FBI: Ransomware gang breached 52 US critical infrastructure orgs

bleepingcomputer.com/news/security/fbi-ransomware-gang-breached-52-us-critical-infrastructure-orgs/

Sergiu Gatlan

By
Sergiu Gatlan

- March 7, 2022
- 03:16 PM
- 0

The US Federal Bureau of Investigation (FBI) says the Ragnar Locker ransomware gang has breached the networks of at least 52 organizations from multiple US critical infrastructure sectors.

This was revealed in a joint TLP:WHITE flash alert published on Monday in coordination with the Cybersecurity and Infrastructure Security Agency.

"As of January 2022, the FBI has identified at least 52 entities across 10 critical infrastructure sectors affected by RagnarLocker ransomware, including entities in the critical manufacturing, energy, financial services, government, and information technology sectors," the federal law enforcement agency said [PDF].

"RagnarLocker ransomware actors work as part of a ransomware family, frequently changing obfuscation techniques to avoid detection and prevention."

The flash alert focuses on providing indicators of compromise (IOCs) organizations can use to detect and block Ragnar Locker ransomware attacks.

IOCs associated with Ragnar Locker activity include info on attack infrastructure, Bitcoin addresses used to collect ransom demands, and email addresses used by the gang's operators.

Although the FBI first became aware of Ragnar Locker in April 2020, Ragnar Locker ransomware payloads were first observed in attacks months before, during late December 2019.

Ragnar Locker operators terminate remote management software (e.g., ConnectWise, Kaseya) used by managed service providers (MSPs) to manage clients' systems remotely on compromised enterprise endpoints.

This allows the threat actors to evade detection and make sure remotely logged-in admins do not interfere with or block the ransomware deployment process.

Request for info linked to Ragnar Locker attacks

The FBI asked admins and security professionals who detect Ragnar Locker activity to share any related information with their local FBI Cyber Squad.

Useful info that would help identify the threat actors behind this ransomware gang includes copies of the ransom notes, ransom demands, malicious activity timelines, payload samples, and more.

The FBI added that it doesn't encourage paying Ragnar Locker ransoms since victims have no guarantee that paying will prevent leaks of stolen data or future attacks.

Instead, ransom payments will further motivate the ransomware gang to target even more victims and incentivizes other cybercrime operations to join in and launch their own ransomware attacks.

However, the federal agency did recognize the damage inflicted to businesses by ransomware attacks, which may force executives to pay ransoms and protect shareholders, customers, or employees.

The FBI also shared mitigation measures to block such attacks and strongly urged victims to report such incidents to their local FBI field office.

Since December, the FBI also revealed that Cuba ransomware compromised the networks of at least 49 US critical infrastructure entities, while the BlackByte ransomware gang hit at least three others.

Related Articles:

FBI: BlackCat ransomware breached at least 60 entities worldwide

FBI warns of ransomware attacks targeting US agriculture sector

US Senate: Govt's ransomware fight hindered by limited reporting

Cybersecurity agencies reveal top initial access attack vectors

US links Thanos and Jigsaw ransomware to 55-year-old doctor