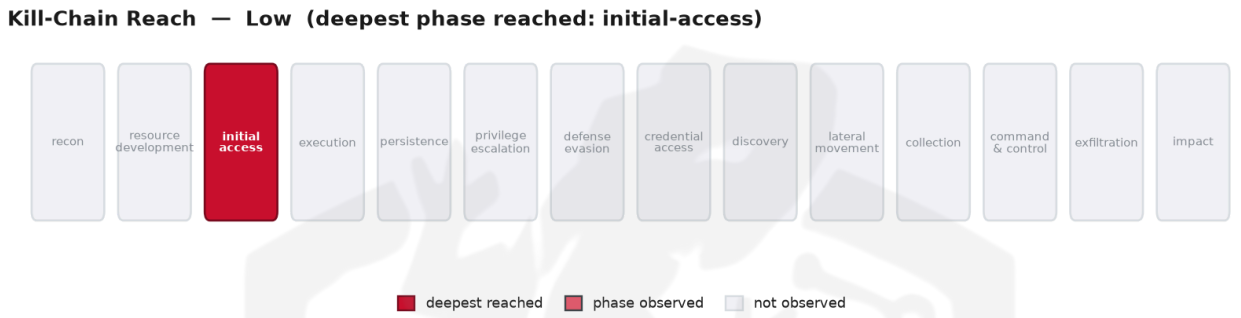
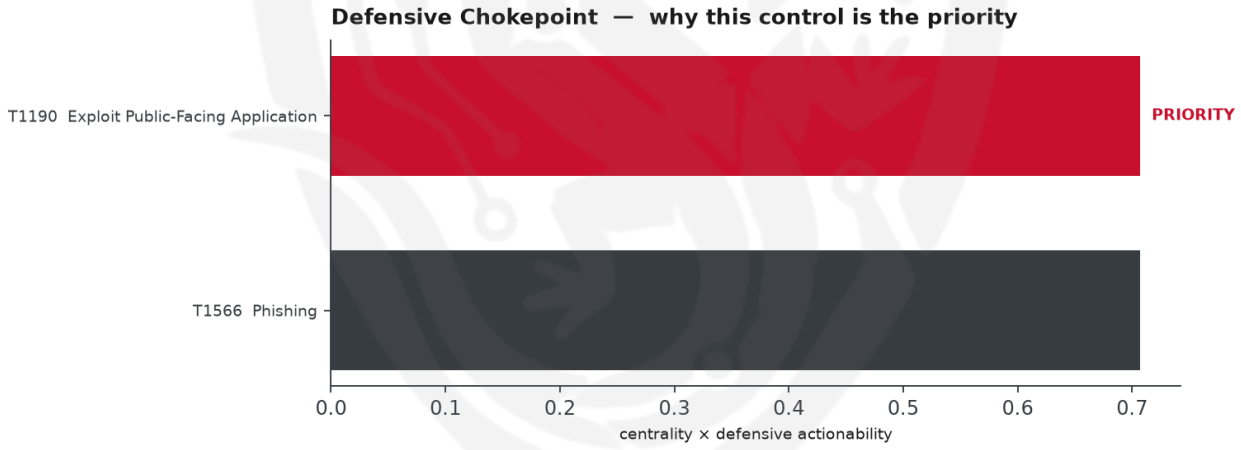
THREAT REPORT: CELINE DION CONCERT TICKET SCAM

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 is targeting individuals in France, particularly in the Media, Hospitality, and Retail sectors, with a potential scam related to Celine Dion concert tickets. The techniques inferred from the report suggest a focus on exploiting public-facing applications and phishing. Priority should be given to patching affected public-facing vulnerabilities and implementing additional security measures. The threat actor remains unattributed.

Threat Overview

The threat actor, whose identity is not specified, is believed to be leveraging techniques such as exploiting public-facing applications and phishing to target victims. The specific malware families and central CVE

exploited are not identified due to insufficient data. The primary targets appear to be in France, across multiple sectors.

Attack Chain and Priority Control

The attack chain involves techniques inferred from the report, including exploiting public-facing applications and phishing. The priority technique is T1190 Exploit Public-Facing Application, which is considered the chokepoint. To mitigate this, the priority control is to "Patch the affected public-facing CVE immediately; apply a WAF virtual patch; restrict management interfaces to VPN-only."

Infrastructure and Corroboration

There is no specific information available on the hosting providers or ASNs used by the threat actor, as indicated by the lack of data in the infrastructure and corroboration section. 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, 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. - T1190 Exploit Public-Facing Application - T1566 Phishing

Analytical Scores

- Priority technique (graph chokepoint): T1190 Exploit Public-Facing Application (centrality 0.7071).
- Operational risk: Low (score 0.138, reaches initial-access).

