Hive Pro

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

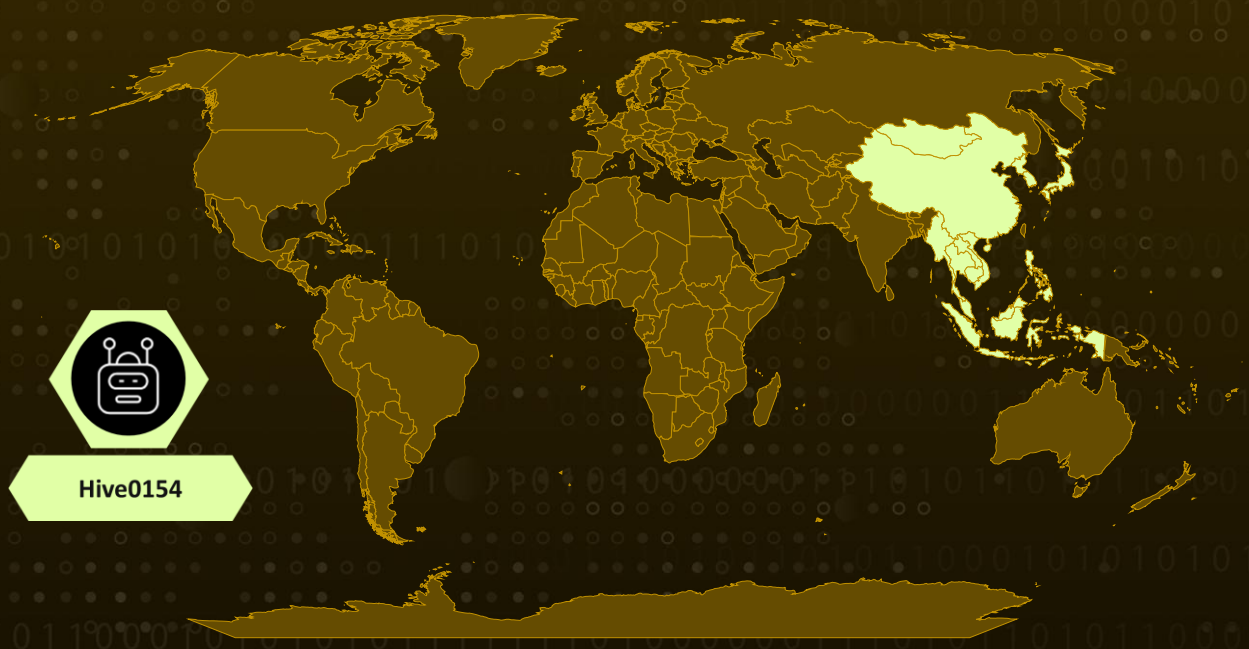
Hive0154 Evolves with SnakeDisk and Enhanced Toneshell Backdoor

Date of Publication	Admiralty Code	TA Number
September 16, 2025	A1	TA2025283

Summary

Attack Discovered: Mid 2025
Targeted Countries: East Asia
Targeted Industries: Government, Defense
Malware: SnakeDisk, Yokai, Pubload, Toneshell
Actor: Hive0154 (aka Mustang Panda, Bronze President, TEMP.Hex, HoneyMyte, Red Lich, Earth Preta, Camaro Dragon, PKPLUG, Stately Taurus, Twill Typhoon, G0129)
Attack: A new wave of activity linked to the China-aligned group Hive0154 reveals a rapidly expanding malware arsenal designed for stealth and persistence. Central to this campaign is SnakeDisk, a USB worm that spreads across removable drives in Thailand, planting the Yokai backdoor for covert command execution. Alongside it, advanced Toneshell variants, most notably the elusive Toneshell9, demonstrate heavy obfuscation, proxy abuse, and beaconing techniques that allow them to blend into normal network traffic. The operation also uses weaponized archives disguised as official government documents and delivered through cloud services, adding a convincing social engineering layer.

Attack Regions



Attack Details

#1 In July 2025, a fresh wave of activity tied to the China-aligned threat actor **Hive0154**, was uncovered, spotlighting a growing and sophisticated malware ecosystem. Among the discoveries were new variants of the long-running Toneshell family, the novel SnakeDisk USB worm, and deployments of the Yokai backdoor. The threat campaign showed clear signs of geographic targeting, with malware samples and weaponized archives surfacing primarily from Singapore and Thailand.

#2 In one campaign, an archive named CallNotes.zip was identified, disguised as an official document from Myanmar, hosted on Box Cloud Storage. The archive contained loaders for Pubload and Toneshell7, while also deploying an obfuscated Toneshell8 variant designed to frustrate analysis. The discovery of SnakeDisk in August marked an escalation, with its USB worming capability likely aimed at infiltrating air-gapped environments within Thai government and military networks.

