Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

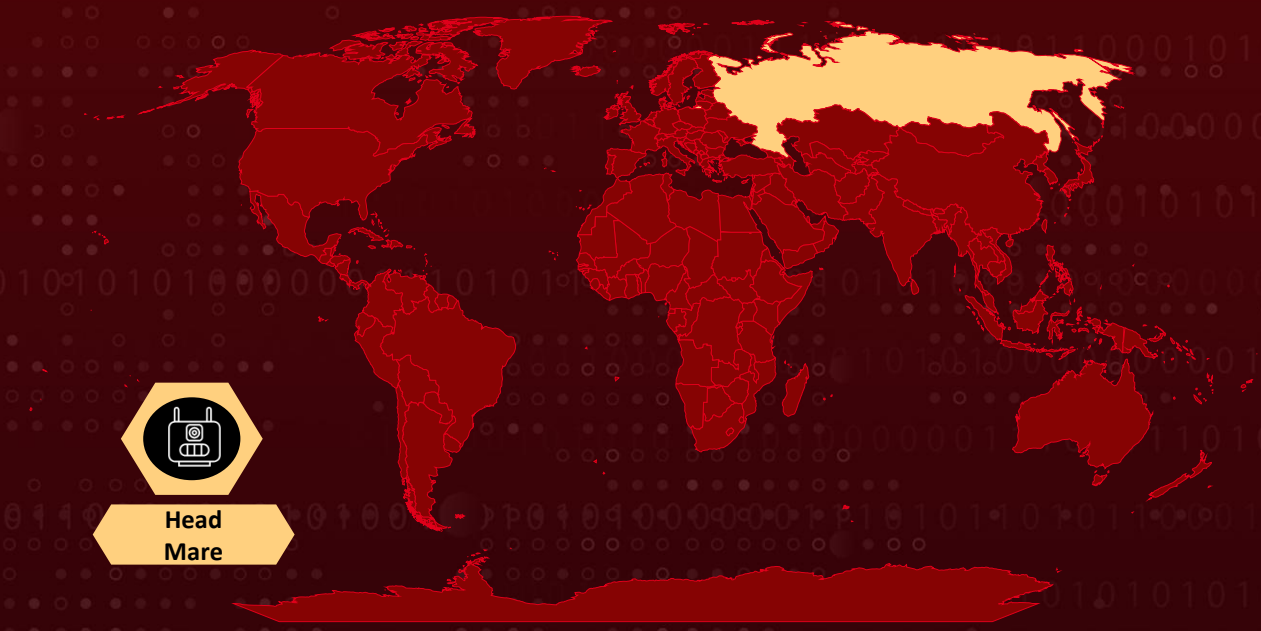
Head Mare Chains TrueConf Server Flaws to Drop PhantomCore and PhantomGraph

Date of Publication	Admiralty Code	TA Number
August 10, 2026	A1	TA2026228

Summary

First Seen: July 2026
Targeted Region: Russia
Targeted Platforms: Windows, Linux
Targeted Products: TrueConf Server, TrueConf Client
Targeted Industries: Instrumentation, Electronics, Transportation, Energy, IT, Software Development
Threat Actor: Head Mare
Malware: PhantomCore, PhantomGraph
Attack: Head Mare is breaking into unpatched TrueConf video conferencing servers by chaining two vulnerabilities that let them run code with SYSTEM privileges. Once inside, they plant a web shell, swap the legitimate TrueConf Client installer for a trojanized one carrying the PhantomCore backdoor, and deploy a second backdoor, PhantomGraph, that uses Microsoft OneDrive as its command-and-control channel. Users pull the poisoned installer as a routine "update," turning a trusted meeting tool into a delivery vehicle for credential theft and remote access.

Attack Regions



Attack Details

#1

Head Mare is actively compromising unpatched TrueConf servers by connecting to TCP port 4307, a service that is open by default and reachable without any authentication. From there the group chains two vulnerabilities, tracked internally by Kaspersky as KLCERT-26-057 and KLCERT-26-058. The first lets the attacker push a malicious script and run it inside TrueConf's sandboxed environment, while the second breaks out of that sandbox to execute commands directly on the underlying operating system. The flaws affect TrueConf Server 5.3.x before 5.3.9, 5.4.x before 5.4.9, 5.5.x before 5.5.5, and older builds; the vendor patched them on June 18, 2026, and the attacks were uncovered the following month. Beyond exploiting the server directly, Head Mare also reaches victims through phishing, other public-facing web servers, and trusted contractors.

