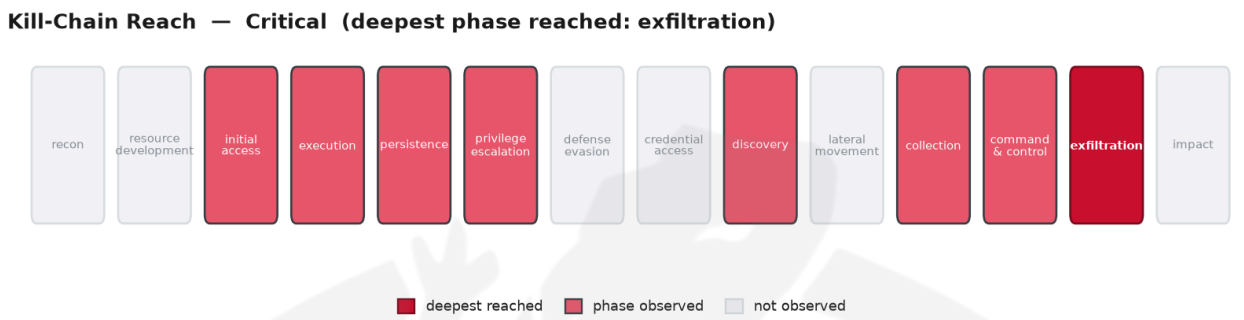
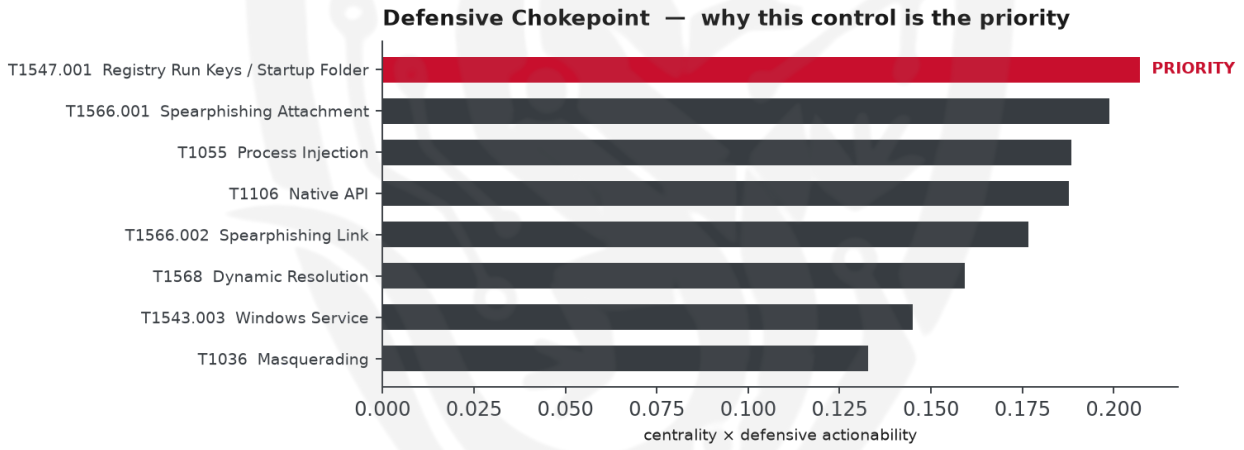
THREAT REPORT: VOID ARACHNE

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 source attributes this activity to Void Arachne, a threat actor targeting the Government of India and its Ministry of Finance tax infrastructure through a multi-stage deployment of DcRAT malware. The campaign, known as Operation DragonReturn, has been observed targeting entities in the British Indian Ocean Territory and India, primarily in the government and finance sectors. Priority should be given to auditing Windows Startup folders and registry keys for unauthorized entries to mitigate the threat. The actor's use of various techniques, including spearphishing and system information discovery, poses a significant risk to the targeted organizations.

Threat Overview

Void Arachne, the attributed threat actor, has been observed using the DcRAT malware family to target government and finance sectors in the British Indian Ocean Territory and India. The central vulnerability exploited in this campaign is currently unknown, but the actor has been observed using a range of

techniques, including screen capture, system owner/user discovery, and bypassing user account control. The targeted organizations should be aware of the potential for data exfiltration and take necessary measures to protect their systems.

