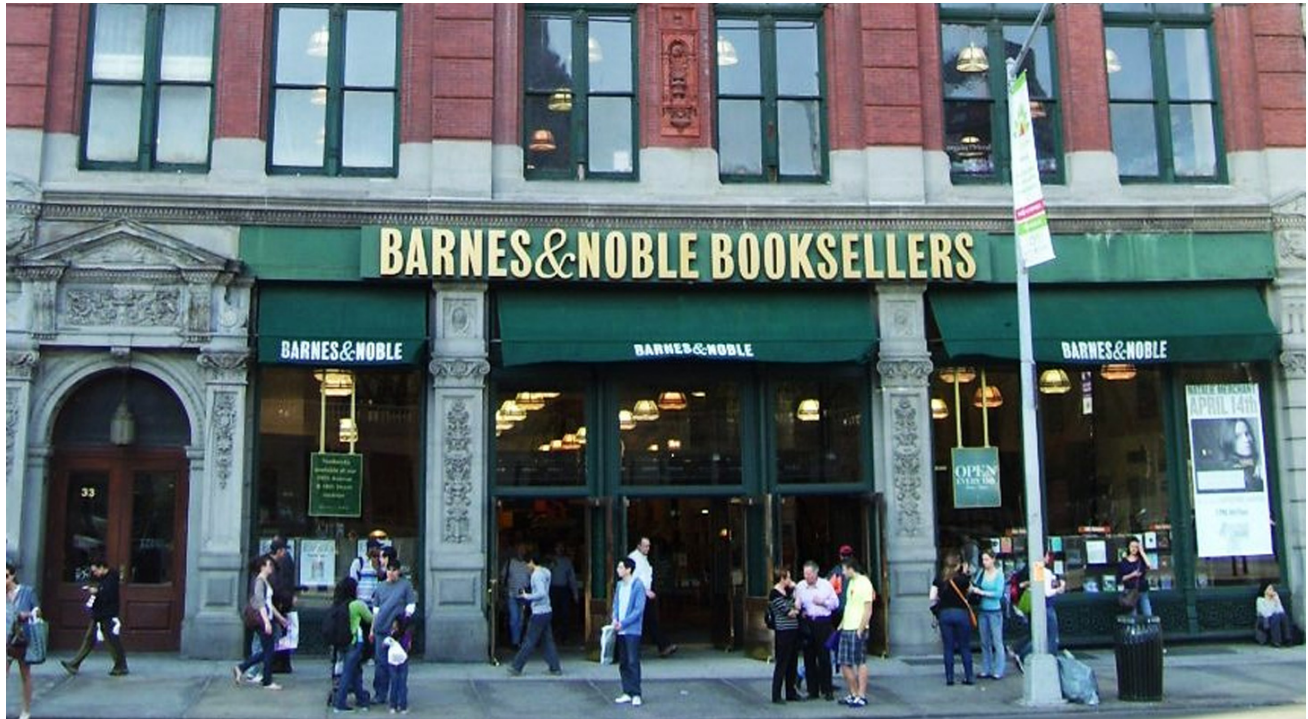
Lawrence Abrams



By

Lawrence Abrams

- October 20, 2020
- 02:53 PM
- 1



The Egregor ransomware gang is claiming responsibility for the cyberattack on U.S. Bookstore giant Barnes & Noble on October 10th, 2020. The attackers state that they stole unencrypted files as part of the attack.

