Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

TLP: WHITE

Australian organisations should urgently adopt an enhanced cybersecurity posture

Entities should follow ACSC advice and act on improving their resilience within a heightened threat environment.

Version 3 - Last Updated: 26 February 2022

Context

On 23 February 2022, the ACSC released an Alert *"Australian organisations encouraged to urgently adopt an enhanced cyber security posture".* This Technical Advisory provides additional information to support entities to take appropriate actions in order to secure their systems and networks.

While the ACSC is not aware of any current or specific threats to Australian organisations, adopting an enhanced cybersecurity posture and increased monitoring for threats will help to reduce the impacts to Australian organisations.

Australian organisations should continue to maintain vigilance to the threat of ransomware. Threat actors believed to be associated with Conti have claimed they will target unspecified critical infrastructure in response to cyber or military actions against Russia. The ACSC has published a profile on Conti's background, threat activity, and mitigation advice. Tactics, techniques and procedures associated with Conti ransomware is included in this advisory.

This advisory has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

This advisory draws on information derived from ACSC partner agencies and industry sources.

ACSC and Partner Reporting

For your convenience below is a collation of ACSC and partner reporting which includes actions to secure systems and networks. For further information see the following:

- US Cybersecurity and Infrastructure Security Agency (CISA): CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats
- UK National Cyber Security Centre: NCSC advises organisations to act following Russia's further violation of Ukraine's territorial integrity
- UK National Cyber Security Centre: New Sandworm malware Cyclops Blink replaces VPNFilter
- UK National Cyber Security Centre: Cyclops Blink Malware Analysis Report
- NZ National Cyber Security Centre: General Security Advisory: Understanding and preparing for cyber threats relating to tensions between Russia and Ukraine
- Canadian Centre for Cyber Security (CCCS): Cyber threat bulletin: Cyber Centre urges Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity

- Russia Cyber Threat Overview and Advisories | CISA
- Joint Cybersecurity Advisory: Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology
- Joint Cybersecurity Advisory: Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments,
- New sophisticated email-based attack from NOBELIUM - Microsoft Security Blog
- NOBELIUM targeting delegated administrative privileges to facilitate broader attacks - Microsoft Security Blog.
- 24 February 2022 tweet by ESET Research
- 24 February 2022 tweet by Symantec Threat Intelligence
- Ransomware Profile: Conti | Cyber.gov.au

Tactics, Techniques, and Procedures (TTPs)

Initial access:

Spear phishing emails may be sent with malicious HMTL attachments. The lures of the spear phishing emails can be tailored to the targeted organisation. HTML files (.html) can contain an obfuscated JavaScript payload, which seeks to mount an .ISO file, much like an external drive. A .lnk file executes a hidden .dll file, which in turn executes further payloads such as Cobalt Strike.

Threat actors use brute force techniques to identify valid account credentials for domain and M365 accounts. After obtaining domain credentials, the actors use them to gain initial access to the networks.

Threat actors send spearphishing emails with links to malicious domains and use publicly available URL shortening services to mask the link. Embedding shortened URLs instead of actor-controlled malicious domains is an obfuscation technique meant to bypass virus and spam scanning tools. The technique often promotes a false legitimacy to the email recipient, increasing the probability of a victim's clicking on the link.

Threat actors use harvested credentials in conjunction with known vulnerabilities—for example, CVE-2020-0688 and CVE-2020-17144—on public-facing applications, such as virtual private networks (VPNs), to escalate privileges and gain remote code execution (RCE) on exposed applications. In addition, threat actors have exploited CVE-2018-13379 on FortiClient to obtain credentials to access networks.

Actors have gained initial access to victim organisations by compromising trusted third-party software. Notable incidents include M.E.Doc accounting software and SolarWinds Orion.

Persistence:
In multiple instances, threat actors maintained persistent access for at least six months. Although the actors have used a variety of malware to maintain persistence, they have also used "living off the land" techniques.

