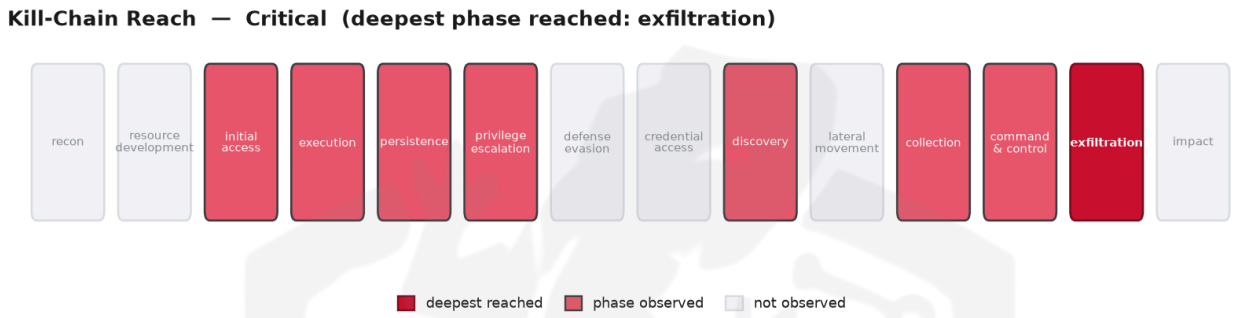
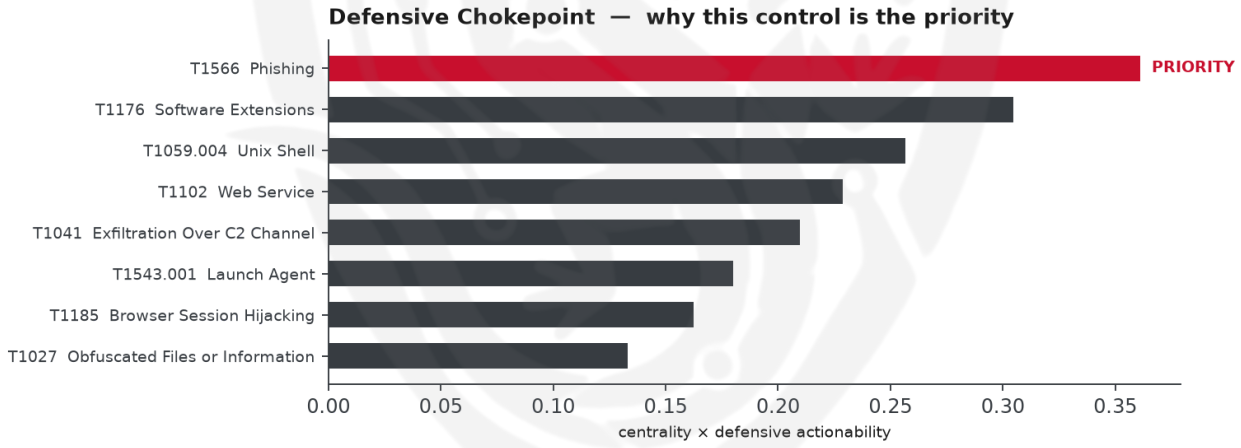
THREAT REPORT: OPERATION FLUTTERBRIDGE: THE FLUTTERSHELL MACOS BACKDOOR

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, associated with the FlutterShell malware family, has been identified as a significant threat, with a critical operational risk band due to its ability to reach exfiltration. The threat actor, whose identity is currently insufficient to determine, has been leveraging various techniques to compromise systems. Priority should be given to defensive actions that mitigate the threat, particularly focusing on the priority technique of phishing. The targeted country and sectors are currently unknown, making it essential to implement robust security measures to protect against this threat.

Threat Overview

The threat actor, responsible for Operation FlutterBridge, is utilizing the FlutterShell malware family to compromise macOS systems. Although the central CVE is currently unknown, the malware family is

exploiting various vulnerabilities to gain access to systems. The victimology of this threat is also unknown, but the techniques used by the threat actor suggest a high level of sophistication.

