JOINT
CYBERSECURITY
ADVISORY

Co-Authored by:

Product ID: AA21-265A

September 22, 2021

TLP:WHITE

Conti Ransomware

SUMMARY

Note: *This Alert uses the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK®) framework, version 9. See the ATT&CK for Enterprise for all referenced threat actor tactics and techniques*.

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have observed the increased use of Conti ransomware in more than 400 attacks on U.S. and international organizations. In typical Conti ransomware attacks, malicious cyber actors steal files, encrypt servers and workstations, and demand a ransom payment.

To secure systems against Conti ransomware, CISA, FBI, and the National Security Agency (NSA) recommend implementing the mitigation measures described in this Advisory, which include requiring multi-factor authentication (MFA), implementing network segmentation, and keeping operating systems and software up to date.

[Click here] for indicators of compromise (IOCs) in STIX format.

Immediate Actions You Can Take Now to Protect Against Conti Ransomware

- Use multi-factor authentication.
- Segment and segregate networks and functions.
- Update your operating system and software.

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field-offices, or the FBI's 24/7 Cyber Watch (CyWatch) at 855-292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov. For NSA client requirements or general cybersecurity inquiries, contact the NSA Cybersecurity Requirements Center at 410-854-4200 or Cybersecurity_Requests@nsa.gov.

This document was developed by CISA, FBI, and NSA in furtherance of their respective cybersecurity missions, including their responsibilities to develop and issue cybersecurity specifications and mitigations.

DISCLAIMER: The information in this Joint Cybersecurity Advisory is provided "as is" for informational purposes only. CISA, FBI, and NSA do not provide any warranties of any kind regarding this information or endorse any commercial product or service, including any subjects of analysis. This document is marked TLP:WHITE. Disclosure is not limited. Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp/.

TECHNICAL DETAILS

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.

Conti actors often gain initial access [TA0001] to networks through:

- Spearphishing campaigns using tailored emails that contain malicious attachments [T1566.001] or malicious links [T1566.002];
    - Malicious Word attachments often contain embedded scripts that can be used to download or drop other malware—such as TrickBot and IcedID, and/or Cobalt Strike—to assist with lateral movement and later stages of the attack life cycle with the eventual goal of deploying Conti ransomware.[1],[2],[3]
- Stolen or weak Remote Desktop Protocol (RDP) credentials [T1078];[4]
- Phone calls;
- Fake software promoted via search engine optimization;
- Other malware distribution networks (e.g., ZLoader); and
- Common vulnerabilities in external assets.

In the execution phase [TA0002], actors run a `getuid` payload before using a more aggressive payload to reduce the risk of triggering antivirus engines. CISA and FBI have observed Conti actors using Router Scan, a penetration testing tool, to maliciously scan for and brute force [T1110] routers, cameras, and network-attached storage devices with web interfaces. Additionally, actors use Kerberos attacks [T1558.003] to attempt to get the Admin hash to conduct brute force attacks.

Conti actors are known to exploit legitimate remote monitoring and management software and remote desktop software as backdoors to maintain persistence [TA0003] on victim networks.[5] The actors use tools already available on the victim network—and, as needed, add additional tools such as Windows Sysinternals and Mimikatz—to obtain users' hashes and clear-text credentials, which enable the actors to escalate privileges [TA0004] within a domain and perform other post-exploitation and lateral movement tasks [TA0008]. In some cases, the actors also use TrickBot malware to carry out post-exploitation tasks.

According to a recently leaked threat actor "playbook,"[6] Conti actors also exploit vulnerabilities in unpatched assets, such as the following, to escalate privileges [TA0004] and move laterally [TA0008] across a victim's network:

- 2017 Microsoft Windows Server Message Block 1.0 server vulnerabilities;[7]
- "PrintNightmare" vulnerability (CVE-2021-34527) in Windows Print spooler service;[8] and
- "Zerologon" vulnerability (CVE-2020-1472) in Microsoft Active Directory Domain Controller systems.[9]

Artifacts leaked with the playbook identify four Cobalt Strike server Internet Protocol (IP) addresses Conti actors previously used to communicate with their command and control (C2) server.

- 162.244.80[.]235
- 85.93.88[.]165
- 185.141.63[.]120
- 82.118.21[.]1

CISA and FBI have observed Conti actors using different Cobalt Strike server IP addresses unique to different victims.

Conti actors often use the open-source Rclone command line program for data exfiltration [TA0010]. After the actors steal and encrypt the victim's sensitive data [T1486], they employ a double extortion technique in which they demand the victim pay a ransom for the release of the encrypted data and threaten the victim with public release of the data if the ransom is not paid.

MITRE ATT&CK TECHNIQUES

Conti ransomware uses the ATT&CK techniques listed in table 1.

