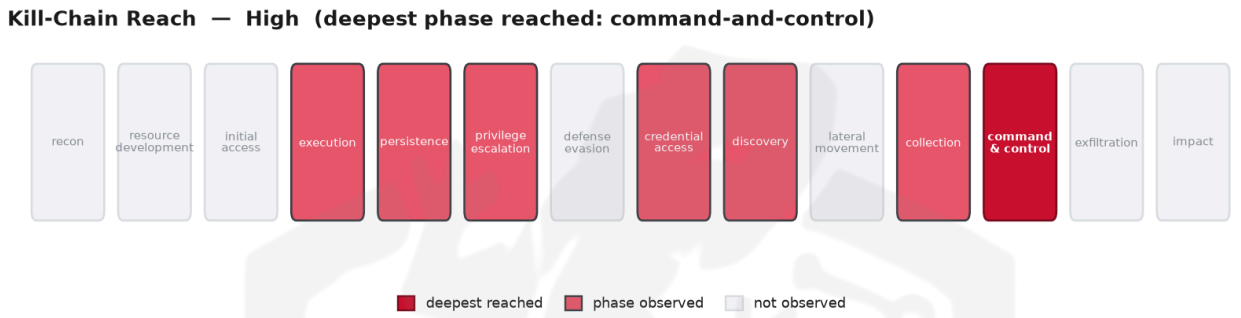
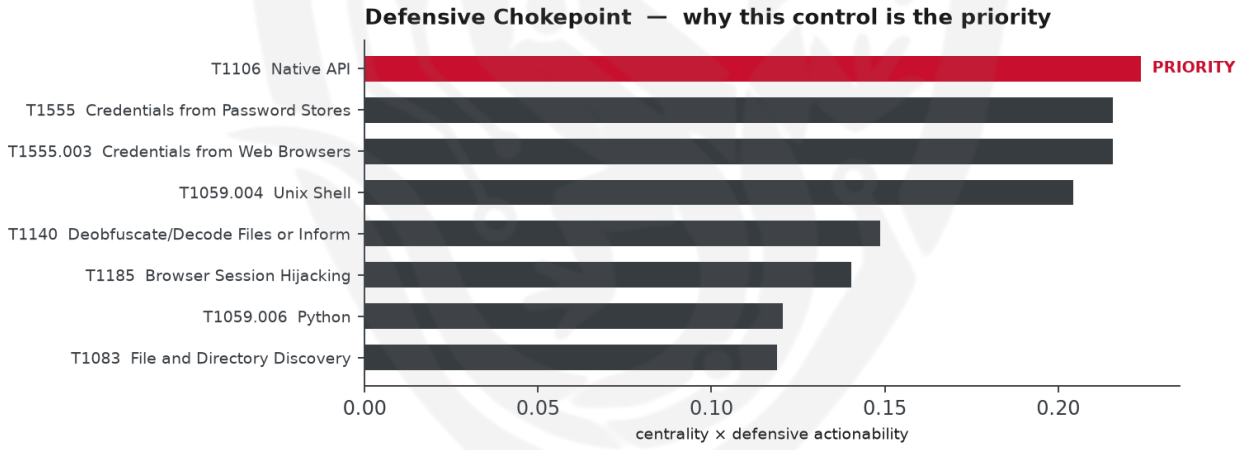
THREAT REPORT: DPRK-ALIGNED MACOS.GASLIGHT CAMPAIGN

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 source attributes this activity to a DPRK-aligned threat actor, who has been observed utilizing the macOS.Gaslight, BONZAI, and AIRPIPE malware families. The targeted country and sectors are not specified due to insufficient data. Priority should be given to enabling EDR API-telemetry and alerting on unusual direct Native API use from non-system processes to defend against this threat. The threat actor's use of various techniques, including standard encoding and symmetric cryptography, poses a significant risk to affected systems.

