elytra security

Integrity. Trust. Clarity.

An ISO/IEC 27001:2022 Certified Company

ETR^3 2025

Elytra Threat, Risk & Resilience Report

Published by Elytra Security Private Limited | CC BY-SA 4.0
elytrasecurity.com | info@elytrasecurity.com

2025

Why This Document Exists

This document is a year-end threat reality record.

It is not a new flagship report.

It does not restate analysis already published in **ETR3 — Elytra Threat, Risk and Resilience Report (October 2025)**.

It does not introduce predictions, playbooks, or recommendations.

Its purpose is narrower and deliberate.

This record exists to capture what the final weeks of 2025 conclusively validated after ETR3 was released. Between November and December, multiple disclosures and confirmations crossed a threshold. They did not introduce new threat classes or novel techniques. Instead, they confirmed patterns already described earlier in the year, with enough repetition and scale that closing the year quietly would have been inaccurate.

The scope of this record is intentionally limited:

- *Timeframe*: Post-ETR3 (November–December 2025)
- *Focus*: confirmation, not discovery
- *Tone*: clinical, evidence-driven, non-alarmist

This document should be read alongside ETR3, not instead of it. ETR3 explains the landscape. This record closes the year by documenting what reality confirmed.

This document records what the final weeks of 2025 conclusively validated after ETR3 was released.

The Confirmation Set

The final weeks of 2025 did not introduce new threat categories. They confirmed what had already been forming in plain sight.

Four signals, observed independently and repeatedly, crossed from inference into record.

Cl0p: continuity, not surprise

Late disclosures confirmed that the campaign did not peak and fade. It persisted. Disclosure timing, not exploit novelty, determined when impact became visible.

Salesforce–Drift OAuth abuse

Additional tenant disclosures in November and December confirmed that OAuth-connected applications had become a quiet, repeatable breach vector. Authorization, once granted, proved difficult to observe and harder to revoke.

Developer trust abuse (WebRAT-class activity)

Continued evidence showed developer workflows and repositories being used for access, persistence, and credential capture. Tooling ecosystems behaved as attack surfaces, not neutral infrastructure.

AI-assisted reconnaissance

Credible reports confirmed the use of AI to accelerate reconnaissance and target selection. The shift was not new attack logic, but faster attacker decision cycles.

None of these signals were novel. Together, they were decisive.
These were not surprises. They were confirmations.

What 2025 Definitively Confirmed

By the end of 2025, several assumptions could no longer be defended. Not because they were theoretically wrong, but because reality repeated itself often enough to remove ambiguity.

Identity misuse dominates initial access

Most material incidents did not begin with exploitation. They began with valid credentials, tokens, or delegated access already in place.

Trust boundaries fail before technical controls

Once trust is granted to an application, integration, or workflow, traditional perimeter and endpoint controls become secondary.

Exploits matter less when authorization already exists

Patch status and CVE severity were frequently irrelevant where access had already been legitimately delegated.

Reconnaissance speed determines outcomes

Attackers who map environments faster than defenders can observe them do not need novel techniques to succeed.

Detection lag is the primary liability

In multiple cases, access persisted quietly not because alerts failed to fire, but because signals were never correlated.

The threat model did not suddenly change in 2025.
What changed was the weight of evidence.

The model changed. The signals caught up.

Salesforce–Drift OAuth: The Clearest Signal

Among all late-year confirmations, the Salesforce–Drift OAuth disclosures were the clearest signal of how the threat model has shifted.

The incidents announced in November and December did not rely on new vulnerabilities. They did not require perimeter bypass or lateral movement. Access already existed, granted through legitimate OAuth-connected applications operating as designed.

> This was not a failure of patching.
> It was not a failure of endpoint security.
> It was not a failure of perimeter defenses.
> It was a failure of assumed trust.

Once authorization was delegated, visibility diminished. Token use blended into normal application behavior. Detection lag increased not because tools were absent, but because delegated access was treated as benign by default.

What made the late disclosures decisive was not scale alone, but repeatability.

The same access model failed in the same way, across different organizations, without triggering early warning.

Authorization proved more dangerous than exploitation.

The Breach Ledger

The following disclosures were confirmed or expanded between November and December 2025. They are listed to document scale, not to analyze causes.
Each entry reflects a confirmed exposure or breach, reported publicly or through regulatory disclosure, during the final weeks of the year.

Entity	Sector	Primary Vector	Impact Class
Multiple enterprise SaaS customers	Technology	OAuth application abuse	Persistent access
Financial services organizations	Financial Services	Credential misuse	Data exposure
Retail and consumer platforms	Retail	Third-party integration abuse	Customer data access
Healthcare service providers	Healthcare	Identity compromise	Sensitive data exposure
Professional services firms	Services	Delegated access misuse	Internal system access

This list is not exhaustive.
It is representative.

The purpose of this ledger is not attribution or diagnosis.
It is to demonstrate that the patterns described earlier did not occur in isolation.

Volume, not novelty, defined the close of 2025.

Closing Note

2025 did not introduce a different threat environment.
It revealed the consequences of an outdated one.

The dominant failures observed this year were not technical.
They were structural.

Access persisted because it was legitimate.
Detection lagged because activity appeared normal.
Exposure scaled because trust was assumed, not verified.

ETR3 documented these patterns earlier in the year.
The final weeks of 2025 confirmed them repeatedly, across sectors and platforms.

The risk is no longer that organizations are unaware of these dynamics.
It is that they continue to operate as if the old assumptions still hold.
This record exists to document that reality.

This document exists to mark that shift.

elytra security

Integrity. Trust. Clarity.

An ISO/IEC 27001:2022 Certified Company

About Elytra Security

Elytra Security is a next-generation cyber and privacy solutions firm delivering operational resilience, regulatory compliance, and advanced threat protection for Indian enterprises.

We combine deep technical capability with regulatory intelligence across DPDPA, CERT-In, ISO standards, and global cybersecurity frameworks.

Our mission is to help organisations secure what matters, build trust, and lead with clarity.

2025

github.com/venkatmangudi-elytra/elytraetr3 | elytrasecurity.com | info@elytrasecurity.com