Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

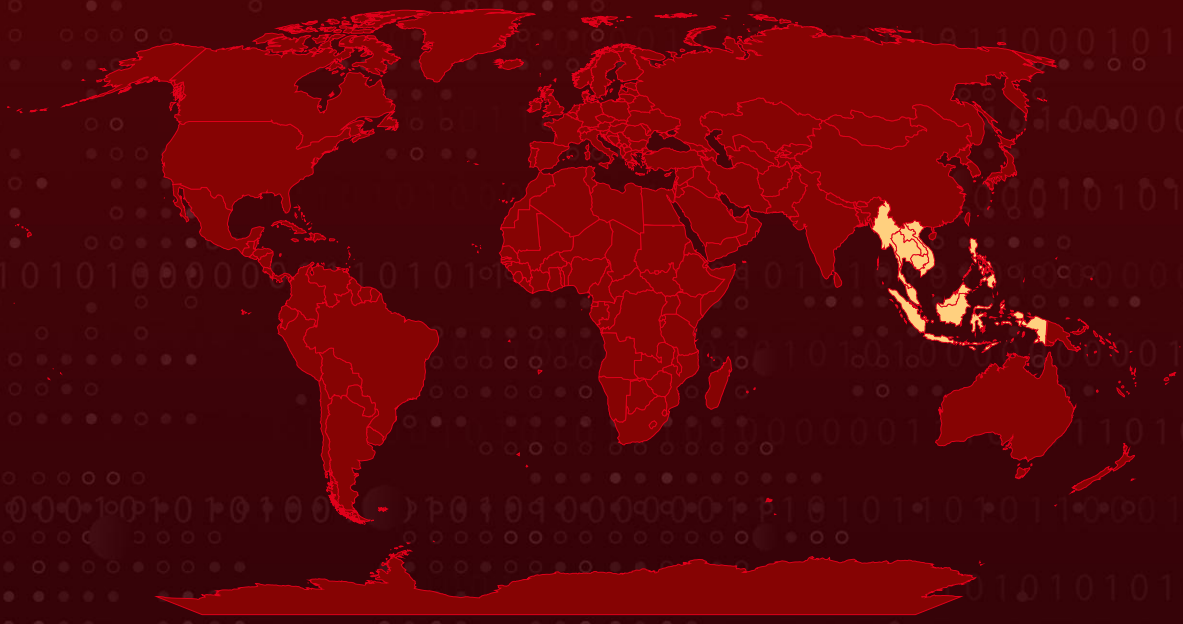
SparkRAT Ignites Cambodia via BYOVD Chain

Date of Publication	Admiralty Code	TA Number
August 28, 2026	A1	TA2026252

Summary

First Seen: Late June 2026
Targeted Regions: Southeast Asia
Targeted Platform: Windows
Targeted Industries: Government, Public Health, Real Estate
Malware: SparkRAT
Attack: A multi-stage campaign targeting Cambodian individuals and organizations delivers SparkRAT through phishing archives that carry Inno Setup installers with localized lures. Execution abuses DLL sideloading via a signed Tencent binary, decrypts stages hidden inside PNG files, patches AMSI and ETW, and installs the vulnerable ardrv.sys driver (CVE-2026-36425) to terminate security products in kernel mode. The final SparkRAT payload is reflectively loaded into ctfmon.exe and communicates with sx.nuihuw.com over port 443.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-36425	OPSWAT AppRemover Arbitrary Process Termination Vulnerability	OPSWAT AppRemover (ardrv.sys)	✗	✗	✓

Attack Details

#1

Individuals and organizations across Cambodia are the intended targets of a newly observed campaign that ultimately drops SparkRAT, an open-source Go-based remote access trojan. The campaign begins with a phishing-style delivery of compressed archives to Cambodian recipients. Each archive contains an Inno Setup executable dressed up as a document, with lure themes tailored to local interest such as government advisories, COVID-19 announcements, dental examination records, real estate listings, and promotional offers. A representative sample carries the filename "Cambodian Government Notice on COVID-19 Prevention and Control (July 7).docx.exe." When the victim runs the installer, it silently drops staging directories under C:\Drivers along with a signed Tencent binary (F7u00ex.exe) and a malicious DLL (WfoY.qf). The signed executable is then abused to sideload the malicious DLL and kick off the infection chain.

