Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

2021-010: ACSC Ransomware Profile - **Conti**

04 March 2022

Context: *Conti is a ransomware variant first observed in early 2020, used by cybercriminals to conduct ransomware attacks against multiple sectors and organisations worldwide, including Australia. Conti is offered as a Ransomware-as-a-Service (RaaS), enabling affiliates to utilise it as desired, provided that a percentage of the ransom payment is shared with the Conti operators as commission. This product provides information related to Conti's background, threat activity, and mitigation advice.*

Ransomware is commonly used for financially motivated crime. On 25 February 2022, the Conti ransomware group published a series of statements regarding their stance in the context of the Russia-Ukraine conflict. The ongoing motivations of the operators of the Conti RaaS are outside the scope of this profile.

Subsequent to the Conti statements, a large volume of technical data has been released on the public internet related to the use of the Conti ransomware. Included in the release is a purported decryption tool for Conti; current public reporting indicates this tool is not effective against newer versions of the Conti ransomware and is therefore unlikely to assist in decrypting files encrypted in future Conti incidents.

The Australian Cyber Security Centre (ACSC) is providing this information to enable organisations to undertake their own risk assessments and take appropriate actions to secure their systems and networks. The ACSC will only revise and update this document in the event of further significant information coming to light.

Key Points

- Conti ransomware restricts access to corporate files and systems by encrypting them into a locked and unusable format. Victims receive instructions on how to engage with the offenders after encryption.
- Conti affiliates have successfully deployed ransomware on corporate systems in a variety of countries and sectors, including in Australia, where the ACSC is aware of multiple victims.
- Conti affiliates are known to implement the 'double extortion' technique by uploading stolen victim data obtained through the commission of the attack in part or full and threatening to sell and/or release additional information if their ransom demands are not met.
- Threat actors involved in the deployment of the Conti ransomware use a range of vectors to gain initial access into victim networks, including exploitation of unpatched vulnerabilities in remote access solutions.

Background

First detected in early 2020, Conti is a ransomware-as-a-service (RaaS) affiliate program associated with Russian-speaking cybercrime actors. Similarities between Conti and the Ryuk ransomware variant have been reported; however, it is unclear if the actors responsible for developing Conti are the same as those linked to Ryuk. The operators of Conti advertise the ransomware to potential affiliates in public and private forums. Conti affiliates have successfully deployed ransomware to target networks worldwide, including in Australia, where the ACSC is aware of multiple Australian victims.

ACSC Australian Cyber Security Centre

Threat activity

The ACSC is aware of an increase in domestic and global Conti activity throughout 2021 and use of Conti ransomware has continued into 2022. This includes the targeting of Australian critical infrastructure, notably including healthcare and energy organisations in 2021. Conti has claimed to have compromised at least 500 organisations worldwide to date.

Tactics, Techniques and Procedures

Threat actors deploying Conti ransomware use a range of initial access vectors to gain access to target networks. Conti threat actors have been widely observed using phished, purchased and brute-forced credentials to gain access to target networks through Remote Desktop Protocol (RDP) connections and commercial Virtual Private Network (VPNs) products, as well as utilising commercially and publicly available penetration testing tools Cobalt Strike and Metasploit.

Conti threat actors have been observed utilising a number of well-known malware variants to gain initial access to target networks including Trickbot, BazarLoader/BazarBackdoor and Emotet.

Other observable Tactics, Techniques, and Procedures (TTPs) associated with Conti ransomware activity include but are not limited to:

- Enumerating Active Directory environments with BloodHound,
- Exfiltrating data through RClone to publicly available cloud file-sharing services,
- Utilising Metasploit and Cobalt Strike for post-compromise exploitation,
- Maintaining persistence on devices with the AnyDesk remote desktop application.

The threat actors involved in the deployment of the Conti ransomware frequently change attack patterns, and quickly take advantage of newly disclosed vulnerabilities to compromise and operate within networks before network owners are able to apply patches or mitigations.

Post-Exploitation

Once encryption of victim data is complete, victims receive a ransom note directing them to either an email address or a URL, from which an affiliate will demand payment. Conti affiliates are known to implement the 'double extortion' technique by uploading exfiltrated victim data to their dedicated leak site (DLS) and threatening to release victim data in tranches if the ransom is not paid. Conti maintains a DLS both on The Onion Router (TOR) network and the publicly accessible internet.

Assistance

The ACSC monitors a variety of ransomware variant activity including, including activity involving Conti. The ACSC is able to provide assistance and advice if required. Organisations that have been impacted or require assistance in regards to a Conti ransomware incident can contact the ACSC via 1300 CYBER1 (1300 292 371), or by submitting a report to cyber.gov.au.