Behavioral Signature Cluster

- Method: technique-overlap cosine vs 170 MITRE ATT&CK Groups (top overlap 0.5; 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
AppleJeus	0.5
GOLD SOUTHFIELD	0.4082
APT30	0.3536
BlackTech	0.3162
Axiom	0.3015

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	ticketmaster-celinedion[.]fr
Domain	axs-billetterie[.]com
Domain	billeteriecelinedion[.]com
Domain	celine-dion-arena[.]com
Domain	celine-dion-paris[.]com
Domain	celinedion-2026[.]com
Domain	celinedion-billetterie[.]com
Domain	celinedion-fr[.]com
Domain	celinedion-france[.]com

Type	Indicator
Domain	celinedion-paris-billetterie[.]com
Domain	celinedion-paris[.]com
Domain	celinedion-paris[.]fr
Domain	celinedion-parisladefense-arena[.]com
Domain	celinedion[.]co
Domain	celinedion2026tour[.]com
Domain	celinedionofficial[.]com
Domain	celinedionparis[.]com
Domain	celinedionparistickets[.]com
Domain	celinedionparsifr[.]com
Domain	celinedionviptickets[.]com
Domain	fr-celinedionparis[.]com
Domain	ticketmaster-celinedion[.]com
Domain	tickets-celinedion[.]com
Domain	252faccount[.]celine-dion-arena[.]com
Domain	252faccount[.]celinedion-paris-billetterie[.]com

Type	Indicator
Domain	252faccount[.]celinedion-parisladefense-arena[.]com
Domain	252faccount[.]ticketmaster-celinedion[.]fr
Domain	account[.]celine-dion-arena[.]com
Domain	account[.]celinedion-paris-billetterie[.]com
Domain	account[.]celinedion-parisladefense-arena[.]com
Domain	account[.]ticketmaster-celinedion[.]fr
Domain	pay[.]celinedion-paris[.]fr
URL	hxxps://www[.]celine-dion-paris[.]com/
URL	hxxps://celinedion-2026[.]com/
URL	hxxps://account[.]celine-dion-arena[.]com/authentication/login?client_id=4983cefd-9810-444e-9eb0-64b4933878eb&locale=en-US&redirect_uri=%2Fauthentication%2Foauth%2Fauthorize%3Fclient_id%3D4983cefd-9810-444e-9eb0-64b4933878eb%26locale%3Den-US%26nonce%3Dc4f2c148-2acb-4684-b19e-097d64ab8dd6%26redirect_uri%3Dhttps%253A%252F%252Faccount[.]celine-dion-arena[.]com%252Fcallback%26response_type%3Dcode%26scope%3Dopenid%2Bemail%2Bcustomer-account-api%253Afull%26state%3DhWNArFqrbMvKRksSv7JganvH
URL	hxxps://account[.]ticketmaster-celinedion[.]fr/authentication/login?client_id=7e7dbd4b-c5a9-4d4e-af60-64fd673ea525&locale=en-US&redirect_uri=%2Fauthentication%2Foauth%2Fauthorize%3Fclient_id%3D7e7dbd4b-c5a9-4d4e-af60-64fd673ea525%26locale%3Den-US%26nonce%3Dcdc91d10-2a95-4f80-92cd-ba9204a5edd7%26redirect_uri%3Dhttps%253A%252F%252Faccount[.]ticketmaster-celinedion[.]fr%252Fcallback%26response_type%3Dcode%26scope%3Dopenid%2Bemail%2Bcustomer-account-api%253Afull%26state%3DhWNAmhJgfrrdQ1bVJJXLbgCh
URL	hxxps://billeteriecelinedion[.]com/en/
URL	hxxps://celine-dion-arena[.]com/
URL	hxxps://celinedion-fr[.]com/
URL	hxxps://celinedion-france[.]com/

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:** T1190 Exploit Public-Facing Application (initial-access)
- **Observed here:** T1190 Exploit Public-Facing Application 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:** T1047 Windows Management Instrumentation (execution)
- **Basis:** of the 22+ groups that use Exploit Public-Facing Application, this pairing runs 2.0x above base rate, a disproportionately-coupled move rather than the obvious one.

The actor could pivot to T1047 Windows Management Instrumentation to maintain their objective by leveraging WMI's native capabilities to execute commands and access sensitive information, potentially exploiting the lack of monitoring and control over WMI activity. This technique may be particularly appealing as it allows the actor to interact with the system in a way that blends in with legitimate administrative activity, making it harder to detect. To counter this potential pivot, the mandated defensive control of monitoring wmiprvse.exe child-process creation, restricting remote WMI (DCOM) at the host firewall, and enabling WMI-Activity operational logging should be implemented.

Also plausible (same tactic): T1053 Scheduled Task/Job (n=23, lift 1.5), T1059 Command and Scripting Interpreter (n=38, lift 1.2)

Detection and hardening for the pivot (T1047 Windows Management Instrumentation)

- **Telemetry:** Sysmon (WMI events); Microsoft-Windows-WMI-Activity/Operational
- **Detect:**
  - Sysmon 19/20/21 (WMI event filter/consumer/binding) for persistence
  - wmic.exe / WmiPrvSE.exe spawning shells; remote WMI process creation
  - WMI-Activity/Operational operations from unusual users/hosts
- **Harden:**
  - Restrict WMI remote access; monitor permanent WMI subscriptions
  - Least-privilege; segment management protocols
- **MITRE:** M1040 Behavior Prevention, M1038 Execution Prevention, M1026 Privileged Account Management · DS0009 Process, DS0005 WMI, DS0017 Command