Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

TLP:White

Summary of Tradecraft Trends for 2019-20: Tactics, Techniques and Procedures Used to Target Australian Networks

Overview

The Australian Cyber Security Centre (ACSC) investigated and responded to numerous cyber security incidents during 2019 and 2020 so far. This advisory provides a summary of notable tactics, techniques and procedures (TTPs) exploited by Advanced Persistent Threats (APT) and cybercriminals identified during the ACSC's investigations. These TTPs are summarised practically in the framework of tactics and techniques provided by MITRE ATT&CK[1]. This technical guidance is provided for IT security professionals at public and private sector organisations.

Recommended mitigations

Partners are strongly encouraged to review their environments for the presence of the exploited vulnerabilities and provided TTPs. Detection of related findings should be reported to the ACSC.

The ACSC strongly recommends implementing ASD's Essential Eight[2]. A review of investigations performed by the ACSC has shown that implementation of ASD's Essential Eight on victim networks would substantially reduce the risk of compromise by the adversary TTPs identified in this advisory.

Detection

This advisory provides information on methods to detect many of the TTPs listed. Additional detailed information on detection for each TTP is available at the associated MITRE ATT&CK link provided. Network owners who discover evidence of the TTPs from this advisory on their systems should contact the ACSC via email at asd.assist@defence.gov.au to report their findings and for further advice.

MITRE ATT&CK™ is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cyber security product and service community.

ATT&CK™

[1] https://attack.mitre.org
[2] https://www.cyber.gov.au/publications/essential-eight-explained

Initial access

The following section covers TTPs related to gaining initial access to vulnerable systems identified during ACSC investigations.

T1190 – Exploit Public-Facing Application

Abuse of file upload functionality

The ACSC has identified legitimate file upload functions on web applications being used to upload malicious files such as web shells to web servers that do not enforce stringent file upload restrictions. Malicious files uploaded to web applications, such as web shells, can allow an actor remote unauthorised access to the web server. This provides the actor with an entry point to conduct further malicious activity.

Network owners should analyse web server file upload locations for web shells[3] and other malicious files. They should also investigate web logs for signs of malicious activity.

Exploitation of Telerik Web User Interface (UI)

The ACSC has identified Telerik Web UI vulnerabilities: ***CVE-2017-9248***[4], ***CVE-2017-11317***[5] and ***CVE-2017-11357***[6] being exploited to gain access to vulnerable systems. The vulnerabilities allow an actor to brute-force a cryptographic key, which can then be used to log into the system and upload malicious files.

Network owners who are running Telerik on servers should refer to ***ACSC Advisory 2019-126***[7] for further guidance on detection, remediation and mitigation of these Telerik Web UI vulnerabilities.

Exploitation of Pulse Connect Secure VPN

The ACSC has identified Pulse Connect Secure vulnerability ***CVE-2019-11510***[8] being exploited to gain access to vulnerable networks. This vulnerability enables an attacker to retrieve arbitrary files, including those containing authentication credentials. Once obtained, an attacker can gain unauthorised access to a victim's network using these authentication credentials, enabling further malicious activity.

Network owners should refer to ***ACSC Advisory 2019-129***[9] for further guidance on detection, mitigation and remediation of the Pulse Connect Secure vulnerability.

Exploitation of Fortigate SSL VPN

The ACSC has identified vulnerabilities ***CVE-2018-13379***[10], ***CVE-2018-13382***[11] and ***CVE-2018-13383***[12] in Fortigate SSL VPN being exploited to gain access to vulnerable networks. These vulnerabilities allow an attacker to retrieve authenticated users credentials. Once an attacker is authenticated, a vulnerability allowing for remote code execution

[3] https://www.cyber.gov.au/advice/detect-and-prevent-web-shell-malware
[4] https://nvd.nist.gov/vuln/detail/CVE-2017-9248
[5] https://nvd.nist.gov/vuln/detail/CVE-2017-11317
[6] https://nvd.nist.gov/vuln/detail/CVE-2017-11357
[7] https://www.cyber.gov.au/threats/advisory-2019-126
[8] https://nvd.nist.gov/vuln/detail/CVE-2019-11510
[9] https://nvd.nist.gov/vuln/detail/CVE-2019-11510
[10] https://nvd.nist.gov/vuln/detail/CVE-2018-13379
[11] https://nvd.nist.gov/vuln/detail/CVE-2018-13382
[12] https://nvd.nist.gov/vuln/detail/CVE-2018-13383

is used to establish a web shell to enable persistent access. Additionally, once authenticated an actor can attempt to modify any users' password.

