FENESTRA TI

GLOBAL INTELLIGENCE. CONNECTED INSIGHT.



THREAT LANDSCAPE

October 2026

Geospatial and cyber threats — ransomware, exploited vulnerabilities, the criminal underground, our own sensor data and three spotlights: the Houthi campaign against Saudi Arabia, the PHP2Shell vulnerabilities and the Binance heist.

CONTENTS

1	EXECUTIVE SUMMARY	Where People And Goods Move	3
2	GEOSPATIAL & PHYSICAL SECURITY	Europe Rises, The Gulf Ignites	5
3	MARITIME & AVIATION SECURITY	A Tanker War And A Grounded Capital	9
4	RANSOMWARE	Qilin Doubles Down	13
5	VULNERABILITIES & EXPLOITATION	The Edge And The Stack	14
6	INTERNET SIGNALS	Found Within Days	16
7	CYBER UNDERGROUND	The Forums Had To Patch Too	18
8a	PHYSICAL SPOTLIGHT	The Houthi Campaign Against Saudi Arabia	19
8b	CYBER SPOTLIGHT	PHP2Shell: Did The Threat Match The Hype?	21
8c	CYBER SPOTLIGHT	The Binance Heist: Largest Crypto Theft On Record	24
	SOURCES	Numbered references	26

EXECUTIVE SUMMARY

WHERE PEOPLE AND GOODS MOVE

October's most serious threats arrived where people and goods move. A Houthi missile struck the passenger terminal of Riyadh's main airport, killing 12 people and injuring 309.[1] The airport then stayed shut for around two weeks.[2] A tanker war across the Strait of Hormuz sank a container ship,[3] and UKMTO data point to October as the worst month for attacks on shipping there since the war began.[4] Drones struck merchant ships in NATO waters off Bulgaria and Romania.[5] In France, a protest movement that began in the high schools of the Paris suburbs ended in rioting, looting and night-time curfews in the capital,[6,7] and was still bringing hundreds of thousands onto the streets on 31 October.[8]

Online, the month was defined by PHP2Shell, a pair of critical flaws in the PHP language behind much of the web. The warnings were loud and immediate. One vendor said 70% of the Internet was affected.[9] Confirmed, successful exploitation took about five days to follow.[10,11] By then the risk looked narrower than first claimed, but the first reported intrusions involved capable actors, one possibly state-linked. The month ended with the largest cryptocurrency theft on record: about US$6.3 billion drained from the Binance exchange on 29 October, which the FBI has attributed to North Korea.[12,13]

Key findings

- **The Houthis turned Saudi airports and energy sites into targets.** After declaring Saudi airspace an "open target" on 5 October,[14] the group struck Riyadh, Abha and Dammam airports and Aramco facilities. Saudi Arabia's share of the month's terrorism events rose by 3.2 percentage points. (Section 2 and Spotlight)
- **France was the month's standout mover.** Its share of protest and unrest events rose more than any other country's, as school protests escalated into nationwide rioting and curfews. Turnout fell on 31 October, but violence at the end of marches did not, and unions have called a national strike for 5 November.[8,15] France was the sharpest edge of a wider wave of youth and cost-of-living protests across Europe, from Italy and Belgium to Greece and Germany. Protest and unrest rose to 43% of Europe's security events, while conflict held steady.[16] (Section 2)
- **Shipping was hit on two fronts.** Attacks around Hormuz continued under a US blockade of Iran, at least 35 in October on UKMTO's data, the most in any month of the war.[4] In the western Black Sea, Romania blamed Russia for a drone that sank a cargo ship.[17] (Section 3)
- **Ransomware concentrated again.** The top three groups' share of victims rose from about a quarter to about 38%. Qilin almost doubled its share in the month an alleged core member was arrested in Germany.[18] (Section 4)
- **Edge devices and the web stack dominated exploited vulnerabilities.** CISA added 36 vulnerabilities to its Known Exploited catalogue, led by VPN, remote-access and email-security appliances, and by PHP. Three Ivanti Connect Secure flaws were exploited as a chain to take over VPN gateways without logging in.[19,20] (Section 5)

- **A cyber attack spoiled food in hundreds of French supermarkets.** On 11–12 October attackers took over end-of-life refrigeration controllers in at least 350 stores; nobody has claimed it.[21,22] (Section 5)
- **Exposure is found in days.** A new VPN login page on Fenestra's sensors was being probed within days of going live, mostly not by research scanners.[16] (Section 6)
- **PHP2Shell hit the criminals too.** Several criminal forums run on PHP went offline on the day of disclosure and returned only after patching.[23] (Sections 7 and Spotlight)
- **North Korea is blamed for the largest crypto theft on record.** About US$6.3 billion left Binance's online wallets on 29 October, traced back to a compromised engineer's laptop. About US$2.7 billion was frozen, but more than US$2.4 billion remains with the attackers.[12,24] On 31 October the FBI attributed the theft to North Korea's TraderTraitor unit.[13] Binance says it has replaced about 95% of the stolen tokens from its own funds.[25] (Spotlight)

Key judgements

- It is **highly likely** that the Houthis continue to target Saudi airports and energy infrastructure in November. A further mass-casualty strike on civil aviation is a **realistic possibility**.
- It is **likely** that attacks on merchant shipping around Hormuz and in the western Black Sea continue. Insurance and routing costs are **likely** to stay elevated.
- It is **likely** that PHP2Shell exploitation grows now that successful exploitation has been demonstrated, concentrated on unpatched and end-of-life PHP installations rather than "70% of the Internet".
- It is **likely** that edge devices remain the main initial-access route for ransomware groups.
- It is **highly likely** that the Binance proceeds are laundered over the coming months and that criminals exploit the theft with fake recovery and refund scams. A further large theft from a crypto platform before the end of the year is a **realistic possibility**.

What this means for boards. The month's attacks hit shared infrastructure: airports, shipping lanes and the software that runs websites. Few organisations own these, but most depend on them. Resilience planning should assume that a regional airport, a sea route or a widely used software component can be unavailable for weeks, not hours.

Probability language. Judgements use the UK Professional Head of Intelligence Assessment yardstick: remote chance (≤5%) · highly unlikely (10–20%) · unlikely (25–35%) · realistic possibility (40–50%) · likely or probably (55–75%) · highly likely (80–90%) · almost certain (≥95%). Figures cover 1–31 October unless stated; month-on-month comparisons use shares of each month's total.

GEOSPATIAL & PHYSICAL SECURITY

EUROPE RISES, THE GULF IGNITES

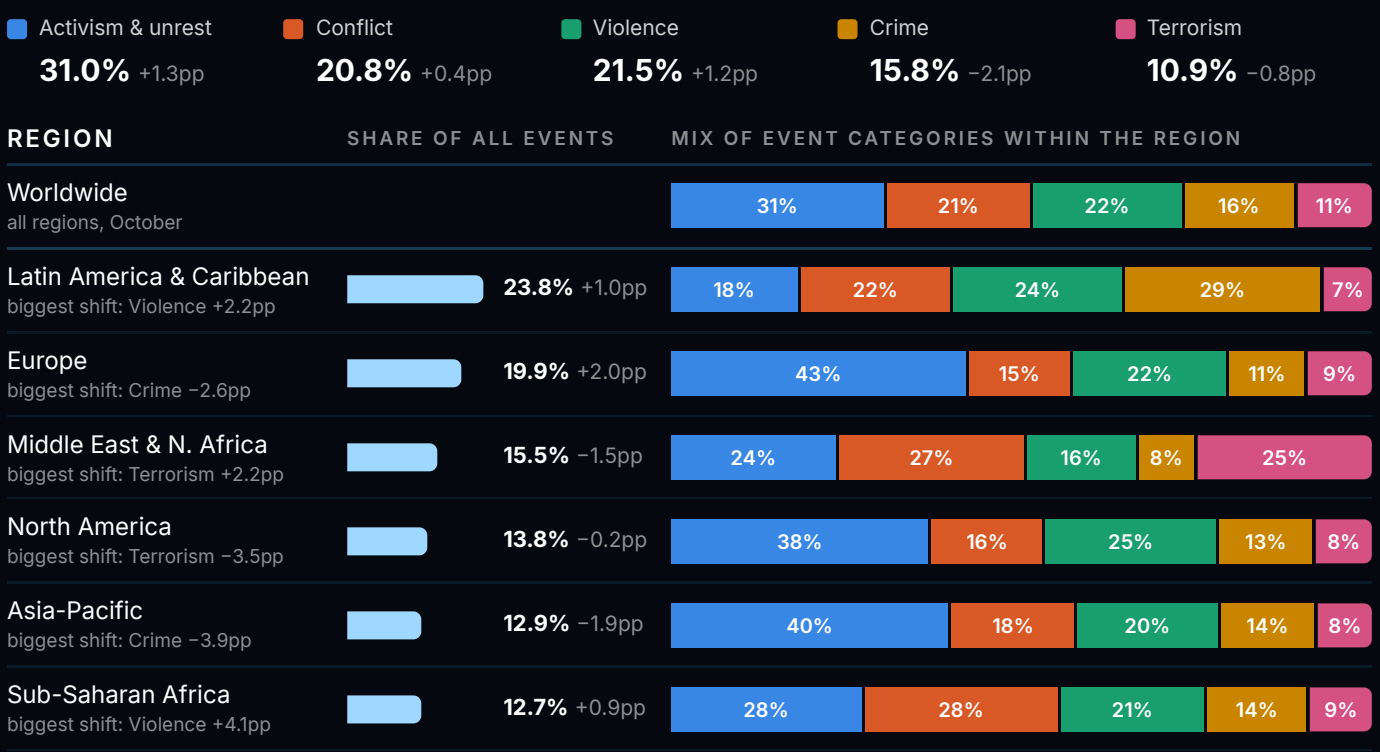


Figure 1. What kind of security events happened, and where. Legend: each category's share of all geolocated physical-security events worldwide in October (1–31 Oct 2026), with the change in percentage points (pp) since September (1–30 Sep). Left bars: each region's share of all events, with its change; the remaining 1.4% occurred at sea (Section 3). Coloured bars: how each region's own events split by category, each adding to 100%; the line under each region names its largest category shift since September. An incident is counted once however widely it was reported; changes are calculated before rounding.[16]

