Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

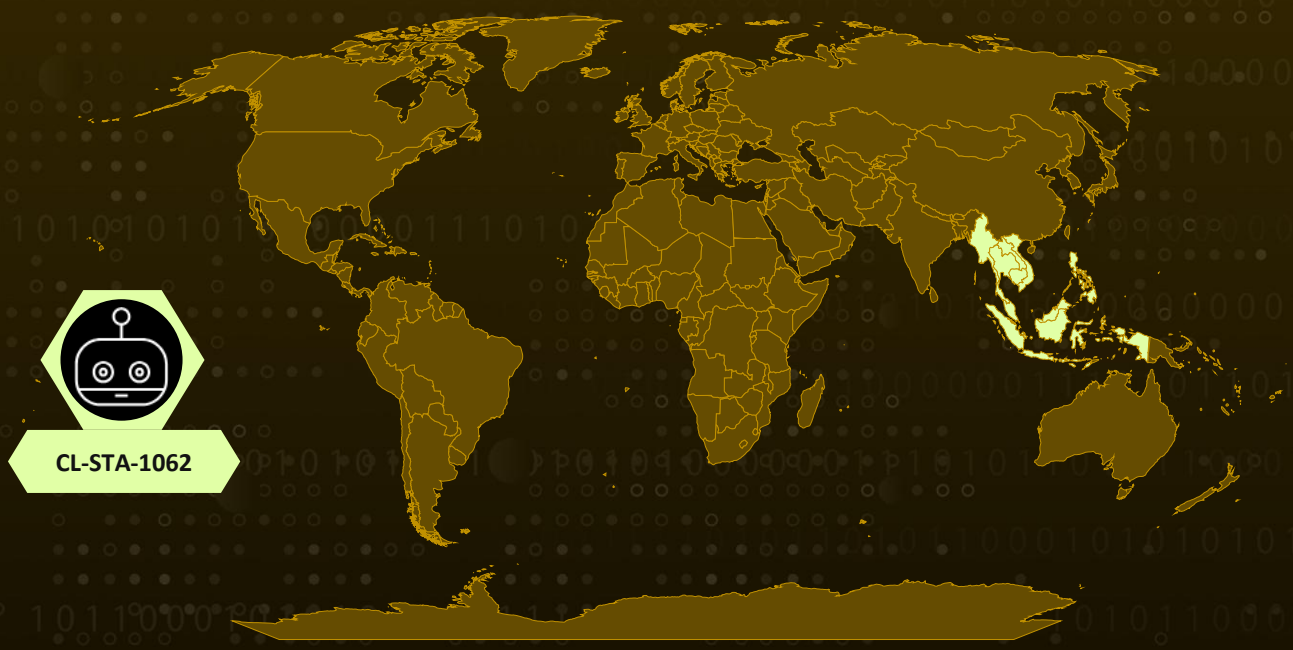
TinyRCT: A Chinese-Speaking APT's Custom Backdoor Quietly Burrows into Southeast Asia

Date of Publication	Admiralty Code	TA Number
June 29, 2026	A1	TA2026181

Summary

First Seen: mid-2025
Targeted Region: Southeast Asia
Targeted Platform: Windows
Targeted Industries: Government, Critical Energy Infrastructure, State-Owned Enterprises
Threat Actor: CL-STA-1062
Malware: TinyRCT
Attack: A Chinese-speaking activity cluster tracked as CL-STA-1062 has been quietly carving its way through Southeast Asian government bodies and state-owned critical energy infrastructure since mid-2025. Operating from a hybrid toolkit of well-worn open-source utilities and a brand-new bespoke backdoor named TinyRCT, the actor compromises victims via ASPX web shells on vulnerable web applications, pivots through networks using SoftEther VPN, VNT, and Yuze tunneling tools disguised as VMware or XDR binaries, and exfiltrates sensitive data including database contents and full web server source trees in password-protected RAR archives. The newly documented TinyRCT, a lightweight C# .NET implant delivered through an AppDomainManager injection chain inside a trojanized chrome_setup.zip package, gives the operator arbitrary command execution, file enumeration and exfiltration, screen capture, and a clean self-destruct option, all wrapped in AES-128-encrypted HTTP traffic.

