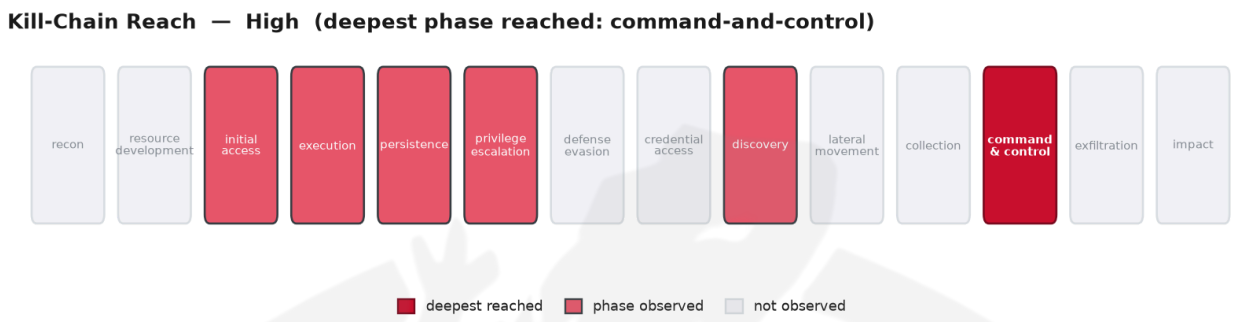
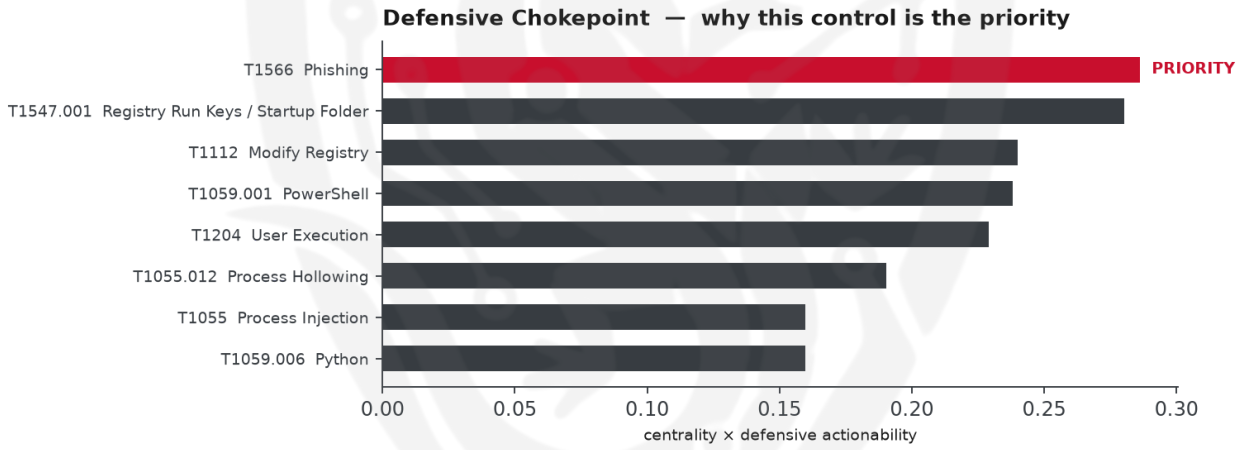
THREAT REPORT: PAYOUTS KING RANSOMWARE

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 Payouts King, a threat actor deploying Edgecution malware. The targeted country and sectors are not specified due to insufficient data. Priority should be given to defending against the initial access broker's tactics, particularly phishing attacks. Enable attachment sandboxing and link rewriting to mitigate the threat.

Threat Overview

Payouts King, the observed threat actor, is utilizing the Edgecution malware family to compromise systems. While the central CVE is not specified due to insufficient data, the actor employs various techniques, including system information discovery, software extensions, and process injection. The victimology of this campaign is not well-defined due to a lack of specific information on targeted countries and sectors.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including scheduled tasks, system information discovery, and process injection, ultimately leading to the deployment of the Edgecution malware. The priority technique identified is T1566 Phishing, which serves as a critical chokepoint in the attack chain. To counter this, the priority control is to "Enable attachment sandboxing and link rewriting; block macro-enabled Office docs from the internet zone; deploy a user report-phish button."

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs observed in relation to this threat. Additionally, no malware families have been corroborated by abuse.ch, and no indicators have been flagged 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)

- T1053.005 Scheduled Task
- T1082 System Information Discovery
- T1176 Software Extensions
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1055 Process Injection
- T1112 Modify Registry
- T1083 File and Directory Discovery
- T1204 User Execution
- T1057 Process Discovery
- T1059.001 PowerShell
- T1547.001 Registry Run Keys / Startup Folder
- T1566 Phishing
- T1055.012 Process Hollowing
- T1027 Obfuscated Files or Information
- T1573 Encrypted Channel
- T1059.006 Python
- T1132 Data Encoding
- T1059.003 Windows Command Shell
- T1071.001 Web Protocols
- T1105 Ingress Tool Transfer

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.2863).
- 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 0.5421; 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
Gorgon Group	0.5421
APT37	0.5376
APT18	0.5185
Higaisa	0.4998
Tropic Trooper	0.4811

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
Hash	3d1158884fb339b3328bd330fcc27598e1f1c94bcac39e75d1a272afa4deee1a
Hash	a08d8e63b0cd3638fb40b8e6da546e26da69439597565827f9cec87915f78568

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 Phishing (initial-access)

- **Observed here:** T1566 Phishing was the only initial-access technique observed in this campaign, so the pivot is projected from cross-actor behaviour.
- **Projected pivot:** T1189 Drive-by Compromise (initial-access)
- **Basis:** 27 of 170 documented groups that use Phishing also use Drive-by Compromise (conditional 0.28, lift 1.5, i.e. ~1.5x base rate). Strongest same-tactic neighbour.

The Payouts King actor could pivot to Drive-by Compromise (T1189) as a means to maintain their objective of initial access, potentially leveraging compromised websites or malicious advertisements to infect user systems. This technique may be used in conjunction with social engineering tactics to increase the likelihood of a successful compromise. To counter this potential pivot, the defensive control of enforcing browser isolation/patching; blocking known-malicious domains at the proxy; and disabling risky plugins should be implemented.

Also plausible (same tactic): T1195 Supply Chain Compromise (n=9, lift 1.4), T1199 Trusted Relationship (n=9, lift 1.3)

- **Defensive countermeasure:** Enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.