Geolocated security events were spread much as in September. Protest and unrest and violence gained ground, crime fell back, and conflict held broadly steady. The more telling picture is regional.

Developing threats by region

- **Europe** gained the most, rising to 19.9% of all events (+2.0 points), mostly because of France. Italy, Greece and Albania also rose as protests spread. Within the region, protest and unrest rose by 2.5 points while conflict held steady, and Ukraine's share was unchanged. Russian hybrid activity continued: Lithuania suspected Russian sabotage in an attempt to burn a Starlink site in Vilnius,[26] and drones breached the no-fly zone over France's main naval base at Toulon.[27]
- **Middle East & North Africa** slipped overall (15.5%), but terrorism's share within the region rose by 2.2 points. The centre of gravity moved to the Gulf. Saudi Arabia rose to 12.9% of the region's events (+6.6 points), level with Yemen (13.4%). Lebanon and Iran fell back.
- **Sub-Saharan Africa** (12.7%) saw violence rise within the region by 4.1 points, with Sudan, Ethiopia and Ghana among the risers.

- **Asia-Pacific** (12.9%) was led by India, with nearly half the region's events. Activism and conflict both rose within the region.
- **North America** (13.8%) slipped slightly overall. Within it, protest activity rose ahead of the US midterm elections on 3 November.
- **Latin America & Caribbean** (23.8%) remained the largest region. Brazil grew, Mexico fell back, and violence rose within the region.

Focus point: France. France's rise was driven by protest. Its share of activism and unrest events rose by 2.1 points, more than any other country's, while Spain, comparable in volume, barely moved. France also saw one terrorist attack: on 23 October a gunman firing from a car killed one person and wounded others in Trappes, west of Paris, which President Macron called a "racist terrorist attack".[28] The movement began in the high schools of Paris's deprived suburbs over school conditions.[6] By 1 October about 2,000 people had been arrested and the government had called a crisis cabinet.[29] Around 400 high schools closed the next day.[30] The Paris police chief said the movement was out of control.[31] Concessions, including 3,000 extra teachers,[32] did not stop a weekend of rioting and looting on 17–18 October.[33] Overnight curfews followed in parts of Paris and other cities.[7] The prime minister blamed "ultra-left" groups and promised a massive security deployment, including counter-terrorism police.[34,35] Curfews in parts of Paris were extended to 26 October.[36]

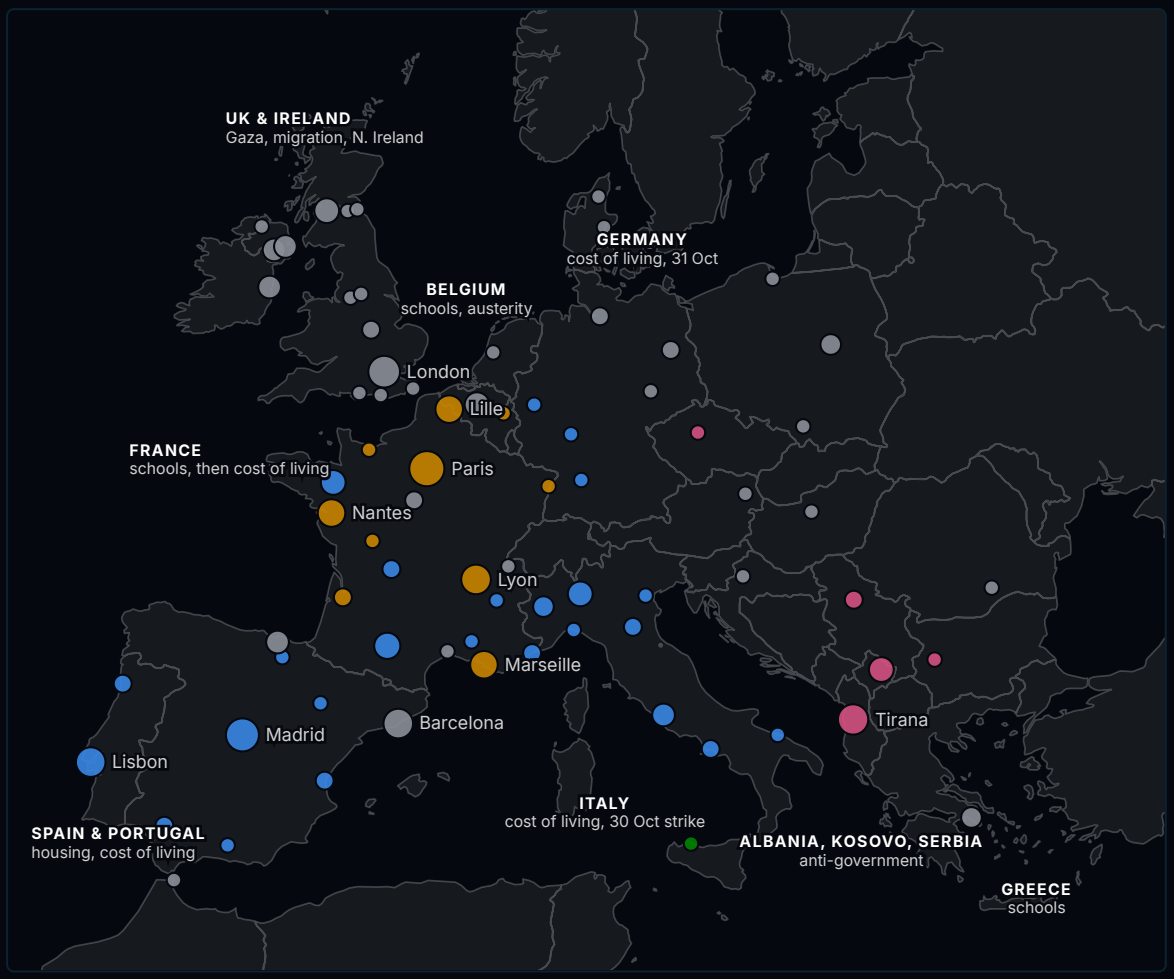
The unrest has an information dimension. False videos circulated by far-right accounts recast the protests as religious or migrant violence.[37] Macron accused foreign leaders of commenting on the riots on the strength of fake AI videos.[38] Marine Le Pen gained in the polls.[39]

31 October: smaller marches, the same violence at the edges. The third Saturday of protests drew about 320,000 people by the interior ministry's count, down from 410,000 a week earlier and 550,000 on 17 October.[8] Some 70,000 police and gendarmes were deployed, and the courts upheld a ban on the central Paris route.[40] Masked groups clashed with police as largely peaceful marches dispersed in Paris, Lyon, Marseille and other cities. A gendarme was hit by a petrol bomb, which the interior minister called attempted murder.[41] By the evening 565 people had been arrested, and five officers were injured in Paris.[15]

Beyond France: a wider European wave. France was not alone. On 17 October, the day of France's worst rioting, hundreds of thousands also marched over the cost of living in Belgium, Italy and Portugal, in separate, uncoordinated demonstrations.[42] Nearly 200 people were detained in Brussels and Liège.[43] In Milan, rioting and looting on the fringes of the marches led to 271 detentions; Italy deployed 500 soldiers to the city and moved to toughen its anti-riot laws.[44] Lorry drivers' fuel-price blockades left at least seven airports in southern Italy short of jet fuel.[45] Students marched in Greece, Spain and Portugal saw housing protests, and protests against the government ran on in Albania,[46,47] and on 31 October a youth movement brought protesters onto the streets of dozens of German cities.[48] In our data, Italy, Greece and Albania were among the risers in Europe's share of events.[16]

Protest and unrest across Europe, October 2026

Towns and cities where protests, strikes, riots or other public disorder were reported during the month, by main driver. Larger dots mean more separate events.



