Sodinokibi Ransomware gang threatens to disclose data from Kenneth Cole fashion firm

securityaffairs.co/wordpress/98694/malware/sodinokibi-kenneth-cole-data-breach.html

February 29, 2020

Not only Maze ransomware gang, the operators behind Sodinokibi Ransomware allegedly leaked the data of Kenneth Cole Productions.

The operators behind Sodinokibi Ransomware have published the download links to archives containing data allegedly stolen from the US firm Kenneth Cole Productions.

The news was first reported by the Under the Breach research group.

> REvil Ransomware group just dumped the files of American fashion house, Kenneth Cole. (@kennethcole)
>
> -Provided a download link with some information about employees and financial information.
>
> -Claiming to have 60,000 personal data and 70,000 financial and work documents. pic.twitter.com/owmE2CdNPL
>
> — Under the Breach (@underthebreach) February 27, 2020

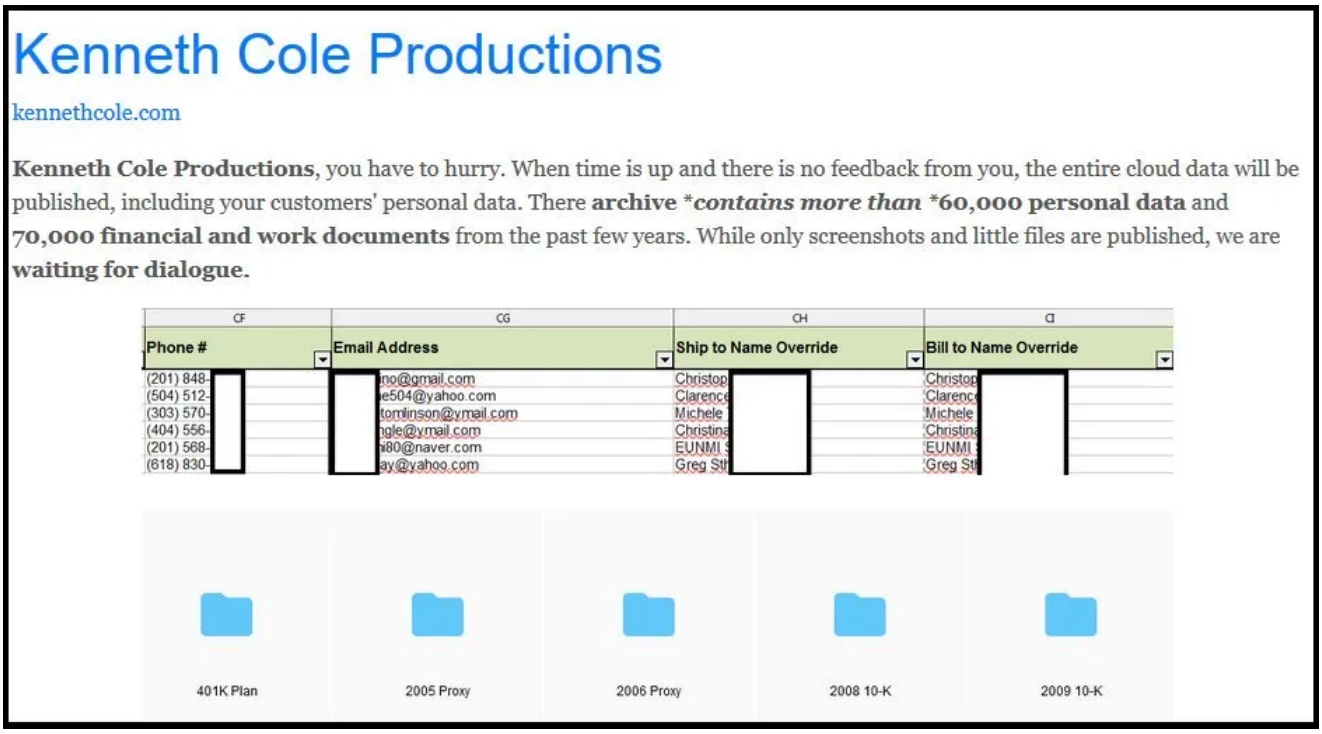
Sodinokibi (aka REvil) is available in the underground market as a Ransomware-as-a-Service model, the gang behind the Sodinokibi ransomware has been very active in the US in recent months, in December, CyrusOne, one of the major US data center provider, was hit by the same ransomware. In January, Synoptek, a California-based IT service provider decided to pay the ransom to decrypt its files after being infected with the Sodinokibi ransomware.

Kenneth Cole Productions, Inc. is an American fashion house founded in 1982 by Kenneth Cole.

The Sodinokibi ransomware operators claim to have stolen over 70,000 documents with financial and work data, and more than 60,000 records of company customers.

The Sodinokibi gang requested the payment of a ransom and threatens to leak online the full dump containing stolen data in case the company will decide to not meet the request.

"*Kenneth Cole Productions, you have to hurry," the ransomware operators said. "When time is up and there is no feedback from you, the entire cloud data will be published, including your customers' personal data."*



In December, for the first time, the crime gang behind the Maze ransomware, decided to blackmail the victims and force them to pay the ransom.

This move is shocking and brings the ransomware attack to a higher level of threat, we can expect that other cybercrime gangs will adopt a similar strategy to blackmail the victims and force them to pay the ransom.

Other groups, such as the Nemty Ransomware and BitPyLock gangs adopted the same technique in January 2020.

Pierluigi Paganini

(SecurityAffairs – hacking, Kenneth Cole)

Back to top

- Home
- Cyber Crime
- Cyber warfare
- APT

- Data Breach
- Deep Web
- Digital ID
- Hacking
- Hacktivism
- Intelligence
- Internet of Things
- Laws and regulations
- Malware
- Mobile
- Reports
- Security
- Social Networks
- Terrorism
- ICS-SCADA
- EXTENDED COOKIE POLICY
- Contact me