



FENESTRA TI

GLOBAL INTELLIGENCE. **CONNECTED INSIGHT.**

THREAT LANDSCAPE

September 2026

Geospatial and cyber threats — ransomware, the criminal underground, our own sensor data and two spotlights: Russian sabotage in Europe and the ShinyHunters extortion group.

CONTENTS

1	EXECUTIVE SUMMARY	The Front Line Is Privately Owned	<u>3</u>
2	GEOSPATIAL & PHYSICAL SECURITY	Terrorism And Conflict Up, Protest Down	<u>5</u>
3	MARITIME & AVIATION SECURITY	Two Chokepoints Under Fire	<u>7</u>
4	RANSOMWARE	The Leaderboard Flattened	<u>9</u>
5	INTERNET SIGNALS	A Baseline From Our Own Sensors	<u>11</u>
6	CYBER UNDERGROUND	AI Moves From Novelty To Commodity	<u>13</u>
7a	PHYSICAL SPOTLIGHT	Russian Hybrid Sabotage In Europe	<u>14</u>
7b	CYBER SPOTLIGHT	ShinyHunters	<u>16</u>
	SOURCES	Numbered references	<u>18</u>

EXECUTIVE SUMMARY

THE FRONT LINE IS PRIVATELY OWNED

On the 25th anniversary of the 9/11 attacks, the Director General of MI5 observed that "many of the assets, systems and services under threat sit in private sector hands. This means many of the most critical decisions will be taken not in COBR but in boardrooms."¹ September's reporting bore that out. Across the geospatial, aviation, maritime and cyber domains, the month's most significant attacks and near-misses landed on privately owned infrastructure. Often, the owners were the first to act.

In the Gulf, energy operators under drone attack are hardening their own facilities; in the UAE this includes steel "coke cages" around fuel tanks.² Qatar and the UAE said publicly that the region cannot rely on the United States alone for its security.³ In Europe, the targets of Russian-directed sabotage were defence manufacturers, a satellite ground station and cargo operations supplying Ukraine, most of them in private hands. Online, a criminal group compromised a law-enforcement jobs portal and hijacked a ransomware gang's leak site in the same week.

Key findings

- **Terrorism and conflict gained ground.** Terrorism rose from 8.5% to 11.7% of geolocated security events and armed conflict from 19.9% to 22.4%, driven by the Houthi campaign against Saudi Arabia and Israeli strikes in Lebanon. Protest activity fell back after a heavy August. (Section 2)
- **The Red Sea front moved ashore.** The Houthis seized Mocha and islands controlling the Bab-el-Mandeb in mid-September, and struck Saudi refining, pipeline and airport targets. Tanker attacks around Hormuz continued all month.^{4,5,6} (Section 3)
- **Russian sabotage in Europe is now openly attributed.** Germany and Estonia formally blamed Russia for the Leipzig drone-bomb attempt and the Milrem Robotics arson. Arson, drone incursions and proxy recruitment followed across at least seven countries, and a UK case reached the courts. (Spotlight)
- **Ransomware became less concentrated, but not less dangerous.** The top three groups' share of victims fell from about a third to just under a quarter. The clearest route in was a network-edge vulnerability: Cisco firewall-management flaws led to Qilin ransomware deployments. (Section 4)
- **ShinyHunters escalated even after an arrest.** A suspected leader was detained on 15 September. The group then defaced the FBI's jobs portal, claimed agents' personal data, extorted the CI0p gang and resumed mass exploitation of Oracle PeopleSoft. (Spotlight)
- **AI access is now an underground commodity.** AI-related content roughly doubled its share of underground forum discussion, and stolen AI and cloud API keys were openly advertised for sale. Fenestra's sensors recorded probing for AI-agent configuration files. (Sections 5 and 6)
- **Exposed industrial systems are found in days.** A Fenestra ICS honeypot was probed by more than 150 distinct addresses in its first week. The most probed protocol is used in electricity-grid control. (Section 5)

Key judgements

- It is **highly likely** that Russian-directed sabotage against European companies supporting Ukraine continues through the winter, and a UK incident is a **realistic possibility**.
- It is **likely** that terrorism's share of security events stays elevated in October while the Houthi–Saudi and Israel–Lebanon fronts remain active.
- It is **likely** that edge-device and business-application vulnerabilities remain the main route into organisations for ransomware and extortion groups. Workarounds that are never patched are **highly likely** to be revisited.
- It is **likely** that ShinyHunters' capability has not been reduced by the September arrest.

What this means for boards. The common thread is that exposure is decided and managed by the organisations that own it. That means patching edge systems rather than relying on workarounds, treating links to Ukraine-bound supply chains as a higher risk factor, training staff to recognise online recruitment approaches, and protecting AI and cloud credentials as seriously as any other production secret.

Probability language. Judgements use the UK Professional Head of Intelligence Assessment yardstick: remote chance ($\leq 5\%$) · highly unlikely (10–20%) · unlikely (25–35%) · realistic possibility (40–50%) · likely or probably (55–75%) · highly likely (80–90%) · almost certain ($\geq 95\%$). Figures cover 1–30 September unless stated; month-on-month comparisons use shares of each month's total.

GEOSPATIAL & PHYSICAL SECURITY

TERRORISM AND CONFLICT UP, PROTEST DOWN

CATEGORY	AUGUST	SEPTEMBER	CHANGE
Terrorism	8.5%	11.7%	+3.1pp
Crime	16.2%	15.2%	-1.1pp
Activism & unrest	36.4%	32.0%	-4.4pp
Violence	18.9%	18.8%	-0.2pp
Conflict	19.9%	22.4%	+2.5pp

Share of geolocated security events, each incident counted once however widely reported. Changes are calculated before rounding.

Terrorism and armed conflict gained ground and protest fell back. Terrorism rose from 8.5% to 11.7% of geolocated security events and armed conflict from 19.9% to 22.4%. Activism and unrest, still the largest category at almost a third of events, fell by more than four points. Crime and violence held steady.⁷

The Middle East drove the rise. The Houthi campaign against Saudi Arabia struck the Jazan refinery, the East-West pipeline and Riyadh's airport,^{6,8,9} and Saudi Arabia's share of terrorism events doubled. Israeli strikes on southern Lebanon continued despite the ceasefire,¹⁰ which lifted Lebanon's share of both terrorism and conflict events. Yemen also rose in conflict reporting. Ukraine and Russia remained the most reported conflict after the United States, but their share fell as the Middle Eastern theatre widened.⁷

Nigeria rose in terrorism and crime reporting. Nigeria's defence authorities reported more than a thousand militants killed and hundreds of kidnap victims rescued over two months. Reports of a secret three-month ceasefire with Boko Haram followed, and the army reshuffled command of the campaign.^{11,12}

Protest paused after a heavy August. The fall in activism came mainly from the United States and India, where August's wave of redistricting disputes and student and exam protests was not repeated.⁷ Europe bucked the trend. France rose as its 2027 presidential campaign got under way and industrial action closed the Eiffel Tower.⁷

Latin America. Brazil and Mexico featured prominently in crime, violence and conflict reporting in September. In the crime category alone, Brazil accounted for about one event in seven and Mexico for about one in twelve.⁷

The West Bank became a diplomatic flashpoint. The UK, France and Canada sanctioned Israeli settlements, and Britain accused settlers of "ethnic cleansing".¹³ Event-coded media data recorded twice as many "mass violence" references as in August, concentrated on Israel, the West Bank and UK reporting of

the sanctions.⁷ In the UK, the Chief Rabbi warned that the sanctions could leave British Jews less safe, a claim the minister rejected.¹⁴

United Kingdom. The UK's share of terrorism events edged up. The main driver was the counter-terrorism operation near RAF Fairford at the end of the month, in which men arrested near the base were later released on police bail.¹⁵ The US and UK gave conflicting public accounts of the threat.¹⁶ Counter-terrorism police said that no improvised explosive devices were found, although petrol was recovered from the vehicles.¹⁷ On 30 September Prime Minister Andy Burnham said the government believed Iran "played a part"; Iran rejected the claim. No one has been charged and the investigation continues.¹⁸ Russian-directed sabotage against UK defence-industrial targets is covered in the physical spotlight.

