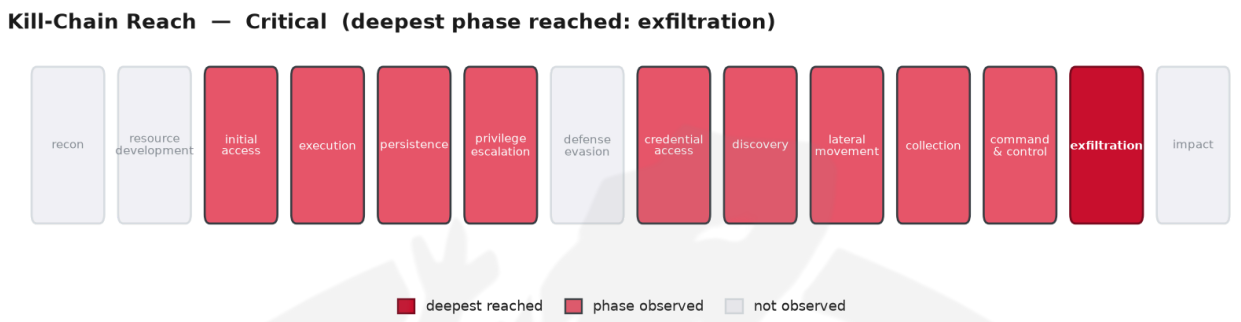
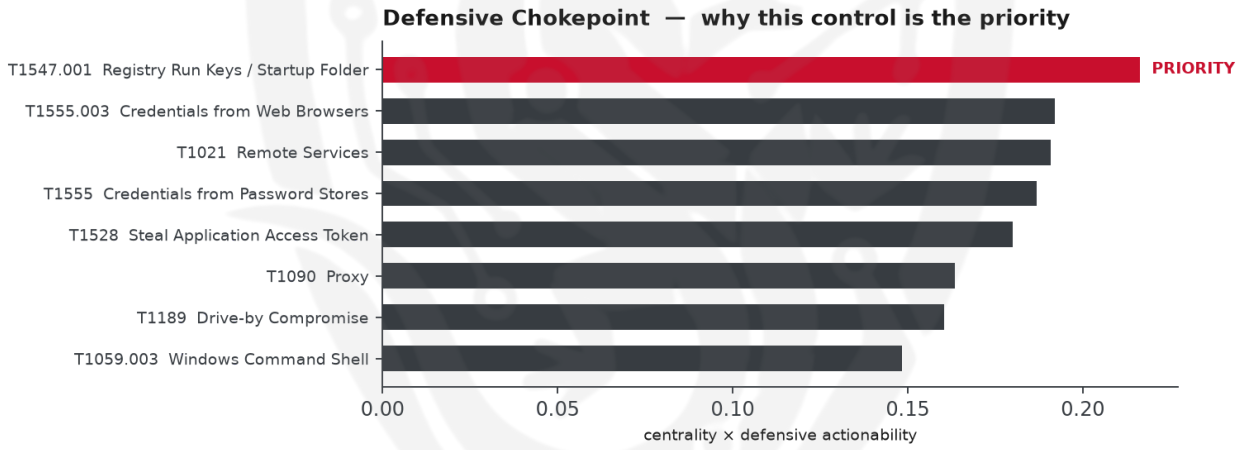
THREAT REPORT: TAG-195

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 TAG-195, a threat actor utilizing various malware families, including TinyEgg, ChonkyChicken, and TerraStealerV2, to target unspecified countries and sectors. The actor's primary objective is to exfiltrate sensitive information, and priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. The threat actor's use of multiple techniques, including screen capture, keylogging, and audio capture, poses a significant risk to affected organizations.

Threat Overview

TAG-195, the observed threat actor, employs a range of malware families, including TinyEgg, ChonkyChicken, ChromEggscalator, TerraStealerV2, TerraLogger, and RevC2, to exploit unspecified vulnerabilities. The actor's victimology is unclear, but their techniques suggest a focus on gathering sensitive information from compromised systems.

Attack Chain and Priority Control

The threat actor's attack chain involves multiple techniques, including screen capture, system owner/user discovery, keylogging, and audio capture, ultimately leading to exfiltration over a command-and-control channel. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which serves as a chokepoint in the attack chain. To mitigate this threat, 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

Although the primary infrastructure details are not available, third-party enrichment sources, such as abuse.ch, have corroborated the presence of malware families like ChromElevator and VenomLoader. However, no indicators have been flagged with high confidence by AbuseIPDB, with the highest confidence seen being 0%.