Table 1: Conti ATT&CK techniques for enterprise

Initial Access		
Technique Title	**ID**	**Use**
Valid Accounts	T1078	Conti actors have been observed gaining unauthorized access to victim networks through stolen Remote Desktop Protocol (RDP) credentials.
Phishing: Spearphishing Attachment	T1566.001	Conti ransomware can be delivered using TrickBot malware, which is known to use an email with an Excel sheet containing a malicious macro to deploy the malware.
Phishing: Spearphishing Link	T1566.002	Conti ransomware can be delivered using TrickBot, which has been delivered via malicious links in phishing emails.
Execution		
Command and Scripting Interpreter: Windows Command Shell	T1059.003	Conti ransomware can utilize command line options to allow an attacker control over how it scans and encrypts files.
Native Application Programming Interface (API)	T1106	Conti ransomware has used API calls during execution.

Persistence		
Valid Accounts	T1078	Conti actors have been observed gaining unauthorized access to victim networks through stolen RDP credentials.
External Remote Services	T1133	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as virtual private networks (VPNs), Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management can also be used externally.
Privilege Escalation		
Process Injection: Dynamic-link Library Injection	T1055.001	Conti ransomware has loaded an encrypted dynamic-link library (DLL) into memory and then executes it.
Defense Evasion		
Obfuscated Files or Information	T1027	Conti ransomware has encrypted DLLs and used obfuscation to hide Windows API calls.
Process Injection: Dynamic-link Library Injection	T1055.001	Conti ransomware has loaded an encrypted DLL into memory and then executes it.
Deobfuscate/Decode Files or Information	T1140	Conti ransomware has decrypted its payload using a hardcoded AES-256 key.
Credential Access		
Brute Force	T1110	Conti actors use legitimate tools to maliciously scan for and brute force routers, cameras, and network-attached storage devices with web interfaces.
Steal or Forge Kerberos Tickets: Kerberoasting	T1558.003	Conti actors use Kerberos attacks to attempt to get the Admin hash.
Discovery		

System Network Configuration Discovery	T1016	Conti ransomware can retrieve the ARP cache from the local system by using the `GetIpNetTable()` API call and check to ensure IP addresses it connects to are for local, non-internet systems.
System Network Connections Discovery	T1049	Conti ransomware can enumerate routine network connections from a compromised host.
Process Discovery	T1057	Conti ransomware can enumerate through all open processes to search for any that have the string `sql` in their process name.
File and Directory Discovery	T1083	Conti ransomware can discover files on a local system.
Network Share Discovery	T1135	Conti ransomware can enumerate remote open server message block (SMB) network shares using `NetShareEnum()`.
Lateral Movement		
Remote Services: SMB/Windows Admin Shares	T1021.002	Conti ransomware can spread via SMB and encrypts files on different hosts, potentially compromising an entire network.
Taint Shared Content	T1080	Conti ransomware can spread itself by infecting other remote machines via network shared drives.
Impact		
Data Encrypted for Impact	T1486	Conti ransomware can use `CreateIoCompletionPort()`, `PostQueuedCompletionStatus()`, and `GetQueuedCompletionPort()` to rapidly encrypt files, excluding those with the extensions of `.exe`, `.dll`, and `.lnk`. It has used a different AES-256 encryption key per file with a bundled RAS-4096 public encryption key that is unique for each victim. Conti ransomware can use "Windows Restart Manager" to ensure files are unlocked and open for encryption.

Service Stop	T1489	Conti ransomware can stop up to 146 Windows services related to security, backup, database, and email solutions through the use of net stop.
Inhibit System Recovery	T1490	Conti ransomware can delete Windows Volume Shadow Copies using `vssadmin`.

MITIGATIONS

CISA, FBI, and NSA recommend that network defenders apply the following mitigations to reduce the risk of compromise by Conti ransomware attacks.

Use multi-factor authentication.

- Require multi-factor authentication to remotely access networks from external sources.

Implement network segmentation and filter traffic.

- Implement and ensure robust network segmentation between networks and functions to reduce the spread of the ransomware. Define a demilitarized zone that eliminates unregulated communication between networks.
- Filter network traffic to prohibit ingress and egress communications with known malicious IP addresses.
- Enable strong spam filters to prevent phishing emails from reaching end users. Implement a user training program to discourage users from visiting malicious websites or opening malicious attachments. Filter emails containing executable files to prevent them from reaching end users.
- Implement a URL blocklist and/or allowlist to prevent users from accessing malicious websites.

Scan for vulnerabilities and keep software updated.

- Set antivirus/antimalware programs to conduct regular scans of network assets using up-to-date signatures.
- Upgrade software and operating systems, applications, and firmware on network assets in a timely manner. Consider using a centralized patch management system.

