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 improve their resilience within a heightened threat environment.

Version: 11 Last Updated: 28 April 2022

Prioritise these actions to defend against malicious cyber activity

Organisations should prioritise the following actions to mitigate against threats posed by a range of malicious cyber actors. Many actors use common techniques such as exploiting internet-facing applications and spear phishing to compromise victim networks. Organisations should ensure they have implemented mitigations against these common techniques and are prepared to detect and respond to cyber security incidents. The following four actions will improve an organisation's resilience in the current threat environment.

1. Patch applications and devices, particularly internet-facing services. Monitor for relevant vulnerabilities and security patches, and consider bringing forward patch timeframes.
2. Implement mitigations against phishing and spear phishing attacks. Disable Microsoft Office macros by default and limit user privileges. Ensure that staff report all suspicious emails received, links clicked, or documents opened.
3. Ensure that logging and detection systems are fully updated and functioning. Prioritise internet-facing and critical network services, and ensure that logs are centrally stored.
4. Review incident response and business continuity plans. Plan responses to network compromise as well as disruptive or destructive activity such as ransomware. Ensure these plans are known to and actionable by staff, and are accessible even when systems are down.

Organisations should also review the Essential Eight and prioritise remediating any identified gaps in Essential Eight maturity. Following this, organisations should review technical details associated with any specific threats they have identified as relevant and incorporate these into monitoring and response plans.

Russian state-sponsored and criminal cyber threats to critical infrastructure

A joint cybersecurity advisory has been coauthored by U.S., Australian, Canadian, New Zealand, and UK cyber authorities, with contributions from industry members of the Joint Cyber Defense Collaborative (JCDC), which provides an overview of Russian state-sponsored advanced persistent threat (APT) groups, Russian-aligned cyber threat groups, and Russian-aligned cybercrime groups to help the cybersecurity community protect against possible cyber threats.

Australian critical infrastructure organisations should review the technical details, mitigations, and advice provided in this joint cybersecurity advisory.

Context

There are no specific or credible cyber threats to Australian organisations at this time.

Following the attack on Ukraine, there is a heightened cyber threat environment globally, and the risk of cyber attacks on Australian networks, either directly or inadvertently, has increased. While the ACSC has no specific intelligence relating to a cyber attack on Australia, this could change quickly.

It is critical that Australian organisations are alert to these threats and take steps to adopt an enhanced cybersecurity posture and increase monitoring for threats. These actions will help to reduce the impacts to Australian organisations of any cyber attacks.

On 23 February 2022, the ACSC released the 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.

This advisory has been compiled with respect to the MITRE ATT&CK® framework, a publicly 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.

Destructive malware targeting organisations in Ukraine

The ACSC is aware of reporting that malicious cyber actors have deployed destructive malware to target organisations in Ukraine. This advisory provides additional indicators of compromise (IOCs) to assist organisations to detect the WhisperGate, HermeticWiper, IsaacWiper, and CaddyWiper destructive malware.

Destructive malware can present a direct threat to an organisation's daily operations, impacting the availability of critical assets and data.

Ongoing threat of ransomware

Australian organisations should continue to maintain vigilance to the threat of ransomware. Malicious cyber 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 recently updated a profile on Conti's background, threat activity, and mitigation advice. The US Cybersecurity and Infrastructure Security Agency (CISA) alert on Conti ransomware has also been updated to include additional indicators of compromise. Tactics, techniques and procedures associated with Conti ransomware are included in this advisory.

Ongoing state-sponsored targeting of network devices

The ACSC is aware that state-sponsored actors continue to target routers and other network devices. The ACSC has previously released an alert relating to Russian state-sponsored targeting of network devices and advised Australian organisations to secure certain Cisco features to mitigate against this activity. The ACSC encourages organisations to refer to these publications as well as the 2018 US Cybersecurity and Infrastructure Security Agency (CISA) publication Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices and the 2022 US National Security Agency (NSA) publication on Network Infrastructure Security Guidance in order to secure their networks against this activity.