Threat Overview

The DPRK-aligned threat actor is utilizing the macOS.Gaslight, BONZAI, and AIRPIPE malware families to carry out their operations. Although the central CVE is not specified due to insufficient data, the threat

actor has been observed exploiting various techniques, including stealing web session cookies, system information discovery, and credentials from password stores. The victimology of this campaign is not well-defined due to the lack of information on targeted countries and sectors.

Attack Chain and Priority Control

The observed techniques used by the threat actor form a complex attack chain, involving standard encoding, symmetric cryptography, and system checks. The priority technique in this chain is T1106 Native API, which serves as a graph chokepoint. To defend against this threat, the priority control is to Enable EDR API-telemetry; alert on unusual direct Native API use from non-system processes.

Infrastructure and Corroboration

There is no observed hosting provider or ASN associated with this campaign, and no malware families have been corroborated by abuse.ch. Additionally, 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)

- T1132.001 Standard Encoding
- T1539 Steal Web Session Cookie
- T1036.005 Match Legitimate Resource Name or Location
- T1573.001 Symmetric Cryptography
- T1497.001 System Checks
- T1082 System Information Discovery
- T1106 Native API
- T1140 Deobfuscate/Decode Files or Information
- T1555 Credentials from Password Stores
- T1185 Browser Session Hijacking
- T1555.003 Credentials from Web Browsers
- T1083 File and Directory Discovery
- T1057 Process Discovery
- T1059.004 Unix Shell
- T1562.001 Impair Defenses: Disable or Modify Tools
- T1102.002 Bidirectional Communication
- T1059.006 Python
- T1543.001 Launch Agent
- T1071.001 Web Protocols

Analytical Scores

- Priority technique (graph chokepoint): T1106 Native API (centrality 0.2797).
- 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 0.4049; 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
Stealth Falcon	0.4049
APT37	0.3721
APT42	0.3719
Inception	0.37
Darkhotel	0.37

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	5555494492fc075f441637fb9d894913dde3a2ea
Hash	6328567511d88fdc2ae0939c5ef17b7a63d2a833881900de018a4f12f4982525
Hash	77b4fd46994992f0e57302cfe76ed23c0d90101381d2b89fc2ddf5c4536e77ca
Hash	b3c56d689414343589f38394d19ba2fe9a518133281200faa0556ba4e4136394
Hash	baabf249c77bc54c54ab0e66e15af798bd28aa5b4683554456a8b73ab8741239

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:** T1106 Native API (execution)
- **Observed here:** DPRK-aligned used T1059.004 Unix Shell here as an alternative execution technique.
- **Projected pivot:** T1059.004 Unix Shell (execution)
- **Basis:** observed in this campaign (an alternative the actor already demonstrated).

The adversary could pivot to using T1059.004 Unix Shell to maintain access and execute commands, potentially leveraging Unix-like shells available on the compromised system to bypass the blocked Native API calls. This shift may allow them to continue their objectives, such as data exfiltration or lateral movement, by utilizing the Unix Shell for command execution. To counter this potential move, the mandated defensive control of Constrain PowerShell for unprivileged users (Constrained Language Mode + AppLocker); enable script-block logging; block wscript/cscript where unneeded should be implemented.

Detection and hardening for the pivot (T1059.004 Command and Scripting Interpreter)

- **Telemetry:** Sysmon / EDR process + command line; PowerShell Script Block Logging (4104); AMSI
- **Detect:**
  - Security 4688 / Sysmon 1 with full command lines; encoded or obfuscated PowerShell
  - PowerShell 4104 script-block content; suspicious cmdlets and download cradles
  - Office or browser processes spawning powershell/cmd/wscript
- **Harden:**
  - Enable Script Block Logging + AMSI; Constrained Language Mode
  - Application control (WDAC/AppLocker); remove/limit unused interpreters
- **MITRE:** M1049 Antivirus/Antimalware, M1038 Execution Prevention, M1042 Disable or Remove Feature, M1045 Code Signing · DS0009 Process, DS0012 Script, DS0017 Command