FENESTRA ASSESSMENT: Terrorism's share of events is **likely** to stay elevated in October. The Houthi-Saudi and Israel-Lebanon fronts show no sign of de-escalation, and Gulf energy and aviation infrastructure remain in range (see Maritime & aviation). **ASSESSMENT ENDS**

FENESTRA ASSESSMENT: The drop in protest activity is **likely** to be temporary. The US mid-term elections on 3 November and France's presidential campaign make a return to higher levels of political protest and unrest in October and November a **realistic possibility**, especially in the United States.

ASSESSMENT ENDS

MARITIME & AVIATION SECURITY

TWO CHOKEPOINTS UNDER FIRE

Strait of Hormuz: attacks became routine. Commercial shipping in and around the Strait was attacked throughout September as the US–Iran conflict flared again. A Bahri VLCC attack killed two crew (31 Aug), as Iran extended its "non-compliant" vessel list to 56 ships.¹⁹ Other incidents included:

- the tanker *Hercules Star*, hit at anchor off Dubai (one dead, one missing; 9 Sep);²⁰
- a Greek-owned VLCC, struck by a drone inside Iraqi waters off Al-Faw (9 Sep);²¹
- the Togo-flagged *Trend*, attacked and stopped by the IRGC, which claimed it had made an "illegal passage" (17 Sep);²²
- two ADNOC-linked tankers, hit on consecutive days (20–21 Sep);²³
- the bulk carrier *Cape Dao*, reportedly torpedoed off Musandam (one crew killed, 23 Sep);²⁴
- the Kuwaiti VLCC *Al Funtas*, struck on 29 Sep after a week-long lull. It was not on Iran's list.²⁵

The US rejected an Iranian claim that a tanker had hit a mine, saying it was struck twice by Iranian weapons.²⁶ War-risk claims since the conflict began have passed \$2 billion, the second-largest marine insurance loss in over a decade.²⁷

FENESTRA ASSESSMENT: It is **highly likely** that attacks on merchant shipping in and around Hormuz continue into October. The IRGC is enforcing its own transit regime through a published "non-compliant" list, and September's strikes reached beyond the Strait itself (Dubai anchorage, Iraqi waters, Musandam). The *Al Funtas* strike shows that ships NOT on the list are also at risk, so staying off the list is **unlikely** to protect a vessel. **ASSESSMENT ENDS**

Bab el-Mandeb: the month's genuine escalation. For the first time, the Houthis took ground on the Strait itself. They seized the port of Mocha on 10 September, then pushed down the coast to the Hanish islands, the Ras Menhali peninsula and Perim Island at the mouth of the Bab el-Mandeb.^{4,5} Government forces pushed back within days,²⁸ and by late September the Houthis were consolidating their hold, which remains tenuous.²⁹ At the same time the group struck Saudi energy and aviation infrastructure:

- the Aramco Jazan refinery, taken offline by drone and missile strikes (7–8 Sep);⁶
- two pumping stations on the East-West Pipeline, the main route for moving Gulf oil around Hormuz;⁸
- a fuel depot beside Riyadh's King Khalid airport, which disrupted flights (19 Sep).⁹

The Houthis also claimed to have shot down a Saudi F-15SA.³⁰ The EU's top diplomat called for more ships and aircraft for Operation Aspides.³¹

FENESTRA ASSESSMENT: The Houthi advance is **highly likely** to be the most consequential maritime development of the month. Holding the shoreline and islands at the Strait's narrowest point would let the group threaten transits with short-range weapons, not only long-range drones and missiles. With Hormuz already contested, and the East-West Pipeline (Saudi Arabia's route for Gulf oil that avoids Hormuz) now damaged, both of the region's main export corridors were under attack in the same month. **ASSESSMENT ENDS**

Somali piracy is back. Hijackings off Somalia have returned to levels not seen in a decade, with eight since late April, fuelled by the Iran war's disruption to naval presence and by instability in Somalia.³² A Greek-managed cargo ship was boarded off Yemen (11 Sep), although the attackers failed to take it.³³ Puntland forces freed the hijacked tanker *Sibu 1* and detained 47 suspects (25 Sep).³⁴

Black Sea and Mediterranean.

- Russian and Ukrainian drones continued to hit merchant ships. A Russian strike killed the master of a Ukraine-bound vessel (17 Sep).³⁵
- A naval-drone (USV) attack on Sochi port injured around 30.³⁶
- In the Baltic, a Ukrainian drone strike set Russia's Ust-Luga export port alight.³⁷
- The war also moved into the Mediterranean: the sanctioned Russian ro-ro *Lady Mariia* was drone-struck near Crete (6 Sep).³⁸

Emerging flashpoint: cyber attacks on ship systems. The LNG carrier *Vivit Africa LNG*, carrying a US cargo to Italy under charter to Vitol, lost access to onboard control systems in what the crew reported as a cyber attack, and diverted without discharging.^{39,40} Reporting describes it as the latest in a number of suspected incidents on tankers.

FENESTRA ASSESSMENT: There is a **realistic possibility** that attacks on shipboard systems become a reported, recurring threat to energy shipping. That depends on attribution, which has not been made public. **ASSESSMENT ENDS**

Drones, shadow fleet, seabed and GPS spoofing.

- Germany formally attributed the failed explosive-drone attack on Leipzig/Halle Airport (4 Aug) to Russia and closed Russia's consulate in Bonn (1 Sep).⁴¹
- Italian Typhoons on NATO Baltic Air Policing shot down a drone over Lithuania. It is believed to have entered from Belarus.⁴²
- EU navies carried out a sixth flag-verification boarding of a suspected shadow-fleet tanker.⁴³
- Finland rehearsed at-sea boardings to prevent undersea sabotage.⁴⁴
- As GPS spoofing concerns rise, Galileo demonstrated a service that authenticates satellite positioning signals for civil users.⁴⁵

RANSOMWARE

THE LEADERBOARD FLATTENED

MEASURE	AUGUST	SEPTEMBER
Top-three groups' share of victims	~32%	~25%
United States share of victims	~34%	32%
Manufacturing	~15%	17%
Technology	~13%	11%
Professional services	~11%	12%
Healthcare	~10%	9%

Share of victims named on ransomware leak sites.⁷

The leaderboard flattened. TheGentlemen and Qilin swapped places at the top, but the top three together fell from roughly a third of all named victims in August to just under a quarter in September, as Clon receded and a long tail of mid-sized and newly observed operations grew. The US remained the most targeted country (~32%), and manufacturing extended its lead as the most-hit sector (17%).

