



TRUST DELIVERED

2025 DBIR & Third Party Breach Risk

A Conversation With Verizon

July 30th, 2025

Philippe Langlois, Sr Principal-Threat Intel, Verizon Business

Charlie Jones, Director Product Management, RL

Paul Roberts, Director, Editorial & Content, RL

About RL



FORTUNE 100

Over 20% of the Fortune 100 Trust RL Solutions



Finance, High Tech, Energy, Gov't, Manufacturing, and Healthcare

10101
11011
11111

Massive volumes of files, huge files, up to an entire software application



Largest Threat Repository of 422B+ searchable files proprietary threat research



60+ Security Companies Trust RL Insights



Fastest and most accurate threat and risk analysis



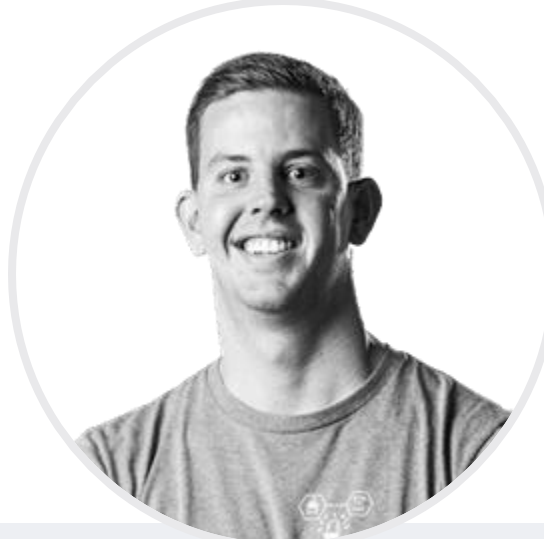
Spectra Core with Complex Binary Analysis deconstructing files in seconds or minutes



Today's Speakers



Philippe Langlois
Sr Principal-Threat Intel,
Verizon Business



Charlie Jones
Director, Product Management
ReversingLabs



Paul Roberts
Director, Editorial & Content
ReversingLabs

Agenda

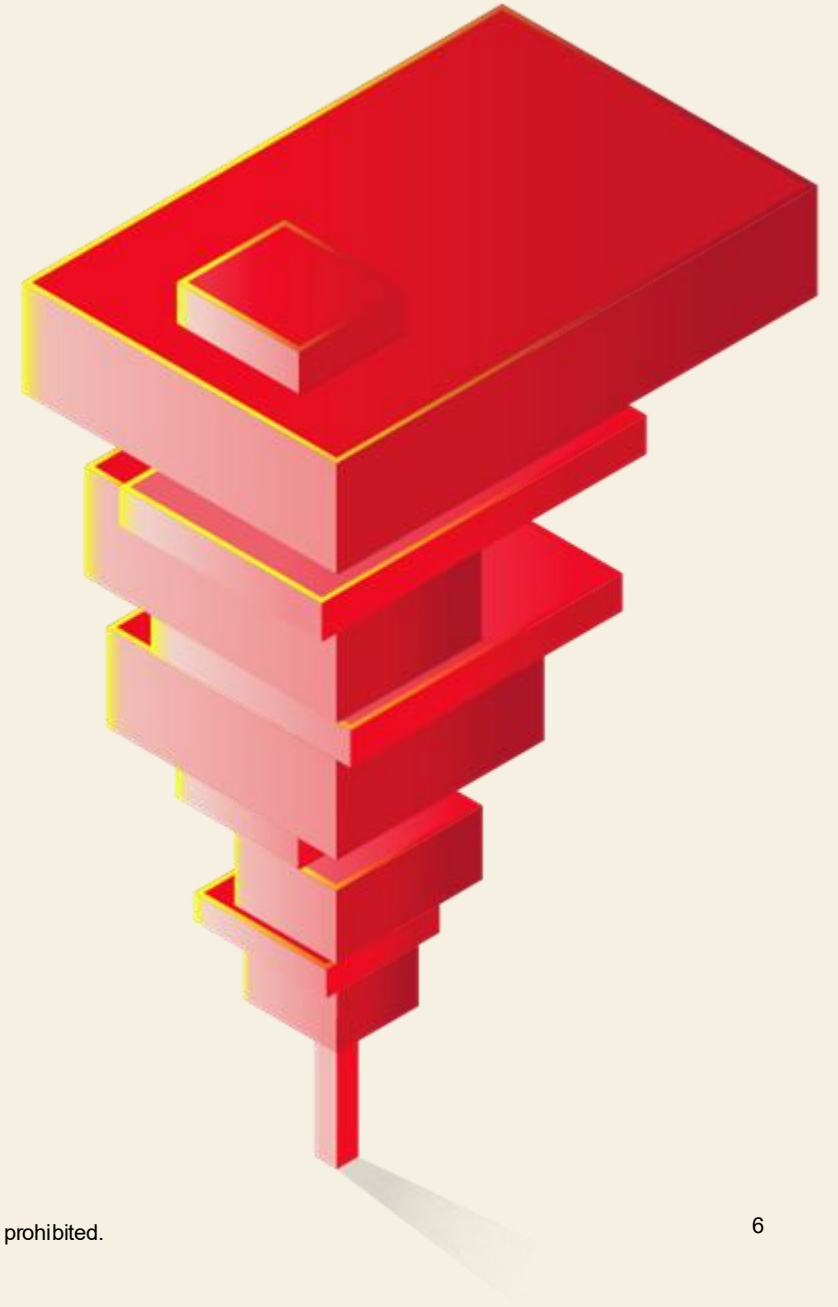
- **2025 DBIR Report Overview**
- **Key Findings**
 - **Third Party Involvement in Breaches**
 - **Sensitive Information Exposure**
 - **Enterprise AI Risks**
- **Q&A**

