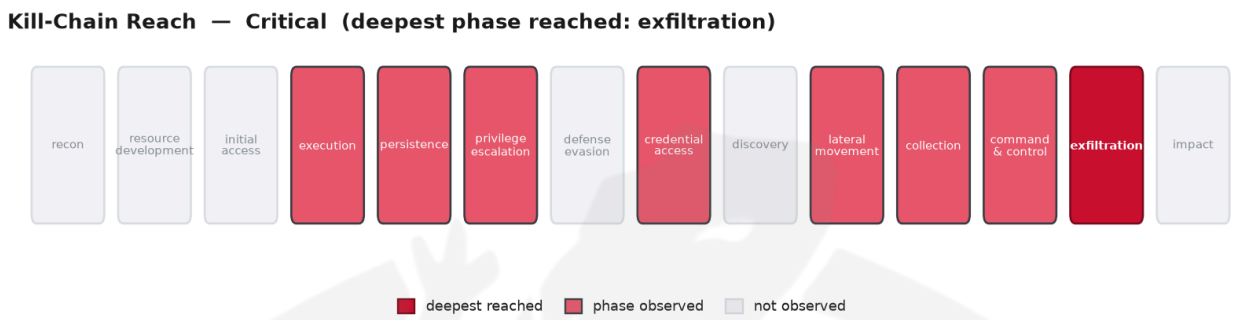
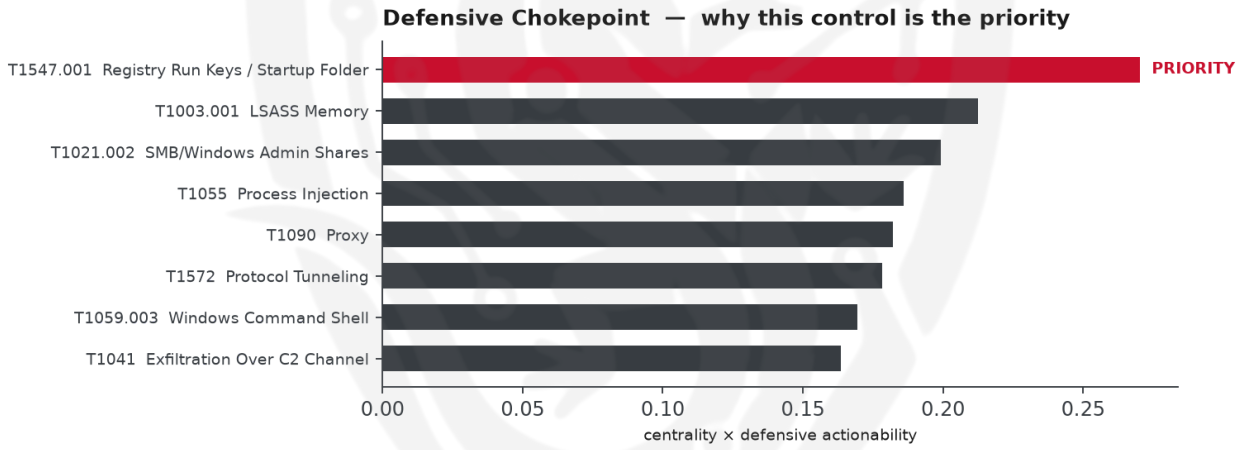
THREAT REPORT: TETRISPHANTOM

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 TetrisPhantom, a threat actor targeting government sectors with a range of malware families, including GoSerpent, McMx, and Mimikatz. The targeted country and central CVE are not specified, but the threat actor's techniques indicate a high level of sophistication. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to mitigate the threat.

Threat Overview

TetrisPhantom, the attributed threat actor, utilizes a variety of malware families to target government sectors. The malware families involved include GoSerpent, McMx, ThumbcacheService, Mimikatz, QuarksDumpLocalHash, Stowaway, TmcLoader, and TmcPayload. The victimology suggests a focus on government entities, although specific details on the targeted country are insufficient.

Attack Chain and Priority Control

The observed techniques employed by TetrisPhantom form a complex attack chain, involving archive utility, standard encoding, security account manager access, and symmetric cryptography, among others. The priority technique identified is T1547.001 Registry Run Keys / Startup Folder, which serves as a critical chokepoint in the attack chain. To counter this, the recommended 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 TetrisPhantom's activities is hosted on providers such as Beyotta Services LLP and Moack.Co.Ltd, as observed in third-party enrichment data. However, no malware families have been corroborated by abuse.ch, and AbuseIPDB confidence levels for indicators are below the threshold, with no indicators reaching an 80% confidence level.

Technical Appendix

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

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

- T1560.001 Archive via Utility
- T1132.001 Standard Encoding
- T1003.002 Security Account Manager
- T1573.001 Symmetric Cryptography
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1021.002 SMB/Windows Admin Shares
- T1572 Protocol Tunneling
- T1003.001 LSASS Memory
- T1090 Proxy
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1095 Non-Application Layer Protocol
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1564.004 NTFS File Attributes
- T1090.001 Internal Proxy

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2846).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4389; 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
BRONZE BUTLER	0.4389
FIN13	0.4288
Ke3chang	0.4211
APT33	0.4063
Higaisa	0.406

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	144[.]48[.]6[.]46	AbuseIPDB 0% (SG) · AS997 Beyotta Services LLP
IP	103[.]138[.]13[.]30	AbuseIPDB 0% (KR) · AS138195 Moack.Co.Ltd
Hash	ebffd5a76aaa690bcdb922f82e0bacc5	
Hash	dc506ff7bb72735444fb3703a6bee6d8	
Hash	d6e86bf8a90e9b632add5fa495f97fbc	
Hash	cb6c4c70a3b171fa3404b8e1a3382116	
Hash	64e9d1950e42bc98486dfd9919463d1c	

Type	Indicator	Context
Hash	cbbb6d483737ea3566726e51752dff40	
Hash	7f223ee0716ce2ad56f55d3744419449	
Hash	19f8befcb035f52bf70094e6b4f5779a	
Hash	846ef7c1c7323849b2a778c5e4cda162	
Hash	d08a059e8b815e3b891505bc8777fc28	
Hash	93a1569d5d5ab2c4761fedf84f83709e	
Hash	313233343536373839306162636465 66	

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:** T1547.001 Registry Run Keys / Startup Folder (persistence)
- **Observed here:** T1547.001 Registry Run Keys / Startup Folder was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1053 Scheduled Task/Job (persistence)
- **Basis:** 37 of 170 documented groups that use Registry Run Keys / Startup Folder also use Scheduled Task/Job (conditional 0.64, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

TetrisPhantom could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and achieve their objectives, potentially by creating a new scheduled task that would allow them to regain access or execute malicious code at a later time. This technique may be particularly appealing as it could enable them to bypass the blocked registry run keys/startup folder control. To counter this potential move, the defensive control would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1078 Valid Accounts (n=27, lift 1.2), T1543 Create or Modify System Process (n=18, lift 1.8)

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