TheGentlemen — the most active group this month. It is also the most active group in Japan in H1 2026, driving a ~4.7% rise in incidents there, mostly against SMEs.⁴⁶ It claimed Veradigm (formerly Allscripts), alleging theft of 3.5 million patients' health records.⁴⁷ Separately, an affiliate was documented using an AI coding agent to run intrusions against at least six organisations.⁴⁸

Qilin — the clearest CVE-to-ransomware link this month. Cisco confirmed that three threat clusters, spanning ransomware and state-sponsored actors, exploited two Secure Firewall Management Center (FMC) flaws, and that in some cases the intrusions ended in Qilin deployment.^{49,50} Microsoft separately profiled **Storm-2570**, an affiliate running the same tradecraft across Qilin, DragonForce, Anubis and BERT deployments.⁵¹

FENESTRA ASSESSMENT: The drop in top-three concentration is **likely** to reflect Clon's burst-driven posting pattern and the affiliate model rather than a real weakening of the leading operations. Affiliates such as Storm-2570 move between ransomware brands with the same tooling, so group-level shares understate how concentrated the underlying intrusion activity is. **ASSESSMENT ENDS**

NOTABLE EXPLOITED VULNERABILITIES

- **CVE-2026-20079 / CVE-2026-20316 — Cisco Secure Firewall Management Center.** Auth bypass to root (CVSS 10.0); exploited by ransomware and state clusters, leading to Qilin deployment; hotfixes available.^{52,49}

- **CVE-2026-88771 / CVE-2026-88772 ("PitScaler") — Citrix NetScaler ADC/Gateway.** Two critical (9.5) zero-days exploited since at least early September for web shells, root access and credential theft in North America and Europe; added to CISA KEV 27 Sep; patch now.^{53,54} (NetScaler again, after CVE-2026-8452 in August.)
- **CVE-2026-85102 / CVE-2026-93616 — Check Point Security Gateway VPN (pre-auth RCE) + Management (pre-auth path traversal).** Exploited; 93616 has been exploited as a zero-day since 23 July; fixes available.^{55,56}
- **CVE-2026-94127 — F5 BIG-IP APM.** Pre-auth RCE (9.8), exploited in the wild when an access policy and OAuth profile are configured; emergency fix 22 Sep.⁵⁷
- **CVE-2026-76460 — Cisco ISE.** Critical (10.0), exploited; CISA KEV 16 Sep.^{58,59}
- **CVE-2026-83548 / CVE-2026-83549 — SonicWall SMA 1000.** Pre-auth SSRF (10.0) + post-auth RCE, both exploited as zero-days.⁶⁰
- **CVE-2026-35273 — Oracle PeopleSoft.** ShinyHunters renewed mass exploitation using a WAF-bypass (URL-encoding) trick, now across sectors (June's wave targeted education).^{61,62}
- **CVE-2026-81963 / CVE-2026-85880 — Windows Update Stack / ALPC privilege escalation.** Exploited zero-days (Patch Tuesday, 8 Sep); 85880 is chained in the "BlueMoon" exploit kit with two Chrome V8 flaws.^{63,64}
- Also exploited: WordPress core CVE-2026-87902 (KEV), JFrog Artifactory CVE-2026-82329, MikroTik RouterOS CVE-2026-67279 ("MikroTrick" chain, KEV), SharePoint CVE-2026-65660 (KEV).
- **Kiteworks (formerly Accellion)** told customers to shut down servers for six hours after "credible threat intelligence" of an imminent attack, then patched a critical flaw and lifted the advisory.^{65,66}

FENESTRA ASSESSMENT: It is **highly likely** that internet-facing security appliances remain the main shared initial-access surface for ransomware and state actors. September repeats August's pattern with new exploited flaws in NetScaler, Check Point, F5 and Cisco firewall management, and the Cisco FMC case directly links an appliance flaw to Qilin deployment. Given Clop's history of mass-exploiting managed file-transfer products (including Accellion FTA), there is a **realistic possibility** that the Kiteworks warning relates to similar targeting; no attribution has been made public. **ASSESSMENT ENDS**

INTERNET SIGNALS

A BASELINE FROM OUR OWN SENSORS

September is the first full month of Fenestra's internet sensor network: SSH/Telnet, multi-protocol and industrial-control-system (ICS) honeypots exposed to the open internet. The figures below set the baseline for month-on-month comparison from October.⁷

A small number of machines did most of the work. Just over half of all SSH/Telnet sessions came from about 110 IP addresses running the same credential-harvesting routine: log in, fingerprint the host, and move on. Around half of all sessions came from infrastructure in Bulgaria.⁷ More than four in five sessions went on to run commands, so these are not just port scans; they are automated attempts to confirm and catalogue working access.

FENESTRA ASSESSMENT: It is **likely** that this concentrated harvesting activity supplies the access-broker market, which sells verified logins to other criminals, rather than being the work of the attackers who eventually use that access. Very few addresses produce most of the volume, which makes blocking by reputation effective for this traffic. **ASSESSMENT ENDS**

How stolen access moves through the underground. Most intrusions are no longer run by one group from start to finish. Access passes along a criminal supply chain, and each stage is a specialist trade:

- **Gaining a foothold.** Automated scanners and credential-harvesting farms, like the cluster above, test exposed logins and unpatched edge devices at scale. Infostealer malware on employees' personal and work devices adds saved passwords and session cookies (see Cyber underground).
- **Brokering access.** Initial access brokers verify what works, assess the victim's size and sector, and sell footholds on underground forums and messaging channels. Price reflects the victim's revenue and the level of privilege on offer.
- **Using access.** Buyers include ransomware affiliates, who often deploy several ransomware brands with the same tooling (see Ransomware), data-theft and extortion groups, fraudsters, and cryptomining and botnet operators.
- **Cashing out.** Encryption and extortion, sale of stolen data, and resale of the same access to further buyers, which is why one breach can lead to repeat incidents.

The practical point is that the cheapest place to break this chain is the first link. An organisation that removes exposed login services, patches edge devices and watches for its staff's credentials in stealer logs gives brokers nothing to sell.

IoT botnets remain the background noise. Default credentials associated with Mirai-family botnets appeared in roughly one in twelve SSH/Telnet sessions, from more than 800 distinct addresses: far more sources, but far less activity per source, than the harvesting cluster.⁷

Secrets, not just vulnerabilities. Almost a quarter of web requests to the multi-protocol sensor were attempts to fetch configuration and secrets files, such as .env files and exposed .git directories, which commonly hold cloud keys, database passwords and API tokens.⁷ More than 8% of web requests claimed to be Googlebot but did not come from Google. Scanners use that disguise to get past bot filtering. A small but new set of addresses probed for AI-agent (MCP) configuration endpoints. The trend mirrors the underground trade in stolen AI API keys (see Cyber underground). Outside the web, Microsoft SQL Server and Windows file sharing (SMB) were the most probed services, together about half of all connections. Only about one in forty source addresses was already known to public threat-intelligence feeds.⁷

Industrial protocols are probed within days of exposure. An ICS honeypot brought online on 24 September was contacted by more than 150 distinct addresses within its first week. IEC 60870-5-104 (used in electricity grid telecontrol) was the most probed protocol, ahead of Modbus and Siemens S7.⁷

FENESTRA ASSESSMENT: It is **almost certain** that any internet-exposed ICS interface will be found and fingerprinted within days. Most of this activity is **likely** to be survey scanning rather than targeted attack preparation, but grid-telecontrol protocols topping the list is consistent with the heightened interest in energy infrastructure noted elsewhere in this report. Operators should assume discovery is immediate and keep these interfaces off the public internet. **ASSESSMENT ENDS**

CYBER UNDERGROUND

AI MOVES FROM NOVELTY TO COMMODITY

AI moved from novelty to commodity. AI-related content almost doubled its share of underground forum discussion month on month, to roughly one post in ten.⁷ The trade has matured from jailbreak prompts and "uncensored" chatbot services into **resale of stolen AI and cloud API keys**: bundles of OpenAI, Anthropic, Google and hyperscaler credentials, some advertised with high spending limits. Offers of free or leaked keys have circulated since at least May; September brought organised sales listings, including a marketplace for Chinese AI-platform keys.⁷

FENESTRA ASSESSMENT: It is **highly likely** that stolen AI API keys are becoming a standard commodity alongside cloud and SaaS credentials. They offer free compute to criminals and a billing-fraud and data-exposure risk to the organisations that own them, and the documented use of AI coding agents by a ransomware affiliate this month (see Ransomware) shows the demand side. Organisations should treat AI platform keys as production secrets: scoped, rotated and monitored for spend anomalies.