2025 Data Breach Investigations Report

**The authoritative source of
cybersecurity breach information**



Overview of Report



A comprehensive look at data breaches

18

years of the Data Breach
investigations Report

22,052

incidents reviewed in our 2025
report

139

victim countries identified

12,195

data breaches analyzed in our
2025 report



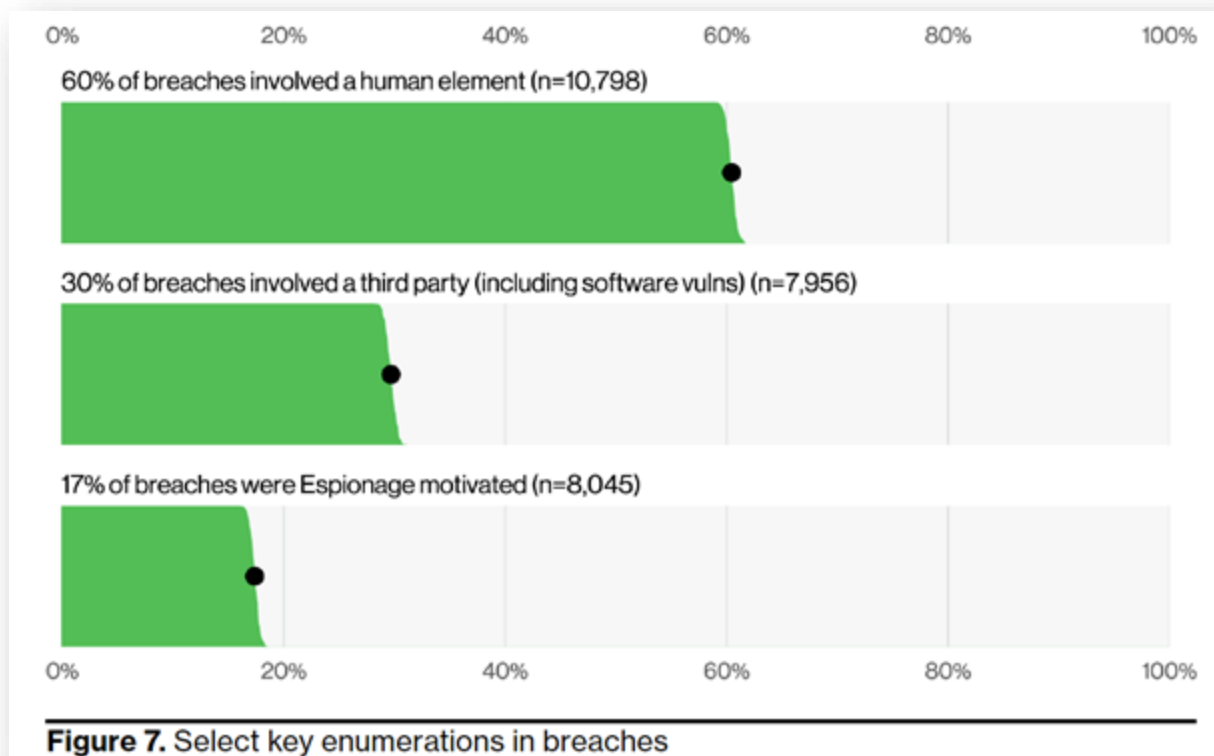
TRUST DELIVERED

Third Party Involvement in Breaches

Third-Party Breaches Up 100%

Yes, includes Third-Party Software

