Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

TLP: WHITE

Document Version: 1.0 (8 May 2020)

2020-009: Advanced Persistent Threat (APT) actors targeting Australian health sector organisations and COVID-19 essential services

Overview

The Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC) is aware that Advanced Persistent Threat (APT) actors are actively targeting health sector organisations and medical research facilities. As the outbreak of the virus continues to impact the health sectors of countries worldwide, APT groups may be seeking information and intellectual property relating to vaccine development, treatments, research and responses to the outbreak as this information is now of higher value and priority globally. Accordingly, Australia's health or research sectors could be at greater threat of being targeted, and potentially compromised, by malicious APT groups.

Due to the increased pressure placed on the health sector to respond to the COVID-19 pandemic, it is critical that health sector organisations ensure that their networks are protected from malicious cyber actors who may seek to disrupt essential services or compromise business-critical systems.

Sophisticated actors will often use the most efficient means available to target a victim's network and, in the current climate, APT groups may seek to maximise on the public desire for COVID-19 related information by generating specific COVID-19 themed spear-phishing emails to attempt to compromise victims.

Adversaries and cybercrime actors have been identified as responsible for compromising email servers of health sector entities in Australia, which are then used to distribute COVID-19 phishing emails in an attempt to deploy malicious software including ransomware or to gain access to other targeted organisations.

Malicious actors view health sector entities as a lucrative target for ransomware attacks. This is because of the sensitive personal and medical data they hold, and how critical this data is to maintaining operations and patient care. A significant ransomware attack against a hospital network would have major impact.

Sophisticated actors have also been seen undertaking brute force attacks using a trial-and-error method to guess login credentials, and password spray attacks that attempt to access numerous accounts with a list of commonly used passwords. Attacks such as these often result in the theft of sensitive data, and underscore the importance of a strong cyber security culture amongst employees. This includes adopting multi-factor authentication, strong password policies, and regular reviews of network logs for signs of malicious activity.

The exploitation of compromised Remote Desktop Protocol (RDP) credentials by malicious actors is also a significant concern, particularly as RDP is widely used by medical clinics and doctors' surgeries to access centralised patient databases and other shared information repositories. Compromised RDP credentials can enable unauthorised access to networks, in a manner that enables the malicious actor's digital footprint and identification to be obscured.

Organisations should implement the recommendations in this advisory in order to mitigate the threat of this malicious activity and harden their network against unauthorised access. The ACSC also recommends that organisations consider the recent joint advice provided by the NCSC-UK and CISA-US:

- https://www.ncsc.gov.uk/news/warning-issued-uk-usa-healthcare-organisations
- https://www.us-cert.gov/ncas/alerts/AA20126A

Threat from APTs

Advanced Persistent Threat (APT) actors is the term given to the most sophisticated and well-resourced type of malicious cyber adversary. Commonly associated with nation states, APTs will seek to compromise networks to obtain economic, policy, legal, or defence and security information for their strategic advantage. APT actors may also seek to achieve disruptive or destructive effects against their targets.

These actors use a range of different tradecraft, making it very difficult to identify patterns. Even the most sophisticated adversaries are not above using relatively simple or basic techniques to achieve their goal. While some APTs use combinations of high-end hacking tools, others will adopt fairly rudimentary methods such as phishing. In all cases, their actions are very deliberate and they carefully tailor their cyber attack to optimise the chances of success, and minimise the chances of detection.

APTs are also very patient adversaries, known to undertake detailed reconnaissance of high value networks over months and sometimes years. They will also track representatives that work in the organisation they are targeting – in an effort to find the weakest link or point of vulnerability they can exploit. Even seemingly basic information such as contact details and employment history on an organisation's website or an employees' social media profile can provide useful leads for APTs to target.

APT actors pose the most significant threat to Australia's national security and economic prosperity.

Threat from cybercriminals

Cybercrime actors are opportunistic and capitalise on natural disasters or significant events to generate profit. They seek to prey on vulnerable people, consumers and organisations, using fear and urgency tactics to distribute malware or steal personal and financial information. Cybercriminals regularly attempt to trick victims into revealing sensitive information, such as user accounts to corporate systems or personal identifying information. Since the onset of the COVID-19 pandemic, the ACSC has identified a range of different email and SMS phishing campaigns being perpetrated by cybercrime actors. For more information refer to the ACSC's Threat Updates on COVID-19 themed malicious cyber activity:

- https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity
- https://www.cyber.gov.au/threats/threat-update-covid-19-malicious-cyber-activity-20-apr-2020

The ACSC has also received reports of senior officials in health and emergency services organisations receiving targeted spear-phishing emails. These were carefully crafted COVID-19 related emails designed to trick the recipient into clicking a link that downloaded malicious software onto their organisations' corporate network.

A particular threat to the health sector is transnational cybercrime syndicates and their affiliates, who develop, share, sell and use sophisticated tools and techniques. There is a booming underground marketplace offering cybercrime-as-a-service, or access to high-end hacking tools that were once only available to nation states. Consequently, the lines between state-sponsored actors and cyber criminals are becoming increasingly blurred and the bar for entry is lower than ever. Malicious actors with minimal technical expertise can now purchase illicit tools and services to generate alternative income streams, launder the proceeds of traditional crimes or undertake network intrusions on behalf of more sophisticated adversities.

Organisations in the health and other critical sectors involved in COVID-19 response activities must remain vigilant against the threat posed by APT and cybercrime actors by ensuring appropriate cyber security protections are in place.

Recommendations for the health sector

The ACSC recommends that organisations in the health sector implement the following cyber security mitigations:

Implement Essential Eight security controls

The ACSC strongly recommends the implementation of the ASD Essential Eight mitigations to mitigate threats of most methodologies used by APT actors to compromise computer networks.