ASSESSMENT ENDS

Edge-device zero-days reach the forums within hours. Citrix's NetScaler "PitScaler" zero-days were being discussed on a darknet hacking forum on the evening of disclosure, with the poster claiming one flaw remains exploitable on default configurations.⁷ That claim is unverified, but it shows how quickly public vulnerability disclosures turn into underground discussion.

Everything else was steady. Carding and fraud content fell back, database and leak trading held steady, and ransomware recruitment/affiliate chatter stayed marginal on open forums. The latter is consistent with that activity running through private channels and the groups' own leak sites (see Ransomware). Stealer logs continued to circulate in volume, and government-portal credentials, concentrated in South Asia, remained among the most frequent entries.⁷

FENESTRA ASSESSMENT: It is **likely** that the September shift reflects changing demand (AI access, fresh edge-device exploits) rather than a change in underground supply. Database and leak trading, a core commodity, shows no meaningful change in share. **ASSESSMENT ENDS**

PHYSICAL SPOTLIGHT

RUSSIAN HYBRID SABOTAGE IN EUROPE

From deniable to declared. In September, European governments stopped hedging. Germany formally attributed the failed explosive-drone attack on a Ukraine-bound Antonov at Leipzig/Halle Airport (4 August) to the Russian state and closed Russia's consulate in Bonn.^{41,69} Investigators later reported that about 1.8 kg of Semtex, hidden in a food tin, failed to detonate only because a wire snapped, while the aircraft held about 25,000 litres of fuel.⁷⁰ Estonia concluded "with certainty" that Russian special services ordered the August arson attack on Milrem Robotics, which supplies Ukraine with unmanned ground vehicles.⁷¹ European Commission President Ursula von der Leyen called such incidents Europe's "new normal".⁷² Counting each development once, however widely it was reported, Fenestra's news collection recorded 39 distinct Russian sabotage developments in Europe in September, against 15 in August. The number of new incidents barely changed (nine against eight). The rise came from attributions, arrests, charges and official statements, which went from seven to 30.⁷

What was hit. The targets form a clear pattern: the companies and logistics that keep Ukraine supplied.

- **Defence manufacturers.** Arson hit a drone-component plant in Lublin, Poland, which the Polish prime minister called "undoubtedly" deliberate and likely Russian-ordered.⁷³ Incendiaries were thrown at a site next to Rohde & Schwarz and Helsing in Munich, and German investigators link that attack to Russian military intelligence (GRU).⁷⁴ A second fire hit an EMCO ammunition store in Bulgaria, which the owner calls sabotage.⁷⁵
- **Connectivity to Ukraine.** A fire at a Starlink/Exatel ground station in central Poland was, according to Poland's digital affairs minister, "deliberately designed to disable the station", which carries internet traffic to the Ukrainian army.⁷⁶
- **Undersea infrastructure.** UK, Norwegian and US forces tracked Russian GUGI submarines near Svalbard. Western officials said the submarines were rehearsing a cable-disabling technique designed to leave no trace.^{77,78}
- **Airspace.** NATO jets shot down a drone over Lithuania.⁴² A Russian drone crossed Moldova and Romania as President Zelenskyy's aircraft departed Chişinău.⁷⁹ Suspected Russian "Gerbera" drones crashed in both countries on 24 September,⁸⁰ and a Russian frigate fired flares at a Danish military helicopter.⁸¹

How it is done: gig-economy sabotage. The operatives are rarely Russian officers. Police detained two Bulgarian nationals over the Munich attack, and three people, two Latvians and a Ukrainian, over an attempted arson at a Ukrainian drone maker's plant in Slovakia.⁸² Denmark's security service warned that Russian services recruit "ordinary Danes" on social media to photograph defence-industry sites.⁸³ In the UK, a Swindon man was charged under the National Security Act. The charges allege he passed the locations of local drone-manufacturing sites to a contact linked to the GRU and offered to carry out sabotage himself.⁸⁴ Separately, a man recruited on Telegram pleaded guilty to vandalising London mosques as part of the Russian network behind the arson attacks on property linked to Sir Keir Starmer.⁸⁵ Germany's

Federal Criminal Police Office (BKA) counted more than 165 suspected sabotage cases and 747 suspicious drone incidents in the first eight months of 2026.⁸⁶ The pace has not risen: police logged 320 suspected sabotage cases across the whole of 2025.⁸⁷

Not everything is Russia. Coordinated obstructions at around 30 points on the Dutch rail network halted trains across much of the country on 15 September. No suspect was identified, and local reporting pointed to protesting farmers.^{88,89} Germany is investigating two attacks on electricity substations in which a foreign state and left-wing extremists are both being considered.⁹⁰

FENESTRA ASSESSMENT: It is **highly likely** that Russian-directed sabotage against European companies that supply or transport materiel to Ukraine will continue through the winter, and **likely** that it will intensify. The EU's foreign policy chief said intelligence shows further sabotage being planned,⁶⁷ Danish defence intelligence expects hybrid warfare to escalate,⁶⁸ and the proxy-recruitment model is cheap, deniable and easy to replace when operatives are arrested. A UK incident is a **realistic possibility**, given the UK's drone-industrial base and the September charge. **ASSESSMENT ENDS**

FENESTRA ASSESSMENT: Most of these targets are privately owned: factories, warehouses, ground stations and logistics hubs. It is **almost certain** that the first line of defence against this threat sits with company security teams rather than governments. This is the MI5 Director General's point that critical decisions will be taken "in boardrooms". Early public attribution is **likely** to continue to lag incidents by weeks, as it did at Leipzig and Milrem, so companies cannot wait for official confirmation before hardening. **ASSESSMENT ENDS**

What to do

- Treat any link to Ukraine-bound supply chains (manufacturing, logistics, telecoms, storage) as a higher risk factor.
- Brief staff and contractors that recruiters approach people online for paid "photo" or "delivery" jobs. Make it easy to report suspicious photography and approaches.
- Review perimeter, CCTV coverage and out-of-hours fire detection at warehouses and construction sites next to sensitive facilities. Consider drone detection at high-value sites.
- Share suspicious-activity reports with national authorities (in the UK, via the NPSA and police). Individual incidents look minor until they are connected.