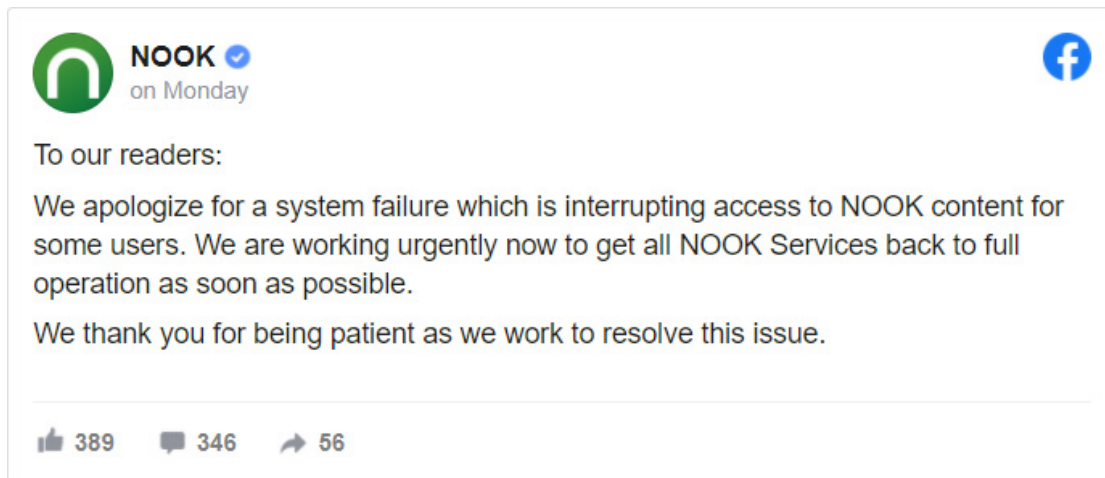
Barnes & Noble is the largest brick-and-mortar bookseller in the United States, with over 600 bookstores in fifty states. The bookseller also operated the Nook Digital, which is their eBook and e-Reader platform.



## **Ransomware attack leads to an outage**

---

On October 10th, users began complaining on Nook's Facebook page and Twitter that they could no longer access their library of purchased eBooks and magazine subscriptions.

In response to the concerns, Barnes & Noble posted an update on the Nook Facebook page stating that they are experiencing a severe system failure and are working to get systems operational again.






NOOK  on Monday 

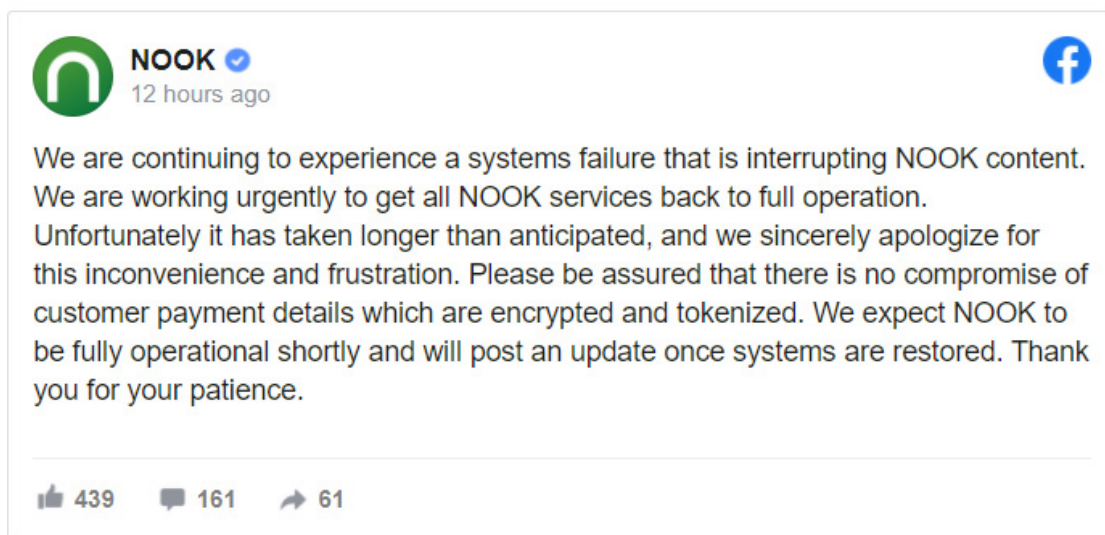
To our readers:



We apologize for a system failure which is interrupting access to NOOK content for some users. We are working urgently now to get all NOOK Services back to full operation as soon as possible.

We thank you for being patient as we work to resolve this issue.

