Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

APT41 Leverages Google Calendar for Command and Control

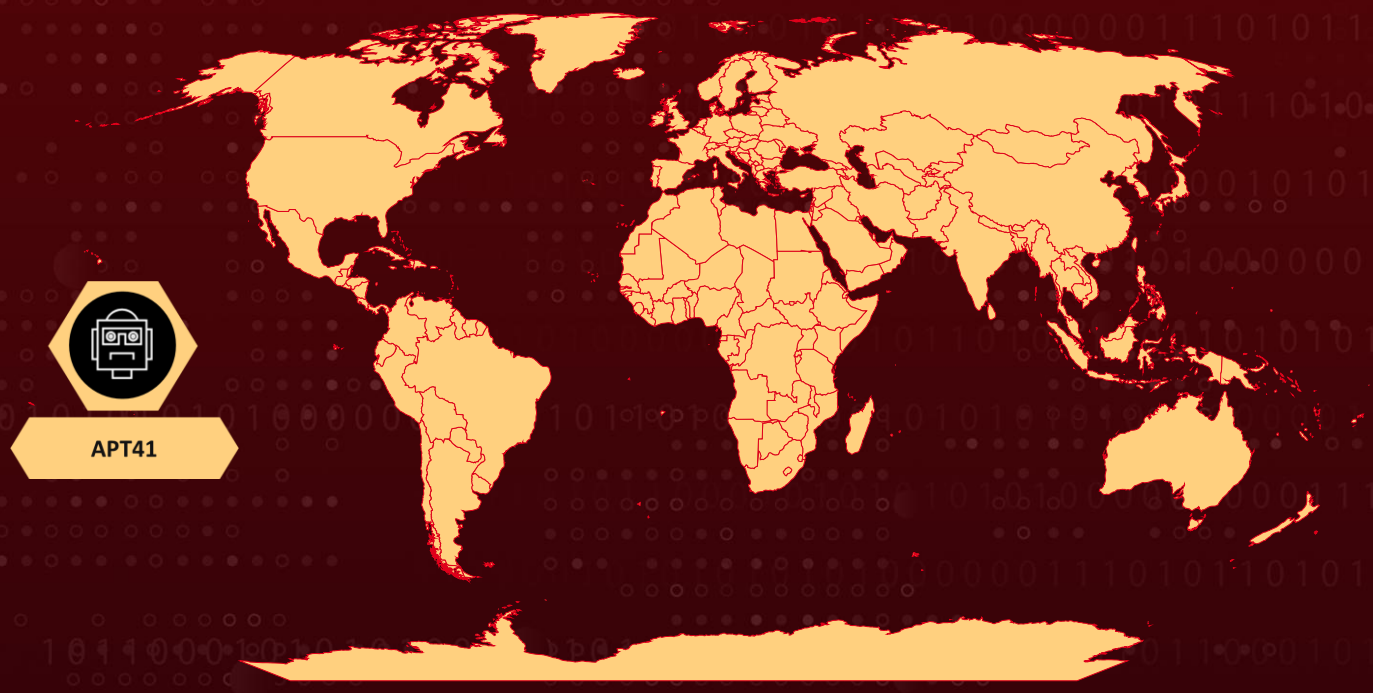
Date of Publication	Admiralty Code	TA Number
May 30, 2025	A1	TA2025168

Summary

Attack Discovered: October 2024
Threat Actor: APT41 (aka HOODOO, WICKED PANDA, Winnti, Group 72, BARIUM, LEAD, GREF, Earth Baku, Brass Typhoon)
Malware: TOUGHPROGRESS
Targeted Region: Worldwide
Targeted Industries: Governments, Shipping, Logistics, Media, Technology, Automotive

Attack: APT41's operation used sophisticated malware, TOUGHPROGRESS, which covertly leveraged trusted cloud services like Google Calendar for command-and-control, bypassing traditional defenses. The campaign reflects a broader shift toward stealthy, cloud-integrated malware ecosystems designed to evade detection, complicate threat hunting, and elevate operational risk for organizations worldwide.