CYBER SPOTLIGHT

SHINYHUNTERS

The month ShinyHunters picked a fight with everyone. The English-speaking extortion collective, tracked by Google as UNC6240, was already one of the most prolific data-theft operations of 2026. In August its leak site named 19 victims, more than a third of them in healthcare and medical technology, many breached through a zero-day in the Metabase analytics platform.^{7,92} In September it turned its attention to government, law enforcement and rival criminals, and became the target of a coordinated international law-enforcement response.

Timeline

- **3–12 Sep, Florida DMV.** The group claimed it scraped more than 200,000 driver records from Florida's "DAVID" law-enforcement driver database from 3 September.⁹³ The state confirmed the breach, tracing it to credentials stolen from a police officer's personal device.⁹⁴
- **11–12 Sep, AI and identity tradecraft.** Anthropic reported disrupting suspected ShinyHunters affiliates who used AI to scan for credentials, map victim networks and exploit stolen AI API keys, including a pipeline that scanned 1.8 million Android apps for hard-coded secrets.^{95,96} Microsoft linked ShinyHunters-associated Storm-3121 to passkey- and single sign-on-themed social engineering used to take over corporate Microsoft 365 accounts.⁹⁷
- **15 Sep, arrest.** Dutch police arrested a 24-year-old Amsterdam man in their ShinyHunters investigation. The arrest was made public on 28–29 September.^{98,99}
- **19–21 Sep, attacking CI0p.** The group hijacked the CI0p ransomware gang's leak site through an unpatched CMS flaw. It named alleged CI0p operators and set an eight-figure extortion demand against the ransomware gang itself. CI0p moved to a new onion address and denied any relationship.^{100,101}
- **22 Sep, the FBI.** ShinyHunters defaced FBIjobs.gov and claimed to hold personal, and in some cases medical, data on almost all FBI agents and job applicants. It demanded that the Bureau withdraw a public advisory about the group.^{102,103} Journalists partially verified samples of the data. The FBI says the point of compromise, whether its own systems or a third-party provider, is still undetermined.^{104,105}
- **25–27 Sep, PeopleSoft again.** Mandiant reported renewed mass exploitation of the Oracle PeopleSoft flaw CVE-2026-35273, first used as a zero-day against universities in May–June. The group now uses a URL-encoding trick to slip past the web application firewall rules many organisations had deployed instead of patching, and targets organisations across sectors worldwide.^{61,62,63}
- **29–30 Sep, escalation of the law-enforcement response.** A Rotterdam court extended the suspect's pre-trial detention by at least 90 days. Dutch police said information about two murders planned abroad was found on his laptop, with indications that he ordered them. The FBI publicly described him as an alleged leader of the group and urged remaining members to turn themselves in.^{106,107}

Through all of this the group's leak site changed character. September brought far fewer new victim postings than August, and the site was increasingly used for public statements aimed at the FBI and CI0p.⁷

FENESTRA ASSESSMENT: It is **likely** that the arrest has not reduced ShinyHunters' operational capability in the short term. The CIOp and FBI operations both followed the arrest, and the PeopleSoft campaign was active at the same time. The move from naming victims to making public statements suggests the group is currently prioritising reputation and retaliation over extortion revenue. A **realistic possibility** is that it leaks the FBI data or makes further high-profile claims against law-enforcement or government targets in October. **ASSESSMENT ENDS**

FENESTRA ASSESSMENT: The threat to organisations is **highly likely** to continue through two routes. The first is social engineering of help desks and single sign-on. The second is exploitation of internet-facing business applications that were mitigated but never patched. The PeopleSoft campaign shows that a WAF rule is a temporary workaround, not a fix, and the Florida breach shows that one set of credentials on a personal device can expose a whole government database. The exposure of personal data on law-enforcement staff also carries a physical-security dimension: groups in the same English-speaking cybercrime ecosystem have previously been linked to swatting and violent attacks against rivals and officials.⁹¹ **ASSESSMENT ENDS**

What to do

- Patch Oracle PeopleSoft for CVE-2026-35273. If you relied on a WAF or proxy block, check it against the URL-encoded variants Mandiant describes.⁶¹
- Require strong identity verification for help-desk password, MFA and passkey resets, and watch for SSO-themed lures.⁹⁷
- Restrict access to sensitive databases from unmanaged personal devices.⁹⁴
- Treat AI platform and cloud API keys as production secrets: scope them, rotate them and monitor their spend (see Cyber underground).

SOURCES

Numbered references to public reporting cited in this briefing. Shares, leak-site, underground and sensor figures are Fenestra analysis of its own collection. Information is correct at time of writing (1 October 2026); some situations described, including ongoing investigations, may have developed since publication.