MAIN DRIVER OF PROTEST AND UNREST BY DAY, OCTOBER

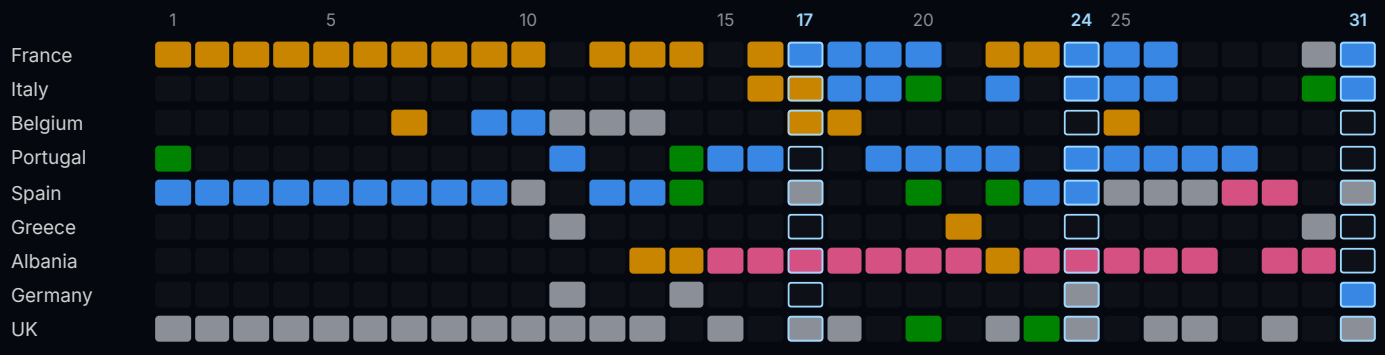


Figure 2. Where and when protest and unrest was reported in Europe, October. Map: towns and cities with protests, strikes, riots or other public disorder, coloured by the main driver of the events there and sized by how many separate events were reported (repeat reports of a place within two days count once). Timeline: each country's main driver on each day, for the countries discussed in the text and the UK. 'Other' includes Gaza and Israel, migration and the far right, Northern Ireland parades, and local causes. Ukraine, Russia, Belarus, Moldova and the South Caucasus are outside the frame. Base map: Natural Earth.[16]

Spillover or coincidence? We cannot tell how far these protests are linked to France. They share grievances: school conditions, housing, wages, and fuel and food prices pushed up by the Hormuz crisis.[46] Some protesters looked to France: Greek students were reported to be inspired by the French demonstrations,[47] and German protesters by movements in France and Italy.[48] We have seen no evidence that the protests are organised across borders. French and Italian ministers blamed foreign powers, including Russia, for inflaming the unrest on social media, and Italy is investigating, but the European Commission has said it has no evidence that foreign manipulation is driving it.[49,50] Markets took note: French bonds and the euro fell after the 17–18 October riots.[51]

The next test: 5 November. French unions called for a day of action on 5 November after talks with the government failed,[52] and the CGT called a strike from that date.[53] Through the last week of October, the CGT and La France Insoumise used their channels to build towards it.[16] UEFA moved a Europa League match because of the planned strike.[54] School and student unions also called for blockades on 3 and 5 November.[55]

FENESTRA ASSESSMENT: Further disorder in French cities in November is **likely**, because the underlying grievances are unresolved and the movement has shown it can mobilise again after concessions. Renewed rioting on the scale of 17–18 October is a **realistic possibility**. It is **highly likely** that the 5 November strike and demonstrations disrupt transport, schools and public services across France. Disorder in the larger cities around them is a **realistic possibility**. Businesses with premises or staff in affected districts should plan around curfew hours, strike days and short-notice closures. Further cost-of-living and youth protests elsewhere in Europe in November are **likely**, because the grievances behind them are shared and unresolved. Organisations operating across several European countries should plan for disruption in more than one country at once, not treat France as a one-off.
ASSESSMENT ENDS

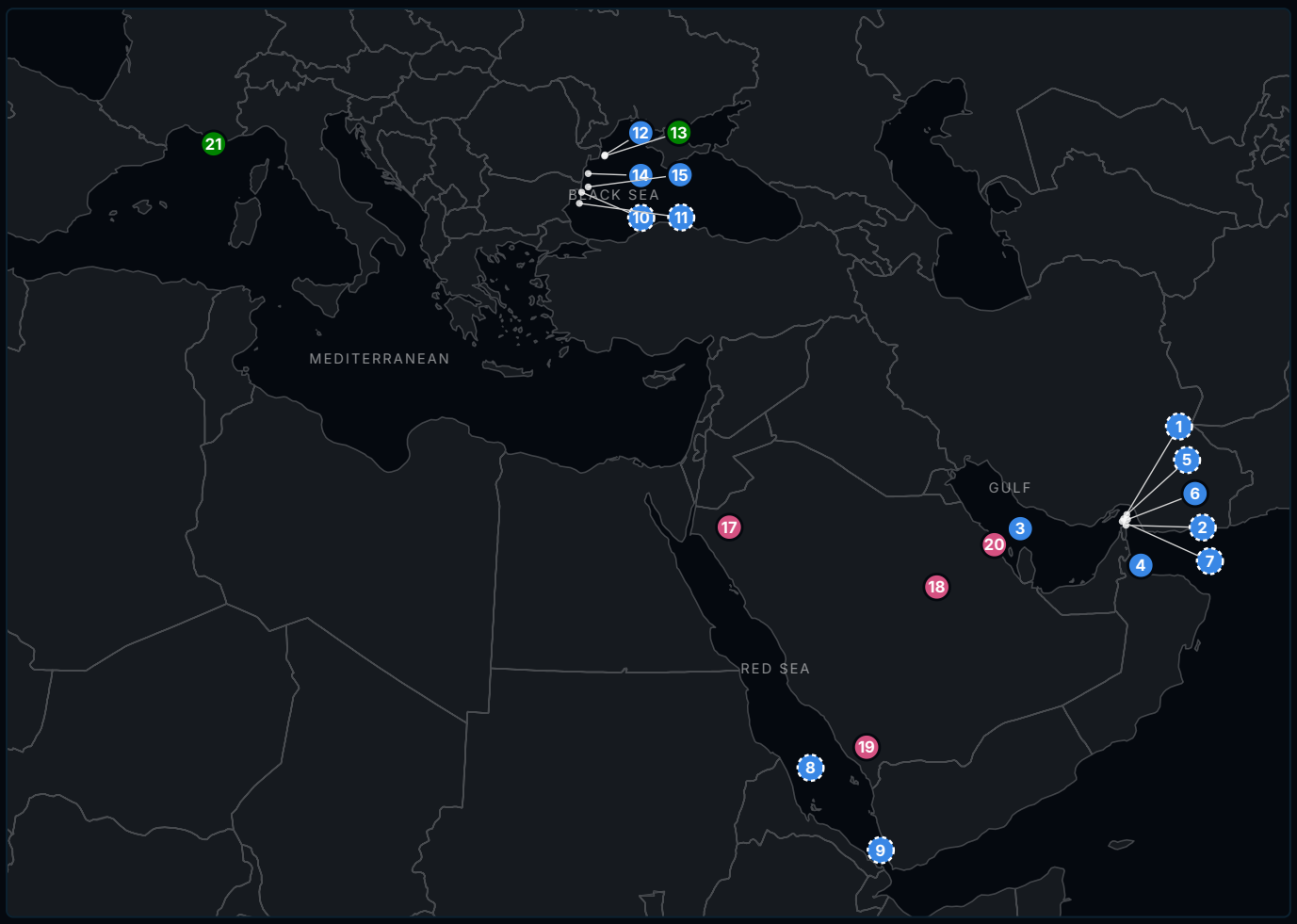
Focus point: Saudi Arabia. Saudi Arabia's share of terrorism events rose by 3.2 points, the largest rise of any country. This was driven by the Houthi campaign against its airports and energy sites, covered in the Physical Spotlight.

MARITIME & AVIATION SECURITY

A TANKER WAR AND A GROUNDED CAPITAL

Maritime and aviation incidents, October 2026

Attacks on shipping, boardings, airport strikes and drone incursions referred to in this section.



