THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

Chinese APT41 Exploits

[Google Calendar]

CATEGORY

Malware

SEVERITY

High

Platforms

Windows

IMPACT

- Data Theft and Surveillance
- Process Injection and Memory-Only Execution
- Operational Disruption
- Regulatory and Reputational Damage

Description

Chinese APT41 Exploits Google Calendar

The researchers have disclosed a **highly sophisticated campaign** by Chinese state-sponsored actor **APT41**, leveraging a new malware strain named **TOUGHPROGRESS** that uses **Google Calendar** as a covert **command-and-control (C2)** channel.

The campaign began in **late October 2024** and was observed targeting **multiple government and industry sectors** across several countries. APT41 is abusing legitimate cloud services like **Google Calendar** to disguise malicious operations as normal business activity, thereby bypassing traditional EDR detections.

Technical Details

Infection Chain Overview:

1. Spear-Phishing Email containing a malicious ZIP file link (hosted on a compromised government site).
2. ZIP contains:
    - A malicious LNK file pretending to be a PDF
    - A folder with "1.jpg" to "7.jpg" (fake arthropod images)
        - 6.jpg: Encrypted payload
        - 7.jpg: DLL used to decrypt and launch payload

Payload Staging Components:

Component	Function
PLUSDROP	DLL decrypts and loads next stage into memory
PLUSINJECT	Hollowing technique used to inject payload into svchost.exe
TOUGHPROGRESS	Final malware that uses Google Calendar API for C2

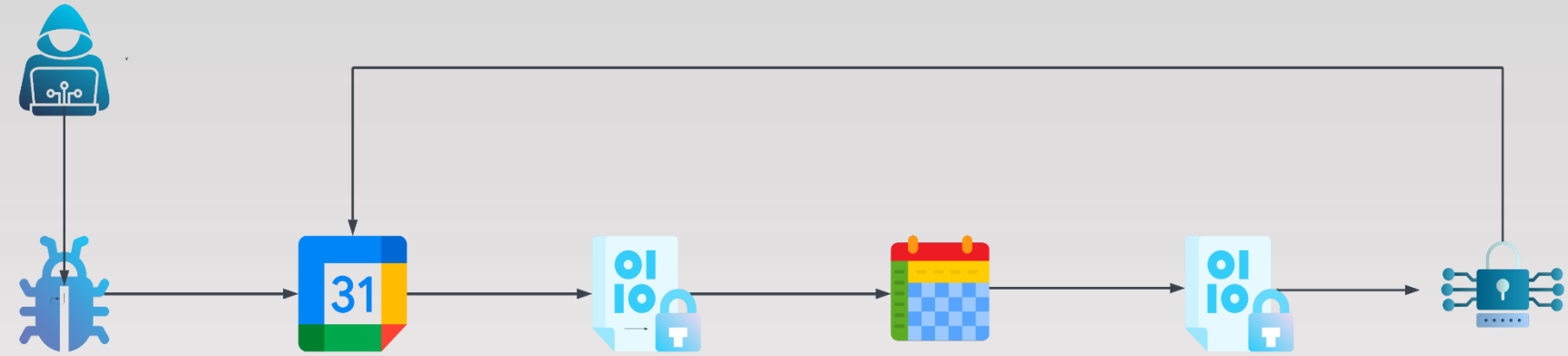
Stealth and Evasion Features

- Memory-only payloads
- Encryption and compression of commands
- Control flow obfuscation
- Scheduled API polling to blend with normal calendar sync
- Deletes calendar events to remove traces

Process Evaluation

TOUGHPROGRESS campaign overview

APT 41



APT41 deploys TOUGHPROGRESS, a malware used by the government-backed threat actor.

TOUGHPROGRESS connects with an attacker-controlled Google Calendar, gaining the ability to read and write events.TOUGHPROGRESS connects with an attacker-controlled Google Calendar, gaining the ability to read and write events.

TOUGHPROGRESS connects with an attacker-controlled Google Calendar, gaining the ability to read and write events.TOUGHPROGRESS connects with an attacker-controlled Google Calendar, gaining the ability to read and write events.

The attacker/operator places encrypted commands into specific calendar event descriptions.

TOUGHPROGRESS polls the calendar continuously, checking for new events.

When an event is found, its description is decrypted. The embedded command is executed on the compromised host. The results are encrypted and sent back via another calendar event.

Indicator of Compromise

SHA-256

469b534bec827be03c0823e72e7b4da0b84f53199040705da203986ef154406a
3b88b3efbdc86383ee9738c92026b8931ce1c13cd75cd1cda2fa302791c2c4fb
50124174a4ac0d65bf8b6fd66f538829d1589edc73aa7cf36502e57aa5513360
151257e9dfda476cdafd9983266ad3255104d72a66f9265caa8417a5fe1df5d7

MD5

876fb1b0275a653c4210aaf01c2698ec
65da1a9026cf171a5a7779bc5ee45fb1
1ca609e207edb211c8b9566ef35043b6
2ec4eeeabb8f6c2970dcbffdcdbd60e3

SHA-1

a04cff8208769ecdc43e14291273c3a540199d07
a6a29946269107b9fd3bcd85386ef9d7438b7ae1
df5ba7ca764063d60eb4dc49d9251c11928b8024
e7ad8d1d670757eba247d4992af54a9003e35a7d

URLs

https://lihi.cc/6dekU
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

Domains

word.msapp.workers.dev
cloud.msapp.workers.dev
term-restore-satisfied-hence.trycloudflare.com
ways-sms-pmc-shareholders.trycloudflare.com
resource.infinityfreeapp.com
pubs.infinityfreeapp.com

Remediation

1. Email Security & User Awareness

- Conduct security awareness training for users to recognize suspicious emails, LNK shortcuts, and unexpected ZIP attachments.
- Block execution of LNK files from email attachments via endpoint protection policies.

2. Endpoint and Network Protection

- Monitor for unusual parent-child process relationships, such as explorer.exe → svchost.exe, which is common in PLUSINJECT-based injections.

3. Detection and Threat Hunting

- Search historical logs for the presence of "PLUSDROP", "PLUSINJECT", or suspicious 6.jpg/7.jpg activity.
- Identify and isolate systems that connected to known malicious domains or IPs related to TOUGHPROGRESS.

4. Incident Response Readiness

- Test your organization's detection and containment capabilities via tabletop exercises involving APT-level threats.
- Establish IOCs (Indicators of Compromise) in EDR/SIEM systems for early warning and blocking.

ThreatCure

Cyber Threat Advisory

Secure your byte world

(Chinese APT41 Exploits

[Google Calendar]