Exploitation of default multi-factor authentication protocols and known vulnerabilities for network access

The US CISA and Federal Bureau of Investigation have released a joint cybersecurity advisory to warn organisations that default multi-factor authentication (MFA) configuration has been exploited, in combination with known vulnerabilities, to allow malicious cyber actors to obtain access to networks. The joint cybersecurity advisory contains technical details on the exploitation as well as mitigations which can be applied to multi-factor authentication systems.

The ACSC urges all organisations to implement multi-factor authentication, disable unused accounts and to review the tactics, techniques, and procedures, indicators of compromise, and mitigation measures described in the joint cybersecurity advisory. If configured correctly, multi-factor authentication remains one of the most effective controls an organisation can implement to prevent an adversary from gaining access to a device or network and accessing sensitive information.

Possible threats to satellite communication networks

The US CISA and FBI have released a joint cybersecurity advisory relating to possible threats to satellite communication (SATCOM) networks. The advisory includes mitigation advice for SATCOM network providers and customers. The ACSC encourages all SATCOM network providers and customers to review the guidance in the joint cybersecurity advisory and the NSA publication on protecting very small aperture terminal (VSAT) communications.

Organisations should ensure that their information is encrypted prior to transmission, secure SATCOM products according to relevant best practices, and ensure appropriate network segmentation is in place. Organisations which rely on SATCOM for connectivity or critical functions should consider their business continuity plans if their SATCOM services are unavailable.

Targeting of the US and international energy sector

The US CISA, FBI and Department of Energy (DOE) have released a joint cybersecurity advisory relating to tactics, techniques, and procedures used to target US and international energy sector organisations between 2011 and 2018. The advisory includes technical details of these intrusion campaigns as well as recommended mitigations for both enterprise and operational technology networks. The ACSC encourages all energy sector organisations to review the guidance in the joint cybersecurity advisory.

The US CISA, DOE, NSA, and FBI have also released a joint cybersecurity advisory warning that malicious cyber actors have the capability to target specific operational technology devices. Organisations which utilise operational technology devices, particularly in the energy sector, should review the advisory and consider implementing the detection, mitigation, and resilience measures outlined to their operational technology environments.

Energy sector organisations should also review industry reporting on new destructive malware used to target an energy sector organisation as recently as April 2022.

Malicious activity occurring against internet-connected uninterruptible power supply devices

The US CISA and Department of Energy (DOE) have warned that malicious cyber actors have gained access to internet-connected uninterruptible power supply (UPS) devices, often through default passwords. Organisations using these and similar devices should ensure that device management interfaces are not accessible from the internet and that default passwords are changed.

Identifying cyber supply chain risks

The ACSC has developed guidance to assist organisations in identifying risks associated with their use of suppliers, manufacturers, distributors and retailers associated with products and services used by the organisation. Organisations should review risks posed by foreign control or interference, poor security practices, lack of transparency, and access and privileges as they relate to businesses in the cyber supply chain. For further information, organisations should review ACSC publications Identifying Cyber Supply Chain Risks and Cyber Supply Chain Risk Management.

Case Study: NotPetya

In 2017, a ransomware campaign known as NotPetya impacted organisations globally. This ransomware was distributed via a malicious software update for legitimate software. Following installation, NotPetya used automated techniques to retrieve legitimate credentials, identify other hosts on the network, and move laterally across a network before encrypting individual files and system partitions on victim hosts.

NotPetya used a range of common Windows utilities and services, as well as exploits for previously-patched vulnerabilities, to move laterally across a network. While the NotPetya attack occurred in June 2017, patches for these vulnerabilities had been released in March 2017.

NotPetya was an example of malicious cyber activity in which a lack of patching and continued use of out-dated protocols presented a significant risk to organisational security. Baseline cyber security measures such as the Essential Eight are applicable at any time and will mitigate against a wide range of malicious cyber activity.

ACSC and Partner Reporting

The below collation of ACSC, partner, and industry reporting provides technical details and mitigation measures relevant to a range of malicious activity. Organisations should review these publications for relevance to their own networks and consider implementing relevant mitigations.

