



## THREAT BULLETINS

### InfraGard FBI Flash - Conti Ransomware Attacks Impact Healthcare and First Responder Networks



TLP:WHITE

May 21, 2021

The United States Federal Bureau of Investigation (FBI) identified at least 16 Conti ransomware attacks targeting US healthcare and first responder networks, including law enforcement agencies, emergency medical services, 9-1-1 dispatch centers, and municipalities within the last year. 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. Like most ransomware variants, Conti typically steals victims' files and encrypts the servers and workstations in an effort to force a ransom payment from the victim. The ransom letter instructs victims to contact the actors through an online portal to complete the transaction. If the ransom is not paid, the stolen data is sold or published to a public site

controlled by the Conti actors. Ransom amounts vary widely and we assess are tailored to the victim. Recent ransom demands have been as high as \$25 million.

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. Loss of access to law enforcement networks may impede investigative capabilities and create prosecution challenges. 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.

Conti actors gain unauthorized access to victim networks through weaponized malicious email links, attachments, or stolen Remote Desktop Protocol (RDP) credentials. Conti weaponizes Word documents with embedded Powershell scripts, initially staging Cobalt Strike via the Word documents and then dropping Emotet onto the network, giving the actor access to deploy ransomware. Actors are observed inside the victim network between four days and three weeks on average before deploying Conti ransomware, primarily using dynamic-link libraries (DLLs) for delivery. The actors first use tools already available on the network, and then add tools as needed, such as Windows Sysinternals and Mimikatz to escalate privileges and move laterally through the network before exfiltrating and encrypting data. In some cases where additional resources are needed, the actors also use Trickbot3. Once Conti actors deploy the ransomware, they may stay in the network and beacon out using AnchorDNS. If the victim does not respond to the ransom demands two to eight days after the ransomware deployment, Conti actors often call the victim using single-use Voice Over Internet Protocol (VOIP) numbers. The actors may also communicate with the victim using ProtonMail, and in some instances victims have negotiated a reduced ransom.

## **Indicators**

Conti actors use remote access tools, which most often beacon to domestic and international virtual private server (VPS) infrastructure

over ports 80, 443, 8080, and 8443. Additionally, actors may use port 53 for persistence. Large HTTPS transfers go to cloud-based data storage providers MegaNZ and pCloud servers. Other indicators of Conti activity include the appearance of new accounts and tools—particularly Sysinternals—which were not installed by the organization, as well as disabled endpoint detection and constant HTTP and domain name system (DNS) beacons, and disabled endpoint detection.

### **Information Requested**

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, Bitcoin wallet information, the decryptor file, and/or a benign sample of an encrypted file. The FBI does not encourage paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. However, the FBI understands that when victims are faced with an inability to function, all options are evaluated to protect shareholders, employees and customers. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to promptly report ransomware incidents to your local field office or the FBI's 24/7 Cyber Watch (CyWatch). Doing so provides the FBI with critical information needed to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under US law.

**Report Source(s)**

FBI

### **Recommendations**

- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement network segmentation.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a

physically separate, segmented, secure location (i.e., hard drive, storagedevice, the cloud).

- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Use multifactor authentication where possible.
- Use strong passwords and regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Require administrator credentials to install software.
- Audit user account with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.
- Focus on cyber security awareness and training. Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e., ransomware and phishing scams).

## **Sources**

Conti.pdf

See Attached

**Alert ID** 28374ade

**[View Alert](#)**

**Tags** FBI Flash

**TLP:WHITE** Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

**For Questions or Comments** Please email us at [toc@h-isac.org](mailto:toc@h-isac.org)

**FBI** The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts may be identified at [www.fbi.gov/contact-us/field](http://www.fbi.gov/contact-us/field). Contact CyWatch by telephone at 855-292-3937 or by email at [CyWatch@fbi.gov](mailto:CyWatch@fbi.gov).

Download Health-ISAC's Information Sharing App.



For more update and alerts, visit: <https://health-isac.cyware.com>

If you are not supposed to receive this email,  
please contact us at [toc@h-isac.org](mailto:toc@h-isac.org).