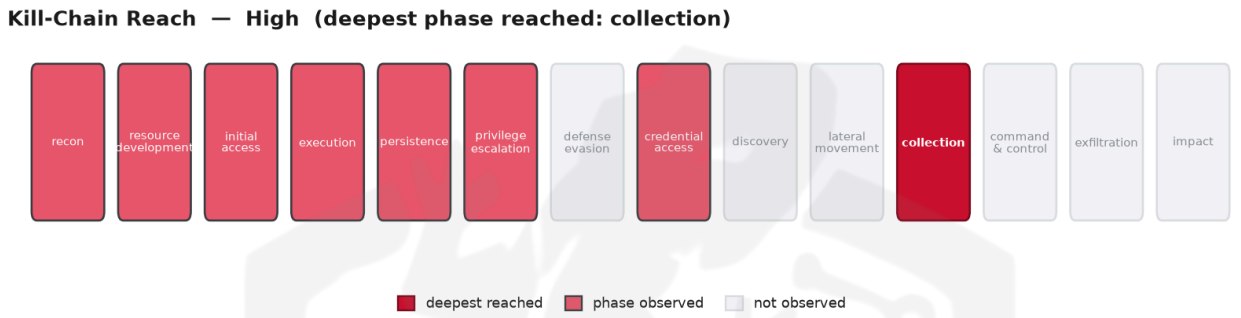
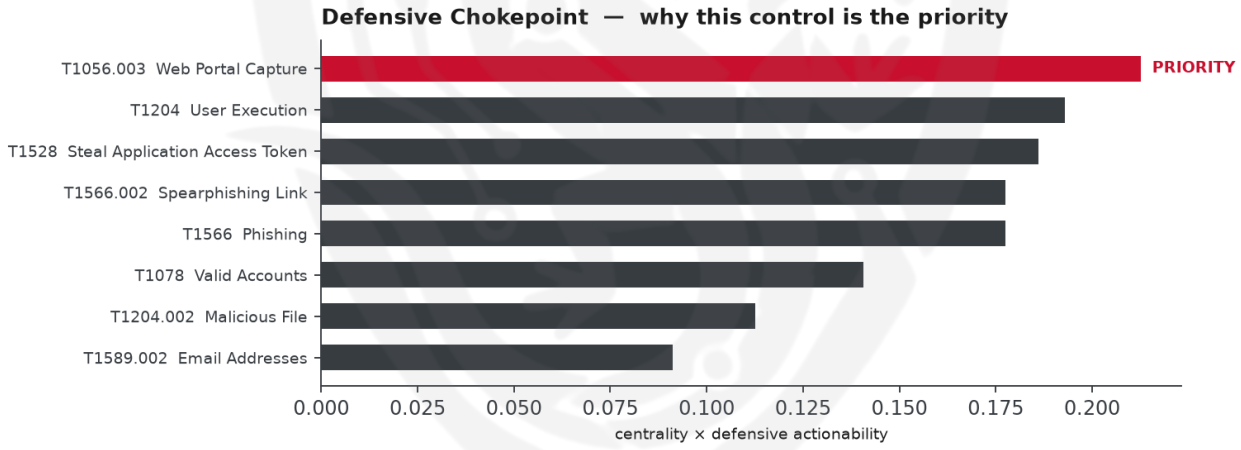
THREAT REPORT: UNKNOWN_ADVERSARY CAMPAIGN

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 observed cluster of activity has been targeting the education sector, with a focus on popular online platforms such as Roblox and Minecraft. The threat actor's tactics and techniques have been identified, but their identity and specific malware families used remain unknown. Priority should be given to defending against web portal capture and input capture techniques. The operational risk band for this threat is considered high, as it reaches the collection stage.

Threat Overview

The threat actor, whose identity is unknown, has been employing various techniques to compromise accounts and gather victim information. The techniques used include acquiring infrastructure, searching

victim-owned websites, and spearphishing. The actor's targets appear to be primarily in the education sector, although specific countries and industries are not identified.

Attack Chain and Priority Control

The observed techniques form a chain of events, starting with acquiring infrastructure and searching victim-owned websites, followed by spearphishing and compromising accounts. The priority technique identified is T1056.003 Web Portal Capture, which serves as a chokepoint in the attack chain. To mitigate this threat, the recommended priority control is to "Alert on keylogging hooks and API-input capture; restrict accessibility/hook installation."

