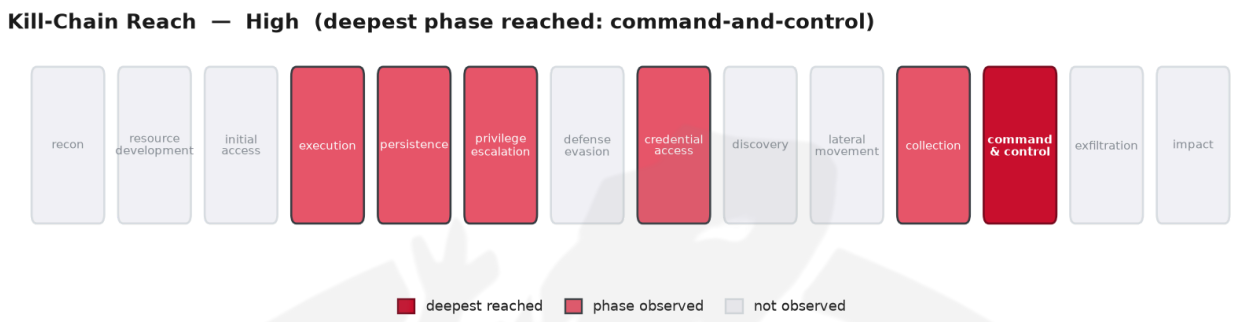
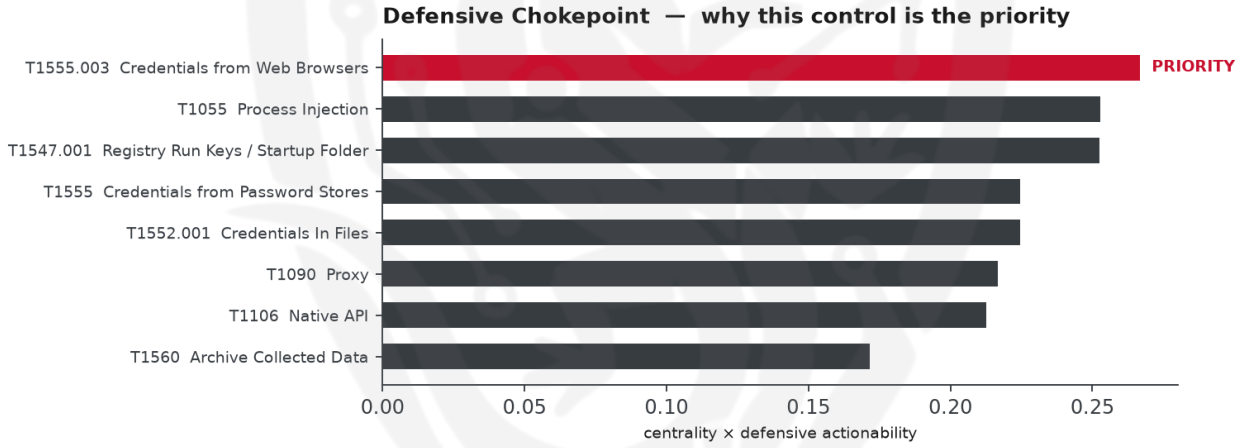
THREAT REPORT: KONTRAKTNIK

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 Kontraktnik, a threat actor utilizing the Dolphin X stealer malware to target over 300 apps and profiles, leveraging various techniques to compromise user credentials. The targeted country and sectors are not specified due to insufficient data. Priority should be given to restricting access to browser credential stores to mitigate the threat. The operational risk band is considered high, indicating a significant command-and-control capability.

Threat Overview

Kontraktnik, the attributed threat actor, employs the Dolphin X malware family to exploit unsuspecting users, although the central CVE exploited is not specified due to insufficient data. The threat actor's victimology is not clearly defined, with targeted countries and sectors remaining unknown.

Attack Chain and Priority Control

The observed techniques form a complex chain, including scheduled tasks, bypassing user account control, and process injection, among others. The priority technique is T1555.003, Credentials from Web Browsers, which serves as a critical chokepoint in the attack chain. To counter this, the recommended priority control is: Restrict access to browser credential stores; alert on reads of Login Data / cookies files by non-browser processes; enforce disk encryption.

Infrastructure and Corroboration

There is no observable hosting provider or ASN associated with the malicious activity, and no malware families have been corroborated by abuse.ch. Additionally, AbuseIPDB has not flagged any indicators with a confidence level 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)

- T1053.005 Scheduled Task
- T1548.002 Bypass User Account Control
- T1106 Native API
- T1555 Credentials from Password Stores
- T1055 Process Injection
- T1560 Archive Collected Data
- T1555.003 Credentials from Web Browsers
- T1090 Proxy
- T1552.001 Credentials In Files
- T1547.001 Registry Run Keys / Startup Folder
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1027 Obfuscated Files or Information

Analytical Scores

- Priority technique (graph chokepoint): T1555.003 Credentials from Web Browsers (centrality 0.3812).
- 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 0.4491; 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
APT37	0.4491
Putter Panda	0.3904
APT33	0.3766
Molerats	0.3615
Patchwork	0.3578

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	thedolphinx[.]top
Domain	backend[.]thedolphinx[.]top
URL	hxxp://backend[.]thedolphinx[.]top:8443
Hash	726e7fe23560fe03ea36163d5f510b494f41a78bf811c92ff219f64b4bfe2be0

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:** T1555.003 Credentials from Web Browsers (credential-access)
- **Observed here:** Kontraktnik used T1552.001 Credentials In Files here as an alternative credential-access technique.
- **Projected pivot:** T1552.001 Credentials In Files (credential-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

Kontraktnik could pivot to T1552.001 Credentials In Files by searching for unsecured files containing credentials on compromised systems, which may allow them to maintain access and achieve their objectives. They may attempt to exploit poorly secured files or configuration files to obtain sensitive

information. To counter this, the defensive control of removing secrets from code/config/registry, deploying a secrets manager, and scanning repos and hosts for credentials should be implemented.

- **Defensive countermeasure:** Remove secrets from code/config/registry; deploy a secrets manager; scan repos and hosts for credentials.