Network owners should refer to the UK's NCSC's ***VPN Vulnerability alert***[13] for further guidance on detection, mitigation and remediation of these Fortigate SSL vulnerabilities.

Exploitation of Citrix ADC

The ACSC has identified vulnerability ***CVE-2019-19781***[14] in Citrix Application Delivery Controller (ADC), Citrix Gateway and Citrix SD-WAN WANOP being exploited to gain access to vulnerable networks. This vulnerability enables unauthenticated users to execute arbitrary code on vulnerable Citrix devices.

The ACSC has observed actors deploying web shells to vulnerable Citrix servers to enable persistent access, avoid detection and perform further malicious activity. Additionally, the ACSC has observed the deployment of additional malicious software to deny exploitation attempts from other malicious actors, preserving the unauthorised access for the initial attacker.

Network owners should refer to ***ACSC Advisory 2020-001***[15] for further guidance on detection, mitigation and remediation of the Citrix vulnerability.

Further information on the ***Exploit Public-Facing Application*** technique[16] is available from MITRE.

T1078 – Valid Accounts

The ACSC has identified successful brute forcing activity against the login pages of web applications. This brute forcing activity has been automated and often includes the use of commercial web application vulnerability scanning tools.

Brute forcing of login pages allows unauthorised access, potentially with elevated privileges, enabling the actor to conduct further malicious activities.

Network owners should analyse web server logs for signs of the following activity indicating brute force login attempts:

- Large volumes of HTTP requests over small periods of time (hours) to web application resources, related to login pages and attempting authentication to one or more legitimate accounts, from the same IP address.
- HTTP user agent strings containing the name of web application vulnerability scanning tools. A list of common tool names is available from OWASP[17].

If signs of brute force login attempts are identified, network owners should analyse the associated web traffic for successful user access from the scanning IP address. This can indicate successful compromise, particularly if the login event follows the scanning period. For example, hundreds of attempts against `login.aspx` followed by a successful login from the same IP may indicate successful unauthorised access.

Further information on the ***Valid Accounts*** technique[18] is available from MITRE.

[13] https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities

[14] https://nvd.nist.gov/vuln/detail/CVE-2019-19781

[15] https://www.cyber.gov.au/threats/advisory-2020-001-active-exploitation-critical-vulnerability-citrix-application-delivery-controller-and-citrix-gateway

[16] https://attack.mitre.org/techniques/T1190/

[17] https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

[18] https://attack.mitre.org/techniques/T1078/

T1193 – Spearphishing Attachment

The ACSC has identified instances where users have executed malware embedded in email attachments. The text of the email provides the user with a plausible reason to open the attachment. Once opened, the malware will exploit an existing vulnerability or execute directly on the user's system.

Network intrusion detection systems and email gateways can be used to detect spearphishing with malicious attachments in transit. Network owners with host-based monitoring capabilities may also be able to detect malicious events once the attachment is opened.

Further information on the ***Spearphishing Attachments*** technique[19] is available from MITRE.

T1189 – Drive-by Compromise

The ACSC has identified instances where users have downloaded malicious Microsoft Access database files. The database files contain a malicious payload that, when opened with Microsoft Access, will create a persistent access for actor interaction with the affected system.

Network owners should analyse user workstations for the following artefacts that can indicate potential compromise:

- Database files with the extension `.accde` appended to a legitimate file extension such as: `.pdf`, `.doc` and `.docx`. For example, `<filename>.docx.accde`
- Database files with the extension `.accdb` located in the `%APPDATA%\Roaming\Microsoft` directory.

Please note: this activity is not indicative of a compromise or vulnerability in any Microsoft product(s).

Further information on the ***Drive-by Compromise*** technique[20] is available from MITRE.

Execution

The following section covers TTPs relating to the execution of a program or code on compromised systems identified during ACSC investigations.