Attack on shipping · Boarding or detention · Attack on an airport or aircraft · Drone or airspace incursion · Approximate position

1. **27 Sep–2 Oct** · Six vessels hit. Strait of Hormuz (approximate) [56]
2. **5–6 Oct** · LR2 tanker hit; 12 seafarers injured. Off Musandam, Oman (approximate) [57]
3. **7 Oct** · Chemical tanker struck by projectiles. 51 nm north of Madinat ash Shamal, Qatar [58]
4. **11 Oct** · Drone strike on tanker; two seafarers missing. Sohar anchorage, Oman [59]
5. **13 Oct** · Container ship sunk (confirmed by Singapore 14 Oct). Near the Strait of Hormuz (approximate) [3]
6. **29 Oct** · Explosives attached to the hull of tanker *Louise 1.* 25 nm north-east of Khasab, Oman [60]
7. **29 Oct** · Tanker *Arzanah* hit by a projectile. Strait of Hormuz (approximate) [61]
8. **5 Oct (reported)** · Product tanker attacked. Red Sea (approximate) [62]
9. **7 Oct** · Armed small boat fires on container ship. Southern Red Sea, north of Bab el-Mandeb (approximate) [63]
10. **6 Oct** · Two ships struck by drones; one sinks. Off Bulgaria (exclusive economic zone) (approximate) [64]
11. **By 13 Oct** · Ship sunk by drone; 11 seafarers missing. Off Bulgaria (approximate) [5]
12. **14 Oct** · Tanker *Wine Trader* struck; seven missing. 13 nm south-east of Sulina, Romania [65]
13. **17 Oct** · Romanian F-16s shoot down two drones. About 13 nm south-east of Sulina [66]
14. **By 23 Oct** · Cargo ship *Khoryv* sunk; one killed, three missing. 13 nm off Constanța, Romania [17]
15. **28 Oct** · Container ship sunk by three drones; crew rescued. 21 nm off Shabla, Bulgaria [67]
16. **30 Sep–1 Oct** · Cyprus-flagged *Vasterbotten* detained. Gulf of Finland (Russian waters) (approximate); outside the map [68]

17 **30 Sep** · flydubai FZ1073 lands after co-pilot attack. Tabuk airport, Saudi Arabia[69]

18 **7–12 Oct** · Repeated strikes; terminal hit on 10 Oct, 12 killed. King Khalid International, Riyadh[70,1]

19 **7 Oct** · Strike kills two. Abha airport, Saudi Arabia[70]

20 **21 Oct** · Strike; death toll rises to two. King Fahd International, Dammam[71]

21 **5–16 Oct** · Drones breach the no-fly zone during an exercise. Toulon naval base, France[27]

Figure 3. Maritime and aviation incidents described in this section. Each pin is an incident cited in the text, placed at the position given by the source (UKMTO, navies, authorities or news reports); dashed outlines mark incidents for which only an area was given. Pins in the Strait of Hormuz and western Black Sea are spread out for legibility, with a line to the reported position. Outside the frame: pin 16 (Gulf of Finland), the French boarding of a sanctioned tanker about 450 nm south of Réunion (reported 13 Oct) and Chinese drones near Okinawa (reported 20 Oct). Base map: Natural Earth.

Strait of Hormuz: a tanker war under blockade. Attacks on merchant shipping in and around the Strait continued all month while the US enforced a blockade of Iranian oil exports.[72] Six vessels were hit between 27 September and 2 October.[56] Twelve seafarers were injured on an LR2 tanker on 5 or 6 October.[57] A tanker attack off Qatar on 7 October showed the threat reaching beyond the Strait.[58] On 11 October a drone struck a tanker at the Sohar anchorage off Oman, leaving two seafarers missing.[59] On 14 October Singapore confirmed that a container ship had sunk near Hormuz.[3] UKMTO reported that most attacks go unreported and that its alert system was being overwhelmed.[73,74] US forces disabled at least one vessel trying to run the blockade.[75] Iran claimed that tankers had hit mines, though evidence was elusive.[76] An oil spill spread along the UAE coast.[77] The IEA moved to speed up releases from oil reserves.[78] A new method appeared late in the month. On the night of 29 October a small boat attached two explosive charges to the hull of the tanker *Louise 1* off Khasab, Oman, starting an engine-room fire; the crew were unhurt and the ship continued its voyage.[60] Another tanker, *Arzanah*, was hit by a projectile the same day.[61] One analyst attributed the hull attack to Iran's Revolutionary Guard navy; this has not been confirmed.[79] UKMTO data suggest at least 35 attacks on shipping in the Gulf and the Strait in October, the worst month since the war began, with traffic through the Strait still about 70% below pre-war levels.[4]

Red Sea and Gulf of Aden. A product tanker was reported attacked in the Red Sea on 5 October,[62] and an armed boat attacked a Singapore-flagged container ship there on 7 October.[63] Risk is being priced in both directions. A Qatari LNG cargo took the rare Red Sea route to Europe,[80] while the US warned of piracy in the Gulf of Aden.[81]

Western Black Sea: attacks in NATO waters. Drones struck two merchant ships off Bulgaria on 6 October, sinking one.[64] More strikes left 11 seafarers missing near NATO waters[5] and seven missing off Romania.[65] Romanian jets shot down suspected Russian drones over its territorial waters,[66] and NATO discussed the attacks.[82] Romania blamed Russia for a drone that sank a Comoros-flagged cargo ship, killing one crew member.[17] On 28 October three drones struck a container ship off Bulgaria and it sank; all crew were rescued.[67]

Shadow fleet and the Baltic. French forces boarded sanctioned tankers in the Indian Ocean, and Russia called it "piracy".[83] A Cyprus-flagged vessel was detained while passing through Russian waters in the Gulf of Finland.[68] A trial over the 2022 Nord Stream sabotage opened in Germany.[84]

Maritime cyber: new detail on a summer incident. US officials were reported in October to have found evidence that hackers accessed the propulsion system of the US-bound supertanker *VL Prosperity*.[85] This is not a new incident. The US Coast Guard and FBI boarded the ship in the Gulf of Mexico in late August

after indications that its network had been compromised.[86] It is also separate from the *Vivit Africa LNG* incident covered in our September report. What is new is the reported reach of the intrusion: into the ship's propulsion, not just its business systems. The claim rests on anonymous officials. How long the hackers had access, what they could control and who was responsible remain unclear, and the FBI said there had been no operational disruption.

> **FENESTRA ASSESSMENT:** It is **likely** that attacks on merchant shipping around Hormuz continue in November while the blockade holds. It is a **realistic possibility** that drone strikes on shipping off Bulgaria and Romania recur. Under-reporting of attacks means operators should treat the absence of alerts as an absence of information, not of risk. **ASSESSMENT ENDS**

Aviation. The Houthis declared Saudi airspace an open target and struck the airports at Riyadh, Abha and Dammam (see Spotlight).[14] EASA widened its conflict-zone warning to Riyadh and Dammam.[87] Lufthansa, Air India, Etihad and Qatar Airways suspended Saudi services,[88,89] and Delta postponed its Saudi launch to 2027.[90] The restrictions fell at a bad time for Europe–Asia routings.[91] Elsewhere, drones breached the no-fly zone over the Toulon naval base,[27] and Japan scrambled fighters as Chinese drones flew near Okinawa.[92]

flydubai FZ1073: a mass-casualty attack narrowly averted. On 30 September the co-pilot of a flydubai Boeing 737 flying from Dubai to Tel Aviv attacked the captain with the cockpit's crash axe and tried to take control of the aircraft.[93] The aircraft plunged around 17,000 feet in under two minutes.[94] The wounded captain opened the cockpit door. Passengers and crew subdued the co-pilot and helped stabilise the aircraft, which diverted to Saudi Arabia.[69,95] More than 170 people were on board, most of them Israeli.[95] The investigation's findings came out through October. The UAE prosecutor general called it an attempted terrorist attack. He said the co-pilot, an Omani national, had planned to crash the aircraft into Tel Aviv's airport and had been inspired by the 11 September 2001 attacks.[96] He had reportedly been barred from flying in Oman over extremist views before flydubai hired him.[93] Investigators reportedly believe he first planned the attack for July.[97] flydubai suspended its Israel flights,[95] and Israel ordered a review of the security of foreign airlines flying to Israel.[96] Al-Qaeda publicly praised the attack and called for more.[98] Within 48 hours, at least 25,000 posts on X pushed conspiracy theories about it.[99]

Much of this is still unverified. The plot details come from UAE prosecutors' statements and anonymous officials, and no trial has taken place. No link to a state or organised group has been shown. Israel's prime minister said it was too early to say who was behind it.[95] The UAE said the co-pilot had passed the required employment and security checks.[96] How someone barred in one country came to fly for an airline serving Israel is the central open question.

> **FENESTRA ASSESSMENT:** Attacks by serving flight crew are rare. This one was stopped by the people on board, not by vetting. It is **likely** that the case leads to tighter aircrew vetting and more sharing of information between countries, especially for airlines flying to Israel. Al-Qaeda's praise increases the risk of copycat attempts. Even so, a similar attack on a commercial flight in the next three months is **unlikely**, but its consequences would be severe. **ASSESSMENT ENDS**

Aerospace supply chain. A cyberattack through an external IT service provider forced Egide, a French aerospace and defence electronics supplier, to partly suspend operations at its Bollène plant from 6 October.[100] In mid-October the company had not yet established what data, if any, was affected.

