Sodinokibi Ransomware Posts Alleged Data of Kenneth Cole Fashion Giant

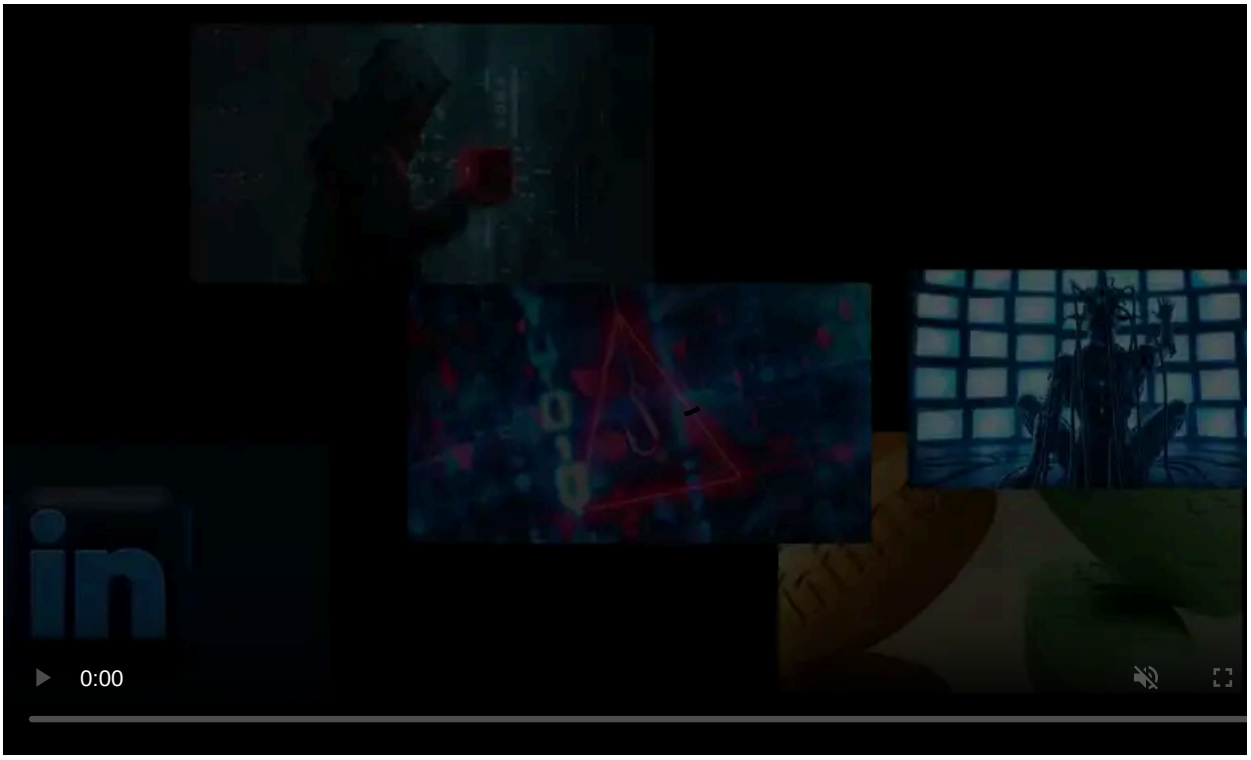
By Sergiu Gatlan

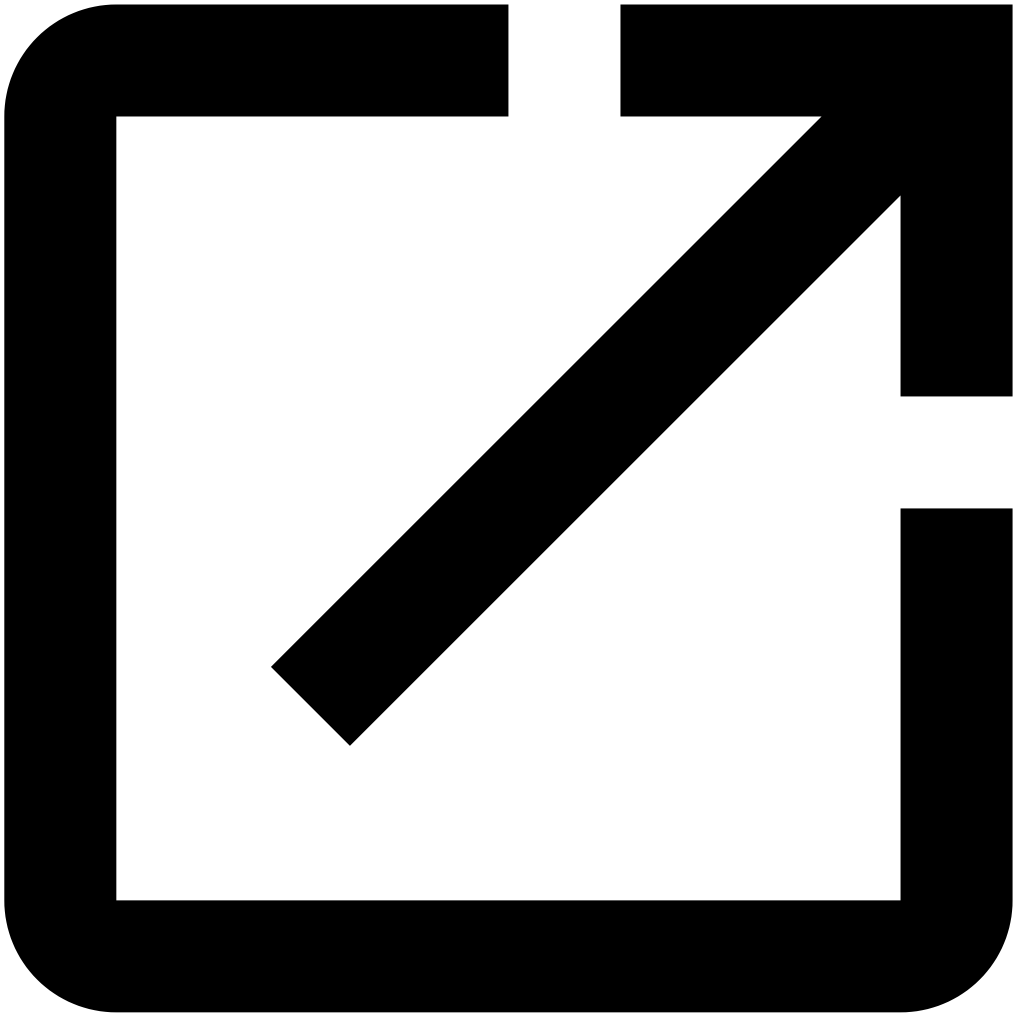
Published: 2020-02-28 · Archived: 2026-04-05 18:14:34 UTC

