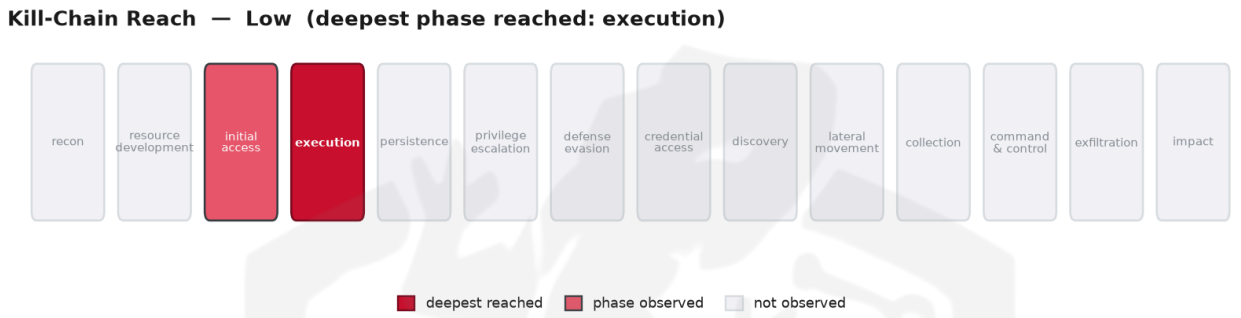
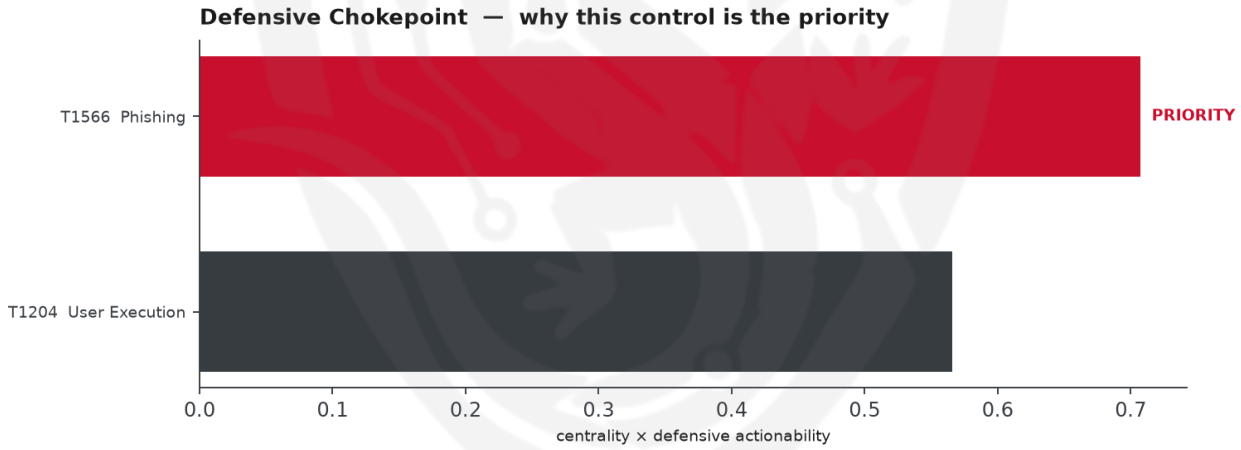
THREAT REPORT: JALISCO TOOLKIT PHISHING SURGE

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 involves the deployment of various malware families, including Jalisco, OmegaLord, and EvilTokens, targeting unknown sectors and countries. The reporting indicates techniques inferred from the report, such as user execution and phishing, are being utilized. Priority should be given to hardening defenses against social-engineering delivery methods. The threat actor's identity and specific targets remain unclear, but the use of phishing techniques suggests a significant risk of initial access.

Threat Overview

The threat actor, whose identity is not specified, is associated with the Jalisco toolkit and other malware families like OmegaLord, EvilTokens, Kali365, Tycoon2fa, Venom, and Darcula. The central vulnerability

exploited is not identified, but the techniques inferred from the report include user execution and phishing. The victimology of this campaign is not well-defined due to insufficient data.

Attack Chain and Priority Control

The observed techniques, inferred from the report, suggest a chain of events that starts with user execution and leads to phishing attempts. The priority technique identified is T1566 Phishing, which serves as a chokepoint in the attack chain. To mitigate this threat, the lead control is to: Harden against social-engineering delivery across email, links and voice/callback lures: attachment sandboxing and link rewriting, block macro-enabled Office docs from the internet zone, train users to verify unexpected requests out-of-band, deploy a report-phish button, and enforce phishing-resistant MFA.

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs used by the threat actor, as the observed indicators do not have a high confidence level according to AbuseIPDB, with the highest confidence seen being 0%. Additionally, no malware families have been corroborated by abuse.ch in this context.

Technical Appendix

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

Observed Techniques (ATT&CK, machine-extracted from report text — reduced confidence)

The source pulse carried no expert ATT&CK tags, so these techniques were inferred from its narrative by a self-consensus LLM extractor and validated against the ATT&CK catalogue. Treat this technique set, and the chokepoint, kill-chain and risk scores derived from it, as lower-confidence than an expert-tagged brief. - T1204 User Execution - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1566 Phishing (centrality 0.7071).
- Operational risk: Low (score 0.17, reaches execution).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.7071; 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	0.7071
TA459	0.5
AppleJeus	0.5
APT12	0.4714
Mofang	0.4714

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	authplanned[.]online
Domain	levaquin2us[.]top
Domain	sessionopen0[.]site
Domain	grantfundingapplications[.]com
Domain	secure-folder-9f8a2983fbf5479e8d8c267e0df4e73d[.]3vvcompany[.]com
URL	hxxps://file[.]kiwi/7ab7c290#z_n5Qh8kwioCUs8jQ6WWhw
Hash	9f8a2983fbf5479e8d8c267e0df4e73d

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, as this technique may allow them to execute malicious code on the client-side by exploiting vulnerabilities in commonly used software, potentially bypassing the phishing block by directly targeting the client application. This technique in particular could be appealing as it would likely enable the actor to leverage existing vulnerabilities in software that the target may have, increasing the chances of successful execution. The defensive countermeasure to mitigate this potential pivot would be to patch client applications (Office, browsers, PDF); enable exploit mitigations (ASLR/DEP/CFG); application isolation.

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