People’s Republic of China (PRC) Ministry of State Security APT40 Tradecraft in Action | CISA

Published: 2024-07-08 · Archived: 2026-04-05 19:07:13 UTC

This advisory, authored by the Australian Signals Directorate’s Australian Cyber Security Centre (ASD’s ACSC), the United States Cybersecurity and Infrastructure Security Agency (CISA), the United States National Security Agency (NSA), the United States Federal Bureau of Investigation (FBI), the United Kingdom National Cyber Security Centre (NCSC-UK), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NCSC-NZ), the German Federal Intelligence Service (BND) and Federal Office for the Protection of the Constitution (BfV), the Republic of Korea’s National Intelligence Service (NIS) and NIS’ National Cyber Security Center, and Japan’s National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and National Police Agency (NPA)—hereafter referred to as the “authoring agencies”—outlines a People’s Republic of China (PRC) state-sponsored cyber group and their current threat to Australian networks. The advisory draws on the authoring agencies’ shared understanding of the threat as well as ASD’s ACSC incident response investigations.

The PRC state-sponsored cyber group has previously targeted organizations in various countries, including Australia and the United States, and the techniques highlighted below are regularly used by other PRC state-sponsored actors globally. Therefore, the authoring agencies believe the group, and similar techniques remain a threat to their countries’ networks as well.

The authoring agencies assess that this group conduct malicious cyber operations for the PRC Ministry of State Security (MSS). The activity and techniques overlap with the groups tracked as Advanced Persistent Threat (APT) 40 (also known as Kryptonite Panda, GINGHAM TYPHOON, Leviathan and Bronze Mohawk in industry reporting). This group has previously been reported as being based in Haikou, Hainan Province, PRC and receiving tasking from the PRC MSS, Hainan State Security Department.[1]

The following Advisory provides a sample of significant case studies of this adversary’s techniques in action against two victim networks. The case studies are consequential for cybersecurity practitioners to identify, prevent and remediate APT40 intrusions against their own networks. The selected case studies are those where appropriate remediation has been undertaken reducing the risk of re-exploitation by this threat actor, or others. As such, the case studies are naturally older in nature, to ensure organizations were given the necessary time to remediate.

APT40 has repeatedly targeted Australian networks as well as government and private sector networks in the region, and the threat they pose to our networks is ongoing. The tradecraft described in this advisory is regularly observed against Australian networks.

Notably, APT40 possesses the capability to rapidly transform and adapt exploit proof-of-concept(s) (POCs) of new vulnerabilities and immediately utilize them against target networks possessing the infrastructure of the associated vulnerability. APT40 regularly conducts reconnaissance against networks of interest, including networks in the authoring agencies’ countries, looking for opportunities to compromise its targets. This regular

reconnaissance postures the group to identify vulnerable, end-of-life or no longer maintained devices on networks of interest, and to rapidly deploy exploits. APT40 continues to find success exploiting vulnerabilities from as early as 2017.

APT40 rapidly exploits newly public vulnerabilities in widely used software such as Log4J (CVE-2021-44228), Atlassian Confluence (CVE-2021-31207, CVE-2021-26084) and Microsoft Exchange (CVE-2021-31207, CVE-2021-34523, CVE-2021-34473). ASD's ACSC and the authoring agencies expect the group to continue using POCs for new high-profile vulnerabilities within hours or days of public release.

This group appears to prefer exploiting vulnerable, public-facing infrastructure over techniques that require user interaction, such as phishing campaigns, and places a high priority on obtaining valid credentials to enable a range of follow-on activities. APT40 regularly uses web shells [T1505.003] for persistence, particularly early in the life cycle of an intrusion. Typically, after successful initial access APT40 focuses on establishing persistence to maintain access on the victim's environment. However, as persistence occurs early in an intrusion, it is more likely to be observed in all intrusions—regardless of the extent of compromise or further actions taken.

Although APT40 has previously used compromised Australian websites as command and control (C2) hosts for its operations, the group have evolved this technique [T1594].

APT40 has embraced the global trend of using compromised devices, including small-office/home-office (SOHO) devices, as operational infrastructure and last-hop redirectors [T1584.008] for its operations in Australia. This has enabled the authoring agencies to better characterize and track this group's movements.

Many of these SOHO devices are end-of-life or unpatched and offer a soft target for N-day exploitation. Once compromised, SOHO devices offer a launching point for attacks that is designed to blend in with legitimate traffic and challenge network defenders [T1001.003].

APT40 does occasionally use procured or leased infrastructure as victim-facing C2 infrastructure in its operations; however, this tradecraft appears to be in relative decline.

ASD's ACSC are sharing some of the malicious files identified during the investigations outlined below. These files have been uploaded to VirusTotal to enable the wider network defense and cyber security communities to better understand the threats they need to defend against.

ASD's ACSC are sharing two anonymized investigative reports to provide awareness of how the actors employ their tools and tradecraft.

Executive Summary

This report details the findings of the ASD's ACSC investigation into the successful compromise of the organization's network between July and September 2022. This investigative report was provided to the organization to summarize observed malicious activity and frame remediation recommendations. The findings indicate the compromise was undertaken by APT40.

In mid-August, the ASD's ACSC notified the organization of malicious interactions with their network from a likely compromised device being used by the group in late August and, with the organization's consent, the ASD's

ACSC deployed host-based sensors to likely affected hosts on the organization's network. These sensors allowed ASD's ACSC incident response analysts to undertake a thorough digital forensics investigation. Using available sensor data, the ASD's ACSC analysts successfully mapped the group's activity and created a detailed timeline of observed events.