“The percentage of breaches where a third party was involved doubled, going from 15% to 30%.”



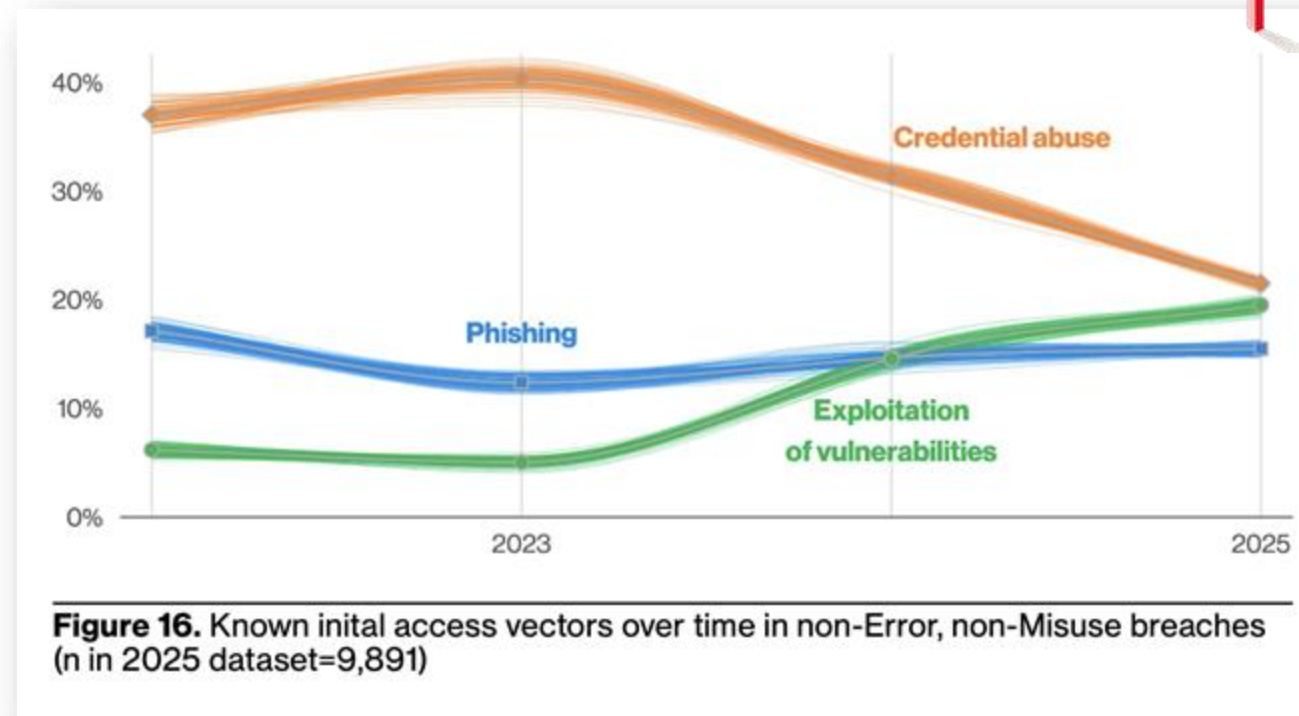
Source: Verizon, [“2025 Data Breach Investigations Report”](#), 2025

Embedding Security in Procurement

Proactively mitigate the risk of vulnerability exploitation in vendor products



“From the discussion, it was clear that having a security outcome component as part of the vendor selection process was more and more justified as we continued to see growth in the exploitation of vulnerabilities as one of our initial access Actions.”