RANSOMWARE

QILIN DOUBLES DOWN

38%
of victims claimed by just three groups
September: 25%

16%
claimed by Qilin alone, almost double its share
September: 9%

36%
of victims were in the United States
September: 32%

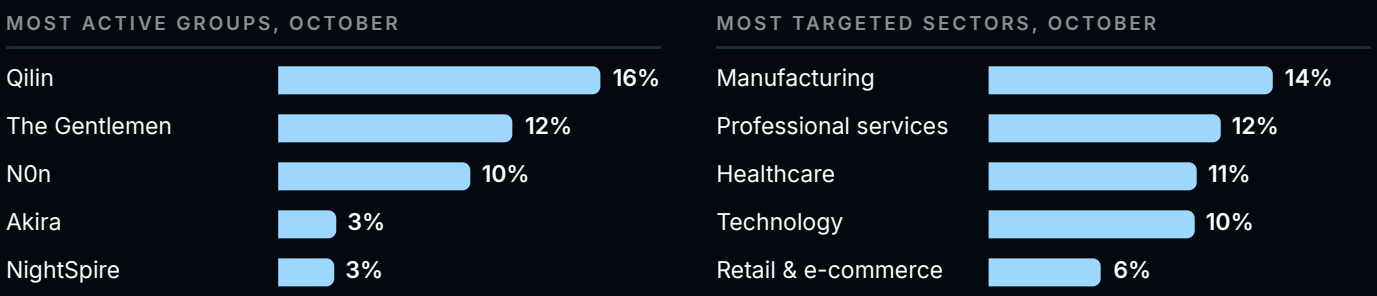


Figure 4. Ransomware in October at a glance. Shares of all victims named on ransomware leak sites, 1–31 October 2026; September figures as published in our September report. N0n's batch of three dozen port and logistics victims posted on 12 October is counted as one event. Sector shares are of all victims, including those whose sector could not be identified.[16]

Ransomware leak sites named considerably more victims than in September, and activity became markedly more concentrated. The top three groups accounted for about 38% of victims, up from about a quarter. Qilin alone took 16%, almost double its September share, in the same month that Germany arrested an alleged core member of the group after extradition from Japan.[18] The arrest has not visibly slowed the group's leak-site output. The Gentlemen, September's leader, finished second with 12%. A fifth of its October total came in a single burst on 31 October: 50 victims from more than 20 countries, posted within twenty minutes.[16] That points to a backlog published at once rather than a sudden surge in attacks, although leak sites do not show when each intrusion took place.

N0n was third. On 12 October it posted three dozen port and logistics organisations within two hours, almost certainly the result of a single compromise of a shared supplier. We count that batch as one event. Even so, N0n's share was almost 10%. The United States accounted for 36% of victims, and manufacturing remained the most affected sector.

The FBI and CISA warned that SafePay has hit more than 600 organisations since 2024.[101] Incident responders described Akira intrusions that relied on legitimate remote tools rather than malware,[102] and access brokers moving through network-edge devices.[103]

FENESTRA ASSESSMENT: It is **likely** that Qilin remains among the top three groups in November despite the arrest, because its affiliate model does not depend on a single operator. Supplier-level compromises that surface as dozens of victims at once, as with N0n, are **likely** to recur in sectors that share a small number of IT providers, such as ports and logistics. **ASSESSMENT ENDS**

VULNERABILITIES & EXPLOITATION

THE EDGE AND THE STACK

CISA added 36 vulnerabilities to its Known Exploited Vulnerabilities catalogue in October, compared with 43 in September.[19] Two clusters dominated. The first was the network edge: VPN, remote-access, email-security and SD-WAN products from Fortinet, Citrix, Ivanti, Palo Alto Networks, Cisco, BeyondTrust and Arista. The second was the web application stack, led by PHP itself.

Five to act on now

VULNERABILITY	WHAT IS EXPLOITED	STATUS
PHP2Shell CVE-2026-109618, -109619	Remote code execution in PHP's request handling	Patched 21 Oct; KEV 26 Oct; successful exploitation reported from 24 Oct (see Spotlight)
Ivanti Connect Secure CVE-2026-104935, -111357, -118527	Chained authentication bypass, code execution and privilege escalation: root on the VPN gateway without logging in	KEV 13 and 30 Oct; exploited as a zero-day chain[104,20]
Palo Alto Networks PAN-OS CVE-2026-0322	Code injection	KEV 14 Oct; separate active exploitation of CVE-2026-0257 reported[105]
BeyondTrust Remote Support CVE-2026-102764	Message-origin flaw allowing file operations on the appliance	KEV 16 Oct; exploited as a zero-day by a suspected China-linked espionage group[106]
Adobe Commerce / Magento CVE-2026-48356	Unrestricted file upload	KEV 27 Oct; e-commerce sites ahead of peak trading

End-of-month additions. In the last week CISA added flaws in Cisco Secure Firewall ASA and FTD software (a denial-of-service flaw Cisco says was exploited this month) and GitLab (unauthenticated code execution through a crafted CI/CD configuration; an attempt against Alpine Linux in October failed),[107] as well as VMware ESX and the Linux kernel.[19]

Old flaws, still exploited. On 8 October CISA added flaws in ProFTPD, ISC BIND and Apache Struts dating from 2015 and 2016, alongside ONLYOFFICE and Strapi. Their addition means attackers are still finding and using unpatched legacy servers.

Backup and media software. Two AhsayCBS backup flaws and four Plex Media Server flaws were added. Backup systems are a prized ransomware target. Home media servers have previously been an entry point into corporate networks via employees' home networks.

Beyond the catalogue. PHP disclosed a further, separate remote code execution flaw (CVE-2026-115560) on 23 October, before a fix was available,[108] and a Brotli flaw dubbed "HTTP2Shell" (CVE-2026-111497) was added to KEV on 27 October. Drupal warned that a highly critical access-bypass flaw in its Commerce Core module (CVE-2026-118539), used on more than 42,000 sites, was being exploited against online stores.[109]

When old controllers become a supply risk. Overnight on 11–12 October, attackers took control of refrigeration controllers in French supermarkets and remotely triggered defrost cycles or overrode temperatures, spoiling fresh food.[21] By 13 October at least 350 stores were affected, across chains including Intermarché, Coopérative U, Carrefour and Monoprix.[22] Paris prosecutors said the attack also caused fires.[110] The controllers were made by Danfoss, which said many affected units had reached end of life, no longer received security updates or were running outdated firmware.[22] The attack appears to have relied on weaknesses known for months rather than a new flaw. No group had claimed it and no ransom had been demanded, which investigators found unusual.[22] Its link, if any, to the unrest in France at the time is unknown.

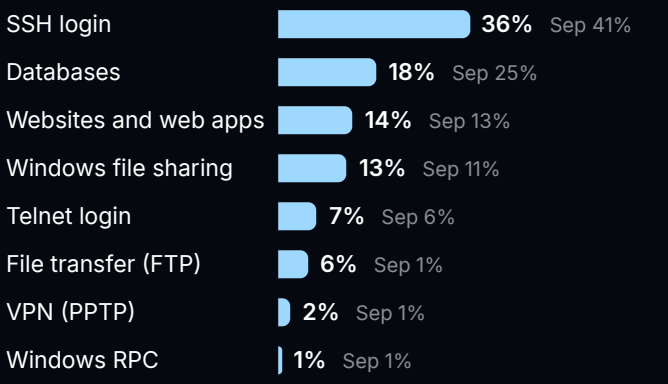
What Fenestra is tracking. Fenestra's sensors already carry detection for probing of Citrix NetScaler, Ivanti Connect Secure, PAN-OS, Fortinet, Cisco SD-WAN and PHP2Shell. Following the BeyondTrust zero-day, we added BeyondTrust Remote Support detection at the end of October. Results will be reported in November. Panoptic matches each new KEV entry against the technology monitored for each client.[16]

FENESTRA ASSESSMENT: It is **highly likely** that edge devices remain the most exploited category in November. The re-listing of decade-old flaws makes it **likely** that attackers are scanning for forgotten, unmanaged systems as deliberately as for new vulnerabilities. Asset inventory is as important as patch speed. Further attacks on internet-connected building and refrigeration controls are a **realistic possibility**, because the French case showed how cheaply end-of-life equipment can be used to cause physical disruption. **ASSESSMENT ENDS**