The operators behind Sodinokibi Ransomware published download links to files containing what they claim is financial and work documents, as well as customers' personal data stolen from giant U.S. fashion house Kenneth Cole Productions.

Sodinokibi (aka REvil) is a Ransomware-as-a-Service operation where the operators manage development of the ransomware and the payment portal used by victims to pay the ransoms, while third-party 'affiliates' are in the business of distributing the ransomware to the targets' systems.

When victims pay, the ransomware payments are then shared between the affiliates and the Sodinokibi operators.


0:00



Kenneth Cole is a privately held fashion firm headquartered in New York, founded 38 years ago, in 1982, and known as "one of the world's most recognized fashion companies."

Threats of publishing all Kenneth Cole stolen data

The ransomware operators claim to have possession of a huge archive of over 70,000 documents with financial and work data, and more than 60,000 records with Kenneth Cole customers' personal information according to the Sodinokibi actors as a researcher at Under the Breach discovered.

BleepingComputer was told that the leaked data allegedly belonging to Kenneth Cole includes employee severance information, cash projections, and money owed to the company.

Sodinokibi also threatens to publish the full data cache if the American fashion house fails to reply to their ransom requests until the ransom's timer runs out.

"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."

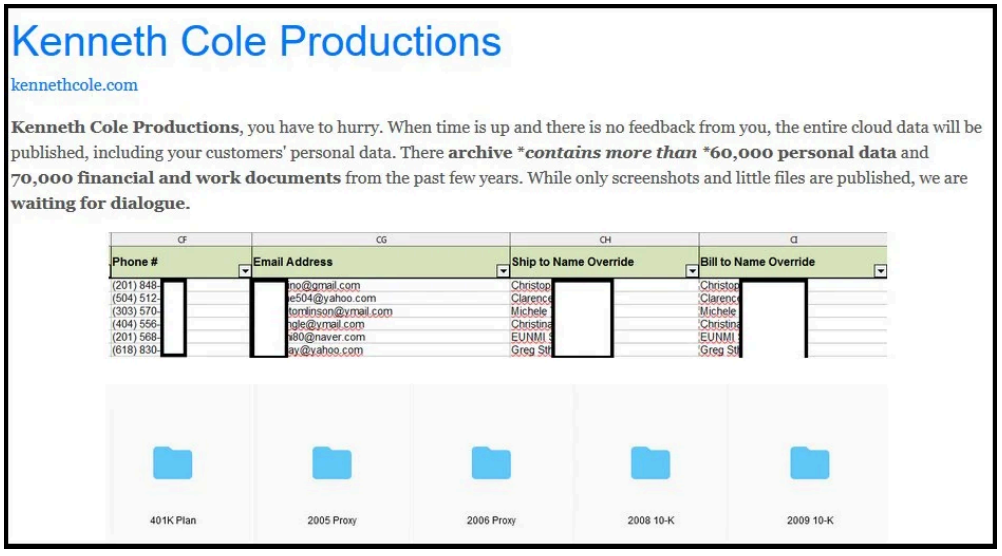


Image: Under the Breach

This wouldn't be the first time Sodinokibi has published data from their victims as we reported when covering the ransomware attack that impacted US IT staffing company Artech Information Systems in January.

At the time the ransomware operators also threatened to sell the data they stole from Artech on several data exchange platforms known as heavily frequented by cybercriminals.

While we were told that the leaked data appears to be legitimate, Kenneth Cole has not responded to our queries to confirm if and when they were attacked, and whether the data belongs to them.

