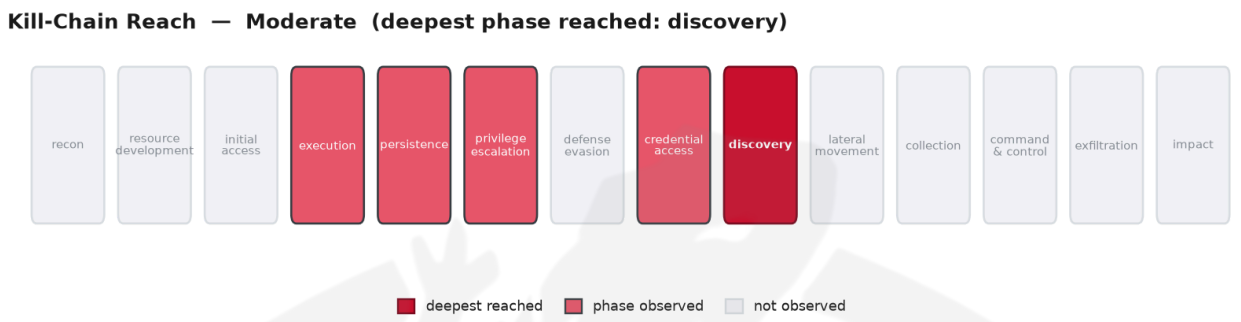
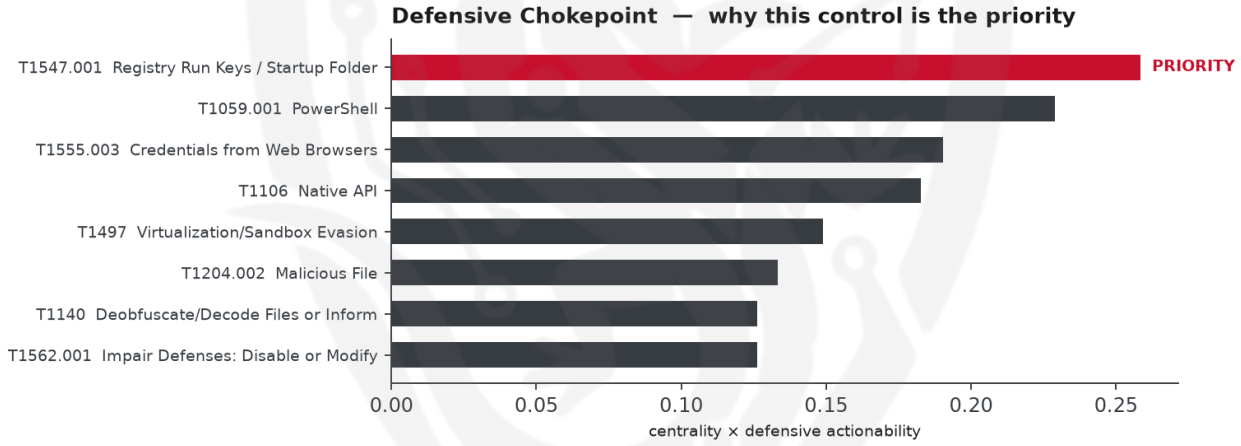
THREAT REPORT: Y2K OPERATORS

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 Y2K Operators, who have been observed utilizing various malware families, including Millenium RAT, AsyncRAT, and njRAT, to target unspecified countries and sectors. The threat actor's primary goal appears to be stealing sensitive information and gaining persistence on compromised systems. Priority should be given to auditing Windows Startup folders and Run/RunOnce registry keys for unauthorized entries to mitigate the threat. The operational risk band is considered Moderate, indicating a significant threat that requires attention.

Threat Overview

Y2K Operators, the attributed threat actor, have been associated with a range of malware families, including Millenium RAT, AsyncRAT, XWorm, njRAT, Njw0rm, LV, Bladabindi, and others. The central vulnerability exploited by the threat actor is currently unknown due to insufficient data. The victimology of the threat is also unclear, with targeted countries and sectors not specified.

Attack Chain and Priority Control

The observed techniques employed by the threat actor form a complex chain, involving various tactics such as stealing web session cookies, bypassing user account control, and discovering system information. The priority technique, T1547.001 Registry Run Keys / Startup Folder, serves as a critical chokepoint in the attack chain. To counter this, the recommended 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 associated with Y2K Operators has been observed to be hosted by providers such as Omegatech LTD and Femo IT Solutions Limited. Additionally, abuse.ch has corroborated the presence of malware families like Amadey, Lumma Stealer, and MilleniumRAT, which are linked to the threat actor. However, AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 29%.

Technical Appendix

Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.

