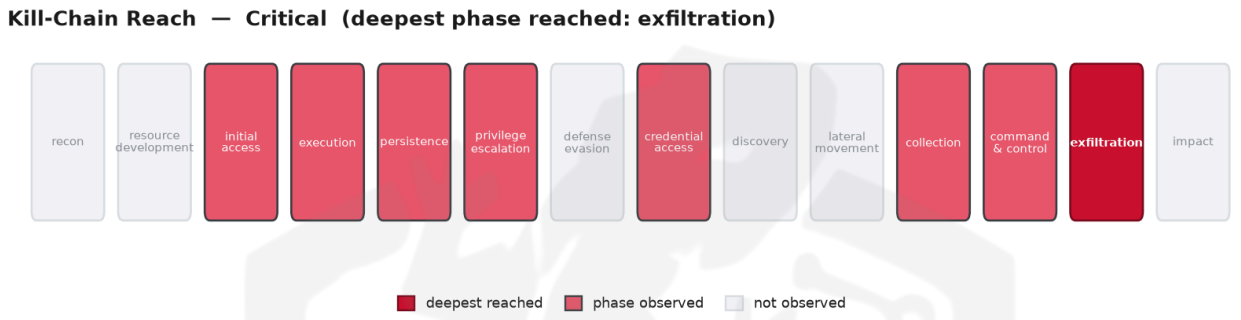
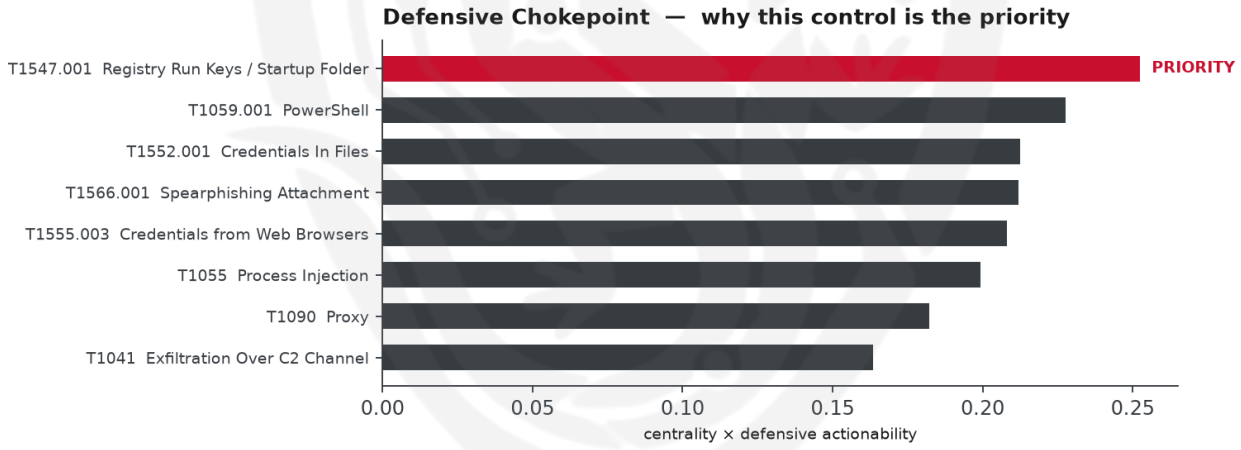
THREAT REPORT: ARMORED LIKHO'S BUSYSNAKE STEALER CAMPAIGN

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 Armored Likho, who has been observed using the BusySnake Stealer, AquilaRAT, and Go2Tunnel malware families to target government and energy sectors in Brazil, Kazakhstan, and the Russian Federation. The threat actor's primary goal appears to be data exfiltration, and priority should be given to defending against this campaign. The lack of a central CVE exploit suggests a potential focus on social engineering and exploitation of user credentials.

