Vice Society: Ransomware Gang Disrupted Spar Stores

govinfosecurity.com/vice-society-ransomware-gang-disrupted-spar-stores-a-18225

Business Continuity Management / Disaster Recovery , Cybercrime , Cybercrime as-a-service

Criminals Dump Data Stolen From Spar Store Operators in England and Isle of Man Mathew J. Schwartz (euroinfosec) • December 30, 2021

Photo: Spar

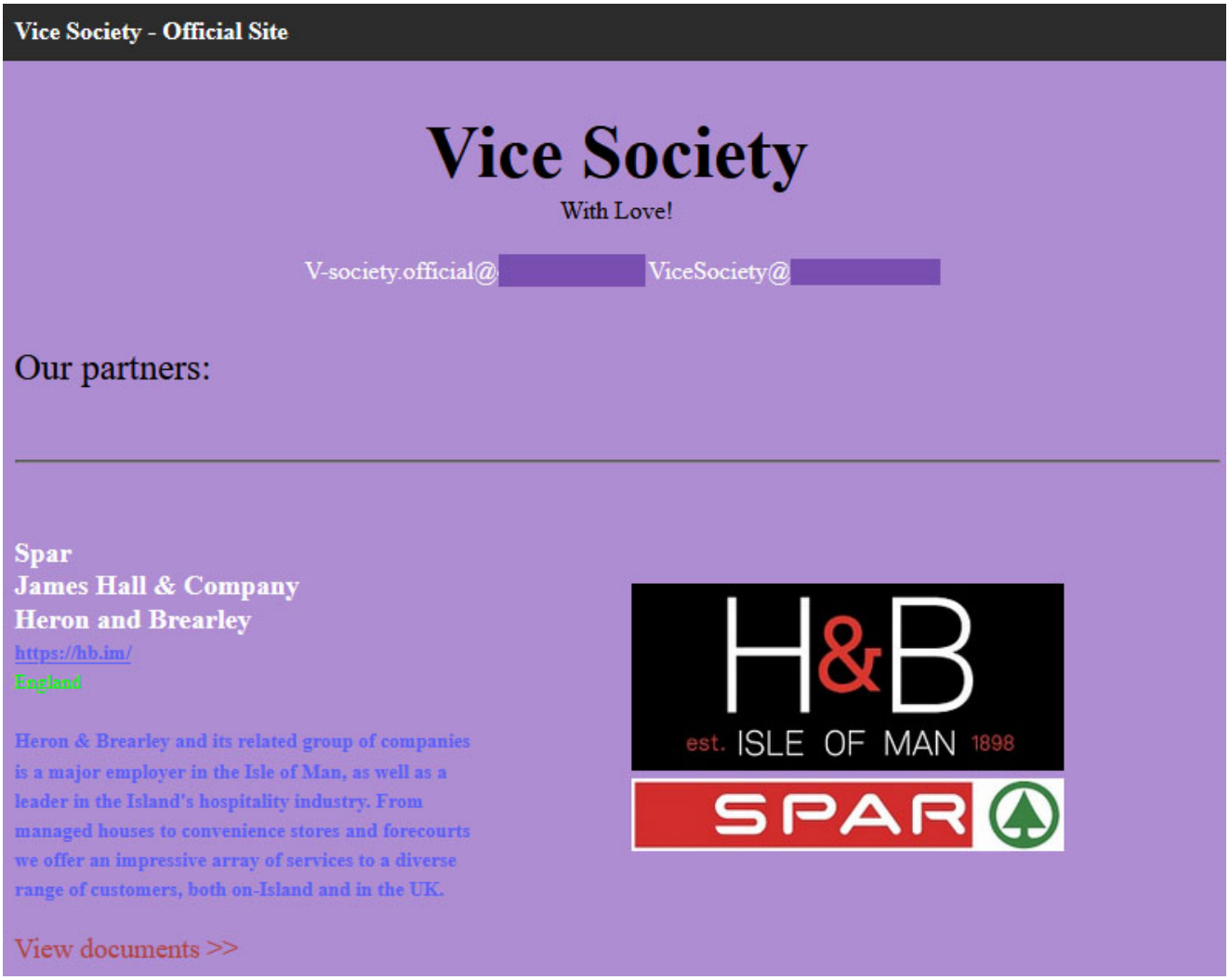
A ransomware operation called Vice Society has claimed credit for attacks that hit two groups of independently owned and operated Spar-branded stores earlier this month.