Reporting on destructive malware, including WhisperGate, HermeticWiper, IsaacWiper, and CaddyWiper

Organisations seeking further information on detecting and mitigating against a range of recently-discovered destructive malware should review the following partner and industry publications:

- WeLiveSecurity: Industroyer2: Industroyer Reloaded
- WeLiveSecurity: CaddyWiper: New wiper malware discovered in Ukraine
- CrowdStrike Blog: Decryptable PartyTicket Ransomware Reportedly Targeting Ukrainian Entities
- ESET Research: Ukraine hit by destructive attacks before and during the Russian invasion with HermeticWiper and IsaacWiper
- WeLiveSecurity: IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine
- Palo Alto Networks Unit 42: Russia-Ukraine Crisis: How to Protect Against the Cyber Impact
- Symantec Threat Intelligence: Ukraine: Disk-wiping Attacks Precede Russian Invasion
- US CISA: Destructive Malware Targeting Organizations in Ukraine

Reporting on ransomware

Organisations seeking further information on detecting and mitigating against ransomware threats should review the following partner and industry publications:

- US CISA: Conti Ransomware
- ACSC: Ransomware Profile: Conti
- US CISA: 2021 Trends Show Increased Globalized Threat of Ransomware
- US CISA: How Can I Protect Against Ransomware?

Reporting on Cyclops Blink malware

Organisations seeking further information on the Cyclops Blink malware, which has widely affected network devices, should review the following UK NCSC publications:

- UK National Cyber Security Centre (NCSC): New Sandworm malware Cyclops Blink replaces VPNFilter
- UK NCSC: Cyclops Blink Malware Analysis Report

Reporting on the wider threat environment, a range of recent malicious cyber activity, and relevant security measures

Organisations seeking further information on a range of recent malicious activity, the wider threat environment, and relevant security measures that organisations can take to defend against these threats should refer to the following reporting:

- ACSC: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure
- US CISA: APT Cyber Tools Targeting ICS/SCADA Devices
- UK Foreign, Commonwealth & Development Office: Russia's FSB malign activity: factsheet
- Google Threat Analysis Group: Tracking cyber activity in Eastern Europe
- US CISA: Mitigating Attacks Against Uninterruptable Power Supply Devices
- US CISA: Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector
- US CISA: Strengthening Cybersecurity of SATCOM Network Providers and Customers
- US CISA: Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability
- Google Threat Analysis Group: An update on the threat landscape
- US CISA: Known Exploited Vulnerabilities Catalog
- US CISA: Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices
- US National Security Agency (NSA): Network Infrastructure Security Guidance
- ACSC: Routers targeted: Cisco Smart Install feature continues to be targeted by Russian state-sponsored actors
- ACSC: Secure the Cisco IOS and IOS XE Smart Install Feature
- US CISA: Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure
- US CISA: Joint Cybersecurity Advisory: Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology
- US NSA: Joint Cybersecurity Advisory: Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments
- Microsoft Security Blog: New sophisticated email-based attack from NOBELIUM
- Microsoft Security Blog: NOBELIUM targeting delegated administrative privileges to facilitate broader attacks.
- 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
- US CISA: CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats
- UK NCSC: NCSC advises organisations to act following Russia's further violation of Ukraine's territorial integrity
- US CISA: Russia Cyber Threat Overview and Advisories

Tactics, Techniques, and Procedures (TTPs)

In the current threat environment, there is a heightened risk that Australian organisations will be impacted by malicious cyber activity, either directly or through unintended or uncontained impacts. Actors may change their TTPs in response to public reporting and cyber security measures adopted by organisations, and new intrusion sets could be discovered. The following TTPs have been selected due to their common use by a range of actors and to illustrate the nature of threats that organisations may face. Organisations should focus on measures to mitigate against commonly used TTPs, while also referring to those identified in this advisory and linked material that may be relevant to them.

Initial access

Phishing and spear phishing emails containing malicious links or attachments are commonly used to establish initial access. Phishing emails may originate from email addresses designed to impersonate a trusted contact, or may be sent from legitimate but compromised email accounts, including as replies to existing email threads. Phishing lures can be complex and tailored to the targeted organisation, and their malicious nature may be obfuscated by the use of tools such as URL-shorteners and typical file types.

