REvil ransomware group returns following Kaseya attack

By Catalin Cimpanu

Published: 2023-01-18 · Archived: 2026-04-05 19:24:26 UTC

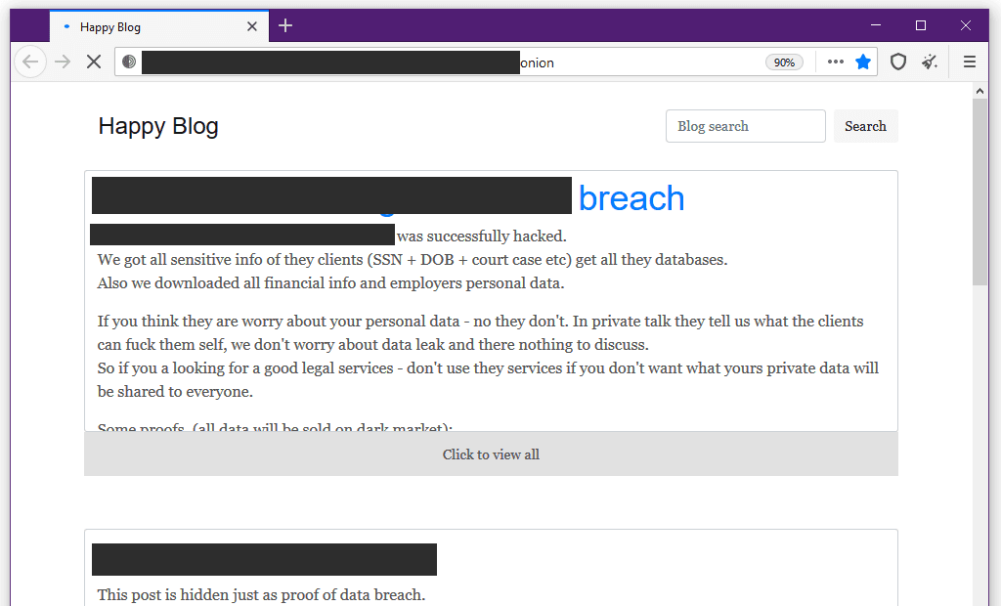
Dark web portals previously operated by the REvil ransomware gang have come back to life earlier today, sparking fears that the once-vaunted ransomware gang will soon resume its attacks.

The website, called the **Happy Blog**, was one of the many servers that REvil members shut down on July 13, earlier this year.

The group took down its web infrastructure following a mass ransomware attack against Kaseya servers during the July 4th US holiday that hit thousands of businesses, an incident that drew veiled threats and the attention of White House officials.

At the time, many suggested the group had disbanded and was preparing to launch a new rebranded ransomware operation in an attempt to throw off US law enforcement investigators and security firms.

But earlier today, almost two months since the shutdowns, the group's Happy Blog, a website where REvil operators typically listed victims who refused to negotiate or pay ransoms, is back online on the dark web, according to security researchers from Recorded Future and Emsisoft.



At the time of writing, the website is still listing the same victims it listed at the time of its shutdown on July 13.

In addition, REvil's "payment portal," where victims are told to go and negotiate with the REvil gang, has also been restored at the same old dark web .onion URL.

At the time of writing, no new REvil samples have been spotted by security researchers, and it remains unclear if REvil operators have also launched new attacks.