T1059 – Command-Line Interface

The ACSC has identified the use of `cmd.exe` and `PowerShell.exe` to execute both actor tools and native Windows commands and utilities.

Further information on the ***Command-Line Interface*** technique[21] is available from MITRE.

T1086 – PowerShell

The ACSC has identified the use of PowerShell scripts to conduct malicious activity on compromised systems. PowerShell can enable an actor to perform a range of offensive techniques on a network. Network owners with host-based monitoring capabilities should analyse networks for signs of the following:

- Command: `powershell -nop -exec bypass -windowsstyle hidden -c c:\ProgramData\<scriptname>.ps1`
- PowerShell scripts communicating with external IP addresses.

[19] https://attack.mitre.org/techniques/T1193/

[20] https://attack.mitre.org/techniques/T1189/

[21] https://attack.mitre.org/techniques/T1059/

- An IIS process (`w3wp.exe`) spawning PowerShell processes.

Further information on the ***PowerShell*** technique[22] is available from MITRE.

T1064 – Scripting

The ACSC has also identified the use of various script languages to automate the execution of other tools and native Windows commands. Script types identified include JavaScript (JScript), Batch files and Microsoft Office macros.

Further information on the ***Scripting*** technique[23] is available from MITRE.

T1106 – Execution through API

The ACSC has identified the use of standard Windows Application Programming Interface (API) calls to execute various tools and commands. These calls originated from actor malware and web shells.

Further information on the ***Execution through API*** technique[24] is available from MITRE.

T1204 – User Execution

Related to T1189 – Drive-by Compromise, in some investigations users subsequently opened the downloaded malicious Microsoft Access database files. The database files contain a malicious payload that, when opened with Microsoft Access, create a persistent access point for an actor to remotely access the affected system.

Further information on the ***User Execution*** technique[25] is available from MITRE.

T1504 – PowerShell Profiles

The ACSC has identified the use of PowerShell profiles that will trigger malware to be executed anytime PowerShell is launched. Malicious PowerShell profiles identified by the ACSC have executed embedded base64 encoded .NET assemblies using the `Assembly.Load()` function. Network owners should analyse the following locations for PowerShell profiles and investigate contents to ensure they do not execute unauthorised code:

- `C:\Users\<user>\Documents\WindowsPowerShell\Microsoft.PowerShell_profile.ps1`
- `C:\Users\<user>\Documents\Profile.ps1`
- `<PowerShell installation>\Microsoft.PowerShell_profile.ps1`

Further information on the ***PowerShell Profile*** technique[26] is available from MITRE.

Custom .NET binaries

The ACSC has identified the use of .NET tools to run arbitrary JavaScript or PowerShell commands on a compromised host. These utilised Outlook tasks to send and receive commands. The ACSC has also identified the use of .NET tools to enhance the capabilities of web shells. Some of the capabilities of these .NET binaries include:

- Chrome browser history dumping
- user keystroke logging

[22] https://attack.mitre.org/techniques/T1086/
[23] https://attack.mitre.org/techniques/T1064/
[24] https://attack.mitre.org/techniques/T1106/
[25] https://attack.mitre.org/techniques/T1204/
[26] https://attack.mitre.org/techniques/T1204/

- process list dumping.

One of the .NET tools had hard coded locations to store some of the files required for functionality. Network owners should analyse the following directories for files named `_wldx`, `_rldx` and other suspicious files:

- `C:\ProgramData\tmp`
- `C:\ProgramData\google`
- `C:\ProgramData\Sun\low`

Persistence

The following section covers TTPs relating to persistence mechanisms identified during ACSC investigations.

T1060 – Registry Run Keys / Startup Folder

The ACSC has identified the creation of link (`.lnk`) files within a user's Startup folder in order to maintain persistent access, for example:

- `%APPDATA%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\<filename>.lnk`

These `.lnk` files would link to a benign Excel spreadsheet which would then load malicious content via actor use of `.xlam` files. These Microsoft Excel `.xlam` files contain malicious macros and were placed into the `XLSTART` folder in the `%APPDATA%` directory. Excel files stored in the `XLSTART` folder are loaded automatically whenever any Excel spreadsheet is opened.

Particular attention should be paid to shortcut files in the Startup folder that reference Excel spreadsheets.

