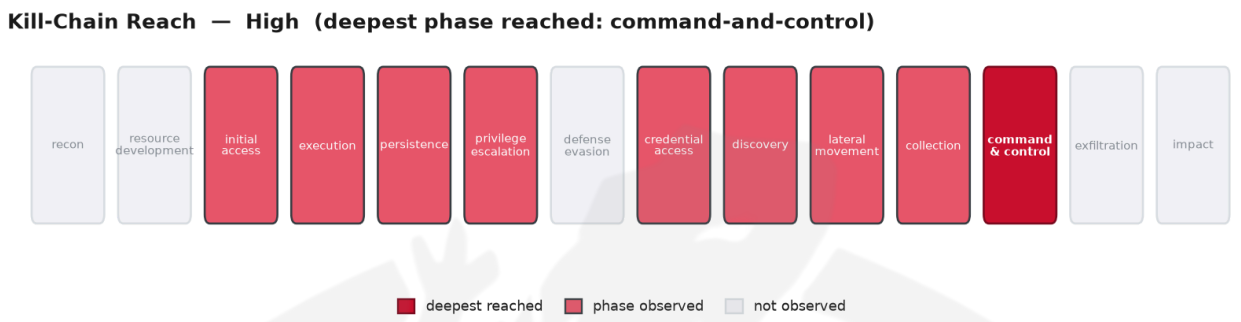
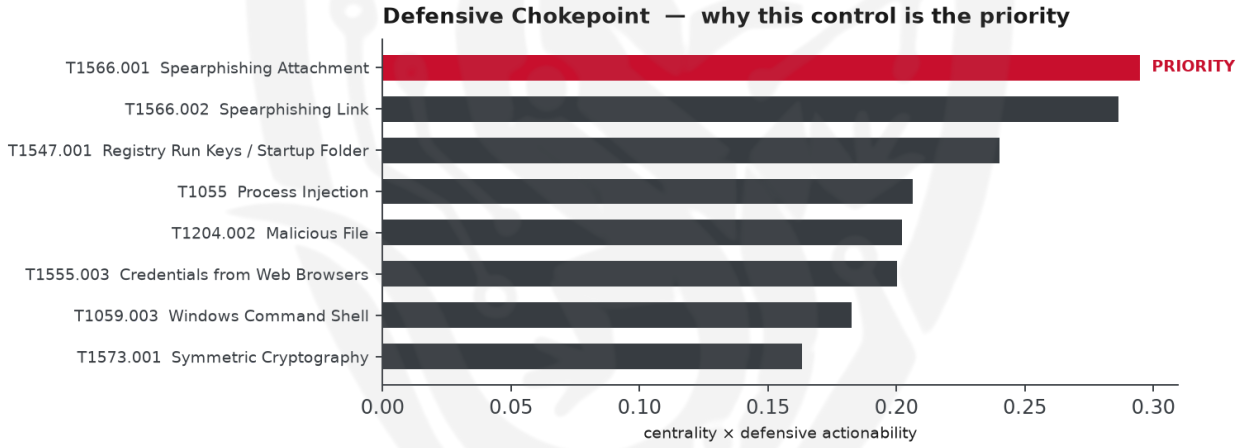
THREAT REPORT: CYLINDRICALCANINE

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 CylindricalCanine, a subgroup responsible for the April DigiCert incident. This threat actor has been observed targeting the finance sector, utilizing various malware families including Golden Gh0st Loader, Golden Gh0st RAT, and Zhong Stealer. The priority defensive action should be taken to mitigate the threat, focusing on email attachments and executable contents. Priority should be given to sandboxing and detonating email attachments to prevent potential breaches.

Threat Overview

CylindricalCanine, the observed threat actor, has been associated with multiple malware families, including Golden Gh0st Loader, Golden Gh0st RAT, gh0st RAT - S0032, Mydoor, Moudoor, and Zhong Stealer. The targeted sector is finance, although the targeted country and central CVE exploited are not specified. The threat actor's techniques include scheduled tasks, screen capture, keylogging, and stealing web session cookies, among others.

