Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

Amaranth-Dragon: Low Noise, High Impact Espionage in Southeast Asia

Date of Publication	Admiralty Code	TA Number
February 06, 2026	A1	TA2026038

Summary

First Seen: March 19, 2025
Targeted Regions: Cambodia, Thailand, Laos, Indonesia, Singapore, Philippines, Brunei, Malaysia, Myanmar, Timor-Leste, Vietnam
Targeted Platform: Windows
Targeted Product: RARLAB WinRAR
Targeted Industries: Government, Law Enforcement
Threat Actor: Amaranth-Dragon
Malware: Amaranth Loader, TGAmaranth RAT
Attack: Amaranth-Dragon, a China-linked APT group associated with the APT-41 ecosystem, conducts highly targeted cyber-espionage campaigns against government and law enforcement agencies across Southeast Asia. The group exploits CVE-2025-8088, a path traversal vulnerability in WinRAR, to achieve arbitrary code execution. They deliver malicious RAR archives via spear-phishing, using geopolitically themed lures related to local political events, official government decisions, and regional security events. The attack chain deploys a custom loader dubbed Amaranth Loader, and in some cases, a Telegram-based RAT TGAmaranth RAT for persistent access and data exfiltration.

Attack Regions

CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-8088	RARLAB WinRAR Path Traversal Vulnerability	RARLAB WinRAR	✓	✓	✓

Attack Details

#1

A new threat actor tracked Amaranth-Dragon exploited the CVE-2025-8088 vulnerability in WinRAR in espionage attacks. Amaranth-Dragon begins its campaigns with carefully crafted spear-phishing emails. These messages deliver weaponized RAR attachments hosted on trusted cloud platforms such as Dropbox, lending them immediate credibility. The attached documents are themed around current regional and geopolitical events, civil servant salary updates in Indonesia, Philippine Coast Guard anniversaries, or joint military exercises between China and Thailand, designed to prompt quick, uncritical engagement.

#2

Once opened, the RAR files exploit CVE-2025-8088, a path traversal flaw that allows the attackers to place malicious CMD or BAT scripts directly into the Windows Startup folder. This ensures execution after a system reboot and establishes an initial foothold. The script then unpacks a password-protected archive and launches a legitimate, signed executable that is vulnerable to DLL search-order hijacking. Through this weakness, the attackers sideload the Amaranth Loader, a 64-bit malicious DLL.

#3

In some operations, Amaranth-Dragon deploys TGAmaranth RAT, a Telegram-based remote access tool with strong anti-debugging and anti-EDR defenses. It actively replaces hooked versions of ntdll.dll with clean copies to bypass security controls and communicates through a hardcoded Telegram bot token.

#4 Through these tools, the group gains full post-exploitation capability, like process discovery, screenshot capture, command execution, and file transfer. Telegram-based control further masks malicious traffic by blending it with legitimate use. Correlation of build times, infrastructure behavior, combined with technical overlaps and shared tradecraft, strongly indicates that Amaranth-Dragon is closely connected to the APT-41 ecosystem.

Recommendations

Update WinRAR to the latest version: Immediately update all WinRAR installations to version 7.13 or later, which addresses CVE-2025-8088. Prioritize systems in government, law enforcement, and organizations operating in Southeast Asia.

Monitor Startup Folder Activity: Implement monitoring for unexpected file creation in the Windows Startup folder (%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup), as this is a key persistence mechanism used by the threat actor.

Detect DLL Sideloading Attempts: Deploy detection rules to identify DLL sideloading attempts, particularly focusing on legitimate executables (such as ZoomUpdate.exe, obs-browser-page.exe, and RemoveBackupper.exe) that load unexpected DLLs from non-standard locations.

Restrict Cloud Storage Access: Implement controls to monitor and restrict downloads from cloud storage platforms, such as Dropbox, particularly password-protected archives, as these are often used to deliver initial payloads while evading automated security scanning.

Network Segmentation: Implement network segmentation to limit lateral movement capabilities if initial compromise occurs, particularly for systems handling sensitive government and law enforcement data.

