SeaChange video platform allegedly hit by Sodinokibi ransomware

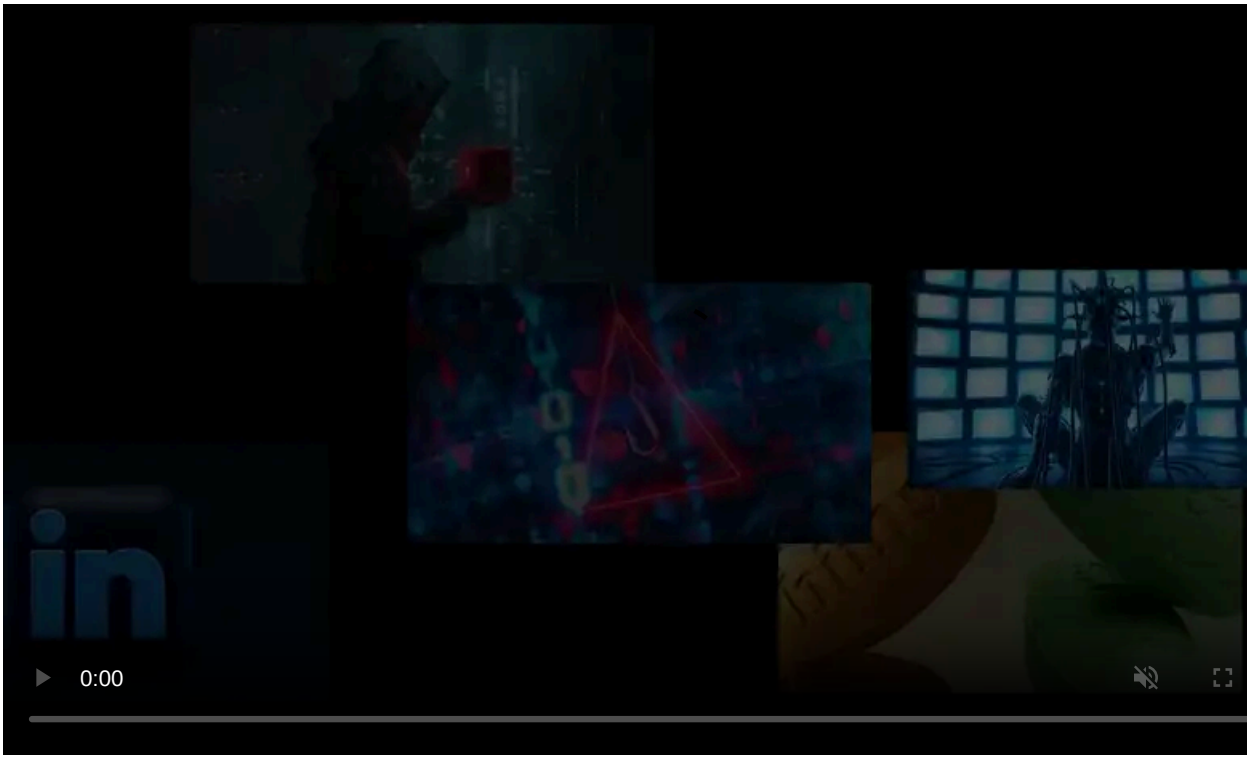
By Lawrence Abrams

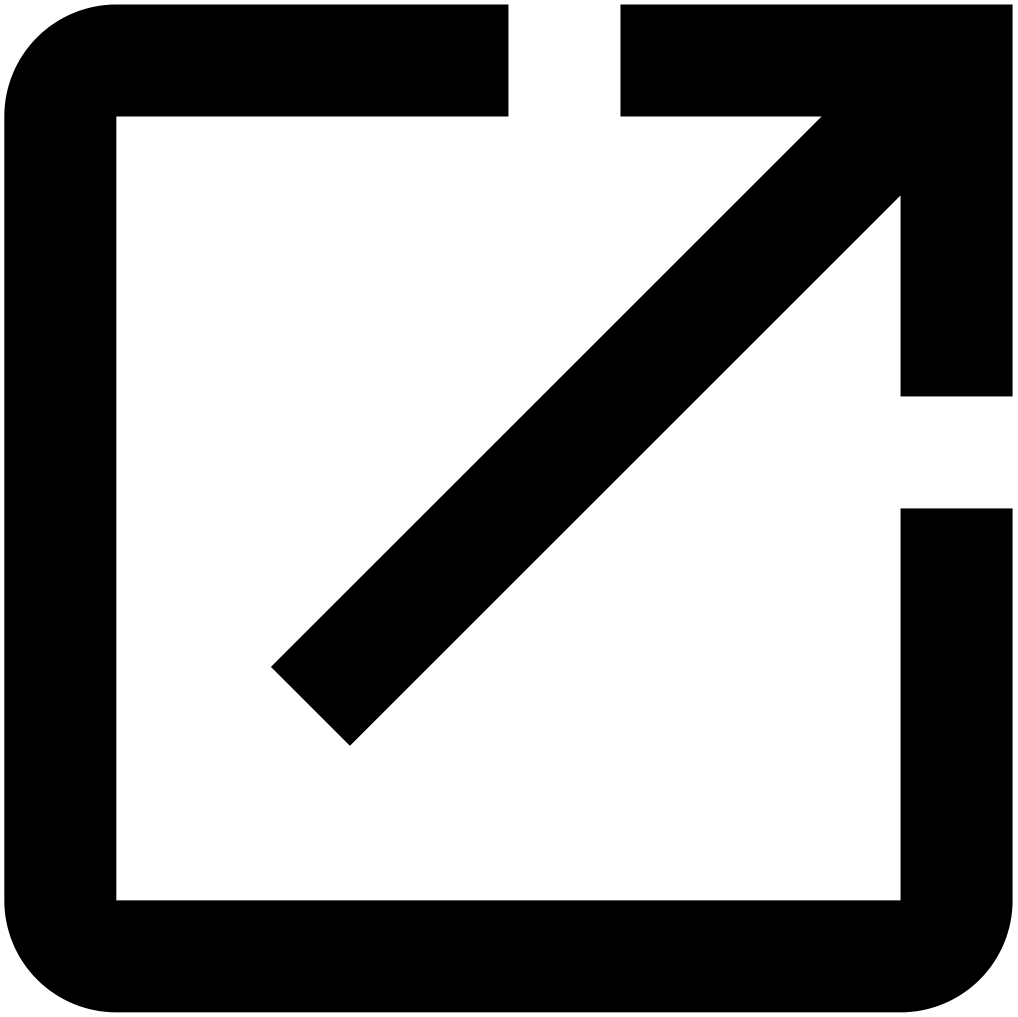
Published: 2020-04-23 · Archived: 2026-04-05 18:25:10 UTC