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
- T1056.001 Keylogging
- T1123 Audio Capture
- T1074.001 Local Data Staging
- T1087.002 Domain Account
- T1115 Clipboard Data
- T1135 Network Share Discovery
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1021 Remote Services
- T1555.003 Credentials from Web Browsers
- T1090 Proxy
- T1049 System Network Connections Discovery
- T1528 Steal Application Access Token
- T1041 Exfiltration Over C2 Channel
- T1547.001 Registry Run Keys / Startup Folder
- T1218.010 Regsvr32
- T1059.003 Windows Command Shell
- T1189 Drive-by Compromise
- T1071.001 Web Protocols

- T1018 Remote System Discovery
- T1046 Network Service Discovery
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2278).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4375; 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
APT39	0.4375
APT3	0.4256
FIN13	0.4082
Ke3chang	0.4009
Threat Group-3390	0.3881

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: ChromElevator, Unknown malware, VenomLoader.
- 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
Domain	xtrafftrck[.]net	Unknown malware · malware_download

Type	Indicator	Context
Domain	screenly[.]cam	Unknown malware · malware_download
Domain	ahdaratlegalservices[.]com	malware_download
Domain	paysolutions[.]ink	malware_download
Domain	aurekh[.]com	malware_download
Hash	6c23b7723a9f69ea48f02c8fe13fd60ecbfc2fb28e32e481c46ec968a66c66cd	VenomLoader
Hash	b7b322f4638ead5c39031ffc7ca8c791c8d47211b09449f7ceb49f0c32a19b45	ChromElevator
Hash	45c8cbaeb5c7708e7b8030e701747c65203958e82eddc41f39e0ca93bd36c114	Unknown malware
Hash	d2e1ab10d5a0c16a724aeda8acb46b38f551ade58137969c3bc3c9cdc0a12425	Unknown malware
Hash	5cae5202ddcc29f19f954d81ba138f11b8a4080d05fef63c05a00b9242c06967	
Hash	9a2d714ddd5c48722c35df8a70e97f12d46bcde05dc79b7242a7e692bd346826	
Hash	6c7619c34497f430c4f7618cfefe07d1defacfae48f6730c20f52e7a7344faa9	
Hash	41aa04782e436345ef45dc159321d5c0e0e5cba300e55a4d1d3194e5c7c5fd97	
Hash	d5dea9a51b984be9d7fa76e3e8ff89cfb97c335927331e8e348b9ee269070c1b	
Hash	16735cb80d796865b2430aa11d21a539fcb00b027932f2c63e4b5c098d26585b	
Hash	e3153ced59bb0376186b0eee0ec68f0b5aa9ae5820ef8508ae4e67625e1a3581	
Hash	6922b319dc96d020738bcf466c4d6d9233e4767b68592e1fd9258a232f166ce1	

Type	Indicator	Context
Hash	03713176e7f0d9f3b37ac6eb644d90bb	
Hash	210f57e3b1c88447ddc11467f7b2fbb9	
Hash	2cc1ec080f7e1fcd2c0c6ae033b988c5	
Hash	2cf627a0a9d64db3e4cd13fda3ce5636	
Hash	3418b6439309250feb2cd983aa00da44	
Hash	396d4f44e429e7128af9c02e0c1bdf99	
Hash	552d991cccd6c5053dfda46c0ac32623	
Hash	60992cdeb88dddfb17e12573e4436c42	
Hash	70983540817fd9ff46204001a7b35ba0	
Hash	7a0edeb5bebc51de8ce455f38d9a7670	
Hash	7c6e4a085b1fd9b98407ba4400f91201	
Hash	8ea54a900bd13ff3ecca01e62428e508	
Hash	960688e3484eb744cdbbee55a7415bd1	ChromElevator
Hash	9bd6f7a308418a2b376e731d9e80bac1	
Hash	9d6f7697c0fbea55d6bfb39642eb87df	
Hash	c21f69bbf1f78ebf4f1aa784cee035ce	
Hash	cbe0daeec71e47840672d930e112d467	
Hash	e4ee5ed330eaa0602f4f637f5567d08e	
Hash	f23cb60ab395cc6bf931eed16b801ed7	
Hash	06eade11e16465edef89ba0199d7d6f8c18a3200	
Hash	10f6effed5a4dfff9b6e94ea90bc2134510f770f	
Hash	26545d3db9802c44145e289b8e989d0a68bf90cb	
Hash	2b57771989fc059bbef8f28fc0ca24eeae7e7863	

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.

The adversary 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 be used to bypass the blocked Registry Run Keys / Startup Folder control, allowing the adversary to adapt and continue their campaign. The defensive control to counter this 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