Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

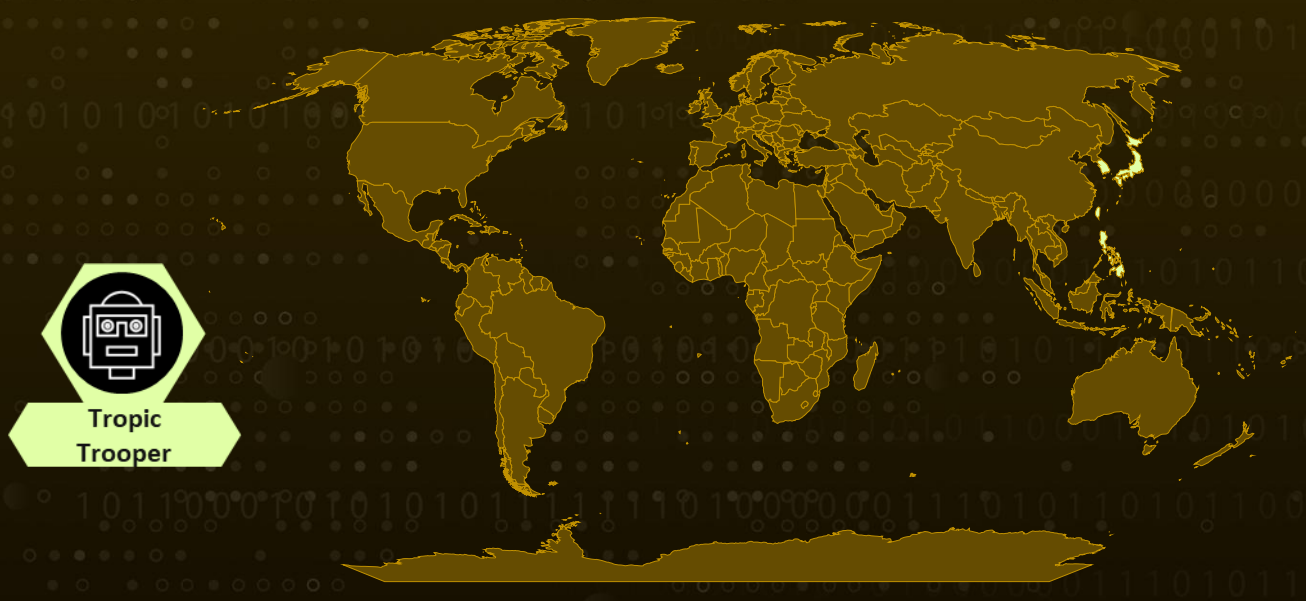
Tropic Trooper Shifts Tradecraft to Open-Source Offensive Frameworks

Date of Publication	Admiralty Code	TA Number
April 24, 2026	A1	TA2026113

Summary

First Seen: March 2026
Targeted Regions: Taiwan, South Korea, Japan, Philippines, Hong Kong
Targeted Platforms: Windows
Targeted Products: SumatraPDF (trojanized as delivery vector), Microsoft Visual Studio Code (abused via tunnels), GitHub (abused as C2 platform), SunloginDesktopAgent (trojanized for secondary infection)
Targeted Industries: Government institutions, Military/Navy agencies, Hospitals, Banks, Transportation, High-tech, Healthcare
Threat Actor: Tropic Trooper (aka APT23, Earth Centaur, KeyBoy, and Pirate Panda)
Malware: EntryShell backdoor, AdaptixC2 Beacon agent, TOSHIS loader
Attack: Tropic Trooper launched a multi-stage intrusion campaign targeting Chinese-speaking individuals in Taiwan along with victims in South Korea and Japan. The operators delivered a ZIP archive containing military-themed document lures alongside a trojanized SumatraPDF reader that silently deployed a TOSHIS loader. The loader fetched encrypted shellcode from a staging server and reflectively loaded an AdaptixC2 Beacon agent that uses a custom listener routing command-and-control traffic through GitHub Issues and repository contents. On high-value hosts the operators deployed Visual Studio Code and established VS Code tunnels for interactive remote access. The same staging infrastructure also hosted a Cobalt Strike Beacon bearing the watermark 520 and the EntryShell custom backdoor, both long-standing hallmarks of Tropic Trooper tradecraft.