1. MI5 — DG Statement on the 25th Anniversary of the 9/11 Attacks (11 Sep).
<https://www.mi5.gov.uk/dg-statement-on-the-25th-anniversary-of-the-911-attacks>
2. The Siasat Daily — Video: UAE builds 'cope cages' to shield fuel tanks from drones (23 Aug).
<https://www.siasat.com/video-uae-builds-cope-cages-to-shield-fuel-tanks-from-drones-3529342/>
3. Euronews — Qatar and UAE say Gulf cannot rely on US alone for region's security (8 Sep).
<http://www.euronews.com/2026/09/08/qatar-and-uae-say-gulf-cannot-rely-on-us-a-lone-for-regions-security>
4. gCaptain (Reuters) — Houthis Seize Mocha, Tightening Grip on Bab el-Mandeb and Red Sea Shipping (10 Sep).
<https://gcaptain.com/houthis-seize-mocha-tightening-grip-on-bab-el-mandeb-and-red-sea-shipment/>
5. South China Morning Post — Yemen's Houthis reach strategic island in Bab el-Mandeb Strait (11 Sep).
<https://www.scmp.com/news/world/middle-east/article/3367232/yemens-houthis-reach-strategic-island-bab-el-mandeb-strait>
6. The Maritime Executive — Houthi Forces Attack Saudi Aramco's Jazan Refinery (8 Sep).
<https://maritime-executive.com/article/houthi-forces-attack-saudi-aramco-s-jazan-refinery>
7. Fenestra TI — Collection and analysis: news and event data, ransomware leak sites, underground forums, stealer logs and Fenestra honeypot sensors (Aug-Sep 2026).
<https://fenestra-ti.com>
8. The Maritime Executive — Saudi East-West Pipeline Suffers Significant Damage in Drone Attack (11 Sep).
<https://maritime-executive.com/article/saudi-east-west-pipeline-suffers-significant-damage-in-drone-attack>
9. AeroTime — Flights disrupted at Riyadh airport after Houthi attack against Saudi Arabia (20 Sep).
<https://www.aerotime.aero/articles/riyadh-airport-flights-disrupted-houthi-attack>
10. Al Jazeera — Israeli strikes continue in southern Lebanon despite ceasefire (27 Sep).
<https://www.aljazeera.com/video/newsfeed/2026/9/27/israeli-strikes-continue-in-southern-lebanon-despite-ceasefire>
11. Al Jazeera — Nigeria, Boko Haram reportedly reach secret three-month ceasefire (9 Sep).
<https://www.aljazeera.com/news/2026/9/9/nigeria-boko-haram-reportedly-reach-secret-three-month-ceasefire>
12. Premium Times — Nigerian Army redeploys top generals, appoints new person to lead Boko Haram war (9 Sep).
<https://www.premiumtimesng.com/news/top-news/908445-nigerian-army-redeploy-top-general-appoints-new-person-to-lead-boko-haram-war.html>
13. Egypt Independent — UK, France and Canada sanction Israeli settlements in West Bank as Britain accuses settlers of 'ethnic cleansing' (10 Sep).
<https://www.egyptindependent.com/uk-france-and-canada-sanction-israeli-settlements-in-west-bank-as-britain-accuses-settlers-of-ethnic-cleansing/>
14. The Guardian — Miliband rejects chief rabbi's claim that West Bank sanctions put UK Jews at risk (9 Sep).
<https://www.theguardian.com/politics/2026/sep/09/ed-miliband-rejects-chief-rabbi-claim-west-bank-sanctions-british-jews-less-safe>
15. BBC News — How did the RAF Fairford incident go from 'suspected bomb plot' to police bail? (29 Sep).
<https://www.bbc.co.uk/news/articles/c6p3kxlx4epwo>
16. Middle East Eye — How RAF Fairford 'bomb plot' narrative fell apart as US and UK made competing claims (29 Sep).
<https://www.middleeasteye.net/news/how-raf-fairford-bomb-plot-narrative-fell-apart-us-and-uk-made-competing-claims>
17. Middle East Eye — UK police say no explosive devices found in airbase probe (29 Sep).
<https://www.middleeasteye.net/live-blog/live-blog-update/uk-police-say-no-explosive-devices-found-airbase-probe>
18. NBC News — Britain believes Iran was involved in incident near air base used by U.S., Prime Minister Andy Burnham says (30 Sep).
<https://www.nbcnews.com/world/united-kingdom/uk-andy-burnham-raf-fairford-air-base-terror-explosives-iran-involved-rcna600713>
19. Seatrade Maritime News — Two crew dead in attack on Bahri VLCC, Iran blacklists more ships (2 Sep).
<https://www.seatrade-maritime.com/security/two-crew-casualties-in-hormuz-attack-iran-blacklists-more-ships>
20. MarineTraffic — Tanker Attacked Off Dubai, One Crew Member Dead and One Missing (9 Sep).
<https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13231/tanker-attacked-off-dubai-one-crew-member-dead-and-one-missing>
21. Splash247 — Greek-owned VLCC hit by drone in Iraqi waters (9 Sep).
<https://splash247.com/greek-owned-vlcc-hit-by-drone-in-iraqi-waters/>
22. MarineTraffic — IREG Claim Attack the Togo-flagged Oil Tanker in Strait of Hormuz (18 Sep).
<https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13251/irgc-claim-attack-the-togo-flagged-oil-tanker-in-strait-of-hormuz>
23. MarineTraffic — Two Commercial Tankers Attacked Crossing Strait of Hormuz (22 Sep).
<https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13259/two-commercial-tankers-attacked-crossing-strait-of-hormuz>
24. MarineTraffic — Indian Crew Member Killed in Attack on Bulk Carrier off Oman (24 Sep).
<https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13262/indian-crew-member-killed-in-attack-on-bulk-carrier-off-oman>
25. The Maritime Executive — Kuwaiti Tanker Struck in the Strait of Hormuz (29 Sep).
<https://maritime-executive.com/article/kuwaiti-tanker-struck-in-the-strait-of-hormuz>
26. gCaptain — U.S. Rejects Iran's Mine Claim as Hormuz Shipping Threat Remains Severe (14 Sep).
<https://gcaptain.com/u-s-rejects-irans-mine-claim-as-hormuz-shipping-threat-remains-severe/>
27. gCaptain — War Risk Claims Top \$2 Billion as Shipping Attacks Spread Beyond Hormuz (3 Sep).
<https://gcaptain.com/war-risk-claims-top-2-billion-as-shipment-attacks-spread-beyond-hormuz/>
28. The Maritime Executive — Houthis Being Pushed Back from Bab el-Mandeb (14 Sep).
<https://maritime-executive.com/article/houthis-being-pushed-back-from-bab-el-mandeb>
29. The Maritime Executive — Houthis Consolidate Gains and Pause Before the Next Push (24 Sep).
<https://maritime-executive.com/article/houthis-consolidate-gains-and-pause-before-the-next-push>
30. FlightGlobal — Houthi rebels claim shoot down of Saudi F-15SA (17 Sep).
[https://www.flightglobal.com/fixed-wing/2026/09/houthi-rebels-claim-shoot-down-of-saudi-f-15sa/](https://www.flightglobal.com/flightglobal.com/fixed-wing/2026/09/houthi-rebels-claim-shoot-down-of-saudi-f-15sa/)
31. gCaptain (Bloomberg) — Kallas Urges EU to Bolster Red Sea Mission Against Houthi Threat (22 Sep).
<https://gcaptain.com/kallas-urges-eu-to-bolster-red-sea-mission-against-houthi-threat/>
32. The Guardian — Hijacking pirates exploit regional chaos to return to seas off Somalia (8 Sep).
<https://www.theguardian.com/world/2026/sep/08/hijacking-pirates-somalia-geopolitical-chaos>
33. Splash247 — Pirates board ship off Yemen (11 Sep).
<https://splash247.com/pirates-board-ship-off-yemen/>
34. MarineTraffic — Oil Tanker Released After Somali Pirate Hijacking, All 20 Crew Reported Safe (26 Sep).
<https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13265/oil-tanker-released-after-somali-pirate-hijacking-all-20-crew-reported-safe>
35. The Maritime Executive — Drone Attack Kills Master, Injures Three Crewmembers in Black Sea (17 Sep).
<https://maritime-executive.com/article/drone-attack-kills-master-injures-three-crew-members-in-black-sea>
36. The Maritime Executive — 30 Reported Injured in USV Attack on Port of Sochi (10 Sep).
<https://maritime-executive.com/article/30-reported-injured-in-usv-attack-on-port-of-sochi>
37. Splash247 — Drone strike sparks fresh fire at Russia's Ust-Luga port (1 Sep).
<https://splash247.com/drone-strike-sparks-fresh-fire-at-russias-ust-luga-port/>

