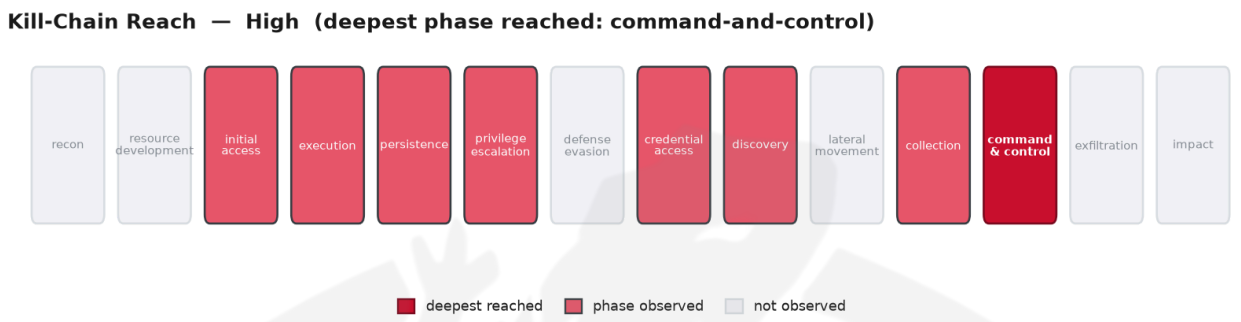
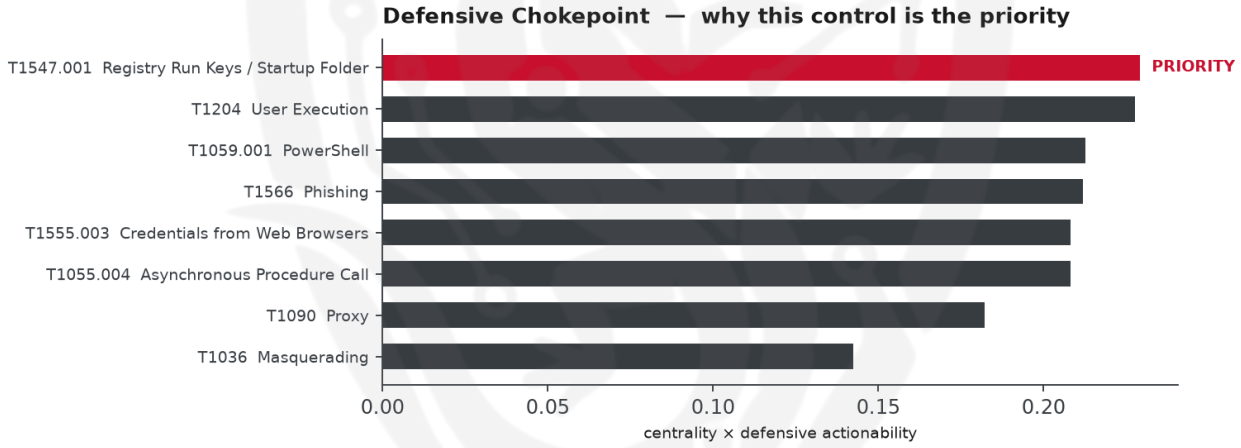
THREAT REPORT: UAT-11795

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 that has been observed deploying the Starland RAT and bespoke WLDR C2 implant in a financially motivated campaign. The targeted countries include the United States of America, Germany, Romania, Venezuela, and the Bolivarian Republic of. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to mitigate the threat. The actor's use of various techniques, including scheduled tasks and screen capture, poses a significant risk to affected systems.

Threat Overview

The threat actor, UAT-11795, has been observed using a range of malware families, including Starland RAT, WLDR agent, CastleStealer, and Remcos RAT. The central vulnerability exploited is currently unknown, but the actor has been targeting various countries and sectors. The actor's techniques include system owner/user discovery, keylogging, and symmetric cryptography, among others.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, starting with initial access and progressing to system information discovery, file and directory discovery, and finally, to command-and-control. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which serves as a 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

The malicious infrastructure is hosted on BL Networks, according to third-party observations. Additionally, abuse.ch has corroborated the presence of an Unknown RAT malware family. However, AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. These corrobations provide additional context to the threat actor's activities but do not override the source's assessment.