A range of malicious cyber actors attain initial access by compromising public-facing services. Malicious cyber activity commonly makes use of known vulnerabilities, for which patches or security measures may exist, to compromise public-facing services and attain initial access.

Malicious actors have also targeted accounts belonging to users on networks, using historically breached passwords or techniques such as brute forcing passwords to attain initial access. Legitimate credentials have been combined with exploitation of vulnerable services to attain initial access or escalated privileges. MFA configurations allowing for device enrolment to inactive accounts have been exploited by actors for initial access.

In some cases, malicious actors have compromised software supply chains in order to establish access to target organisations.

Persistence

Malicious cyber actors may seek to establish persistence, including for extended periods of time, using native tools and common or custom malware, including malware developed for specific devices. Actors use tools such as scheduled tasks, compromised update mechanisms, and compromised or actor-created accounts (including administrative accounts) to maintain access to victim networks. MFA configurations which “fail open” can be exploited by actors for persistence.

Discovery

Actors may use dedicated tooling or built-in system utilities to scan internal networks and discover hosts for lateral movement. Actors may conduct internal scanning automatically or manually. Actors may use data stored on compromised hosts to discover information about other hosts or accounts.

Lateral movement

Actors may use legitimate credentials, administrative privileges, and built-in system utilities to conduct lateral movement using only resources which are already present in the victim environment. Actors may also use malware or post-exploitation tools to conduct lateral movement by exploiting vulnerable services or hosts internal to a victim environment.

Impact

Actors may cause an impact to victim organisations by deploying ransomware or disruptive or destructive malware. Disruptive or destructive malware may be disguised and ransomware and present a ransom note despite not having a recovery mechanism.

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.

1. Patch applications and devices, particularly internet-facing services. Monitor for relevant vulnerabilities and security patches, and consider bringing forward patch timeframes. Review the US CISA catalogue of known exploited vulnerabilities for relevance to your systems.

2. Implement mitigations against phishing and spear phishing attacks. Disable Microsoft Office macros by default and limit used privileges. Ensure that staff report all suspicious emails received, links clicked, or documents opened.

3. 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. Prioritise internet-facing and critical network services, and ensure that logs are centrally stored.

4. Review incident response and business continuity plans. Plan responses to network compromise as well as disruptive or destructive activity such as ransomware. Ensure these plans are known to and actionable by staff, and are accessible even when systems are down.

5. Organisations should also review the Essential Eight and prioritise remediating any identified gaps in Essential Eight maturity. Following this, organisations should review technical details associated with any specific threats they have identified as relevant and incorporate these into monitoring and response plans.

6. Review the TTPs and IOCs contained in this product and linked reporting to determine if related activity has occurred on your organisation's network, and establish detections on such activity where feasible.

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:

Tables of notable tactics and techniques

Notable tactics, techniques, and procedures used against defence contractor networks

On 16 February 2022, CISA published details of malicious activity including the below TTPs. Please see CISA publication Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology for more detail on this activity.

Tactic	Technique	Procedure
Reconnaissance [TA0043] **Credential Access [TA0006]**	Gather Victim Identity Information: Credentials [T1589.001] Brute Force [T1110]	Malicious cyber 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]	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.
Initial Access [TA0001]	Valid Accounts [T1078] Exploit Public-Facing Application [T1190]	Actors used credentials in conjunction with known vulnerabilities on public-facing applications, such as virtual private networks (VPNs)—CVE-2020-0688

Tactic	Technique	Procedure
Privilege Escalation [TA0004]		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]	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]	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, 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, actors used legitimate credentials to exfiltrate emails from the victim's enterprise email system.
Persistence [TA0003] **Lateral Movement [TA0008]**	Valid Accounts [T1078]	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, actors used BloodHound to map the Active Directory.
Discovery [TA0007]	Domain Trust Discovery [T1482]	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]	Actors used multiple disparate nodes, such as VPSs, to route traffic to the target.

Notable tactics, techniques, and procedures identified as posing a risk to US critical infrastructure

On 11 January 2022, CISA published details of malicious activity including the below TTPs. Please see CISA publication Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure for more detail on this activity.