Network owners should also analyse the following location for any malicious `.xlam` files, noting that not all `.xlam` files in this location will be malicious:

- `%APPDATA%\Roaming\Microsoft\Excel\XLSTART`

Further information on the ***Registry Run Keys / Startup Folder*** technique[27] is available from MITRE.

T1100 – Web Shell

The ACSC has identified widespread use of web shells as a persistence mechanism on both internet facing and internal systems. Web shells enable an actor to have persistent, remote unauthorised access to the web server where the shell is located, often running at the same privilege level used by the web application, potentially up to SYSTEM level privileges. Web shells discovered during investigations have existed as both standalone files, consisting solely of malicious web shell code, and also as legitimate files where an actor has modified a legitimate file to contain malicious web shell code.

Further information on web shells can be found at https://www.cyber.gov.au.

Further information on the ***Web Shell*** technique[28] is available from MITRE.

T1108 – Redundant Access

The ACSC has identified the use of multiple web shells on compromised hosts as a means of redundant access. Network owners should be aware during investigations that multiple copies of the same or similar malicious files such as web shells may be present on a compromised host and provide persistent access for an actor.

[27] https://attack.mitre.org/techniques/T1060/
[28] https://attack.mitre.org/techniques/T1100/

Further information on the ***Redundant Access*** technique[29] is available from MITRE.

T1504 – PowerShell Profiles

In addition to its previously identified use as an Execution technique the ACSC also identified the use of PowerShell profiles as a Persistence technique. There is no existing MITRE ATT&CK technique which accurately represents the use of PowerShell Profiles as a Persistence technique.

Privilege escalation

The following section covers privilege escalation techniques identified during ACSC investigations.

T1068 – Exploitation for Privilege Escalation

RottenPotato

The ACSC has identified the use of the RottenPotato exploit to gain SYSTEM level privileges on vulnerable systems. The exploit works by tricking the *NT AUTHORITY\SYSTEM* account into authenticating via NTLM to a compromised TCP endpoint. A man-in-the-middle attack is performed on the authentication process, allowing an actor to impersonate the SYSTEM security token. The following is a list of Remote Procedure Call (RPC) event indicators that can be used to detect the use of RottenPotato on a system. Network owners should consider implementing a single rule, covering the following three indicators, into their host- based monitoring watch lists:

- *Microsoft_Windows_RPC.InterfaceUuid == {99fcfec4-5260-101b-bbcb-00aa0021347a}*
- *Microsoft_Windows_RPD.NetworkAddress == "127.0.0.1"*
- *Microsoft_Windows_RPC.AuthenticationService == Microsoft_Windows_RPC. AuthenticationServices.Value_9*

Further information on the ***Exploitation for Privilege Escalation*** technique[30] is available from MITRE.

Defence evasion

The following section covers defence evasion techniques identified during ACSC investigations.

T1099 – Timestomp

The ACSC has identified the utilisation of timestomping in an attempt to prevent detection of malicious files dropped on systems. Timestomping is the process of modifying timestamps on files in order to make them appear as if they were created or modified at a different time. Common examples identified during investigations involve time stomping web shells so that the timestamp matches the parent folder or another file located in the same directory.

During investigations, network owners should investigate potential timestomping activity and not solely rely on file creation or modification timestamps as indicators of recent activity. Network owners with host-based monitoring may be able to detect file modification changes to file timestamps. The following list of indicators may indicate timestomping has occurred:

- Differences between the *$STANDARD_INFORMATION* and *$FILE_NAME* timestamps for the same file.
- Files that have all zeroes in the timestamp nanosecond field.

[29] https://attack.mitre.org/techniques/T1108/
[30] https://attack.mitre.org/techniques/T1068/

Further information on the ***Timestomp*** technique[31] is available from MITRE.

T1070 – Indicator Removal on Host

Clear Windows event logs

The ACSC has identified the clearing of Windows event logs in an attempt to hide evidence of malicious activity. To detect Windows event log clearing, network owners should monitor for:

- The creation of Windows Security Log Event ID 1102 which is created whenever the Windows Security Log is cleared.
- Any suspicious gaps between events based on time difference, or event record number value.

Deleting web server web request logs

The ACSC has identified the deletion of web server request log files, typically when the web server also hosted a web shell. Network owners should review web server logging locations to ensure the log files present are consistent with defined logging settings and retention period.