See Also: OnDemand | Understanding Human Behavior: Tackling Retail's ATO & Fraud Prevention Challenge

On Dec. 6 via Twitter, Spar reported that for some of its U.K. operations, "there has been an online attack on our IT systems which is affecting stores' ability to process card payments, meaning that a number of Spar stores are currently closed."

No specific ransomware group was blamed for the attack. But the Vice Society ransomware group on Friday claimed credit for the hit via its data leak site, says Israeli threat intelligence firm Kela.

Specifically, Vice Society says it infected systems at James Hall & Co., which acts as the primary wholesaler to more than 600 Spar stores in the north of England, and Heron and Brearley, owner of Mannin Retail, which operates 19 Spar stores on the Isle of Man. The Isle of Man is a self-governing British Crown Dependency located in the Irish Sea between Great Britain and Northern Ireland.



Screenshot from the Vice Society data leak site (Source: Kela)

"When browsing through files leaked by Vice Society, Kela saw documents apparently related to Spar operations, as well as to both companies mentioned in the listing," Victoria Kivilevich, director of threat research at Kela, tells Information Security Media Group. "The gang published more than 93,000 files."

Attack Aftermath

The naming of the victims by Vice Society, as well as the dumping of their allegedly stolen data, suggests that neither business paid a ransom to the attackers.

Heron and Brearley didn't immediately respond to a request for comment. Multiple emails sent to James Hall & Co., for which the website continues to be offline, were returned as undeliverable.

Britain's National Cyber Security Center on Dec. 10 confirmed that James Hall & Co. had been attacked.

"We are aware of an incident affecting some Spar stores serviced by James Hall & Co. in the North of England and are working with partners in response," an NCSC spokesman said at the time. "James Hall & Co. has confirmed that it is now bringing affected stores back online."

The NCSC also urged organizations to follow its ransomware guidance "help mitigate attacks, their impact and enable effective recovery."

More Attacks

Vice Society first launched its data leak site in May, on which it listed Indianapolis, Indiana-based Eskenazi Health, a public health provider. The same month, the group also appeared to have been behind a ransomware attack against New Zealand's Waikato District Health Board.

> And now Vice Society launched their data leak site. At least one of the victims was hit by ransomware just recently in May. https://t.co/sbreVwximY pic.twitter.com/abUvSPMupC— KELA (@Intel_by_KELA) June 24, 2021

Since then, the group has continued to rack up new victims. In the past week, for example, beyond the Spar operators, the gang has also claimed credit for infecting with ransomware a Brazilian dental company and a Colombian university.

Data-Leaking Ransomware Groups Continue

Vice Society is just one of a number of active ransomware groups that run data leak sites. In the past 10 days, Kela says multiple groups have listed fresh victims on their sites. The groups include Alphv - aka Blackcat, AvosLocker, AtomSilo, BlackByte, Clop, Conti, 54bb47h, Grief, Hive, LockBit, LV, Quantum, Rook, Snatch and Vice Society.

The monthly total number of victims being listed on ransomware groups' data leak sites continues to increase. Cybersecurity firm Group-IB has reported that for the 12 months ending on June 30, the number of publicly listed initial access offers - compared to the preceding 12-month period - nearly tripled, increasing from 362 to 1,099.

That trend has been continuing, says Allan Liska, an intelligence analyst at threat intelligence firm Recorded Future. In September, he reported that the total number of monthly victims being listed across all ransomware groups' data leak sites had hit an all-time high.

But the number of victims of ransomware groups remains unclear, in part because multiple gangs don't run data leak sites or attempt to publicly name and shame victims. And of the ones that do, Group-IB estimates that only 13% of such groups' victims ever get listed on a

data leak site.