Tactic	Technique	Procedure
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]	Actors have conducted spearphishing campaigns to gain credentials of target networks.

Resource Development [TA0042]	Develop Capabilities: Malware [T1587.001]	Actors have developed and deployed malware, including ICS-focused destructive malware.
Initial Access [TA0001]	Exploit Public Facing Applications [T1190]	Actors use publicly known vulnerabilities, as well as zero-days, in internet-facing systems to gain access to networks.
Initial Access [TA0001]	Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]	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.
Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]	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]	Actors have used credentials of existing accounts to maintain persistent, long-term access to compromised networks.
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001] and Password Spraying [T1110.003]	Actors have conducted brute-force password guessing and password spraying campaigns.
Credential Access [TA0006]	OS Credential Dumping: NTDS [T1003.003]	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]	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]	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]	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]	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]	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.

Notable tactics, techniques, and procedures associated with the Cyclops Blink malware

On 23 February 2022, the UK NCSC published details of malicious activity including the below TTPs. Please see UK NCSC publication New Sandworm malware Cyclops Blink replaces VPNFilter for more detail on this activity.

Tactic	**Technique**	**Procedure**
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 Initialisation Scripts: RC Scripts [T1037.004]	Actors execute software on device startup using a modified S51armled RC script.

Persistence [TA0003]	Pre-OS Boot: System Firmware [T1542.001]	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]	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]	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]	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. 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]	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.

Notable tactics, techniques, and procedures associated with Conti ransomware

On 4 March 2022, the ACSC updated Ransomware Profile: Conti, which includes the below TTPs.

Tactic	**Technique**	**Procedure**
Initial Access [TA0001]	Exploit Public-Facing Application [T1190]	Malicious cyber 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.

Tactic	Technique	Procedure
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.
Persistence [TA0003]	External Remote Services [T1133]	Actors have used the commercial remote access software "AnyDesk" to persist on victim systems.
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.

Notable tactics, techniques, and procedures associated with destructive malware

On 1 March 2022, ESET Research published details of malicious activity including the below TTPs. Please see ESET publication IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine for more detail on this activity.

Tactic	Technique	Procedure
Resource Development [TA0042]	Obtain Capabilities: Tool [T1588.002] Obtain Capabilities: Code Signing Certificates [T1588.003]	Malicious cyber actors have used RemCom and possibly Impacket for remote access and lateral movement. Actors have acquired code-signing certificates with which malicious executables have been signed.
Initial Access [TA0001]	Valid Accounts: Domain Accounts [T1078.002]	Actors have deployed destructive malware using Group Policy Objects.
Execution [TA0002]	Command and Scripting Interpreter: Windows Command Shell [T1059.003] Native API [T1106] System Services: Service Execution [T1569.002] Windows Management Instrumentation [T1047]	Actors have used native tools such as the Windows command prompt and native APIs in destructive malware attacks. Destructive malware has made use of drivers to corrupt data, and has made use of Windows Management Instrumentation to spread to other hosts.
Discovery [TA0007]	Remote System Discovery [T1018]	Destructive malware may scan local IP ranges to discover additional reachable hosts.

Tactic	Technique	Procedure
Lateral Movement [TA0008]	Remote Services: SMB/Windows Admin Shares [T1021.002] Remote Services: Distributed Component Object Model [T1021.003]	Destructive malware may spread to additional hosts using SMB or WMI functionality such as WbemLocator.
Impact [TA0040]	Disk Wipe: Disk Structure Wipe [T1561.002] Disk Wipe: Disk Content Wipe [T1561.001] Data Destruction [T1485]	Destructive malware has corrupted MBRs, MFTs, as well as individual files located within system and user directories.