Attack Chain and Priority Control

The attack chain involves a series of techniques, including malicious file execution, code signing, system information discovery, and browser session hijacking, ultimately leading to exfiltration over a command and control channel. The priority technique in this chain is T1566 Phishing, which serves as a critical chokepoint. To mitigate this threat, 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 currently no information available on the hosting providers or ASNs observed to be associated with this threat. Additionally, no malware families have been corroborated by abuse.ch, and no indicators have been flagged with a confidence level of 80% or higher 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)

- T1204.002 Malicious File
- T1553.002 Code Signing
- T1082 System Information Discovery
- T1176 Software Extensions
- T1185 Browser Session Hijacking
- T1102 Web Service
- T1041 Exfiltration Over C2 Channel
- T1566 Phishing
- T1059.004 Unix Shell
- T1027 Obfuscated Files or Information
- T1543.001 Launch Agent
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.3611).
- Operational risk: Critical (score 0.968, reaches exfiltration).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.3961; 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
Windshift	0.3961
Dark Caracal	0.3895
APT19	0.3859
Inception	0.3744
Gallmaker	0.3656

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	atsheisdomestic[.]org
Domain	etoftheappyrince[.]org
Domain	healightejustb[.]org
Domain	sinterfumesco[.]com
Domain	event[.]process[.]name
Domain	event[.]process[.]parent[.]name
URL	hxxps://atsheisdomestic[.]org/update-thanks[.]html
URL	hxxps://atsheisdomestic[.]org/api/podcasts
URL	hxxps://atsheisdomestic[.]org/api/subscribe
URL	hxxps://atsheisdomestic[.]org/api/update-delay

Type	Indicator
URL	hxxps://etoftheappyrince[.]org
URL	hxxps://etoftheappyrince[.]org/[.][.][.]
URL	hxxps://etoftheappyrince[.]org/api/pdfs
URL	hxxps://etoftheappyrince[.]org/api/update-delay
URL	hxxps://etoftheappyrince[.]org/summarize-text
URL	hxxps://etoftheappyrince[.]org/update-thanks[.]html
URL	hxxps://healightejustb[.]org/api/central-config
URL	hxxps://healightejustb[.]org/checkForNewVersion
URL	hxxps://healightejustb[.]org/summarize-text
URL	hxxps://healightejustb[.]org/welcome_page[.]html
URL	hxxps://healightejustb[.]org/welcome_page[.]js
Hash	363923500ce942bf1a953e8a4e943fbf1fb1b5ed6e5d247964c345b3ad5bfc34
Hash	638b0a77a6d686849a78b500adf5e565
Hash	c40126fea6ed24652a3e4e19205075cb02cca3e2
Hash	605169623267c4eb73693b22b811dc7a
Hash	b4aa7255af4b016586090a5b451300fa
Hash	ffd773f157df70291f0910a45a1d8d9a
Hash	134517796178a150a1585672be134169d6877082b598d840baa3f37b0222be26
Hash	2c5bc9e95e1e9b73e3ba8870a008802899866a2c0e2e10112aefddf7a96af04e
Hash	32da1437a2734224406c7e5e8d756f0c0cd58c0c959478571cbfc0cd564d018a
Hash	6c3f61d46d4de26b9cb16808bf17c33ae69f651a4b879e7b5612ff7f548e2a82
Hash	bf90fb31e6024d7e6616f5acd0e8aa28738a9095a508c1a986e1e974cb9e79a0
Hash	cc4f048e66c5ab3c0f1d767bb8fc464d082641f4888ea3cd14ea3775077c4bf2
Hash	f544bfab72d380cc20692d8ec9d31ea666785fe225dccd55beab29a3c0fdfad2
Hash	fc091ddb4d845280aeb7745cfdb6b7cb0013abc35db9e634f055b8e8fb0b5b1e

Type	Indicator
Hash	a247a63644c3475f436d076f55523ea39afd8c41
Hash	bb1e6e2650d3d77d732c5eb5176011f914dd87df

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 actor could pivot to T1189 Drive-by Compromise to keep their objective after the block, as this technique may allow them to compromise a system by exploiting vulnerabilities in browsers or plugins, potentially bypassing the initial phishing attempt. This could be achieved by compromising a website the target frequently visits, which would likely lead to a drive-by download of malicious code. The defensive control to mitigate this would be to enforce browser isolation/patching; block known-malicious domains at the proxy; disable risky plugins.

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.