Infrastructure and Corroboration

The malicious infrastructure associated with this threat has been observed to be hosted on various providers, including Florian Kolb, DigitalOcean LLC, Private Layer Inc, and PebbleHost Ltd. However, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with high confidence 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)

- T1583 Acquire Infrastructure
- T1594 Search Victim-Owned Websites
- T1204.002 Malicious File
- T1566.002 Spearphishing Link
- T1598.003 Spearphishing Link
- T1586.002 Email Accounts
- T1608.001 Upload Malware
- T1583.001 Domains
- T1589 Gather Victim Identity Information
- T1056.003 Web Portal Capture
- T1589.002 Email Addresses
- T1586 Compromise Accounts
- T1608 Stage Capabilities
- T1528 Steal Application Access Token
- T1204 User Execution
- T1590 Gather Victim Network Information
- T1566 Phishing
- T1078 Valid Accounts
- T1056 Input Capture
- T1598 Phishing for Information

Analytical Scores

- Priority technique (graph chokepoint): T1056.003 Web Portal Capture (centrality 0.3037).
- Operational risk: High (score 0.604, reaches collection).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5244; 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
EXOTIC LILY	0.5244
Star Blizzard	0.5221
IndigoZebra	0.4518
Silent Librarian	0.45
Moonstone Sleet	0.3795

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	45[.]11[.]229[.]230	AbuseIPDB 0% (DE) · AS58087 Florian Kolb
IP	167[.]71[.]73[.]127	AbuseIPDB 0% (NL) · AS14061 DigitalOcean LLC
IP	179[.]43[.]150[.]242	AbuseIPDB 0% (CH) · AS51852 Private Layer Inc
IP	45[.]143[.]198[.]6	AbuseIPDB 0% (GB) · AS212027 PebbleHost Ltd
Domain	roblox-com[.]com	
Domain	blox[.]ink	

Type	Indicator	Context
Domain	bloxlink[.]net	
Domain	bloxlink[.]site	
Domain	www-roblox[.]pw	
Domain	www[.]robiox[.]com[.]ua	
Domain	robiox[.]com[.]ua	
Domain	robiox[.]com[.]ps	
Domain	robiox[.]com[.]gr	
Domain	www[.]r[.]oblox[.]com[.]et	
Domain	verify-bloxlink[.]cfd	
Domain	r[.]oblox[.]com[.]et	
Domain	ro-verify[.]net	
Domain	shortsurl[.]bio	
Domain	rover-linked[.]com	
Domain	autosecure[.]cy	
Domain	bloxlink[.]com	
Domain	bloxlink[.]pro	
Domain	bloxlink[.]xyz	
Domain	blxup[.]shop	
Domain	freerobux[.]top	
Domain	htps-www-roblox[.]co	
Domain	httpss--roblox[.]co	
Domain	luau-lang[.]org	
Domain	oblox[.]shop	
Domain	rblox[.]shop	
Domain	rblxo[.]shop	

Type	Indicator	Context
Domain	ro-verify[.]ink	
Domain	ro-verify[.]org	
Domain	robbux[.]com	
Domain	robloxcommunity[.]com	
Domain	robloxcorporation[.]com	
Domain	robloxfree[.]com	
Domain	robloxgift[.]live	
Domain	robloxiuty[.]top	
Domain	robloxsupport[.]com	

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:** T1056.003 Web Portal Capture (credential-access)
- **Observed here:** the threat actor used T1056 Input Capture here as an alternative credential-access technique.
- **Projected pivot:** T1056 Input Capture (credential-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The threat actor could pivot to T1056 Input Capture to maintain their objective of capturing sensitive information, potentially by leveraging keyboard hooks or API calls to intercept user input. This would likely involve exploiting vulnerabilities in software or manipulating system configurations to facilitate input capture. The defensive countermeasure to mitigate this potential pivot is to implement the mandated control: Alert on keylogging hooks and API-input capture; restrict accessibility/hook installation.

- **Defensive countermeasure:** Alert on keylogging hooks and API-input capture; restrict accessibility/hook installation.