From July to August, key actor activity observed by the ASD's ACSC included:

- Host enumeration, which enables an actor to build their own map of the network;
- Web shell use, giving the actor an initial foothold on the network and a capability to execute commands; and
- Deployment of other tooling leveraged by the actor for malicious purposes.

The investigation uncovered evidence of large amounts of sensitive data being accessed and evidence that the actors moved laterally through the network [T1021.002]. Much of the compromise was facilitated by the group's establishment of multiple access vectors into the network, the network having a flat structure, and the use of insecure internally developed software that could be used to arbitrarily upload files. Exfiltrated data included privileged authentication credentials that enabled the group to log in, as well as network information that would allow the actors to regain unauthorized access if the original access vector was blocked. No additional malicious tooling was discovered beyond those on the initially exploited machine; however, a group's access to legitimate and privileged credentials would negate the need for additional tooling. Findings from the investigation indicate the organization was likely deliberately targeted by APT40, as opposed to falling victim opportunistically to a publicly known vulnerability.

Investigation Findings

In mid-August 2022, the ASD's ACSC notified the organization that a confirmed malicious IP believed to be affiliated with a state-sponsored cyber group had interacted with the organization's computer networks between at least July and August. The compromised device probably belonged to a small business or home user.

In late August, the ASD's ACSC deployed a host-based agent to hosts on the organization's network which showed evidence of having been impacted by the compromise.

Some artefacts which could have supported investigation efforts were not available due to the configuration of logging or network design. Despite this, the organization's readiness to provide all available data enabled ASD's ACSC incident responders to conduct comprehensive analysis and to form an understanding of likely APT40 activity on the network.

In September, after consultation with the ASD's ACSC, the organization decided to denylist the IP identified in the initial notification. In October, the organization commenced remediation.

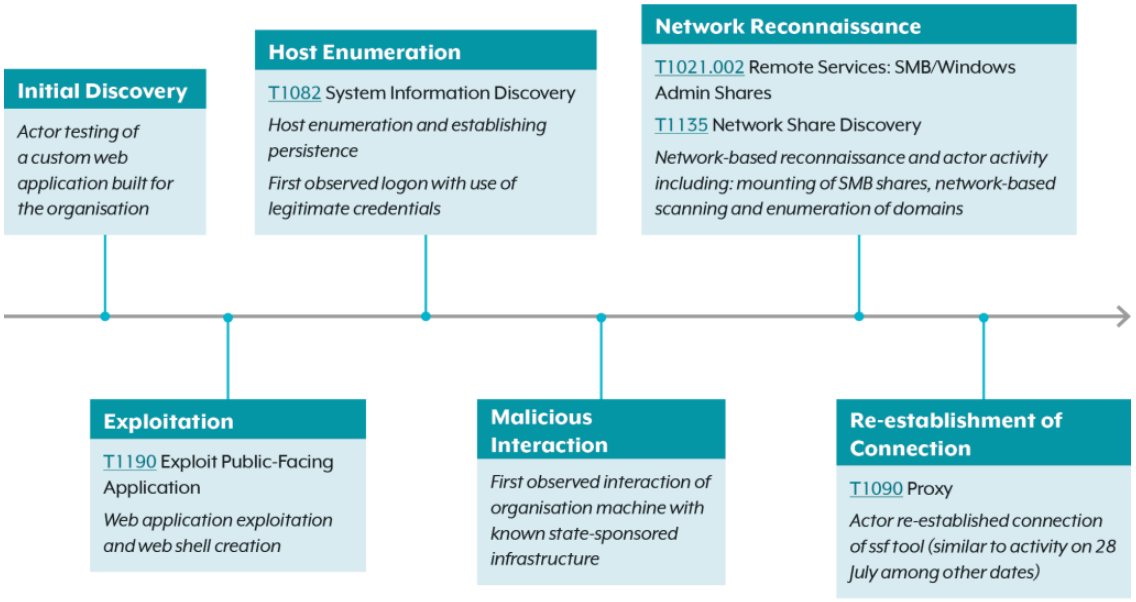
Details

Beginning in July, actors were able to test and exploit a custom web application [T1190] running on `<webapp>2-ext`, which enables the group to establish a foothold in the network demilitarized zone (DMZ). This was leveraged to enumerate both the network as well as all visible domains. Compromised credentials [T1078.002

] were used to query the Active Directory [T1018] and exfiltrate data by mounting file shares [T1039] from multiple machines within the DMZ. The actor carried out a Kerberoasting attack in order to obtain valid network credentials from a server [T1558.003]. The group were not observed gaining any additional points of presence in either the DMZ or the internal network.

Visual Timeline

The below timeline provides a broad overview of the key phases of malicious actor activity observed on the organization's network.



Detailed Timeline

July: The actors established an initial connection to the front page of a custom web application [T1190] built for the organization (hereafter referred to as the "web application" or "`webapp`") via a transport layer security (TLS) connection [T1102]. No other noteworthy activity was observed.

July: The actors begin enumerating the web application's website looking for endpoints[2] to further investigate.

July: The actors concentrate on attempts to exploit a specific endpoint.

July: The actors are able to successfully POST to the web server, probably via a web shell placed on another page. A second IP, likely employed by the same actors, also begins posting to the same URL. The actors created and tested a number of likely web shells.

The exact method of exploitation is unknown, but it is clear that the specific endpoint was targeted to create files on `<webapp>2-ext`.

ASD's ACSC believes that the two IP address connections were part of the same intrusion due to their shared interest and initial connections occurring minutes apart.