Attack Regions



Attack Details

#1 APT41, a Chinese state-sponsored cyber espionage group, continues to demonstrate its global reach and operational versatility. Their campaigns have targeted a broad spectrum of industries, including government, logistics, media, technology, and automotive underscoring the indiscriminate nature of modern nation-state cyber threats.

#2 In a recent operation, APT41 weaponized spear-phishing emails to deliver a malicious ZIP archive hosted on a compromised government website. Inside the archive was a cleverly disguised LNK file masquerading as a PDF document, alongside a collection of JPG images, two of which were malicious. When the LNK file was opened, it silently executed malicious code, deleted itself, and displayed a decoy PDF document.

#3 At the core of this operation was TOUGHPROGRESS, an advanced malware framework built for stealth, resilience, and operational control. Uniquely, it leverages Google Calendar as an unconventional command-and-control (C2) mechanism. Once embedded in a compromised system, TOUGHPROGRESS creates calendar events with encrypted payloads hidden in event descriptions.

#4 The malware continuously polls Google Calendar, retrieving these events, decrypting their contents, and executing the embedded commands. Results from those commands are then encrypted and written back into new calendar events, creating a discreet, cloud-based communication channel that blends seamlessly into legitimate traffic.

#5 TOUGHPROGRESS is engineered with a modular architecture, deploying three distinct payloads in sequence. Each module serves a specific function and incorporates sophisticated evasion techniques, including memory-resident execution, encryption, compression, process hollowing, and control flow obfuscation.

#6 APT41's operation highlights a growing trend where attackers exploit trusted cloud services like Google Calendar for covert command-and-control, bypassing traditional defenses. Their use of modular, memory-resident malware with advanced evasion tactics signals a shift toward stealthier, harder-to-detect threats that blend into everyday infrastructure raising both operational risk and the complexity of modern threat hunting.

Recommendations

Strengthen Email Filtering Systems: Implement robust email security filters to detect and block spear-phishing emails, especially those with ZIP archives, disguised files, or embedded malicious links. Ensure these systems are updated frequently to recognize evolving threats.

Ensure Strong File Integrity Monitoring: Regularly check for unauthorized file changes and the creation of suspicious files on endpoints, such as files masquerading as PDFs or JPGs. Monitoring tools should be configured to alert when files, especially in ZIP archives, deviate from normal behaviors.

Review and Strengthen Cloud Application Security: Implement proactive security measures such as continuous monitoring and anomaly detection for cloud apps. Ensure that any suspicious behavior is flagged, investigated, and mitigated promptly to avoid further compromise.

Review and Restrict API Access: Ensure that API access to cloud services, such as Google Calendar, is tightly controlled. Review API keys and authentication mechanisms, limiting permissions to only what is necessary for business operations and applying the principle of least privilege.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0005 Defense Evasion
TA0007 Discovery	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
T1566 Phishing	T1566.001 Spearphishing Attachment	T1204 User Execution	T1204.002 Malicious File
T1059 Command and Scripting Interpreter	T1036 Masquerading	T1036.008 Masquerade File Type	T1140 Deobfuscate/Decode Files or Information

T1027 Obfuscated Files or Information	**T1027** Obfuscated Files or Information	**T1027.005** Indicator Removal from Tools	**T1620** Reflective Code Loading
T1055 Process Injection	**T1055.012** Process Hollowing	**T1102** Web Service	**T1001** Data Obfuscation
T1041 Exfiltration Over C2 Channel	**T1005** Data from Local System		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	469b534bec827be03c0823e72e7b4da0b84f53199040705da203986ef154406a, 3b88b3efbdc86383ee9738c92026b8931ce1c13cd75cd1cda2fa302791c2c4fb, 50124174a4ac0d65bf8b6fd66f538829d1589edc73aa7cf36502e57aa5513360, 151257e9dfda476cdafd9983266ad3255104d72a66f9265caa8417a5fe1df5d7
MD5	876fb1b0275a653c4210aaf01c2698ec, 65da1a9026cf171a5a7779bc5ee45fb1, 1ca609e207edb211c8b9566ef35043b6, 2ec4eeeabb8f6c2970dcbffdcdbd60e3
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
URLs	hxxps[:]//lihi[.]cc/6dekU, hxxps[:]//lihi[.]cc/v3OyQ, hxxps[:]//lihi[.]cc/5nlgd, hxxps[:]//lihi[.]cc/edcOv, hxxps[:]//lihi[.]cc/4z5sh, hxxps[:]//tinyurl[.]com/mr42t4yv, hxxps[:]//tinyurl[.]com/hycev3y7, hxxps[:]//tinyurl[.]com/mpa2c5wj, hxxps[:]//tinyurl[.]com/3wnz46pv,