Attack Regions



Attack Details

#1

The China-linked advanced persistent threat (APT) known as Tropic Trooper appears to be changing up its tactics, techniques, and procedures (TTPs), with an odd spear-phishing effort. The intrusion begins with a ZIP archive delivered to Chinese-speaking targets that contains a blend of outdated decoy documents alongside one file engineered to lure execution. The weaponized component is an executable, a trojanized copy of the open-source SumatraPDF reader that preserves the legitimate certificate and PDB path but carries an invalidated digital signature. Execution requires user interaction, consistent with Tropic Trooper's long-standing preference for socially engineered spearphishing attachments and fake installer files, which has been documented across the group's campaigns targeting Taiwan, the Philippines, Hong Kong, and earlier air-gapped military and government environments reached through USBferry infections.

#2

Once launched, the trojanized binary hijacks its own control flow by redirecting function into malicious code, a departure from earlier TOSHIS variants that modified the executable entry point directly. The loader constructs stack strings containing the command-and-control, a destination path for the decoy file, DLL names, and a cryptographic key, then resolves Windows APIs dynamically using Adler-32 hashes. It downloads a decoy AUKUS-themed PDF via ShellExecuteW to distract the victim while pulling a second-stage shellcode from the same staging IP, decrypting it in memory. The decrypted shellcode is an AdaptixC2 Beacon agent that is reflectively loaded into the running process. Persistence is established through scheduled tasks created with schtasks /create using names crafted to blend with legitimate services, with triggers configured to run the AdaptixC2 agent on an hourly cadence at the highest run level.

#3

After the Beacon establishes itself, the operators move into a reconnaissance and hands-on-keyboard phase. The agent first queries ipinfo.io to learn its external IP before beaconing out through a custom listener that communicates with the threat-actor-controlled GitHub repository. When a victim is assessed as valuable, the operators download the Visual Studio Code command-line binary from Microsoft's CDN and invoke code tunnel user login --provider github, redirecting the device-login output to z.txt to complete authentication and establish an interactive VS Code tunnel for hands-on access. On some hosts the operators additionally install trojanized alternatives such as SunloginDesktopAgent.exe to better camouflage their footprint, and they have been observed staging Roslyn, the open-source .NET compiler, for trusted-developer-utility proxy execution of malicious code.

#4

For collection and exfiltration, the Beacon uses its native fileupload capability to pull arbitrary files from the compromised host and channels all outbound data through the same GitHub API surface used for command delivery. Output is Base64-encoded, split into 30-megabyte parts when necessary, and written as individual files under the repository's contents tree. Operational security is tight: Beacons are deleted within roughly ten seconds of upload to destroy the session keys and prevent passive decryption of captured traffic. The same staging server that hosts the AdaptixC2 shellcode was also observed serving a Cobalt Strike Beacon marked with the watermark 520 and an EntryShell custom backdoor using the AES-128 ECB key afkngaikfaf, both of which align with previously documented Tropic Trooper tooling and cement the attribution.

Recommendations

Detect Trojanized SumatraPDF and Invalid Code Signatures: Deploy endpoint detection rules that flag SumatraPDF-named binaries whose Authenticode signature is present but cryptographically invalid, and match the file hashes listed in the IoC section. Consider blocking unsigned or revoked-signature executables from executing out of user profile, Downloads, and Temp directories.

Monitor GitHub API Egress for Beaconing Behavior: Inspect HTTPS traffic to api.github.com for process origins that do not correspond to sanctioned developer tooling or CI agents, especially POSTs to /repos/ /issues, PUTs to /repos/ /contents, and repeated polling of issues?state=open. Establish a baseline of legitimate GitHub usage per endpoint and alert on deviations, including uploads of base64 blobs larger than a few megabytes.

Restrict and Audit Visual Studio Code Tunnel Usage: Tropic Trooper weaponizes the legitimate code tunnel feature. Where VS Code tunnels are not required, block the code.exe CLI from invoking the tunnel command, strip the VS Code CLI binary from standard endpoint images, and alert on any process tree that writes device-login output to files such as z.txt, z2.txt, or files in C:\Users\Public\Documents. Require SSO-enforced GitHub accounts that cannot be authorized from unmanaged devices.