#3 The Toneshell malware line itself showed a steady evolution throughout 2025. Version 8, observed in March, introduced junk code and a custom Linear Congruential Generator (LCG) to obscure operations, while obfuscating response codes sent to its C2 infrastructure. By July, the emergence of Toneshell9 represented a major leap forward: a stealthy sideloaded DLL packed with anti-analysis techniques, proxy enumeration, and a custom beaconing system built to mimic legitimate TLS traffic. This variant proved particularly stealthy, running undetected across scanning platforms and capable of maintaining two reverse shells simultaneously while blending seamlessly into enterprise network traffic.

#4 SnakeDisk added another layer of danger, spread aggressively via USB devices. It verified execution on Thai machines, ensured only one instance ran at a time, and used low-level storage APIs to identify and infect removable drives. Once active, it hid files on the USB while dropping its own malicious executables under disguised filenames. The worm also embedded payloads that leveraged DLL sideloading to execute under the guise of legitimate software. With these mechanisms, SnakeDisk appeared designed for long-term persistence, silent propagation, and eventual deployment of Yokai, a modular backdoor enabling attackers to run arbitrary commands and maintain covert access.

#5 Taken together, the findings point to a broad, interlinked malware ecosystem under Hive0154's control. This suggests at least three overlapping subclusters, each anchored by distinct strains like Toneshell, SnakeDisk, or Yokai. While it remains unclear whether these represent separate operational units or a single coordinated effort, the consistent focus on Thailand signals a strategic campaign. Hive0154 has a well-documented history of targeting both public and private sector organizations, and this latest toolkit underscores its intent to refine its arsenal for global operations.

Recommendations

Harden USB and removable media use: Limit the use of USB drives and other removable devices, especially in sensitive or air-gapped environments. Where possible, disable autorun features, and only allow trusted, scanned devices to be connected. Worms like SnakeDisk thrive on unchecked USB use.

Monitor unusual network behavior: Set up monitoring for strange or hidden network traffic, such as TLS connections that don't match typical patterns or proxy server lookups from endpoints. Malware like Toneshell9 hides inside "normal-looking" traffic, so spotting the odd behaviors early is key.

Strengthen email and cloud storage defenses: Phishing lures and weaponized archives were central to this campaign. Use secure email gateways, enable multifactor authentication, and train staff to recognize suspicious attachments or links, even if they appear to come from trusted organizations or cloud platforms.

Enhance Endpoint Protection: Deploy next-generation antivirus (NGAV) and endpoint detection & response (EDR) solutions to identify and block malware. Leverage behavioral analysis and machine learning-based detection to spot suspicious activity.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	**TA0002** Execution	**TA0003** Persistence	**TA0005** Defense Evasion
TA0005 Defense Evasion	**TA0007** Discovery	**TA0011** Command and Control	**T1091** Replication Through Removable Media
T1574 Hijack Execution Flow	**T1574.001** DLL	**T1105** Ingress Tool Transfer	**T1027** Obfuscated Files or Information
T1090 Proxy	**T1071** Application Layer Protocol	**T1059** Command and Scripting Interpreter	**T1547** Boot or Logon Autostart Execution

T1547.001 Registry Run Keys / Startup Folder	**T1656** Impersonation	**T1566** Phishing	**T1070** Indicator Removal
T1053 Scheduled Task/Job	**T1204** User Execution	**T1036** Masquerading	**T1140** Deobfuscate/Decode Files or Information
T1082 System Information Discovery	**T1012** Query Registry		

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f8b28cae687bd55a148d363d58f13a797486f12221f0e0d080ffb53611d54231, 8132beeb25ce7baed0b561922d264b2a9852957df7b6a3daacfbb3a969485c79, d1466dca25e28f0b7fae71d5c2abc07b397037a9e674f38602690e96cc5b2bd4, 1272a0853651069ed4dc505007e8525f99e1454f9e033bcc2e58d60fdafa4f02, b8c31b8d8af9e6eae15f30019e39c52b1a53aa1c8b0c93c8d075254ed10d8dfc, 7087e84f69c47910fd39c3869a706e55324783af8d03465a9e7bfde52fe4d1d6, 38fcd10100f1bfd75f8dc0883b0c2cb48321ef1c57906798a422f2a2de17d50c, 69cb87b2d8ee50f46dae791b5a0c5735a7554cc3c21bb1d989baa0f38c45085c, 564a03763879aaed4da8a8c1d6067f4112d8e13bb46c2f80e0fcb9ffdd40384c, e4bb60d899699fd84126f9fa0dff72314610c56fffca3d11f3b6fc93fcb75e00, c2d1ff85e9bb8feb14fd015dceee166c2e52e2226c07e23acc348815c0eb4608, bdbc936ddc9234385317c4ee83bda087e389235c4a182736fc597565042f7644,