July: The group continue to conduct host enumeration, looking for privilege escalation opportunities, and deploying a different web shell. The actors log into the web application using compromised credentials for `<firstname.surname>@<organisation domain>`.

The actors' activity does not appear to have successfully achieved privilege escalation on `<webapp>2-ext`. Instead, the actors pivoted to network-based activity.

July: The actor tests the compromised credentials for a service account[3] which it likely found hardcoded in internally accessible binaries.

July: The actors deploy the open-source tool Secure Socket Funnelling, which was used to connect out to the malicious infrastructure. This connection is employed to tunnel traffic from the actor's attack machines into the organization's internal networks, whose machine names are exposed in event logs as they attempt to use the credentials for the service account.

August: The actors are seen conducting a limited amount of activity, including failing to establish connections involving the service account.

August: The actors perform significant network and Active Directory enumeration. A different compromised account is subsequently employed to mount shares[4] on Windows machines within the DMZ, enabling successful data exfiltration.

This seems to be opportunistic usage of a stolen credential on mountable machines in the DMZ. Firewalls blocked the actor from targeting the internal network with similar activity.

August – September: The SSF tool re-established a connection to a malicious IP. The group are not observed performing any additional activities until their access is blocked.

September: The organization blocks the malicious IP by denylisting it on their firewalls.

Actor Tactics and Techniques

The MITRE ATT&CK framework is a documented collection of tactics and techniques employed by threat actors in cyberspace. The framework was created by U.S. not-for-profit The MITRE Corporation and functions as a common global language around threat actor behavior.

The ASD's ACSC assesses the following techniques and tactics to be relevant to the actor's malicious activity:

Reconnaissance

T1594 – Search Victim-Owned Websites

The actor enumerated the custom web application's website to identify opportunities for accessing the network.

Initial Access

T1190 – Exploit Public-Facing Application (regarding exploiting the custom web application)

T1078.002 – Valid Accounts: Domain Accounts (regarding logging on with comprised credentials)

Exploiting internet-exposed custom web applications provided an initial point of access for the actor. The actor was later able to use credentials they had compromised to further their access to the network.

Execution

T1059 – Command and Scripting Interpreter (regarding command execution through the web shell)

T1072 – Software Deployment Tools (regarding the actor using open-source tool Secure Socket Funnelling (SSF) to connect to an IP)

Persistence

T1505.003 – Server Software Component: Web Shell (regarding use of a web shell and SSF to establish access)

Credential Access

T1552.001 – Credentials from Password Stores (regarding password files relating to building management system [BMS])

T1558.003 – Steal or Forge Kerberos Tickets: Kerberoasting (regarding attack to gain network credentials)

Lateral movement

T1021.002 – Remote Services: SMB Shares (regarding the actor mounting SMB shares from multiple devices)

Collection

T1213 – Data from Information Repositories (regarding manuals/documentation found on the BMS server)

Exfiltration

T1041 – Exfiltration Over C2 Channel (regarding the actor's data exfiltration from Active Directory and mounting shares)

Case Study 2

This report has been anonymized to enable wider dissemination. The impacted organization is hereafter referred to as "the organization." Some specific details have been removed to protect the identity of the victim and incident response methods of ASD's ACSC.

Executive Summary

This report details the findings of ASD's ACSC investigation into the successful compromise of the organization's network in April 2022. This investigation report was provided to the organization to summarize observed malicious activity and frame remediation recommendations. The findings indicate the compromise was undertaken by APT40.

In May 2022, ASD’s ACSC notified an organization of suspected malicious activity impacting the organization’s network since April 2022. Subsequently, the organization informed ASD's ACSC that they had discovered malicious software on an internet-facing server which provided the login portal for the organization’s corporate remote access solution. This server used a remote access login and identity management product and will be referred to in this report as 'the compromised appliance'. This report details the investigation findings and remediation advice developed for the organization in response to the investigation conducted by the ASD’s ACSC.

Evidence indicated that part of the organization’s network had been compromised by malicious cyber actor(s) via the organization’s remote access login portal since at least April 2022. This server may have been compromised by multiple actors, and was likely affected by a remote code execution (RCE) vulnerability that was widely publicized around the time of the compromise.

Key actor activity observed by the ASD’s ACSC included:

- Host enumeration, which enables an actor to build their own map of the network;
- Exploitation of internet-facing applications and web shell use, giving the actor an initial foothold on the network and a capability to execute commands;
- Exploitation of software vulnerabilities to escalate privileges; and
- Credential collection to enable lateral movement.

The ASD’s ACSC discovered that a malicious actor had exfiltrated several hundred unique username and password pairs on the compromised appliance in April 2022, as well as a number of multi-factor authentication codes and technical artefacts related to remote access sessions. Upon a review by the organization, the passwords were found to be legitimate. The ASD’s ACSC assesses that the actor may have collected these technical artefacts to hijack or create a remote login session as a legitimate user, and access the organization’s internal corporate network using a legitimate user account.

Investigation Summary

The ASD’s ACSC determined that the actor compromised appliance(s) which provide remote login sessions for organization staff and used this compromise to attempt to conduct further activity. These appliances consist of three load-balanced hosts where the earliest evidence of compromise was detected. The organization shut down two of the three load-balanced hosts shortly after the initial compromise. As a result, all subsequent activity occurred on a single host. The other servers associated with the compromised appliance were also load-balanced in a similar manner. For legibility, all compromised appliances are referred to in most of this report as a “single appliance.”

