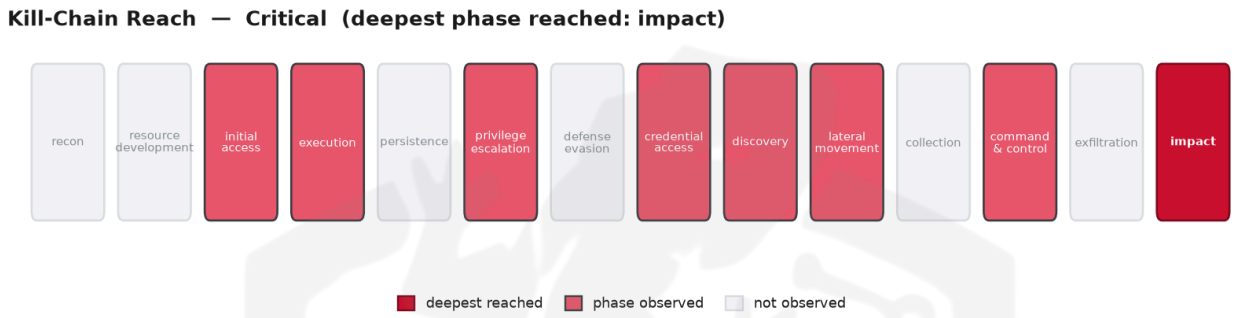
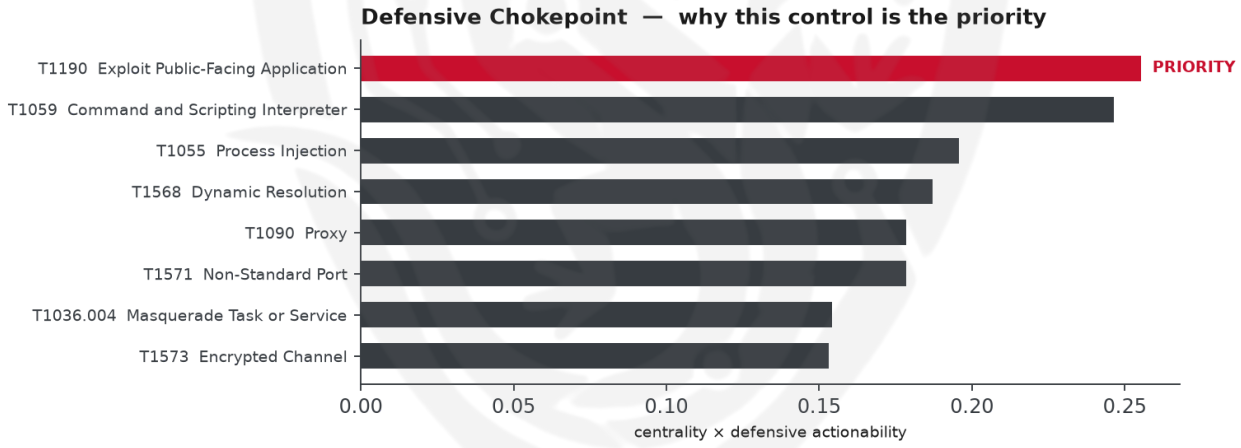
THREAT REPORT: DYSPHORIA BOTNET TARGETS CHINA'S TECHNOLOGY SECTOR

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

The observed cluster of activity has been linked to the Dysphoria botnet, which has been targeting China's technology sector. The malware, including Dysphoria, jackskid, and fbot, exploits several vulnerabilities, with CVE-2020-25499 being a central one. Priority should be given to patching the affected public-facing applications and restricting management interfaces to VPN-only. The threat actor's use of various techniques, including exploit public-facing applications and process injection, poses a significant risk to the targeted sector.

Threat Overview

The threat actor, whose identity is currently insufficient to determine, is utilizing the Dysphoria, jackskid, and fbot malware families to target China's technology sector. The exploited vulnerability, CVE-2020-

25499, is a key component of the attack. The victimology suggests that the threat actor is focusing on the technology sector in China, with the goal of compromising public-facing applications.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, including password guessing, SSH, application layer protocol, and exploit public-facing application. The priority technique, T1190 Exploit Public-Facing Application, is the graph chokepoint. To mitigate this threat, the priority control is to: Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only. In parallel, patch CVE-2020-25499 on all affected systems.

Infrastructure and Corroboration

The malicious infrastructure is hosted on various providers, including InterKVM Host SRL, Global Connectivity Solutions LLP, and Swissnet LLC. Abuse.ch has corroborated the presence of Jackskid and Mirai malware families, in addition to unknown malware. According to AbuseIPDB, at least one indicator has a confidence level of 100%, indicating a high likelihood of malicious activity.

