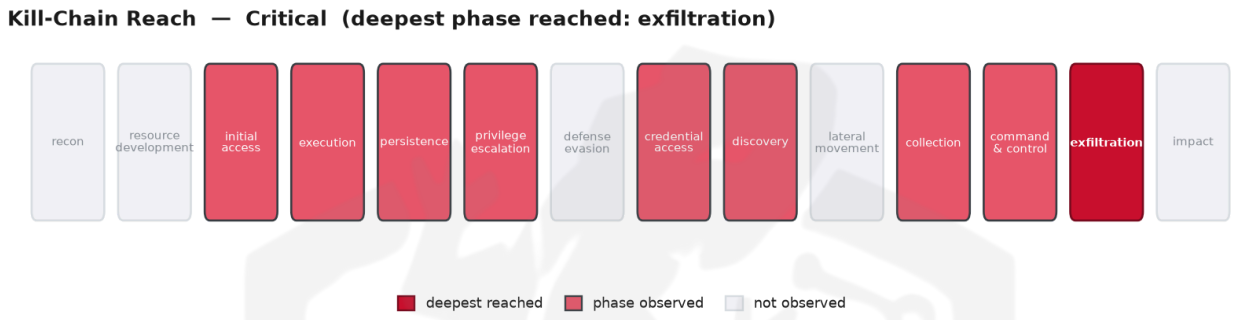
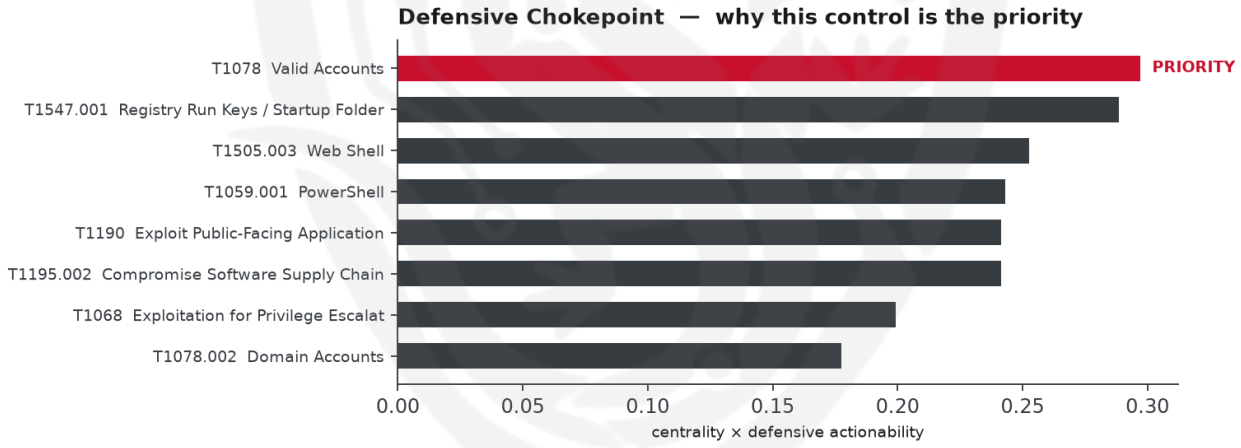
THREAT REPORT: HEAD MARE EXPLOITS TRUECONF SERVERS TO DELIVER PHANTOMCORE

Visual Summary



How far down the attack chain this campaign reached; deepest phase in crimson.



The control that most disrupts the attack (priority in crimson).

Summary

Head Mare leverages unpatched TrueConf video-conferencing servers to deliver the PhantomCore and PhantomGraph malware families to conference participants. The campaign’s victims are not identified in the source, indicating a broad, opportunistic targeting approach. The activity culminates in credential theft, system discovery, and data exfiltration to cloud storage. Priority should be given to enforcing multi-factor authentication on all accounts, disabling dormant or over-privileged accounts, and alerting on impossible-travel or anomalous logons.