The actor is believed to have used publicly known vulnerabilities to deploy web shells to the compromised appliance from April 2022 onwards. Threat actors from the group are assessed to have attained escalated privileges on the appliance. The ASD’s ACSC could not determine the full extent of the activity due to lack of logging availability. However, evidence on the device indicates that an actor achieved the following:

- The collection of several hundred genuine username and password pairs; and
- The collection of technical artefacts which may have allowed a malicious actor to access a virtual desktop infrastructure (VDI) session as a legitimate user.

The ASD's ACSC assesses that the actor would have sought to further the compromise of the organisation network. The artefacts exfiltrated by the actor may have allowed them to hijack or initiate virtual desktop sessions as a legitimate user, possibly as a user of their choice, including administrators. The actor may have used this access vector to further compromise organization services to achieve persistence and other goals.

Other organization appliances within the hosting provider managed environment did not show evidence of compromise.

Access

The host with the compromised appliance provided authentication via Active Directory and a webserver, for users connecting to VDI sessions [T1021.001].

Location	Compromised appliance hostnames (load-balanced)
Datacentre 1	HOST1, HOST2, HOST3

The appliance infrastructure also included access gateway hosts that provide a tunnel to the VDI for the user, once they possess an authentication token generated and downloaded from the appliance.

There was no evidence of compromise of any of these hosts. However, the access gateway hosts logs showed evidence of significant interactions with known malicious IP addresses. It is likely that this reflected activity that occurred on this host, or network connections with threat actor infrastructure that reached this host. The nature of this activity could not be determined using available evidence but indicates that the group sought to move laterally in the organization's network [TA0008].

Internal Hosts

The ASD's ACSC investigated limited data from the internal organization's network segment. Attempted or successful malicious activity known to have impacted the internal organization's network segment includes actor access to VDI-related artefacts, the scraping of an internal SQL server [T1505.001], and unexplained traffic observed going from known malicious IP addresses through the access gateway appliances [TA0011].

Using their access to the compromised appliance, the group collected genuine usernames, passwords [T1003], and MFA token values [T1111]. The group also collected JSON Web Tokens (JWTs) [T1528], which is an authentication artefact used to create virtual desktop login sessions. The actor may have been able to use these to create or hijack virtual desktop sessions [T1563.002] and access the internal organization network segment as a legitimate user [T1078].

The actor also used access to the compromised appliance to scrape an SQL server [T1505.001], which resided in the organization's internal network. It is likely that the actor had access to this data.

Evidence available from the access gateway appliance revealed that network traffic occurred through or to this device from known malicious IP addresses. As described above, this may indicate that malicious cyber actors impacted or utilized this device, potentially to pivot into the internal network.

Investigation Timeline

The below list provides a timeline of key activities discovered during the investigation.

Time	Event
April 2022	Known malicious IP addresses interact with access gateway host HOST7. The nature of the interactions could not be determined.
April 2022	All hosts, HOST1, HOST2 and HOST3, were compromised by a malicious actor or actors, and web shells were placed on the hosts. A log file was created or modified on HOST2. This file contains credential material likely captured by a malicious actor. The /etc/security/opasswd and /etc/shadow files were modified on HOST1 and HOST3, indicating that passwords were changed. Evidence available on HOST1 suggests that the password for user ‘sshuser’ was changed.
April 2022	HOST2 was shut down by the organization. Additional web shells (T1505.003) were created on HOST1 and HOST3. HOST1experienced SSH brute force attempts from HOST3. A log file was modified (T1070) on HOST3. This file contains credential material (T1078) likely captured by a malicious actor. JWTs were captured (T1528) and output to a file on HOST3. HOST3 was shut down by the organization. All activity after this time occurs on HOST1.
April 2022	Additional web shells were created on HOST1 (T1505.003). JWTs were captured and output to a file on HOST1.
April 2022	Additional web shells are created on HOST1 (T1505.003), and a known malicious IP address interacts with the host (TA0011). A known malicious IP address interacts with access gateway host HOST7.

Time	Event
May 2022	A known malicious IP address interacted with access gateway host HOST7 (TA0011). An authentication event for a user is linked to a known malicious IP address in logs on HOST1. An additional web shell is created on this host (T1505.003).
May 2022	A script on HOST1 was modified by an actor (T1543). This script contains functionality which would have scraped data from an internal SQL server.
May 2022	An additional log file on HOST1 was last modified (T1070). This file contains username and password pairs for the organization network, which are believed to be legitimate (T1078).
May 2022	An additional log file was last modified (T1070). This file contains JWTs collected from HOST1.
May 2022	Additional web shells were created on HOST1 (T1505.003). On this date, the organization reported the discovery of a web shell with creation date in April 2022 to ASD's ACSC
May 2022	A number of scripts were created on HOST1, including one named Log4jHotPatch.jar.
May 2022	The iptables-save command was used to add two open ports to the access gateway host. The ports were 9998 and 9999 (T1572).

Actor Tactics and Techniques

Highlighted below are several tactics and techniques identified during the investigation.

Initial access

T1190 Exploit public facing application

The group likely exploited RCE, privilege escalation,
and authentication bypass vulnerabilities in the remote access login and identity management product to gain initial access to the network.

This initial access method is considered the most likely due to the following:

- The server was vulnerable to these CVEs at the time;
- Attempts to exploit these vulnerabilities from known actor infrastructure; and
- The first known internal malicious activity occurred shortly after attempted exploitation attempts were made.

Execution

T1059.004 Command and Scripting Interpreter: Unix Shell

The group successfully exploited the above vulnerabilities may have been able to run commands in a Unix shell available on the affected appliance.