- 38. MarineTraffic** — Sanctioned Russian Cargo Ship Attacked Near Crete (7 Sep).
<https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13226/sanctioned-russian-cargo-ship-attacked-near-crete>
- 39. gCaptain (Bloomberg)** — Another Tanker Suffers Failure as Crew Suspect Cyber Attack (18 Sep).
<https://gcaptain.com/another-tanker-suffers-failure-as-crew-suspect-cyber-attack/>
- 40. Splash247** — Crew claims hackers seized control of LNG carrier safety systems (20 Sep).
<https://splash247.com/crew-claims-hackers-seized-control-of-lng-carrier-safety-systems/>
- 41. AeroTime** — Germany blames Russia for failed explosive drone attack at Leipzig Airport (2 Sep).
<https://www.aerotime.aero/articles/germany-russia-leipzig-airport-explosive-drone-attack>
- 42. AeroTime** — NATO fighters shoot down drone over Lithuania after airspace incursion (14 Sep).
<https://www.aerotime.aero/articles/nato-fighters-shoot-down-drone-over-lithuania-after-airspace-incursion>
- 43. MarineTraffic** — European Naval Forces Board Suspected Russian Shadow Fleet Vessel for Flag Verification (1 Sep).
<https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13208/european-naval-forces-board-suspected-russian-shadow-fleet-v>
- 44. gCaptain (Reuters)** — Finland Practices Ship Boardings at Sea to Stop Undersea Sabotage (17 Sep).
<https://gcaptain.com/finland-practices-ship-boardings-at-sea-to-stop-undersea-sabotage/>
- 45. FlightGlobal** — Galileo satellites demonstrate position-authentication service as spoofing concerns rise (17 Sep).
<https://www.flightglobal.com/archive/2026/09/galileo-satellites-demonstrate-position-authentication-service-as-spoofing-concerns-rise/>
- 46. Cisco Talos** — Ransomware incidents in Japan in the first half of 2026 (17 Sep).
<https://blog.talosintelligence.com/ransomware-incidents-in-japan-in-the-first-half-of-2026/>
- 47. The Record** — Electronic health record company says customer data stolen in breach (9 Sep).
<https://therecord.media/electronic-health-record-company-says-customer-data-stolen-in-breach>
- 48. Check Point Research** — AI Threat Landscape Digest: July–August 2026 (17 Sep).
<https://research.checkpoint.com/2026/ai-threat-landscape-digest-july-august-2026/>
- 49. The Hacker News** — Cisco FMC Flaws Exploited to Steal Credentials and Deploy Qilin Ransomware (24 Sep).
<https://thehackernews.com/2026/09/cisco-fmc-flaws-exploited-to-steal.html>
- 50. BleepingComputer** — InfraTrust report warns network management systems under attack (23 Sep).
<https://www.bleepingcomputer.com/news/security/infustrust-report-warns-network-management-systems-under-attack/>
- 51. Microsoft Threat Intelligence** — Beyond the ransomware: Tracking Storm-2570's consistent tradecraft (24 Sep).
<https://www.microsoft.com/en-us/security/blog/2026/09/24/beyond-ransomware-tracking-storm-2570-consistent-tradecraft-across-deployments/>
- 52. BleepingComputer** — Cisco confirms CVE-2026-20079 Secure FMC flaw exploited in attacks (9 Sep).
<https://www.bleepingcomputer.com/news/security/cisco-confirms-cve-2026-20079-secure-fmc-flaw-exploited-in-attacks/>
- 53. CISA** — Critical Zero-Day Vulnerabilities Exploited in Citrix NetScaler ADC, Gateway (27 Sep).
<https://www.cisa.gov/news-events/alerts/2026/09/27/critical-zero-day-vulnerabilities-exploited-citrix-netscaler-adc-gateway>
- 54. BleepingComputer** — Hackers exploit Citrix NetScaler zero-day to deploy web shells (29 Sep).
<https://www.bleepingcomputer.com/news/security/hackers-exploit-citrix-netscaler-zero-day-to-deploy-web-shells/>
- 55. Check Point** — Security Advisory – Active Exploitation of CVE-2026-85102 and CVE-2026-93616 (22 Sep).
<https://blog.checkpoint.com/security/security-advisory-action-required-active-exploitation-of-cve-2026-85102-and-a-management-pre-authentication-vulnerability-cve-2026-93616/>
- 56. BleepingComputer** — Check Point warns of hackers exploiting Security Gateway VPN RCE flaw (23 Sep).
<https://www.bleepingcomputer.com/news/security/check-point-warns-of-hackers-exploiting-security-gateway-vpn-rce-flaw/>
- 57. Security Affairs** — F5 BIG-IP APM Zero-Day Exploited in Zero-Day RCE Attacks (23 Sep).
<https://securityaffairs.com/199619/security/f5-big-ip-apm-zero-day-exploited-in-zero-day-rce-attacks.html>
- 58. CISA** — CISA Adds Two Known Exploited Vulnerabilities to Catalog (16 Sep).
<https://www.cisa.gov/news-events/alerts/2026/09/16/cisa-adds-two-known-exploited-vulnerabilities-catalog>
- 59. Check Point Research** — 21st September – Threat Intelligence Report (21 Sep).
<https://research.checkpoint.com/2026/21st-september-threat-intelligence-report/>
- 60. Check Point Research** — 7th September – Threat Intelligence Report (7 Sep).
<https://research.checkpoint.com/2026/7th-september-threat-intelligence-report/>
- 61. Google Threat Intelligence (Mandiant)** — ShinyHunters Renewed Mass Exploitation Campaign Targeting Oracle PeopleSoft (25 Sep).
<https://cloud.google.com/blog/topics/threat-intelligence/shinyhunters-renewed-mass-exploitation-campaign-targeting-oracle-peoplesoft/>
- 62. BleepingComputer** — ShinyHunters uses WAF bypass trick in Oracle PeopleSoft attacks (26 Sep).
<https://www.bleepingcomputer.com/news/security/shinyhunters-uses-waf-bypass-trick-in-oracle-peoplesoft-attacks/>
- 63. The Record** — Microsoft posts nearly 1,000 bugs for Patch Tuesday as CISA warns two being exploited (8 Sep).
<https://therecord.media/microsoft-patch-tuesday-september-2026>
- 64. BleepingComputer** — New 'BlueMoon' kit exploited Windows and Chrome zero-day flaws (10 Sep).
<https://www.bleepingcomputer.com/news/security/new-blue-moon-kit-exploited-windows-and-chrome-zero-day-flaws/>
- 65. The Record** — Kiteworks urges customers to stop using platform after warning from federal intelligence agencies (25 Sep).
<https://therecord.media/kiteworks-urges-customers-to-stop-using-systems-incident>
- 66. BleepingComputer** — Kiteworks patches critical flaw, brings customer systems online (29 Sep).
<https://www.bleepingcomputer.com/news/security/kiteworks-lifts-shutdown-warning-after-patching-critical-flaw/>
- 67. Euronews** — EU ministers plan hybrid threat response amid warnings of Russian sabotage (28 Sep).
<https://www.euronews.com/2026/09/28/eu-ministers-plan-response-to-hybrid-threats-amid-warnings-of-russian-sabotage>
- 68. The Guardian** — Russia could attack a Nato country within months, Danish intelligence says (24 Sep).
<https://www.theguardian.com/world/2026/sep/24/russia-could-attack-a-nato-country-within-months-danish-intelligence-says>
- 69. The Guardian** — Germany blames Russia for drone attack at Leipzig airport (1 Sep).
<https://www.theguardian.com/world/2026/sep/01/germany-blames-russia-drone-attack-leipzig-airport>
- 70. Kyiv Post (citing Welt am Sonntag)** — Leipzig Drone Attack Explosives Disguised in Food Can, Probe Finds (12 Sep).
<https://www.kyivpost.com/post/84360>
- 71. BBC News** — Estonia blames Russia for arson at defence company supplying Ukraine (29 Sep).
<https://www.bbc.co.uk/news/articles/c6m2714er4jxo>
- 72. Euronews** — Von der Leyen: Russian drone incidents in Europe are the 'new normal' (2 Sep).
<http://www.euronews.com/my-europe/2026/09/02/von-der-leyen-russian-drone-incidents-in-europe-are-the-new-normal>
- 73. Notes from Poland** — Polish drone plant fire "undoubtedly" arson and likely ordered by Russia, says Tusk (2 Sep).
<https://notesfrompoland.com/2026/09/02/polish-drone-plant-fire-undoubtedly-arson-and-likely-ordered-by-russia-says-tusk/>
- 74. Kyiv Independent (citing FAZ)** — Germany links arson attack near Ukraine-supplying drone maker Helsing to Russia's GRU (26 Sep).
<https://kyivindependent.com/germany-links-arson-attack-near-ukraine-supplying-drone-maker-helsing-to-russias-gru/>
- 75. BBC News** — Bulgaria investigates fire at weapons site that owner calls sabotage (12 Sep).
<https://www.bbc.co.uk/news/articles/cd94kj17zvwo>
- 76. Euronews** — Fire at Starlink station in central Poland was 'sabotage,' digital affairs minister says (24 Sep).
<https://www.euronews.com/2026/09/24/fire-at-starlink-station-in-central-poland-was-sabotage-digital-affairs-minister-says>
- 77. Euronews** — NATO allies successfully thwart Russian undersea cable sabotage operation (10 Sep).
<https://www.euronews.com/my-europe/2026/09/10/nato-allies-successfully-thwart-russian-undersea-cable-sabotage-operation>
- 78. The Maritime Executive** — Report: Russia Develops Untraceable Method to Disable Subsea Cables (10 Sep).
<https://maritime-executive.com/article/report-russia-develops-untraceable-method-to-disable-subsea-cables>