#2

After escaping the sandbox, the attackers gain code execution as NT AUTHORITY\SYSTEM and overwrite the server's public\js\locale.php file with a web shell that gives them durable remote control. They use that web shell to map the IT environment, pull privileged access to the TrueConf database, and replace the legitimate TrueConf Client installer with a trojanized, unsigned build that carries the PhantomCore backdoor. PhantomCore keeps its foothold through a COM CLSID registry key so it loads automatically when the system starts. Alongside it, Head Mare deploys PhantomGraph, a backdoor deliberately split into two modules: SysExcSvc.dll fetches commands and returns their output through a Microsoft OneDrive account acting as command-and-control, while SysReadSvc.dll reads, executes, and stores the results. Both are registered as Windows services through a Base64-encoded PowerShell command, and the two-part design is meant to slip past EDR detection.

#3

Working through PhantomGraph, the operators dumped the memory of the LSASS process to harvest credentials and ran quick reconnaissance with hostname and whoami to profile each compromised host. The blast radius reaches well beyond direct customers, because employees at organizations that do not even run TrueConf themselves can be infected simply by joining an online meeting on a compromised counterparty's server and downloading the poisoned installer as an update.

#4

For command-and-control and to move stolen data, PhantomGraph tunnels its traffic through a legitimate Microsoft OneDrive account, blending exfiltration into normal cloud activity, and the operators also stood up a reverse SSH tunnel for interactive access. Detected overlapping tools utilizing GitHub as an alternative command-and-control channel and identified an ELF rootkit deployed on Linux hosts. The analysis also highlights code similarities between PhantomGraph and PhantomCore, linking both clearly to Head Mare's arsenal. Multiple campaigns built on this toolkit are currently active against Russian organizations across several sectors.

Recommendations

- **Update TrueConf Server Immediately:** Upgrade every TrueConf Server instance to version 5.3.9, 5.4.9, or 5.5.5, released on June 18, 2026, which closes the KLCERT-26-057 and KLCERT-26-058 vulnerabilities exploited in this attack.
- **Verify Client Installer Signatures:** Confirm that any TrueConf Client distributed from your server carries a valid TrueConf digital signature, since the malicious installers seen in this campaign are unsigned. Authenticity can also be checked against the vendor's official download page.
- **Restrict Access to Port 4307/TCP:** Limit exposure of TrueConf's default 4307/TCP service to trusted management networks, as attackers use this port to reach the server without authentication.
- **Watch for LSASS Access and SSH Tunnels:** Alert on LSASS memory dumping, including access via comsvcs.dll, and on unexpected outbound SSH tunnels, both of which were used after compromise in this campaign.
- **Scrutinize Counterparty Meeting Installers:** Treat any client downloaded when joining an external partner's TrueConf meeting as untrusted, because a compromised counterparty server can push infected installers to your staff.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1199: Trusted Relationship	
	T1566: Phishing	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.003: Windows Command Shell
Persistence	T1505: Server Software Component	T1505.003: Web Shell
	T1543: Create or Modify System Process	T1543.003: Windows Service
	T1546: Event Triggered Execution	T1546.015: Component Object Model Hijacking
Privilege Escalation	T1068: Exploitation for Privilege Escalation	
Defense Evasion	T1027: Obfuscated Files or Information	
	T1036: Masquerading	
Credential Access	T1003: OS Credential Dumping	T1003.001: LSASS Memory
Discovery	T1082: System Information Discovery	
	T1033: System Owner/User Discovery	
Command and Control	T1102: Web Service	T1102.002: Bidirectional Communication
	T1572: Protocol Tunneling	
Exfiltration	T1041: Exfiltration Over C2 Channel	

Indicators of Compromise (IOCs)

