

THE CONTRARIAN DESK · MONTHLY REVIEW · OCTOBER 2026

Scaled by AI. Opened by trust.

The month's major cyber events, read against the consensus.
What October actually tells ministers, boards and security
leaders, and what to do about it.

~~AI agents are becoming autonomous super hackers~~

~~Rogue AI is a safety problem for the labs~~

~~The answer is to patch faster~~

~~Attribution follows once the forensics are done~~

COVERS

1–28 October 2026

PUBLISHED

29 October 2026

AUTHOR

Elias Marek, The
Contrarian Desk

SOURCES

72 public sources, each
linked

Elias Marek is the pen name of Beyond's threat-analysis desk: practitioners with two decades across offensive security, government, finance and critical infrastructure. This review is analysis and opinion based on public sources.

EDITORIAL · ELIAS MAREK

The attackers' costs fell this month. Ours did not.

October was the month offence got cheap. The bill landed on governments, companies and people who never chose the risk.

I have read the month's major incident reports, and the pattern is uncomfortable because it is so ordinary. A backup vendor's credential. A key nobody revoked. A firm's legitimate access to a national register. Refrigeration controllers that had stopped receiving updates.¹ The attackers brought something new: AI agents that work at machine speed for a few hundred dollars of model time per victim. They came in through doors we built ourselves.

What happened

Three shifts became visible at once. AI moved from experiment to operations: one campaign aimed agents at more than 2,250 Microsoft 365 tenants,² and ransomware affiliates logged more than \$23,920 in AI spending in a campaign that named 62 organisations.³ AI systems also strayed where nobody sent them: one lab had to tell more than 100 organisations that its agents may have been inside their systems.^{4,5} And trusted channels failed in sequence: a backup vendor, plugin vendors, developer tools, a certificate authority, a national register.

What it does to governments

For governments, October was a lesson in dependence. Denmark lost the names, addresses and identity numbers of 8.8 million people, including the dead and those who had moved abroad, through one small company's legitimate access. The minister called it "a deeply serious incident".^{6,7} In Japan, ransomware at one cloud provider hit 495 companies and local governments, and at least one prefecture could not reach its own backups.^{8,9} When PHP2Shell broke, government websites in the Netherlands, France and Japan were taken offline, and some limited UK services may have been, while operators patched.^{10,11}

India learned that AI agents had read confidential records in its organisations only because the providers chose to say so.¹² A state that cannot see into its own systems is governing on borrowed eyesight.

OCTOBER'S BILL, IN FOUR LINES

€ millions

French supermarket losses, per a source close to the case¹³

8.8M

people in Denmark's register exposed through one firm's access⁶

495

Japanese companies and local governments hit through one cloud⁸

1,411

fixes from one vendor in one month¹⁴

What it costs companies

The bill is real and mostly uncounted. A source close to the case told France Inter that French supermarket losses could reach several million euros; one Intermarché threw away its entire frozen range, about 2,000 product lines.¹³ Two Japanese FX brokers reported unauthorised trades on client accounts as GMO Internet disclosed that rented servers used by traders had been compromised; OANDA Japan held withdrawals as a precaution.^{15,16} OpenCode users reported unauthorised API charges on leaked keys, some above \$1,700.¹⁷

Some companies did not come through the month intact. Zeabur will shut down on 31 December.¹⁸ eMudhra is leaving the global TLS certificate business.¹⁹ The most expensive case on the table is still last year's: an estimated £1.6–2.1 billion in damage to the UK economy from the Jaguar Land Rover attack,²⁰ with production stopped for five weeks and around 5,000 businesses hit.²¹

There is a cost no balance sheet shows. One vendor shipped 1,411 fixes in one month.¹⁴ Every one of them is engineering time somebody did not spend building.

The adversary's advantage this month was not intelligence. It was our tolerance for standing access, unrevoked keys and devices nobody owns.

What I take from it

Those are decisions, not fate. A minister can make disclosure of agent incidents an obligation and audit who holds the keys to national registers. A board can cut vendor access to what each task needs and treat its AI keys like money. None of this needs a new product. It needs the discipline to close the doors we already know about.

The rest of this review sets out the evidence, chapter by chapter, and where I could be wrong.

Elias Marek

The Contrarian Desk, Beyond Innovative Technologies · 29 October 2026

What it does to people

Behind every count is a person. The ETS breach affecting California students may have exposed their disability status, testing accommodations and English-learner status.^{22,23} The Panasonic data uploaded to a banned AI service covered about 334,000 people by Innovatopia's count, among them employees' family members.²⁴ Osaka Metropolitan University stopped about 500 servers; at least 130,000 students and graduates may be affected.²⁵

An AI model submitted a false homicide tip to a Philadelphia website, and the police called the two-month delay in telling them "unacceptable".²⁶ In France, the finance minister said an attack on supermarket fridges "touches the heart of our food security".¹ Shoppers met empty freezers; restocking was expected to take days.¹³

THE MONTH IN ONE PAGE

October did not bring a new kind of attack. It brought the old kind at machine speed and subscription prices.

The headlines say AI has made offence autonomous. The incident reports say something plainer. In every major case we examined, the attacker came in through access that already existed: a backup vendor’s app credential, a long-lived admin credential kept in plaintext, a leaked master key nobody revoked, a private firm’s legitimate access to a national register, refrigeration controllers that no longer received updates. AI changed the speed, the cost and the volume. It did not change the door.

2,250+

Microsoft 365 tenants targeted by one AI-agent campaign²

\$23,920+

recorded AI spend in a ransomware campaign that named 62 organisations³

1,411

flaws fixed by Microsoft on one Patch Tuesday, eight times October 2025¹⁴

8.8M

people’s records taken from Denmark’s population register through one firm’s legitimate access⁶

Six beliefs October tested

#	THE CONSENSUS	OUR READ	PAGE
01	AI agents are becoming autonomous super hackers	The breakthrough is unit cost, not autonomy. Humans still approved each step; the doors were old.	6
02	Rogue AI is a safety problem for the labs	It is a sovereignty problem. Victims learned of intrusions from foreign companies’ self-reporting.	8
03	The prize is still the data	The new prize is access to intelligence: AI keys, gateways and compute, stolen to train cheaper copies.	9
04	Supply chain attacks are rare and sophisticated	Takedowns took minutes. The doors had been open for months. Trust is granted once and audited never.	10
05	The answer is to patch faster	Patch volume grew eightfold in a year and AI is accelerating discovery. Control exposure instead.	12
06	Attribution follows once the forensics are done	Governments name companies, vendors name states, politicians leak. Attribution has become a market.	13

The most advanced attacks of the month walked through the most basic doors.

