National Security Agency Central Security Service
Defending our Nation. Securing the Future.

CISA, FBI, and NSA Release Conti Ransomware Advisory to Help Organizations Reduce Risk of Attack

WASHINGTON –
The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) published a cybersecurity advisory today regarding increased Conti ransomware cyberattacks. The advisory includes technical details on the threat and mitigation steps that public and private sector organizations can take to reduce their risk to this ransomware.

CISA and the FBI have observed over 400 attacks using Conti ransomware against U.S. and international organizations to steal files, encrypt servers and workstations, and demand a ransom payment to return stolen sensitive data. While Conti is considered a ransomware-as-a-service (RaaS) model ransomware variant, there is variation in its structure that differentiates it from a typical affiliate model. It is likely that Conti developers pay the deployers of the ransomware a wage rather than a percentage of the proceeds from a successful attack.

“Americans are routinely experiencing real-world consequences of the ransomware epidemic as malicious cyber actors continue to target large and small businesses, organizations, and governments,” said Eric Goldstein, Executive Assistant Director for Cybersecurity, CISA. “CISA, FBI, and NSA work tirelessly to assess cyber threats and advise our domestic and international partners on how they can reduce the risk and strengthen their own capabilities. We encourage Americans to visit stopransomware.gov to learn how to improve their own cybersecurity to mitigate risk of becoming a victim of ransomware.”

“The FBI, along with our partners at CISA and NSA, is committed to providing resources in an effort to help public and private sector entities protect their systems against ransomware attacks,” said Assistant Director Bryan Vorndran of the FBI’s Cyber Division. “Our collaborative partnerships and common sense of purpose are essential to our collective fight and when combined with our world-class capabilities, we can discourage this criminal behavior by enacting a wide range of consequences against these malicious cyber actors.”

“The cyber criminals now running the Conti ransomware-as-a-service have historically targeted critical infrastructure, such as the Defense Industrial Base (DIB), prior to Conti campaigns, and the advisory highlights actions organizations can take right now to counter the threat,” said Rob Joyce, Director of Cybersecurity at NSA. “NSA works closely with our partners, providing critical intelligence and enabling operations to counter ransomware activities. We highly recommend using the mitigations outlined in

this advisory to protect against Conti malware and mitigate your risk against any ransomware attack."

Using the MITRE ATT&CK common lexicon of adversary behavior, the advisory highlights observed Conti actors' techniques used to conduct their exploits, such as spearphishing campaigns, remote monitoring and management software, the "PrintNightmare" vulnerability, and remote desktop software. Also, artifacts from a recently leaked threat actor "playbook" identify Internet Protocol (IP) addresses Conti actors have used for their malicious activity. Organizations should read and implement the recommended mitigations and continue to be vigilant against this ongoing ransomware threat.

If an organization should become a victim of ransomware, CISA, FBI and NSA strongly discourage paying the ransom. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and does not guarantee that a victim's files will be recovered. As a cybersecurity community, one of the best ways to prevent future ransomware attacks and hold these criminals accountable is for cyberattack victims to report it.

The advisory can be found here and is available on the new, whole-of-government ransomware website, Stopransomware.gov.