BITSIGHT Luminate EXCHANGE

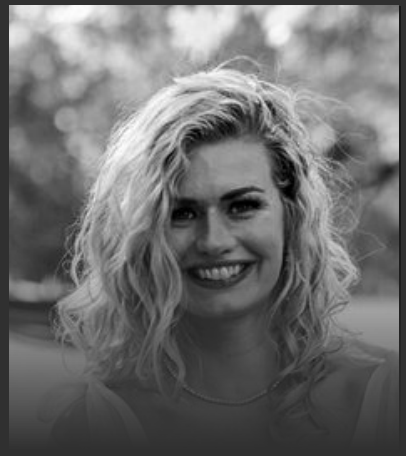
04

Bitsight TRACE Research

BITSIGHT

Speakers

BITSIGHT Luminate EXCHANGE



Emma Stevens

BITSIGHT THREAT RESEARCHER

João Godinho

BITSIGHT THOUGHT LEADERSHIP

BITSIGHT

BITSIGHT Luminate EXCHANGE

BITSIGHT TRACE

BITSIGHT

BITSIGHT Luminate EXCHANGE

BITSIGHT RESEARCH

Ransomware with a Twizt: Inside the Phorpiex Botnet

Read blog post

BITSIGHT RESEARCH

RondoDox Botnet: From Zero to 174 Exploited Vulnerabilities

Read blog post

BITSIGHT RESEARCH

4 Predictions Our Researchers Say Could Break (or Break Through) in 2026

Read blog post

BITSIGHT RESEARCH

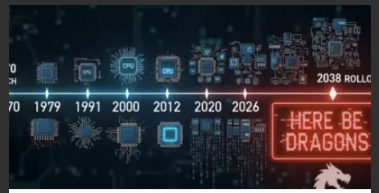
OPC UA Exposure Snapshot: A Year in Review of Internet-Facing Devices

Read blog post

BITSIGHT RESEARCH

CVE-2025-55182: First Days of React2Shell Exploitations

Read blog post



BITSIGHT RESEARCH

Forward to the Past: The Y2K38 Problem Ahead

Read blog post

BITSIGHT RESEARCH

Red Vulns Rising: Examining Chinese National Vulnerability Databases

Read blog post

BITSIGHT RESEARCH

OpenClaw (ex-Moltbot (ex-Clawdbot)): The AI Butler With Its Claws On The Keys To Your Kingdom

Read blog post

BITSIGHT

BITSIGHT TRACE RESEARCH

Exposure and Threat Intelligence

BITSIGHT Luminate EXCHANGE

1B+

Monthly Observations

Bitsight's Groma scanning engine maintains a continuous global survey of the public-facing Internet.

200M+

Monthly Infections

Bitsight's Sinkhole infrastructure gathers infection telemetry from around the world infected machines.

50M+

Monthly Records

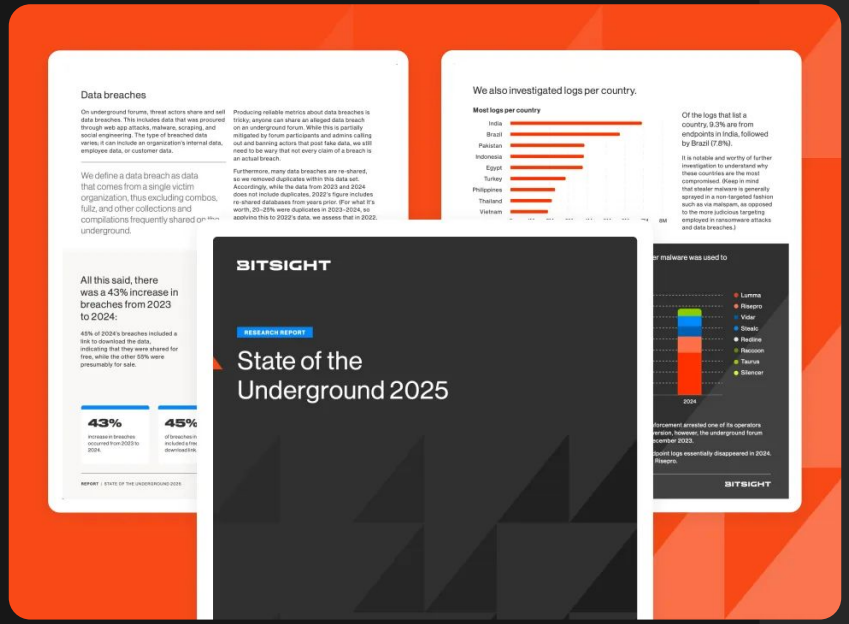
Bitsight Threat Intelligence maintains visibility into restricted, invite-only areas of the dark web.