TYPE	VALUE
URLs	hxxps[:]//my5353[.]com/ppOH5, hxxps[:]//my5353[.]com/nWyTf, hxxps[:]//my5353[.]com/fPUcX, hxxps[:]//my5353[.]com/ZwEkm, hxxps[:]//my5353[.]com/vEWiT, hxxps[:]//reurl[.]cc/WNr2Xy, hxxps[:]//www[.]googleapis[.]com/calendar/v3/calendars/ff57964096cadc1a8733cf566b41c9528c89d30edec86326c723932c1e79ebf0[@]group[.]calendar[.]google[.]com/events
Hostname	104075625139-l53k83pb6jbbc2qbreo4i5a0vepen41j[.]apps[.]googleusercontent[.]com

References

https://cloud.google.com/blog/topics/threat-intelligence/apt41-innovative-tactics

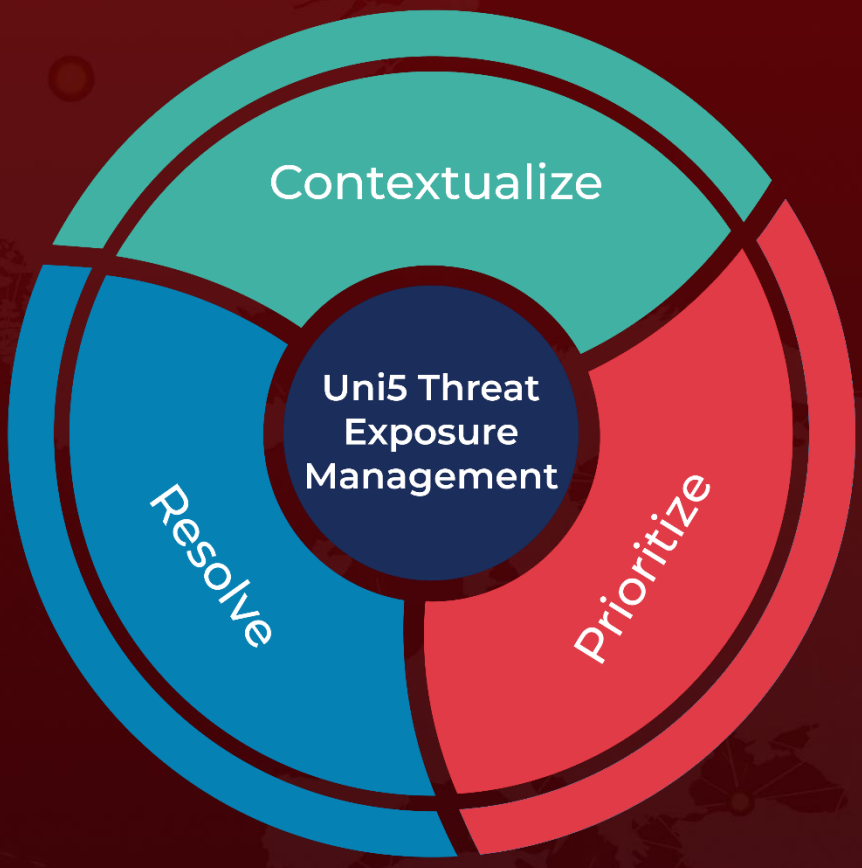
https://attack.mitre.org/groups/G0096/

https://www.fbi.gov/wanted/cyber/apt-41-group

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 30, 2025 • 5:30 AM

More at www.hivepro.com