TYPE	VALUE
SHA256	f0fec3b271b83e23ed7965198f3b00eece45bd836bf10c038e9910675bafefb1, e7b29611c789a6225aebbc9fee3710a57b51537693cb2ec16e2177c22392b546, 9ca5b2cbc3677a5967c448d9d21eb56956898ccd08c06b372c6471fb68d37d7d, 318a1ebc0692d1d012d20d306d6634b196cc387b1f4bc38f97dd437f117c7e20, 0d632a8f6dd69566ad98db56e53c8f16286a59ea2bea81c2761d43b6ab4ecafd, 39e7bbcceddd16f6c4f2fc2335a50c534e182669cb5fa90cbe29e49ec6dfd0df, 05eb6a06b404b6340960d7a6cf6b1293e706ce00d7cba9a8b72b3780298dc25d, dd694aaf44731da313e4594d6ca34a6b8e0fcce505e39f8273b9242fdf6220e0, bb5bb82e5caf7d4dbbe878b75b23f793a5f3c5ca6dba70d8be447e8c004d26ce, 35bec1d8699d29c27b66e5646e58d25ce85ea1e41481d048bcea89ea94f8fb4b
IPv4	188[.]208[.]141[.]196, 146[.]70[.]29[.]229, 123[.]253[.]34[.]44
Domain	www[.]slickvpn[.]com
URL	hxxp[:]//118[.]174[.]183[.]89/kptinfo/import/index[.]php

References

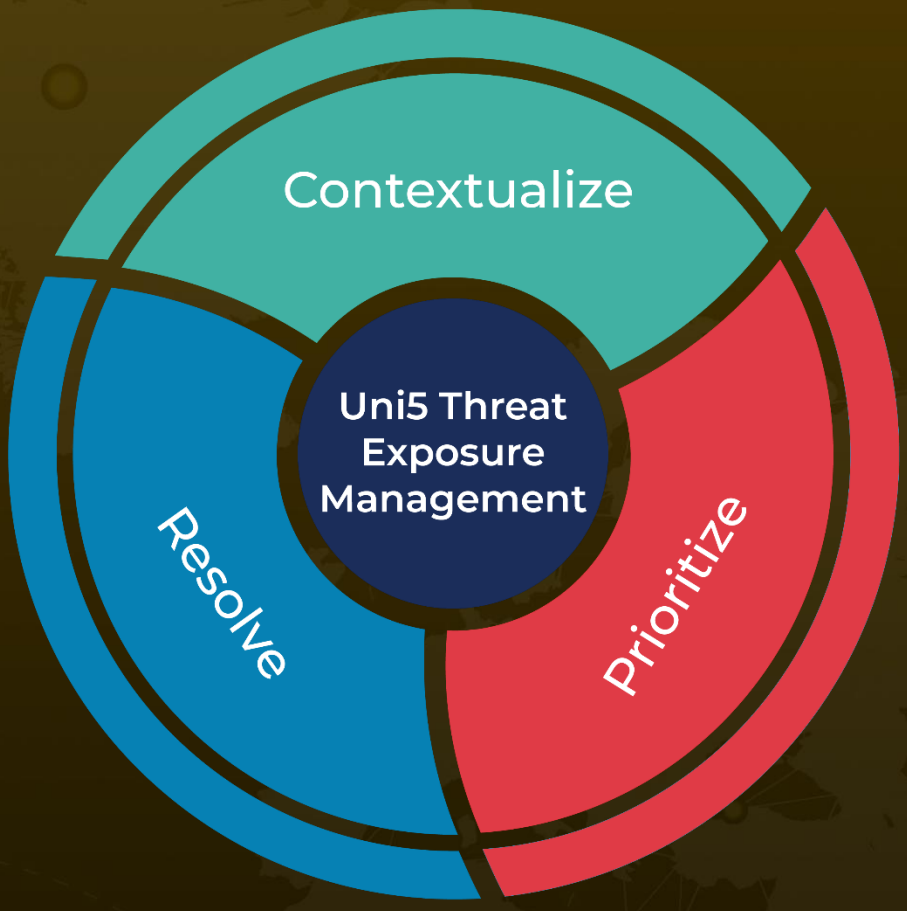
https://www.ibm.com/think/x-force/hive0154-drops-updated-toneshell-backdoor

https://hivepro.com/threat-advisory/chinese-apt-earth-preta-runs-spearphishing-campaigns/

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

September 16, 2025 . 10:30 PM

More at www.hivepro.com