---




 389  346  56



NOOK  12 hours ago 

We are continuing to experience a systems failure that is interrupting NOOK content. We are working urgently to get all NOOK services back to full operation. Unfortunately it has taken longer than anticipated, and we sincerely apologize for this inconvenience and frustration. Please be assured that there is no compromise of customer payment details which are encrypted and tokenized. We expect NOOK to be fully operational shortly and will post an update once systems are restored. Thank you for your patience.

---

 439  161  61

Late Wednesday night, Barnes & Noble disclosed that they suffered a cyberattack on October 10th, 2020.

As part of this attack, ransomware attackers actors gained access to corporate network for the company. After discovering the attack, Barnes and Noble shut down their network to prevent the attack's further spread, which led to a service outage.

"It is with the greatest regret we inform you that we were made aware on October 10, 2020 that Barnes & Noble had been the victim of a cybersecurity attack, which resulted in unauthorized and unlawful access to certain Barnes & Noble corporate systems."

"We write now out of the greatest caution to let you know how this may have exposed some of the information we hold of your personal details," Barnes & Noble stated in their email.

# BARNES & NOBLE

Dear Barnes & Noble Customer,

It is with the greatest regret we inform you that we were made aware on October 10, 2020 that Barnes & Noble had been the victim of a cybersecurity attack, which resulted in unauthorized and unlawful access to certain Barnes & Noble corporate systems.

We write now out of the greatest caution to let you know how this may have exposed some of the information we hold of your personal details.

Firstly, to reassure you, there has been no compromise of payment card or other such financial data. These are encrypted and tokenized and not accessible. The systems impacted, however, did contain your email address and, if supplied by you, your billing and shipping address and telephone number. We currently have no evidence of the exposure of any of this data, but we cannot at this stage rule out the possibility. We give below answers to some frequently asked questions.

We take the security of our IT systems extremely seriously and regret sincerely that this incident has occurred. We know also that it is concerning and inconvenient to receive notices such as this. We greatly appreciate your understanding and thank you for being a Barnes & Noble customer.

Barnes & Noble

FAQ

## **notification**

Barnes & Noble states that no payment details have been exposed but are unsure at this time if the hackers accessed other personal information.

They do admit that email addresses, billing addresses, shipping addresses, and purchase history were exposed on the hacked systems.

In response to our queries about the attack, Barnes & Noble shared the following statement.

"As the letter to our customers explains, we closed down all our networks immediately once a cybersecurity attack was suspected. We engaged then a firm of cybersecurity consultants to evaluate the nature of the threat. With their guidance, we have cautiously restored our networks which by its nature has taken time. We acted as quickly as we could given the circumstances and notified customers once we were able to give credible information of what happened. No credit card details are stored on Barnes & Noble systems and therefore

## **Barnes & Noble email**

the speculation that financial loss from fraudulent activity could result is inaccurate. As of writing, the cybersecurity consultants have detected no evidence of data having been exposed. We have acted therefore with an abundance of caution. We regret sincerely that in so acting we have caused disruption to our customers, especially those of NOOK."

## Egregor claims to have stolen Barnes & Noble data

After publishing our report on the Barnes & Noble cyberattack, BleepingComputer was contacted by a threat actor who stated that the Egregor ransomware operation was behind the attack.

Egregor is a relatively new but active ransomware gang that began operating in the middle of September 2020.

BleepingComputer was told that Barnes & Noble's corporate network was compromised by threat actors who stole unencrypted "financial and audit" data from their systems.

After the hacker gained access to a Windows domain administrator account, another threat actor was given access to the network on October 10th, 2020, who then encrypted the network's devices.

