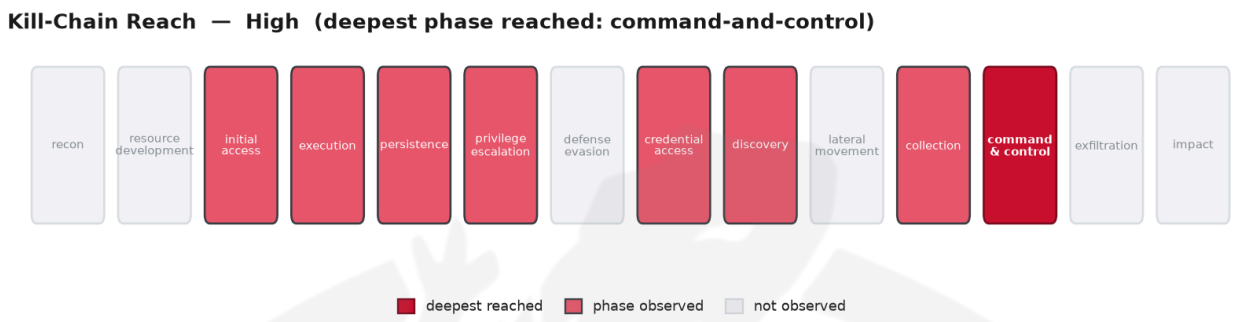
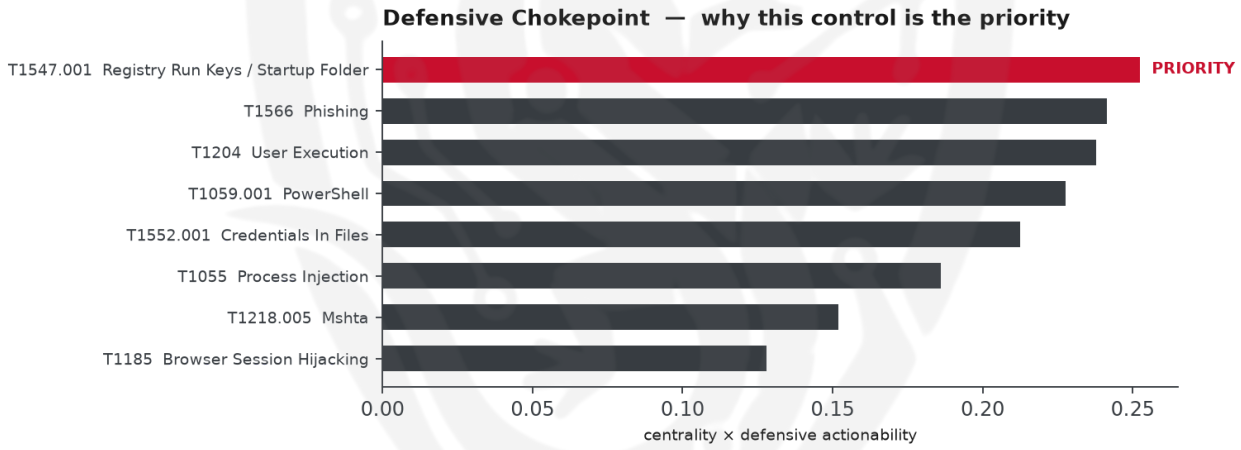
THREAT REPORT: UAT-11795

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 targeting the United States of America with a range of malware families, including Starland RAT, WLDR agent, CastleStealer, and Remcos RAT. The actor's techniques include scheduled tasks, keylogging, and system information discovery, among others. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries. The threat actor's activities pose a high operational risk, reaching command-and-control levels.

Threat Overview

UAT-11795, the observed threat actor, utilizes a variety of malware families, including Starland RAT, WLDR agent, CastleStealer, and Remcos RAT, to target victims in the United States of America. The central vulnerability exploited is currently unknown due to insufficient data. The actor's techniques include

scheduled tasks, keylogging, system information discovery, and other methods to gain access to and control over victim systems.

Attack Chain and Priority Control

The threat actor's attack chain involves a series of techniques, including scheduled tasks, keylogging, and system information discovery, ultimately leading to the establishment of persistence and control. 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 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 campaign. Additionally, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with a confidence level of 80% or higher by AbuseIPDB, 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
- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1082 System Information Discovery
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1185 Browser Session Hijacking
- T1083 File and Directory Discovery
- T1552.001 Credentials In Files
- T1218.005 Mshta
- T1204 User Execution
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1566 Phishing
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information
- T1071.001 Web Protocols
- T1059.005 Visual Basic

- T1055.001 Dynamic-link Library Injection

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2658).
- 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 0.5189; 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	0.5189
Inception	0.5045
Dark Caracal	0.4949
RedCurl	0.4811
Molerats	0.4707

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	w32[.]b8be9a5e0a-95[.]sbx[.]tg
Hash	38de5b216c33833af710e88f7f64fc98
Hash	9f1f11a708d393e0a4109ae189bc64f1f3e312653dcf317a2bd406f18ffcc507
Hash	9896a6fcb9bb5ac1ec5297b4a65be3f647589adf7c37b45f3f7466decd6a4a7f
Hash	66c72019eafa41bbf3e708cc3824c7c4447bdab6

Type	Indicator
Hash	2915b3f8b703eb744fc54c81f4a9c67f
Hash	c2efb2dcacba6d3ccc175b6ce1b7ed0a
Hash	b34d42e320d6674d7747fcb93083c6d59feadb99
Hash	90b1456cdbe6bc2779ea0b4736ed9a998a71ae37390331b6ba87e389a49d3d59
Hash	0398df5a18f71efcfeef4571a2cef577
Hash	b8be9a5e0a191050f9099c11c155b436863e9bc43bc904cdb842e249679aa35a

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:** UAT-11795 used T1053.005 Scheduled Task here as an alternative persistence technique.
- **Projected pivot:** T1053.005 Scheduled Task (persistence)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The adversary, UAT-11795, could pivot to utilizing Scheduled Task (T1053.005) to maintain persistence and achieve their objectives, potentially by creating a new scheduled task that blends in with legitimate system activity. They may attempt to leverage this technique to execute malicious code at a later time, evading detection. To counter this, the defensive control would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Detection and hardening for the pivot (T1053.005 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