Ragnar Locker Breached 52 Organizations and Counting, FBI Warns

cyware.com/news/ragnar-locker-breached-52-organizations-and-counting-fbi-warns-0588d220/

The Ragnar Locker ransomware group has so far targeted over 50 organizations based in the U.S, with most victims in critical infrastructure sectors, according to the FBI.

The attack on critical infrastructure

A recent joint alert by the FBI and the CISA provides technical details about Ragnar Locker, including IOCs that organizations can use to spot and block ransomware.

- The agency observed 52 entities across 10 critical infrastructure sectors that were targeted by Ragnar Locker.
- These belonged to several critical sectors including manufacturing, financial services, energy, IT, government, and others.
- The IOCs in the alert has information such as Bitcoin addresses to collect the ransom and email addresses of operators.

More details about the attack

The ransomware operators terminate remote management software such as ConnectWise and Kaseya to evade detection and ensure logged-in admins do not interfere with the deployment process.

Closing lines

The FBI has asked security professionals to share any related information, such as copies of the ransom notes, malicious activity timelines, ransom demands, payload samples, and other IOCs with the local FBI Cyber Squad. This may help identify the attackers behind this ransomware group.

Ragnar Locker | ConnectWise | Critical Infrastructure Attacks

Publisher

Cyware