Threat Overview

The source attributes this activity to Head Mare. The adversary distributes the PhantomCore and PhantomGraph malware families by exploiting vulnerabilities in unpatched TrueConf server installations.

No specific CVE is cited, and the victim profile is unspecified beyond participants of TrueConf-based video conferences.

Attack Chain and Priority Control

The observed attack chain begins with exploitation of the public-facing TrueConf application (T1190) to gain initial access, followed by deployment of a web shell (T1505.003) and execution of PowerShell scripts (T1059.001). The payload is deobfuscated (T1140) and installed as a Windows service (T1543.003) with persistence via registry run keys (T1547.001). The malware conducts system information discovery (T1082), file and directory discovery (T1083), and credential dumping (T1003) while keylogging (T1056.001). Valid accounts are leveraged to move laterally (T1078 Valid Accounts), and data is exfiltrated to cloud storage (T1567.002) using dead-drop resolvers (T1102.001).

Priority technique: T1078 Valid Accounts
Priority control: Enforce MFA on all accounts; disable dormant and over-privileged accounts; alert on impossible-travel and anomalous logons.

Infrastructure and Corroboration

The source's enrichment indicates that the malicious infrastructure is hosted by several providers, including JSC MediaSoft Ekspert, CGI Global Limited, Scalaxy B.V., and JSC RTComm.RU. AbuseIPDB reports no high-confidence malicious indicators associated with the observed IPs, and abuse.ch does not corroborate any additional malware families.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1056.001 Keylogging
- T1003 OS Credential Dumping
- T1543.003 Windows Service
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1505.003 Web Shell
- T1070.001 Indicator Removal
- T1083 File and Directory Discovery
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1078 Valid Accounts
- T1068 Exploitation for Privilege Escalation
- T1027 Obfuscated Files or Information

- T1195.002 Compromise Software Supply Chain
- T1567.002 Exfiltration to Cloud Storage
- T1078.002 Domain Accounts
- T1071.001 Web Protocols
- T1564.001 Hidden Files and Directories
- T1102.001 Dead Drop Resolver

Analytical Scores

- Priority technique (graph chokepoint): T1078 Valid Accounts (centrality 0.2973).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4609; reference threshold tau = 0.6).
- These are behavioural resemblances for defensive playbook cross-referencing, not an identity assessment. Where the source pulse names an actor, that attribution is authoritative; the overlaps below neither confirm nor contest it.

Nearest historical profiles by behavioural overlap (resemblance only):

Historical Profile	Behavioural Overlap
Threat Group-3390	0.4609
APT18	0.4303
BlackByte	0.427
Tropic Trooper	0.4148
APT32	0.3901

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.

Indicators of Compromise (defanged — non-clickable)

The network and file indicators observed in this activity are listed below for blocklisting:

Type	Indicator	Context
IP	194[.]87[.]239[.]71	AbuseIPDB 0% (RU) · AS48347 JSC MediaSoft Ekspert

Type	Indicator	Context
IP	194[.]87[.]93[.]153	AbuseIPDB 0% (RU) · AS48347 JSC MediaSoft Ekspert
IP	31[.]59[.]102[.]61	AbuseIPDB 0% (LV) · AS56971 CGI Global Limited
IP	38[.]244[.]205[.]244	AbuseIPDB 0% (FI) · AS58061 Scalaxy B. V.
IP	81[.]177[.]32[.]12	AbuseIPDB 0% (RU) · AS8342 JSC RTComm.RU
Domain	penzadogshelter[.]site	
Domain	urbanpixel[.]store	
Domain	vks[.]gossopka[.]forum	
Hash	0e4541c3153ec5ed01497f19cf4f63d0	
Hash	0e79996d9483d1e44fea32b0a48c2c19	
Hash	129462164a7d52e9ea8560b60f0412c5	
Hash	12d4e8f5295f2ef7e0f9bfc0f4830939	
Hash	2bb75c20e778eb5c416965bd4d4259b1	
Hash	43f435c3c437bc879a2d7d4634f43494	
Hash	489f43be558b2679284ceabed7adc4f3	
Hash	4d27b4eb1c5dbb3d8160f29b8119523e	
Hash	748c9f8cb10650006162049 35f96207f	
Hash	7f267006cac10f341c356b62fe493527	
Hash	8fcc3e4ccbf1725d9989fb464abf3561	
Hash	aee9642b45b099cb7f3053b9b680b425	
Hash	b348642146ea34771e5785c5857950f5	
Hash	b3a6fee3307f1c26841fd5c603e2b013	

