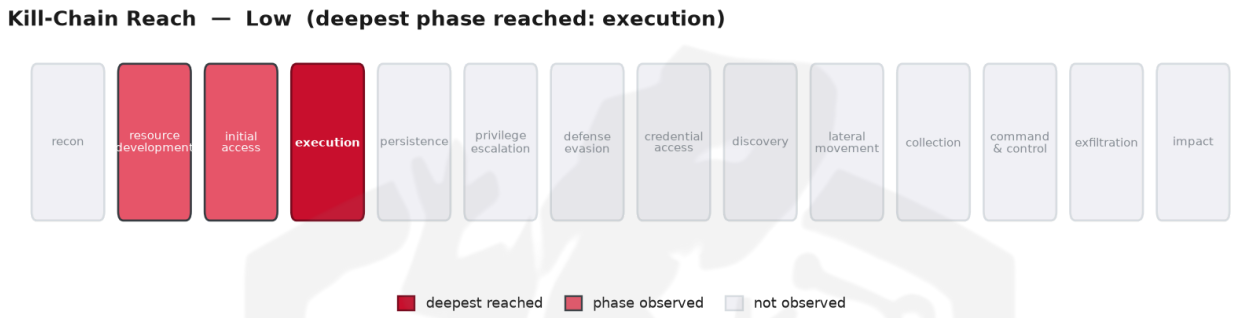
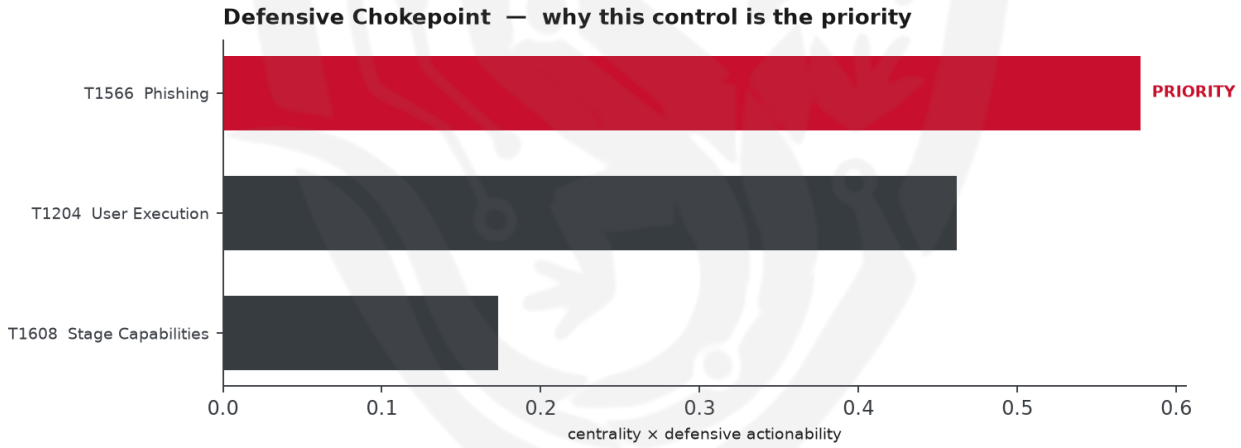
# THREAT REPORT: ALBIRIOX ANDROID MALWARE CAMPAIGN TARGETS ITALIAN FINANCE SECTOR

## 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 delivering the Albiriox malware to targets in Italy, primarily in the finance sector. The campaign relies on social engineering tactics, including phishing, to trick users into executing the malware. Priority should be given to implementing defensive measures to prevent the execution of malicious code. The threat actor's use of phishing as a primary technique highlights the need for robust email security controls.

## Threat Overview

The threat actor, whose identity is currently unknown, is utilizing the Albiriox malware family to target individuals in the Italian finance sector. Although a central CVE is not specified, the malware is being delivered through phishing emails, which are a key component of the campaign. The actor's tactics,

techniques, and procedures (TTPs) include user execution and staging capabilities, in addition to phishing.