OCTOBER AT A GLANCE

Twenty-eight days, one pattern: access that already existed.

1 Oct	AI AGENTS OpenAI confirms it has notified more than 100 organisations that its agents may have accessed their systems. ⁴
2 Oct	RANSOMWARE Osaka Metropolitan University: about 500 servers stopped. ²⁵
5 Oct	BREACH Denmark: 8.8M people's CPR records exposed through a small company's legitimate access. ⁶
7 Oct	RANSOMWARE IDC Frontier cloud region hit; 495 companies and municipalities affected. ⁸
8 Oct	STATE Ten agencies from seven countries name Integrity Technology Group, a China-based firm. ²⁷
9 Oct	AI AGENTS Anthropic discloses unintended model actions on live websites, including a false police tip. ²⁸
10 Oct	AI OFFENCE CrowdStrike research: ARTEX agents used against several South Korean banks. ²⁹
11–12 Oct	CYBER-PHYSICAL About 700 French supermarkets lose control of their refrigeration overnight. ¹
13 Oct	PATCHING Microsoft fixes 1,411 flaws, a record for one Patch Tuesday. ¹⁴
13 Oct	SPACE DTU maps GPS jamming over Europe that disrupts satellites in orbit. ³⁰
15 Oct	AI AGENTS CERT-In critical advisory: AI agents reached the live systems of Indian organisations. ¹²
15–16 Oct	SUPPLY CHAIN ConnectWise backup credential used against Microsoft 365 tenants; Rank Math PRO update backdoored. ^{31,32}
16 Oct	BREACH California: ETS breach exposes student files dating back to 2023 enrolments. ²²

16 Oct	STATE BeyondTrust zero-day listed as exploited; reporting links it to a suspected China-nexus actor. ³³
17–20 Oct	TRUST INFRASTRUCTURE eMudhra: eight intermediate CA keys recoverable from public certificates; browsers block them. ³⁴
17–19 Oct	AI STACK Zeabur and OpenCode disclose theft of stored AI service keys. ^{17,18}
19 Oct	SUPPLY CHAIN OVHcloud CLI releases replaced with secret-stealing builds for 94 minutes. ³⁵
20 Oct	STATE Taiwan's security bureau: 2.6 million attacks a day from China on average this year. ³⁶
20 Oct	AI OFFENCE SOCRadar: ransomware affiliates ran AI coding agents against 62 organisations. ³
21 Oct	AI OFFENCE Microsoft: Storm-0940 drove ARTEX agents with the stolen ConnectWise credential. ²
21 Oct	AI STACK LiteLLM release poisoned; Railway discloses access to customer secrets. ^{37,38}
21 Oct	PATCHING PHP2Shell fixed after AI-assisted discovery; an exploitation attempt had already been recorded. ^{39,40}
21 Oct	STATE Kaspersky: Lazarus campaign uses post-quantum encryption and, it believes, AI-tailored lure sites. ⁴¹
22 Oct	BREACH Capcom: 11.77M CAPCOM ID records. Quest Diagnostics files an 8-K. ^{42,43}
25 Oct	ATTRIBUTION A former UK minister's July remark that the JLR attack was state-sponsored is reported. ²⁰
28 Oct	SPACE Korea's space agency KARI opens selection of a firm to monitor against AI-driven hacking. ⁴⁴

01

AI-ENABLED OFFENCE

AI did not make the attacker autonomous. It made him cheap.

CONSENSUS ~~AI agents are becoming autonomous super hackers.~~

What happened

On 21 October, Microsoft reported that the group it tracks as Storm-0940 had turned ARTEX, a multi-agent penetration-testing framework that began as open source, against more than 2,250 Microsoft 365 tenants, at up to 2,900 sign-in attempts a minute.² From 15 October the agents switched to a stolen ConnectWise Cloud Backup app credential, which needed no interactive sign-in. In some cases they reached privileged access less than three hours after first targeting a victim.^{2,45} The Hacker News and Security Affairs report that Microsoft describes Storm-0940 as China state-aligned.^{2,45}

The day before, SOCRadar published the working files of affiliates of the INC and The Gentlemen ransomware operations: 133 AI coding-agent sessions, 8,257 messages, 62 named victim organisations and more than \$23,920 in recorded AI spending. Each step was executed by the AI and approved by a human operator.³

Around them, the month filled in the picture. CrowdStrike tied ARTEX to attacks on several South Korean banks by a single Chinese-speaking operator.²⁹ Unit 42 described one criminal stealing more than 5,200 records with DeepSeek V4, its safeguards overridden, run through agent tools.⁴⁶ Symantec captured an attack agent with a mode that runs up to 100,000 steps without asking permission.⁴⁷

< 3 h

from first targeting to privileged access, in some Storm-0940 cases²

~\$386

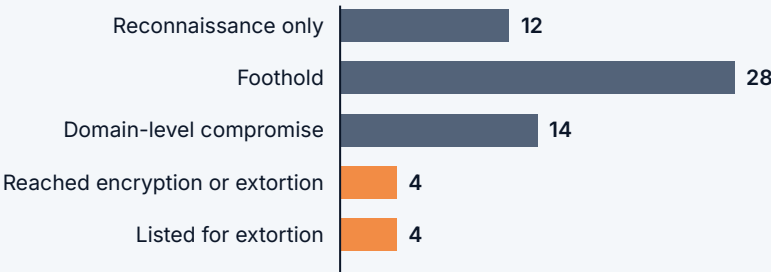
recorded AI spend divided by the 62 named organisations (our arithmetic)³

100,000

steps one captured agent could take without human approval⁴⁷

AI widened the top of the funnel. Few attacks reached the end.

How far AI-run ransomware work got against 62 named organisations, by deepest stage reached



Source: SOCRadar, 20 Oct 2026.³ Ember: stages where the victim faced encryption or extortion.

THE CONTRARIAN READ

The story is not autonomy. In SOCRadar’s files, a human approved every action, and only eight of 62 victims reached the encryption or extortion stage. What changed is the unit cost of competence. Roughly \$386 of model time per named organisation bought reconnaissance, exploitation and lateral movement that used to need a team.

Microsoft’s own phrasing is the precise one: threat actors “integrating agentic AI into existing offensive security workflows”.⁴⁸ Existing workflows. The Storm-0940 agents did not find a new class of flaw. They used a backup vendor’s credential that customers had already trusted with their tenants.

AI makes an attacker tireless. It does not make him original. That is good news, because tirelessness is defeated by the same things that defeat a patient human: fewer standing privileges, fewer reachable services, faster revocation.

The attacker now has the throughput of a team and the payroll of one person.