BITSIGHT

ANNUAL RISK REVIEWS ARE TOO SLOW FOR TODAY'S THREAT PACE.

2026 Security Landscape Overview

BITSIGHT Luminate EXCHANGE



Key Findings & Insights

- State of the Underground 2026 provides a comprehensive analysis of global cyber threats.
- Targeted research into country-specific vulnerabilities and data breach trends.
- Critical focus on the evolution of ransomware and credential theft.
- Annual risk reviews are too slow for today's threat pace.

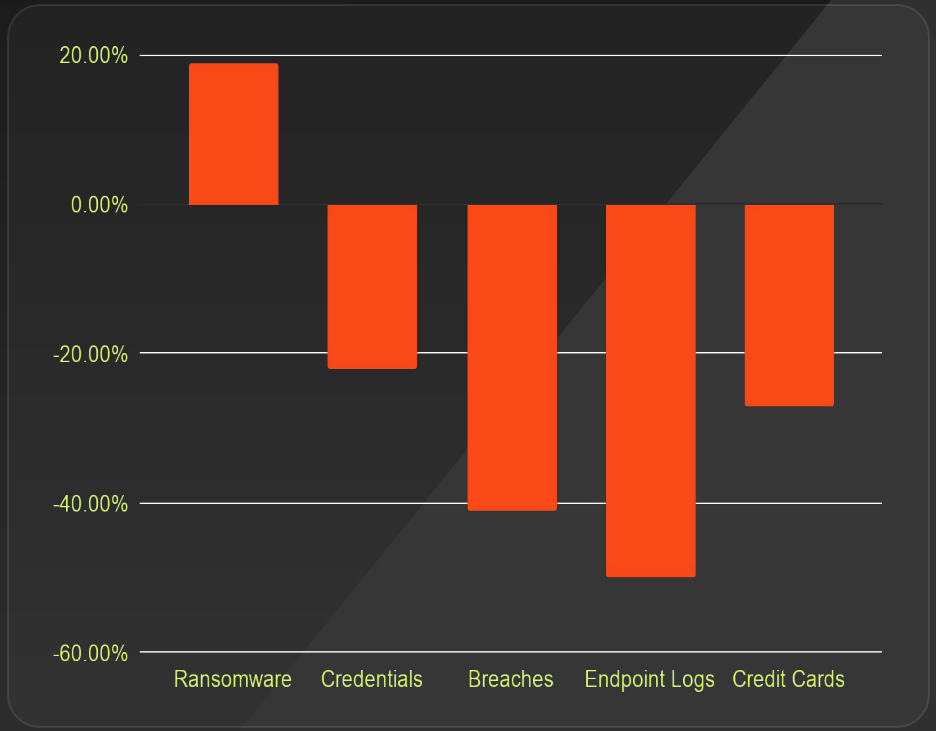
BITSIGHT

A Closer Look Tells a Different Story

LOWER BREACH COUNTS DON'T MEAN LOWER RISK.

Chess, not Checkers

- Overall decline in exposed data
- Europe second most targeted region
- We are winning, right?



Thank you

We will not take any questions.

REACTIVE COMPLIANCE IS NOT ENOUGH ANYMORE.