Source: Verizon, [“2025 Data Breach Investigations Report”](#), 2025

Vendor Risk Mitigation

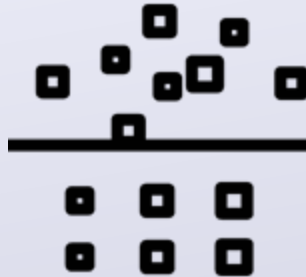
Defense strategies differ based on nature of relationship

1



**Vendor that connects to
your network**

2



**Vendor hosting your
data in their environment**

3



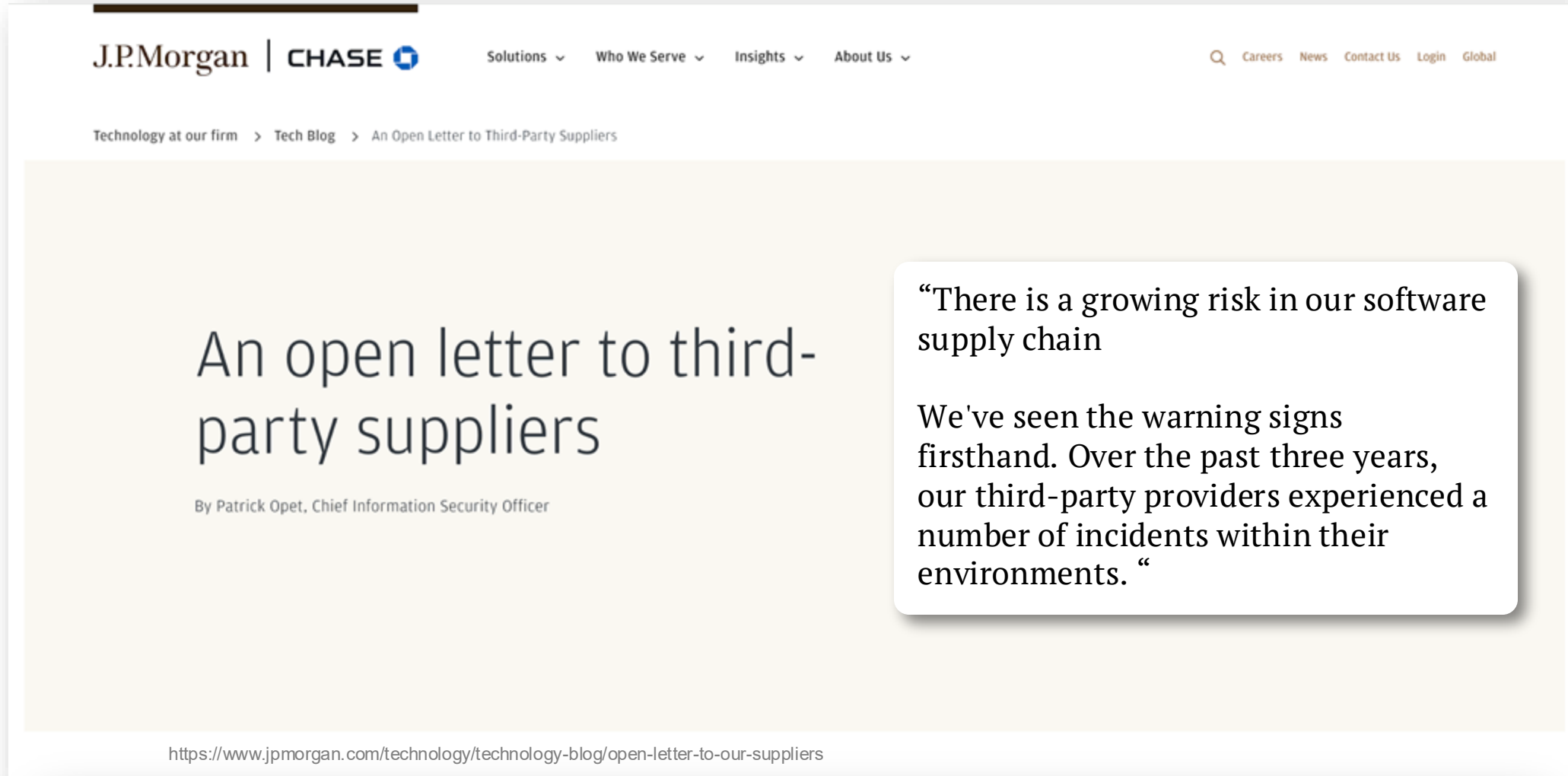
**Vendor in your supply
chain**



“If you were in any other industry and a fundamental flaw was introduced in your supply chain due to defective raw materials or machinery, your organization would at the very least be sending a sternly worded letter to the supplier.”

