Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

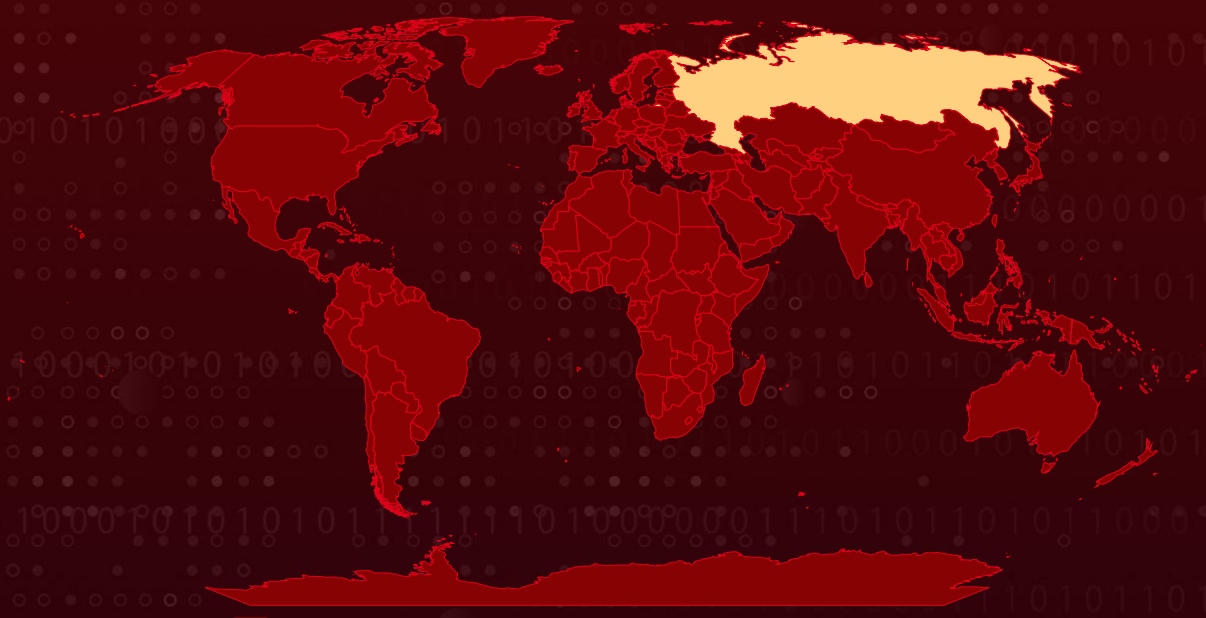
HelloNet Campaign Targets Russian Infrastructure via ViPNet Update Abuse

Date of Publication	Admiralty Code	TA Number
July 22, 2026	A1	TA2026208

Summary

First Seen: May 2026
Targeted Country: Russia
Campaign: HelloNet campaign
Targeted Platform: Windows
Targeted Product: InfoTeCS ViPNet
Targeted Industries: Government, Energy, Transport, Education, Logistics
Threat Actor: Unknown Chinese-speaking APT group
Malware: HelloInjector, HelloProxy, HelloExecutor, HelloCleaner, HelloBackdoor
Attack: HelloNet is an ongoing espionage campaign, active since at least May 2026, that abuses the trusted update mechanism of the ViPNet secure-networking suite to plant a modular implant chain inside large Russian government and critical-infrastructure organizations. By sideloading a malicious DLL through a signed update process, the operators gain stealthy, persistent, high-privilege access while blending into legitimate software behavior, then use purpose-built tools to proxy traffic, run reconnaissance, tunnel data out over SSH, and scrub logs to cover their tracks. Attribution is low confidence, tentatively pointing to a Chinese-speaking group based on soft artifacts. The campaign's abuse of a security product's own update pipeline makes it a serious supply-of-trust threat that conventional signature- and vulnerability-based defenses are unlikely to catch.

Attack Regions



Attack Details

#1 HelloNet is an advanced persistent threat campaign disclosed in public reporting on 16 July 2026, notable for weaponizing a trusted security product against the very organizations it is meant to protect. Rather than exploiting a vulnerability, the operators abused the update mechanism of ViPNet, a secure-networking software suite, to deliver a modular implant chain into large enterprises. The campaign has been active since at least May 2026 and remained ongoing at the time of publication.

#2 At its core, the operation is a supply-channel and living-off-trust attack. ViPNet is widely deployed to build encrypted networks across government and critical infrastructure, so its update system is inherently trusted and its executables are digitally signed. By inserting themselves into this pipeline, the attackers gained a stealthy, high-privilege foothold that blends with legitimate software behavior, a pattern already observed a year earlier when a ViPNet-mimicking backdoor was documented, signaling sustained adversary interest in this vector.

#3 The attack chain begins with a malicious wtsapi32.dll planted in the ViPNet Update System directory, which is sideloaded by the signed update binary itcsrvup64.exe at system startup, establishing persistence through a trusted process. This loader (HelloInjector) injects a payload into a netsvcs svchost.exe instance using native NT APIs (NtWriteVirtualMemory, NtCreateThreadEx).

