Ransomware Gang Demands $42 Million From Celebrity Law Firm

The operators of the REvil ransomware strain are attempting to ratchet up the pressure on a high-profile New York law firm to pay a $42 million ransom before releasing more data on the firm's roster of celebrity clients, according to multiple reports and security experts.

In this case, the operators of the REvil ransomware are focusing their pressure campaign on the law firm of Grubman Shire Meiselas and Sacks, which represents some of the most recognizable celebrities in the world, including Lady Gaga, Madonna, Mariah Carey, U2, Bruce Springsteen, Mary J. Blige and many others.

Earlier this month, the REvil operators claimed to have breached the law firm, according to Bleeping Computer. On May 11, Grubman Shire Meiselas and Sacks confirmed to entertainment news site Variety that the firm was hit with a "cyberattack," which turned out to be REvil ransomware. At that time, the gang asked for $21 million to decrypt the firm's data, according to a copy of the ransom note seen by cybersecurity firm Emsisoft and shared with Information Security Media Group.

It's not clear if the Grubman Shire Meiselas and Sacks law firm decided to communicate or negotiate with the REvil operators, although the criminal gang claims that the firm offered a payment of $365,000, according to the posting provided by Emsisoft.

When full ransom demands were not met by Thursday, the REvil operators began releasing some of the data that they claim to have in their possession. This included what appears to be about 2 GB of legal and contractual data related to Lady Gaga, according to Emsisoft.

On Friday, the REvil, which is also known as Sodin and Sodinokibi, posted a notice to their dark net web portal that it was now demanding $42 million from the law firm, according to Emsisoft. In addition, the ransomware gang also threatened to released data related to President Donald Trump.

"There's an election race going on, and we found a ton of dirty laundry on time. Mr. Trump, if you want to stay president, poke a sharp stick at the guys, otherwise you may forget this ambition forever," according to the REvil post. "And to you voters, we can let you know that after such a publication, you certainly don't want to see him as president. Well, let's leave out the details. The deadline is one week."

The problem with that threat is the Trump has never been a client of the Grubman Shire Meiselas and Sacks either as a real estate developer, television celebrity or president, according to the New York Post, which cited sources. The FBI is also now looking into the incident as well, according to Forbes.

Whether the REvil gang has data related to Trump, the attack has put the law firm in a nearly impossible position, says Terence Jackson, CISO of security firm Thycotic.

"The documents have already been leaked and there is no guarantee if they pay the ransom in full the documents won't get leaked anyway," Jackson tells ISMG. "The reputational damage is already done. I'm also sure the firm is keenly aware of the potential legal issues they are facing."

Ransomware as Extortion Racket

Over the past several weeks, more organizations have not only had to deal with the threat of crypto-locking malware targeting their data, but ongoing threats by various ransomware gangs to steal and release this information if payments are not met.

After the operators of the Maze ransomware first pioneered the tactic of threatening to dump data if victims did not play in 2019, other gangs followed suit. This includes REvil, DoppelPaymer, MegaCortex, Nemty and Snatch.

More recently, a group known as Ako announced it is now targeting some large victims with two ransoms: One in return for receiving a decryptor, and another to not dump stolen files. The asking price for the second ransom demand is between $100,000 and $2 million, according to reports.

"Ransomware groups are now weaponizing data and using it against the companies from which it was stolen," says Brett Callow, a threat analyst with Emsisoft who's been following this latest round of ransomware and extortion threats.

"They no longer simply threaten to publish it, they also threaten to sell it competitors, expose dirty secrets or use it to attack companies' business partners," Callow notes.

"Further, certain groups now charge separate amounts for decryption and deletion of the stolen data. Should a company pay only for decryption, its data is published together with details of the amount of ransom paid."

In the past several months, REvil or Sodinokibi have managed to extort large ransom from several victims.

In April, the Wall Street Journal reported that Travelex, a London-based foreign currency exchange that does business in 26 countries, including the U.S., paid REvil $2.3 million to regain access to its data following an attack on New Year's Eve.

Extract from - REvil Gang Ups Ransom Ante After Releasing Data on Lady Gaga
Asokan_akshaya) • May 16, 2020
Managing Editor of DataBreach Today Scott Ferguson contributed to this report.