RelianceCyber

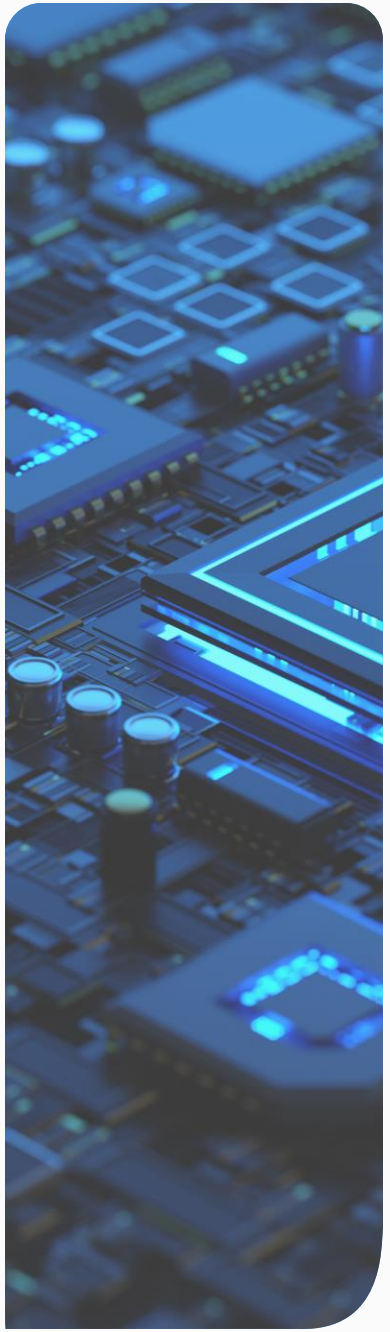
TLP: CLEAR

Threat Intelligence

ATP40 Threat Actor Profile

Written by: Adam Schweizer

Date: 2024-07-24



RelianceCyber

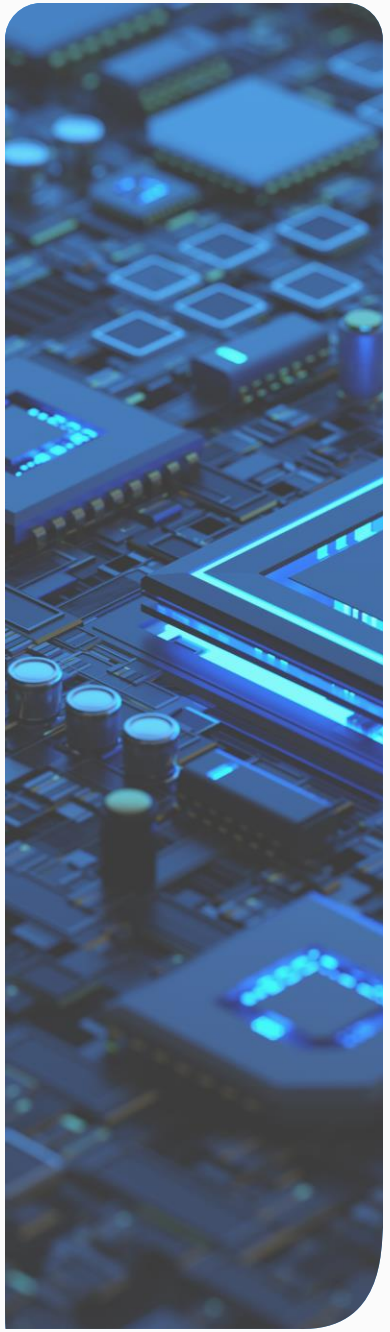
Executive Summary

The Reliance Cyber Threat Actor Profile Report aims to help businesses understand & manage the associated risks by providing the most relevant information and mitigation advisory. If you require any additional information about this report or the advice contained therein; please contact your Customer Success representative.

1. **Key Recommendations** – List of recommended mitigations to help mitigate threats associated with APT40 known activity. (Page 4)
2. **Threat Actor Profile**– The APT40 introduction, notable attacks timeline, tactics, techniques and procedures and a visualized Tactics, Techniques and Procedures (TTPs) map. (Pages 5-11)
3. **Sources & Additional Resources** – List of sources used to produce this report and additional resources that have detailed information (Page 12)

RelianceCyber

Key Recommendations



RelianceCyber

Key Recommendations

Reliance Cyber have reviewed the threat actor activity and suggest below some of the key mitigations.

APT40 Mitigations

TA.APT40.001 - Ensure centralised logging and review log retention for suitable periods.
This point is covered for XDR Customers.