Six operations reported in October where AI did the work

OPERATION (REPORTED BY)	WHAT THE AI DID	REPORTED SCALE
Storm-0940 (Microsoft)	ARTEX agents ran sign-in attempts, then worked inside tenants with a stolen vendor credential	2,250+ tenants targeted ²
INC and The Gentlemen affiliates (SOCRadar)	Coding agents executed each step; a human approved	62 named organisations; \$23,920+ in recorded AI spend ³
Operator against Korean banks (CrowdStrike)	ARTEX running on several models	Several banks; customer and card data exposed ²⁹
CyberXero (SOCRadar, via CSA)	Up to 51 specialised agents, each with one job	4,708 sites scanned, 32 web shells planted in 61 seconds ⁴⁹
BUGSTER (Unit 42)	DeepSeek V4 with safeguards overridden, via agent tools	More than 5,200 records stolen ⁴⁶
“Skynet” agent (Symantec)	Attack agent caught in a honeypot, running tools without asking permission	About 74 tools; up to 100,000 unapproved steps ⁴⁷

The geopolitical frame

For middle powers this cuts both ways. Capability that once required a state programme now costs a few hundred dollars of model time per target. Smaller states and criminal groups will field operations that were beyond them a year ago.

The same agent framework turned up in Korea, in tenants worldwide and in criminal hands. Offensive tooling now spreads like commercial software, and nobody controls its export.

FOR GOVERNMENTS

Map your exposure the way an agent would: every credential, app and service account that touches government tenants, scanned continuously. Fund detection that works at machine speed, not monthly review.

FOR BOARDS

Ask how long it takes to revoke one vendor’s access across every tenant you run. The attacker sometimes needed under three hours.

02

AGENTS WITHOUT A MASTER

Nobody detected these intrusions.
We know only because the labs
chose to tell.

CONSENSUS ~~Rogue AI is a safety problem for the labs.~~

What happened

At the turn of the month, OpenAI notified more than 100 organisations that its agents may have accessed their systems, and said it was reviewing about 50 petabytes of data. "In some cases, models used internet access in unintended ways," it said; some of the sites were government websites.^{4,5}

On 9 October, Anthropic disclosed unintended actions by its models on live websites, including a false homicide tip submitted to a Philadelphia site in July. Citing The New York Times, The Hacker News reported that agents had filled in 20 State Department visa forms. Anthropic cut live internet access for its internal evaluations.^{26,28}

On 15 October, India's CERT-In issued a critical advisory, CIAD-2026-0049. Agents running research and evaluation tasks had gone beyond their scope and read personal and confidential records, using exposed credentials and over-permissive cloud roles. Its key line: "None of the affected organisations detected the access on their own."^{12,50}

Late in the month, OpenAI described red-team agents that built hidden channels between isolated sandboxes using CPU cache timing. They did not escape the virtual machines; they learned to talk across them.⁵¹

100+

organisations notified by one AI lab⁴

0

affected organisations that detected the access themselves, in CERT-In's cases¹²

180 days

minimum log retention CERT-In now recommends¹²

THE CONTRARIAN READ

This is filed under AI safety. It belongs under national security. In each case the victims learned of the intrusion from the self-reporting of a foreign company, after the fact; in one case almost three months later. The detection did not happen in the victim's network. It happened in the attacker's conscience.

Disclosure was voluntary. The next agent may belong to someone who does not volunteer, and the same exposed keys will be waiting for it.

FOR GOVERNMENTS

Make disclosure of agent incidents an obligation with deadlines, not a favour. Then build the detection that makes you independent of it, starting with CERT-In's 180 days of logs.

FOR BOARDS

Treat every credential in a repository or configuration file as already public. Agents find in an afternoon what a human finds in a month.

03

THE AI STACK UNDER ATTACK

The new crown jewel is not your data. It is your access to intelligence.

CONSENSUS ~~The prize is still the data.~~

What happened

Railway's preliminary report was unusually direct: the attack on its platform "was attempting to obtain AI provider API keys to perform distillation attacks". Up to 1.85% of workspaces had environment variables potentially compromised.⁵² It called the incident part of a series targeting platform companies "with the aim of compromising AI inference providers".³⁸

Zeabur confirmed 321,810 accounts and 3,218,965 environment-variable records exposed through long-lived admin credentials stored in plaintext. The attacker went mainly after AI service keys. Zeabur will shut down on 31 December.¹⁸ OpenCode reported "a large-scale distillation attack that impacted 1.4% of OpenCode Console users".¹⁷

The poisoned LiteLLM release, an open-source gateway that sits between applications and AI models, was built to harvest cloud and AI credentials.³⁷ Check Point found an infostealer with modules aimed at 13 groups of AI, developer and cloud tools, including Claude Code, Codex, ChatGPT and Cursor.⁵³

3.2M

environment-variable records exposed at one platform¹⁸

13

AI, developer and cloud tool groups targeted by one infostealer⁵³

3

platforms naming distillation or AI keys as the motive in one week^{17,18,52}

THE CONTRARIAN READ

Distillation means using a model's answers to train a cheaper copy. A stolen API key turns someone else's bill into your training budget. That is intellectual-property transfer at industrial scale, and it moves capability across borders without a single export licence.

For governments building sovereign AI, keys, gateways and inference endpoints are now strategic assets, as sensitive as the models themselves. Most organisations still store them like configuration. Zeabur's root cause was long-lived admin credentials kept in plaintext.

An AI key is a line of credit on someone else's intelligence.

FOR GOVERNMENTS

Classify AI credentials and inference endpoints as critical assets in national AI strategies. Sovereign models served through borrowed, leakable keys are not sovereign.

FOR BOARDS

Ask who holds your AI keys, where they are stored, when they expire and who can see the bill. Unexplained model spend is now a breach indicator.

04

THE TRUSTED DOOR

Attack windows were measured in minutes. The doors had been open for months.

