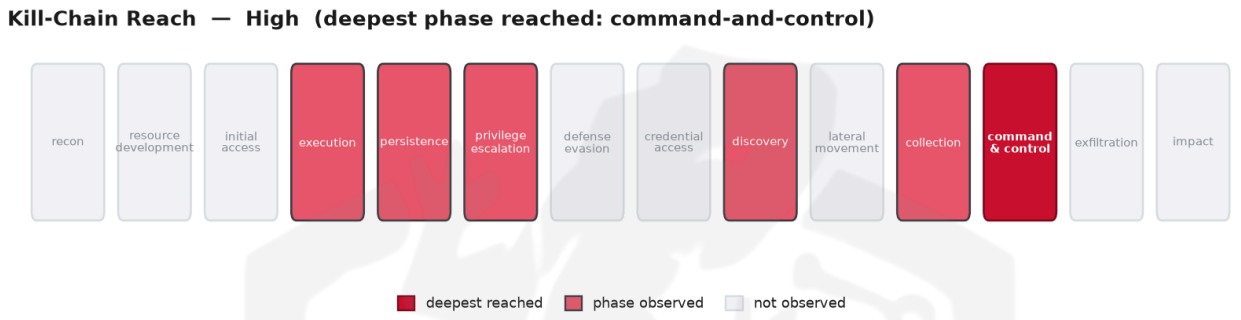
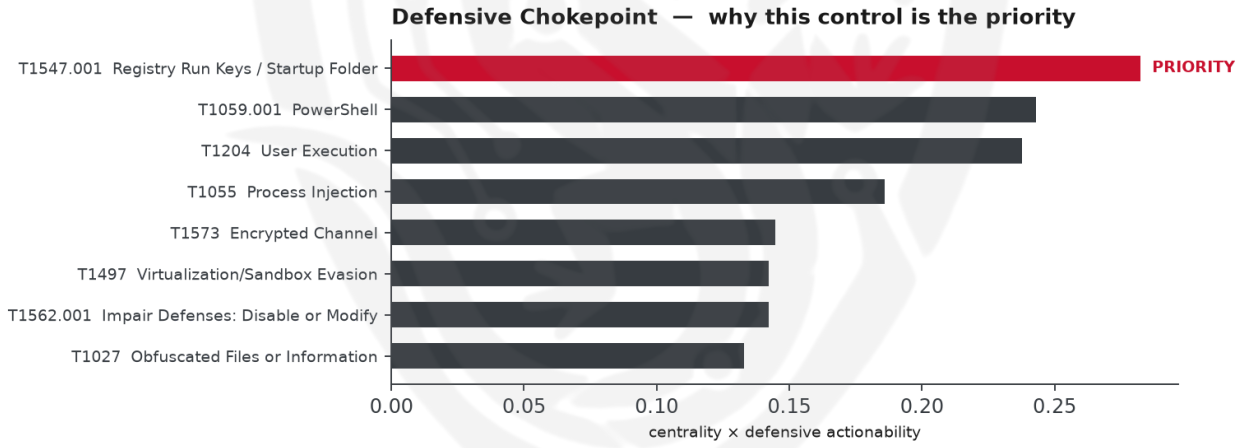
THREAT REPORT: UAT-11795 CLICKFIX-THEMED CAMPAIGN

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 source attributes this activity to UAT-11795, a threat actor deploying Starland RAT and WLDR framework, primarily targeting the finance sector in countries including the United States of America, Germany, Romania, Venezuela, and the Bolivarian Republic of. The campaign's impact necessitates priority defensive action, focusing on auditing Windows Startup folders and registry keys for unauthorized entries. Given the operational risk band is high, reaching command-and-control levels, immediate attention is required to mitigate potential breaches.

Threat Overview

UAT-11795, the attributed threat actor, utilizes a range of malware families including Starland RAT, WLDR, CastleStealer, and Remcos RAT. The primary targets are within the finance sector across multiple

countries. While the central CVE is insufficient, the actor's techniques involve various system discoveries, data capture, and evasion methods, indicating a sophisticated approach to compromising systems.

Attack Chain and Priority Control

The attack chain involves multiple techniques, starting from user execution and process discovery, moving through system information and owner discovery, to more intrusive methods like screen capture and data extraction from local systems. The priority technique identified is T1547.001, Registry Run Keys / Startup Folder, which serves as a critical chokepoint in the attack chain. The concrete control to mitigate this involves auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries, with a specific alert on .lnk or script creation in Startup by browser/email temp paths.

