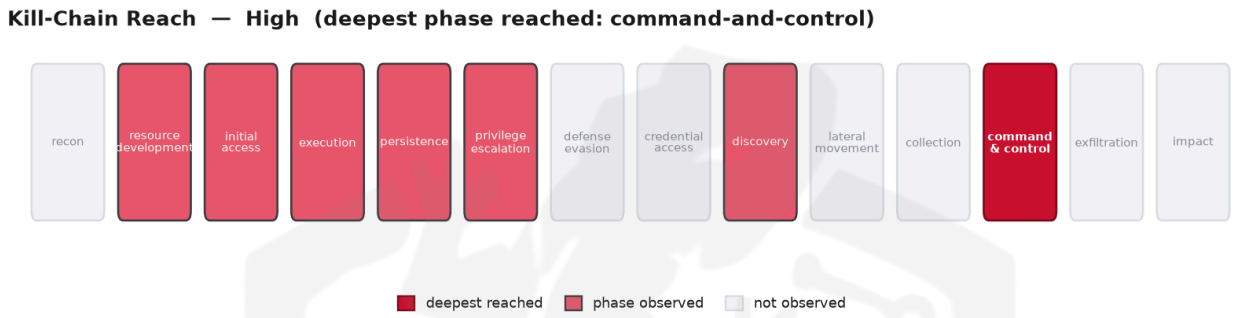
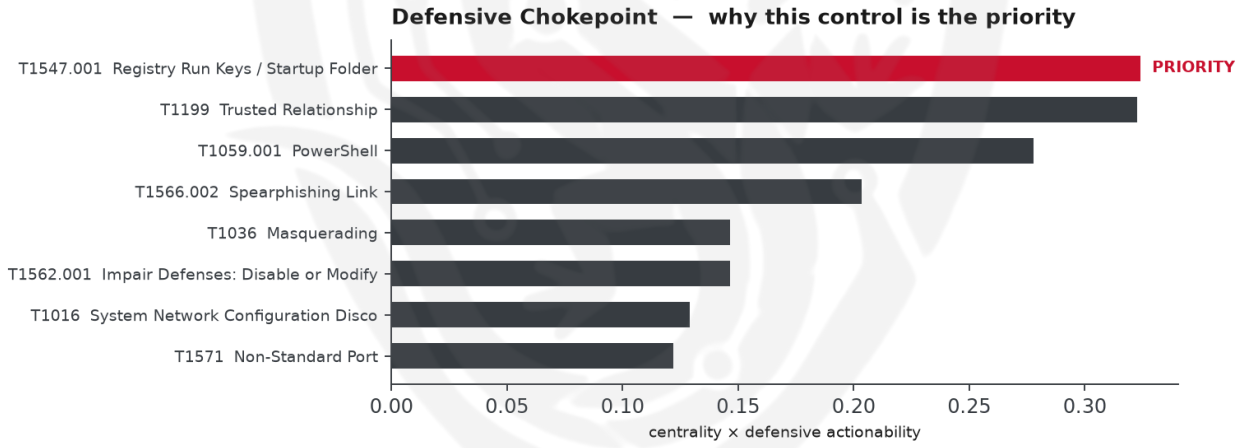
THREAT REPORT: UNKNOWN_ADVERSARY PHOTO ZIP CAMPAIGN

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 is targeting the hospitality industry with a Photo ZIP campaign, delivering a Node.js implant for persistent access. The campaign involves multiple malware families, including TonRAT, Wacatac, and PureRat. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. The threat actor's identity and targeted country remain unknown, but the sectoral focus and technical mechanics are clear.

Threat Overview

The threat actor, whose identity is insufficient to determine, is utilizing a range of techniques to gain persistent access to hospitality industry targets. The malware families involved include TonRAT, Wacatac, and PureRat, although the central vulnerability exploited remains unknown. The actor is targeting the

hospitality sector, leveraging techniques such as JavaScript, malicious files, and spearphishing links to establish a foothold.

Attack Chain and Priority Control

The observed techniques form a complex chain, with the threat actor leveraging various methods to establish persistence and evade detection. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which serves as a critical 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

The malicious infrastructure is hosted on Omegatech LTD, according to third-party observations. Additionally, abuse.ch has corroborated the presence of Unknown Loader, Unknown malware, and Vidar malware families, although these do not override the primary malware families identified. AbuseIPDB has flagged indicators with a low confidence level, with the highest confidence seen at 2%, which is below the threshold for high-confidence 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)

- T1059.007 JavaScript
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1583.001 Domains
- T1036 Masquerading
- T1016 System Network Configuration Discovery
- T1583.006 Web Services
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1199 Trusted Relationship
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1584.006 Web Services
- T1571 Non-Standard Port
- T1027 Obfuscated Files or Information
- T1027.004 Compile After Delivery

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.3412).
- Operational risk: High (score 0.636, reaches command-and-control).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5715; 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
LazyScripter	0.5715
TA2541	0.483
Transparent Tribe	0.4663
Earth Lusca	0.4507
ZIRCONIUM	0.4485

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 2%.
- Malware families corroborated by abuse.ch: Unknown Loader, Unknown malware, Vidar.
- 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	178[.]16[.]54[.]27	AbuseIPDB 2% (NL) · AS202412 Omegatech LTD
Domain	zloapobikahy23[.]bond	Vidar
Domain	prejointl[.]info	
Domain	recallnine[.]info	
Domain	visaphoto-secure[.]info	

Type	Indicator	Context
Domain	ministrew[.]info	malware_download
Domain	heliosup[.]info	
Domain	docshub-secure[.]com	
Domain	visaimage-storage[.]icu	
Domain	safephoto-vault[.]info	
Domain	keypmenu[.]info	
Domain	kellystreets[.]info	
Domain	image-vlt[.]info	
Domain	visaphoto-vault[.]info	
Domain	safe-picvault[.]info	
Domain	safedoc-storage[.]info	
Domain	photobook-reserv[.]pro	
Domain	imagestore-hub[.]info	
Domain	photo-box[.]info	
Domain	photo-hub-io[.]info	
Domain	sec-safe-dc[.]info	
Domain	hakeiwjs727wj[.]com	
Domain	photo-dekor[.]xyz	
Domain	photobookadm[.]pro	Vidar · malware_download
Domain	haobbao[.]com	
Domain	recstrace[.]info	
Domain	vertualstreak[.]info	
Domain	dancamp[.]info	
Domain	docshub-01[.]info	
Domain	montagelips[.]info	

Type	Indicator	Context
Domain	safedocphoto[.]info	
Domain	visaimages[.]info	
Domain	photo-26254[.]cfd	
Domain	photo-26654[.]cfd	
Domain	photo-26656[.]cfd	Unknown malware
Domain	photo-26653[.]cfd	Unknown malware
Domain	photo-27857[.]cfd	Unknown Loader
Domain	widjssij728dj[.]com	
Domain	reservebookphot[.]pro	
Domain	finallyrain[.]info	

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 actor could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and achieve their objectives, potentially by scheduling a new task that blends in with legitimate system activity. This technique may be particularly appealing as it allows the actor to execute their payload at a specified time or interval, potentially evading detection. To counter this, the defensive control would involve alerting on new scheduled tasks (Event ID 4698); restricting 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