Malicious actors have moved laterally through networks, compromised user and administrator accounts, hosts and servers including Domain Controllers. The actors have downloaded additional malware and continued to communicate with infrastructure that is known to be compromised or co-opted. The actors have scheduled and executed malicious PowerShell scripts and deployed malicious .dll files and other tools, including Cobalt Strike Beacons, in an attempt to establish persistence.

The actors have used a Powershell® cmdlet (New-ManagementRoleAssignment) to grant the 'ApplicationImpersonation' role to a compromised account.

Privilege Escalation:
Malicious actors have targeted and compromised privileged Cloud Administrator's systems and accounts. Subsequently, actors have attempted to generate various Azure Active Directory (AAD) tokens, create users and grate roles to users and applications to maintain persistence.

Credential Access:
Malicious actors can operate a Kubernetes cluster, which allows them to conduct distributed and large-scale targeting using password spray and password guessing.

Lateral Movement:
After some victims reset passwords for individually compromised accounts, the actors have pivoted to other accounts, as needed, to maintain access.

Collection:
Using compromised M365 credentials, including global admin accounts, the threat actors can gain access to M365 resources, including SharePoint pages, user profiles, and user emails

Mitigation / How do I stay secure?

The ACSC recommends that organisations urgently adopt an enhanced cyber security posture. This should include reviewing and enhancing detection, mitigation, and response measures.

Organisations should ensure that logging and detection systems in their environment are fully updated and functioning and apply additional monitoring of their networks where required.

Review the TTPs contained in this product to determine if related activity has occurred on your organisation's network. The ACSC recommends organisations focus on monitoring for:

- AD configuration changes.
- Abuse of delegated privileges and service principles in Azure.
- Active Directory Federation Services (ADFS) changes.
- Consider conditional access policies to prevent login events from unusual locations, including TOR.

Assistance / Where can I go for help?

The ACSC is monitoring the situation and is able to provide assistance or advice as required. Organisations that have been impacted or require assistance can contact the ACSC via **1300 CYBER1** (1300 292 371).

APPENDIX A:

Table of notable tactics and techniques

Tactic	Technique	Procedure
Reconnaissance [TA0043] **Credential Access [TA0006]**	Gather Victim Identity Information: Credentials [T1589.001] Brute Force [T1110]	Threat actors used brute force to identify valid account credentials for domain and M365 accounts. After obtaining domain credentials, the actors used them to gain initial access.
Initial Access [TA0001]	External Remote Services [T1133]	Threat actors continue to research vulnerabilities in Fortinet's FortiGate VPN devices, conducting brute force attacks and leveraging CVE-2018-13379 to gain credentials to access victim networks.