Monitor Suspicious Ingress Tool Transfer: Build detections for cURL invocations downloading from code.visualstudio.com, bashupload[.]app, or any IP-literal HTTP source into user-profile or Public directories, and for mass renaming of downloaded archives to short names such as v.zip. Correlate with Microsoft Defender or AMSI alerts on subsequent shellcode activity.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Resource Development	T1585: Establish Accounts	T1585.003: Cloud Accounts
	T1587: Develop Capabilities	T1587.001: Malware
	T1588: Obtain Capabilities	T1588.001: Malware
		T1588.002: Tool
	T1608: Stage Capabilities	T1608.001: Upload Malware
		T1608.002: Upload Tool
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1204: User Execution	T1204.002: Malicious File
	T1106: Native API	
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
Persistence	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
	T1547: Boot or Logon Autostart Execution	T1547.004: Winlogon Helper DLL
Defense Evasion	T1036: Masquerading	T1036.001: Invalid Code Signature
		T1036.004: Masquerade Task or Service
	T1620: Reflective Code Loading	

Tactic	Technique	Sub-technique
Defense Evasion	T1027: Obfuscated Files or Information	T1027.007: Dynamic API Resolution
		T1027.013: Encrypted/Encoded File
	T1127: Trusted Developer Utilities Proxy Execution	
Discovery	T1016: System Network Configuration Discovery	
Collection	T1005: Data from Local System	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1219: Remote Access Tools	T1219.001: IDE Tunneling
	T1105: Ingress Tool Transfer	
	T1132: Data Encoding	T1132.001: Standard Encoding
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
		T1573.002: Asymmetric Cryptography
Exfiltration	T1567: Exfiltration Over Web Service	T1567.001: Exfiltration to Code Repository
	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	158[.]247[.]193[.]100, 58[.]247[.]193[.]100, 47[.]76[.]236[.]58
Domains	stg.lsmartv[.]com, bashupload[.]app
URLs	hxxps[:]//api[.]github[.]com/repos/cvaS23uchsahs/rss/issues, hxxps[:]//47[.]76[.]236[.]58[:]4430/Originate/contacts/CX4YJ5JI7RZ, hxxps[:]//47[.]76[.]236[.]58[:]4430/Divide/developement/GIZWQVCLF, hxxps[:]//stg[.]lsmartv[.]com[:]8443/Originate/contacts/CX4YJ5JI7RZ, hxxps[:]//stg[.]lsmartv[.]com[:]8443/Divide/developement/GIZWQVCLF
SHA256	a4f2131eb497afe5f78d8d6e534df2b8d75c5b9b565c3ec17a323afe5355da26, 47c7ce0e3816647b23bb180725c7233e505f61c35e7776d47fd448009e887857, aeec65bac035789073b567753284b64ce0b95bbae62cf79e1479714238af0eb7, 7a95ce0b5f201d9880a6844a1db69aac7d1a0bf1c88f85989264caf6c82c6001, 3936f522f187f8f67dda3dc88abfd170f6ba873af81fc31bbf1fdbcad1b2a7fb, 6eaea92394e115cd6d5bab9ae1c6d088806229aae320e6c519c2d2210dbc94fe, b92a3a1cf5786b6e08643483387b77640cd44f84df1169dd00efde7af46b5714, 3c29c72a59133dd9eb23953211129fd8275a11b91a3b8dddb3c6e502b6b63edb
SHA1	2c65433696037f4ce0f8c9a1d78bdd6835c1b94d, 19e3c4df728e3e657cb9496cd4aaf69648470b63, bd618c9e1e10891fe666839650fa406833d70afd, 6c68dc2e33780e07596c3c06aa819ea460b3d125, adb47733c224fc8c0f7edc61becb578e560435ab, c2051635ccfdc0b48c260e7ceeee3f96bf026fea, 343be0f2077901ea5b5b9fb97d97892ac1a907e6, 401cc16d79d94c32da3f66df21d66ffd71603c14

TYPE	VALUE
MD5	67fcf5c21474d314aa0b27b0ce8befb2, 89daa54fada8798c5f4e21738c8ea0b4, e2dc48ef24da000b8fc1354fa31ca9ae, 2d7cc3646c287d6355def362916c6d26, 71fa755b6ba012e1713c9101c7329f8d, c620b4671a5715eec0e9f3b93e6532ba, 9a69b717ec4e8a35ae595aa6762d3c27, 3238d2f6b9ea9825eb61ae5e80e7365c

References

https://www.zscaler.com/blogs/security-research/tropic-trooper-pivots-adaptixc2-and-custom-beacon-listener

https://documents.trendmicro.com/assets/Tech-Brief-Tropic-Trooper-s-Back-USBferry-Attack-Targets-Air-gapped-Environments.pdf

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 Demo of **HivePro**.

REPORT GENERATED ON

April 24, 2026 • 06:00 AM

More at www.hivepro.com