- https://www.cyber.gov.au/publications/essential-eight-explained

Specifically, to combat the threat of this recent spate of malicious activity, health sector organisations should implement the following mitigations.

Enabling Multi-Factor Authentication (MFA)

MFA is one of the most effective controls an organisation can implement to prevent an adversary from gaining unauthorised access to a device or network and then compromising sensitive information. When implemented correctly, MFA can make it significantly more difficult for an adversary to steal legitimate credentials to facilitate further malicious activities on a network.

Using MFA provides a secure authentication mechanism that is far less susceptible to brute force attacks. For more information on MFA, please visit: https://www.cyber.gov.au/publications/multi-factor-authentication.

Block Macros

Where possible, the ACSC recommends blocking macros from the internet, and only allowing the execution of vetted and approved macros.

In many cases, initial infection of a network occurs via an embedded macro in a Microsoft Office document. Disabling all unknown macros can significantly reduce the network's risk-surface.

Implementing regular patching of systems and applications

Software patches are released by device and software manufacturers to fix flaws in previous versions, including cyber security vulnerabilities. Malicious actors are constantly looking for vulnerabilities in devices and software versions that can be exploited. Once a vulnerability is in the public domain, malicious actors will begin exploiting it within a matter of days or weeks. Timely patching of vendor-supported security vulnerabilities is one of the most important steps an organisation can take to protect computer systems from cybercriminals and other malicious actors. For more information on patching, please visit;

- https://www.cyber.gov.au/advice/patching-and-updating.
- https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches

Making regular back-ups of critical systems and databases

Due to the large amounts of patient and other sensitive data they hold, health sector entities are a very attractive organisation for malicious adversaries to target with a ransomware attack. Regularly backing up of computers, databases and IoT devices, and choosing automatic back-ups where possible, will ensure quick and easy restoration of critical systems and services. Keep back-ups separate from corporate computers, on separate devices or use a secure cloud service.

Implement additional security controls

The ACSC publishes a comprehensive list of Strategies to Mitigate Cyber Security Incidents.

- https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents

Health sector organisations should also consider implementing the following specific mitigations.

Alert and Educate Staff

Consider sending out an organisation wide alert to raise awareness of the dangers associated with opening attachments on unusual emails. Consider implementing an education program to improve staff awareness of cyber security, or how to spot suspicious emails. For more details on how to implement a successful staff awareness program see ACSC's Improving staff awareness publication.

- https://www.cyber.gov.au/advice/improving-staff-awareness

Email content scanning

Phishing emails have been used to spread malware across a network, with the initial intrusion linked to an email containing a malicious attachment. Email content filters and dynamic email analysis sandboxing capabilities could be put in place to prevent malicious content from reaching users and reduce the likelihood of compromise. To complement this, antivirus software using heuristics and reputation ratings should also be installed to identify and prevent malicious attachments that do make it to end users.

Develop/update incident response plans

Organisations should ensure that they have an up-to-date Incident Response Plan (IRP) that includes procedures to respond to a ransomware infection. In most situations, the aim of the ransomware procedures will be to:

- Quickly identify affected systems;
- Quarantine the affected systems and isolate business critical systems;
- Identify and implement security controls to prevent the propagation of the ransomware to other systems; and
- Preserve evidence for future analysis and restoration from backup.

During the COVID-19 pandemic, systems that support an organisation pandemic response and patient care functions should be considered business critical. The IRP should document a tested procedure for isolating these systems so that they can be quickly placed under protection if a ransomware outbreak occurs.

Implementing Network Segmentation and Segregation

APT actors use techniques that allow them to move laterally within an organisations network. Network segmentation involves partitioning a network into smaller networks; while network segregation involves developing and enforcing a ruleset for controlling the communications between specific hosts and services.

When implementing network segmentation and segregation, the aim is to restrict the level of access to sensitive information, hosts and services while ensuring an organisation can continue to operate effectively. Network segmentation and segregation measures must be carefully planned, robustly enforced, closely monitored and implemented in a manner that ensures the security controls cannot be bypassed.
For more information on Network Segmentation and Segregation, please visit:
https://www.cyber.gov.au/publications/implementing-network-segmentation-and-segregation

Cyber Incident Reporting

If you have questions about this advice or have indications that your network has been compromised, contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).

Reporting Cybercrime

The ACSC manages ReportCyber, an online portal for reporting cybercrime incidents. The portal is designed for individuals, businesses and large organisations to report a variety of computer-enabled crimes, such as online frauds, ransomware, identity theft, romance scams, online image abuse and business email compromise.

Once a cybercrime is reported, the matter is referred to law enforcement and national security agencies for assessment, investigation and resolution where possible. Reporting incidents helps the Australian Government better understand and develop strategies to disrupt and prevent online threats impacting Australia's interests and the community. More information, including accessing the ReportCyber online portal, please visit: https://www.cyber.gov.au/report

Traffic light protocol

The following table lists the classification levels used in the traffic light protocol (TLP) and describes the restrictions on access and use for each classification level.

TLP classification	Restrictions on access and use
RED	Access to and use by your ACSC security contact officer(s) only. You must ensure that your ACSC security contact officer(s) does not disseminate or discuss the information 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 security contact officer(s).
AMBER	Restricted internal access and use only. Subject to the below, you shall only make AMBER publications available to your employees on a 'need to know basis' strictly for your internal processes only to assist in the protection of your ICT systems. In some instances you may be provided with AMBER publications which are marked to allow you to also disclose them to your contractors or agents on a need-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 publications 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 publication. You may not publish or post on the web or otherwise release it in circumstances where confidentiality may not be maintained.
WHITE	Not restricted. WHITE publications 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 ACSC that is not classified in accordance with the TLP must be treated as AMBER classified information, unless otherwise agreed in writing ACSC.