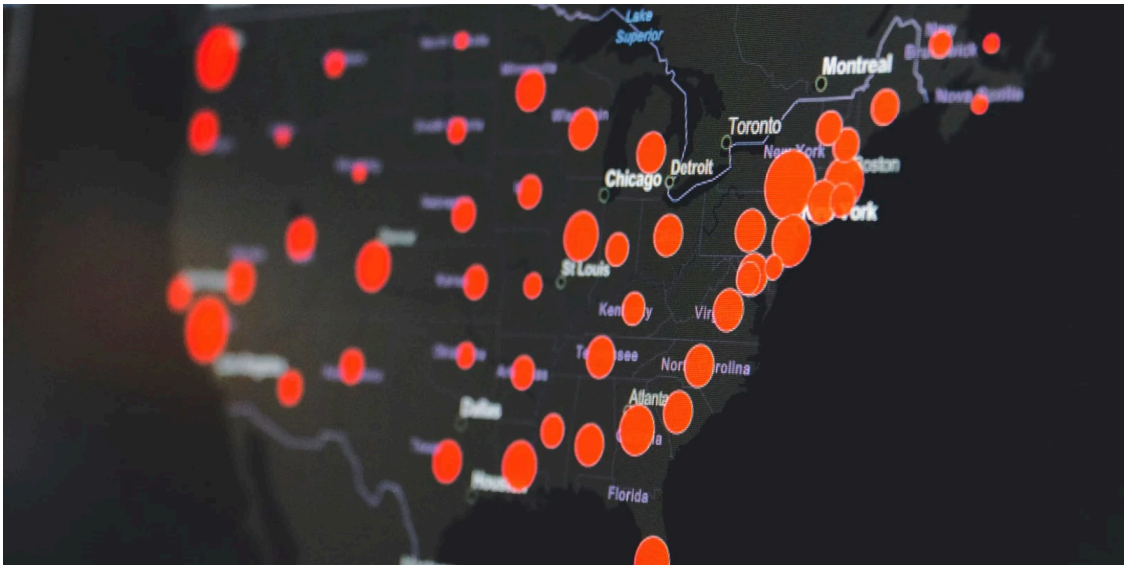
FBI: Conti ransomware attacked 16 US healthcare, first responder orgs

