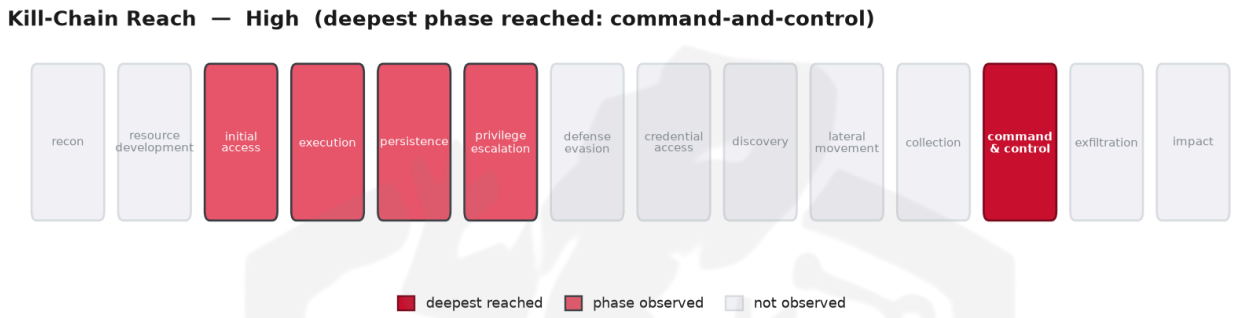
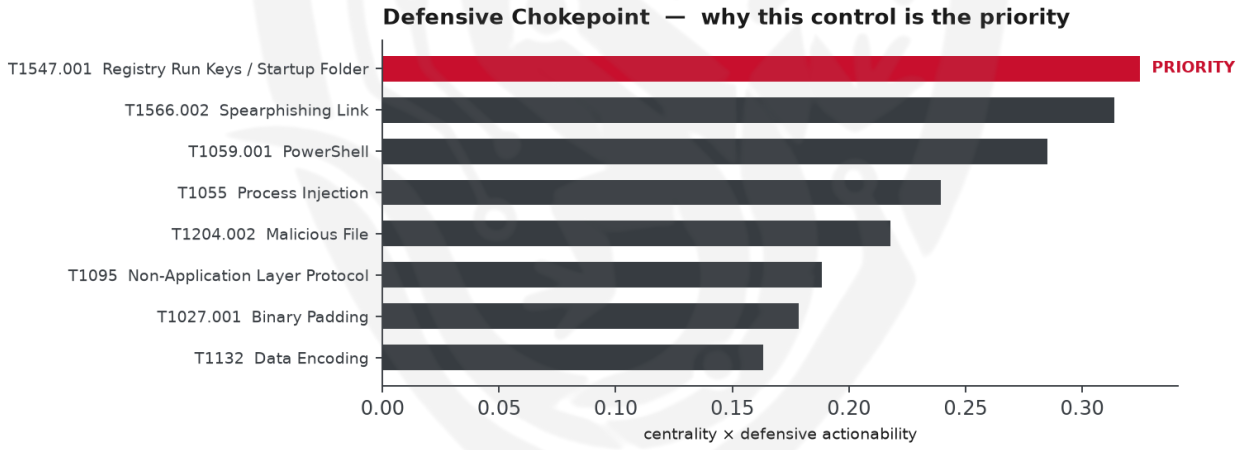
THREAT REPORT: NETSUPPORT RMM EMAIL-BASED ATTACK

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 observed cluster of activity involves the delivery of a MediaFire ZIP file, which executes a chain of techniques to compromise the target system. The malware family used in this attack is NetSupport RMM. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to prevent further compromise. The threat actor's identity and targeted country remain unknown.

Threat Overview

The threat actor, whose identity is unknown, utilizes the NetSupport RMM malware family to carry out the attack. The victimology and targeted sectors are also unknown. The attack involves a series of

techniques, including scheduled tasks, malicious files, and process injection, to establish a foothold on the target system.

Attack Chain and Priority Control

The attack chain involves multiple techniques, including scheduled tasks, rundll32, and process injection, which ultimately lead to the execution of malicious code. The priority technique in this chain is T1547.001 Registry Run Keys / Startup Folder, which is the graph chokepoint. To mitigate this threat, 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

There is no available information on the hosting providers or ASNs observed in this attack. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence of 80% or higher.

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
- T1218.011 Rundll32
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1055 Process Injection
- T1027.001 Binary Padding
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1095 Non-Application Layer Protocol
- T1132 Data Encoding
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.342).
- 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 0.5517; 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	0.5517
Molerats	0.5421
LazyScripter	0.533
TA551	0.5217
Rancor	0.5213

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
Domain	bsc[.]blockrazor[.]xyz
Domain	xn--fiqq24b9hejs1c[.]clickvector[.]tech

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:** T1543 Create or Modify System Process (persistence)

- **Basis:** of the 18+ groups that use Registry Run Keys / Startup Folder, this pairing runs 1.8x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1543 Create or Modify System Process to maintain persistence by disguising their malicious code as a legitimate system process, potentially leveraging the Windows service management functionality to blend in with normal system activity. This technique may be particularly appealing as it allows the actor to operate with elevated privileges and evade detection, which could be a next logical step after being blocked from using registry run keys or startup folders. The defensive countermeasure to mitigate this would be to implement the mandated control: Restrict service/daemon creation to admins; monitor service and driver installs.

Also plausible (same tactic): T1098 Account Manipulation (n=12, lift 2.0), T1112 Modify Registry (n=17, lift 1.7)

Detection and hardening for the pivot (T1543 Create or Modify System Process)

- **Telemetry:** Windows Security / System log; Sysmon
- **Detect:**
  - System 7045 (new service installed); Security 4697 (service installed)
  - Sysmon 1 for sc.exe / services created; unusual ImagePath or user-context services
  - Registry writes under HKLM\SYSTEM\CurrentControlSet\Services
- **Harden:**
  - Restrict service creation to admins; application control on service binaries
  - Baseline installed services and alert on new/anomalous ones
- **MITRE:** M1047 Audit, M1028 Operating System Configuration, M1026 Privileged Account Management · DS0019 Service, DS0024 Windows Registry, DS0009 Process