Attack Chain and Priority Control

The observed techniques used by CylindricalCanine form a complex attack chain, involving various methods to gain access and maintain control over the targeted systems. The priority technique identified is T1566.001 Spearphishing Attachment, which serves as a critical chokepoint in the attack chain. To counter this, the priority control is to "Sandbox and detonate email attachments; block executable/script archive contents at the gateway; strip mark-of-the-web bypass; user report-phish button."

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with CylindricalCanine's infrastructure. Additionally, no malware families have been corroborated by abuse.ch, and there are no indicators with an AbuseIPDB 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
- T1113 Screen Capture
- T1056.001 Keylogging
- T1539 Steal Web Session Cookie
- T1036.005 Match Legitimate Resource Name or Location
- T1087.002 Domain Account
- T1204.002 Malicious File
- T1573.001 Symmetric Cryptography
- T1566.002 Spearphishing Link
- T1566.001 Spearphishing Attachment
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1555.003 Credentials from Web Browsers
- T1070.001 Indicator Removal
- T1547.001 Registry Run Keys / Startup Folder
- T1059.003 Windows Command Shell
- T1027.002 Software Packing
- T1071.001 Web Protocols
- T1574.002 Hijack Execution Flow
- T1021.001 Remote Desktop Protocol
- T1090.001 Internal Proxy

Analytical Scores

- Priority technique (graph chokepoint): T1566.001 Spearphishing Attachment (centrality 0.2949).
- 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 0.528; 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
Higaisa	0.528
RedCurl	0.5237
APT39	0.5179
BRONZE BUTLER	0.5105
Silence	0.4898

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
URL	hxxp://uu[.]goldeyeuu[.]io:5188
URL	hxxp://api[.]keensie[.]com:5198
URL	hxxp://wk[.]goldeyeuu[.]io:5188
Hash	1abffe97aafe9916b366da57458a78338598cab9742c2d9e03e4ad0ba11f29bf
Hash	4eaebd93e23be3427d4c1349d64bef4b5fc455c93aebb9b5b752981e9266488e
Hash	dd44dabff536a1aa9b845dd891ad483162d4f28913344c93e5d59f648a186098
Hash	54def291b6bd573186734895b7ed03b6

Type	Indicator
Hash	639b0dd0fe4da3f4743de6347d7d58b7
Hash	efe7a351491008a2ccb6b5d586904aba
Hash	f04ccc9a18dc71ccc4d4b1f651d3d0d2af8ab402
Hash	f1888d0b44e5e1d5864ca5a9e93bf65c09411320
Hash	2031a71c399563adaf1572e10abb395387eb132208a001c5e140496d7a3e0b26
Hash	27b722c66f69e360c4da106daacf3b9eeaabd20634d7e5eff45a28bd70ebfd65
Hash	2b0071007c3f5fa8e949a8de53be03e97901dd505694ca939b575a49e4fdbdbb
Hash	3313f347e83aaf48ea31fb1d49fc37452f48f81d20a1b93009e2e78385ff4bba
Hash	81e276aaa3eb9b3f595663c316b3c6414cc3dde5e6cc3a82856b7276acabb7de
Hash	8a913610e905c3dd1f657811ea3b1933471b230f88e1c155616099a03ab0abc0
Hash	d1b1938963037aa332591a4c999523a05886d1f62d80e03f0adc22630b8671c4
Hash	f67de637fca127212dc60b9a02f74e66dbd602b3b9f6f6e4f2b75614c1f9e944

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:** T1566.001 Spearphishing Attachment (initial-access)
- **Observed here:** CylindricalCanine used T1566.002 Spearphishing Link here as an alternative initial-access technique.
- **Projected pivot:** T1566.002 Spearphishing Link (initial-access)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

CylindricalCanine could pivot to T1566.002 Spearphishing Link to maintain their campaign momentum by enticing victims to click on malicious links, which may bypass traditional attachment-based defenses. This shift would likely involve crafting convincing emails with embedded links that appear legitimate, in an attempt to trick users into divulging sensitive information or downloading malware. To counter this potential move, the defensive control of enabling attachment sandboxing and link rewriting, blocking macro-enabled Office docs from the internet zone, and deploying a user report-phish button should be implemented.

Detection and hardening for the pivot (T1566.002 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