Attack Chain and Priority Control

The observed attack chain involves a range of techniques, including initial spearphishing attempts, followed by system information discovery, and eventually, the establishment of a malicious presence on the compromised system. The priority technique in this chain is T1547.001 Registry Run Keys / Startup Folder, which is used to maintain persistence on the compromised system. To mitigate this threat, the priority control is to "Audit Windows Startup folders and Run/RunOnce registry keys for unauthorized entries; alert on .lnk or script creation in Startup by browser/email temp paths."

Infrastructure and Corroboration

The malicious infrastructure associated with this campaign has been observed to be hosted on providers including CTG Server Limited, China Telecom, and Turing Group Limited. While no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence by AbuseIPDB, this information provides context to the campaign's infrastructure and highlights the need for continued monitoring and vigilance.

Technical Appendix

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

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

- T1113 Screen Capture
- T1033 System Owner/User Discovery
- T1548.002 Bypass User Account Control
- T1204.002 Malicious File
- T1543.003 Windows Service
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1106 Native API
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1036 Masquerading
- T1055 Process Injection
- T1010 Application Window Discovery
- T1568 Dynamic Resolution
- T1497 Virtualization/Sandbox Evasion
- T1057 Process Discovery

- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1095 Non-Application Layer Protocol
- T1518.001 Security Software Discovery
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2181).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.6041; 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
Windshift	0.6041
APT37	0.5505
Tropic Trooper	0.535
Darkhotel	0.5075
Higaisa	0.4894

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	27[.]50[.]54[.]191	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	117[.]44[.]201[.]119	AbuseIPDB 0% (CN) · AS4134 China Telecom
IP	118[.]107[.]0[.]197	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
IP	204[.]194[.]48[.]250	AbuseIPDB 0% (US) · AS140869 Turing Group Limited
IP	223[.]26[.]63[.]40	AbuseIPDB 0% (HK) · AS152194 CTG Server Limited
Domain	1kkkkddd[.]com	
Domain	govtop[.]one	
Domain	ikkkkddd[.]com	
Domain	jiayingjing[.]com	
Domain	kkxqbh[.]top	
Domain	simaqz[.]com	
URL	hxxp://govtop[.]one/incometax	
Hash	7ec462f138432f4da43d942488d3d428	
Hash	b26c01dfcc0cdcb30f4a9058f880fb80	
Hash	dda082a12bb43eb34b9b37bf9e62d5f0	
Hash	5260ac8e82c1280950425bb12ddfb5435ff20539	
Hash	7d06bac0114e4c1e9a300d6310a29cf92956c933	
Hash	ac2eeef05f568ad36bdcd807159313862a84387d	
Hash	19ca5fe04ca45a18c5bad9658ff73a8f39fe20ced78f690595f1b4c5a90af324	

Type	Indicator	Context
Hash	2f2f8f92af86fb962c30c4c1c9d673f9d94886373d0fcf78f8d105c051ffc643	
Hash	34d1231a3bf1e13a9b90daecb5c74d52aea94ca54427b203d77e1adc61a5c4f9	
Hash	4a040770fd81d0db9e04cb8dbd2e07e61969072962bb4e736b7c7001444cc2fa	
Hash	589aa1f7252cae74538343cd35443c0a8f58ed280f2016918b6e539a0c09529a	
Hash	5a00485968679dc0ed6d80b659f48287603864c223e952918d2c2aaddfa2d280	
Hash	5e97f7c17bf0466355be0438c7cc3e2e4d125e31368f2fbcb8e1d79cb97f137a	
Hash	6c774188a54ae07ae896abdf1ea6695cc29f529388888665e05322af3e9178e1	
Hash	7e142c8fa614cc39d0453aa648b12209821c6bcbb77ee02094f70161b40d50ae	
Hash	8ed95259300ca268279867d2999d9c4f6585c6c45308635fc39af87da27546b5	
Hash	a8614dfad5fd2a79302a7c4829a0fed6f3a0a46b11beb28f89531cdfa83d32b3	
Hash	b0fcd7d9396e70b89e8292f6b80f933607b6fc9a9d3d4dd4ca69b408a2625932	
Hash	c6651d6ce31c3a00357e579981d48c0da942b5bbe1582bf3d612a07dc3bc0ff6	
Hash	c6fc06db6a1318152c09200352b40c8fa794f1089988835c1df92174347be8ec	
Hash	ec5d4103b3d97885e9575ad045b2ef5467bf9fccf71828e418e6488d78983146	
Hash	eccff5c026a01cbe91db45cd0289f8822985aa5183f096d8add69762696d100d	
Hash	fc17d5b4d64cb61a5aa8fb6bbe1e94885f129b2bf8ee91bca1ccca2b537f6616	

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