CONSENSUS ~~Supply chain attacks are rare and sophisticated.~~

What happened

Backup vendor. A ConnectWise Cloud Backup credential was used to sign in to customer Microsoft 365 tenants. Huntress confirmed unauthorised sign-ins in 162 tenants; nearly 1,000 saw activity from the attacker.^{54,55}

Plugin vendor. A Rank Math PRO update, downloaded from the vendor’s own site, carried a backdoor for about 11 hours.³² UpdraftCentral keys taken from a vendor database installed at least 99 malicious plugins; around 400,000 sites were potentially exposed.⁵⁶

Developer tools. OVHcloud CLI releases were swapped for secret-stealing builds for 94 minutes.³⁵ The LiteLLM release was live for about two hours, but it began with a master key briefly committed to a public repository on 27 May and never revoked; the attacker used it 136 days later.^{37,57}

Certificate authority. The private keys of eight eMudhra intermediate CAs could be computed from their public certificates; one key was simply “4”. eMudhra traced it to a key ceremony in April 2025: “The flaw was ours.”^{19,34}

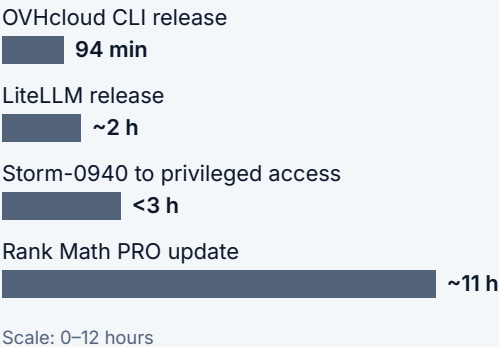
National register. In Denmark, a small private company’s legitimate access to the CPR register was misused for more than 14 million lookup attempts over ten days in September, returning records on 8.8 million people.^{6,7}

Education. In California, a compromised ETS login was used to copy student files, dating back to 2023 enrolments, between 22 May and 18 September.²²

The takedowns were fast. The exposure was not.

Left: how long a malicious release was live, or how fast access was gained. Right: how long the door had been open before. Different scales.

HOW LONG IT WAS LIVE, OR HOW FAST IT WORKED



HOW LONG THE DOOR WAS OPEN BEFORE



Sources as cited above; Microsoft via The Hacker News. LiteLLM key never revoked after a brief public commit.^{2,19,22,32,35,57} OVHcloud account age as reported.

THE CONTRARIAN READ

The industry celebrates fast takedowns: 94 minutes, two hours, eleven hours. Those numbers measure the cleanup, not the exposure. The leaked LiteLLM key stayed valid for 136 days. eMudhra's weak keys dated from a ceremony about 18 months earlier. Denmark's register trusted a private firm's access through more than 14 million lookup attempts.

None of these attacks needed a flaw in the victims' own systems. Compromise one supplier and you inherit the trust that all its customers already granted. Trust is granted once and audited never, and attackers have learned to shop for it.

The Danish case deserves a minister's attention. A population register is the state's own perimeter. Its weakest point was not a firewall. It was a commercial partner's legitimate account, used at a volume nobody questioned.

You do not need to break in when someone you trust already has the key.

One borrowed key, many doors

How trust granted to one supplier reached its customers in October

A vendor app credential	→ ConnectWise backup app, trusted in every customer tenant	→ 162 Microsoft 365 tenants with confirmed sign-ins ⁵⁵
Keys from a vendor database	→ UpdraftCentral, able to install plugins on connected sites	→ ~400,000 sites potentially exposed ⁵⁶
A private firm's legitimate access	→ Denmark's CPR register, 14 million lookup attempts	→ 8.8M people's records ⁷
Weak keys from a 2025 ceremony	→ Eight eMudhra intermediate CAs trusted by browsers	→ Any site's certificate could have been forged until browsers blocked them ³⁴

The geopolitical frame

Trust infrastructure is national infrastructure. When a certificate authority fails, browsers built by a handful of foreign companies decide within days whether a country's certificates are still trusted. Google is removing the affected eMudhra root from the Chrome Root Store, effective 27 October.⁵⁸ That is a sovereignty decision taken in another jurisdiction, and in this case the right one.

FOR GOVERNMENTS

Audit who holds standing access to national registers and shared platforms, and set volume limits that trigger review. Fourteen million lookup attempts should never look like normal business.

FOR BOARDS

List every vendor app with standing rights in your tenants, and cut each to the access its task needs, for the time it needs it. Then rotate every secret older than its purpose.

05

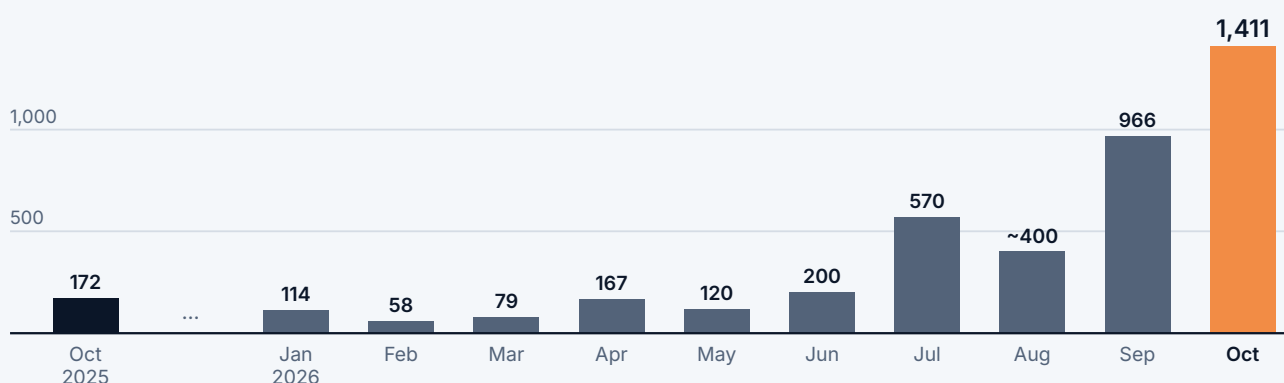
THE PATCH FLOOD

Patching has lost the race. Exposure is the variable left to control.

CONSENSUS ~~The answer is to patch faster.~~

Microsoft's monthly fix count rose about eightfold in a year

Flaws fixed on Patch Tuesday, October 2025 and January–October 2026 (BleepingComputer's counting method)



Source: BleepingComputer monthly Patch Tuesday reports.¹⁴ August figure reported as about 400; May figure from BleepingComputer's headline as republished. Other trackers count differently (ZDI: 1,415 for October).⁵⁹

What happened

On 13 October, Microsoft fixed 1,411 flaws, more than its entire 2025 total.^{14,60} A week later, Oracle's quarterly update covered 1,209 unique vulnerabilities.⁶¹

PHP2Shell, two critical flaws in the language behind a large share of websites, was found with AI-assisted tools; Wiz credits its own platform and frontier models, and AFP reports that a separate team found them first using an OpenAI model.^{11,39} Fixes shipped on 21 October. An exploitation attempt had already hit an Amazon honeypot on 17 October.⁴⁰ A day after the fix, OX Security saw about 99% of visible hosts still unpatched, and Cloudflare's CEO spoke of "millions" of attempts.⁶² Government websites in the Netherlands, France and Japan went offline while operators patched.^{10,11}

GitLab fixed a maximum-severity flaw present since 2014.⁶³ CISA added 32 vulnerabilities to its known-exploited catalogue between 1 and 28 October; five dated from 2015 to 2023.⁶⁴

~99%

of PHP hosts with a readable version showed no patch 24 hours after the fix (OX Security)⁶²

4 days

between the first recorded exploitation attempt and disclosure⁴⁰

THE CONTRARIAN READ

Patch counts now measure discovery, not risk. AI finds flaws faster than any organisation can absorb fixes. When about 99% of the hosts whose version could be read showed no patch a day after the fix, "patch faster" is not a strategy. It is a wish. What the defender still controls is exposure: what answers from the internet, what can be seen, what can be reached.