TA.APT40.002 - Ensure all internet exposed hosts and services (incl. web servers, remote access gateways and web applications), where possible, are patched or mitigations are applied within 48 hours.

TA.APT40.003 - Effective network segmentation ensures that data cannot be easily located and accessed by a Threat Actor. Unless required, ensure traffic between computers is blocked to help mitigate the lateral movement techniques. Ensure that Active Directory and other important servers are only accessible via hardened 'jump servers'.

TA.APT40.004 - Disable unused network services, ports and protocols.

TA.APT40.005 - Use well-tuned Web application firewalls(WAFs) to protect web servers and applications. See examples.

TA.APT40.006 - Enforce least privilege to limit access to servers, file shares, and other resources.

TA.APT40.007 - Replace end-of-life equipment.

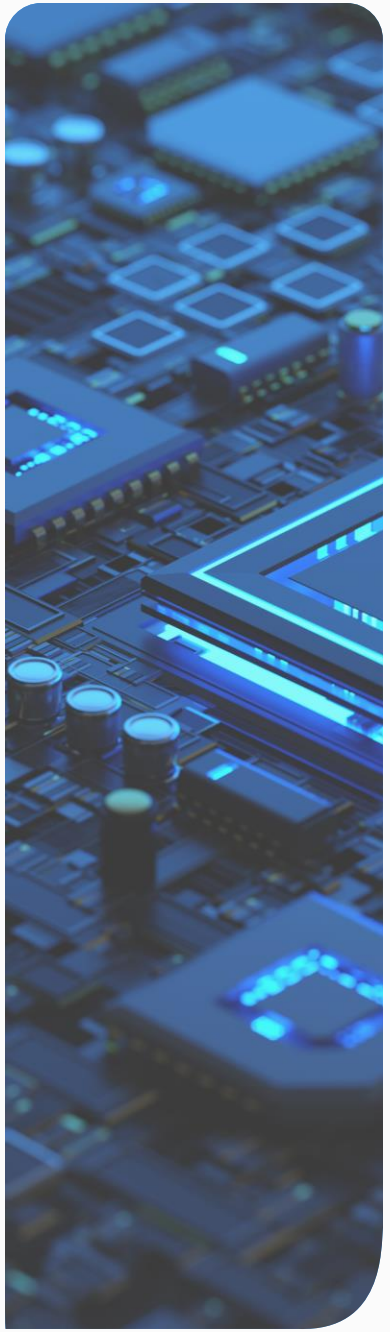
TA.APT40.008 - Implement MFA and managed service accounts. MFA should be applied to all internet accessible remote access services, including Web and cloud-based email, Collaboration platforms, Virtual private network connections and Remote desktop services.

Action: Please ensure all of the above actions are either remediated or appropriately risk managed.

RelianceCyber

Threat Intelligence

APT40 Threat Actor Profile



RelianceCyber

APT40 Threat Actor Profile – Introduction

APT40 Alternative Names

BRONZE MOHAWK, GADOLINIUM, Gingham Typhoon, Kryptonite Panda, Leviathan, Mudcarp, Red Ladon, TA423, TEMP.Periscope

About APT40

APT40 is a Chinese state-sponsored threat activity group that has reportedly been active since at least 2013. In 2020 and 2021, the group was the subject of a series of reports by the doxxing persona Intrusion Truth as well as a subsequent US Department of Justice indictment.

These sources attributed the group to a series of front companies, such as Hainan Xiandun Technology Development Co. Ltd. (海南仙盾科技开发有限公司), operating from Hainan in the People's Republic of China. The front companies were further linked to individuals working at Hainan University and the group reportedly operated under the direction of Hainan State Security Department (HSSD), a provincial-level institution of China's Ministry of State Security (MSS).

APT40 has historically targeted a wide range of industries including defense and government organizations, engineering firms, shipping and transportation, manufacturing, and research universities in the United States, Western Europe, Australia, and the South China Sea.