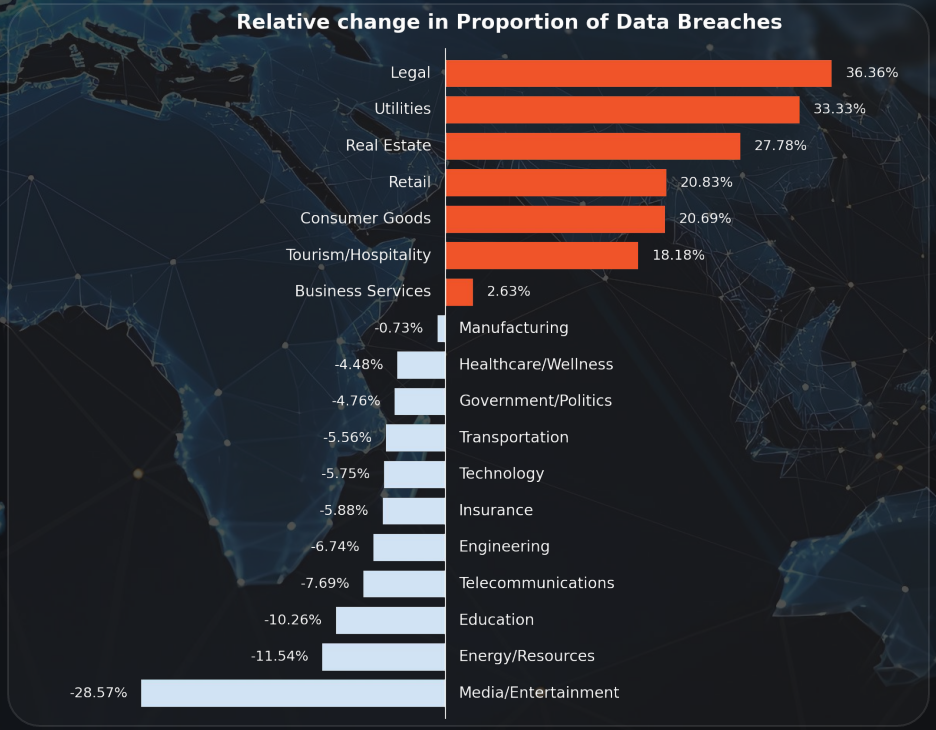
New Era of Threats

- Threat actors are shifting from data theft to direct disruption
- Ransomware and hacktivism are taking center stage
- Attackers are adopting AI to move faster and hit harder
- Geopolitical conflict is giving attackers more visibility, resources, and momentum
- Your supply chain is not your friend

THREAT ACTORS ARE SHIFTING TARGETS.

New Targets in the UK

- CNI is under fire: **93% reported a cyber incident in 2026**
- APT groups are going straight after critical infrastructure (CVE-2021-22681)
- ICS attacks are rising, putting real-world operations at risk



Still Exposed

YOUR ATTACK SURFACE IS GROWING FASTER THAN YOUR CONTROLS.

BITSIGHT Luminate EXCHANGE

Internet Exposure

Threat actors take advantage of the increased attack surface due to the increase of internet exposed devices.

34M IPs

In 2025 alone we measured 34M vulnerable IPs and more than 675,000 vulnerable entities.

45%

YoY increase in vulnerable IPs.

27%

YoY increase in vulnerable entities.

BITSIGHT

YOUR VENDORS' EXPOSURE BECOMES YOUR LIABILITY.

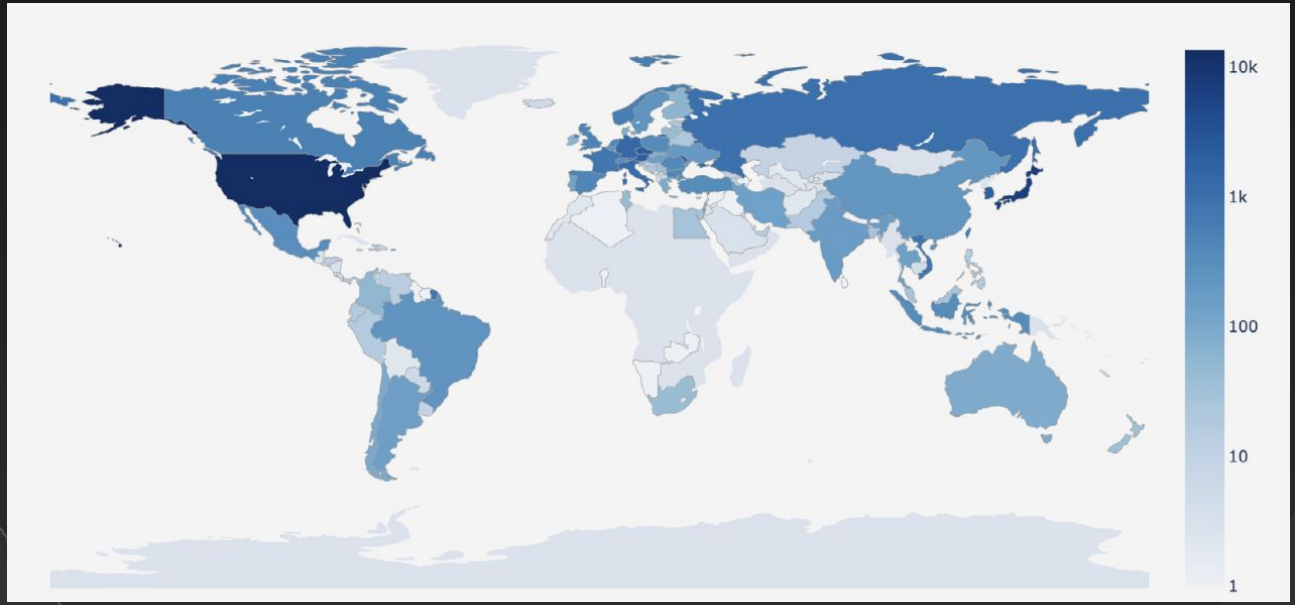
BITSIGHT Luminate EXCHANGE

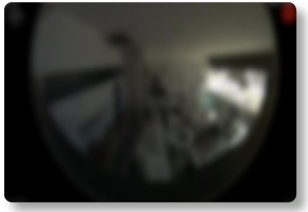
40,000 Exposed Cameras → Exposed Vendors → Exposed You.

your CCTV is vulnerable and can be exposed,

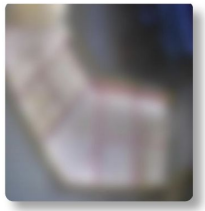
fix it pls - DIY or Telegram me - faxociety.