Complete details of the commands run by actors cannot be provided as they were not logged by the appliance.

Persistence

T1505.003 Server Software Component: Web Shell

Actors deployed several web shells on the affected appliance. It is possible that multiple distinct actors deployed web shells, but that only a smaller number of actors conducted activity using these web shells.

Web shells would have allowed for arbitrary command execution by the actor on the compromised appliances.

Privilege escalation

T1068 Exploitation for Privilege Escalation

Available evidence does not describe the level of privilege attained by actors. However, using web shells, the actors would have achieved a level of privilege comparable to that of the web server on the compromised appliance. Vulnerabilities believed to have been present on the compromised appliance

would have allowed the actors to attain root privileges.

Credential access

T1056.003 Input Capture: Web Portal Capture

Evidence on the compromised appliance showed that the actor had captured several hundred username-password pairs, in clear text, which are
believed to be legitimate. It is likely that these were captured using some modification to the genuine authentication process which output the credentials to a file.

T1111 Multi-Factor Authentication Interception The actor also captured the value of MFA tokens

corresponding to legitimate logins. These were likely captured by modifying the genuine authentication process to output these values to a file. There is no evidence of compromise of the “secret server’ which
stores the unique values that provide for the security of MFA tokens.

T1040 Network Sniffing

The actor is believed to have captured JWTs by capturing HTTP traffic on the compromised appliance.
There is evidence that the utility tcpdump was executed on the compromised appliance, which may have been how the actor captured these JWTs.

T1539 Steal Web Session Cookie

As described above, the actor captured JWTs, which are analogous to web session cookies. These could have been reused by the actor to establish further access.

Discovery

T1046 Network Service Discovery

There is evidence that network scanning utility nmap was executed on the compromised appliance to scan other appliances in the same network segment. This was likely used by the actor to discover other reachable network services which might present opportunities for lateral movement.

Collection

Available evidence does not reveal how actors collected data or exactly what was collected from the compromised appliance or from other systems. However, it is likely that actors had access to all files on the compromised appliance, including the captured credentials [T1003], MFA token values [T1111], and JWTs described above.

Command and Control

T1071.001 Application Layer Protocol: Web Protocols

Actors used web shells for command and control. Web shell commands would have been passed over HTTPS using the existing web server on the appliance [T1572].

T1001.003 Data Obfuscation: Protocol Impersonation

Actors used compromised devices as a launching point for attacks that are designed to blend in with legitimate traffic.

Detection and mitigation recommendations

The ASD's ACSC strongly recommends implementing the ASD Essential Eight Controls and associated Strategies to Mitigate Cyber Security Incidents . Below are recommendations for network security actions that should be taken to detect and prevent intrusions by APT40, followed by specific mitigations for four key TTPs summarized in Table 1.

Detection

Some of the files identified above were dropped in locations such as C:\Users\Public* and C:\Windows\Temp*. These locations can be convenient spots for writing data as they are usually world writable, that is, all user accounts registered in Windows have access to these directories and their subdirectories. Often, any user can subsequently access these files, allowing opportunities for lateral movement, defense evasion, low-privilege execution and staging for exfiltration.

The following Sigma rules look for execution from suspicious locations as an indicator of anomalous activity. In all instances, subsequent investigation is required to confirm malicious activity and attribution.

Title: World Writable Execution - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Description: Detect process execution from C:\ Windows\Temp.

Background: This rule looks specifically for execution out of C:\ Windows\Temp*. Temp is more broadly used by benign applications and thus a lower confidence malicious indicator than execution out of other world writable subdirectories in C:\Windows.

Removing applications executed by the SYSTEM or NETWORK SERVICE users substantially reduces the quantity of benign activity selected by this rule.

This means that the rule may miss malicious executions at a higher privilege level but it is recommended to use other rules to determine if a user is attempting to elevate privileges to SYSTEM.

Investigation:

1. Examine information directly associated with this file execution, such as the user context, execution integrity level, immediate follow-on activity and images loaded by the file.
2. Investigate contextual process, network, file and other supporting data on the host to help make an assessment as to whether the activity is malicious.
3. If necessary attempt to collect a copy of the file for reverse engineering to determine whether it is legitimate.

References:

Process Execution from an Unusual Directory

Author: ASD’s ACSC

Date: 2024/06/19

Status: experimental

Tags:

- tlp.green
- classification.au.official
- attack.execution

Log Source:

category: process_creation
product: windows

Detection:

temp:
Image|startswith: 'C:\\Windows\\Temp\\'

common_temp_path:
Image|re|ignorecase: 'C:\\Windows\\Temp\\\{[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]{12}\}\\'

system_user:
User:

- 'SYSTEM'
- 'NETWORK SERVICE'

dismhost:

- Image|endswith: 'dismhost.exe'

known_parent:

- ParentImage|endswith:
- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

condition: temp and not (common_temp_path or system_user or dismhost or known_parent)

False positives:

- Allowlist auditing applications have been observed running executables from Temp.
- Temp will legitimately contain an array of setup applications and launchers, so it will be worth considering how prevalent this behavior is on a monitored network (and whether or not it can be allowlisted) before deploying this rule.

Level: low

Title: World Writable Execution - Non-Temp System Subdirectory

ID: 5b187157-e892-4fc9-84fc-aa48aff9f997

Description: Detect process execution from a world writable location in a subdirectory of the Windows OS install location.

Background:

This rule looks specifically for execution out of world writable directories within C:\ and particularly C:\Windows*, with the exception of C:\Windows\Temp (which is more broadly used by benign applications and thus a lower confidence malicious indicator).