INTERNET SIGNALS

FOUND WITHIN DAYS

SERVICES PROBED, OCTOBER



WHERE PROBING CAME FROM, OCTOBER

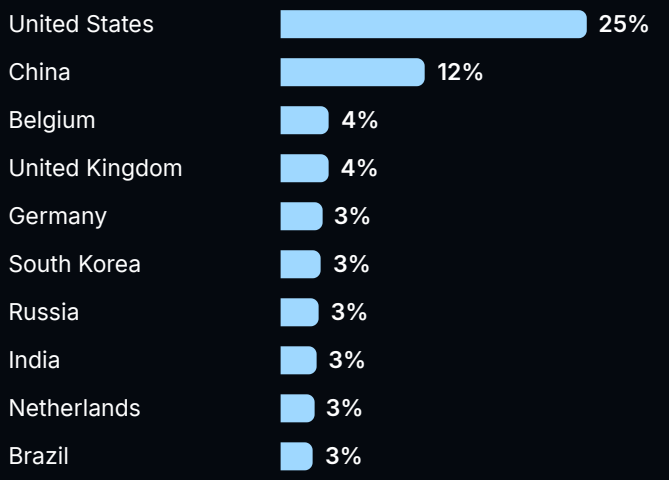
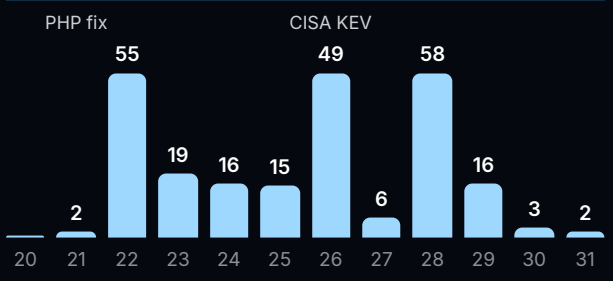


Figure 5. What was probed, and from where. Left: each service's share of all probes recorded by Fenestra's sensors in October (SSH and Telnet sessions, other connections, industrial-control sessions), with the late-September share for comparison. Right: share of the distinct internet addresses that probed the sensors in October, by the country where the address is hosted, after removing 1,218 addresses identified as known research scanners. Hosting country is not the attacker's nationality: much probing runs through rented servers and compromised machines.[16]

PHP2SHELL PROBES PER DAY, FROM 20 OCTOBER



AVERAGE PER DAY, SELECTED SIGNATURES

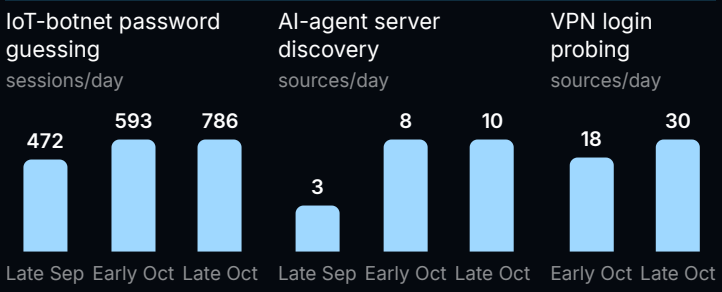


Figure 6. Activity for signatures Fenestra tracks. Left: connections per day matching our PHP2Shell signature; the PHP fix was published on 21 October and CISA listed the flaws as exploited on 26 October. Right: average per day in comparable periods: password guessing typical of IoT botnets (sessions), and the number of distinct addresses looking for exposed AI-agent servers and for our VPN login decoy (live from 3 October, so no September figure).[16]

Fenestra runs its own internet sensors, which present decoy services to the internet and record what is sent to them. They show what attackers try, not whether those attempts would succeed against a real system.

Exposure is found in days. In early October we added a decoy VPN login page of a type widely targeted by attackers. Within days it was being probed by about 18 distinct addresses a day, rising to about 30 a day in the second half of the month. Only around a quarter of that traffic came from known research scanners, and the rest included direct requests for the login and login-check pages.[16] Any newly exposed remote-access service should be assumed to be discovered within the week.

Botnet credential-stuffing in bursts. Credential guessing typical of IoT botnets rose from about 8% of SSH and Telnet sessions in late September to 14% in the second half of October. It arrived in short, one-day bursts on 6, 20 and 28 October. In the latest window, almost half of these sessions came from two web-hosting servers in the US. Both run the control-panel, mail and database services typical of hosting servers. One hosts a legitimate organisation's website and email, so it is very likely compromised. We cannot see how either server was compromised. The servers themselves, not just the websites on them, are being reused as attack infrastructure.[16]

Industrial protocols probed daily. Our industrial-control decoy recorded around 60–70 sessions a day in October. IEC-104 (used in electricity-grid control) and Modbus were the most probed protocols, with Modbus in the lead in the second half of the month, ahead of Siemens S7 and SNMP.[16]

AI-agent discovery widens. Requests looking for exposed AI-agent servers (Model Context Protocol endpoints) came from more than 100 distinct addresses in the first half of October, up from about 20 in late September.[16]

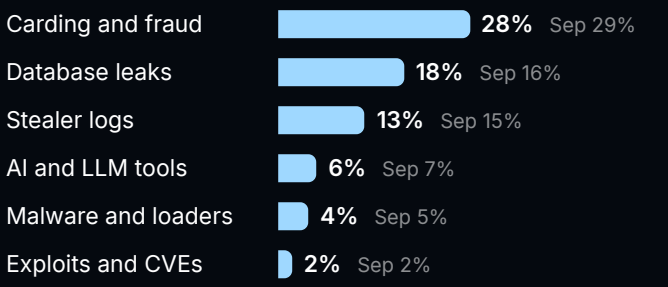
PHP2Shell. Probing for PHP2Shell began before the patch was published. It peaked on 26 and 28 October, after exploitation was confirmed, then eased in the last days of the month (see Spotlight).

Shifting service mix. Database-server (MSSQL) traffic fell as a share of connections through the month, after a distributed brute-force campaign in the second week of October ended. Web traffic rose.[16]

CYBER UNDERGROUND

THE FORUMS HAD TO PATCH TOO

WHAT UNDERGROUND FORUMS DISCUSSED, OCTOBER



SOCIAL POSTS VS UNDERGROUND FORUMS MENTIONING A VULNERABILITY, OCTOBER

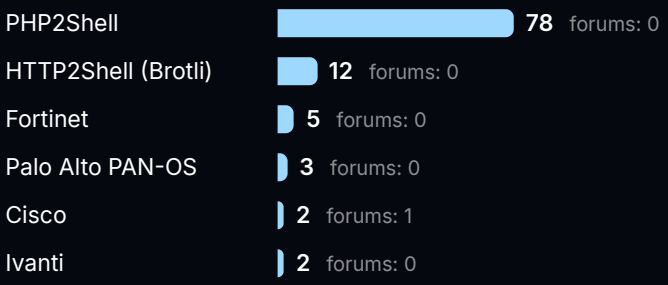


Figure 7. Underground discussion: what was talked about, and where. Left: share of posts on the main underground forums we monitor that touch each theme (a post can touch several), averaged across forums so that no single forum dominates; late-September share for comparison. Right: posts mentioning the month's high-profile vulnerabilities on open social channels (bars) against underground forums: 105 against 1 in total. A post counts if it names the vulnerability or quotes its CVE number; for vendor products, it must name the product and either quote one of October's CVE numbers for it or refer to a vulnerability, exploit or patch. Social-channel counts run from 18 October, covering the whole PHP2Shell period.[16]

PHP2Shell reached the forums themselves. Many criminal forums run on PHP. On 21 October, the day of disclosure, several went offline.[23] Our monitoring saw at least two major English-language forums become unreachable for around half a day. One returned stating that it had patched PHP2Shell and other vulnerabilities.[16] The people who sell exploits had to patch like everyone else. Exploit and access offers specific to PHP2Shell remained rare through the month. Every post naming PHP2Shell that we collected was on open social channels. None was on the criminal forums (Figure 7).[16]

Fraud and leaks dominated. Carding and fraud remained the largest single theme, at around 28% of forum posts. Database leaks grew to about 18%, from 16% in September. On one major leak forum, more than a third of posts concerned leaked databases. Stealer logs and combolists remained a staple, at about 13%.[16]

AI cooled from September's peak. AI-related discussion fell back to under 6% of posts, from almost 7%, and fell on the two largest forums after September's surge. It has not disappeared: stolen AI and cloud API keys and "jailbroken" model access continue to be offered.[16]

Vulnerability talk happened in the open. The month's high-profile flaws were discussed almost entirely on open social channels. Posts naming them there outnumbered criminal-forum posts by more than fifty to one. Exploit and CVE talk on the forums stayed marginal, at about 2% of posts. Where WordPress appeared on the forums, it was mainly in sales of stolen website-administrator logins, not as a vulnerability.[16]

Forum trust remains low. The best-known dark-web discussion forum's address continued to serve a takeover page all month. Users have no reliable way to tell a genuine relaunch from a law-enforcement or rival operation.

