THREAT BULLETINS

UPDATE: Joint Cybersecurity Advisory - Conti Ransomware

TLP:WHITE

Mar 10, 2022

Health-ISAC is issuing a threat bulletin regarding ongoing and increased Conti Ransomware activity provided in an updated Joint Cybersecurity Advisory (AA21-265A) by the United States Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), and the United States Secret Service (USSS). Conti Ransomware affiliates remain active in which reported cyber attacks stemming from their ransomware-as-a-service (RaaS) operations against US and international organizations are increasing.

Updated March 9, 2022:

This Joint Cybersecurity Advisory was updated to include new indicators of compromise and the United States Secret Service as a co-author.

Updated February 28, 2022:

Conti cyber threat actors remain active and reported Conti ransomware attacks against US and international organizations have risen to more than 1,000. Notable attack vectors include Trickbot and Cobalt Strike.

While there are no specific or credible cyber threats to the US homeland currently, CISA, FBI, and the NSA encourage organizations to review this advisory and apply the recommended mitigations.

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 US and international organizations. (See FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks.) 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 multifactor authentication (MFA), implementing network segmentation, and keeping operating systems and software up to date.

All members are encouraged to review AA21-265A: Conti Ransomware which has been attached to this alert.

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 used by affiliate cyber actors and receives a share 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.
- 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)
- 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. 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," 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
- "PrintNightmare" vulnerability (CVE-2021-34527) in Windows Print spooler service
- "Zerologon" vulnerability (CVE-2020-1472) in Microsoft Active Directory Domain Controller systems.

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.

Additional Details:
For additional details including the list of updated indicators of compromise and MITRE ATT&CK Techniques, please see the full report here.

Organizations are encouraged to ingest the updated IOCs manually if no automatic ingestion systems are implemented. For Health-ISAC members who have implemented the Health-ISAC Indicator Threat Sharing (HITS) program, the IOCs related to this alert have been automatically imported into your environment.

Reference(s)	cisa, IC3

Recommendations

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

- 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.

CISA offers a range of no-cost cyber hygiene services to help critical infrastructure 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.

Sources
AA21-265A: Conti Ransowmare

FBI Flash: Conti Ransomware Attacks Impact Healthcare and First Responder Networks

Alert ID bfcdaad9

View Alert

Tags Joint Cybersecurity Advisory, Conti, Conti Ransomware

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

Download Health-ISAC's Information Sharing App. 

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