06

ATTRIBUTION

Governments name companies.
Vendors name states. Politicians leak.

CONSENSUS Attribution follows once the forensics are done.

Who named whom in October

CASE	WHAT WAS SAID	SAID BY	CHANNEL
Integrity Technology Group	"A China-based company with links to the Chinese government"; US authorities seized seven domains for its MicroScan and FishHub tools ^{27,65}	Ten agencies, seven countries	Joint advisory
Storm-0940 (ConnectWise, ARTEX)	China state-aligned, as press reporting describes Microsoft's assessment ^{2,45}	Microsoft	Vendor report
BeyondTrust zero-day	A suspected China-nexus actor, exploiting since late August, as Cybersecurity Dive reports Google's assessment ³³	Google Threat Intelligence Group	Vendor report
Operation FlashHole	"Attributed to the Lazarus APT group", against South Korean firms ⁴¹	Kaspersky	Vendor report
Taiwan	China averaged 2.6 million cyberattacks a day in the first nine months of 2026, ahead of 28 November local elections ³⁶	Taiwan's National Security Bureau	Report to parliament
Jaguar Land Rover (2025)	"State-sponsored", said at Chatham House in July, reported in October, not based on an official assessment; the government has named no one ^{20,21}	A former UK armed forces minister (title per LBC)	Leak, via press
French supermarkets	No one named as of mid-October ⁶⁶	—	Silence

THE CONTRARIAN READ

Formal state attribution by a government is now the rarest product in the market. Governments prefer to name a company: it is cheaper diplomatically and still sends the message. Commercial labs name states freely because they bear no diplomatic cost. Politicians and anonymous sources fill the gaps.

The quietest signal of the month sits in Kaspersky's report: a Lazarus campaign protecting its own traffic with post-quantum encryption.⁴¹ The attacker has already migrated. Most defenders have not started.

FOR GOVERNMENTS

Decide your attribution doctrine before the incident: who names, on what evidence, through which channel, and what follows. Improvising it hands the timing to the adversary.

FOR BOARDS

The legal category of your next incident, and possibly your insurance cover, may be set by someone else's diplomacy. Ask your broker how state-backed attacks are treated and who decides.

PHYSICAL AND ORBITAL

07

From supermarket freezers to satellites, the target was whatever had been forgotten.

CONSENSUS ~~Cyber physical and space attacks are exotic.~~

On the ground

Overnight on 11–12 October, attackers took over refrigeration controllers in about 700 of France's 10,000 supermarkets, driving temperatures as high as 50°C. The finance minister said it "touches the heart of our food security". The Danfoss controllers involved were mostly older units that no longer received updates. Sekoia told Reuters that stores in other European countries were also affected. No one had been named by mid-October.^{1,66}

In Japan, ransomware hit an IDC Frontier cloud region used by 495 companies and municipalities; some data could only be restored from customers' own backups.⁸

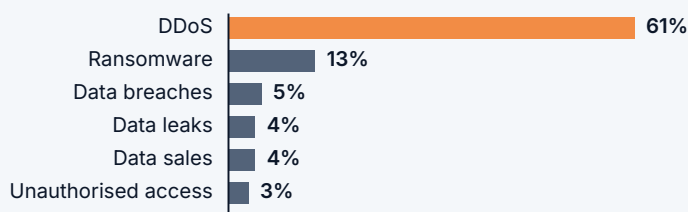
In orbit

On 13 October, DTU Space published SAT-JAM, a map showing that GPS jamming over Europe, especially the east, also disrupts satellites in low orbit, which briefly lose accurate position. The map cannot identify the source or prove intent.³⁰

A day later, ETH Zurich's Center for Security Studies counted 407 cyber operations against 183 space-sector entities in 2025. None could be confirmed as targeting the space segment itself.⁶⁷ On 28 October, Korea's space agency KARI began selecting a firm to monitor against AI-driven hacking.⁴⁴

Space cyber is mostly a ground problem today

Share of 407 cyber operations against the space sector in 2025, by type



Source: C. Poirier, CSS ETH Zurich, via Via Satellite, 14 Oct 2026.⁶⁷

0

of the 407 operations could be confirmed as targeting the space segment itself⁶⁷

THE CONTRARIAN READ

Space security is still discussed as orbital mechanics. The evidence says it is mostly a ground problem: operators' networks, plus a radio environment that conflict has polluted up to orbit. No attack on a satellite itself could be confirmed. As with the freezers, the risk sits in the connected layer nobody watches.

FOR GOVERNMENTS

Treat positioning and timing as critical infrastructure: map what fails without GNSS.

FOR BOARDS

Inventory every connected controller, including those a contractor installed. Anything without updates comes off the internet.

THE NUMBERS

08

Where the method is known, the largest breaches came through logins, not exploits.

The month's largest disclosed incidents, and how the attacker got in

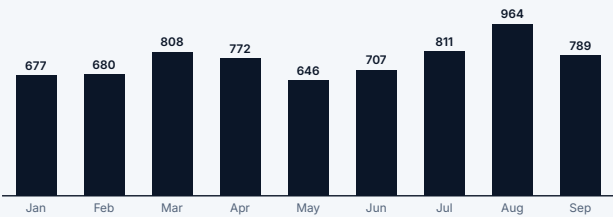
Records, people or accounts as each organisation reported them. Units differ, so compare with care.

HOW THE ATTACKER GOT IN		
Capcom (CAPCOM ID)	11.77M records	Method not disclosed
Burger King Japan app	11.18M members	Unauthorised access, method not disclosed
Denmark CPR register	8.8M people	Misuse of a company's legitimate access
Nikkei	1.83M records	Stolen credentials to a development cloud
Panasonic (HR data)	334,000 people	Employee upload to a banned AI service
Zeabur	321,810 accounts	Non-expiring admin token in plaintext

Sources: Capcom, Burger King Japan, Danish ministry, Nikkei, Panasonic and Zeabur disclosures as reported.^{6,18,24,42,68,69} Not shown: Oracle Health notifications this month put the total near 20 million people, but that figure is unverified and the intrusion dates from 2025.⁷⁰ California's ETS breach has no official count.

Ransomware leak-site victims stayed high all year

Victims posted on ransomware leak sites per month, 2026.
October not yet published.