Further information on the ***Indicator Removal on Host*** technique[32] is available from MITRE.

T1107 – File Deletion

The ACSC has identified the deletion of files created during attacks in an attempt to hide evidence of the compromise occurring. This can include deleting temporary files produced by malicious tools.

Further information on the ***File Deletion*** technique[33] is available from MITRE.

T1045 – Software Packing

The ACSC has identified the use of software packing to change the signature of malicious files in order to avoid signature based detection. Network owners should not solely rely on file signatures as a means of detecting malicious activity and should ensure other methods such as heuristic analysis are utilised to increase chances of malware detection.

Further information on the ***Software Packing*** technique[34] is available from MITRE.

T1158 – Hidden Files and Directories

The ACSC has identified the use of hidden file and directory attributes as a defence evasion technique during investigations. Network owners should be aware of potentially hidden files and folders when searching for malicious files during investigations and ensure the `display all files` command line argument is used for both built-in Windows and Linux tools and where available in third party tools.

Further information on the ***Hidden Files and Directories*** technique[35] is available from MITRE.

[31] https://attack.mitre.org/techniques/T1068/
[32] https://attack.mitre.org/techniques/T1070/
[33] https://attack.mitre.org/techniques/T1107/
[34] https://attack.mitre.org/techniques/T1107/
[35] https://attack.mitre.org/techniques/T1107/

Credential access

The following section covers TTPs relating to gaining access to user credentials identified during ACSC investigations.

T1003 – Credential Dumping

The ACSC has identified the use of the Mimikatz tool to obtain user credentials on compromised machines. The information obtained from this tool can enable unauthorised access to user accounts and the ability to access accounts with higher privileges.

Further information on the detection and mitigation of Mimikatz[36] is available from MITRE.

Further information on the ***Credential Dumping*** technique[37] is available from MITRE.

T1056 – Input Capture

The ACSC has identified the use of a key logger to obtain user credentials and other sensitive information. The information obtained can be used by an actor to gain further unauthorised access to user accounts on a network, access higher privileged accounts or access personal accounts (for example, if a user logs into private email or social media using a compromised machine). The key logger identified during ACSC investigations logged the output of captured keystrokes to a file named *log.log* in the following directories:

- *C:\ProgramData\*
- *C:\ProgramData\tmp*

The key logger identified during ACSC investigation also utilised the *SetWindowsHookEx* Windows API method to install a procedure for keyboard input capture.

Further information on the ***Input Capture*** technique[38] is available at MITRE.

T1081 – Credentials in Files

The ACSC has identified the accessing of configuration files on compromised hosts, as well as remote Server Message Block (SMB) admin shares, in order to harvest potentially hardcoded credentials and gain information relating to network configuration. The information gained from these files can be used to gain unauthorised access to other restricted parts of the network, or access to an account with higher privileges. Network owners should review all web application configuration files to ensure that credentials are not hardcoded.

In addition, network owners should analyse network logs for the following activity relating to remote SMB admin shares:

- *\\C$\Windows\system32\inetsrv\config\applicationHost.config*
- *\\C$\Program Files\Microsoft\Exchange Server\V15\ClientAccess\Autodiscover\web.config*

Further information on the ***Credentials in Files*** technique[39] is available at MITRE.

[36] https://attack.mitre.org/software/S0002/
[37] https://attack.mitre.org/techniques/T1003/
[38] https://attack.mitre.org/techniques/T1056/
[39] https://attack.mitre.org/techniques/T1081/

T1110 – Brute Force

As outlined in the initial access section of this report, the ACSC has identified brute force techniques to gain access to web application user accounts. Additionally, the ACSC has identified brute force techniques as part of the exploitation of Telerik vulnerabilities (outlined in T1190 – Exploit Public-Facing Application).

Further information on the ***Brute Force*** technique[40] is available at MITRE.

Discovery

The following section covers TTPs relating to discovery and reconnaissance identified during ACSC investigations.