Tactic	Technique	Procedure
Initial Access [TA0001] **Privilege Escalation [TA0004]**	Valid Accounts [T1078] Exploit Public-Facing Application [T1190]	Threat actors used credentials in conjunction with known vulnerabilities on public-facing applications, such as virtual private networks (VPNs)—CVE-2020-0688 and CVE-2020-17144—to escalate privileges and gain remote code execution (RCE) on the exposed applications.
Initial Access [TA0001] **Defense Evasion [TA0005]**	Phishing: Spearphishing Link [T1566.002] Obfuscated Files or Information [T1027]	Threat actors sent spearphishing emails using publicly available URL shortening services. Embedding shortened URLs instead of the actor-controlled malicious domain is an obfuscation technique meant to bypass virus and spam scanning tools. The technique often promotes a false legitimacy to the email recipient and thereby increases the possibility that a victim clicks on the link.
Initial Access [TA0001] **Credential Access [TA0006]**	OS Credential Dumping: NTDS [T1003.003] Valid Accounts: Domain Accounts [T1078.002]	Threat actors logged into a victim’s VPN server and connected to the domain controllers, from which they exfiltrated credentials and exported copies of the AD database ntds.dit.
Initial Access [TA0001] **Privilege Escalation [TA0004]** **Collection [TA0009]**	Valid Accounts: Cloud Accounts [T1078.004] Data from Information Repositories: SharePoint [T1213.002]	In one case, the actors used valid credentials of a global admin account within the M365 tenant to log into the administrative portal and change permissions of an existing enterprise application to give read access to all SharePoint pages in the environment, as well as tenant user profiles and email inboxes.
Initial Access [TA0001] **Collection [TA0009]**	Valid Accounts: Domain Accounts [T1078.002] Email Collection [T1114]	In one case, the threat actors used legitimate credentials to exfiltrate emails from the victim's enterprise email system.
Persistence [TA0003] **Lateral Movement [TA0008]**	Valid Accounts [T1078]	Threat actors used valid accounts for persistence. After some victims reset passwords for individually compromised accounts, the actors pivoted to other accounts, as needed, to maintain access.
Discovery [TA0007]	File and Network Discovery [T1083]	After gaining access to networks, the threat actors used BloodHound to map the Active Directory.
Discovery [TA0007]	Domain Trust Discovery [T1482]	Threat actors gathered information on domain trust relationships that were used to identify lateral movement opportunities.
Command and Control [TA0011]	Proxy: Multi-hop Proxy [T1090.003]	Threat actors used multiple disparate nodes, such as VPSs, to route traffic to the target.
Reconnaissance [TA0043]	Active Scanning: Vulnerability Scanning [T1595.002]	Malicious cyber actors have performed large-scale scans in an attempt to find vulnerable servers.
Reconnaissance [TA0043]	Phishing for Information [T1598]	Malicious cyber actors have conducted spearphishing campaigns to gain credentials of target networks.
Resource Development [TA0042]	Develop Capabilities: Malware [T1587.001]	Malicious cyber actors have developed and deployed malware, including ICS-focused destructive malware.
Initial Access [TA0001]	Exploit Public Facing Applications [T1190]	Malicious cyber actors use publicly known vulnerabilities, as well as zero-days, in internet-facing systems to gain access to networks.

Tactic	Technique	Procedure
Initial Access [TA0001]	Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]	Malicious cyber actors have gained initial access to victim organizations by compromising trusted third-party software. Notable incidents include M.E.Doc accounting software and SolarWinds Orion.
Initial Access [TA0001]	Exploit Public-Facing Application [T1190]	Threat actors search for and opportunistically exploit vulnerabilities in internet facing applications and devices to gain access to victim networks.
Initial Access [TA0001]	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.
Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]	Malicious cyber actors have used cmd.exe to execute commands on remote machines. They have also used PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and to execute other commands.
Persistence [TA0003]	Valid Accounts [T1078]	Malicious cyber actors have used credentials of existing accounts to maintain persistent, long-term access to compromised networks.
Persistence [TA0003]	External Remote Services [T1133]	Actors have used the commercial remote access software “AnyDesk” to persist on victim systems.
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001] and Password Spraying [T1110.003]	Malicious cyber actors have conducted brute-force password guessing and password spraying campaigns.
Credential Access [TA0006]	OS Credential Dumping: NTDS [T1003.003]	Malicious cyber actors have exfiltrated credentials and exported copies of the Active Directory database ntds.dit.
Credential Access [TA0006]	Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]	Malicious cyber actors have performed “Kerberoasting,” whereby they obtained the Ticket Granting Service (TGS) Tickets for Active Directory Service Principal Names (SPN) for offline cracking.
Credential Access [TA0006]	Credentials from Password Stores [T1555]	Malicious cyber actors have used previously compromised account credentials to attempt to access Group Managed Service Account (gMSA) passwords.
Credential Access [TA0006]	Exploitation for Credential Access [T1212]	Malicious cyber actors have exploited Windows Netlogon vulnerability CVE-2020-1472 to obtain access to Windows Active Directory servers.
Credential Access [TA0006]	Unsecured Credentials: Private Keys [T1552.004]	Malicious cyber actors have obtained private encryption keys from the Active Directory Federation Services (ADFS) container to decrypt corresponding SAML signing certificates.
Command and Control [TA0011]	Proxy: Multi-hop Proxy [T1090.003]	Malicious cyber actors have used virtual private servers (VPSs) to route traffic to targets. The actors often use VPSs with IP addresses in the home country of the victim to hide activity among legitimate user traffic.
Execution [TA0002]	Command and Scripting Interpreter: Unix Shell [T1059.004]	Malicious cyber actors execute downloaded files using the Linux API function execlp
Persistence [TA0003]	Boot or Logon Initialization Scripts: RC Scripts [T1037.004]	Malicious cyber actors execute software on device startup using a modified S51armled RC script.

