Bond Case Briefs

Municipal Finance Law Since 1971

FBI: Ransomware Attackers Have Code to Halt Critical Infrastructure

Monitoring remote access technology will be especially important for limiting the reach of malicious actors, allied cybersecurity agencies said in a report on trends they've observed over the last year in a booming ransomware industry.

Cyber attackers who hold a victim's system hostage by encrypting its data until their demands are met may be laying off "big game" in the U.S., but they've been working on code that could threaten a lot more real-world damage against those they do choose to target, according to a joint advisory from the FBI and domestic and international partner agencies.

"Although most ransomware incidents against critical infrastructure affect business information and technology systems, the FBI observed that several ransomware groups have developed code designed to stop critical infrastructure or industrial processes," reads the advisory released Wednesday.

The joint advisory, released along with the National Security Agency and Cybersecurity and Infrastructure Security Agency, as well as their counterparts in Australia and the United Kingdom, examines ransomware trends that emerged in 2021 and offers mitigation strategies for network defenders.

In May, after Colonial Pipeline paid ransomware attackers $5 million to release their system, the company said it had proactively disconnected the operational technology—think valves, and pressure gauges—that control its physical processes, and federal agencies said there was no evidence the hackers got beyond their information technology realm.

As OT and IT have become increasingly intertwined to create greater efficiency of industrial control systems, the sector has become a frequent target of ransomware perpetrators and other malicious actors. One high-profile example of the kind of damage cyber adversaries can do by manipulating OT came last year when an attack attempted to change the chemicals in a Florida water treatment plant to levels that would be unsafe for the community it serves.

The ransomware business model that has allowed for large scale commoditization of exploits has only continued to advance over last year, according to the joint advisory.

"The market for ransomware became increasingly 'professional' in 2021, and the criminal business model of ransomware is now well established," the agencies wrote. "In addition to their increased use of ransomware-as-a-service, ransomware threat actors employed independent services to negotiate payments, assist victims with making payments and arbitrate payment disputes between themselves and other cyber criminals."

That could be especially bad news for owners and operators of slightly smaller critical infrastructure sectors that rely on industrial control systems. The advisory notes—at least in the U.S.—ransomware perpetrators appear to be staying away from "big game" targets like Colonial Pipeline after U.S.

authorities subsequently disrupted their operations.

“The FBI observed some ransomware threat actors redirecting ransomware efforts away from ‘big-game’ and toward mid-sized victims to reduce scrutiny,” the advisory reads.

The advisory shares a host of recommendations for mitigating meaner ransomware attacks to come, including reduced reliance on remote access technology and tightly monitoring their use if it can’t be avoided.

Route Fifty

By Mariam Baksh

FEBRUARY 10, 2022