#2

Once the loader is sideloaded, it registers a Vectored Exception Handler and triggers a debugbreak() exception to jump into its main routine, an unusual control-flow trick that also frustrates simple debuggers. Before continuing, it runs a timing-based anti-sandbox check to filter out analysis environments that manipulate sleep delays. From there, the loader parses encrypted shellcode hidden inside the IDAT chunks of four PNG files, decrypts each stage at runtime, and injects the payloads into legitimate Windows processes vssvc.exe, svchost.exe, and ctfmon.exe. Persistence is set up in parallel through a Windows service named "TaskHandler" created via sc.exe and a scheduled task of the same name that runs F7u00ex.exe at system start under NT AUTHORITY\SYSTEM. The final embedded payload, reflectively loaded into ctfmon.exe, is identified as SparkRAT, an open-source Go-based remote access trojan.

#3

Rather than moving laterally across a network in the traditional sense, this campaign focuses on elevating privileges and dismantling on-host defenses. When the loader is not already running as SYSTEM, it searches for winlogon.exe, opens its process token, and impersonates the SYSTEM token to gain higher rights. It then strips key privileges from any Huorong Internet Security tokens it finds and sets their integrity level to Untrusted, effectively blinding the endpoint product. In parallel, the shellcode patches AMSI and ETW to suppress script-scanning and telemetry, and adds Microsoft Defender registry exclusions for the staging paths and injected host processes. The most impactful step is a Bring Your Own Vulnerable Driver (BYOVD) routine that installs ardrv.sys, the OPSWAT AppRemover driver affected by CVE-2026-36425, and invokes its unprotected IOCTL 0x2420031 to terminate security processes from 360 Total Security, Huorong, Microsoft Defender, and Tencent PC Manager in kernel mode. A user-mode cleanup path that enables SeDebugPrivilege and calls TerminateProcess handles anything the kernel path misses.

#4

With the environment stripped of defenses, the reflectively loaded SparkRAT payload takes over. It decrypts its embedded configuration using AES-CTR and validates the result against a stored MD5 hash before loading it into memory. The active configuration points to a primary command-and-control server at sx.nuihuw.com over port 443, with nuihuw.top:443 acting as a failover endpoint if the primary becomes unreachable. Each implant is identified by a unique UUID and communicates using a 256-bit key. Because SparkRAT is a full-featured Go-based RAT, the operators gain interactive remote access to the compromised host, and file transfer, shell command execution, and follow-on data theft all run through this same encrypted HTTPS channel, blending exfiltration into normal-looking outbound traffic on port 443. The activity is tracked as an unattributed cluster with possible Chinese-language development or deployment links and loose operational overlaps with the broader Silver Fox ecosystem, held at low confidence.

Recommendations

Restrict Vulnerable OPSWAT Driver: Audit endpoints for the affected version of ardrv.sys shipped with OPSWAT AppRemover, remove it where it is not required, and block the driver hash in EDR and application-control policies until a vendor-patched build is deployed.

Block Known IOCs at the Perimeter: Add sx[.]nuihuw[.]com and nuihuw[.]top to DNS sinkholes and outbound proxy blocklists, and import the listed SHA-256 hashes into EDR, AV, and email-gateway rulesets so any sample from this cluster is quarantined on first contact.

Enable Microsoft Vulnerable Driver Blocklist: Turn on the Microsoft Vulnerable Driver Blocklist through WDAC or HVCI so drivers like ardrv.sys, zam64.sys, and BootRepair.sys referenced by this loader cannot be loaded, even by an installer running with local administrator rights.

Hunt for Persistence Artifacts: Search for Windows services or scheduled tasks named "TaskHandler," staging directories under C:\Drivers\mQm and C:\Drivers\XF, and Microsoft Defender exclusions covering C:\Drivers or system binaries such as vssvc.exe and ctfmon.exe.

Harden Email and Attachment Defenses: Deploy attachment sandboxing that can detonate compressed archives containing Inno Setup installers, and block or warn on double-extension filenames such as ".docx.exe" at the mail gateway.