PHYSICAL SPOTLIGHT

THE HOUTHI CAMPAIGN AGAINST SAUDI ARABIA

The Houthis' October campaign against Saudi Arabia was the most serious sustained attack on Gulf civil aviation in years. It came as Saudi-backed Yemeni government forces opened a counter-offensive, and Riyadh said there would be no truce until the government regained territory.[111]

Timeline of the main strikes on Saudi territory



1 Oct	**Madinah power station** · Drone attack, according to the Saudi-led coalition; the Houthis denied targeting holy sites[112]
3 Oct	**Aramco facility south of Riyadh** · Fire and smoke seen; Houthi claim, called misleading by the coalition[113]
5 Oct	**Saudi airspace** · Houthis declare it an "open target", holy sites excepted, and warn airlines[14]
7 Oct	**Riyadh and Abha airports** · Three foreign nationals killed, dozens injured[70]
8–9 Oct	**Riyadh airport** · Aircraft damaged; a Saudia pilot among three killed[114,115]
10 Oct	**Riyadh airport passenger terminal** · 12 killed, 309 injured (Saudi civil aviation authority)[1]
11–12 Oct	**Riyadh airport** · Fresh strike: one killed, 11 injured; suspension extended[116]
14 Oct	**Aramco, Eastern Province** · Aramco site hit as attacks were exchanged[117]
21 Oct	**King Fahd Airport, Dammam** · Death toll rose to two[71]
24 Oct	**Yanbu and Taif** · Missiles towards the Red Sea oil terminal intercepted[118]
25 Oct	**Riyadh airport** · Flights resume after about two weeks[2]
27–28 Oct	**Ras Tanura** · Houthi claim on Aramco's terminal; oil prices rise[119,120]
30–31 Oct	**Saudi airspace: Riyadh, Madinah, Eastern Province, the south** · Drones and a ballistic missile intercepted; debris fell in Riyadh without injuries[121,122]

By 16 October the coalition counted 17 killed and more than 330 injured in attacks on Riyadh airport alone.[123] Later reports put the death toll from the 10 October terminal strike at 13.[121] Interception debris also damaged a kindergarten and a medical centre in Riyadh.[124] Iran denied directing the attacks.[125] Inside Yemen, Houthi strikes included a missile attack that killed around 50 recruits at a government camp.[126] On 30 October the Houthis fired missiles at the presidential palace and the airport in Aden, seat of the internationally recognised government.[127]

The response widened the conflict. Turkey announced troop and air-defence deployments to Saudi Arabia,[128] Egypt approved sending troops,[129] and the UK deployed Typhoon jets.[130] The US ordered some diplomats to leave the kingdom.[131] Saudi Arabia postponed major events.[132]

Security resilience: where the exposure is

SECTOR	EXPOSURE SHOWN IN OCTOBER	RESILIENCE PRIORITIES
Aviation and airports	Terminal strike, a two-week closure of the capital's airport, damaged aircraft, airline suspensions	Alternative routings and hubs, travel approval for staff, shelter-in-place plans at airports
Energy	Madinah power station, Aramco sites, the Yanbu terminal targeted, Ras Tanura claimed	Site protection, contractor safety, continuity plans for supply interruption
Ports and shipping	Military options weighed to protect Yanbu;[133] Red Sea and Gulf attacks (Section 3)	War-risk cover, routing decisions, crew welfare
Staff and travellers	Foreign nationals among the dead; diplomatic departures	Duty-of-care tracking, evacuation plans, embassy registration
Events and hospitality	Major events postponed	Contingency dates, crowd-safety and insurance planning

Supply-chain effects. The closures and airspace restrictions disrupted Europe–Asia air routings,[91] with knock-on effects for air freight through Riyadh and Dammam. Oil prices reacted to the strikes,[120] and shipping through the Red Sea and Gulf faces higher risk and cost. Organisations dependent on Gulf energy, air cargo through Saudi hubs or Red Sea routes should review contingency stock and alternative routes.

> **FENESTRA ASSESSMENT:** It is **highly likely** that the Houthis continue to strike Saudi airports and energy sites in November, because the campaign has drawn a large international response without being halted. A further strike causing mass casualties at a civil airport is a **realistic possibility**. Short-notice closure of Saudi airports and airspace should be treated as a planning case, not a remote scenario. **ASSESSMENT ENDS**

CYBER SPOTLIGHT

PHP2SHELL: DID THE THREAT MATCH THE HYPE?

PHP2Shell is the name given to two critical flaws in PHP (CVE-2026-109618 and CVE-2026-109619), the language behind a large share of the web. Details leaked before the fixes were published on 21 October.[134] The question for defenders was not whether the flaws were serious, but how quickly and how widely they would be used.

PHP2Shell, 20–31 October: from alarm to confirmed exploitation



17 Oct	Exploitation attempts began four days before the patches, Amazon later said[135]
20 Oct	Exploit details leak publicly, the evening before the fixes[16,134]
21 Oct	PHP publishes fixes; CISA urges immediate patching; SANS raises its threat level[136,137]
21 Oct	"70% of the Internet" affected (Wiz); "attacks ongoing" (Patchstack)[9,138]
22 Oct	"One in ten organisations impacted", meaning targeted, not compromised (Check Point)[139]
23 Oct	First weaponised attempt on Fenestra's sensors (RedTail botnet), about 41 hours after the advisory; success unknown[16]
23 Oct	CrowdStrike: obstacles to weaponising; "millions of attacks, no confirmed successful exploits"[140,10]
23–24 Oct	24 firewalls rooted by chaining PHP2Shell with a Linux flaw; reported 28 Oct, actor unnamed[141]
24 Oct	Working shells on a researcher's deliberately favourable decoys; reported 26 Oct[142,11]
24 Oct	Many people mistaking old exploits for PHP2Shell (Marcus Hutchins)[143]
26 Oct	CISA adds both flaws to its Known Exploited Vulnerabilities catalogue[19]
26 Oct	Unit 42 retracts an update linking a government intrusion to the flaws[144]
26 Oct	Suspected North Korean group checks 216 hosts; no compromise confirmed[145]
27 Oct	CISA confirms exploitation in attacks, without details[146]

Figure 8. PHP2Shell: claims, doubts and confirmed exploitation. Top: dated events from the sources cited in this spotlight, by type (dates are when the event happened; some were reported later). Bottom: connections per day matching Fenestra's PHP2Shell signature. A sensor records attempts; it cannot show whether an attempt would have succeeded.[16]

The alarm (21–22 October). On the day of disclosure, one vendor said the flaws affected 70% of the Internet.[9] Another said attacks were already under way.[138] CISA urged immediate patching,[136] and the SANS Internet Storm Center raised its threat level.[137] Amazon said exploitation attempts had begun four days before the patches.[135] Check Point reported that one in ten organisations had been "impacted",[139] meaning targeted rather than compromised. One commentary called it "Log4Shell at AI speed".[147]

The gap (23–25 October). Within two days the tone changed. CrowdStrike assessed that obstacles to weaponising the flaws would likely constrain immediate widespread exploitation.[140] Experts downplayed the viability of the available exploits,[148] and SANS questioned whether exploitation was reliable.[149] One headline summed it up: millions of attacks, no confirmed successful exploits.[10] Marcus Hutchins noted that many people were mistaking old exploits for PHP2Shell.[143] Unit 42 later retracted an update that had linked a European government intrusion to the flaws.[144] Meanwhile Mirai botnet operators joined in,[150] and PHP warned of a further, unpatched flaw.[108]

First confirmed exploitation (24–28 October). The first well-evidenced success came from a researcher's own decoy servers. On 24 October they recorded working shells, reported on 26 October, five days after the patches.[142,11] The decoys used a configuration deliberately favourable to the exploit, and the researcher warned that this said nothing about reliability elsewhere. CISA added both flaws to its Known Exploited Vulnerabilities catalogue[19] and confirmed exploitation in attacks, without publishing details.[146] On 28 October a security firm reported that an actor had chained PHP2Shell with a Linux privilege-escalation flaw. The actor rooted 24 firewalls from one vendor on 23–24 October and went further into one US government-affiliated network.[141] The firm did not name the actor. Its China link rests on the choice of target countries, not on shared tools or infrastructure. Separately, a suspected North Korean group was reported to be checking 216 possibly unpatched hosts. No compromises from that activity have been confirmed, and the attribution is moderate-confidence.[145]

What our sensors saw. Fenestra's sensors recorded PHP2Shell probing from before the patch was published.[16] Most early traffic came from self-identified scanning tools and lightly modified public proof-of-concept code: tests, not attacks. The first weaponised payload arrived about 41 hours after the advisory. It came from the RedTail cryptomining botnet (also labelled Prometei), which had already been active against our SSH sensors, and it tried to fetch and run its installer. That was days before public reports of confirmed exploitation. A decoy records attempts. It cannot show whether an attempt would have worked against a real server, and we have no evidence that RedTail's did. Activity did not fade after launch week. Tagged connections reached new peaks on 26 and 28 October, after the confirmation news, before easing in the last days of the month. Dozens of distinct sources had probed our sensors by month end.[16]

The criminals had to patch too. Many criminal forums run on PHP. Several went offline on the day of disclosure,[23] and at least one returned only after announcing that it had patched.[16]

So, did the threat match the hype? Not in the first week. The scale claims described exposure, not exploitation. Turning the flaws into reliable code execution was harder than the headlines suggested, and depended on specific PHP versions and configurations. But the gap was days, not months. Botnet

operators were sending weaponised attempts within two days, although their success has not been confirmed. The first well-evidenced intrusions followed within a week, including a firewall campaign that one firm links, on limited evidence, to China-nexus actors.

