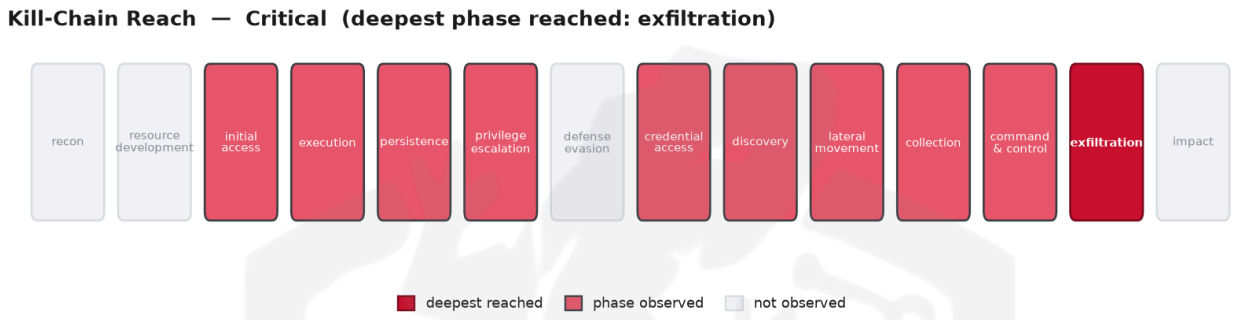
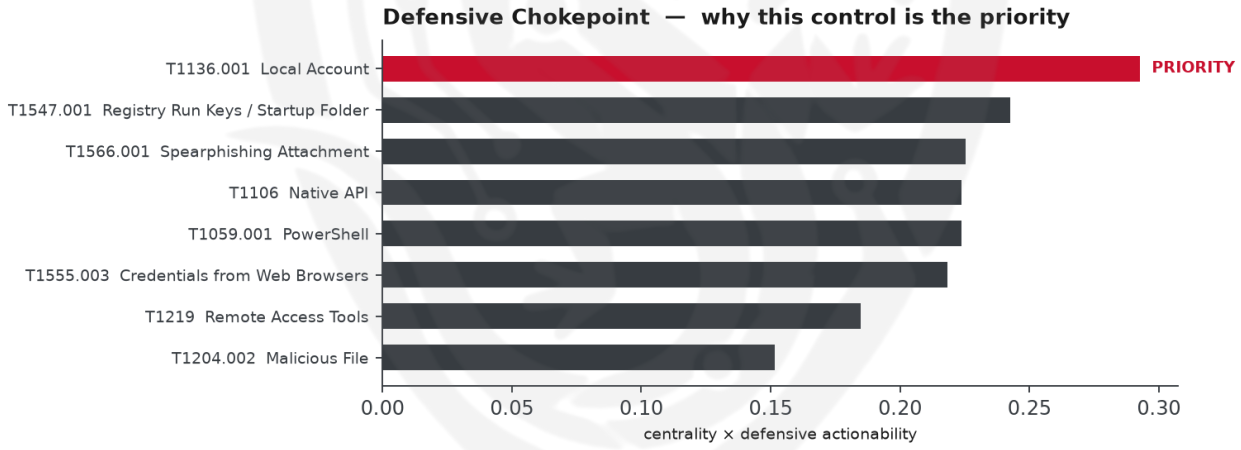
THREAT REPORT: LARVA-24009 PHISHING EMAIL ATTACK

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 Larva-24009, a threat actor targeting the healthcare sector with a phishing email attack. The attack involves the use of malware families such as QuasarRAT, UltraVNC, and Notifier. Priority should be given to defending against this attack, as it has the potential to lead to exfiltration of sensitive data. The threat actor's techniques and tactics indicate a high level of sophistication, making it essential to take immediate action to prevent further compromise.

Threat Overview

Larva-24009, the observed threat actor, utilizes a range of malware families, including QuasarRAT, UltraVNC, and Notifier, to target healthcare organizations. The actor's tactics involve exploiting various techniques, including scheduled tasks, screen capture, keylogging, and spearphishing attachments. The

victimology of this attack is focused on the healthcare sector, although specific country targets are not identified.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including scheduled tasks, screen capture, keylogging, and spearphishing attachments, ultimately leading to exfiltration of sensitive data. The priority technique in this chain is T1136.001 Local Account, which is the graph chokepoint. To mitigate this threat, the priority control is to "Alert on new local/domain account creation (Event ID 4720/4728); enforce approval workflow for account provisioning."

Infrastructure and Corroboration

The malicious infrastructure associated with this attack is hosted on Contabo Inc. The use of Quasar RAT malware has been corroborated by abuse.ch, providing additional context to the attack. 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)

- T1053.005 Scheduled Task
- T1113 Screen Capture
- T1056.001 Keylogging
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1082 System Information Discovery
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1219 Remote Access Tools
- T1555.003 Credentials from Web Browsers
- T1136.001 Local Account
- T1083 File and Directory Discovery
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1027 Obfuscated Files or Information
- T1567.002 Exfiltration to Cloud Storage
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer
- T1021.001 Remote Desktop Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1136.001 Local Account (centrality 0.3082).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5521; 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
Confucius	0.5521
Molerats	0.5477
Ajax Security Team	0.5196
APT39	0.5164
APT37	0.4907

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Quasar RAT.
- 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	217[.]77[.]6[.]50	AbuseIPDB 0% (US) · Quasar RAT · AS40021 Contabo Inc.
Domain	pozeny[.]shop	
Domain	aonexa[.]shop	
Domain	mainsec[.]site	
Domain	serverdock[.]online	

Type	Indicator	Context
Domain	final[.]mainsec2[.]site	
Hash	10b40185106eb3760cb71c46117aa0bf	
Hash	1500fefcdda275b70e2051a3e7d9f794	
Hash	2973fda8d0d0fa0200a05889fce85df6	
Hash	444fb3592cd1848660259a913684795b	
Hash	4ad28d0313549e98383144d82982be6e	

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:** T1136.001 Local Account (persistence)
- **Observed here:** T1136.001 Local Account was the only persistence technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1098 Account Manipulation (persistence)
- **Basis:** of the 13+ groups that use Local Account, this pairing runs 5.6x above base rate, a disproportionately-coupled move rather than the obvious one.

Larva-24009 could pivot to T1098 Account Manipulation in an attempt to maintain access and evade detection by modifying existing accounts to elevate privileges, which may allow them to bypass the blocked local account creation. This technique in particular would likely be appealing as it enables the adversary to manipulate account settings without creating new accounts, potentially flying under the radar. To counter this, the defensive control of alerting on privilege/group changes and credential additions to accounts (Event ID 4738/4670) and reviewing conditional-access changes should be implemented.

Also plausible (same tactic): T1505 Server Software Component (n=12, lift 2.9), T1133 External Remote Services (n=10, lift 2.8)

Detection and hardening for the pivot (T1098 Account Manipulation)

- **Telemetry:** Windows Security (account management); Azure AD audit logs
- **Detect:**
  - Security 4728/4732/4756 (added to security-enabled groups), 4738 (account changed), 4670 (permissions changed)
  - New credentials/keys added to accounts or app registrations in the IdP
  - MFA method added or reset outside a normal workflow

- **Harden:**
  - Alert on privileged-group changes; approval workflow for role grants
  - Monitor and restrict service-principal credential additions
- **MITRE:** M1032 Multi-factor Authentication, M1026 Privileged Account Management, M1018 User Account Management · DS0002 User Account, DS0026 Active Directory