TYPE	VALUE
MD5	4d27b4eb1c5dbb3d8160f29b8119523e, 748c9f8cb1065000616204935f96207f, c5a460e4e68a088f6e51b2c6474642ec, 129462164a7d52e9ea8560b60f0412c5, ec0bf4a2186a88874e9f26f07cfeb532, b348642146ea34771e5785c5857950f5, c915cb6c2aeb863ee8479238e1644217, 0e79996d9483d1e44fea32b0a48c2c19, 2bb75c20e778eb5c416965bd4d4259b1, b3a6fee3307f1c26841fd5c603e2b013, 8fcc3e4ccbf1725d9989fb464abf3561, 489f43be558b2679284ceabed7adc4f3, dd1fd2b459b97b7d59375cb8383cd19a, 0e4541c3153ec5ed01497f19cf4f63d0, 12d4e8f5295f2ef7e0f9bfc0f4830939, 7f267006cac10f341c356b62fe493527, ee2861d5965e8730708cd1da8a93fa4c, c3a2abe8756910f42582b04a44ea3514, 43f435c3c437bc879a2d7d4634f43494, aee9642b45b099cb7f3053b9b680b425
IPv4	81[.]177[.]32[.]12, 194[.]87[.]239[.]71, 194[.]87[.]93[.]153, 38[.]244[.]205[.]244, 31[.]59[.]102[.]61
Domains	penzadogshelter[.]site, trendy-market[.]site, bright-deals[.]site, nova-stream[.]site, rinomobile[.]ink, urbanpixel[.]store, flexish[.]shop, media-hub[.]today, cosmetic-deals[.]store, vks[.]gossopka[.]forum

TYPE	VALUE
File Path	C:\Windows\System32\inetsrv\SysExcSvc.dll, C:\Windows\System32\inetsrv\SysReadSvc.dll, C:\Windows\System32\inetsrv\graphi-refresh.dat, C:\Windows\System32\inetsrv\share\input_*.txt, C:\Windows\System32\inetsrv\share\output_*.txt, %TEMP%\cmd_cmd_*.bat, %LOCALAPPDATA%\TrueConf\Client\api-ms-win-crt-time-l1-1-0-2.dll, /etc/systemd/system/omicluster.service, /etc/systemd/system/schedul2-bin.service, /opt/acronis/bin/schedul2-bin, /omi/bin/omicluster, /usr/lib64/libzvbi-tchain.so.2, /var/tmp/cx2
Registry Key	HKEY_CURRENT_USER\Software\Classes\CLSID\{0340F119-A598-4ed9-B0AC-6F6A12D3E755}\InprocServer32
SHA256	0ED9306DEABDDAA587AD75D0775F7E63B27857A13ADCC870DC9F8C92A9DDC6DA, E66BBB6C651B5AB839434B8E62F502169F35894E28DBE9F3275911582ECCD250, B9E4052B310F9451ECA9784A4A33BF5282D1BD07E3359EBA9648BE625E2E40DD, 9464A414FD542F6E6B6245669EE947DFCBC9BA7C0641195C1E60E5C569B7269B, 23176FF5E92798B97341440A2A76F782729193C6FF65F71B8B6A315A2D507674, 171856ED2026C0099F7D84E06963D25B35627CFE45674BC82AB0F254A639613F, 3DB4B29804E36890B431D7C71796DF63A3DE367A2482FA588AEDE9E3C4FE6D3E, 2B1DD2B3C8508D5116BC3883FF619FD752EB662FD81CBA176CFE412E97A4BCBB, A9D5F0E32DD7E0B1F7B0A1D901212F2BF9150C2E37EE60DCBBD53FC18D3C8DD2, 72029A4D4790784DD3029D13E73F57494DCB8F8187CA234B131E2B825BD84336, CEEA2F175EAA02919E8B5161C2ECF585DE3E8B6D586BCA8046EEE2E3F4EFA386, EF8D99FDCD6E184F6DC5E0F57E1A78C6DF542505436FDE66D70BAAB994470B7B, 157103FF2306A8EF27F539307AA8CC3CDA392320770C0F434F00B02AEEB1DCAE,

TYPE	VALUE
SHA256	4463687E07B1566323A84209972DE041031972F2A02DFCD6F1F0699C335EC5A6, 21AB543D257FA6A71B5087F533BFCE54211D20D5FBA003F2FF7458F8FE695640, 0FCE4B732CE10C72093587E82CA9747A885430E366934DDC27E437443FF0CC0E, 0A8709032E890EE923D00A98C81DD188F1A8D0D3EA8DF5A65663AF5521C052CC, 91AA91ADB87674B5357CFA07A9B9C1C657EA052D081C6754C109CB64D187DBCF, 19262A37F9E5ED51A274B77BC73C3F9C2C2C7A2A567FA958ABF2D4FFEB426F12, 632F6D47E1CFBD4FABE2E85E9BA38EBA7DA33B0BADEC568935FA132E5A3A8160

References

https://securelist.ru/tr/head-mare-targets-trueconf-server-with-phantomcore/116557/

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 10, 2026 • 08:30 AM

More at www.hivepro.com