By Sergiu Gatlan

Published: 2021-05-21 · Archived: 2026-04-06 03:13:39 UTC

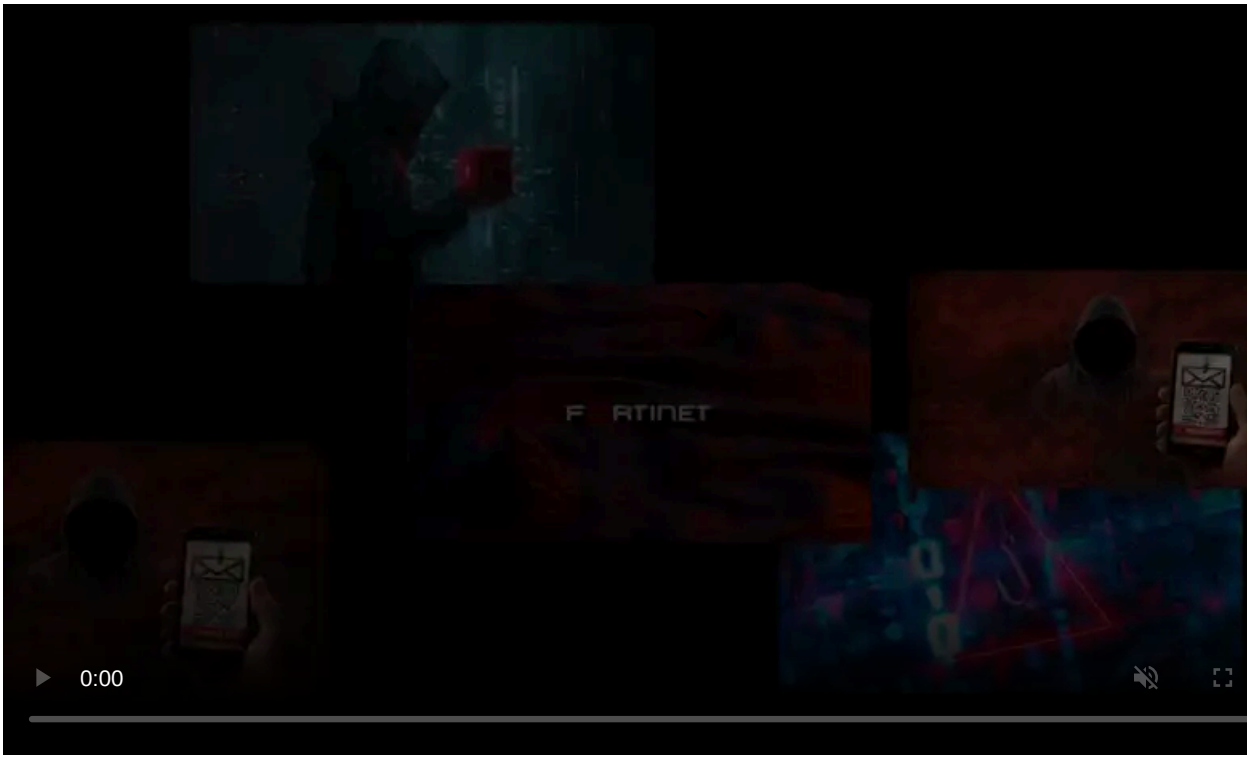


The Federal Bureau of Investigation (FBI) says the Conti ransomware gang has attempted to breach the networks of over a dozen U.S. healthcare and first responder organizations.

The info was shared via a TLP:WHITE flash alert issued Thursday to help system admins and security professionals defend their orgs' networks against future Conti attacks.

At least 16 organizations targeted

"The FBI identified at least 16 Conti ransomware attacks targeting U.S. healthcare and first responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year," the FBI Cyber Division said.


F RTINET
0:00

"These healthcare and first responder networks are among the more than 400 organizations worldwide victimized by Conti, over 290 of which are located in the U.S."

According to the FBI, Conti ransom demands are custom-tailored to each victim, with recent ones being as high as $25 million.

Additionally, if the ransom is not paid within eight days, Conti ransomware operators would also contact their victims using Voice Over Internet Protocol (VOIP) services (a tactic also used by Doppelpaymer and other groups) or encrypted email services.

Victims are urged to share information on Conti ransomware attacks that hit their networks to help the FBI prevent future attacks and identify the gang members' identities.

> Cyber attacks targeting networks used by emergency services personnel can delay access to real-time digital information, increasing safety risks to first responders and could endanger the public who rely on calls for service to not be delayed. [..] Targeting healthcare networks can delay access to vital information, potentially affecting care and treatment of patients including cancellation of procedures, rerouting to unaffected facilities, and compromise of Protected Health Information. — FBI Cyber Division

The Conti ransomware gang

Conti ransomware is a private Ransomware-as-a-Service (RaaS) operation believed to be controlled by a Russian-based cybercrime group known as Wizard Spider.

Conti shares some of its code with the notorious Ryuk Ransomware, whose TrickBot distribution channels they started using after Ryuk activity decreased around July 2020.

This ransomware gang has recently breached the networks of Ireland's Health Service Executive (HSE) and Department of Health (DoH), asking the former to pay a $20 million ransom after successfully encrypting its systems.

Even though the DoH was able to block Conti from encrypting its systems, the HSE was not as lucky and was had to shut down all I.T. systems to prevent the ransomware from spreading through its network.

Following the attack on Ireland's public healthcare system, the Conti gang released a free decryptor for the HSE but warned that the 700 GB of data stolen from their network will still be released or sold.

The U.S. government previously warned the healthcare industry of ransomware targeting hospitals and healthcare providers in October 2020, after Ryuk operators took down the computer and phone systems of Fortune 500 hospital and healthcare services provider Universal Health Services (UHS).