Threat Overview

Armored Likho is utilizing a range of malware families, including BusySnake Stealer, AquilaRAT, and Go2Tunnel, to compromise targets. The observed techniques include screen capture, keylogging, and

stealing web session cookies, among others. The targeted countries are Brazil, Kazakhstan, and the Russian Federation, with a focus on government and energy sectors.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including initial access, execution, and exfiltration. The priority technique is T1547.001 Registry Run Keys / Startup Folder, which is a critical chokepoint in the attack chain. To mitigate this threat, 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 is hosted on providers such as Namecheap Inc. and BL Networks, as observed by third-party sources. However, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB confidence of 80% or higher, 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)

- T1113 Screen Capture
- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1204.002 Malicious File
- T1566.001 Spearphishing Attachment
- T1140 Deobfuscate/Decode Files or Information
- T1219 Remote Access Tools
- T1055 Process Injection
- T1555.003 Credentials from Web Browsers
- T1090 Proxy
- T1552.001 Credentials In Files
- T1041 Exfiltration Over C2 Channel
- 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
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1547.001 Registry Run Keys / Startup Folder (centrality 0.2658).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5477; 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
Ajax Security Team	0.5477
Molerats	0.5004
Inception	0.4951
Dark Caracal	0.4857
Gorgon Group	0.4815

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	Context
IP	159[.]198[.]41[.]140	AbuseIPDB 0% (US) · AS22612 Namecheap Inc.
IP	159[.]198[.]32[.]222	AbuseIPDB 0% (US) · AS22612 Namecheap Inc.
IP	159[.]198[.]75[.]219	AbuseIPDB 0% (US) · AS22612 Namecheap Inc.
IP	69[.]67[.]173[.]153	AbuseIPDB 0% (RO) · AS399629 BL Networks

Type	Indicator	Context
Domain	lvl99[.]store	
Domain	arvax[.]xyz	
Domain	grked[.]online	
Domain	ndrt[.]ink	
Domain	onetoken[.]ink	
Domain	varenie[.]live	
Domain	winupdate[.]ink	
Domain	winupdate[.]live	
Domain	myboard[.]chickenkiller[.]com	
Domain	myboard[.]twilightparadox[.]com	
Hash	8a100cbdf79231e70cee2364ebd9a4433fda6b4de4929d705f26f7b68d6aeb79	
Hash	393b498f2114cabc0b29d5fcd9dc6723	
Hash	a0b80c0ec77f62b0ed46edb3fef05ccb88c74afb	
Hash	0041fd1b2358cd08dbcbc28ea8fc3d20	
Hash	006887732ca4a4a46a97989cf4deeef6	
Hash	07213c419489c02791e8d67b91e404ef	
Hash	1096268fa2b3d454c86cf851cb782319	
Hash	1dba3e505491a260a44c867902c3296e	
Hash	2dfa1d949872c1b2f04952dd3e5f5d8f	

Type	Indicator	Context
Hash	5d5c3e483c5e544260ce98fc29fbf192	
Hash	6b45ddb39a6e86229348dcbba3857e7c	
Hash	7141917cba2eee2b4d31107faccf3a39	
Hash	732c31acf971a81c7e51b2a3dae82020	
Hash	78135f72ab148a0cc074f6b2dd51fff6	
Hash	7db9c688c620e54e8c69b7e52a7579fb	
Hash	80b7700053e115d65365ce7330383320	
Hash	8188b2f347b77d65d08cfb23808ac244	
Hash	894332174f536c2e1efeda05cba79f8b	
Hash	90378881856abfa47d7745c0a3ef9dc8	
Hash	a0ec7a8e61eff3f445a7455b3aef9fbb	
Hash	c019797a00fd56edb1f468ac0a598510	
Hash	c7622a1effa27bbfee6d6e03d6474343	
Hash	cf74ac018d158ea2c2cfa1b1d71d95bc	
Hash	ddff82a115558584bbd7741d4ffb35b4	
Hash	e2550cfad9dcc880bf04f6048f90868c	
Hash	f2ab09d7e7a375a192508a5014aa2ee4	

Reputation by AbuseIPDB · malware attribution by abuse.ch · Geo/ASN data by IP2Location LITE.