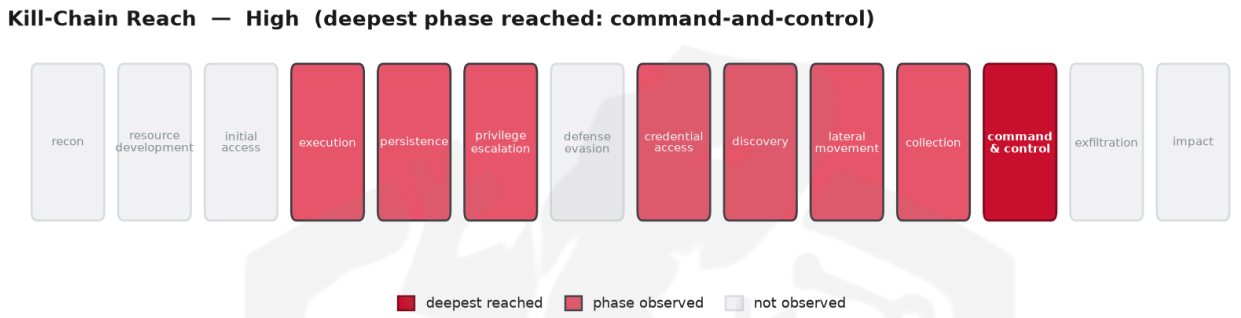
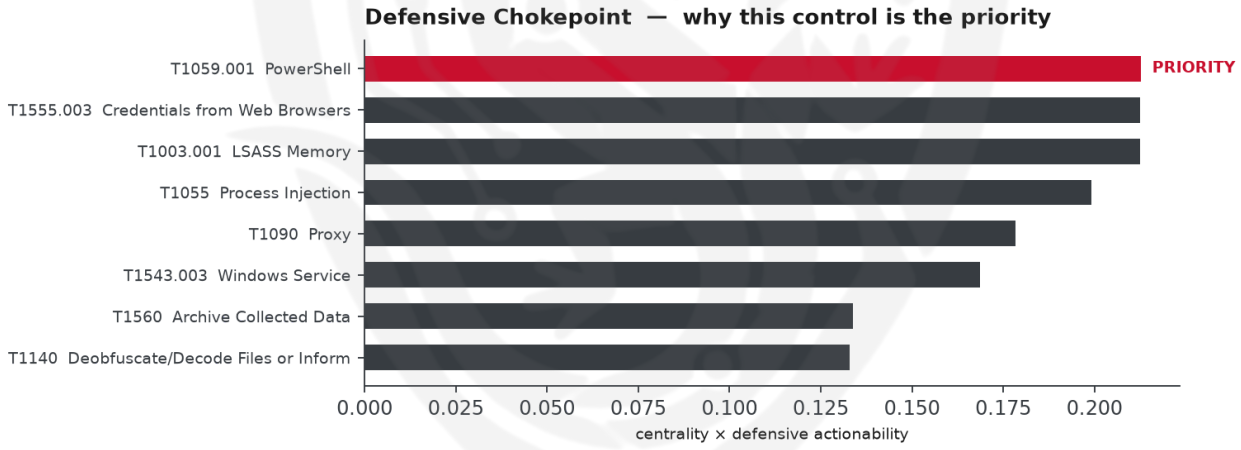
THREAT REPORT: CENTRAL ASIA CAMPAIGN WITH OCTLURK AND SILKLURK BACKDOORS

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 has been targeting countries in Central Asia, including Afghanistan, Kazakhstan, Kyrgyzstan, Syrian Arab Republic, Tajikistan, and Uzbekistan, with a focus on government, healthcare, and education sectors. The threat actor is utilizing various malware families, including OctLurk, SilkLurk, and PlugX, to gain access to sensitive information. Priority should be given to constraining PowerShell to prevent further exploitation. The threat actor's use of multiple techniques, including scheduled tasks and keylogging, highlights the need for comprehensive defensive measures.

Threat Overview

The threat actor, whose identity is currently insufficient to determine, is using a range of malware families, including OctLurk, SilkLurk, LurkProxy, and PlugX, to target organizations in Central Asia. The malware is

designed to collect sensitive information, including emails and credentials, and to establish a persistent presence on compromised systems. The victimology suggests that the threat actor is interested in gaining access to government, healthcare, and education systems.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex chain, including scheduled tasks, keylogging, email collection, and process injection. The priority technique is T1059.001 PowerShell, which is used to execute malicious commands and scripts. To mitigate this threat, the priority control is to Constrain PowerShell (Constrained Language Mode + AppLocker/WDAC); enable script-block and module logging; alert on encoded commands.