Discovery techniques identified

Due to the significant overlap with many of the techniques in the Discovery tactic category, many of the Discovery techniques the ACSC identified during its investigations are aggregated below:

- T1007 – System Service Discovery
- T1016 – System Network Configuration Discovery
- T1018 – Remote System Discovery
- T1033 – System Owner/User Discovery
- T1046 – Network Service Scanning
- T1049 – System Network Connections Discovery
- T1082 – System Information Discovery
- T1083 – File and Directory Discovery
- T1087 – Account Discovery
- T1135 – Network Share Discovery
- T1482 – Domain Trust Discovery.

The ACSC has identified the use of reconnaissance tools *PowerSploit* and *SharpHound* during investigations. Both tools provide a variety of functions relating to MITRE ATT&CK Discovery techniques.

Use of native Windows utilities

The ACSC identified the use of common native Windows utilities used for the discovery of various hosts and other resources on victim networks. Examples of these utilities are *net*, *ping* and *sc*.

Use of PowerSploit

In addition to the standard use of built-in Windows commands, the ACSC has identified use of the PowerShell tool *PowerSploit* to enumerate user accounts, network devices and network shares following initial compromise.

Further information on the functionality of *PowerSploit* is available from the *PowerSploit* GitHub repository[41].

[40] https://attack.mitre.org/techniques/T1110/

[41] https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon

Use of SharpHound

The ACSC has identified the use of the reconnaissance tool *`SharpHound`*, a C# implementation of *`BloodHound`*, to enumerate Active Directory users, objects and trust information within compromised Windows environments.

Further information on the functionality of *`SharpHound`* is available from the *`SharpHound`* GitHub repository[42].

Further information on the discovery tactics identified above is available from MITRE[43].

Lateral movement

The following section covers TTPs relating to lateral movement through networks identified during ACSC investigations.

T1021 – Remote Services

Use of Secure Shell (SSH)

The ACSC has identified the use of Secure Shell (SSH) for lateral movement across networks by abusing legitimate SSH administrative credentials, as well as the enabling of SSH on hosts where the functionality was previously disabled. SSH can allow an actor to remotely send encrypted commands to compromised hosts and also upload and download files. Network owners should identify network hosts that have a legitimate requirement for SSH to be enabled and enforce strict monitoring and access control. Unauthorised SSH activity occurring on hosts should be investigated for potential malicious activity.

Use of Remote Desktop Protocol (RDP)

The ACSC has identified the use of Remote Desktop Protocol (RDP) for lateral movement between Windows hosts by utilising stolen credentials. Network owners should ensure the use of RDP is strictly controlled and monitored on corporate networks and disabled on systems where it is not required.

Further information on the ***Remote Services*** technique[44] is available from MITRE.

T1077 – Windows Admin Shares

The ACSC has identified the use of admin SMB shares for lateral movement across networks during investigations. Using SMB shares, an actor can run remote commands or copy malicious files, such as web shells, to compromise other computers on a network. Network owners should analyse network logs for the use of admin shares and investigate potential further malicious activity. Examples of key admin shares targeted by the actor were:

- *`\\<hostname>\C$`*
- *`\\<hostname>\ADMIN$`*
- *`\\<hostname>\IPC$`*

Further information on ***Windows Admin Shares*** technique[45] is available from MITRE.

[42] https://github.com/BloodHoundAD/SharpHound
[43] https://attack.mitre.org/tactics/TA0007/
[44] https://attack.mitre.org/techniques/T1021/
[45] https://attack.mitre.org/techniques/T1021/

T1134 – Access Token Manipulation

The ACSC has identified the use of access token manipulation during investigations. Using the `LazyCat` tool, the actor was able to acquire user access tokens, and reuse these to escalate privileges in order to access devices of interest. Specifically, the actor was observed using tokens to escalate privileges during interaction with web shells.

Further information on the ***Access Token Manipulation*** technique[46] is available from MITRE.

T1080 – Tainted Shared Content

The ACSC has identified the uploading of malicious content to corporate file repositories. This was used as a mechanism for gaining access to other victim networks, by tricking users into downloading and running the malicious content on external systems. The uploaded files were named using seemingly legitimate filenames, often based on the naming conventions of surrounding files. Network owners should ensure permissions for file repositories and shares are strictly controlled and should analyse file shares and repositories for malicious content.

Further information on ***Tainted Shared Content*** technique[47] is available from MITRE.

Collection

The following section covers TTPs relating to the collection of data from compromised systems identified during ACSC investigations.

