Severity: High

Date: 10th Oct 2023

Description

The Ransomed.vc ransomware/extortion group was first reported by cybersecurity researchers in August 2023. The group targets organizations from various sectors, such as finance, insurance, technology, and telecommunications, primarily located in the United States and Europe.

Ransomed.vc compromises the victims' servers, steals their data, and extorts them to pay a ransom or else they will face a GDPR fine when the group exposes their data. It is unclear whether the threat actors encrypt the victims' files (as the group name suggests) or just steal files and extort payment for deleting or not publishing them.

The domain of Ransomed.vc was originally created as a competitor for the popular underground hacking forum, Breached, but soon was repurposed as a data leak site for ransomware victims. The leak site contains an indication of the victims who paid or did not pay the ransom and ways to contact the threat actors through email or Telegram. In addition, the site presents an invitation for affiliates to join the ransomware operation. On their Telegram channel, t itled: "Ransomed.vc - Peace Tax Agency," the threat actors claim that they attack "the people that disturb the peace" and make them "pay a tax for it."

Impact

The group demands ransoms of between €50,000 to €200,000.

Among RansomedVC past victims, according to the group's leak site: State Farm Insurance, S&P Global, TransUnion,

Optimity, A1 Telekom Austria, and I&G Insurance Brokers.

On **October 5, 2023**, Ransomed.vc created a data leak entry for the District of Columbia Board of Elections (DCBOE). The threat actors allegedly stole the personal data of 600,000 D.C. voters and already published the data of one individual as proof (including the individual's name, registration ID, voter ID, partial Social Security number, driver's license number, date of birth, phone number, email address, and more). According to the DCBOE's investigation, the attackers accessed. The information through the web server of Data Net, the hosting provider for Washington D.C.'s election authority.

While Ransomed.vc claimed responsibility for the attack, security researchers found that the same dataset was put for sale two days earlier on the underground hacking forums, Breach Forums and Sinister.ly, by a user named "pwncoder." Those posts have since been deleted.

IOC

URL's

(http://k63fo4qmdnl4cbt54sso3g6s5ycw7gf7i6nvxl3wcf3u6la2mlawt5qd.onion)

(http://f6amq3izzsgtna4vw24rpyhy3ofwazlgex2zqdssavevvkklmtudxjad.onion/)

Emails

(admin@ransomed.vc)

(RFadmin@thesecure.biz)

Domains

(ransomed.vc)

Reference Links

https://www.hackread.com/ransomedvc-ransomware-group-sony-cyberattack/