Infrastructure and Corroboration

There is currently no information available on the hosting providers or ASNs used by the threat actor, and no malware families have been corroborated by abuse.ch. Additionally, 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
- T1114 Email Collection
- T1543.003 Windows Service
- T1119 Automated Collection
- T1005 Data from Local System
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1560 Archive Collected Data
- T1555.003 Credentials from Web Browsers
- T1003.001 LSASS Memory
- T1090 Proxy
- T1083 File and Directory Discovery
- T1059.001 PowerShell
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1132 Data Encoding
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1021.001 Remote Desktop Protocol

Analytical Scores

- Priority technique (graph chokepoint): T1059.001 PowerShell (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 0.4636; 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
RedCurl	0.4636
APT3	0.455
Stealth Falcon	0.4336
Ke3chang	0.4286
APT39	0.4232

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	confbase[.]mdpsupport[.]net
Domain	fm01[.]clouddevicemetrics[.]com
Domain	ssl[.]blsouqs[.]com
Domain	about[.]blsouqs[.]com
Domain	api2[.]annoyingremote[.]com
Domain	ctyuhjerf[.]kozow[.]com

Type	Indicator
Domain	digital[.]leroymerling[.]com
Domain	dns[.]multitoconference[.]com
Domain	dns[.]ssentialserv[.]xyz
Domain	gycudore[.]kozow[.]com
Domain	rgnojb[.]casacam[.]net
Domain	tj[.]tajikistandip[.]com
Domain	tyhbgtyuj[.]gleeze[.]com
Domain	uyhvfredc[.]accesscam[.]org
Domain	wedfcvbn[.]gleeze[.]com
Hash	62944e26b36b1dcace429ae26ba66164
Hash	cf903e4a1629aa0582fd0363b5786676
Hash	9a1dd1d96481d61934dcc2d568971d06
Hash	18dc8bff47cc282508354771d0c8cf8c
Hash	cc5cc2546d3ea8e27250cc4bec24f6ca13caf341
Hash	23b122deea347dbe2407c1542c1cc6caaafca537eb5d1950a4ed7c8a69395dbb
Hash	082d49ef9f14e6811d68c7e0e82e5069
Hash	1415a78b75de7db4ba3d1e61d7db4501
Hash	2a571f6cee42a17d873f4c942649813f
Hash	2f18472866f38c1e1c2c5c14b9a6ab56
Hash	32a5985543433a4f60da2fafd873b927
Hash	37dc84e4bcad92fa28f1e7778d088283
Hash	3c9a1ba8e0c7475706adc6376e9d7b7c
Hash	45cf5916fab4272a1313c26e67aa9220
Hash	4e6d5c4770d5a822d7fcce6a74f7ad73
Hash	5e26df131ff0a679a0a2699b723b46e3

Type	Indicator
Hash	6ecf84fb18f6747ed08d7598364d853a
Hash	7c2f64461bb519c6cbf1fc687675514c
Hash	8269d6ba1b6842f9152c90cf7add9b93
Hash	a0cc7accc79abb0287aaba825d0351f0
Hash	a4d550a3ba0cd073fe3839b99d98a7a8
Hash	a56cce62930a6bee80d679b4c495a340
Hash	b874123a80fc4f40e06872b9cb54ebc6
Hash	be4731c09734da2e8eb6814a9c82f266
Hash	ef59aad625eebda8650aec5820d6ce69

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:** T1059.001 PowerShell (execution)
- **Observed here:** T1059.001 PowerShell was the only execution technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 40+ groups that use PowerShell, this pairing runs 1.3x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain their access and reconnaissance capabilities, as this technique allows them to leverage the existing Windows management infrastructure to gather information and interact with the system, potentially bypassing the restrictions imposed by the blocked PowerShell control. This technique may be particularly appealing to the actor because it enables them to execute commands and access system information in a more stealthy manner, which could help them to achieve their objectives without being detected. To counter this potential move, the mandated defensive control is to monitor wmiprvse.exe child-process creation; restrict remote WMI (DCOM) at the host firewall; enable WMI-Activity operational logging.

Also plausible (same tactic): T1574 Hijack Execution Flow (n=32, lift 1.2), T1106 Native API (n=19, lift 1.3)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command