AppData folders are excluded if a file is run as SYSTEM - this is a benign way in which many temporary application files are executed.

After completing an initial network baseline and identifying known benign executions from these locations, this rule should rarely fire.

Investigation:

1. Examine information directly associated with this file execution, such as the user context, execution integrity level, immediate follow-on activity and images loaded by the file.
2. Investigate contextual process, network, file and other supporting data on the host to help make an assessment as to whether the activity is malicious.
3. If necessary attempt to collect a copy of the file for reverse engineering to determine whether it is legitimate.

References:

mattifestation / WorldWritableDirs.txt
Process Execution from an Unusual Directory

Author: ASD's ACSC

Date: 2024/06/19

Status: experimental

Tags:

- tlp.green
- classification.au.official
- attack.execution

Log source:

category: process_creation
product: windows

Detection:

writable_path:
Image|contains:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'

- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'
- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'

- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:
Image|contains: '\\AppData\\'
User: 'SYSTEM'
condition: writable_path and not appdata

False positives:

Allowlist auditing applications have been observed running executables from these directories.

It is plausible that scripts and administrative tools used in the monitored environment(s) may be located in one of these directories and should be addressed on a case-by-case basis.

Level: high

Title: World Writable Execution - Users

ID: 6dda3843-182a-4214-9263-925a80b4c634

Description: Detect process execution from C:\Users\Public* and other world writable folders within Users.

Background:

AppData folders are excluded if a file is run as SYSTEM - this is a benign way in which many temporary application files are executed.

Investigation:

1. Examine information directly associated with this file execution, such as the user context, execution integrity level, immediate follow-on activity and images loaded by the file.
2. Investigate contextual process, network, file and other supporting data on the host to help make an assessment as to whether the activity is malicious.
3. If necessary attempt to collect a copy of the file for reverse engineering to determine whether it is legitimate.

References:

Process Execution from an Unusual Directory

Author: ASD’s ACSC

Date: 2024/06/19

Status: experimental

Tags:

- tlp.green
- classification.au.official
- attack.execution

Log source:

category: process_creation
product: windows

Detection:
users:
Image|contains:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata:
Image|contains: '\\AppData\\'
User: 'SYSTEM'
condition: users and not appdata

False positives:

It is plausible that scripts and administrative tools used in the monitored environment(s) may be located in Public or a subdirectory and should be addressed on a case-by-case basis.

Level: medium

Mitigations

Logging

During ASD's ACSC investigations, a common issue that reduces the effectiveness and speed of investigative efforts is a lack of comprehensive and historical logging information across a number of areas including web server request logs, Windows event logs and internet proxy logs.

ASD's ACSC recommends reviewing and implementing their guidance on Windows Event Logging and Forwarding including the configuration files and scripts in the Windows Event Logging Repository and the Information Security Manual's Guidelines for System Monitoring, to include centralizing logs and retaining logs for a suitable period.

Patch Management

Promptly patch all internet exposed devices and services, including web servers, web applications, and remote access gateways. Consider implementing a centralized patch management system to automate and expedite the process. ASD's ACSC recommend implementation of the ISM's Guidelines for System Management, specifically, the System Patching controls where applicable.

Most exploits utilized by the actor were publicly known and had patches or mitigations available.

Organizations should ensure that security patches or mitigations are applied to internet facing infrastructure within 48 hours, and where possible, use the latest versions of software and operating systems.

Network Segmentation

Network segmentation can make it significantly more difficult for adversaries to locate and gain access to an organizations sensitive data. Segment networks to limit or block lateral movement by denying traffic between computers unless required. Important servers such as Active Directory and other authentication servers should only be able to be administered from a limited number of intermediary servers or "jump servers." These servers should be closely monitored, be well secured and limit which users and devices are able to connect to them.

Regardless of instances identified where lateral movement is prevented, additional network segmentation could have further limited the amount of data the actors were able to access and extract.

Additional Mitigations

The authoring agencies also recommend the following mitigations to combat APT40 and others' use of the TTPs below.

- Disable unused or unnecessary network services, ports and protocols.
- Use well-tuned Web application firewalls (WAFs) to protect webservers and applications.
- Enforce least privilege to limit access to servers, file shares, and other resources.
- Use multi-factor authentication (MFA) and managed service accounts to make credentials harder to crack and reuse. MFA should be applied to all internet accessible remote access services, including:
  - Web and cloud-based email;
  - Collaboration platforms;
  - Virtual private network connections; and
  - Remote desktop services.
- Replace end-of-life equipment.

Mitigation Strategies/Techniques

TTP	Essential Eight Mitigation Strategies	ISM Controls
Initial Access T1190 Exploitation of Public-Facing Application	• Patch applications • Patch operating systems • Multi-factor authentication • Application control	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Execution T1059 Command and Scripting Interpreter	• Application control • Restrict Microsoft Office macros • Restrict administrative privileges	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657

TTP	Essential Eight Mitigation Strategies	ISM Controls
		ISM-1890
Persistence T1505.003 Server Software Component: Web Shell	• Application Control • Restrict administrative privileges	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Initial Access / Privilege Escalation / Persistence T1078 Valid Accounts	• Patch operating systems • Multi-factor authentication • Restrict administrative privileges • Application control • User application hardening	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

For additional general detection and mitigation advice, please consult the Mitigations and Detection sections on the MITRE ATT&CK technique web page for each of the techniques identified in the MITRE ATT&CK summary at the end of this advisory.

