REvil ransomware threatens to leak A-list celebrities' legal docs

By Ionut Ilascu

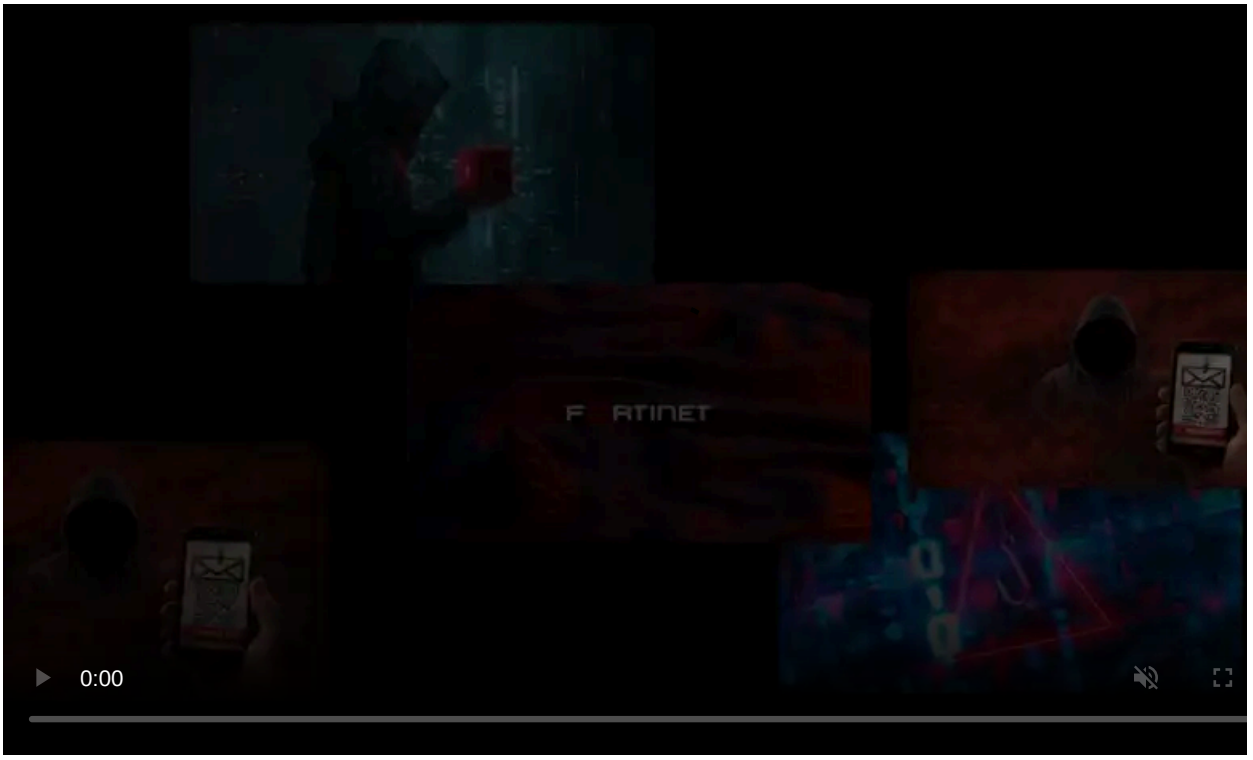
Published: 2020-05-08 · Archived: 2026-04-06 00:19:32 UTC

The Sodinokibi ransomware group threatens to release hundreds of gigabytes of legal documents from a prominent entertainment and law firm that counts dozens of international stars as their clients.

Grubman Shire Meiselas & Sacks (GSMLaw) is based in New York and represents dozens of heavyweight artists. Looking at its list of clients, you can spot names that are known all over the world: Madonna, Lady Gaga, Elton John, Robert de Niro, Nicki Minaj, Chris Brown, Usher, U2, Timbaland, Rick Ross, and many others.

Big names all over

The company, self described as “universally recognized as one of the premier entertainment and media law firms in the country,” specializes in all areas of entertainment and media.


F RTINET
0:00

On its website, the company says that its “ability to advise and service clients in all aspects of their careers and businesses is unparalleled.”

Sodinokibi, also referred to as Sodin or REvil by some publications, allegedly hacked GSMLaw. To support their claim, the hackers published a screenshot of the folders they have.

The hackers say that the type of data they have includes contracts, phone numbers, email addresses, personal correspondence, non-disclosure agreements. However, the trove is not limited to these and supposedly is 756GB large.

To prove beyond dispute that they have the information they claim, Sodin also provides snippets from a legal agreement in 2013 signed by Christina Aguilera and an artist featured in one of her music projects. Aguilera’s name is not present on the list of clients, indicating that she no longer retains the firm’s services.

A fragment from another agreement between a crew member of the Madonna World Tour 2019-2020 and Live Nation Tours company.

The document is signed July 17, 2019 and contains the name of the crew member along with their social security number.

BleepingComputer has contacted partners at Grubman Shire Meiselas & Sacks for comments and is currently awaiting a reply.

Judging by Sodinokibi's past reputation, the actor is unlikely to make empty threats as in the past they have sold data stolen from victims that did not pay the ransom.

Their leak site currently has over two dozen entries for victims that did not pay the what the hackers asked. These companies are now risking data belonging them and their customers to be sold on various underground markets.

Sodinokibi is among the most profitable ransomware-as-a-business operations. Its affiliates use experts for breaking into private networks and navigating them undetected in search of the most valuable systems.

In March, they announced a "forced" switch from bitcoin to Monero cryptocurrency, to make it harder for law enforcement to track them.

Their main objective is to make money and they're at the top of the game.

Source: https://www.bleepingcomputer.com/news/security/revil-ransomware-threatens-to-leak-a-list-celebrities-legal-docs/