Notable tactics, techniques, and procedures associated with the exploitation of default MFA configurations

On 15 March 2022, CISA published details of malicious activity including the below TTPs. Please see CISA publication Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability for more detail on this activity

Tactic	Technique	Procedure
Initial Access [TA0001]	Valid Accounts [T1078]	Malicious cyber actors used compromised credentials in order to access MFA device enrolment for a victim account.
Privilege Escalation [TA0004]	Exploitation for Privilege Escalation [T1068]	Actors exploited the known vulnerability 'PrintNightmare' (CVE-2021-34527) to obtain administrative privileges.
Persistence [TA0003]	Modify Authentication Process [T1556]	Actors modified system files to effectively disable MFA on the victim network.
	External Remote Services [T1133]	Actors directly connected to the victim network's virtual private network to conduct further activity.
Defence Evasion [TA0005]	Modify Registry [T1112]	Actors used the regedit tool to modify registry data.
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001]	Actors initially compromised a victim account using a brute-force attack.
	OS Credential Dumping: NTDS [T1003.003]	Actors may have used the utility ntdsutil to enumerate user accounts.
Discovery [TA0007]	Remote System Discovery [T1018]	Actors used the built-in ping utility to check connectivity to victim hosts.
Lateral Movement [TA0008]		Actors used combinations of the above techniques to move laterally to victim hosts.
Collection [TA0009]	Archive Collected Data: Archive via Utility [T1560.001]	Actors may have used a RAR utility to archive victim data.

Tables of relevant indicators of compromise (IOCs)

IOCs associated with a sophisticated malicious email campaign

On 27 May 2021, Microsoft published details of malicious activity including the below IOCs. Please see Microsoft publication New sophisticated email-based attack from NOBELIUM for more detail on this activity.

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

IOCs associated with the Cyclops Blink malware

On 23 February 2022, the UK NCSC published details of malicious activity including the below IOCs. Please see UK NCSC publication New Sandworm malware Cyclops Blink replaces VPNFilter for more detail on this activity.

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
100.43.220[.]234	IPv4 address	C2 server IP address
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

IOCs associated with WhisperGate, HermeticWiper, IsaacWiper, and CaddyWiper destructive malware

Multiple organisations have published details of malicious activity including the below IOCs. Please see CISA publication Destructive Malware Targeting Organizations in Ukraine and ESET Research publications IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine and CaddyWiper: New wiper malware discovered in Ukraine for more detail on this activity.

a196c6b8ffcb97ffb276d04f354696e2391311db3841ae16c8c9f56f36a38e92	SHA-256	Hash of malicious executable (WhisperGate)
dcbbae5a1c61dbbbb7dcd6dc5dd1eb1169f5329958d38b58c3fd9384081c9b78	SHA-256	Hash of malicious executable (WhisperGate)
0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da	SHA-256 hash	Trojan.Killdisk (HermeticWiper)
1bc44eef75779e3ca1eefb8ff5a64807dbc942b1e4a2672d77b9f6928d292591	SHA-256 hash	Hash of malicious executable (HermeticWiper)
a952e288a1ead66490b3275a807f52e5	MD5 hash	RCDATA_DRV_X64 (HermeticWiper)
231b3385ac17e41c5bb1b1fcb59599c4	MD5 hash	RCDATA_DRV_X86 (HermeticWiper)
095a1678021b034903c85dd5acb447ad	MD5 hash	RCDATA_DRV_XP_X64 (HermeticWiper)
eb845b7a16ed82bd248e395d9852f467	MD5 hash	RCDATA_DRV_XP_X86 (HermeticWiper)
a64c3e0522fad787b95bfb6a30c3aed1b5786e69e88e023c062ec7e5cebf4d3e	SHA-256 hash	Trojan.Killdisk (HermeticWiper)
4dc13bb83a16d4ff9865a51b3e4d24112327c526c1392e14d56f20d6f4eaf382	SHA-256 hash	Ransomware (HermeticWiper)
3c557727953a8f6b4788984464fb77741b821991acbf5e746aebdd02615b1767	SHA-256 hash	Hash of malicious executable (HermeticWiper)
2c10b2ec0b995b88c27d141d6f7b14d6b8177c52818687e4ff8e6ecf53adf5bf	SHA-256 hash	Hash of malicious executable (HermeticWiper)
06086c1da4590dcc7f1e10a6be3431e1166286a9e7761f2de9de79d7fda9c397	SHA-256 hash	Hash of malicious executable (HermeticWiper)
ad602039c6f0237d4a997d5640e92ce5e2b3bba3	SHA-1 hash	Hash of malicious file (IsaacWiper)
736a4cfad1ed83a6a0b75b0474d5e01a3a36f950	SHA-1 hash	Hash of malicious file (IsaacWiper)
e9b96e9b86fad28d950ca428879168e0894d854f	SHA-1 hash	Hash of malicious file (IsaacWiper)
98b3fb74b3e8b3f9b05a82473551c5a77b576d54	SHA-1 hash	Hash of malicious executable (CaddyWiper)