- 79. Euronews** — Timeline: How a Russian drone nearly hit Zelenskyy's plane in Moldova (10 Sep).
<http://www.euronews.com/my-europe/2026/09/10/timeline-how-a-russian-drone-nearly-hit-zelenskyy-s-plane-in-moldova>
- 80. Kyiv Independent** — Suspected Russian drones crash in Romania, Moldova (24 Sep).
<https://kyivindependent.com/suspected-russian-drones-crash-in-romania-moldova/>
- 81. Kyiv Post** — Russian Frigate Fires Flares at Danish Military Helicopter in International Waters (15 Sep).
<https://www.kyivpost.com/post/84541>
- 82. Meduza** (citing FAZ) — German investigators suspect Russian military intelligence organized an arson attack near defense firms in Munich (25 Sep).
<https://meduza.io/en/news/2026/09/25/german-investigators-suspect-russian-military-intelligence-organized-an-arson-attack-near-defense-firms-in-munich>
- 83. Euronews** — Denmark's intelligence agency warns Russia 'actively' preparing acts of sabotage (3 Sep).
<http://www.euronews.com/my-europe/2026/09/03/denmarks-intelligence-agency-warns-russia-actively-preparing-acts-of-sabotage>
- 84. Euronews** — Brit accused of feeding Russian military intelligence details of UK drone factories (10 Sep).
<https://www.euronews.com/my-europe/2026/09/10/brit-accused-of-feeding-russian-military-intelligence-details-of-uk-drone-factories>
- 85. BBC News** — Ukrainian guilty of vandalism at mosques linked to Russian network behind Starmer arson attack (17 Sep).
<https://www.bbc.co.uk/news/articles/c8dx5gldrk0ko>
- 86. Kyiv Post** (citing SZ/NDR/WDR) — Germany Records 165 Suspected Sabotage Cases This Year (4 Sep).
<https://www.kyivpost.com/post/83740>
- 87. IamExpat** (citing SZ/NDR/WDR) — Germany logs 165 suspected sabotage cases so far in 2026 (15 Sep).
<https://www.iamexpat.de/expat-info/germany-news/germany-logs-165-suspected-sabotage-cases-so-far-2026>
- 88. Euronews** — Suspected sabotage brings Dutch rail network to a standstill on Budget Day (15 Sep).
<https://www.euronews.com/my-europe/2026/09/15/suspected-sabotage-brings-dutch-rail-network-to-a-standstill-on-budget-day>
- 89. Al Jazeera** — Angry Dutch farmers blamed for railway sabotage: What happened? (16 Sep).
<https://www.aljazeera.com/news/2026/9/16/angry-farmers-blamed-for-dutch-railway-sabotage-what-happened>
- 90. Kyiv Post** — Germany Probes Two Sabotage Attacks on Power Grid (2 Sep).
<https://www.kyivpost.com/post/83589>
- 91. BBC News** — Inside the FBI hack: Agents fearful and angry after 'dangerous' data breach (26 Sep).
<https://www.bbc.co.uk/news/articles/cm4gjlgzjdgo>
- 92. BleepingComputer** — Mathspace discloses data breach affecting over 1 million people (7 Sep).
<https://www.bleepingcomputer.com/news/security/mathspace-discloses-data-breach-affecting-over-1-million-people/>
- 93. BleepingComputer** — ShinyHunters hackers claim breach of Florida "DAVID" DMV database (9 Sep).
<https://www.bleepingcomputer.com/news/security/shinyhunters-hackers-claim-breach-of-florida-david-dmv-database/>
- 94. The Record** — Florida says motor vehicle data breach tied to credentials stolen from officer's personal device (11 Sep).
<https://therecord.media/florida-shiny-hunters-motor-vehicle>
- 95. The Record** — Anthropic caught Russia-linked spies using Claude in hacking operations (11 Sep).
<https://therecord.media/anthropic-russia-hackers-claude>
- 96. BleepingComputer** — Hackers abused Claude to extract secrets from 1.8M Android apps (12 Sep).
<https://www.bleepingcomputer.com/news/security/hackers-abused-claude-to-extract-secrets-from-18m-android-apps/>
- 97. BleepingComputer** — Passkey-themed phishing attacks lead to Microsoft 365 data theft (12 Sep).
<https://www.bleepingcomputer.com/news/security/passkey-themed-phishing-attack-lead-to-microsoft-365-data-theft/>
- 98. KrebsOnSecurity** — Dutch Police Arrest 'Reformed' Hacker in Shiny Hunters Investigation (28 Sep).
<https://krebsonsecurity.com/2026/09/dutch-police-arrest-reformed-hacker-in-shiny-hunters-investigation/>
- 99. BleepingComputer** — Dutch police confirm arrest in ShinyHunters hacking investigation (29 Sep).
<https://www.bleepingcomputer.com/news/security/dutch-police-confirm-arrest-in-shinyhunters-hacking-investigation/>
- 100. The Record** — ShinyHunters cybercrime gang takes over CIOp ransomware site, demands extortion payment (21 Sep).
<https://therecord.media/shinyhunters-clop-cyberattack-website>
- 101. BleepingComputer** — ShinyHunters hacked Clop leak site using Grav CMS path traversal flaw (26 Sep).
<https://www.bleepingcomputer.com/news/security/shinyhunters-hacked-clop-leak-site-using-grav-cms-path-traversal-flaw/>
- 102. The Record** — FBI investigating alleged ShinyHunters breach of its jobs site (23 Sep).
<https://therecord.media/fbi-investigating-alleged-shinyhunters-job-site-breach>
- 103. The Guardian** — FBI investigates breach of jobs website as hackers claim 'very sensitive data' stolen (23 Sep).
<https://www.theguardian.com/us-news/2026/sep/23/fbi-jobs-website-hacked>
- 104. Al Jazeera** — FBI investigates alleged theft of 'very sensitive' employee data (23 Sep).
<https://www.aljazeera.com/news/2026/9/23/fbi-says-investigating-breach-of-very-sensitive-data-by-hackers>
- 105. NPR** — FBI hunting the hackers who stole its employees' sensitive data (30 Sep).
<https://www.npr.org/2026/09/30/nx-s1-5985202/fbi-hack-shinyhunters>
- 106. BleepingComputer** — FBI tells ShinyHunters members to turn themselves in after recent arrest (30 Sep).
<https://www.bleepingcomputer.com/news/security/fbi-tells-shinyhunters-members-to-turn-themselves-in-after-recent-arrest/>
- 107. BBC News** — Dutch police arrest suspected member of group that claimed FBI hack (29 Sep).
<https://www.bbc.co.uk/news/articles/cw5ym18znr0ro>