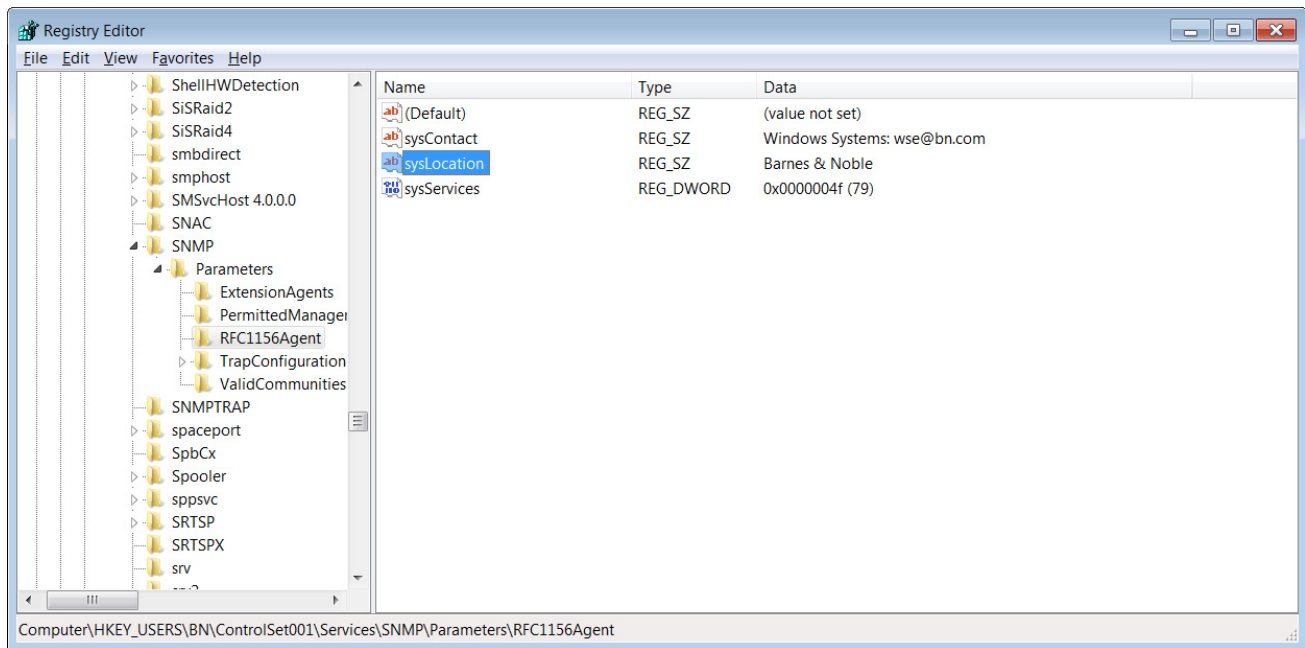
Today, the Egregor ransomware operation confirmed the threat actor's statements and published files that they claim were stolen during the attack on Barnes & Noble.

The screenshot shows a ransomware site with the following elements:

- Header: "Barnes & Noble Booksellers, Inc." with a "New" badge and "Published: 1%" badge.
- Section: "First part of data" (purple button).
- Text: "This is small proof pack for Barnes and Nobble. If they are not contact us we prepare another pack with Barnes and Noble users personal data."
- URL: "http://www.barnesandnoble.com/"
- Address: "122 Fifth Avenue, New York, NY 10011"
- Section: "First part of data" (purple button).
- Hashtag: "# ransomware" (purple button).
- Visits: "Visited: 232" (blue button).

### Barnes & Noble data leak on Egrogor site

Strangely, instead of leaking stolen files, the leaked data contains two Windows Registry hives that appear to have been exported from Barnes & Noble's Windows servers during the attack.



### Leaked Registry hive

While this corroborates that Egregor was involved in the attack, it does not necessarily prove that Egregor stole any financial documents or other files.

BleepingComputer has reached out again to Barnes & Noble with questions regarding this development.

Egregor also recently attacked game developers Crytek and Ubisoft, whose stolen data was also leaked online.

### Related Articles:

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

[Costa Rica declares national emergency after Conti ransomware attacks](#)

[Quantum ransomware seen deployed in rapid network attacks](#)

[New Black Basta ransomware springs into action with a dozen breaches](#)

[American Dental Association hit by new Black Basta ransomware](#)

- [Barnes & Noble](#)
- [Cyberattack](#)
- [Data Exfiltration](#)
- [Egregor](#)

- [NOOK](#)
- [Ransomware](#)
- [Registry](#)

[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](#)

## Comments

---



[Matthew123454321](#) - 1 year ago

- 
- 

My mother received a letter, from Barnes and Noble, regarding this hack - She is a Barnes and Noble rewards member.

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:**

---