40,000 Exposed Cameras

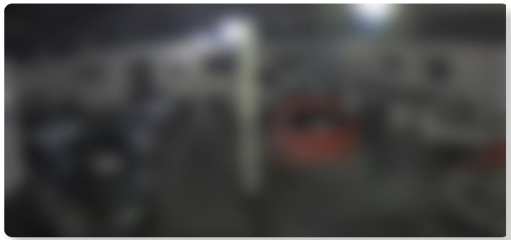




Screenshot 16: *A camera monitoring a smartphone and electronics store.*



Screenshot 17: *A camera closely watching a jewelry showcase.*



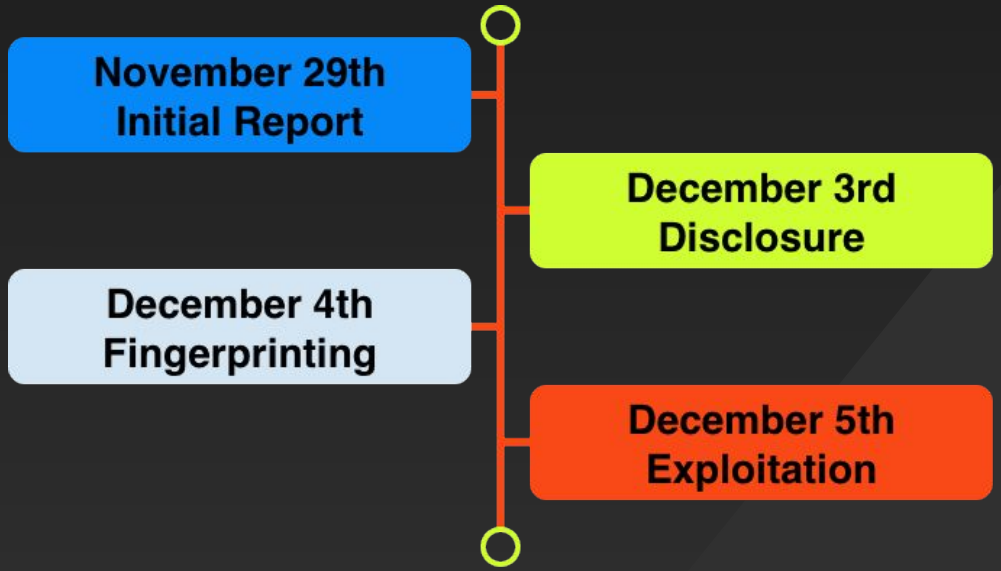
Screenshot 18: *A camera watching the interior of a luxury car dealership exposing a Porsche 911 (992), two Chevy Corvette Z06, a Bentley Flying Spur and a Mercedes-Benz SLS 63 AMG[4].*

BITSIGHT

PATCH TIMELINES MUST MATCH ATTACKER TIMELINES

BITSIGHT Luminate EXCHANGE

Your Supply Chain Exploited in Under 48 Hours



BITSIGHT

Who's Pulling the Strings?

RISK PRIORITIZATION SHOULD FOLLOW ATTACKER INTENT.

Motivation Drives Behavior

BITSIGHT Luminate EXCHANGE

Financial

Profit-driven operations and extortion

Ideological

Ideological influence and disruption

State-Backed

Strategic espionage and national interests

Top 5 threat actors were responsible for **41.4%** of all ransomware attacks!

Top 10 – 57.7%

BITSIGHT

YOU MAY NOT BE THE TARGET, BUT YOU CAN STILL BE THE IMPACT.

Know Your Enemy. And Theirs.

BITSIGHT Luminate EXCHANGE

Hello!

Visit our Blog:
Tor Browser Links:
http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd[.]onion/
Links for normal browser:
http://redacted/

>>> Your data is stolen and encrypted.

If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind that once your data appears on our leak site, it could be bought by your competitors at any second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your company will be safe.

BITSIGHT

ATTACKERS TARGET WHO IS MOST PRESSURED TO PAY, LIKE YOUR CRITICAL VENDORS.

BITSIGHT Luminate EXCHANGE

Nothing to Lose. Everything to Gain. They Don’t Need You First

Ransomware is up!