Attack Regions



Attack Details

#1

A Chinese-speaking advanced persistent threat (APT) actor tracked as CL-STA-1062 has been linked to a new custom backdoor called TinyRCT, deployed in a series of cyberattacks targeting government entities and critical infrastructure across Southeast Asia. The intrusions typically begin with the attackers' exploiting vulnerabilities in public-facing web applications and dropping ASPX web shells onto the compromised servers. These web shells become the operator's central console, used to run arbitrary commands, stage additional tooling, and conduct initial system and network reconnaissance. Alongside the web shell path, researchers have documented a parallel delivery chain that begins with a malicious archive named chrome_setup.zip, which bundles a legitimate signed chrome_setup.exe with a malicious chrome_setup.exe.config and a rogue MyAppDomainManager.dll. When a user runs the trusted executable from the Downloads folder, the .NET runtime parses the adjacent configuration file and obediently loads the malicious DLL as the application's domain manager, allowing the attacker's code to execute inside a signed and trusted process from the very first instruction.

#2

Once the loader passes its environment check, it reaches out to the staging server at 139[.]180[.]134[.]221 to pull down PerfWatson2.exe, the TinyRCT payload, and drops it into %LOCALAPPDATA% under a filename that mimics the legitimate Microsoft Visual Studio telemetry component. Persistence is established through a scheduled task named GoogleUpdaterTaskSystem140.0.7272.0, configured to run at the highest available privileges on every user logon. TinyRCT itself runs its own environment check, confirming it was launched from %LOCALAPPDATA% before doing anything else, then fingerprints the host by collecting the current username, machine name, OS version, local IP addresses, execution path, process ID, and a freshly generated GUID, which it bundles and ships to the C2 over an encrypted HTTP POST.

#3

For lateral movement and broader access, the operators lean heavily on open-source tools. Mimikatz is used to harvest credentials, JuicyPotato is deployed for local privilege escalation, and fscan handles network and vulnerability enumeration. Traceroute helps the attackers map paths between government networks for follow-on compromise. Tunnelling and command-and-control are routed through SoftEther VPN, Yuze (a SOCKS5 proxy), and VNT (an open-source VPN), each disguised as legitimate VMware components such as vmtools.exe and vmwared.exe or as an endpoint security tool named XDRAgent.exe. In one observed intrusion, the attackers used a web shell to extract a password-protected RAR archive containing a SoftEther VPN binary masquerading as vmtools.exe, and in another they registered a scheduled task to execute a VNT binary at login under a VMware-themed name.

#4

Data exfiltration is methodical and quiet. TinyRCT polls the C2 at 45[.]32[.]113[.]172 every ten seconds over plain HTTP, encrypting every byte of payload with AES-128 in CBC mode using the hardcoded key ThisIsASecretKey87654321 and a null initialisation vector. When tasked to exfiltrate a file, the malware compresses the contents with gzip, encrypts the result, and ships it in 40 KB chunks to keep the network footprint discreet. Screenshots are captured as JPEG, compressed, encrypted, and exfiltrated through the same channel. Bulk theft is handled differently: the attackers exfiltrated MSSQL database contents via direct query, archived entire web server source code directories into password-protected RAR files for staging, and routed bulk traffic through their SoftEther and VNT tunnels. When the operator decides the host has served its purpose, the self-destruct command removes the GoogleUpdater scheduled task and triggers a legacy choice.exe-based self-deletion routine that introduces a three-second delay to guarantee the malware process has fully exited and released its file handle before the executable is wiped from disk.

Recommendations

- **Restrict Untrusted Binary Execution from User Profile Locations:** Deploy application control and behavioral monitoring policies that block or alert on execution of unsigned or unknown binaries running from %LOCALAPPDATA%, %USERPROFILE%\Downloads, and other user-writable paths, since TinyRCT and its loader both rely on these directories for execution context.

- **Hunt for AppDomainManager Injection Indicators:** Audit endpoints for .NET applications running with adjacent .config files that reference unsigned application domain manager DLLs in non-standard paths. Treat any executable paired with a MyAppDomainManager.dll or comparable injection-ready configuration as suspicious until proven otherwise.