T1005 – Data from Local System

The ACSC has identified data being collected from local systems during investigations.

Further information on the ***Data from Local System*** technique[48] is available from MITRE.

T1039 – Data from Network Shared Drive

The ACSC has identified data being collected from network shares during investigations. Network owners with host-based monitoring or internal network logging in place should analyse logs for command line parameters which could indicate enumeration of network shares across the network.

Further information on the ***Data from Network Shared Drive*** technique[49] from MITRE.

T1056 – Input Capture

The ACSC has identified the use of input capture to obtain account credentials for user accounts on compromise machines. Detailed information for the Input Capture technique are outlined in the credential access section of this report.

Further information on the ***Input Capture*** technique[50] is available at MITRE.

[46] https://attack.mitre.org/techniques/T1134/
[47] https://attack.mitre.org/techniques/T1080/
[48] https://attack.mitre.org/techniques/T1005/
[49] https://attack.mitre.org/techniques/T1039/
[50] https://attack.mitre.org/techniques/T1056/

T1074 – Data Staged

The ACSC has identified the staging of data prior to exfiltration often in conjunction with the use of data compression format such as `.zip` or `.rar`. Common folder paths identified during investigations used for data staging and general actor use include:

- `C:\ProgramData\`
- `C:\ProgramData\google\`
- `C:\ProgramData\tmp\`
- `C:\ProgramData\Sun\low`
- `$Recycle.Bin`
- `[DRIVE]:\Temp`
- `[DRIVE]:\`
- `[DRIVE]:\inetpub\`
- `C:\ProgramData\.rnd`

Further information on the ***Data Staged*** technique[51] is available at MITRE.

T1114 – Email Collection

The ACSC has identified the compromise of email accounts and corporate Microsoft Exchange servers to collect sensitive information from affected organisations. Email collection has been performed via:

- The export of entire Exchange mailboxes once the actor had access to the appropriate Exchange servers.
- Accessing email accounts and their contents via Outlook Web Access using stolen credentials.

Malicious network traffic associated with OWA and Exchange is difficult to identify, if a compromise has occurred on a network, network owners should review OWA and Exchange network logs for activity from confirmed malicious or suspicious IP addresses.

Further information on the ***Email Collection*** technique[52] is available at MITRE.

T1213 – Data from Information Repositories

The ACSC has identified the use of tools with the capability to interact with affected organisation’s information repositories, particularly Structured Query Language (SQL) databases. This functionality existed as a .NET module, but also the capability to test connections to SQL databases.

Further information on the ***Data from Information Repositories*** technique[53] is available at MITRE.

Command and control

The following section covers TTPs relating to command and control (C2) techniques identified during ACSC investigations.

[51] https://attack.mitre.org/techniques/T1074/
[52] https://attack.mitre.org/techniques/T1114/
[53] https://attack.mitre.org/techniques/T1213/

T1071 – Standard Application Layer Protocol

Web shell tasking

The ACSC has identified HTTP/HTTPS web shell traffic to be the primary means of C2 for the actor. This was identified both for actor interaction with external facing hosts as well as internal hosts. The ACSC has identified the use of web shell tunnelling to remotely send commands to endpoints, by utilising a series of connected web shells on compromised hosts. Web shell tunnelling allows an actor to remotely run commands on hosts that are normally not internet facing, such as internal intranet servers.

Individual web requests to a web shell can look very similar to legitimate web requests. However there are some characteristics of web shell traffic which network owners should investigate:

- Large numbers of web requests, typically HTTP POSTs, to a single resource with little to no interaction with any other web application content or functionality.
- If cookies are implemented by a web application, the lack of a HTTP Cookie header or lack of a valid Cookie value, can indicate non-browser generated requests.
- Unusual user agents which can indicate non-browser generated requests (e.g. `python-requests/2.2.1` and `CPython/2.7.2`).

Please note that an actor can alter their web shell requests to include legitimate cookie values and user agents, or falsify web request behaviour to appear like legitimate browsing.

To detect if a web shell discovered on a network may be part of a web shell tunnel, network traffic on the compromised host should be analysed for incoming HTTP POST requests to the web shell, paired with outgoing HTTP POST requests from the web server that occur around the same time. If the incoming and outgoing web shell HTTP POST requests are from organisation controlled IP ranges, the associated hosts should be investigated further to determine if they contain web shells or other malicious content.