Technical Appendix

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

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

- T1110.001 Password Guessing
- T1021.004 SSH
- T1071 Application Layer Protocol
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1190 Exploit Public-Facing Application
- T1055 Process Injection
- T1090 Proxy
- T1059 Command and Scripting Interpreter
- T1568 Dynamic Resolution
- T1036.004 Masquerade Task or Service
- T1571 Non-Standard Port
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1095 Non-Application Layer Protocol
- T1498 Network Denial of Service
- T1046 Network Service Discovery
- T1021.001 Remote Desktop Protocol
- T1008 Fallback Channels

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.2553).
- Operational risk: Critical (score 1.0, reaches impact).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3438; 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
menuPass	0.3438
Rocke	0.3317
BackdoorDiplomacy	0.3257
Lazarus Group	0.3204
Fox Kitten	0.3191

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 100%.
- Malware families corroborated by abuse.ch: Jackskid, Mirai, Unknown malware.
- Note: enrichment raises the severity signal (an IOC at or above 80% AbuseIPDB confidence, or a confirmed malware-family hit). This is context, not a change to the source assessment.

Indicators of Compromise (defanged — non-clickable)

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

Type	Indicator	Context
IP	92[.]42[.]100[.]131	AbuseIPDB 7% (IT) · Mirai · AS25198 InterKVM Host SRL
IP	78[.]153[.]155[.]152	AbuseIPDB 100% (US) · AS215540 Global Connectivity Solutions LLP
IP	217[.]60[.]195[.]160	AbuseIPDB 77% (NL) · Mirai · AS209373 Swissnet LLC

Type	Indicator	Context
IP	76[.]164[.]203[.]171	AbuseIPDB 0% (ES) · AS25198 InterKVM Host SRL
IP	144[.]31[.]38[.]215	
Domain	c2[.]saintpetersburgresident[.]ru	Mirai
Domain	peer[.]saintpetersburgresident[.]ru	Mirai
Domain	dysphoria[.]androiddebugbridge[.]su	Jackskid
Domain	jerusalem[.]androiddebugbridge[.]su	Jackskid
Domain	kieron[.]androiddebugbridge[.]su	Jackskid
Domain	node[.]androiddebugbridge[.]su	Jackskid
Domain	telaviv[.]androiddebugbridge[.]su	Jackskid
Domain	wow[.]androiddebugbridge[.]su	Jackskid
URL	hxxp://login[.]trees4sale[.]net:9000	
Hash	17c5f13da5b62b155dd973f9062f12061687cc44ee9150d42871005ab5b9c4b5	Mirai
Hash	b55bd5db1e23f5f8da29de762624a69fda49e4c12030adb1bd5907e5c62d150e	Mirai
Hash	336db0baaeb3528aad5ec906dbd2253827900e60d697be3e8d830c232c7d07d3	Mirai
Hash	0269c367eff172f6bfcb54ed717a3f9520be4130c4ab4d2f4a5c95c8dbaead5b	Mirai
Hash	1c5080b6fa705f69758a8add633e3314f1953308ff68750be9455340bc91536b	Jackskid
Hash	19dfcbd3726d6803844fb30dc04502ef	Mirai
Hash	25081bdec05f64eb4f313420c82d8de957e30026	Unknown malware

Type	Indicator	Context
Hash	d0310e982b671884e67580d627b1ad9dbaeaf2f68fef0611526615604ed93449	Mirai
Hash	b17532532560628d67674ca968c38b47	Mirai
Hash	d993c59e338b0b3160f053ccd4a90794	Mirai
Hash	73651c02b29f1c07e3177e86c967fc45e9f30f0f	Unknown malware
Hash	8db6c78533c176f13b61405cdc3f8fad703325f1	Unknown malware
Hash	955ff909972958098f0d4a06bcc4d6b9eea90449	Unknown malware
Hash	9c1716d770ea69e8e1418d96d52222396ecb4362	Unknown malware
Hash	a3b9575897c16cbf6afe3af1aa8b55171ea6edf9	Unknown malware
Hash	b0782a9d6eef2ce02f734a6e5e1d8e0f9a2b65be	Unknown malware
Hash	b7faa44ab0772047a8581bbfdd9c561e28fc66de	Unknown malware
Hash	c1bedea261f325441fb9a75c50b11d0c8fb01ac6	Unknown malware
Hash	dcea71b9ab9de8efca301de9e2f7bf11c7132364	Unknown malware
Hash	df510f6f69a5c149c216c7b3accc4f460d8cf363	Unknown malware
Hash	e7e1694162639ed587625432a79cfaa49f560d11	Unknown malware
Hash	0eb9d7be572752b2978458a54c9e2222	Mirai
Hash	2ca1c7f343ad6e8ff1d1e4055ae80130	Mirai
Hash	4544683ef9879b53dee835de76d59b3f	Mirai
Hash	6c07b423216bcb472cfc437b621f1cc8	Mirai
Hash	7e24b6f83f38fd25eaf5f17b137b2407	

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:** T1190 Exploit Public-Facing Application (initial-access)

- **Observed here:** T1190 Exploit Public-Facing Application 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:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 22+ groups that use Exploit Public-Facing Application, this pairing runs 2.0x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain their objective by leveraging WMI's native capabilities to execute commands and access sensitive information, potentially using it to scan for and exploit local vulnerabilities or to establish persistence. This technique may be particularly appealing as it allows the actor to interact with the system in a way that blends in with legitimate administrative activity, making it harder to detect. To counter this potential move, the mandated defensive control is to monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=23, lift 1.5), T1569 System Services (n=8, lift 1.8)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command