REvil Disappears Again: ‘Something Is Rotten in the State of Ransomware’

flashpoint-intel.com/blog/revil-disappears-again/

October 18, 2021

Blogs

Blog

Flashpoint analysts are tracking the evolving situation around the re-disappearance of REvil. As of October 17, 2021, the REvil leaks blog, known as the Happy Blog, is offline and inaccessible.

Flashpoint analysts are tracking the evolving situation around the re-disappearance of REvil. As of October 17, 2021, the REvil leaks blog, known as the Happy Blog, is offline and inaccessible.

Additionally, on October 17, a REvil operator announced that the ransomware group was shutting down on the high-tier Russian language forum XSS after their domain had been “hijacked.” The threat actor explained that an unidentified person had used the private Tor keys of the group’s former spokesperson, “Unknown,” to access the REvil domain.

After the ransomware group shut down in July 2021, REvil operators believed Unknown had disappeared. However, between noon and 5pm Moscow time, the REvil operation stated that the REvil domain was accessed using Unknown’s keys, confirming their concerns that a third-party has backups with their service keys. The REvil operator added that the REvil

server was compromised and the hijacker deleted “0-neday’s” access to their hidden admin server. 0_neday believes the hijacker was looking for them. 0_neday signed off XSS and wished the participants “good luck”

Flashpoint analysts note that this was an unexpected turn in REvil’s attempt to reconstitute their operations, as the group had just begun recruiting new affiliates on the RAMP forum, and offering unusually high commissions of 90 percent to attract affiliates. Flashpoint analysts are tracking the situation and will provide updates as they arise.

Users on XSS were generally incredulous at this new announcement. The spokesperson of the LockBit ransomware gang claimed this new disappearance is proof that the REvil re-emergence in September was part of an elaborate FBI plot to catch REvil affiliates. Several threat actors agreed with the Lockbit representative and added that they believed that REvil will re-emerge again under a totally new name, leaving behind recent scandals without having to pay out old affiliates. Another threat actor added, paraphrasing Shakespeare, “Something is rotten in the state of ransomware.”

On October 18, at 10AM EST, the XSS moderators closed the thread where REvil made the announcement and advised fellow users to block REvil accounts.