- Profit-driven and adaptive
- Built for scale and speed
- Targeting identity and transactions
- Blending into legitimate activity

BITSIGHT

ASSOCIATION ALONE CAN CREATE EXPOSURE

BITSIGHT Luminate EXCHANGE

Geopolitical Tensions, Cyber Consequences

THREAT ACTOR PROFILE

TeaMp0isoN

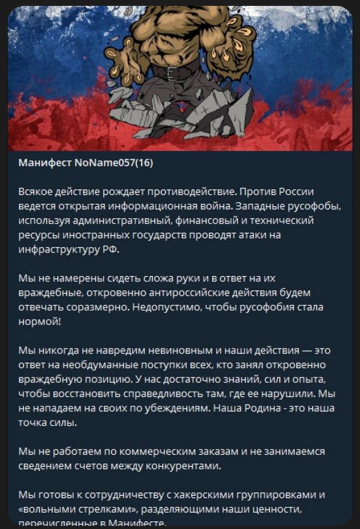
Actively targets:

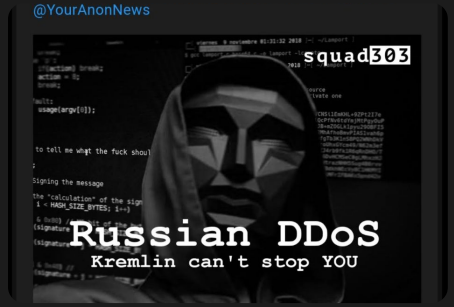
- NATO
- English Defence League

Supports:

- Palestine
- Pro-Islam

OPERATIONAL EVIDENCE





BITSIGHT Luminate EXCHANGE

State Power in Cyberspace

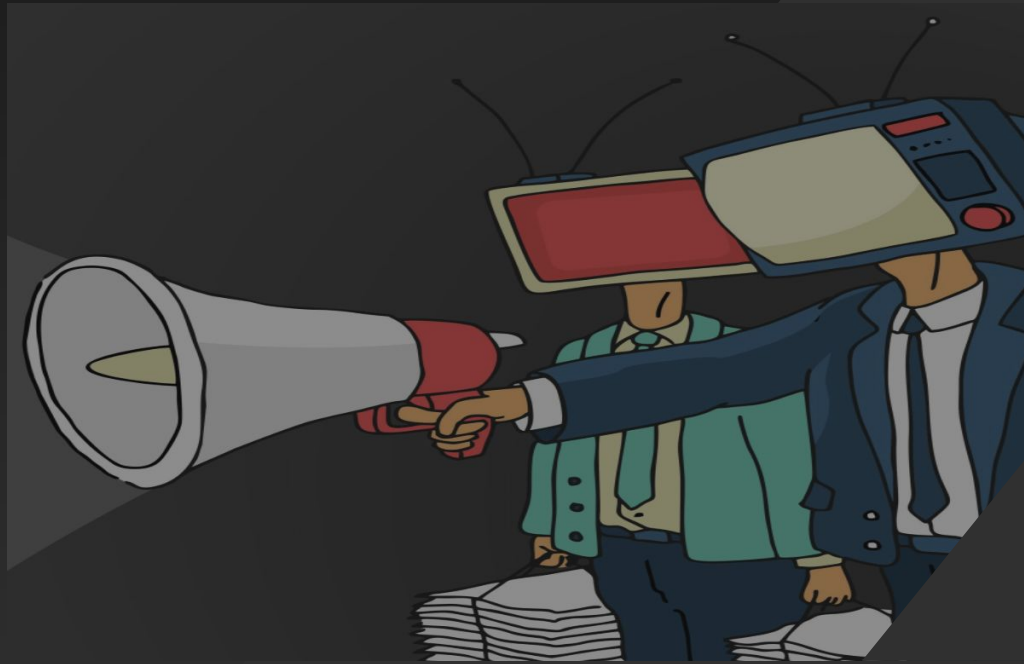
- Mission-driven
- Focused on espionage, disruption, and influence
- $$$ Talks
- Hexagonal Rodent

THIS IS NOT THE TIME TO EASE CONTROLS.

BITSIGHT Luminate EXCHANGE

Breaches down? A Decline Worth Questioning

- Narrative as a Weapon
- Ego-Driven Attacks
- What Goes Unseen
- Nation-State vs. Financial Actors



BITSIGHT

The Gaps Attackers Find

BITSIGHT Luminate EXCHANGE

Non-Linear Attacks

Attackers don't need a direct path to hurt you.

Evolving TTPs

Controls decay. GRC has to revalidate them.

Third-Party Risk

A Third-Party Mistake, First-Party Consequences

BITSIGHT

VENDOR RISK. CASCADING IMPACT.

BITSIGHT Luminate EXCHANGE

Higher Stakes, Greater Impact

Industrial Control Systems/Operational Technology (ICS/OT)

- March 2026, Iran-attributed attack on the national wheat silo management system of Jordan.
- NoName 057(16) targeting ICS/OT.