Review Pastebin Access: Monitor and consider restricting access to Pastebin, as the threat actor has used accounts on this platform (amaranthbernadine) to host AES encryption keys for payload decryption.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spear-phishing Attachment
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
		T1059.001: PowerShell
	T1203: Exploitation for Client Execution	
Persistence	T1547: Boot or Logon Autostart Execution	T1547.001: Registry Run Keys / Startup Folder
	T1053: Scheduled Task/Job	
Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1027: Obfuscated Files or Information	T1027.013: Encrypted/Encoded File
	T1140: Deobfuscate/Decode Files or Information	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1622: Debugger Evasion	
	T1055: Process Injection	T1055.012: Process Hollowing
	T1620: Reflective Code Loading	
Credential Access	T1056: Input Capture	
Discovery	T1057: Process Discovery	
	T1082: System Information Discovery	
Collection	T1113: Screen Capture	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1102: Web Service	T1102.002: Bidirectional Communication
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography
	T1105: Ingress Tool Transfer	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	8aacc30dac2ca9f41d7dd6d2913d94b0820f802bc04461ae65eb7cf70b53a8ab
SHA1	259819d1ae6421c2871f2ba0d128089036a0b29b, 92b8fa4d3e7f42036fc297a3b765e365e27cdce5, e34d7e8ba4bb949aa5c491b950ab30688d5dbadc, 19abb00922f4fb3d4b28713bc866a033a11c1567, 3a647d54f0866496d6d71c7b8e9f928759d535fd, 44ac2785b0352113ed12b856ec4507fa0b897adf, 53641ae0acb0fd986b30bdb1766086140abdc625, 7ed0e7b80d4b5cddf10b0a6907755c607f37d7fe, a80c9e1b3116f882d4f25e1934a2e890706ba44c, b0b95528f5df65140540e473a5ac477d7f4dff87, d70bad36a4060f93a3c5c9092bbf299c463a1451, d80edb2d04670d304713b148d6a721498f842376, ec61fd29b0ebc597847325a61aceac5eeab4ae2c, 1c1d53cb0f2a2d9b6d7ddb4ed55ed18880ae45e6, 3823415ce9d1408a6595035e1cb634b2e261e005, 40550c3696581a00b976adddbbef145f2531770e, 5670d4688b2ec8b414a96aa795d81b78580ae20b, 582d275c4f10c8632294cadcf56df13729612de2, 78066f82804410625f6cd02a913464e163c5613e, 85a31476dd35ff67439a2cbb4dea40e3223f8eaf, b93db4606ab2233a6d48b9658ab7ca432ba93985, c582718d37e9563f019e3ef78e736a0282203371, ccd6e41f343ed719ac61c05d0435a3c3bfd67d2a, e739b3cffbb94357390a0f451d8f4171fdb9200b, ed0232814fe9adb9fe62e04c8982cebf5c5e79ab, ff4e717f9fa54cbaadadf145433df4f8292c56c1, 00351add8e0bca838e8dac40875b8ad5195805bd, 481d50d5ab7c0a41a7c4fabb01b5c50c8f4fabf2, 718c5846d3b903e3e9e2df9281f5e25b371465f2, 9afadca9b2dad54004bd376dbee7e98c38dbdf50, b4dc300031edf5dd4968028146b0d608bdd975c5, c54a68d6bcc6d04ff08ad9619706e54923a20248, cd949663598c49141a98b438cf408113602e5c19, ddea99cb2db5e95552dccc8804125f19b30af536, 803fb65a58808fd3752f9f76b5c75ca914196305, 733714767a49c00c5c825c8e689da0c3bb23fbfa, 9905c672b9c32f7a09fbebb7b54e9371f08af354, d751647a2c831b4e20aba2aab9de7feb9c6a9e7d, e2520eb81665015778d915f0f0f749889a7fb1f5, e866edf14b208076d83417d9757056e7a12dca73