Remove unnecessary applications and apply controls.

- Remove any application not deemed necessary for day-to-day operations. Conti threat actors leverage legitimate applications—such as remote monitoring and management software and remote desktop software applications—to aid in the malicious exploitation of an organization's enterprise.
- Investigate any unauthorized software, particularly remote desktop or remote monitoring and management software.

- Implement application allowlisting, which only allows systems to execute programs known and permitted by the organization's security policy. Implement software restriction policies (SRPs) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular internet browsers or compression/decompression programs.
- Implement execution prevention by disabling macro scripts from Microsoft Office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full Microsoft Office suite applications.
- See the joint Alert, Publicly Available Tools Seen in Cyber Incidents Worldwide—developed by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom—for guidance on detection and protection against malicious use of publicly available tools.

Implement endpoint and detection response tools.

- Endpoint and detection response tools allow a high degree of visibility into the security status of endpoints and can help effectively protect against malicious cyber actors.

Limit access to resources over the network, especially by restricting RDP.

- After assessing risks, if RDP is deemed operationally necessary, restrict the originating sources and require multi-factor authentication.

Secure user accounts.

- Regularly audit administrative user accounts and configure access controls under the principles of least privilege and separation of duties.
- Regularly audit logs to ensure new accounts are legitimate users.

Review CISA's APTs Targeting IT Service Provider Customers guidance for additional mitigations specific to IT Service Providers and their customers.

Use the Ransomware Response Checklist in case of infection.

If a ransomware incident occurs at your organization, CISA, FBI, and NSA recommend the following actions:

- **Follow the Ransomware Response Checklist** on p. 11 of the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide.
- **Scan your backups.** If possible, scan your backup data with an antivirus program to check that it is free of malware.
- **Report incidents immediately** to CISA at https://us-cert.cisa.gov/report, a local FBI Field Office, or U.S. Secret Service Field Office.
- **Apply incident response best practices** found in the joint Advisory, Technical Approaches to Uncovering and Remediating Malicious Activity, developed by CISA and the cybersecurity authorities of Australia, Canada, New Zealand, and the United Kingdom.

CISA, FBI, and NSA strongly discourage paying a ransom to criminal actors. Paying a ransom may embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or may fund illicit activities. Paying the ransom also does not guarantee that a victim's files will be recovered.

ADDITIONAL RESOURCES

- The Digital Forensics, Incident Response (DFIR) Report: BazarLoader to Conti Ransomware in 32 Hours (September 2021): https://thedfirreport.com/2021/09/13/bazarloader-to-conti-ransomware-in-32-hours/
- NSA Info Sheet: Transition to Multi-Factor Authentication (August 2019): https://media.defense.gov/2019/Sep/09/2002180346/-1/-1/0/Transition%20to%20Multi-factor%20Authentication%20-%20Copy.pdf
- NSA Cybersecurity Information Sheet: Segment Networks and Deploy Application-Aware Defenses (September 2019): https://media.defense.gov/2019/Sep/09/2002180325/-1/-1/0/Segment%20Networks%20and%20Deploy%20Application%20Aware%20Defenses%20-%20Copy.pdf
- NSA Cybersecurity Information Sheet: Hardening Network Devices (August 2020): https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF

Free Cyber Hygiene Services

CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

StopRansomware.gov

The StopRansomware.gov webpage is an interagency resource that provides guidance on ransomware protection, detection, and response. This includes ransomware alerts, reports, and resources from CISA and other federal partners, including:

- CISA and MS-ISAC: Joint Ransomware Guide
- CISA Insights: Ransomware Outbreak
- CISA Webinar: Combating Ransomware

Rewards for Justice Reporting

The U.S. Department of State's Rewards for Justice (RFJ) program offers a reward of up to $10 million for reports of foreign government malicious activity against U.S. critical infrastructure. See the RFJ website for more information and how to report information securely.

REFERENCES

[1] MITRE ATT&CK: Conti

[2] MITRE ATT&CK: TrickBot

[3] MITRE ATT&CK: IcedID

[4] FBI FLASH: Conti Ransomware Attacks Impact Healthcare and First Responder Networks

[5] Ransomware Daily: Conti Ransomware Gang Playbook Mentions MSP Software – ChannelE2E

[6] Cisco Talos blog: Translated: Talos' insights from the recently leaked Conti ransomware playbook

[7] Microsoft Security Bulletin MS17-010 – Critical: Security Update for Microsoft Windows SMB Server

[8] Microsoft Security Update: Windows Print Spooler Remote Code Execution Vulnerability – CVE-2021-34527

[9] Microsoft Security Update: Netlogon Elevation of Privilege Vulnerability – CVE-2020-1472