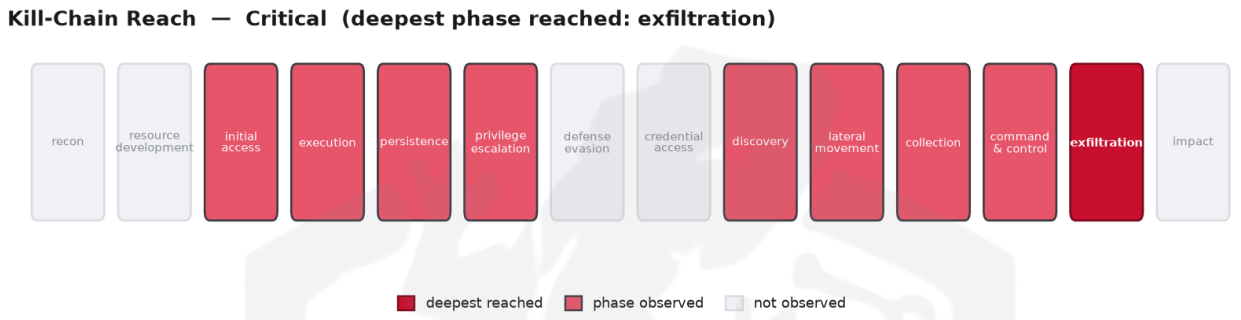
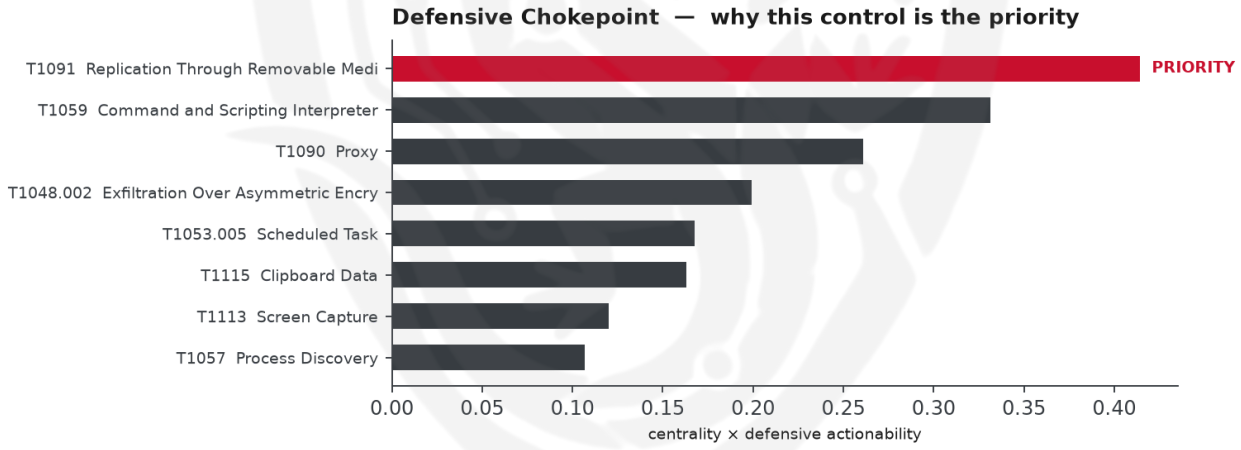
THREAT REPORT: UNKNOWN_ADVERSARY CRYPTO CLIPPER CAMPAIGN

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 identified utilizing malware families such as CryptoBandits and Contebrew, although the specific threat actor remains unknown. This campaign targets unspecified countries and sectors, exploiting various techniques to maintain persistence and control. Priority should be given to defending against the replication through removable media technique. The lack of specific attribution and targeted sectors makes it crucial to focus on the technical aspects of the attack to develop effective defensive strategies.

Threat Overview

The threat actor, referred to here as the observed cluster of activity, utilizes the CryptoBandits and Contebrew malware families. While the central CVE remains insufficient, the techniques employed include

scheduled tasks, screen capture, clipboard data theft, and more, indicating a sophisticated approach to data exfiltration and system control. The victimology of this campaign is not well-defined due to insufficient data on targeted countries and sectors.

Attack Chain and Priority Control

The attack chain involves a series of techniques including scheduled tasks, screen capture, and replication through removable media, among others. The priority technique identified is T1091 Replication Through Removable Media, which serves as a critical chokepoint in the attack chain. To mitigate this, the specific MITRE ATT&CK mitigation for T1091 should be applied, which involves adding host/network detections and implementing least-privilege controls around replication through removable media.

Infrastructure and Corroboration

There is no significant third-party corroboration regarding the hosting providers or ASNs observed in this campaign. Additionally, no malware families have been corroborated by abuse.ch, and AbuseIPDB has not flagged any indicators with a confidence level of 80% or higher, with the highest confidence seen being 0%. This lack of corroboration underscores the need to rely on the observed techniques and mitigation strategies to counter the threat.