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
- T1056.001 Keylogging
- T1573.001 Symmetric Cryptography
- T1082 System Information Discovery
- T1140 Deobfuscate/Decode Files or Information
- T1036 Masquerading
- T1555.003 Credentials from Web Browsers
- T1090 Proxy
- T1083 File and Directory Discovery
- T1055.004 Asynchronous Procedure Call
- 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
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2413).
- 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 0.5298; 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	0.5298
Inception	0.5281
APT37	0.5173
Winter Vivern	0.5132
Higaisa	0.5109

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 0%.
- Malware families corroborated by abuse.ch: Unknown 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	193[.]149[.]176[.]254	AbuseIPDB 0% (US) · AS399629 BL Networks
Domain	windowscreenrepairnearme[.]com	Unknown RAT

Type	Indicator	Context
Domain	zynaris[.]io	
Domain	aipythondevs[.]com	
Domain	alphabitcapital[.]info	
Domain	eorthopaedics[.]com	
Domain	niggerdemon[.]in	
Domain	sastoro[.]com	
Domain	web-devtools[.]com	
URL	hxxps://eorthopaedics[.]com/feed/cew78zwvd2/	
URL	hxxps://eorthopaedics[.]com/feed/gnsmetadyx54/	
URL	hxxps://eorthopaedics[.]com/feed/note	
URL	hxxps://sastoro[.]com/alpha/dpyb8w3ycih8/	
URL	hxxps://sastoro[.]com/alpha/nrpilqjnut/	
URL	hxxps://web-devtools[.]com/dopfile	
URL	hxxps://web-devtools[.]com/file[.]zip	
URL	hxxps://web-devtools[.]com/starlandfox	
URL	hxxps://web-devtools[.]com/x32remka	
URL	hxxps://windowscreenrepairnearme[.]com/command	
Hash	a6821c7e9bfe2e6af0f690d906ec6a26161e2198c256fb60f3b4731c317f3ad9	
Hash	c33f097fdb2b69b4cbb1c3f29ae88b43	
Hash	650e751e8ee5f5958c6a70288a24a4e3d19904a2	

Type	Indicator	Context
Hash	162e436f18fe6099c57855c8d63fd747493624e87702dc749b242eb9a6b758ca	
Hash	17e41d66ebfd56edc960f58f4285697ceceaa812514bb15092672c747979896e	
Hash	1a01ad25712d306f27f526332fdccf959f2de53207b54e4e80f60faa804d6cb6	
Hash	1b46f761719dce44baa2d7b417c5214fc41c080f7f9ba485e7e489d949097f1f	
Hash	2751281d3800d82ecd3fad7c1d2293f3b947875a343b0672b4f4024a261165d2	
Hash	2a27b3415114b874da295c19cce5227a8b8d9525cc2da331034a1f45528eecae	
Hash	2c7a99f137efd718f89cf8b260379c99af89ea1939568df09314918f2c5999a3	
Hash	365024336c7681ac0854321ac6c140a245b9593285da02d2a590124cdc592370	
Hash	36e3838d07978f49ebe6546d57d2f311b8d6566558bcd58448e921c988cc346a	
Hash	451ac8ca34d5bcdfe476465f69eb517b2608f267c7e8d69f8ef36197a6f1d949	
Hash	47dedb08385449d48d8b6543030310317c92cddafa25e14ee0cb9a32d53ced5c	
Hash	575ce92c473e6d47810321e309a4e29dd7f52f4152526b0bdca80f54b53aed2f	
Hash	5b9bf7957a9f8869c87ace1a6d76b48e2623073e72739ad0636b5dfa4bb2e0c3	
Hash	603fd9724de346a06e00c1b8502c2ac1180812a18bbf30032dab8d469e5c18e1	
Hash	6ae334ce60d1a9b7fb96d1d0d0eda5ec7c2c31d3f0cf3e4d7e3056504d50043d	
Hash	6ca7a458985350ac082a9c9820d7f8d39128a4c4bda2f5d32f169a45b7b22bc6	

Type	Indicator	Context
Hash	7dc77a5abab119960fbe42b1535c957020cce1b8e0a3cf58d4eddc51b5bf9940	
Hash	896185a89bd7eb0520b03fdcfb8db0be98b43cf15f14041d73b23d3988c1bcab	

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:** 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 could pivot to utilizing Scheduled Task (T1053.005) to maintain persistence and achieve their objectives, potentially by creating a new task that blends in with legitimate system activity. This approach may allow them to bypass the blocked Registry Run Keys / Startup Folder control, as Scheduled Task provides an alternative means to execute malicious code at system startup or on a scheduled basis. The defensive control to counter this 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