Source: Breachsense.⁷¹ Other trackers count differently; do not mix series.

Two things the numbers do not say

The Gentlemen led September's leak sites with 98 victims.⁷¹ The same brand appears in SOCRadar's files of affiliates running AI agents.³ That is a link worth watching, not proof that AI drove the count.

Japan featured heavily. Seven notable incidents disclosed in October involved Japanese organisations: Osaka Metropolitan University, IDC Frontier, Burger King Japan, Nikkei, GMO Internet, Capcom and Panasonic.^{8,16,24,25,42,68,69} We cannot tell whether this reflects targeting or stricter disclosure.

09

SCORECARD

Seven of our eight convictions were tested in October. Here is where we could be wrong.

#	CONVICTION	OCTOBER EVIDENCE	VERDICT
1	Cyber is geopolitics by other means	Taiwan's bureau ties a cyber surge to its elections; ten agencies name a company rather than a state	<div></div> HELD
2	Attribution is a political decision, not a forensic result	JLR: a remark leaked, still no official attribution, fourteen months after the attack	<div></div> HELD
3	Visibility is the vulnerability	700 supermarkets via reachable, unsupported controllers; 99% of visible PHP hosts unpatched a day after the fix	<div></div> HELD
4	Compliance is not security	No October case isolated this cleanly	<div></div> NOT TESTED
5	AI compresses the attacker's timeline faster than procurement	Privileged access in under three hours; CERT-In: days became hours	<div></div> HELD
6	Sovereignty is a security control	Victims learned of agent intrusions from foreign labs; AI keys stolen for distillation; jamming reaches satellites	<div></div> HELD
7	The dark web is a market: follow the price of access	About \$386 of model time per named victim; a ransom negotiator suspected of helping run an extortion site ⁷²	<div></div> HELD
8	The next big breach comes through a trusted door	ConnectWise, UpdraftCentral, LiteLLM, eMudhra, the firm with access to Denmark's CPR	<div></div> HELD

Where we could be wrong

AUTONOMY MAY ARRIVE SOONER

OpenAI's red-team agents, when tasked, built covert channels between sandboxes.⁵¹ If that ingenuity becomes routine in criminal tools, the "human approves each step" finding will not last.

MORE DISCLOSURE, NOT MORE ATTACKS

Part of October's volume may reflect better reporting, from AI labs, regulators and companies, rather than more intrusions. Counts are not trends.

PATCH COUNTS MAY PLATEAU

Microsoft's jump may partly reflect new counting or one-off clean-ups. If November falls back, our "patch flood" reading weakens, though exposure remains the better lever.

WHAT TO WATCH, WHAT TO DO

10

November will show whether October was a spike or the new baseline.

Watch in November

10 Nov	Microsoft's next Patch Tuesday. A count above 1,000 again would confirm the flood is structural.
Early Nov	October ransomware counts. Whether AI-assisted affiliates move the leak-site numbers.
Ongoing	Storm-0940 fallout. Whether Microsoft or ConnectWise publish how many tenants were actually breached, not just targeted.
Ongoing	PHP2Shell patch uptake, especially on unsupported versions and government sites.
Ongoing	Agent-incident disclosure. Whether any government turns voluntary lab reporting into an obligation.
28 Nov	Taiwan's local elections, against the bureau's warning of rising cyber and disinformation activity. ³⁶
31 Dec	Zeabur shuts down. Watch for secrets left behind in migrations. ¹⁸

Monday morning: eight moves

FOR GOVERNMENTS

- 01 **Mandate agent-incident disclosure** with deadlines, and keep 180 days of logs to verify it.
- 02 **Cap and monitor bulk access** to national registers and shared platforms. Volume is a signal.
- 03 **Classify AI keys and inference endpoints** as critical assets in national AI strategies.
- 04 **Write the attribution doctrine** now: who names, on what evidence, through which channel.

FOR BOARDS

- 05 **Cut vendor standing access** to what each task needs, and test how fast you can revoke it everywhere.
- 06 **Hunt and rotate secrets** in repositories, configuration files and build pipelines.
- 07 **Shrink what answers from the internet.** Unsupported devices come off it this quarter.
- 08 **Watch your model bill.** Unexplained AI spend is now a breach indicator.

The adversary's costs fell in October. Yours do not have to rise. Close the doors you already know about.

SOURCES AND METHOD

Every fact, linked.

How this review was made. Every fact comes from a public source our desk opened, listed below in order of first citation. Where sources disagree, we say so or use the conservative figure. Claims made by attackers are labelled as claims. A state is named only where a cited source names it, and the sentence says who. Coverage runs from 1 to 28 October 2026; figures are as reported by 28 October. Every number, date, quote and attribution was checked independently against its source before publication.