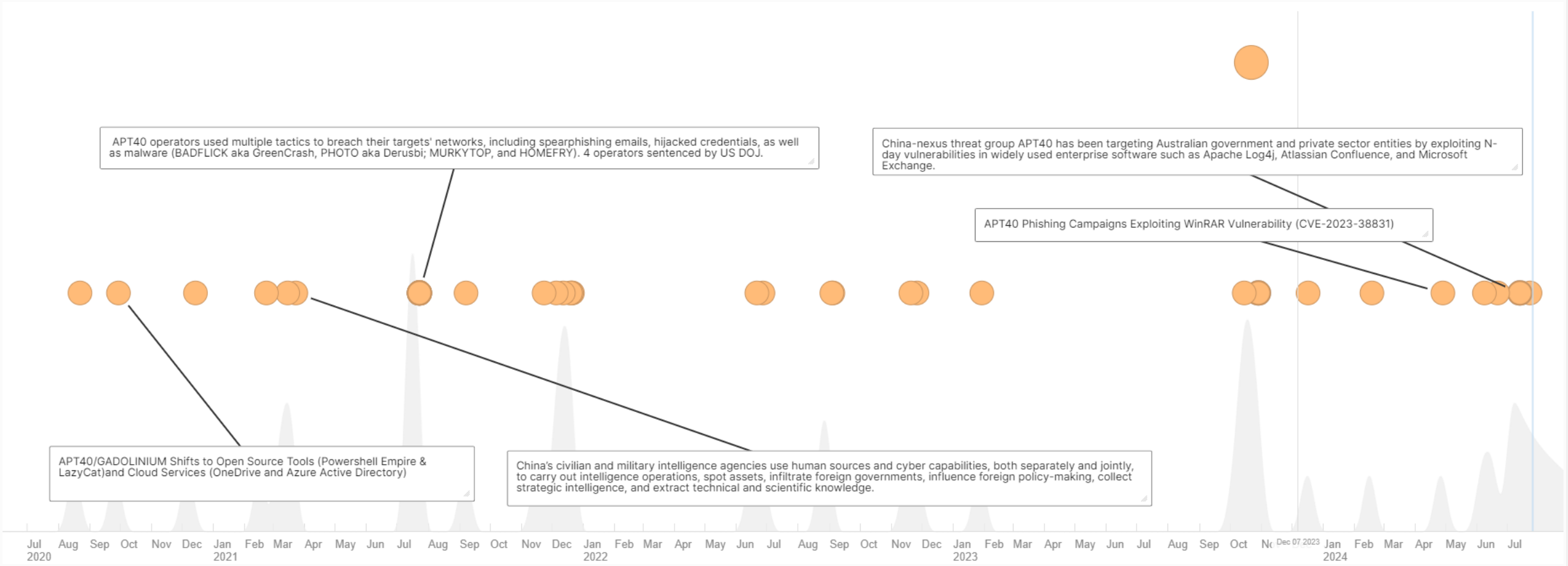
The group has shown a particular interest in maritime technology and countries strategically important to China's Belt and Road initiative. APT40 has been observed using a mixture of open-source and custom malware, including several custom tools shared across multiple Chinese state-sponsored groups such as the JavaScript-based web reconnaissance and exploitation framework ScanBox.

Open source tools used by APT40 include Cobalt Strike Beacon, Powershell Empire, Meterpreter, and Mimikatz. The group has also used custom tools that have not been linked to other groups, including AIRBREAK, DADBOD, DADJOKE, and BADFLICK.

Action: Informational only. No actions needed.

RelianceCyber

APT40 Attacks Timeline



Action: Informational only. No actions needed.

RelianceCyber

APT40 Threat Actor Tactics, Techniques and Procedures

Reliance Cyber have reviewed the latest observed activities attributed to the APT40 Threat Actor and below provide a summary of the most important activity.

EXPLOITATION OF PUBLIC FACING APPLICATIONS

This group appears to prefer exploiting vulnerable, public-facing infrastructure [T1190] 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. 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

DEPLOYMENT OF WEB SHELLS

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.

Action: See page 4 for recommendations.

RelianceCyber

APT40 Threat Actor Tactics, Techniques and Procedures

Reliance Cyber have reviewed the latest observed activities attributed to the APT40 Threat Actor and below provide a summary of the most important activity.

CREDENTIAL ACCESS

Input Capture: Web Portal Capture [T1056.003] **-** 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.

Multi-Factor Authentication Interception [T1111] - 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.

Network Sniffing [T1040] - 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 (JSON Web Tokens).

Action: See page 4 for recommendations.

RelianceCyber

APT40 Threat Actor Tactics, Techniques and Procedures

Reliance Cyber have reviewed the latest observed activities attributed to the APT40 Threat Actor and below provide a summary of the most important activity.

Steal Web Session Cookie [T1539] - 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.

COMMAND AND CONTROL

Data Obfuscation: Protocol Impersonation [T1001.003] - Actors used compromised devices as a launching point for attacks that are designed to blend in with legitimate traffic.