Type	Indicator	Context
Hash	c3a2abe8756910f42582b04a44ea3514	
Hash	c5a460e4e68a088f6e51b2c6474642ec	
Hash	dd1fd2b459b97b7d59375cb8383cd19a	
Hash	ec0bf4a2186a88874e9f26f07cfeb532	
Hash	ee2861d5965e8730708cd1da8a93fa4c	
Hash	7b9c37d82be5102e47a267e9f3c7c16b23bb1114	
Hash	ac9f013ad20aab607264d7cfe69ad153a4224d4b	
Hash	b7cea387205e16c9f43d750035e77735415dad34	
Hash	ce1ae52bd60bf4a15a8d9aa597989b0d9df8ff3b	
Hash	f9a692dadf9cc72352b979b1ecb80eb09ddf941a	
Hash	0ed9306deabddaa587ad75d0775f7e63b27857a13adcc87 0dc9f8c92a9ddc6da	
Hash	0fce4b732ce10c72093587e82ca9747a885430e366934ddc 27e437443ff0cc0e	
Hash	72029a4d4790784dd3029d13e73f57494dcb8f8187ca234b 131e2b825bd84336	
Hash	b9e4052b310f9451eca9784a4a33bf5282d1bd07e3359eba 9648be625e2e40dd	
Hash	ceea2f175eaa02919e8b5161c2ecf585de3e8b6d586bca80 46eee2e3f4efa386	
Hash	4bbe23daa43583037420ff17b6c6d0844523037c	
Hash	4333f52668996c0fa44c14fefba7fecc	
Hash	1587b6b1949c83e5916cabe9b5882a2ce4d26902	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.

Flame Cell // Adversary Pivot [BETA]

BETA. A hypothetical tabletop projection, anchored to documented ATT&CK behaviour and technique co-occurrence across 170 tracked groups. It is not a prediction; treat it as a war-game prompt and review before acting. Spot a pivot that looks wrong? norbert@salacti.com

- **Control applied:** T1078 Valid Accounts (initial-access)
- **Observed here:** T1078 Valid Accounts was the initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1053 Scheduled Task/Job (execution)
- **Basis:** of the 31+ groups that use Valid Accounts, this pairing runs 1.4x above base rate, a disproportionately-coupled move rather than the obvious one.

With T1078 Valid Accounts blocked, Head Mare could preserve the same objective by pivoting to T1053 Scheduled Task/Job, a technique disproportionately paired with it across tracked groups. Defensive countermeasure: Alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1569 System Services (n=13, lift 2.0), T1072 Software Deployment Tools (n=6, lift 2.3)

Detection and hardening for the pivot (T1053 Scheduled Task/Job)

- **Telemetry:** Windows Security (Object Access audit); Microsoft-Windows-TaskScheduler/Operational; Sysmon
- **Detect:**
  - Security 4698 (task created), 4702 (updated), 4700/4701 (enabled/disabled), 4699 (deleted)
  - TaskScheduler/Operational 106 (registered), 140 (updated), 141 (deleted)
  - Sysmon 1 for schtasks.exe and at.exe; Sysmon 11 for writes under C:\Windows\System32\Tasks\
- **Harden:**
  - Restrict schtasks/at to administrators; disable the legacy at.exe
  - Baseline the legitimate task creators and alert on anything outside it
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0003 Scheduled Job, DS0009 Process, DS0022 File