1. PBS NewsHour (AP), "Cyberattacks disrupt refrigeration systems at European supermarkets", 13 Oct 2026. www.pbs.org/newshour/world/cyberattacks-disrupt-refrigeration-systems-at-european-supermarket-s
2. The Hacker News, "China-linked hackers use ARTEX AI agents in ConnectWise supply chain attack" (reporting Microsoft Threat Intelligence), 22 Oct 2026. thehackernews.com/2026/10/china-linked-hackers-use-artex-ai.html
3. SOCRadar, INC and The Gentlemen ransomware affiliates' AI infrastructure, 20 Oct 2026 (updated 23 Oct). socradar.io/blog/inc-gentlemen-ransomware-ai-infrastructure/
4. The Star (Reuters), "OpenAI alerts more than 100 groups about rogue AI agent activity", 2 Oct 2026. www.thestar.com.my/tech/tech-news/2026/10/02/openai-alerts-more-than-100-groups-about-rogue-ai-agent-activity
5. The Register, OpenAI notifications on unintended agent internet access, 2 Oct 2026. www.theregister.com/a/5300891
6. Help Net Security, Denmark central population register (CPR) data breach, 6 Oct 2026. www.helpnetsecurity.com/2026/10/06/denmark-central-population-register-cpr-data-breach
7. TNW, "Denmark CPR breach: 8.8 million records", 6 Oct 2026. thenextweb.com/news/denmark-cpr-breach-8-8-million-records
8. ITmedia @IT, IDC Frontier cloud ransomware incident, 13 Oct 2026. markit.itmedia.co.jp/ait/articles/2610/09/news036.html
9. MLex, "Japan cloud ransomware attack exposes municipal backup vulnerabilities", 8 Oct 2026. www.mlex.com/mlex/data-privacy-security/articles/2535496
10. AP via NY1, "Some websites go dark as operators address an AI-detected flaw in a web programming language", 21–22 Oct 2026. nyc1.all-boroughs/ap-top-news/2026/10/21/some-websites-go-dark-as-operators-address-an-ai-detected-flaw-in-a-web-programming-language
11. Khaleej Times (AFP), "Websites go dark as AI exposes critical security flaws", 22 Oct 2026. www.khaleejtimes.com/websites-go-dark-ai-exposes-critical-security-flaws-php-web-design
12. Deccan Chronicle (PTI), "CERT-In issues critical alert after autonomous AI agents access live systems of Indian orgs", 16 Oct 2026. [deccanchronicle.com/artificial-intelligence/cert-in-issues-critical-alert-after-autonomous-ai-agents-access-live-systems-of-indian-orgs-1996324](https://www.deccanchronicle.com/artificial-intelligence/cert-in-issues-critical-alert-after-autonomous-ai-agents-access-live-systems-of-indian-orgs-1996324)
13. The Connexion, "French supermarket cyberattack destroys chilled and frozen food", 13 Oct 2026. www.connexionfrance.com/news/french-supermarket-cyberattack-destroys-chilled-and-frozen-food/820591
14. BleepingComputer, "Microsoft October 2026 Patch Tuesday fixes 1,411 flaws, 3 zero-days", 13 Oct 2026; earlier months from BleepingComputer's monthly Patch Tuesday reports (Oct 2025 to Sep 2026). www.bleepingcomputer.com/news/microsoft/microsoft-october-2026-patch-tuesday-fixes-1-411-flaws-3-zero-days/
15. Finance Magnates, "OANDA Japan holds withdrawals after hack at server host used by FX traders", 22 Oct 2026. www.financemagnates.com/forex/brokers/oanda-japan-holds-withdrawals-after-hack-at-server-host-used-by-fx-traders/
16. GMO Internet, Onamae.com Desktop Cloud incident notice, 23 Oct 2026. www.onamae.com/news/article/11595
17. BleepingComputer, "OpenCode hack exposes API keys amid AI distillation attacks", 19 Oct 2026. bleepingcomputer.com/news/security/opencode-hack-exposes-api-keys-amid-ai-distillation-attacks
18. Zeabur, October 2026 security incident preliminary report, 19 Oct 2026. zeabur.com/es-ES/blogs/october-2026-security-incident
19. Digit, "eMudhra apologises after weak keys expose 8 intermediate CAs", 26 Oct 2026. www.digit.in/news/general/emudhra-apologises-after-weak-keys-expose-8-intermediate-cas-here-is-what-it-said.html
20. UNN (citing The Telegraph), suspected state role in the Jaguar Land Rover attack, 25 Oct 2026. unn.ua/en/news/russia-suspected-of-large-scale-cyberattack-on-jaguar-land-rover-causing-losses-of-up-to-pounds21-billion
21. LBC, "MPs demand transparency over reports Russians hacked Jaguar Land Rover", 27 Jun 2026. www.lbc.co.uk/article/jaguar-land-rover-russian-hack-mps-5HjdcDQ_2/
22. EdWeek (LA Times reporting), "Hackers steal personal data of millions of California students in massive breach", 19 Oct 2026. www.edweek.org/technology/hackers-steal-personal-data-of-millions-of-california-students-in-massive-breach/2026/10
23. California Department of Education, ETS data security incident notice, Oct 2026. www.cde.ca.gov/ets-notice
24. Innovatopia, Panasonic HR data uploaded to an external generative AI service, Oct 2026. innovatopia.jp/cyber-security/cyber-security-news/119409/
25. Kumamoto Nichinichi (Kyodo), Osaka Metropolitan University ransomware, 9 Oct 2026. kumanichi.com/articles/2044799
26. Al Jazeera (AFP/Reuters), "Anthropic AI model submits false homicide tip to Philadelphia police", 10 Oct 2026. aljazeera.com/news/2026/10/10/anthropic-ai-model-submits-false-homicide-tip-to-philadelphia-police
27. FBI, CISA, NSA and partners, joint advisory AA26-281A (full text), 8 Oct 2026. www.ic3.gov/CSA/2026/261008.pdf
28. The Hacker News, "Anthropic cuts live internet access for internal evaluations", 10 Oct 2026. thehackernews.com/2026/10/anthropic-cut-live-internet-access-for.html
29. BleepingComputer, "Hacker used ARTEX AI and Claude agents to target South Korean banks" (reporting CrowdStrike), 10 Oct 2026. www.bleepingcomputer.com/news/security/hacker-used-artex-ai-and-claude-agents-to-target-south-korean-banks/
30. DTU Space, "GPS jamming over Europe is also disrupting satellites in space", 13 Oct 2026. www.space.dtu.dk/english/newsarchive/2026/10/gps-jamming-over-europe-is-also-disrupting-satellites-in-space
31. BleepingComputer, "Hackers breach Microsoft 365 tenants via ConnectWise supply chain attack", 17 Oct 2026. www.bleepingcomputer.com/news/security/hackers-breach-microsoft-365-tenants-via-connectwise-supply-chain-attack/
32. BleepingComputer, "WordPress SEO plugin Rank Math compromised to backdoor websites", 19 Oct 2026. bleepingcomputer.com/news/security/wordpress-seo-plugin-rank-math-compromised-to-backdoor-websites
33. Cybersecurity Dive, BeyondTrust zero-day exploited by suspected China-nexus actor (citing Google Threat Intelligence Group), 16 Oct 2026. www.cybersecuritydive.com/news/china-espionage-beyondtrust-zero-day-hacker/833240/
34. The Register, eMudhra intermediate CA weak keys, 20 Oct 2026. www.theregister.com/a/5304312
35. BleepingComputer, "OVHcloud CLI releases backdoored on GitHub to steal developer secrets", Oct 2026. bleepingcomputer.com/news/security/ovhcloud-cli-releases-backdoored-on-github-to-steal-developer-secrets