Tactic	Technique	Procedure
Persistence [TA0003]	Pre-OS Boot: System Firmware [T1542.001]	Malicious cyber actors' malware maintains persistence through legitimate device firmware update processes by patching firmware when it is downloaded to the device.
Defence Evasion [TA0005]	Impair Defences: Disable or Modify System Firewall [T1562.004]	Malicious cyber actors may modify the Linux `iptables` firewall to enable C2 communication over port numbers from a stored list.
Defence Evasion [TA0005]	Masquerading: Match Legitimate Name or Location [T1036.005]	Malicious cyber actors may rename running processes to masquerade as Linux kernel threads.
Discovery [TA0007]	System Information Discovery [T1082]	Malicious executables may regularly query device information.
Command and Control [TA0011]	Encrypted Channel: Asymmetric Cryptography [T1573.002] Data Encoding: Non-Standard Encoding [T1132.002]	Malicious cyber actor malware C2 messages are individually encrypted using AES-256-CBC and sent underneath TLS. OpenSSL library functions are used to encrypt each message using a randomly generated key and IV, which are then encrypted using a hard-coded RSA public key. Malicious cyber actors may use custom binary schemes to encode specific commands to be executed, as well as any command parameters.
Command and Control [TA0011] **Exfiltration [TA0010]**	Fallback Channels [T1008] Non-Standard Port [T1571] Exfiltration Over C2 Channel [T1041]	Malicious cyber actors' malware may randomly select a C2 server from lists of IPv4 addresses and port numbers. Ports may be non-standard ports not typically associated with web traffic. Actors may exfiltrate data over these C2 channels.
Lateral Movement [TA0008] **Privilege Escalation [TA0004]** **Discovery [TA0007]**	Various	Actors have deployed widely-used malware and post-exploitation tools such as Trickbot, Cobalt Strike and the Metasploit framework 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.
Exfiltration [TA0010]	Exfiltration Over Web Service [T1567]	Actors have exfiltrated sensitive data and threatened to publicly release it. Actors have exfiltrated data to a legitimate and publicly available web service, and in some cases have used legitimate tools such as RClone.

Indicators of compromise (IOC)

