Ragnar ransomware gang hit 52 critical US orgs, says FBI

By Jessica Lyons

Published: 2022-03-09 · Archived: 2026-04-02 12:35:57 UTC

The Ragnar Locker ransomware gang has so far infected at least 52 critical infrastructure organizations in America across sectors including manufacturing, energy, financial services, government, and information technology, according to an FBI alert this week.

The Feds said [PDF] they became aware in early 2020 of the ransomware crew and its preferred tactic: double extortion. The crooks steal sensitive data, encrypt a victim's systems, and threaten to leak the stolen documents if the ransom to restore the files isn't paid.

To date, the Ragnar Locker criminals have posted stolen data from at least ten organizations on their publicity website, according to Acronis. As of January, the gang has hit entities across nearly a dozen critical sectors, according to the FBI flash alert, which provided technical details about how the ransomware attacks work:

The Ragnar Locker malware uses Windows API GetLocaleInfoW to identify the infected machine's location. If the victim's locale is one of a dozen European and Asian countries, including Russia and Ukraine, the infection process terminates.

As the ransomware is deployed, it kills services commonly used by managed service providers to remotely control networks and attempts to silently delete all shadow copies of documents so that users can't recover encrypted files.

And finally, Ragnar Locker encrypts organizations' data. But instead of choosing which files to encrypt, it selects folders *not* to 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 explained.

- Lapsus$ extortionists dump Samsung data online, chaebol confirms security breach
- Conti ransomware gang's source code leaked
- Second data-wiping malware found in Ukraine, says ESET
- Insurance giant Aon confirms it has suffered 'cyber incident'

For example, if the logical drive being processed is the C: drive, the malware does not encrypt files in folders names Windows, Windows.old, Mozilla, Mozilla Firefox, Tor browser, Internet Explorer, $Recycle.Bin, Program Data, Google, Opera, or Opera Software.

The FBI urged victims to report ransomware attacks to their local field office. And while it "does not encourage paying a ransom to criminal actors," it acknowledged that this can be a tricky business decision. Executives should "evaluate all options to protect their shareholders, employees, and customers," before deciding whether to pay, it added. ®

Source: https://www.theregister.com/2022/03/09/fbi_says_ragnar_locker_ransomware/