## Attack Chain and Priority Control

The attack chain begins with phishing emails, which are used to trick users into executing the malware. The malware then uses staging capabilities to establish a foothold on the compromised device. The priority technique in this campaign is T1566 Phishing, which serves as the initial entry point for the malware. 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 no available information on the hosting providers or ASNs used by the threat actor. 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.

---

## Technical Appendix

*Ground-truth telemetry from the source pulse; analytical scores are secondary and clearly labelled.*

### Observed Techniques (ATT&CK, expert-tagged by source)

- T1608 Stage Capabilities
- T1204 User Execution
- T1566 Phishing

### Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.7071).
- Operational risk: Low (score 0.191, reaches execution).

### Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5774; 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 |
|---|---|
| APT30 | 0.5774 |

| Historical Profile | Behavioural Overlap |
|---|---|
| Mustard Tempest | 0.4082 |
| TA459 | 0.4082 |
| AppleJeus | 0.4082 |
| APT12 | 0.3849 |

### 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 | unicredit-tme[.]shop |
| URL | hxxp://unicredit-tme[.]shop/ |
| Hash | 6aa665d2f33f03a549c14edec772cf2c |
| Hash | 146c62f408b6d7db4c832a6b5f7bdacb1cff2c69121b9b2f7e80646c37910abd |
| Hash | 1e99972b1d84b131eb55a6b49f64871c5c0c6a1bb2a099a84313001b69dc53e8 |
| Hash | 206fdbe992b44ebd6720c49c79a5da3bdcb48d0d799a0ff3458323caac3cc490 |
| Hash | 4b9a95ebf5e471d11443fa2f19b75595fc1fcf6be234024cc1d4a2255068c19b |
| Hash | e0fc365c042e708c8d04b5431238958586194cc4a8cbe069411a26dcfcc4e9b6 |
| Hash | efc81267da3ad48cc779e9aed8f9232504ed7c85abf3958a87ba2ae68056ae23 |
| Hash | fb43c4191c40f159167a98a4ac20bf23ae66a8ec27a919f703e953933e22a266 |

---

## 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 initial-access control point; blocking a means-of-entry rarely stops a determined actor, so the pivot projects forward to the execution stage they must still reach.
- **Projected pivot:** T1203 Exploitation for Client Execution (execution)
- **Basis:** of the 38+ groups that use Phishing, this pairing runs 1.6x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1203 Exploitation for Client Execution to maintain their objective by leveraging vulnerabilities in client applications, such as browsers or Office software, which may be exposed through user interaction or unpatched software, thereby potentially allowing the execution of malicious code on the client-side. This technique may be particularly appealing as a follow-up to phishing attempts, as it can exploit the trust established through social engineering. To counter this potential pivot, the mandated defensive control of patching client applications, enabling exploit mitigations such as ASLR, DEP, and CFG, and implementing application isolation would likely be effective.

**Also plausible (same tactic):** T1053 Scheduled Task/Job (n=43, lift 1.3), T1106 Native API (n=18, lift 1.6)

**Detection and hardening for the pivot (T1203 Exploitation for Client Execution)**

- **Telemetry:** EDR process + memory telemetry; Office/browser/reader child-process telemetry; Windows Error Reporting (application crashes)
- **Detect:**
  - Office, browser or PDF-reader processes (winword/excel/outlook/acrobat/chrome) spawning shells or LOLBINs
  - Sysmon 1 anomalous children of document/browser apps; unbacked-memory execution right after a client crash
  - WER application-crash events for client apps immediately followed by a new child process
- **Harden:**
  - Patch client software fast (browsers, Office, PDF, Java); retire end-of-life plugins
  - ASR rules blocking Office child processes; exploit protection (DEP/ASLR/CFG) and browser sandboxing
- **MITRE:** M1048 Application Isolation and Sandboxing, M1050 Exploit Protection, M1051 Update Software, M1040 Behavior Prevention on Endpoint · DS0009 Process, DS0011 Module, DS0015 Application Log