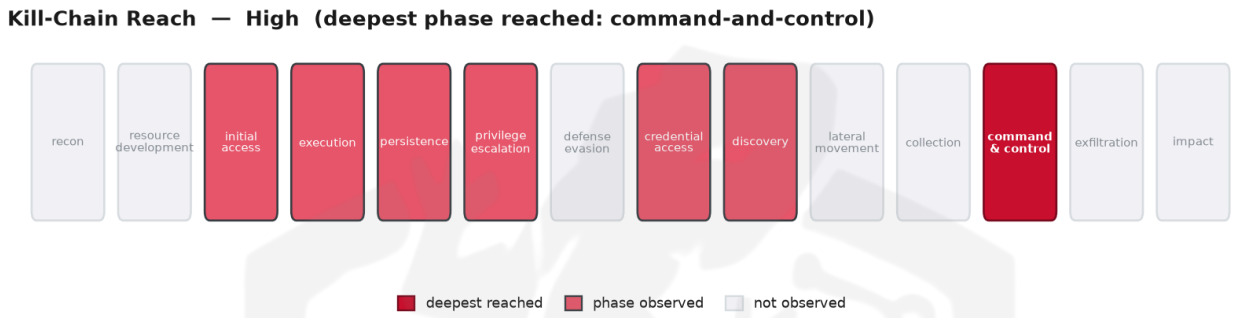
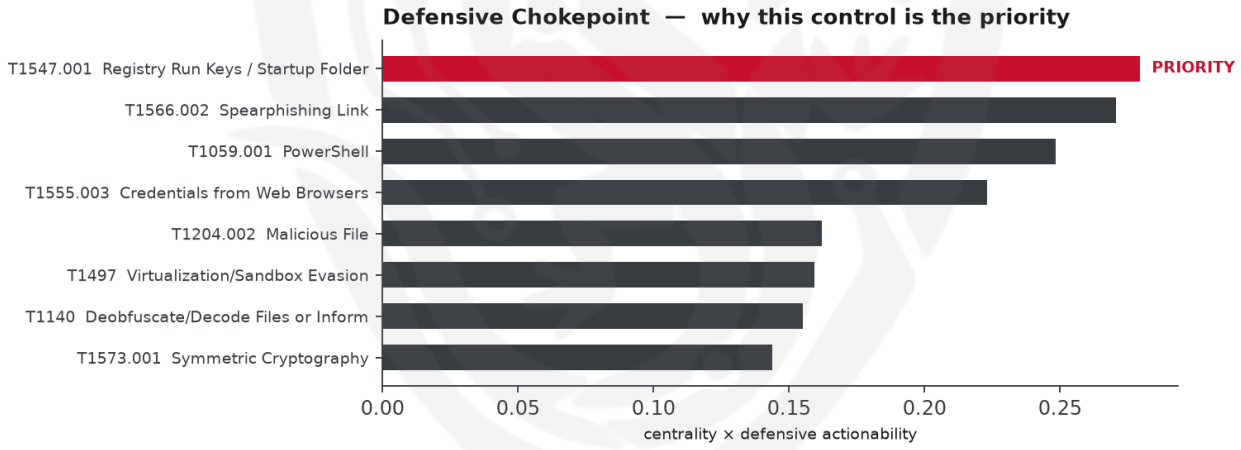
THREAT REPORT: UNKNOWN_ADVERSARY ABUSES TON BLOCKCHAIN

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 targeting Japan's hotel industry, utilizing the TONResolver malware family to compromise systems. The threat actor's tactics involve a range of techniques to gain and maintain access to victim networks. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to mitigate the threat. The targeted sector is hospitality, specifically in Japan.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, is using the TONResolver malware family to target Japanese hotels. The central vulnerability exploited is not specified, but the malware family

is known to be involved in the abuse of the TON blockchain. The victimology indicates a focus on the hospitality sector in Japan.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, including standard encoding, JavaScript usage, and symmetric cryptography, among others. The priority technique identified is T1547.001 Registry Run Keys / Startup Folder, which serves as a chokepoint in the attack chain. To counter this, 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

Although the primary infrastructure details are not available, third-party corroboration from abuse.ch indicates the presence of Unknown Loader, Unknown malware, and Vidar malware families. However, according to AbuseIPDB, there are no indicators with a confidence level of 80% or higher, 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)

- T1132.001 Standard Encoding
- T1059.007 JavaScript
- T1539 Steal Web Session Cookie
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1566.002 Spearphishing Link
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1555.003 Credentials from Web Browsers
- T1497 Virtualization/Sandbox Evasion
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1102.001 Dead Drop Resolver
- T1043 Commonly Used Port

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2943).
- 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 0.56; 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
Molerats	0.56
Inception	0.5488
APT33	0.5251
APT19	0.495
Windshift	0.4899

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- 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
Domain	zloapobikahy23[.]bond	Vidar
Domain	photobook-reserv[.]pro	
Domain	photo-41473[.]xyz	
Domain	photo-5512473[.]xyz	
Domain	photo-1642054[.]cfd	

Type	Indicator	Context
Domain	photo-4773041[.]cfd	
Domain	photo-31642054[.]cfd	
Domain	photo-1773041[.]cfd	
Domain	photo-2773041[.]cfd	
Domain	photo-1777041[.]cfd	
Domain	photo-dekor[.]xyz	
Domain	photo-5542054[.]cfd	
Domain	photo-3777041[.]cfd	
Domain	photo-21454[.]cfd	
Domain	photo-62454[.]cfd	malware_download
Domain	bjsdaklska283saik[.]com	
Domain	bookaboutphoto[.]pro	
Domain	photo-26254[.]cfd	
Domain	photo-26654[.]cfd	
Domain	photo-26554[.]cfd	
Domain	haddjskak827sja[.]com	Unknown malware
Domain	photo-26652[.]cfd	Unknown malware
Domain	hakdsiwqs281ks[.]com	Unknown malware
Domain	photo-26656[.]cfd	Unknown malware
Domain	dsjkaksfks324das[.]com	Unknown malware
Domain	photo-26653[.]cfd	Unknown malware
Domain	havasssj291sld[.]com	Unknown malware
Domain	photo-27657[.]cfd	Unknown malware
Domain	jsdakksd283ksl[.]com	Unknown malware
Domain	photo-27757[.]cfd	Unknown malware

Type	Indicator	Context
Domain	photo-26657[.]cfd	Unknown malware
Domain	haskakwo291sa[.]com	Unknown malware
Domain	tonajukbhuakpo2[.]shop	Unknown Loader
Domain	hsaertyuoang34[.]sbs	
Domain	amanohuguta[.]cfd	
Domain	bookphotoreserv[.]pro	
Domain	widjssij728dj[.]com	
Domain	reservebookphot[.]pro	
Domain	photo-5342054[.]cfd	
Domain	bookreservphoto[.]pro	

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 scheduling a new task to execute their malicious payload at a later time. This technique may be particularly appealing as it allows the actor to blend in with legitimate system activity, making it more challenging to detect. To counter this potential move, the defensive control would involve alerting on new scheduled tasks (Event ID 4698), restricting schtasks/at to admins, and baselining 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