BITSIGHT

TRUST SIGNALS LEVERAGED FOR ATTACKS

The Enemy Looks Residential

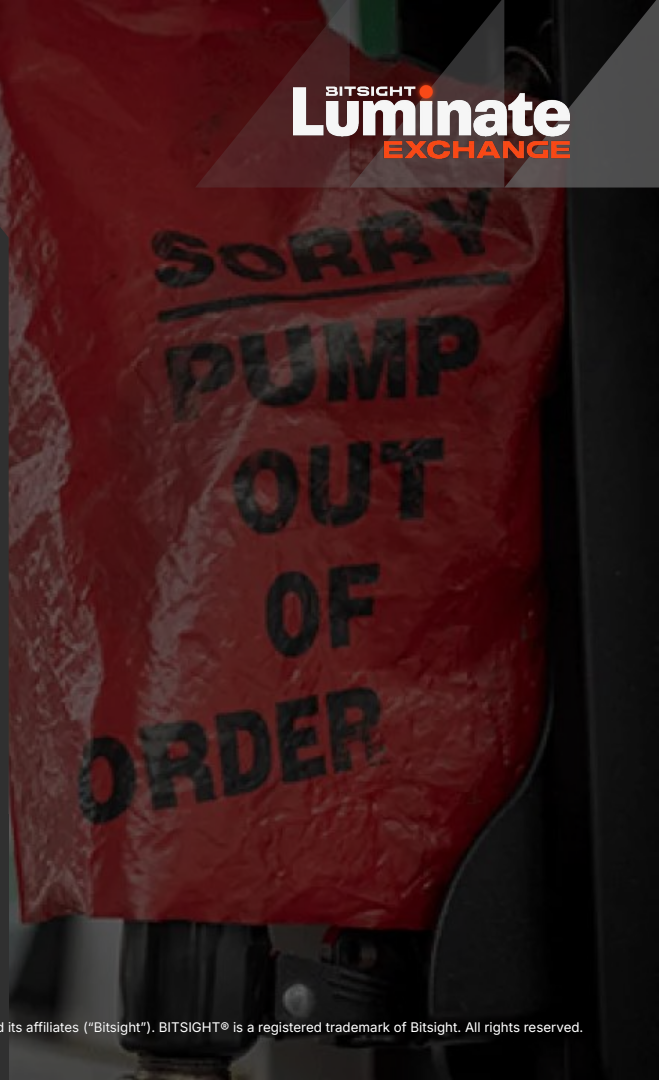
The Home Network Threat

- Residential targets used as proxies
- Bypassing IP/Geo restrictions
- A launchpad for account takeover, fraud, reconnaissance, and spam
- When trust signals fail, third-party risk increases.

YOUR RESILIENCE DEPENDS ON YOUR SUPPLIERS' RESILIENCE.

What Keeps Us Running Is at Risk

- TfL: 10M impacted. Critical services disrupted.
- Essential services depend on supplier ecosystems
- UK critical infrastructure and key resources are a target for APTs and profit-driven actors



TAKEDOWNS BUY TIME, NOT SAFETY

The Whack-a-Mole Effect

BITSIGHT Luminate EXCHANGE

Persistent Threat Resurgence

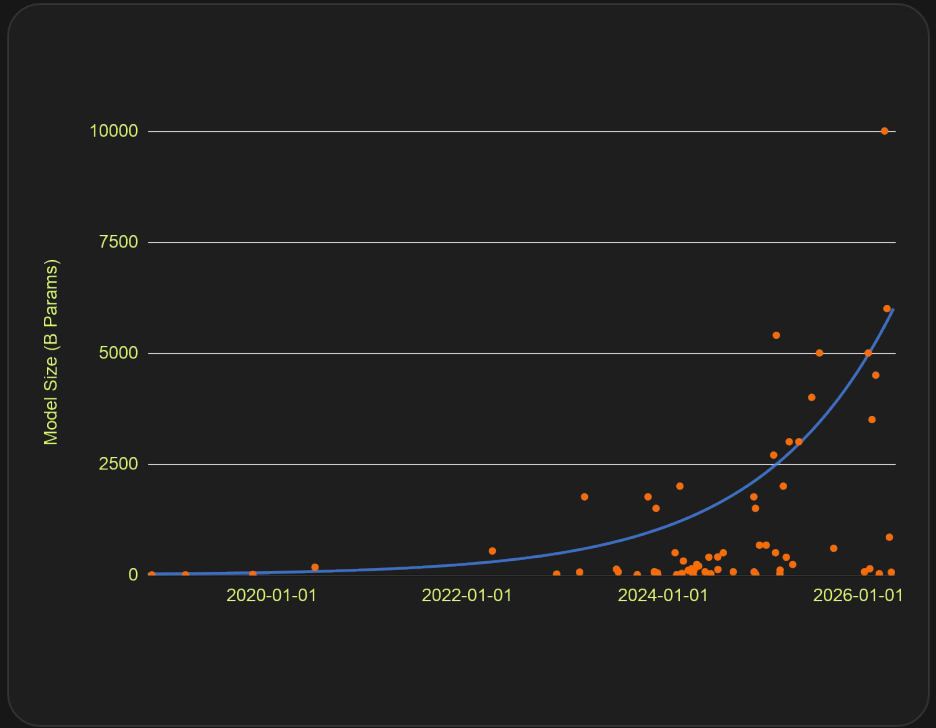
- Actors rebrand, regroup, and return
- TTPs shift as defenses catch up
- Decentralized networks keep campaigns alive