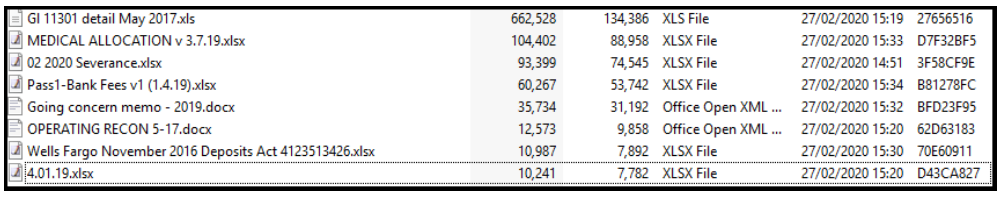


Image: Under the Breach

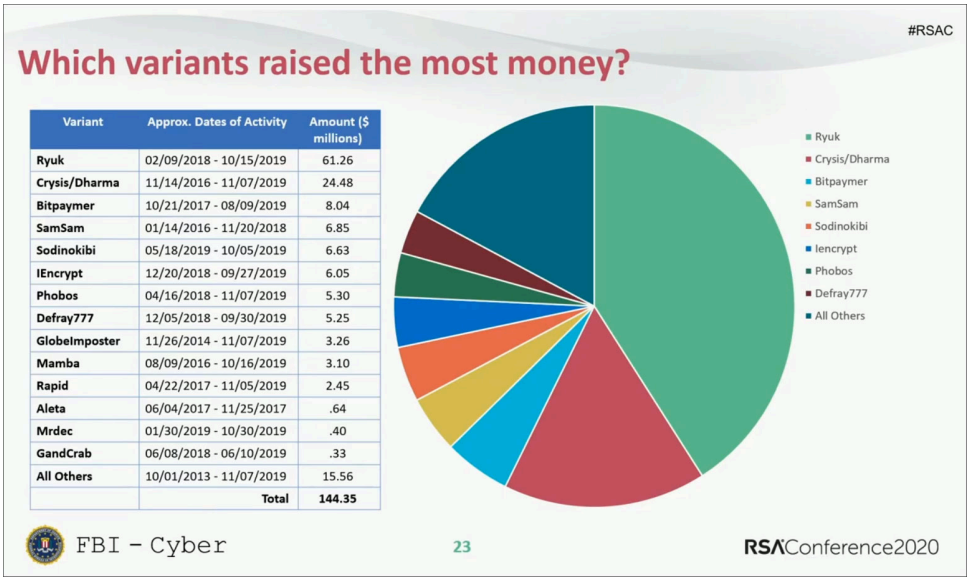
Stolen data is now used to 'incentivize' victims to pay

Collecting and stealing sensitive data before encrypting systems with ransomware and then leaking the stolen data in stages until the victims give in and pay the ransom is a recently adopted tactic by ransomware gangs.

This new alarming trend was started by Maze Ransomware in late November 2019 and was soon adopted by Sodinokibi, Nemty Ransomware, and BitPyLock during January 2020.

To make matters even worse for future ransomware victims, Sodinokibi also recently shared plans to email stock exchanges like NASDAQ about attacks on publicly traded companies to hurt their stock, something that can be used as an extra pressure point to convince them to pay ransoms.

Just to get an idea of the scale of the ransoms asked by ransomware gangs during the last six years, the FBI said earlier this week at the RSA security conference that victims have paid more than $140 million worth of bitcoins to ransomware operators based on analysis of collected ransom notes and ransomware bitcoin wallets.



Variant	Approx. Dates of Activity	Amount ($ millions)
Ryuk	02/09/2018 - 10/15/2019	61.26
Crysis/Dharma	11/14/2016 - 11/07/2019	24.48
Bitpaymer	10/21/2017 - 08/09/2019	8.04
SamSam	01/14/2016 - 11/20/2018	6.85
Sodinokibi	05/18/2019 - 10/05/2019	6.63
IEncrypt	12/20/2018 - 09/27/2019	6.05
Phobos	04/16/2018 - 11/07/2019	5.30
Defray777	12/05/2018 - 09/30/2019	5.25
GlobeImposter	11/26/2014 - 11/07/2019	3.26
Mamba	08/09/2016 - 10/16/2019	3.10
Rapid	04/22/2017 - 11/05/2019	2.45
Aleta	06/04/2017 - 11/25/2017	.64
Mrdec	01/30/2019 - 10/30/2019	.40
GandCrab	06/08/2018 - 06/10/2019	.33
All Others	10/01/2013 - 11/07/2019	15.56
	Total	144.35

Ryuk took first place in a top of ransomware families that raked in $61.26 million in ransoms, way in front of Crysis/Dharma with $24.48 million and Bitpaymer with $8.04 million.

Despite some of the huge numbers seen by the FBI while analyzing the ransom amounts paid by ransomware victims, it's important to note that the full ransom amount is most probably a lot larger given that the agency didn't have access to all the wallets and ransom notes.

Also, many of the victims that got hit by ransomware prefer to keep the attacks under wraps fearing the impact on their stock prices.