Verizon 2025 Data Breach Investigations Report

Speaking of a sternly written letter....



The screenshot shows the top of a J.P. Morgan Chase website. The header includes the J.P. Morgan Chase logo, navigation links for Solutions, Who We Serve, Insights, and About Us, and a search bar with links for Careers, News, Contact Us, Login, and Global. Below the header, a breadcrumb trail reads: Technology at our firm > Tech Blog > An Open Letter to Third-Party Suppliers. The main content area has a light beige background. On the left, the title 'An open letter to third-party suppliers' is displayed in a large, dark font, followed by the author 'By Patrick Opet, Chief Information Security Officer' in a smaller font. On the right, a white box contains a quote: 'There is a growing risk in our software supply chain' followed by 'We've seen the warning signs firsthand. Over the past three years, our third-party providers experienced a number of incidents within their environments. '.

J.P.Morgan | CHASE

Solutions ▾ Who We Serve ▾ Insights ▾ About Us ▾

Search Careers News Contact Us Login Global

Technology at our firm > Tech Blog > An Open Letter to Third-Party Suppliers

An open letter to third-party suppliers

By Patrick Opet, Chief Information Security Officer

“There is a growing risk in our software supply chain

We've seen the warning signs firsthand. Over the past three years, our third-party providers experienced a number of incidents within their environments. “

<https://www.jpmorgan.com/technology/technology-blog/open-letter-to-our-suppliers>

RL's 2025 SSCS Report

A deep dive into commercial VPN client security

RL Threat Researchers evaluated 20 distinct versions of VPN clients from six, prominent vendors and found worrying trends.

- 7 of 20 VPN packages contained one or more software vulnerabilities that are patch mandated and/or that are being actively exploited by malware.
- A VPN package from a prominent vendor contained 50 CVEs
 - 4 CVEs rated “critical” severity and actively exploited by malware
 - 12 CVEs rated “high” severity
 - CVEs dated back to 2009 with patches available but not applied
- 4 of 20 VPN packages we scanned contained exposed developer secrets - a popular target for malicious actors.





TRUST DELIVERED

Sensitive Information Exposure

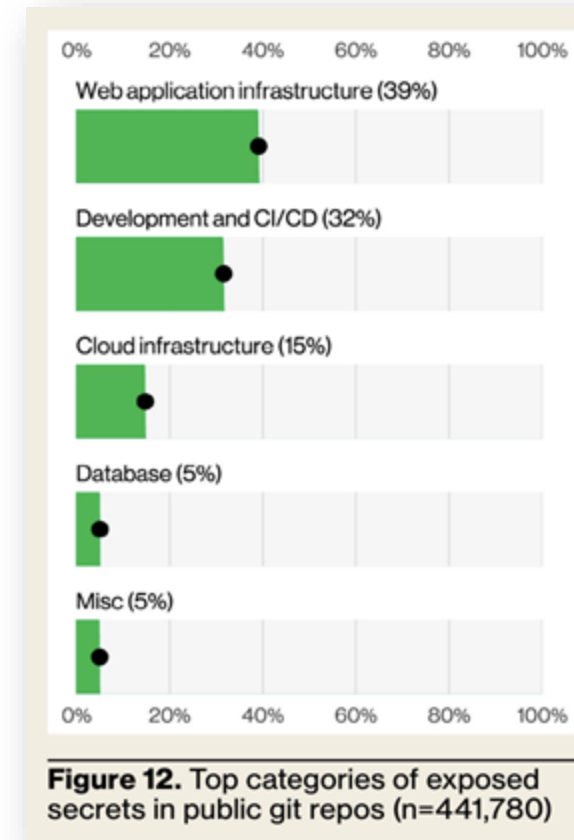
Secrets Exposed

Exploring the categories of enterprise secrets leaked in public



Key Findings

- 50% of all development and CI/CD secrets that are being leaked are Gitlab tokens
- 66% of disclosed web application infrastructure secrets are JSON Web Tokens (JWT), commonly used in authentication, session management and access control mechanisms.
- 43% of disclosed cloud-infrastructure secrets are Google Cloud API keys.