AI Proliferation

AI EXPANDS OPPORTUNITY AND CAPABILITY

Models are Growing

- Exponential growth
- Market divergence
- Future Plateau



AI LETS ATTACKERS MOVE FASTER AND SCALE CHEAPER

This is Already Happening

Malicious Interest

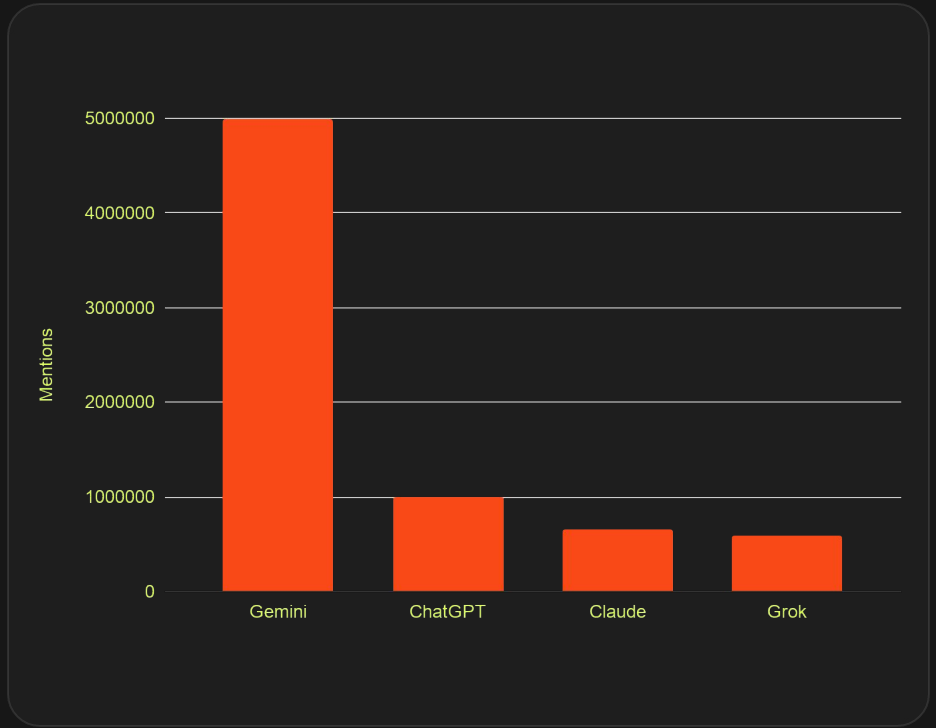
Threat Actors are interested in using AI - HexagonalRodent, StarFraud, Vercel.ai

Efficiency Gains

Evidence of AI to increase productivity

Operational Hurdles

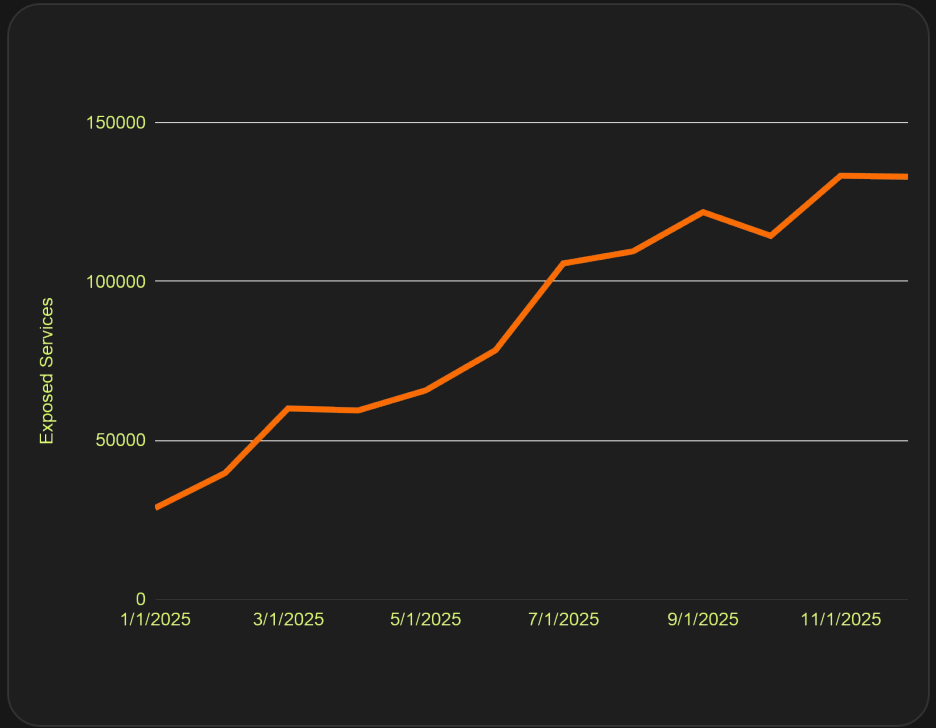
Threat Actors face even more issues than SaaS on AI usage