#4 The main payload, HelloProxy, hooks network-related APIs using a legitimate API-hooking library and intercepts AFD IOCTLs to hinder user-mode security tools, while listening on ports 5003 and 5060 behind a handshake-gated C2. From there, HelloExecutor performs internal reconnaissance and harvests ViPNet Administrator and Client export paths, a Rust-based HelloBackdoor on port 443 enables command execution and file transfer, and an SSH reverse tunnel via a renamed legitimate tunneling utility provides persistent egress. Finally, HelloCleaner scrubs ViPNet log files to erase traces, delivering impact through persistent remote access and anti-forensic cleanup.

#5 Targeting spans government, energy, transport, education, logistics, and industry, a critical-infrastructure footprint concentrated on large Russian organizations. Attribution remains low confidence: reporting tentatively points to an unknown Chinese-speaking group based on two soft artifacts, both flagged as possibly unintentional with false flags not excluded.

#6 In conclusion, HelloNet is a disciplined, trust-abusing intrusion set built for stealth, persistence, and cleanup rather than noise. Defenders should prioritize hunting for anomalous wtsapi32.dll in the ViPNet directory, detecting renamed tunneling binaries on their original PE metadata, and monitoring the handshake-gated C2 patterns on ports 5003/5060 and the HelloBackdoor activation string on port 443.

Recommendations

Restrict and Monitor the ViPNet Update Directory: Treat C:\Program Files (x86)\InfoTeCS\VIPNet Update System as a high-value path and alert on the creation of any .dll or .exe there, especially wtsapi32.dll, that lacks a valid InfoTeCS signature, since the attackers persist by sideloading an unsigned DLL into the update service.

Validate ViPNet Update Process Signatures: Detect launches of Itcsrvup64.exe or Itcsrvup.exe that carry an invalid signature or a signature without InfoTeCS as the manufacturer, and flag any child processes these update executables spawn that are not the expected ViPNet binaries (wmail, monitor, itcsrvup64).

Hunt for svchost Injection from the Update Service: Monitor for process injection into svchost.exe originating from itcsrvup64.exe, which is the core behavior of HelloInjector; the legitimate update component has no reason to write memory into system processes.

Alert on Anomalous svchost Behavior: Watch for svchost.exe instances spawning reconnaissance commands (net use/group, sc query/start/stop, ping, ipconfig, netstat) or performing file and process creation, as HelloExecutor operates from within an injected svchost context.

Detect Renamed PuTTY/Plink Tunnels: Identify SSH tunneling tools by their original PE metadata rather than filename, since the operators renamed Plink/PuTTY to frontpage.exe and pagent.exe; alert on command lines containing reverse-forward patterns such as port:address:port regardless of the executable name.

Block and Watch Known C2 Infrastructure: Block outbound connections to 5[.]39[.]253[.]206 and 176[.]32[.]34[.]135 and inspect for the non-standard tunnel and listener ports (5003, 5060, 443 with the HelloBackdoor activation string) referenced in this advisory.

Adopt a Layered Detection Architecture: Combine endpoint (EDR), network (NDR/IDS), and SIEM detections to catch this intrusion set across its lifecycle, since no single stage, sideloading, injection, tunneling, or C2, is reliably visible from one control alone.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Persistence	T1574: Hijack Execution Flow	T1574.002: DLL Side-Loading
	T1543: Create or Modify System Process	T1543.003: Windows Service
Defense Evasion	T1055: Process Injection	
	T1036: Masquerading	T1036.005: Match Legitimate Name or Location
	T1562: Impair Defenses	T1562.001: Disable or Modify Tools
	T1070: Indicator Removal	T1070.004: File Deletion
	T1112: Modify Registry	
	T1218: System Binary Proxy Execution	
Execution	T1059: Command and Scripting Interpreter	T1059.003: Windows Command Shell
	T1569: System Services	T1569.002: Service Execution
Discovery	T1016: System Network Configuration Discovery	
	T1018: Remote System Discovery	
	T1082: System Information Discovery	

Tactic	Technique	Sub-technique
Discovery	T1057: Process Discovery	
	T1007: System Service Discovery	
	T1083: File and Directory Discovery	
Collection	T1005: Data from Local System	
	T1074: Data Staged	T1074.001: Local Data Staging
Command and Control	T1105: Ingress Tool Transfer	
	T1090: Proxy	
	T1572: Protocol Tunneling	
Lateral Movement	T1021: Remote Services	T1021.004: SSH

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	16C211C96735F2FAE9361B89BD7A31BF, 1BFE2B9493128574907A8279256A8BCC, f9eed2f0158dc98e7012fb809152209c, 6001829A128FE264B4403138700C11A8, EE4FF46DDD8489E81447962F927BC3F6, 41c938b3cd7e55d4077e34976929b140, B103CD21280B4061F88B2BCC51394894, 9F5606A0755BC633B9BD7DB6D179C09E, 0CFDFFC56F0FA325D0C4D24780B46597
SHA256	68b4c76a2280e3c31130d4de12b12dfd479a476f347f5b4a58cb2483d74aba7e, ffdc194775b2904564bbbd1cf0eb01d1a01f83ef5197d1612b6e2d69de7a4732
IPv4	5[.]39[.]253[.]206, 176[.]32[.]34[.]135
Filenames	wtsapi32.dll, puh.exe, store.exe, frontpage.exe, pagent.exe
File Paths	C:\users\public\music\frontpage.exe, C:\users\public\tesh4RPC.txt, infotecs\vipnet client\puh.exe, infotecs\vipnet client\store.exe

References

https://securelist.com/tr/hellonet-vipnet/120700/

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

July 22, 2026 • 07:30 AM

More at www.hivepro.com