Egregor Claims Responsibility for Barnes & Noble Attack, Leaks Data

By Tara Seals

Published: 2020-10-21 · Archived: 2026-04-05 22:47:50 UTC

The ransomware gang claims to have bought network access to the bookseller's systems before encrypting the networks and stealing "financial and audit data."

The Egregor ransomware gang has reportedly taken responsibility for the Barnes & Noble cyberattack, first disclosed on Oct. 15.

The bookseller warned last week that it had been hacked in emailed notices to customers, noting that a cyberattack happened on Oct. 10, "which resulted in unauthorized and unlawful access to certain Barnes & Noble corporate systems."

Some indications — such as its Nook e-reader service being taken offline starting the weekend before — also pointed to a possible ransomware attack, though the company still hasn't yet confirmed that. Some store workers told an e-reader blog that their physical registers were having trouble over that weekend, too.

Now, the Egregor group – a new kid on the block, having emerged only in September – said that its malware was responsible, and claimed to have stolen unencrypted "financial and audit" data.

It's unclear if that refers to internal corporate data or consumer information. The book giant stressed in its notice to customers that all exposed user financial data was "encrypted and tokenized and not accessible. At no time is there any unencrypted payment information in any Barnes & Noble system."

In correspondence with Bleeping Computer, a member of the group said that someone was able to gain access to a Windows domain administrator account, before handing over (or selling) that access to the Egregor gang.

And indeed, network-access sellers have become "a central pillar of criminal underground activity in 2020," according to a recent Accenture report. For prices between $300 and $10,000, ransomware groups have the opportunity to easily buy initial network access to already-compromised companies on underground forums.

That investment has apparently paid off: Egregor has also now published "two Windows Registry hives that appear to have been exported from Barnes & Noble's Windows servers during the attack," according to the media report. The files however don't prove that the gang has financial data.

Threatpost has reached out to Barnes & Noble for confirmation and details.

For the full Threatpost report on the hack, including coverage of the threats to consumers and researcher reactions, please click here.

Egregor Ramps Up

Egregor was first spotted in the wild in September, using a tactic of siphoning off corporate information and threatening a "mass-media" release of it before encrypting all files.

Just this week, it claimed to have hacked gaming giant Ubisoft, lifting the source code for Watch Dogs: Legion, which is due to be released on Oct. 29. It's a highly anticipated release thanks to its 4K visuals, "ray tracing" capabilities and a planned Assassin's Creed crossover.

It also took responsibility for a separate attack on gaming creator Crytek, relating to gaming titles like Arena of Fate and Warface. In both cases, as with Barnes & Noble, it published inconclusive information on its leak site showing that it accessed files, but not necessarily the source code that it said that it had.

Egregor is an occult term meant to signify the collective energy or force of a group of individuals, especially when the individuals are united toward a common purpose — apropos for a ransomware gang. According to a recent analysis from Appgate, the code seems to be a spinoff of the Sekhmet ransomware (itself named for the Egyptian goddess of healing).