Reporting

Australian organizations: visit cyber.gov.au or call 1300 292 371 (1300 CYBER 1) to report cybersecurity incidents and to access alerts and advisories.

Canadian organizations: report incidents by emailing CCCS at contact@cyber.gc.ca.

New Zealand organizations: report cyber security incidents to incidents@ncsc.govt.nz or call 04 498 7654.

United Kingdom organizations: report a significant cyber security incident at National Cyber Security Centre (monitored 24 hours) or, for urgent assistance, call 03000 200 973.

U.S. organizations: report incidents and anomalous activity to CISA 24/7 Operations Center at report@cisa.gov ✉ or (888) 282-0870 and/or to the FBI via your local FBI field office, the FBI's 24/7 CyWatch at (855) 292-3937, or CyWatch@fbi.gov✉. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by the authoring agencies.

MITRE ATT&CK – Historical APT40 Tradecraft of Interest

Reconnaissance (TA0043)	
Search Victim-Owned Websites [T1594]	Gather Victim Identity Information: Credentials [T1589.001]
Active Scanning: Vulnerability Scanning [T1595.002]	Gather Victim Host Information [T1592]
Search Open Websites/Domains: Search Engines [T1593.002]	Gather Victim Network Information: Domain Properties [T1590.001]
Gather Victim Identity Information: Email Addresses [T1589.002]	

Resource Development (TA0042)	
Acquire Infrastructure: Domains [T1583.001]	Acquire Infrastructure [T1583]
Acquire Infrastructure: DNS Server [T1583.002]	Compromise Accounts [T1586]
Develop Capabilities: Code Signing Certificates [T1587.002]	Compromise Infrastructure [T1584]
Develop Capabilities: Digital Certificates [T1587.003]	Develop Capabilities: Malware [T1587.001]
Obtain Capabilities: Code Signing Certificates [T1588.003]	Establish Accounts: Cloud Accounts [T1585.003]
Compromise Infrastructure: Network Devices [T1584.008]	Obtain Capabilities: Digital Certificates [T1588.004]

Initial Access (TA0001)	
Valid Accounts [T1078]	Phishing [T1566]
Valid Accounts: Default Accounts [T1078.001]	Phishing: Spearphishing Attachment [T1566.001]
Valid Accounts: Domain Accounts [T1078.002]	Phishing: Spearphishing Link [T1566.002]
External Remote Services [T1133]	Exploit Public-Facing Application [T1190]
Drive-by Compromise [T1189]	

Execution (TA0002)	
Windows Management Instrumentation [T1047]	Command and Scripting Interpreter: Python [T1059.006]
Scheduled Task/Job: At [T1053.002]	Command and Scripting Interpreter: JavaScript [T1059.007]
Scheduled Task/Job: Scheduled Task [T1053.005]	Native API [T1106]
Command and Scripting Interpreter [T1059]	Inter-Process Communication [T1559]
Command and Scripting Interpreter: Windows Command Shell [T1059.003]	System Services: Service Execution [T1569.002]
Command and Scripting Interpreter: PowerShell [T1059.001]	Exploitation for Client Execution [T1203]
Command and Scripting Interpreter: Visual Basic [T1059.005]	User Execution: Malicious File [T1204.002]
Command and Scripting Interpreter: Unix Shell [T1059.004]	Command and Scripting Interpreter: Apple Script [T1059.002]
Scheduled Task/Job: Cron [T1053.003]	Software Deployment Tools [T1072]

Persistence (TA0003)	
Valid Accounts [T1078]	Server Software Component: Web Shell [T1505.003]
Office Application Startup: Office Template Macros [T1137.001]	Create or Modify System Process: Windows Service [T1543.003]
Scheduled Task/Job: At [T1053.002]	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]
Scheduled Task/Job: Scheduled Task [T1053.005]	Boot or Logon Autostart Execution: Shortcut Modification [T1547.009]

Persistence (TA0003)	
External Remote Services [T1133]	Hijack Execution Flow: DLL Search Order Hijacking [T1574.001]
Scheduled Task/Job: Cron [T1053.003]	Hijack Execution Flow: DLL Side-Loading [T1574.002]
Account Manipulation [T1098]	Valid Accounts: Cloud Accounts [T1078.004]
Valid Accounts: Domain Accounts [T1078.002]	

Privilege Escalation (TA0004)	
Scheduled Task/Job: At [T1053.002]	Create or Modify System Process: Windows Service [T1543.003]
Scheduled Task/Job: Scheduled Task [T1053.005]	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder [T1547.001]
Process Injection: Thread Execution Hijacking [T1055.003]	Boot or Logon Autostart Execution: Shortcut Modification [T1547.009]
Process Injection: Process Hollowing [T1055.012]	Hijack Execution Flow: DLL Search Order Hijacking [T1574.001]
Valid Accounts: Domain Accounts [T1078.002]	Exploitation for Privilege Escalation [T1068]
Access Token Manipulation: Token Impersonation/Theft [T1134.001]	Event Triggered Execution: Unix Shell Configuration Modification [T1546.004]
Process Injection: Dynamic-link Library Injection [T1055.001]	Valid Accounts: Domain Accounts [T1078.002]
Valid Accounts: Local Accounts [T1078.003]	

Defense Evasion (TA0005)	
Rootkit [T1014]	Indirect Command Execution [T1202]
Obfuscated Files or Information [T1027]	System Binary Proxy Execution: Mshta [T1218.005]
Obfuscated Files or Information: Software Packing [T1027.002]	System Binary Proxy Execution: Regsvr32 [T1218.010]
Obfuscated Files or Information: Steganography [T1027.003]	Subvert Trust Controls: Code Signing [T1553.002]