AI ADOPTION IS OUTPACING AI GOVERNANCE

AI Risk is Scaling Fast

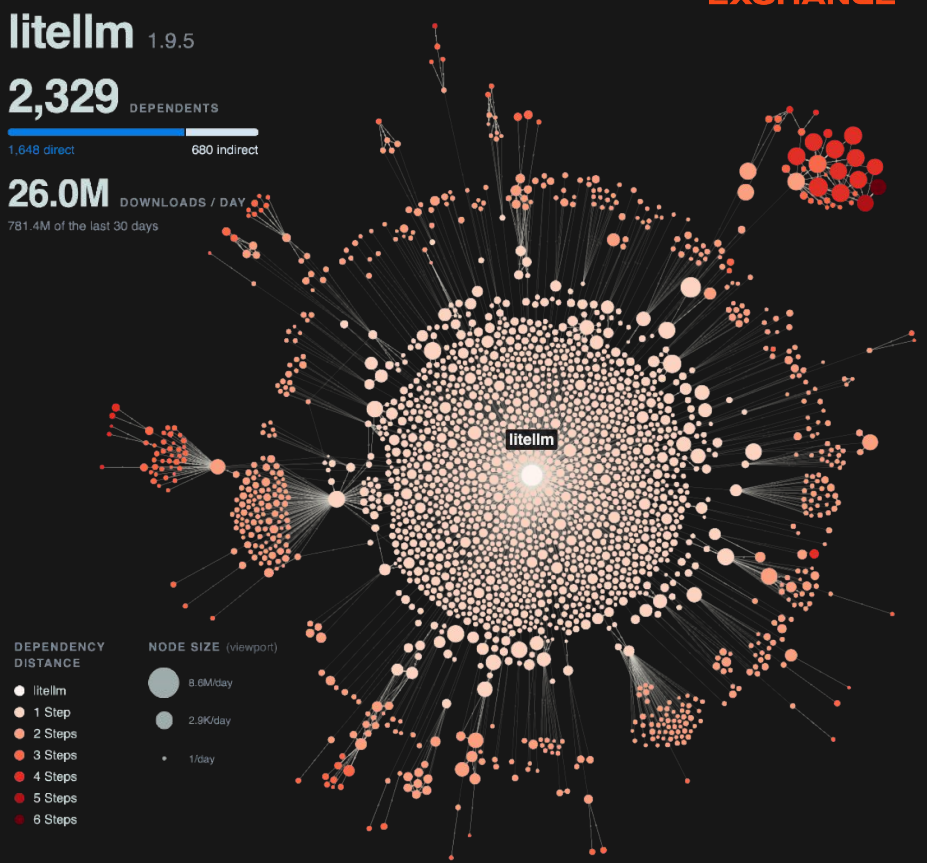
- **360% increase**
- **One million+ services**
- **Continued Rise**



BITSIGHT Luminate EXCHANGE

LiteLLM Case

- TeamPCP compromise in early March
- 26M Downloads per day
- Trust exploitation at scale + credential concentration + transitive exposure



BITSIGHT

What the future holds

Cyber risk is no longer contained

Global Tensions Fuel Risk

Geopolitical conflict is giving attackers more visibility, resources, and momentum

Ransomware and hacktivism are taking center stage

The shift towards disruption

AI Changes Everything

AI is expanding your attack surface faster than governance can keep up.

Your supply chain is not your friend

Your biggest risk isn't you, it's your suppliers, software, and ecosystem.

BITSIGHT

BITSIGHT

BITSIGHT Luminate EXCHANGE

Thank you

João Godinho
joao.godinho@bitsight.com

Emma Stevens
emma.stevens@bitsight.com