Raise Awareness on Localized Lures: Train users, especially those in Cambodian government, healthcare, and real-estate sectors, to recognize lure themes that impersonate official notices and to verify unexpected government or health documents through official channels before opening them.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1566: Phishing	T1566.001: Spearphishing Attachment
Execution	T1204: User Execution	T1204.002: Malicious File
	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
Persistence	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1053: Scheduled Task/Job	T1053.005: Scheduled Task

Tactic	Technique	Sub-technique
Privilege Escalation	T1134: Access Token Manipulation	T1134.001: Token Impersonation/Theft
	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1055: Process Injection	
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
		T1562.006: Indicator Blocking
	T1112: Modify Registry	
	T1497: Virtualization/Sandbox Evasion	T1497.003: Time Based Evasion
	T1027: Obfuscated Files or Information	
	T1140: Deobfuscate/Decode Files or Information	
Discovery	T1518: Software Discovery	T1518.001: Security Software Discovery
	T1057: Process Discovery	
Command and Control	T1071: Application Layer Protocol	T1071.001: Web Protocols
	T1573: Encrypted Channel	T1573.001: Symmetric Cryptography

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA256	f7b9ab6c6d46b9b82c9c5a4deebf2f77ef1cbfffe2bf11c5c412f9f4f416d9ab, 0a050e1d5338b936037f0928039c26893a553c3170b16b82bf75a9113b34a52f, 7504887e1e195ad585cffa5b6a5034161a7cc49f351123d60def79302bdb8326, 7ef1757e773270f5f0799797861290097a202dc1fe7a1eab13373d8a132da0d0, 0f0f06669c4bf4d222384b23766b93fb2f8a370047af50a8d5009564959f6171, 603247ade94f89f46d781b707fad7a73f959a7ea6553e1447753e52a2ea4b694, 14eae85f027a94dbd1814f0925c5ec541ba8dfe6a850ab4004cfc95d67a1516d, 61a061293a2d872267a08ff66e57d3e01113fd0a395be6661960e69d15a7cca3, 91ddd3c7a02138fc033a3337245a6adc9f8a5aeb4953f07e689c119b40d7dfaa, d0c13e5b3c097143129e6d2bfc698570f3f2c0325cc2b0a1dacbacbf87f25330, d8b0b96a9afd7a81807e225ae9979438ecf53a02c87995dac31723308d05722c, dd12a110462803cc2f930b6f53920c391e1e50424dfb64e084649d7124ff8d82, dedd917feb42d18a3d0b927d4bcfadd5248a7291a76ad43d502087b5c23c7b89, fc664ae8c0efe751bb05bca24d5ff0f9295bd85d4e70d1f64f687c8b17002ca7, 03d763330b711c6c933883e6cc9e11b8ba2eac3845b01798beddaef998b2c017, 2b676d28b2fdcc062ae6a3c1dd590001c9f80a417a510cc2ebbfe25c33cc020a, 2e5e5f7590bd34fd6883cc488243f24d536a0b9f27f63c64420052471c58ecaf, 37c463e9d3e629e29699bf65279b9996dd5efb88921d57d2892fc33ef6efec25, 4088200eb4e87a335ab600f14c22d8f7305f8a2a7e58e825e789f69ba2bf1f93, 49a53cd161508c5fd690575b013f1b484db77ee94a4adf2bbd52e08418097f0f,

TYPE	VALUE
SHA256	541fedb12cd4fa6a21be87c244f3ef09b7ab8e6e3031fd090f4848989854deca, 54f3e991b892f61dfa67143d319a6a0fedf19a9c9f9bef2cba72becebfad2b2c, 5512d1e7545adf6af071698cd3d0124e2044bb670eef761179a2d14ad2bbda5a, 635c9cccbc247c655971f8c7efb05e7418707614b1b2baa9c07cada7ece75ea6, 6adb46283b92308d57b32cd5c442f6b7852b960235265d97b2f6b4ea7b4635d3, 6c1c3e7b3ba87781f34c047b28418f7745a9c3ad45eb9a7ec00da8a9893e6bd7, 8009e75fcb20fb1faa0f13f4d4f1cd3d5eff2ed025e0f81a1da9ea31d93e0dee, 8b39e5b5ab169ba07eec0d9c421d07ae96df4a16cc2f93f4ca0d521bdb3164bb
Domains	sx[.]nuihuw[.]com, nuihuw[.]top
Filenames	Cambodian Government Notice on COVID-19 Prevention and Control (July 7).docx.exe, F7u00ex.exe, WfoY.qf, 56360VK1ES8.yvap, BssBfeFFoA3A.nz, cnV.rb, d7zzQhzRglBv.es, ardrv.sys

Patch Link

https://www.opswat.com/products/oesis-framework/application-removal

References

https://www.acronis.com/en/tru/posts/cambodia-focused-cluster-uses-multi-stage-infection-chain-with-localized-lures/

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

August 28, 2026 • 08:30 AM

More at www.hivepro.com