Defense Evasion (TA0005)	
Obfuscated Files or Information: Compile After Delivery [T1027.004]	File and Directory Permissions Modifications: Linux and Mac File and Directory Permissions Modification [T1222.002]
Masquerading: Match Legitimate Name or Location [T1036.005]	Virtualisation/Sandbox Evasion: System Checks [T1497.001]
Process Injection: Thread Execution Hijacking [T1055.003]	Masquerading [T1036]
Reflective Code Loading [T1620]	Impair Defences: Disable or Modify System Firewall [T1562.004]
Process Injection: Process Hollowing [T1055.012]	Hide Artifacts: Hidden Files and Directories [T1564.001]
Indicator Removal: File Deletion [T1070.004]	Hide Artifacts: Hidden Window [T1564.003]
Indicator Removal: Timestomp [T1070.006]	Hijack Execution Flow: DLL Search Order Hijacking [T1574.001]
Indicator Removal: Clear Windows Event Logs [T1070.001]	Hijack Execution Flow: DLL Side-Loading [T1574.002]
Modify Registry [T1112]	Web Service [T1102]
Deobfuscate/Decode Files or Information [T1140]	Masquerading: Masquerade Task or Service [T1036.004]
Impair Defenses [T1562]	

Credential Access (TA0006)	
OS Credential Dumping: LSASS Memory [T1003.001]	Unsecured Credentials: Credentials in Files [T1552.001]
OS Credential Dumping: NTDS [T1003.003]	Brute Force: Password Guessing [T1110.001]
Network Sniffing [T1040]	Forced Authentication [T1187]
Credentials from Password Stores: Keychain [T1555.001]	Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]
Input Capture: Keylogging [T1056.001]	Multi-Factor Authentication Interception [T1111]
Steal Web Session Cookie [T1539]	Steal Application Access Token [T1528]

Credential Access (TA0006)	
Exploitation for Credential Access [T1212]	Brute Force: Password Cracking [T1110.002]
Input Capture: Web Portal Capture [T1056.003]	OS Credential Dumping: DCSync [T1003.006]
Credentials from Password Stores [T1555]	Credentials from Password Stores: Credentials from Web Browsers [T1555.003]
Discovery (TA0007)	
System Service Discovery [T1007]	System Information Discovery [T1082]
Application Window Discovery [T1010]	Account Discovery: Local Account [T1087.001]
Query Registry [T1012]	System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®
File and Directory Discovery [T1083]	System Time Discovery [T1124]
Network Service Discovery [T1046]	System Owner/User Discovery [T1033]
Remote System Discovery [T1018]	Domain Trust Discovery [T1482]
Account Discovery: Email Account [T1087.003]	Account Discovery: Domain Account [T1087.002]
System Network Connections Discovery [T1049]	Virtualisation/Sandbox Evasion: System Checks [T1497.001]
Process Discovery [T1057]	Software Discovery [T1518]
Permission Groups Discovery: Domain Groups [T1069.002]	Network Share Discovery, Technique T1135 - Enterprise | MITRE ATT&CK®
System Network Configuration Discovery: Internet Connection Discovery [T1016.001]	
Lateral Movement (TA0008)	
Remote Services: Remote Desktop Protocol [T1021.001]	Remote Services [T1021]
Remote Services: SMB/Windows Admin Shares [T1021.002]	Use Alternate Authentication Material: Pass the Ticket [T1550.003]
Remote Services: Windows Remote Management [T1021.006]	Lateral Tool Transfer [T1570]

Collection (TA0009)	
Data from Local System [T1005]	Archive Collected Data: Archive via Library [T1560.002]
Data from Network Shared Drive [T1039]	Email Collection: Remote Email Collection [T1114.002]
Input Capture: Keylogging [T1056.001]	Clipboard Data [T1115]
Automated Collection [T1119]	Data from Information Repositories [T1213]
Input Capture: Web Portal Capture [T1056.003]	Data Staged: Remote Data Staging [T1074.002]
Data Staged: Local Data Staging [T1074.001]	Archive Collected Data [T1560]
Email Collection [T1114]	

Exfiltration (TA0010)	
Exfiltration Over C2 Channel [T1041]	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol [T1048.002]
Exfiltration Over Alternative Protocol [T1048]	Exfiltration Over Web Service: Exfiltration to Cloud Storage [T1567.002]

Command and Control (TA0011)	
Data Obfuscation: Protocol Impersonation [T1001.003]	Web Service: Dead Drop Resolver [T1102.001]
Commonly Used Port [T1043]	Web Service: One-way Communication [T1102.003]
Application Layer Protocol: Web Protocols [T1071.001]	Ingress Tool Transfer [T1105]
Application Layer Protocol: File Transfer Protocols [T1071.002]	Proxy: Internal Proxy [T1090.001]
Proxy: External Proxy [T1090.002]	Non-Standard Port [T1571]
Proxy: Multi-hop Proxy [T1090.003]	Protocol Tunnelling [T1572]
Web Service: Bidirectional Communication [T1102.002]	Encrypted Channel [T1573]
Encrypted Channel: Asymmetric Cryptography [T1573.002]	Ingress Tool Transfer [T1105]
Proxy, Technique T1090 - Enterprise | MITRE ATT&CK®	

Impact (TA0040)	
Service Stop [T1489]	Disk Wipe [T1561]
System Shutdown/Reboot [T1529]	Resource Hijacking [T1496]

Notes