Verizon 2025 Data Breach Investigations Report

Secrets Exposed

Diving deeper into the categories of secrets identified in NPM

Types of Discovered npm Secrets 2024

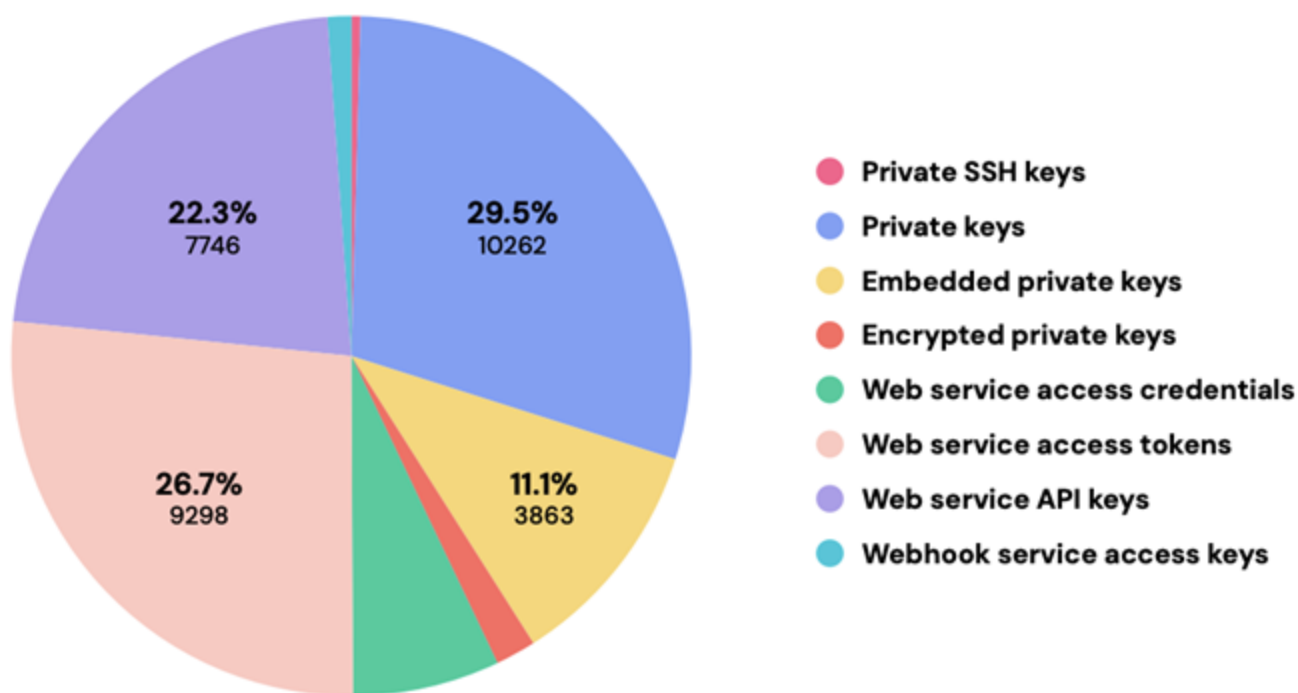
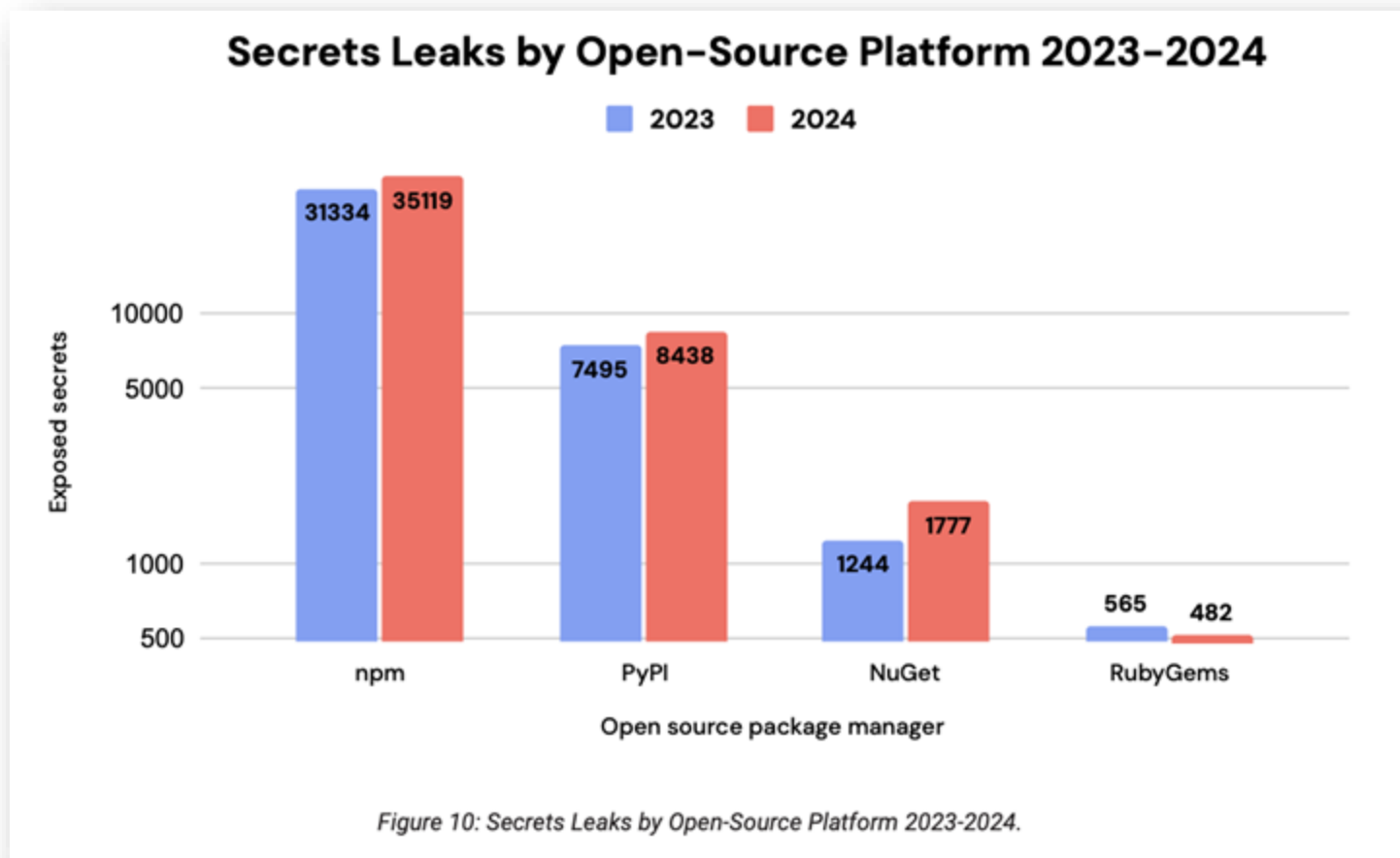