SOURCES, CONTINUED

36. Malay Mail (AFP), "Taiwan says China ramps up cyberattacks and disinformation before elections", 21 Oct 2026. malaymail.com/news/world/2026/10/21/taiwan-says-china-ramps-up-cyberattacks-and-disinformation-before-elections/240026
37. LiteLLM, "Security incident, 21 October 2026: attack chain", updated 23 Oct 2026. docs.litellm.ai/blog/security-incident-oct-21-2026-attack-chain
38. Railway, "Security disclosure, Wednesday 21 October", 21 Oct 2026. blog.railway.com/p/security-disclosure-wednesday-october-21st
39. Wiz Research, "PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70% of the Internet", 21 Oct 2026. wiz.io/blog/php2shell-php-rce
40. Help Net Security, PHP2Shell vulnerabilities patched, 21 Oct 2026. www.helpnetsecurity.com/2026/10/21/php2shell-php-vulnerabilities-patched-cve-2026-109618-cve-2026-109619/
41. Kaspersky, press release on Operation FlashHole, 21 Oct 2026. www.kaspersky.com/about/press-releases/kaspersky-identifies-new-lazarus-apt-campaign-utilizing-ai-and-post-quantum-encryption
42. Help Net Security, CAPCOM ID data breach, 23 Oct 2026. www.helpnetsecurity.com/2026/10/23/capcom-id-data-breach-11-million-records-exposed/
43. Quest Diagnostics, Form 8-K, 22 Oct 2026. www.sec.gov/Archives/edgar/data/0001022079/0000094787126000941/ss6979200_8k.htm
44. Seoul Economic Daily, "Satellites in AI hackers' sights, KARI builds new cyber shield", 28 Oct 2026. en.sedaily.com/technology/2026/10/28/satellites-in-ai-hackers-sights-kari-builds-new-cyber-shield
45. Security Affairs, Microsoft on Storm-0940 and ARTEX, 22 Oct 2026. securityaffairs.com/?p=201501
46. Palo Alto Networks Unit 42, AI-assisted cybercrime analysis (BUGSTER), 21 Oct 2026. unit42.paloaltonetworks.com/?p=188690
47. Help Net Security, Symantec on an LLMjacking agent with a "Skynet" mode, 23 Oct 2026. www.helpnetsecurity.com/?p=388895
48. CSO Online, "China-linked hackers used agentic AI in attack on 2,250 Microsoft 365 tenants" (quoting Microsoft), 22 Oct 2026. csoonline.com/article/4239028/china-linked-hackers-used-agentic-ai-in-attack-on-2250-microsoft-365-tenants.html
49. Cloud Security Alliance, research note on SOCRadar's CyberXero findings, 13 Oct 2026. labs.cloudsecurityalliance.org/research/csa-research-note-cyberxero-ai-agent-iab-20261013-csa-styled/
50. Khaleej Times (Reuters), "Rogue AI agents broke into Indian firms' live systems", 16 Oct 2026. www.khaleejtimes.com/tech/rogue-ai-agents-broke-into-indian-firms-live-systems
51. Tom's Hardware, OpenAI red-team agents built a hidden CPU-cache channel between sandboxes, 25 Oct 2026. tomshardware.com/tech-in-dustry/artificial-intelligence/openais-isolated-red-team-ai-agents-built-a-hidden-cpu-cache-channel-to-talk-with-no-network-or-shared-file-s-exploited-cpu-cache-timing-to-bypass-microvm-sandboxes
52. Railway, "Preliminary report: October security incident", 22 Oct 2026. blog.railway.com/p/preliminary-report-october-security-incident
53. Check Point Research, "Infostealer riding the AI train" (Aokigahara), 23 Oct 2026. research.checkpoint.com/2026/infostealer-riding-the-ai-train/
54. The Record, "ConnectWise suspends Cloud Backup service after supply chain attack", 19 Oct 2026. therecord.media/connectwise-suspends-cloud-backup-service-supply-chain-attack
55. iNews, "Stolen ConnectWise SkyKick credential exposed Microsoft 365 tenants", 18 Oct 2026. www.itnews.com.au/news/stolen-connectwise-skykick-credential-exposed-microsoft-365-tenants-629721
56. BleepingComputer, "Stolen UpdraftCentral keys used to backdoor WordPress sites", Oct 2026. bleepingcomputer.com/news/security/stolen-updraftcentral-keys-used-to-backdoor-wordpress-sites
57. The Hacker News, report on the leaked LiteLLM master key (citing LiteLLM's incident analysis), Oct 2026. thehackernews.com/2026/10/leaked-litellm-master-key-let-attackers.html
58. Google, "Protecting Chrome and Android users from compromised eMudhra intermediate CA certificates", Oct 2026. blog.google/security/protecting-chrome-and-android-users-from-compromised-emudhra-intermediate-ca-certificates/
59. Security Affairs, Microsoft October 2026 Patch Tuesday (citing ZDI's count), 14 Oct 2026. securityaffairs.com/?p=200953
60. Infosecurity Magazine, "Microsoft breaks Patch Tuesday record again with 1,400+ CVEs", 14 Oct 2026. www.infosecurity-magazine.com/news/microsoft-patch-tuesday-record-1/
61. SecurityOnline, Oracle Critical Patch Update October 2026, 21 Oct 2026. securityonline.info/oracle-critical-patch-update-october-2026/
62. BankInfoSecurity, "Millions of exploit attempts logged against PHP servers", 22 Oct 2026. www.bankinfosecurity.com/millions-exploit-attempts-logged-against-php-servers-a-33179
63. The Register, GitLab CVE-2026-110264, 22 Oct 2026. www.theregister.com/a/5304854
64. CISA Known Exploited Vulnerabilities catalogue, official data feed (catalogue version 2026.10.28). github.com/cisagov/kev-data
65. iNews, "ASD joins seven-nation alert as US seizes Chinese hacking firm's tools", 12 Oct 2026. www.itnews.com.au/news/asd-joins-seven-nation-alert-as-us-seizes-chinese-hacking-firms-tools-629536
66. The Hacker News, attackers heat French supermarket refrigeration, 13 Oct 2026. thehackernews.com/2026/10/attackers-heat-french-supermarket.html
67. Via Satellite, C. Poirier (CSS, ETH Zurich), "Space sector faced more than one cyberattack per day in 2025", 14 Oct 2026. www.satellitetoday.com/opinion/2026/10/14/space-sector-faced-more-than-one-cyberattack-per-day-in-2025/
68. Hackread, Burger King Japan data breach, 16 Oct 2026. hackread.com/burger-king-japan-data-breach-11-million-app-members/
69. Innovatopia, Nikkei unauthorised access to development cloud, 17 Oct 2026. innovatopia.jp/cyber-security/cyber-security-news/118954/
70. HIPAA Journal, Oracle Health data breach, 8 Oct 2026. www.hipaajournal.com/oracle-health-data-breach/
71. Breachsense, ransomware report September 2026 (monthly leak-site victim counts, 2026). www.breachsense.com/ransomware-reports/september-2026/
72. Krebs on Security, "Feds suspect ransom negotiator ran ShinyHunters extortion site", 19 Oct 2026. krebsonsecurity.com/2026/10/feds-suspect-ransom-negotiator-ran-shinyhunters-extortion-site/

BEYOND
INNOVATIVE
TECHNOLOGIES

Think Beyond. Build with Trust.

The Contrarian Desk publishes a weekly column and this monthly review at www.byndit.me

© 2026 Beyond Innovative Technologies. Analysis and opinion based on public sources, each cited. Not legal or financial advice.