Outlook.com Mailbox tasking

The ACSC has identified the use of Microsoft Outlook tasks as a C2 vector for communicating with malware on a compromised host. The malware connects to an actor controlled Office 365 Outlook email account using hardcoded credentials that are contained in the binary. The malware uses the Microsoft Exchange SOAP or REST API to both retrieve tasking and upload tasking responses.

Detection of this C2 mechanism can be difficult as the network traffic associated will appear largely indistinguishable from legitimate HTTPS traffic to legitimate Outlook domains. Network owners should analyse networks for unusual processes communicating with legitimate Microsoft Outlook and Office365 domains, such as PowerShell and Microsoft Access processes.

Note: this is not indicative of a compromise or vulnerability in any Microsoft product.

Further information on the ***Standard Application Layer Protocol*** technique[54] is available from MITRE.

Exfiltration

The following section covers TTPs relating to data exfiltration identified during ACSC investigations.

[54] https://attack.mitre.org/techniques/T1071/

T1002 – Data Compressed

The ACSC has identified the use of file compression prior to exfiltration of data. The actor created archives of victim files and directories, such as `.zip` and `.rar` files, to reduce the data transfer size. Data exfiltration from networks is often difficult to detect, especially without robust network monitoring in place. Following a compromise, the presence of compressed archives containing victim data could indicate data exfiltration.

Further information on the ***Data Compressed*** technique[55] is available from MITRE.

T1022 – Data Encrypted

The ACSC has identified the use of encryption to help prevent the detection of exfiltrated data. There were two main forms of encryption identified:

- SSL/TLS based encryption was utilised by placing the data to be exfiltrated in a web server directory, on a web server that supports HTTPS, and then downloading the data using HTTP.
- Data compression tools that utilised passwords to create encrypted archives, such as `.zip` and `.rar` files.

Further information on the ***Data Encrypted*** technique[56] is available from MITRE.

T1048 – Exfiltration Over Alternative Protocol

The ACSC has identified exfiltration via different techniques to those used for C2 and staging. For example, while web shells were used to perform actions on compromised hosts, the actor would typically place files to be exfiltrated in publically accessible web server directories, and then download those files directly rather than via the web shell.

Network owners should monitor web server folders and web server traffic for the creation and retrieval of large files, particularly on web servers that do not host large individual files.

Further information on the ***Exfiltration Over Alternative Protocol*** technique[57] is available from MITRE.

T1041 – Exfiltration Over Command and Control (C2) Channel

The ACSC has identified the use of web shell C2 channels as a mechanism for exfiltrating files from networks. If a web shell has been discovered, network owners should analyse network communication logs for outgoing traffic from the web shell and calculate the total size of the traffic, a large volume of traffic (>1MB) can indicate the web shell is being used to exfiltrate data.

Further information on the ***Exfiltration Over Command and Control Channel*** technique[58] is available from MITRE.

Impact

T1486 – Data Encrypted for Impact

The ACSC has identified instances of encrypted data on systems and networks resulting in disruption to the availability of resources. An actor will attempt to render stored data inaccessible by encrypting files and withholding access to a decryption key. In cases of ransomware this is designed to extract monetary compensation in exchange for the decryption key.

[55] https://attack.mitre.org/techniques/T1002/
[56] https://attack.mitre.org/techniques/T1022/
[57] https://attack.mitre.org/techniques/T1048/
[58] https://attack.mitre.org/techniques/T1041/

The ACSC does not recommend paying a ransom as there is no guarantee that paying will restore your files, it may also make you vulnerable to further attacks. If you discover you are infected with ransomware it is recommended that you report the infection and seek assistance from a cyber security expert.

Network owners can monitor for the creation of suspicious files as well as unusual file modification activity, especially in user directories. Network owners should also consider regularly taking and testing data backups (with storage offline) that can be used to restore organisational data, minimising the impact of data encryption.

Further information on ransomware can be found at https://www.cyber.gov.au.

Further information on the ***Data Encrypted for Impact*** technique[59] is available from MITRE.

[59] https://attack.mitre.org/techniques/T1486/

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.