- **Monitor Scheduled Task Creation for Highest-Privilege Logon Triggers:** Generate high-severity alerts on schtasks invocations that combine /rl highest with /sc onlogon, especially when the task name impersonates Google Updater, Visual Studio, or other widely trusted vendor components.

- **Patch and Harden Public-Facing Web Applications:** Prioritize patching of internet-exposed ASPX, IIS, and web application stacks, perform regular web shell scans across web roots, and enforce strict outbound network controls from web servers to disrupt the actor's preferred initial-access path.

Strengthen Credential Hygiene and Privileged Account Controls: Enforce least-privilege access, disable interactive logons for service accounts, rotate domain administrator credentials regularly, and deploy LSASS protection (Credential Guard, RunAsPPL) to blunt Mimikatz-style credential dumping.

Segment Critical Infrastructure and Government Networks: Apply strict network segmentation between internet-facing systems, internal government networks, and operational technology environments to limit the lateral movement opportunities that CL-STA-1062 has exploited to pivot between government entities and energy operators.

Conduct Threat Hunting Aligned to CL-STA-1062 TTPs: Run regular threat hunts for AppDomainManager hijacking artifacts, GoogleUpdaterTaskSystem-style scheduled tasks, choice.exe-based self-deletion patterns, and curl-driven exfiltration of system enumeration data, particularly in government and energy sector environments across the Asia-Pacific region.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
		T1059.001: PowerShell
	T1204: User Execution	T1204.002: Malicious File
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task

Tactic	Technique	Sub-technique
Persistence	T1574: Hijack Execution Flow	T1574.014: AppDomainManager
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task
Defense Evasion	T1574: Hijack Execution Flow	T1574.014: AppDomainManager
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1497: Virtualization/Sandbox Evasion	
	T1070: Indicator Removal	T1070.004: File Deletion
		T1070.009: Clear Persistence
	T1027: Obfuscated Files or Information	
Credential Access	T1003: OS Credential Dumping	
Discovery	T1082: System Information Discovery	
	T1083: File and Directory Discovery	
	T1016: System Network Configuration Discovery	
	T1087: Account Discovery	
	T1049: System Network Connections Discovery	
	T1046: Network Service Discovery	

Tactic	Technique	Sub-technique
Collection	T1005: Data from Local System	
	T1113: Screen Capture	
	T1560: Archive Collected Data	T1560.001: Archive via Utility
	T1213: Data from Information Repositories	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1572: Protocol Tunneling	
	T1090: Proxy	
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	
	T1030: Data Transfer Size Limits	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	00e09754526d0fe836ba27e3144ae161b0ecd3774abec5560504a16a67f0087c, f34bd1d485de437fe18360d1e850c3fd64415e49d691e610711d8d232071a0b1, dce5df29bddff5a4ddaea5c4fec14da91f7b69063a6e1c45ed61e5da4fc6c87b, cbfe8de6ffadbb1d396f61e63eb18e8b11c29527c1528641e3223d4c516cf7c3, 4e1f8888d020decd09799ec946f1bf677cac6612b24582ddbf4d8ede425d8384, 9b481b69cd91b09fa7bae7428f646dd89473a4c03393e43da81fe756cde1c472
IPv4	139[.]180[.]134[.]221, 202[.]182[.]102[.]5, 45[.]76[.]210[.]43, 45[.]32[.]113[.]172
URLs	hxxp[:]//139[.]180[.]134[.]221/sdksdk608/1[.]zip, hxxp[:]//139[.]180[.]134[.]221/sdksdk608/anydesk_0117[.]zip, hxxp[:]//139[.]180[.]134[.]221/sdksdk608/hamcore[.]se2, hxxp[:]//139[.]180[.]134[.]221/sdksdk608/httpdf, hxxp[:]//139[.]180[.]134[.]221/sdksdk608/vpn_bridge[.]config, hxxp[:]//139[.]180[.]134[.]221/sdksdk608/win-vpn[.]rar, hxxp[:]//139[.]180[.]134[.]221/PerfWatson2[.]exe

References

https://unit42.paloaltonetworks.com/cl-sta-1062-tinyrct-backdoor/

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

June 29, 2026 • 10:00 AM

More at www.hivepro.com