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
- T1113 Screen Capture
- T1115 Clipboard Data
- T1091 Replication Through Removable Media
- T1090 Proxy
- T1059 Command and Scripting Interpreter
- T1048.002 Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
- T1057 Process Discovery
- T1027 Obfuscated Files or Information

Analytical Scores

- Priority technique (graph chokepoint): T1091 Replication Through Removable Media (centrality 0.4144).
- Operational risk: Critical (score 0.906, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3636; 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
MoustachedBouncer	0.3636
Molerats	0.3015
BlackOasis	0.3015
Higaisa	0.2825
Stealth Falcon	0.2767

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	facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd[.]onion
Domain	ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd[.]onion
Domain	cgky6bn6ux5wvlybtmm3z255igt52ljml2ngnc5qp3cnw5jlglamisad[.]onion
Domain	he5vnov645txpcv57el2theky2elesn24ebvgwfoewlpftksxp4fnxad[.]onion
Domain	shinypogk4jjniry5qi7247tznop6mxdrdte2k6pdu5cyo43vdzmrwid[.]onion
Domain	7goms4byw26kkbaanz5a5u5234gusot7rp5imzc3ozh66wwcvmcudjid[.]onion
Domain	gfoqsewps57xcyxoedle2gd53o6jne6y5nq5eh25muksqwzutzq7b3ad[.]onion
Domain	j3bv7g27oramhbxxuv6gl3dcyfmf44qnvju3offdyrap7hurfprq74qd[.]onion
Domain	lyhizqy2js2eh6ufngkbzntouiikdek5zsdj3qwa22b4z6knpqorgiad[.]onion
Domain	wt26llpl5k6gok3vnaxmucwgzv2wk3l7nuibbh25clghrtus3p5ctsid[.]onion

Type	Indicator
Hash	03b51af0a04467cebfa235199db4c02e
Hash	bbe05d2f2487ed09e1062111fd448822364a44a7
Hash	0020d23b0f9c5e6851a7f737af73fd143175ee47054931166369edd93338538a
Hash	100407796028bf3649752d9d2a67a0e4394d752eb8de86daa42920e814f3fae8
Hash	20db98af3037b197c8a846dbf17b87fc6f049c3e0d9a188f9b9a74d3916dd5e1
Hash	23c1e673f315dafa14b73034a90dd3d393a984451ff6601b8be8142be6487b43
Hash	35a6bc44b176a050fd6824904b7604f0f45b0fdfa26bf9500b9e05973b387cfd
Hash	67fc5cf395e28294bbb91ed0e954fdf2e80ebd9119022a115a42c286dc8bacf5
Hash	7630debd35cac6b7d58c4427695579b3e3a8b1cc462f523234cd6c698882a68c
Hash	7787a9a7d8ae393aa32f257d083903c4dc9b97a1e5b0458c4cd480d4f3cb5b05
Hash	9d90f54ae36c6c5435d5b8bed40faf54cc91f6db28574a6310b5ffaeb0362e96
Hash	a7abf1d9d6686af1cefcd60b17a312e7eb8cfe267def1ec34aeab6128c811630
Hash	b2777b73a4c33ac6a409d475057843be6b5d32262ef28a1f1ff5bb52e3834c5f
Hash	c824630154ac4fdfce94ded01f037c305eab51e9bef3f493c60ff3184a640502
Hash	cf9fc891ea5ca5ecd8113ef3e69f6f52ff538b6cccbdaa9559106fc72bc6da30
Hash	d14b80cbd1a19d4ad0473a0661297f8fdf598e81ff6c4ab24e212dcad2e54b3f
Hash	d43bf94f0cb0ab97c88113b7e07d1a4024d1610617b5ad05882b1dbab89e15ba
Hash	f3b54984caca95fd496bcfe5d7db1611b08d2f5b7d250b43b430e5d76393f9e0

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:** T1091 Replication Through Removable Media (initial-access)
- **Observed here:** T1091 Replication Through Removable Media was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1566 Phishing (initial-access)

- **Basis:** 7 of 170 documented groups that use Replication Through Removable Media also use Phishing (conditional 0.88, lift 1.5, i.e. ~1.5x base rate). Strongest same-tactic neighbour.

The actor could pivot to T1566 Phishing to maintain their objective by attempting to trick users into divulging sensitive information or installing malware, potentially exploiting the lack of caution when interacting with emails or messages. This technique may be used as an alternative to replicate their malicious activities, as it can be more challenging to detect and block compared to removable media. The defensive control to counter this would be to enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button.

Detection and hardening for the pivot (T1566 Phishing)

- **Telemetry:** Email security gateway logs; Endpoint (Office child processes); Proxy/DNS
- **Detect:**
  - Office apps (winword/excel) spawning script or LOLBIN child processes
  - Mark-of-the-Web bypass; ISO/IMG/LNK/HTML-smuggling attachments detonating
  - First-contact domains and newly registered domains in mail links
- **Harden:**
  - Attachment sandboxing; block high-risk types (iso, img, lnk, htm) at the gateway
  - Attack-surface-reduction rules for Office child processes; user reporting button
- **MITRE:** M1049 Antivirus/Antimalware, M1031 Network Intrusion Prevention, M1017 User Training, M1021 Restrict Web-Based Content · DS0015 Application Log, DS0009 Process, DS0029 Network Traffic