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed in this campaign. Additionally, no malware families have been corroborated by abuse.ch, and AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. This lack of corroboration highlights the need for vigilance based on the techniques and malware families identified rather than relying on external infrastructure indicators.

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
- T1033 System Owner/User Discovery
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1497 Virtualization/Sandbox Evasion
- T1204 User Execution
- T1057 Process Discovery
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1012 Query Registry
- T1614 System Location Discovery
- T1518.001 Security Software Discovery

- T1071.001 Web Protocols
- T1124 System Time Discovery

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2973).
- 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 0.562; 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
Stealth Falcon	0.562
Windshift	0.5
Inception	0.4551
Darkhotel	0.4551
APT37	0.4518

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
Hash	a6821c7e9bfe2e6af0f690d906ec6a26161e2198c256fb60f3b4731c317f3ad9
Hash	c33f097fdb2b69b4cbb1c3f29ae88b43
Hash	650e751e8ee5f5958c6a70288a24a4e3d19904a2
Hash	1b46f761719dce44baa2d7b417c5214fc41c080f7f9ba485e7e489d949097f1f

Type	Indicator
Hash	2a27b3415114b874da295c19cce5227a8b8d9525cc2da331034a1f45528eecae
Hash	2c7a99f137efd718f89cf8b260379c99af89ea1939568df09314918f2c5999a3
Hash	365024336c7681ac0854321ac6c140a245b9593285da02d2a590124cdc592370
Hash	36e3838d07978f49ebe6546d57d2f311b8d6566558bcd58448e921c988cc346a
Hash	451ac8ca34d5bcdfe476465f69eb517b2608f267c7e8d69f8ef36197a6f1d949
Hash	575ce92c473e6d47810321e309a4e29dd7f52f4152526b0bdca80f54b53aed2f
Hash	5b9bf7957a9f8869c87ace1a6d76b48e2623073e72739ad0636b5dfa4bb2e0c3
Hash	603fd9724de346a06e00c1b8502c2ac1180812a18bbf30032dab8d469e5c18e1
Hash	6ca7a458985350ac082a9c9820d7f8d39128a4c4bda2f5d32f169a45b7b22bc6
Hash	7dc77a5abab119960fbe42b1535c957020cce1b8e0a3cf58d4eddc51b5bf9940
Hash	896185a89bd7eb0520b03fdcfb8db0be98b43cf15f14041d73b23d3988c1bcab
Hash	964256d3259b6e0c701ec04116c45cf0ec381c1c209dc29b09a7930cd7a4810b
Hash	a080b5380ccc8fc40b24c02151d305efc32d931dc547881e01a2e6f2b070c7dc
Hash	a1835d333ac3db961a8ff1f4864e3c10a6f73a872c040599091390a009ac7804
Hash	a32ac345e39cb7606322e2155bd7b4d6941c1678619e48d1f14d9301ee53e6c0
Hash	0ddc62ec74a816a8a0607b16f2be9073
Hash	3111f846b1cb76de775eabb62625cdda
Hash	38167e35c0ceb08f2d11dc271243db3c
Hash	57c6617c205f8dc296c41606ccc5cc16
Hash	6337c9dcd6b6c7c122e26b008032e8ba
Hash	7ed31a99036b9aecb028707ae082b108
Hash	844c462e920593242594050f82643f7b
Hash	9000b4d28f2736cf84147ddc0ff3b59e
Hash	90dc1e26741120859d97cd287da38a78
Hash	a86b42c731d12b5a4fb156ee3175fe86

Type	Indicator
Hash	b099fe4c46c53403b7657cbfe18b8ac4
Hash	b2b25a59e1e0cc74804344d631629fd2

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 adversary, UAT-11795, could pivot to T1543 Create or Modify System Process by attempting to create a malicious system process that mimics a legitimate one, potentially allowing them to maintain persistence and evade detection. This technique may be particularly appealing as it could enable the adversary to execute their malicious code with system-level privileges, which would likely be necessary to achieve their objective after being blocked from using Registry Run Keys / Startup Folder. To counter this potential move, the mandated defensive control of restricting service/daemon creation to admins and monitoring service and driver installs should be implemented.

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