TYPE	VALUE
IPv4	92[.]223[.]120[.]10, 92[.]223[.]124[.]45, 92[.]223[.]76[.]20, 92[.]38[.]170[.]6, 93[.]123[.]17[.]151
Domains	dns[.]annasoft[.]gcdn[.]co, phnompenhpost[.]net, todaynewsfetch[.]com
URLs	hxxp[:]//dropbox[.]com/scl/fi/csggj44n9255y3vsjhh0p/wsNativePush[.]zip?rlkey=oaffvs9si6wkc6j4ccushn133&st=osdl9su7&dl=1, hxxp[:]//dropbox[.]com/scl/fi/ln6q8ip8k3dvx6xxyi71s/gs[.]rar?rlkey=w9vg1ehva23iitfdt5oh2x6cj&st=pwq86nfo&dl=1, hxxp[:]//dropbox[.]com/scl/fi/rl6nbtvfzllgovofmbdsm/FSTR_HADR[.]zip?rlkey=bql8d9zl3gz1ctfftbby6lob7&st=sc98u44d&dl=1, hxxp[:]//catalogs[.]dailydownloads[.]net/archives/microsoft/office/@MrPresident_001_bot[.]rar, hxxp[:]//daily[.]getfreshdata[.]com/dailynews/environment[.]enc, hxxp[:]//daily[.]getfreshdata[.]com/dailynews/key[.]txt, hxxp[:]//pastebin[.]com/raw/2AGrG4i1, hxxp[:]//pastebin[.]com/raw/ASXindCH, hxxp[:]//pastebin[.]com/raw/Z7xayGZ8, hxxp[:]//analytics[.]freshdatainsights[.]org/display/2025/uid_8oQRkgpvMSgmBFt9/WondershareApplicationManual[.]pdf, hxxp[:]//drive[.]easyboxsync[.]com/resources/channels/v7/cambodia64, hxxp[:]//get[.]storagesync[.]biz/resources/newspaper/2018/forecast2018, hxxp[:]//live[.]easyboxsync[.]com/resources/gup/notepad, hxxp[:]//news[.]dostpagasa[.]com/llehs/jdkasdnkaf[.]enc, hxxp[:]//softwares[.]dailydownloads[.]net/products/microsoft/office/product-key/DB2F[.]activation[.]key, hxxp[:]//updates[.]dailydownloads[.]net/docs/microsoft/office/Office_Activation_Manual_DB2F[.]pdf

Patch Link

https://www.win-rar.com/download.html?&L=0

References

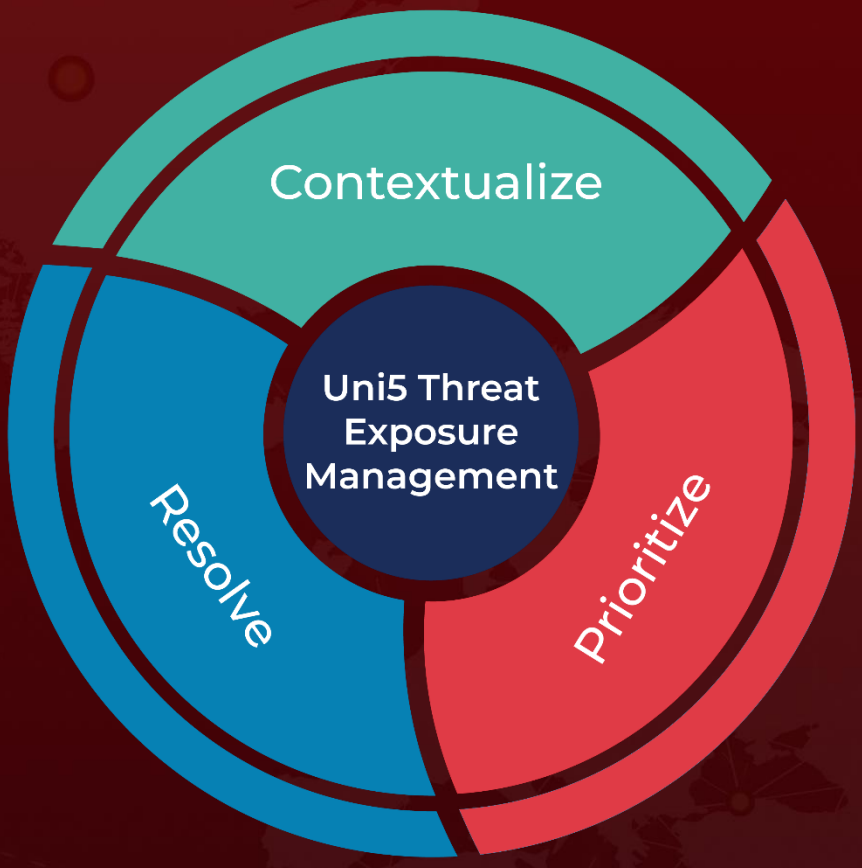
https://research.checkpoint.com/2026/amaranth-dragon-weaponizes-cve-2025-8088-for-targeted-espionage/

https://hivepro.com/threat-advisory/zero-day-in-winrar-actively-weaponized-by-multiple-threat-groups/

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

February 06, 2026 • 05:30 AM

© 2026 All Rights are Reserved by Hive Pro

More at www.hivepro.com