FBI Warns of Uptick in Ragnar Locker Ransomware Activity

By Prajeet Nair

Archived: 2026-04-05 19:26:37 UTC

Business Continuity Management / Disaster Recovery , Fraud Management & Cybercrime , Governance & Risk Management

Bureau Says the Attacks Are Hitting Many Sectors (@prajeetspeaks) • November 25, 2020

A screenshot of the FBI alert

The FBI has sent out a private industry alert warning about an increase in attacks using Ragnar Locker ransomware.

See Also: Reduce Cloud Risk in Healthcare with Security by Default

Researchers first spotted Ragnar Locker in 2019. The FBI alert notes that its cyber division has been closely monitoring the malware since April, when its operators encrypted a large corporation's files and demanded an $11 million ransom to avoid release of 10 terabytes of sensitive company data.

"Since then, Ragnar Locker has been deployed against an increasing list of victims, including cloud service providers, communication, construction, travel and enterprise software companies," according to the alert.

Recent Attacks

Ragnar Locker has been linked to other high-profile security incidents over the last several months, including attacks targeting Energias de Portugal, or EDP, an energy company; Campari, an Italian liquor company; and

Capcom, a Japanese gaming firm (see: *Gaming Company Confirms Ragnar Locker Ransomware Attack*).

Ragnar Locker is one of several ransomware variants used to not only encrypt files of victims but also to exfiltrate data. Once this information is stolen, cybercriminals threaten to release the information as a way to make victims pay a ransom. Earlier his month, the Ragnar Locker gang hacked into a Facebook account and posted an ad about the Campari attack to pressure that company into paying (see: *Ransomware Gang Devises Innovative Extortion Tactic*).

Brett Callow, a threat analyst with the security firm Emsisoft, says the operators behind Ragnar Locker want to embarrass companies as much as possible to force them to pay a ransom and to serve as a warning to future victims.

"The group recently added an interesting element to their extortion attempts: namely, using compromised Facebook accounts to run ad campaigns in an effort to apply further pressure to their victims," Callow says. "While novel, the development was not particularly surprising. Other groups have put up press releases and contacted reporters directly, so an ad campaign was a logical progression."

Understanding Ragnar Locker

In an April report, Microsoft noted that Ragnar Locker is one of four strains of ransomware - also including Maze, RobbinHood and Vatet - that regularly get dropped onto systems after attackers gain remote access using stolen or brute-forced Remote Desktop Protocol credentials (see: *10 Ransomware Strains Being Used in Advanced Attacks*).

The FBI alert also notes that the operators behind Ragnar Locker use numerous obfuscation techniques to avoid detection by security tools.

Once planted inside a network, the ransomware conducts reconnaissance of the infrastructure, according to the FBI.

"Ragnar Locker encrypts all available files of interest," according to the FBI alert. "Instead of choosing which files to encrypt, Ragnar Locker chooses which folders it will not encrypt. Taking this approach allows the computer to continue to operate 'normally' while the malware encrypts files with known and unknown extensions containing data of value to the victim."

The FBI alert notes that Ragnar Locker uses several types of custom-packing algorithms to encrypt the data and encrypts the targeted files using a Windows XP virtual machine that it deploys through the victim's network (see: *RagnarLocker Deploys a Virtual Machine to Hide Ransomware*).

The ransomware also looks to kill other malware that might be operating within the same network at the same time, according to the alert. It also "checks for current infections to prevent multiple encryption transforms of the data, potentially corrupting it. The binary gathers the unique machine [Globally Unique Identifier], operating system product name and user name currently running the process."

The alert also notes that, if Ragnar Locker infects devices in certain countries, such as Russia or Ukraine, it terminates without encrypting files.

Victims typically receive a plain-text note identifying Ragnar Locker as the attacker and providing instructions for how to pay the ransom and contact the attackers, the FBI adds.