IOCs associated with exploitation of default MFA configurations

On 15 March 2022, CISA published details of malicious activity including the below IOCs. Please see CISA publication Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability for more detail on this activity

45.32.137[.]94	IPv4 address	C2 server IP address
191.96.121[.]162	IPv4 address	C2 server IP address
173.239.198[.]46	IPv4 address	C2 server IP address
157.230.81[.]39	IPv4 address	C2 server IP address

IOCs associated with destructive malware targeting energy sector organisations in Ukraine

On 13 April 2022, ESET Research published details of new destructive malware used to target an energy sector organisation as recently as April 2022. Please see ESET Research publication Industroyer2: Industroyer Reloaded for more detail on this activity.

fd9c17c35a68fc505235e20c6e50c622aed8dea0	SHA-1 hash	Hash of malicious file
6fa04992c0624c7aa3ca80da6a30e6de91226a16	SHA-1 hash	Hash of malicious file
9ce1491ce69809f92ae1fe8d4c0783bd1d11fbe7	SHA-1 hash	Hash of malicious file
0090cb4de31d2d3bca55fd4a36859921b5fc5dae	SHA-1 hash	Hash of malicious file

d27d0b9bb57b2bab881e0efb97c740b7e81405df	SHA-1 hash	Hash of malicious file
3cdbc19bc4f12d8d00b81380f7a2504d08074c15	SHA-1 hash	Hash of malicious file
8fc7646fa14667d07e3110fe754f61a78cfde6bc	SHA-1 hash	Hash of malicious file

Document Change Log

Version	Date	Change Summary
11	28 April 2022	▪ Addition of link to the joint cybersecurity advisory on Russian state-sponsored and criminal cyber threats to critical infrastructure ▪ Addition of information relating to targeting of UPS devices ▪ Addition of information on identifying cyber supply chain risks ▪ Addition of information and IOCs relating to destructive activity targeting an energy sector organisation ▪ Addition of links to a Google Threat Analysis Group blog and a UK Government factsheet.
10	25 March 2022	▪ Addition of link to CISA-FBI advisory on SATCOM security ▪ Addition of link to CISA-FBI-DOE advisory on targeting of US and international energy sector organisations ▪ Addition of STIX file to advisory web page
9	16 March 2022	▪ Addition of link to updated US CISA Conti Ransomware Advisory ▪ Addition of link to Google Threat Analysis Group blog ▪ Addition of information relating to CaddyWiper malware ▪ Addition of information and mitigation advice in relation to the exploitation of default MFA configurations by malicious actors.
8	9 March 2022	▪ Addition of NotPetya case study and priority actions ▪ Revisions to relevant reporting list ▪ Revisions to Tactics, Techniques, and Procedures (TTPs) and Mitigations sections ▪ Addition to malware associated with Conti
7	4 March 2022	▪ Structural changes ▪ Addition of links to a CrowdStrike blog relevant to the HermeticWiper-associated ransomware ▪ Addition of links to US CISA publication on threats to US Critical Infrastructure, US CISA Known Exploited Vulnerabilities Catalog, and NSA publication Network Infrastructure Security Guidance ▪ Addition of information and links relating to targeting of network devices.

6	2 March 2022	▪ Addition of links, IOCs, and TTPs associated with IsaacWiper
5	28 February 2022	▪ Addition of links to Symantec Threat Intelligence and Palo Alto Networks Unit 42 blogs on HermeticWiper ▪ Addition of further IOCs associated with HermeticWiper
4	27 February 2022	▪ Addition of link to CISA Alert AA22-057A - Destructive Malware Targeting Organizations in Ukraine ▪ Addition of further IOCs associated with HermeticWiper
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.

TLP: WHITE

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.