ADVISORY FOR ICM SECTOR

APT41 Recent Activities

Original report published on: May 29, 2025[1]

Executive Summary

Google Threat Intelligence Group (GTIG) published a report on APT41, a cyber espionage group known for targeting government entities and various sectors including media and entertainment, and technology.

GTIG identified a compromised government website being used to distribute malware to other government entities. This malware dubbed "TOUGHPROGRESS", used Google Calendar as a command and control (C2) channel to evade detection by blending in with legitimate activities.

Background

Since August 2024, APT41 has been observed using free web hosting services to distribute malware families including VOLDEMORT, DUSTTRAP, and TOUGHPROGRESS.

In this campaign, the malware was delivered through spear-phishing emails linking to ZIP archives hosted on compromised government websites. The malware operates through a three-stage infection chain, with each module performing a specific function while employing advanced stealth techniques such as memory-only payloads, encryption, compression, process hollowing, control flow obfuscation. The stages include:

1. PLUSDROP – a DLL that decrypts and executes the next payload stage in memory.
2. PLUSINJECT – launches and performs process hollowing on a legitimate "svchost.exe" process to inject the final payload.
3. TOUGHPROGRESS – executes actions on the compromised hosts, using Google Calendar as a C2 channel.

Detection and Mitigation

IMDA recommends organisations to perform continual testing and validation of existing security controls to ensure detection and prevention against the PLUSDROP, PLUSINJECT and TOUGHPROGRESS malware identified in this advisory:

- Scan for Indicators of Compromise to detect threat activities (Annex A).
- Refer to the MITRE ATT&CK techniques in this advisory (Annex B):
    - Create, test and validate detection rules against the threat behaviours.
    - Validate and deny/disable processes, ports and protocols that have no business need.
- Use detection rules to detect suspicious use of Google Calendar APIs (e.g. scripts).
- Use EDR/XDR to detect memory-only payloads, non-disk-resident DLLs and unusual in-memory execution patterns.
- Implement application whitelisting to prevent unauthorised DLL or script execution.
- Regularly audit and rotate OAuth tokens, and revoke access for suspicious service accounts using Google Workspace APIs.
- Be alert for suspicious emails, particularly those containing phishing attempts or malicious attachment(s), and educate employees on social engineering tactics used by APTs.

IMDA encourages organisations to conduct thorough analyses to identify potential risks and assess their potential impact prior to deploying defensive measures.

Annex A - Indicators of Compromise

SHA256 Hash	Description
469b534bec827be03c0823e72e7b4da0b84f53199040705da203986ef154406a	出境海關申報清單.zip
3b88b3efbdc86383ee9738c92026b8931ce1c13cd75cd1cda2fa302791c2c4fb	申報物品清單.pdf.lnk
50124174a4ac0d65bf8b6fd66f538829d1589edc73aa7cf36502e57aa5513360	6.jpg
151257e9dfda476cdafd9983266ad3255104d72a66f9265caa8417a5fe1df5d7	7.jpg

MD5 Hash	Description
876fb1b0275a653c4210aaf01c2698ec	出境海關申報清單.zip
65da1a9026cf171a5a7779bc5ee45fb1	申報物品清單.pdf.lnk
1ca609e207edb211c8b9566ef35043b6	6.jpg
2ec4eeeabb8f6c2970dcbffdcdbd60e3	7.jpg

Domain	Description
word[.]msapp[.]workers[.]dev	Cloudflare Workers
cloud[.]msapp[.]workers[.]dev	
term-restore-satisfied-hence[.]trycloudflare[.]com	TryCloudflare
ways-sms-pmc-shareholders[.]trycloudflare[.]com	
resource[.]infinityfreeapp[.]com	InfinityFree
pubs[.]infinityfreeapp[.]com	
https[:]//lihi[.]cc/6dekU	URL Shortener
https[:]//lihi[.]cc/v3OyQ	
https[:]//lihi[.]cc/5nlgd	
https[:]//lihi[.]cc/edcOv	
https[:]//lihi[.]cc/4z5sh	
https[:]//tinyurl[.]com/mr42t4yv	
https[:]//tinyurl[.]com/hycev3y7	
https[:]//tinyurl[.]com/mpa2c5wj	
https[:]//tinyurl[.]com/3wnz46pv	
https[:]//my5353[.]com/ppOH5	
https[:]//my5353[.]com/nWyTf	

https[:]//my5353[.]com/fPUcX	
https[:]//my5353[.]com/ZwEkm	
https[:]//my5353[.]com/vEWiT	
https[:]//reurl[.]cc/WNr2Xy	
104075625139- l53k83pb6jbbc2qbreo4i5a0vepen41j.apps.googleusercontent.com	Calendar
https[:]//www[.]googleapis[.]com/calendar/v3/calendars/.57964096c adc1a8733cf566b41c9528c89d30edec86326c723932c1e79ebf0@gro up.calendar.google.com/events	

Annex B - MITRE ATT&CK Tactics and Techniques

Tactic	Technique ID	Technique Name
Initial Access	T1566.002	Phishing: Spearphishing Link
Execution	T1204.002	User Execution: Malicious File
Defence Evasion	T1027	Obfuscated Files or Information
	T1055.009	Process Injection: Proc Memory
	T1036.008	Masquerading: Masquerade File Type
Command and Control	T1102	Web Service

References

1. ^ “Mark Your Calendar: APT41 Innovative Tactics”