2523f94bd4fba4af76f4411fe61084a7e7d80dec163c9ccba9226c80b8b31252	SHA-256	Malicious ISO file (container)
d035d394a82ae1e44b25e273f99eae8e2369da828d6b6fdb95076fd3eb5de142	SHA-256	Malicious ISO file (container)
94786066a64c0eb260a28a2959fcd31d63d175ade8b05ae682d3f6f9b2a5a916	SHA-256	Malicious ISO file (container)
48b5fb3fa3ea67c2bc0086c41ec755c39d748a7100d71b81f618e82bf1c479f0	SHA-256	Malicious shortcut (LNK)
ee44c0692fd2ab2f01d17ca4b58ca6c7f79388cbc681f885bb17ec946514088c	SHA-256	Cobalt Strike Beacon malware
ee42ddacbd202008bcc1312e548e1d9ac670dd3d86c999606a3a01d464a2a330	SHA-256	Cobalt Strike Beacon malware
usaid.theyardservice[.]com	Domain	Subdomain used to distribute ISO file
worldhomeoutlet[.]com	Domain	Subdomain in Cobalt Strike C2
dataplane.theyardservice[.]com	Domain	Subdomain in Cobalt Strike C2
cdn.theyardservice[.]com	Domain	Subdomain in Cobalt Strike C2
static.theyardservice[.]com	Domain	Subdomain in Cobalt Strike C2
theyardservice[.]com	Domain	Actor controlled domain
a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	SHA-256	Hash of malicious executable
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	SHA-256	Hash of malicious executable
50df5734dd0c6c5983c21278f119527f9fdf6ef1d7e808a29754ebc5253e9a86	SHA-256	Hash of executable code segment
c082a9117294fa4880d75a2625cf80f63c8bb159b54a7151553969541ac35862	SHA-256	Hash of executable code segment
4e69bbb61329ace36fbe62f9fb6ca49c37e2e5a5293545c44d155641934e39d1	SHA-256	Hash of executable code segment
ff17ccd8c96059461710711fcc8372cfea5f0f9eb566ceb6ab709ea871190dc6	SHA-256	Hash of executable code segment
96.80.68[.]193	IPv4 address	C2 server IP address
188.152.254[.]170	IPv4 address	C2 server IP address
208.81.37[.]50	IPv4 address	C2 server IP address
70.62.153[.]174	IPv4 address	C2 server IP address
2.230.110[.]137	IPv4 address	C2 server IP address
90.63.245[.]175	IPv4 address	C2 server IP address
212.103.208[.]182	IPv4 address	C2 server IP address
50.255.126[.]65	IPv4 address	C2 server IP address
78.134.89[.]167	IPv4 address	C2 server IP address
81.4.177[.]118	IPv4 address	C2 server IP address
24.199.247[.]222	IPv4 address	C2 server IP address
37.99.163[.]162	IPv4 address	C2 server IP address
37.71.147[.]186	IPv4 address	C2 server IP address
105.159.248[.]137	IPv4 address	C2 server IP address
80.155.38[.]210	IPv4 address	C2 server IP address
217.57.80[.]18	IPv4 address	C2 server IP address
151.0.169[.]250	IPv4 address	C2 server IP address
212.202.147[.]10	IPv4 address	C2 server IP address
212.234.179[.]113	IPv4 address	C2 server IP address
185.82.169[.]99	IPv4 address	C2 server IP address
93.51.177[.]66	IPv4 address	C2 server IP address
80.15.113[.]188	IPv4 address	C2 server IP address
80.153.75[.]103	IPv4 address	C2 server IP address
109.192.30[.]125	IPv4 address	C2 server IP address
912342f1c840a42f6b74132f8a7c4ffe7d40fb77	SHA-1 hash	Hash of malicious executable
61b25d11392172e587d8da3045812a66c3385451	SHA-1 hash	Hash of malicious executable
1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591	SHA-256 hash	Hash of malicious executable

Document Change Log

Version	Date	Change Summary
3	26 February 2022	▪ Addition of Conti ransomware profile and associated TTPs
2	24 February 2022	▪ Addition of links to UK NCSC Cyclops Blink reports ▪ Addition of link to ESET Research tweet ▪ Addition of link to Symantec Threat Intelligence tweet ▪ Addition of TTPs from UK NCSC Cyclops Blink malware analysis report ▪ Addition of IOCs from UK NCSC, ESET Research and Symantec Threat Intelligence
1	23 February 2022	First published.

Traffic light protocol

Alert classification	Restriction on access and use
RED	**Highly restricted** **Access to and use by your Australian Cyber Security Centre (ACSC) contact officer(s) only.** You must ensure that your ACSC contact officer(s) does not disseminate or discuss RED alerts with any other person, and you shall ensure that you have appropriate systems in place to ensure that the information cannot be accessed or used by any person other than your ACSC contact officer(s).
AMBER	**Restricted internal access and use only.** Subject to the below, you shall only make AMBER alerts available to your employees on a 'needs-to-know basis' strictly for your internal purposes only to assist in the protection of your information and communications technology (ICT) systems. In some instances you may be provided with AMBER alerts which are marked to allow you to also disclose it to your contractors or agents on a 'needs-to-know basis' strictly for your internal purposes only to assist in the protection of your ICT systems.
GREEN	**Restricted to closed groups and subject to confidentiality** You may share GREEN alerts with external organisations, information exchanges or individuals in the network security, information assurance or critical network infrastructure community that agree to maintain the confidentiality of the information in the alert. You may not publish or post online or otherwise release it in circumstances where confidentiality may not be maintained.
WHITE	**Not restricted** WHITE alerts are not confidential. They contain information that is for public, unrestricted dissemination, publication, web-posting or broadcast. You may publish the information, subject to copyright and any restrictions or rights noted in the information.
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.