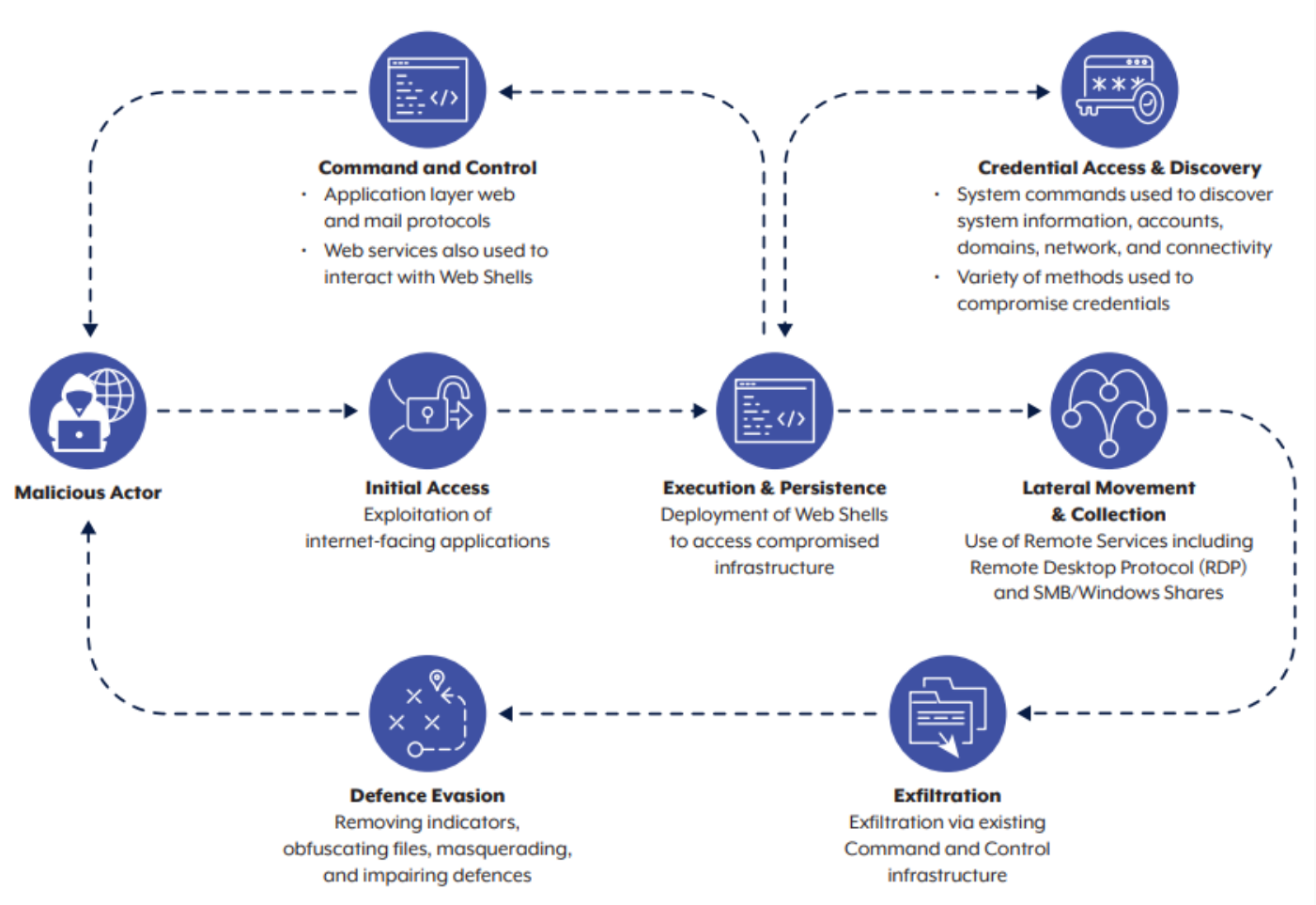
LATERAL MOVEMENT, COLLECTION, EXFILTRATION

Remote Services: SMB Shares [T1021.002] - Threat Actor mounted SMB shares from multiple devices
Data from Information Repositories [T1213] - Regarding manuals/documentation found on the BMS server
Exfiltration Over C2 Channel [T1041] - Regarding the actor's data exfiltration from Active Directory and mounting shares

Action: See page 4 for recommendations.

RelianceCyber

APT40 Threat Actor Profile – Notable Observed TTPs



https://www.cyber.gov.au/sites/default/files/2024-07/apt40-advisory-prc-mss-tradecraft-in-action.pdf

Action: Informational only. No actions needed.

RelianceCyber

Sources & Additional Resources

https://www.cyber.gov.au/sites/default/files/2024-07/apt40-advisory-prc-mss-tradecraft-in-action.pdf

Insikt Group (Recorded Future) Reporting

RELIANCECYBER.COM