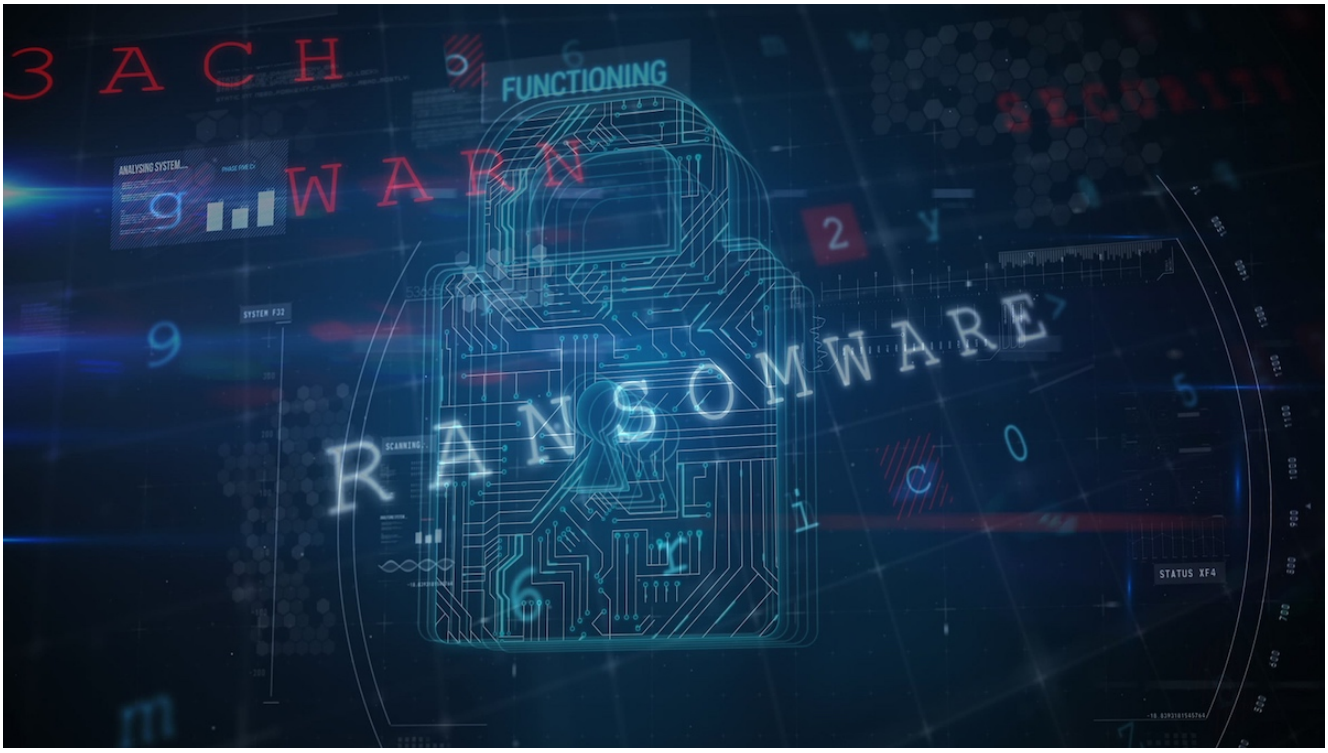
CISA Gets Proactive With New Pre-Ransomware Alerts



The US Cybersecurity and Infrastructure Security Agency (CISA) this week announced a new initiative to alert organizations of early-stage ransomware attacks.

Since the start of the year, the agency has notified more than 60 organizations in the energy, education, healthcare, water/wastewater, and other sectors. Many of these organizations were able to mitigate the attack before data was encrypted and exfiltrated.

A proactive cyber defense capability, pre-ransomware notifications are meant to warn organizations that they were breached, so that they can evict threat actors from their networks before file-encrypting ransomware is deployed.

“We know that ransomware actors often take some time after gaining initial access to a target before encrypting or stealing information, a window of time that often lasts from hours to days. This window gives us time to warn organizations

that ransomware actors have gained initial access to their networks," Joint Cyber Defense Collaborative (JCDC) associate director Clayton Romans notes.

By taking immediate action when receiving an early warning, organizations can reduce potential data loss, avoid impact on operations, and reduce financial impact and other detrimental consequences.

The notifications, Romans says, are sent based on tips received from the cybersecurity research community, threat intelligence companies, and infrastructure providers. Once a tip is received, CISA's field personnel notifies the victim organization and provides it with mitigation instructions.

If the victim is an entity outside the US, CISA works with international CERT partners to deliver the notification.

"In cases where ransomware actors have already encrypted a network and are holding data and systems for ransom, JCDC works closely with the victim organizations to provide threat actor tactics, techniques, and procedures (TTPs) as well as guidance to help reduce the impact of an attack," Romans explains.

CISA urges organizations to report observed ransomware attacks, including indicators of compromise and TTPs, to help prepare mitigation guidance for future attacks.

Related: Cyber Insights 2023 | Ransomware

CISA Gets Proactive With New Pre-Ransomware Alerts