A leading supplier of video delivery software solutions is reportedly the latest victim of the Sodinokibi Ransomware, who has posted images of data they claim to have stolen from the company during a cyberattack.

SeaChange, a Waltham, Massachusets company with locations in Poland and Brazil, is an on-premise or remotely managed video-on-demand and streaming platform provider. SeaChange's customers include the BBC, Verizon, DISH, COX, DirecTV, and COX.

Since last year, ransomware operators have been launching data leak sites that they use to publish files stolen from victims when performing a ransom attack.


0:00

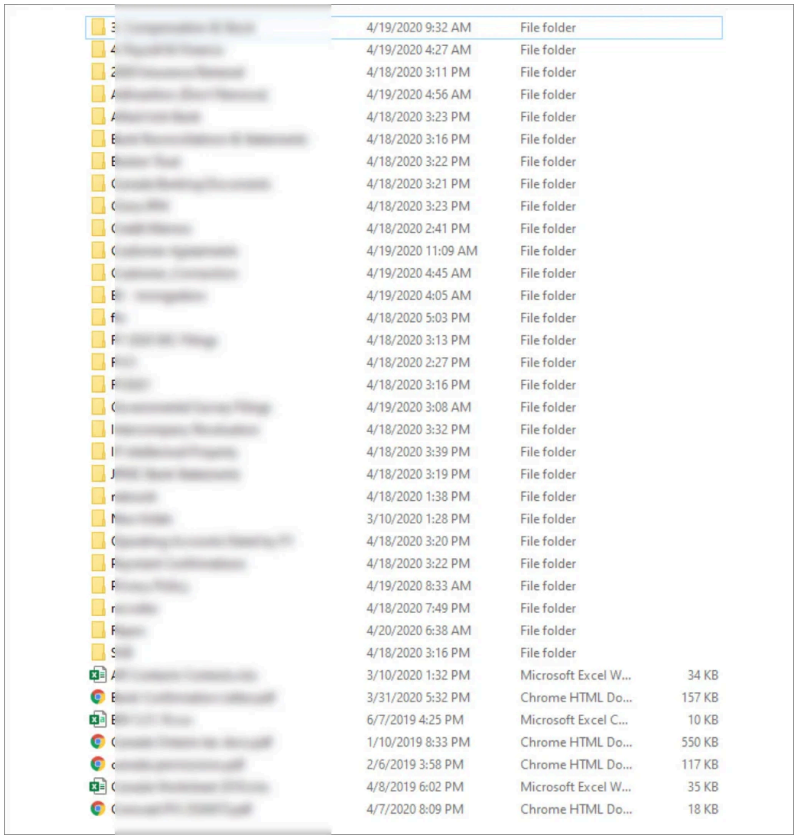


Ransomware operators use this tactic to scare and pressure non-paying victims into paying a ransom.

Sodinokibi posts images of SeaChange's data

In an update to their data leak site, Sodinokibi (REvil) has created a new victim page for SeaChange where they have published images of some of the documents that they have stolen during an alleged attack.

These images include a screenshot of folders on a server they claim to have had access to, a bank statement, insurance certificates, a driver's license, and a cover letter for a proposal for a Pentagon video-on-demand service.



Alleged SeaChange directory listing posted by REvil

When we asked the Sodinokibi operators how much the ransom was and the amount of data stolen, they refused to provide any further information.

"Thank you for your interest and your questions, but I really can't answer.
We publish confidential information about companies if they ignore us for a long time or decide not to pay. Otherwise, we are not ready to share any information about them in their own interests, including share which companies we have encrypted, how much data we have stolen, etc."

It is common for ransomware operators to slowly release small amounts of stolen data to continue applying pressure on their victims.

When asked if the DOD was aware of this breach, we were told that the DOD will not comment on network intrusions or investigations.

"In accordance with policy, we will have no information to provide on possible network intrusions or investigations into possible network intrusions in either DOD or contractor networks," Lt Col Robert Carver, a Department of Defense spokesman, told BleepingComputer.

When BleepingComputer reached out to SeaChange to learn if they were aware of the posting of this data, we did not receive a response to our multiple queries.

Update 4/24/20: Added statement from the DOD.

Source: https://www.bleepingcomputer.com/news/security/seachange-video-platform-allegedly-hit-by-sodinokibi-ransomware/