Mitigations

Technique	Procedure	Mitigations
Initial Access [TA0001]		
Exploit Public-Facing Application [T1190]	Threat actors search for and opportunistically exploit vulnerabilities	Update Software [M1051]

	in internet facing applications and devices to gain access to victim networks.	Establish processes to identify, assess and patch vulnerabilities affecting internet facing applications and devices within appropriate timeframes. This allows organisations to address security vulnerabilities before they are discovered and exploited by actors. See also: • Assessing Security Vulnerabilities and Applying Patches
Valid Accounts [T1078]	Actors have obtained credentials for valid accounts and gain access victim networks. Actors have used phishing and password brute forcing techniques to obtain credentials. They have also purchased credentials or collected them from publicly available breaches.	Multi-factor authentication [M1032] Require multifactor authentication for all user accounts, particularly privileged accounts. This prevents actors from accessing valid accounts with stolen credentials. See also: • Multi-factor Authentication - Technique D3-MFA • Implementing Multi-Factor Authentication • Strategies to Mitigate Cyber Security Incidents – Mitigation Details User training [M1017] Educate users to avoid password reuse. This prevents actors from obtaining credentials through public breaches or by compromising non-corporate systems. See also: • Creating Strong Passphrases
Persistence [TA0003]		
External Remote Services [T1133]	Actors have used the commercial remote access software “AnyDesk” to persist on victim systems.	Filter Network Traffic [M1037] Prevent network traffic from unknown or untrusted origins from accessing remote services on internal systems. This prevents actors from directly connecting to remote access services they have established for persistence. See also: • Inbound Traffic Filtering - Technique D3-ITF Network Segmentation [M1030] Segment networks and restrict traffic for remote access services where possible. This limits the

		ability of threat actors moving laterally within compromised networks. Utilising network segmentation as a form of defence in depth also prevents actors from connecting to external remote access services that they have established for persistence via compromised systems within victim networks. See also: • Broadcast Domain Isolation - Technique D3-BDI • Implementing Network Segmentation and Segregation
Exfiltration [TA0010]		
Exfiltration Over Web Service [T1567]	Actors have exfiltrated sensitive data and threatened to publicly release it. Actors have exfiltrated data to legitimate and publicly available web service, and in some cases have used legitimate tools such as RClone.	Encrypt Sensitive Information [M1041] Encrypt sensitive data at rest. This prevents actors from accessing sensitive data even if they can access the systems storing the data. Network Segmentation [M1030] Segment networks to separate sensitive data, and services that provide access to sensitive data, from corporate environments. This prevents adversaries from compromising vulnerable systems, such as desktop environments, and immediately accessing and exfiltrating sensitive data. See also: • Broadcast Domain Isolation - Technique D3-BDI • Implementing Network Segmentation and Segregation Restrict Web-Based Content [M1021] Restrict access to web-based storage services from corporate networks, except where required for legitimate business activity. This prevents actors from directly uploading sensitive data to blocked web-based storage services.
Lateral Movement [TA0008], Privilege Escalation [TA0004], Discovery [TA0007]		

Various	Actors have deployed widely-used malware and post-exploitation tools such as Trickbot, BazarLoader/BazarBackdoor, Emotet, Cobalt Strike and Metasploit on victim networks. These techniques are commonly used to move laterally through victim networks, harvest credentials, elevate privileges, exfiltrate data and deploy additional tools such as encryption binaries. In addition, actors have used the reconnaissance tool BloodHound [S0521] to map victims' Active Directory environments.	Network Segmentation [M1030] Segment networks and restrict or monitor certain types of traffic that are commonly used for lateral movement or reconnaissance. This prevents actors from moving laterally in networks and accessing sensitive systems or data. See also: • Broadcast Domain Isolation - Technique D3-BDI • Implementing Network Segmentation and Segregation Privileged Account Management [M1026] Restrict administrative privileges to operating systems and applications based on user duties. This reduces actors' ability to elevate privilege, move laterally in networks, bypass security controls and access sensitive data. See also: • Restricting Administrative Privileges Update Software [M1051] Patch applications and operating systems and keep them up to date. This prevents actors from exploiting known vulnerabilities in applications and operating systems to elevate privilege, bypass security controls and move laterally in networks. See also: • System Patching
Impact [TA0040]		
Data Encrypted for Impact [T1486]	Actors have used Conti ransomware to encrypt valuable data, disrupt operations, and extort payment from victims.	Backup Data [M1053] Perform daily backups and keep them offline and encrypted. Test recovery and integrity procedures to make sure data and operations can be quickly and reliably restored. This will allow business operations to be recovered if data is encrypted, reducing the impact of a ransomware attack. Note that backups will not mitigate risks where sensitive data is exfiltrated and released. See also: • Data backup and restoration

ACSC Australian Cyber Security Centre

Document Change Log

Version	Date	Change summary
2	4 March 2022	▪ Structural changes ▪ Context statement updated to reflect February 2022 statements from the operators of the Conti ransomware; public leak of data related to the use of Conti ransomware ▪ Update to advice on advice on protecting valid accounts ▪ Additions to malware used to gain initial access.
1	10 December 2021	First published.

ACSC Australian Cyber Security Centre

Traffic light protocol

TLP Level	Restriction on access and use
RED	**Not for disclosure, restricted to participants only.** Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
AMBER	**Limited disclosure, restricted to participant's organisations.** Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organisations involved. Recipients may only share TLP:AMBER information with members of their own organisation, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**
GREEN	**Limited disclosure, restricted to the community.** Sources may use TLP:GREEN when information is useful for the awareness of all participating organisations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organisations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not released outside of the community.
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.
Not classified	Any information received from the ACSC that is not classified in accordance with the Traffic light protocol must be treated as AMBER classified unless otherwise agreed in writing by the ACSC.