Observed Techniques (ATT&CK, expert-tagged by source)

- T1539 Steal Web Session Cookie
- T1548.002 Bypass User Account Control
- T1036.005 Match Legitimate Resource Name or Location
- T1204.002 Malicious File
- T1082 System Information Discovery
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1555.003 Credentials from Web Browsers
- T1217 Browser Information Discovery
- T1083 File and Directory Discovery
- T1497 Virtualization/Sandbox Evasion
- T1057 Process Discovery
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1012 Query Registry
- T1614 System Location Discovery
- T1518.001 Security Software Discovery
- T1059.003 Windows Command Shell
- T1070.004 File Deletion
- T1518 Software Discovery

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2721).
- Operational risk: Moderate (score 0.539, reaches discovery).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.4951; 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
Darkhotel	0.4951
Patchwork	0.4607
Malteiro	0.4415
Tropic Trooper	0.4372
APT37	0.426

Enrichment Signal

- Highest AbuseIPDB confidence among IOCs: 29%.
- Malware families corroborated by abuse.ch: Amadey, Lumma Stealer, MilleniumRAT, MillenuimRAT, Shim RAT, Unknown Stealer.
- 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	62[.]60[.]226[.]97	AbuseIPDB 0% (DE) · Unknown Stealer · AS214351 Femo IT Solutions Limited
IP	130[.]12[.]180[.]43	AbuseIPDB 29% (DE) · Amadey · AS202412 Omegatech LTD

Type	Indicator	Context
IP	158[.]94[.]208[.]168	AbuseIPDB 12% (DE) · AS202412 Omegatech LTD
Domain	blackhatusa[.]com	malware_download
Domain	modedapk[.]net	Lumma Stealer
URL	hxxps://blackhatusa[.]com/update[.]exe	malware_download
URL	hxxps://blackhatusa[.]com/clip[.]exe	malware_download
URL	hxxps://blackhatusa[.]com/setup[.]exe	malware_download
URL	hxxp://130[.]12[.]180[.]43/files/7924412375/upOSLDn[.]exe	malware_download
URL	hxxp://158[.]94[.]208[.]168/files/8514679081/DRTjyu7[.]exe	malware_download
Hash	7b6473f036225bc35da89e5049ae55ba	
Hash	ddbc1037925f7d6c07a9ddbe38286a2fcedc4890	
Hash	ccca11a6d5835999c40a0a5264084b3740633600c157754fad2ef59559e31736	
Hash	a1c160243efd54a9bf00655966971aae	MilleniumRAT
Hash	cc2c9d90ffba060c9521d40776ffaa907ecec2bb	MilleniumRAT
Hash	512adab2c69feaf026adfb12cbd7d2eb4fee746120491e44f476eebddcbb19f2	MilleniumRAT
Hash	66bf111030a2e22db575c0b7b7b677208745eef8b44265bb4259f41f126f1bf8	MillenuimRAT
Hash	7d8b6a64f7b65b281e7b5568929c6f96c62bbae9628162aabe7d8140a86d3de8	Shim RAT
Hash	754ba4fb2e083944f84ba50b90ddda87	
Hash	f27b08a8347e1ba84a61fbfe58edcb8f84d06642	
Hash	5a23ca644cb1f310be1abd5f6c6a3b3e15681ced99b0947a7f3465a79aae5089	

Type	Indicator	Context
Hash	8f8a71352d2f18162f2f74090dc6f0cae6b37029e3244e6522825ade75163055	MillenuimRAT
Hash	a8acc24bb3e6a1a3b66a31ceaefda07d4a0e17415468683458b499f2ba240450	
Hash	d55ce447e249ef9045750865fa196c8ca8434c8c484f861b7bdecbceeab7c16e	
Hash	ad0f892b7b99b68491ade4949ef6b575e64d9df5f84a53019b5c1e4eeb4c46a9	
Hash	1d699a46339626db299548e32ed3a77eec267840c3de39b49caf38b88aeb150d	MillenuimRAT
Hash	066576554f9eff84eaa415a4bd012b2e	
Hash	07a364ba1b34d0b04bb68872006d9615	
Hash	195d1c56f35d7a8d38e2ab0cdc1fa8cd	
Hash	1ef2f666b543293aaec55d10fbc4bc46	
Hash	35af4c61ce04f0c0796baf5831e2ef24	
Hash	35dfec976f6fd85f76d011d0075b5926	
Hash	3c1032e271dd885e912a79c67f2855e7	
Hash	4f32d85224309688c600c21865294717	
Hash	52deca7016315faf844f0ba0d754027e	
Hash	53e78d1fef04a39353a7dbc19f8ac86d	
Hash	6dc5e2f50900ba1e7a4ee87f950fa409	MilleniumRAT
Hash	87e06d8cec9cf7c2808d17c836089053	
Hash	89aa2ce1978f3386f9ee433515e457b1	
Hash	a0503abcebf054a006fd4436a73c2dd7	

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:** 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:** T1053 Scheduled Task/Job (persistence)
- **Basis:** 37 of 170 documented groups that use Registry Run Keys / Startup Folder also use Scheduled Task/Job (conditional 0.64, lift 1.9, i.e. ~1.9x base rate). Strongest same-tactic neighbour.

The Y2K Operators could pivot to utilizing T1053 Scheduled Task/Job to maintain persistence and achieve their objectives, potentially by creating new scheduled tasks that mimic legitimate system activities. This technique may allow them to bypass the blocked Registry Run Keys / Startup Folder control, as scheduled tasks can still be used to execute malicious code at recurring intervals. To counter this potential move, the defensive control would be to alert on new scheduled tasks (Event ID 4698); restrict schtasks/at to admins; baseline legitimate task creators.

Also plausible (same tactic): T1078 Valid Accounts (n=27, lift 1.2), T1543 Create or Modify System Process (n=18, lift 1.8)

Detection and hardening for the pivot (T1053 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