Figure 13: Secrets Discovered on npm in 2024.

“When looking at the types of secrets that were most often discovered lurking in open-source repositories, the vast majority — close to 80% — fell into three categories: private keys, web-service API keys, or web-service access tokens”

Development Secrets Leaks Jump 12%

Secrets exposure increasing across major OSS communities



“Secrets leaks across the four major open-source repositories RL tracks — npm, PyPI, NuGet, and RubyGems — continued to be a major issue in 2024, with the number of discovered secrets detected by RL standing at 45,816 through September 30, 2024 — a 12% increase from the same period a year earlier.”



TRUST DELIVERED

Enterprise AI and ML Risks

GenAI Risk in Corporate Environments

Growing concerns of non-integrated/sanctioned AI use



“Analyzing data from corporate browser monitoring systems, we found that 14% of employees were routinely accessing GenAI systems on their corporate devices. Figure 24 illustrates an even more concerning picture: A large number of those were either using a non-corporate email as the identifier of their account (72%) or using their corporate email without an integrated authentication system such as Security Assertion Markup Language (SAML) in place (17%), suggesting that accessing those systems may not be a part of the sanctioned applications allowed in their corporate environment.”



Figure 24. Percentage breakdown of GenAI service access account types (each glyph is 0.5%)

The **ML**elephant in the Room

PICKLE FILES: THE NEW ML MODEL ATTACK VECTOR

Your favorite brined serialization format, now with a side of attack framework

By: Eoin Wickens, Marta Janus, Tom Bonner



BLEEPINGCOMPUTER

Home > News > Security > Malicious AI models on Hugging Face backdoor users' machines

Malicious AI models on Hugging Face backdoor users' machines

By **Bill Toulas**

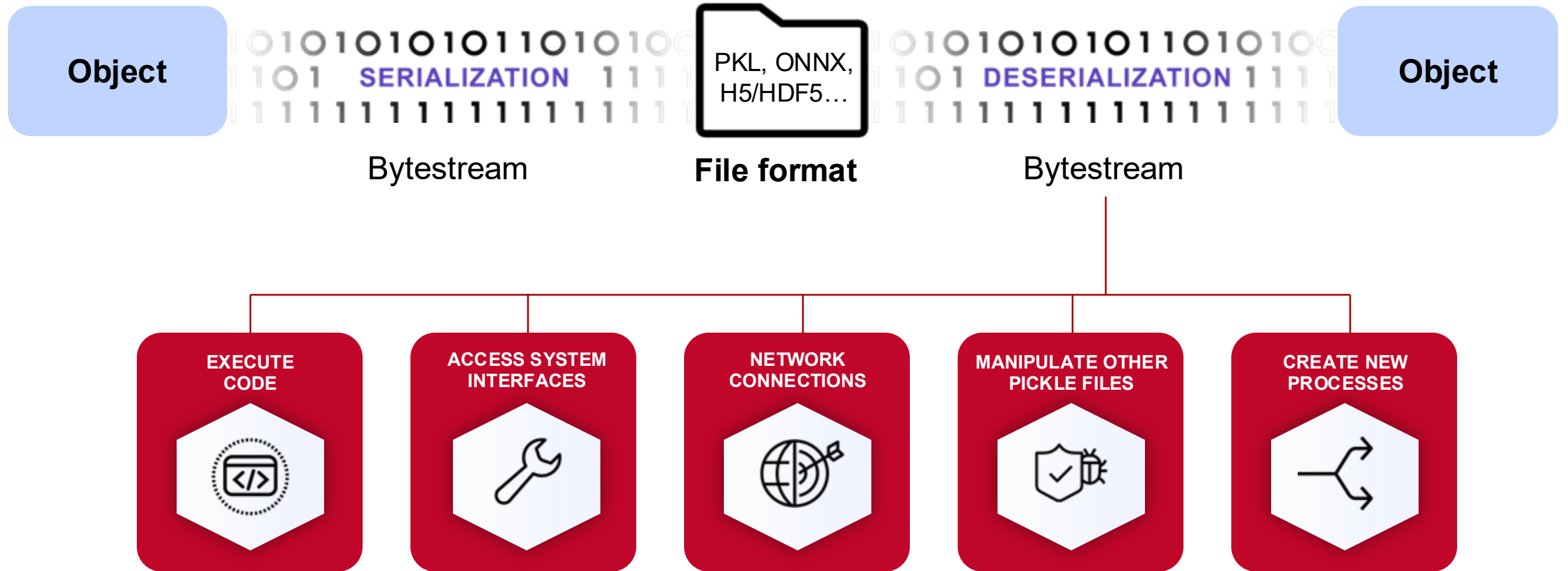
February 28, 2024 05:12 PM 1



80% OF ML MODELS ARE
Vulnerable to Code Injection and Arbitrary Code Execution



Using Deserialization to Spread Malware



Establishing a Robust SSCS Strategy



Build SAFE.

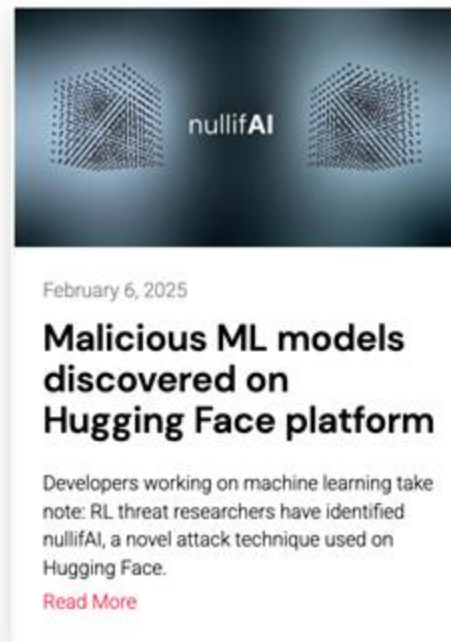


Buy SAFE.



Stay SAFE.

Additional Resources



Upcoming Events





ЯЛ

Thank You