> **FENESTRA ASSESSMENT:** It is **likely** that PHP2Shell exploitation grows through November, concentrated on unpatched and end-of-life PHP installations and on appliances that embed PHP. It is **unlikely** to reach the "70% of the Internet" scale first claimed. Organisations that patched in the first week are in a strong position. Those relying on the early "no confirmed exploitation" reporting are not.
> **ASSESSMENT ENDS**

What to do. Patch PHP to the fixed releases, including PHP builds bundled in appliances and hosting panels. Retire end-of-life PHP branches. Check web logs for unusually large multipart requests to PHP endpoints using upload-progress fields. Track PHP's separate advisory for CVE-2026-115560.

CYBER SPOTLIGHT

THE BINANCE HEIST: LARGEST CRYPTO THEFT ON RECORD

On the evening of 29 October, attackers moved about US$6.3 billion out of the cryptocurrency exchange Binance, the world's largest.[12] It is the largest crypto theft on record, about four times the US$1.5 billion stolen from Bybit in February 2025, which was previously the largest.[24] Binance says customer funds were not affected. The losses came from the exchange's own "hot" wallets, which are kept online to process withdrawals. Binance has pledged to cover them in full.[151] By 1 November it said it had replaced about 95% of the stolen tokens with company funds, the rest being less liquid assets, and that it would begin a phased resumption of withdrawals that day.[25]

Twenty minutes, ten blockchains. The outflows began at about 20:05 GMT. Most of the money left within around 20 minutes, across ten blockchains.[24] The attack was prepared at least a day and a half in advance. The operating wallet was funded through a cryptocurrency mixer, and the malicious code was tested on other wallets first.[152] On Ethereum, the attackers had a Binance wallet sign, in advance, a batch of 50 permissions that handed its control to a contract only they could command. On the other nine chains, Binance's own wallets sent the funds through normal, validly signed transactions, all within about half an hour. That pattern points to access to the exchange's signing systems, not to a single stolen key.[152]

How they got in. Binance's first account traced the breach to a DevOps engineer's compromised laptop. That gave access to a service container from which unauthorised withdrawals could be submitted. Binance said it had found no evidence that any wallet's private key had leaked.[24] It has since found "additional points of breach". It says the attacker used a self-destruct mechanism that erased tools and traces.[151] The full picture is not yet public, and Binance has promised a technical post-mortem.

The race to freeze. Stablecoin issuers and blockchain operators froze about US$2.7 billion within hours, among them Tether, Circle, Ripple, World Liberty Financial and Arbitrum. The attackers raced them, selling stablecoins and borrowing against other stolen assets. They were left holding more than US$2.4 billion in Ether and Bitcoin, which cannot be frozen.[12,24] Binance suspended withdrawals, including in Brazil,[153] and set aside US$6.34 billion of company funds to cover the losses. It promised a proof-of-reserves report so the public can check its holdings.[151] Bitcoin fell by up to 2% and Ether by more than 3% the next morning.[154]

Who did it. Two blockchain-analysis firms, TRM Labs and Chainalysis, attribute the theft "with high confidence" to TraderTraitor. This is a North Korean state-backed unit also known as Lazarus Group or APT38. Stolen funds were seen mixing in wallets with proceeds of last month's US$387 million theft from the Bitget exchange, which is also blamed on North Korea.[12,155] The FBI blamed the same group for the Bybit theft.[12] The attribution began with private analysts tracing funds on-chain. On 31 October the FBI confirmed it: it said North Korea was responsible, that TraderTraitor actors were converting the stolen assets into Ether, and urged companies to block transactions linked to the laundering addresses.[13] President Trump has said the US is not yet certain.[156] The FBI and the US Secret Service are working with the exchange.[157]

What Fenestra's collection shows. Public warnings appeared on social media within about half an hour of the first outflows. That was roughly an hour before Binance's first statement, which spoke only of a "potential security issue".[16,158] By 1 November we had seen no discussion of the theft on the criminal forums we monitor. Attackers on this scale have no need to sell what they took on the forums; their problem is laundering it. Separately, the prediction market Polymarket paused trading the same evening after a compromised third-party script drained about US$2.5 million from users.[159] No link between the two has been shown.

FENESTRA ASSESSMENT: It is **highly likely** that the attribution to North Korea holds. The FBI's finding matches the scale, tradecraft and fund-mixing of the group behind the Bybit theft. It is **highly likely** that the unfrozen funds, more than US$2.4 billion, are laundered over the coming weeks and months through cross-chain bridges, mixers and over-the-counter brokers. Little of that balance is **likely** to be recovered. It is **highly likely** that criminals exploit the incident with fake "recovery", refund and support scams aimed at Binance customers. A further large theft from a crypto platform before the end of the year is a **realistic possibility**. The same group has struck repeatedly, including Bybit last year and KelpDAO and Bitget this year,[12] and North Korea is accused of relying on cybercrime to finance itself.[155]
ASSESSMENT ENDS

What it means beyond crypto. The entry point was an engineer's laptop, not a flaw in a blockchain. Any organisation where a developer or operations engineer can reach systems that move money should assume those people are being targeted. That covers payment platforms, treasury systems and signing services. The defences are separating developer access from production signing, adding independent approval and rate limits on large or unusual transfers, and monitoring developer endpoints as closely as servers.

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 (2 November 2026); some situations described, including ongoing investigations, may have developed since publication.

1. Arab News — Riyadh airport attack killed 12 people and wounded over 300 more, says Saudi civil aviation agency (10 Oct).
https://www.arabnews.com/saudi-arabia/riyadh-airport-attack-killed-12-people-and-wounded-over-300-more-says-saudi-civil-aviation-agency-3005640

2. The Hindu — Riyadh airport resumes flights following Houthi attacks (25 Oct).
https://www.thehindu.com/news/international/riyadh-airport-resumes-flights-following-houthi-attacks/article71622578.ece

3. Seatrade Maritime News — Update: Singapore confirms container ship sunk in Hormuz amid fresh Iran attacks (14 Oct).
https://www.seatrade-maritime.com/security/iran-claims-mine-sank-container-ship-amid-fresh-hormuz-attacks

4. Middle East Eye — Hormuz shipping traffic remains 70% below pre-war levels, UKMTO says (31 Oct).
https://www.middleeasteye.net/live-blog/live-blog-update/hormuz-shipping-traffic-remains-70-below-pre-war-levels-ukmto-says

5. gCaptain — 11 Missing as Drone Attacks Strike Two Ships Near NATO Waters (13 Oct).
https://gcaptain.com/11-missing-as-drone-attacks-strike-two-ships-near-nato-waters/

6. Dawn — High school students in Paris' deprived suburbs spark national protest movement (3 Oct).
https://www.dawn.com/news/2034461/high-school-students-in-paris-deprived-suburbs-spark-national-protest-movement

7. Daily Maverick — France imposes curfews in parts of Paris, other cities after weekend of riots (19 Oct).
https://www.dailymaverick.co.za/article/2026-10-19-france-imposes-curfews-in-parts-of-paris-other-cities-after-weekend-of-riots/

8. Euronews — France's third weekend of social protests sees lower turnout and early clashes in major cities (31 Oct).
https://www.euronews.com/2026/10/31/frances-third-weekend-of-social-protests-sees-lower-turnout-and-early-clashes-in-major-cit

9. Wiz Research — PHP2Shell: AI uncovers critical RCE vulnerabilities affecting 70% of the Internet (21 Oct).
https://www.wiz.io/blog/php2shell-php-rce

10. Security Affairs — PHP2Shell: Millions of Attacks, No Confirmed Successful Exploits Yet (23 Oct).
https://securityaffairs.com/201538/hacking/php2shell-millions-of-attacks-no-confirmed-successful-exploits-yet.html

11. SecurityWeek — PHP2Shell Exploitation Moves From Probes to Working Shells (26 Oct).
https://www.securityweek.com/php2shell-exploitation-moves-from-probes-to-working-shells/

12. The Record (Recorded Future News) — Binance hit by record $6.3 billion crypto hack, scrambles to freeze funds (30 Oct).
https://therecord.media/binance-hit-by-record-6-billion-crypto-hack

13. The Guardian — Binance says 90% of losses from $6.3bn hack covered as FBI says North Korea behind attack (1 Nov).
https://www.theguardian.com/business/2026/nov/01/binance-losses-covered-hack-fbi-north-korea-cryptocurrency

14. Middle East Eye — Houthis target Riyadh airpot, declare Saudi airspace open target except for holy sites (5 Oct).
https://www.middleeasteye.net/live-blog/live-blog-update/houthis-target-riyadh-airpot-declare-saudi-airspace-open-target-except

15. France Bleu — Mobilisation du 31 octobre : 565 interpellations dans toute la France, un gendarme visé par un cocktail molotov (1 Nov).
https://www.ici.fr/infos/economie-social/mobilisation-du-31-octobre-565-interpellations-dans-toute-la-france-un-gendarme-vise-par-un-cocktail-molotov-3052852

16. Fenestra TI — Collection and analysis: news and event data, ransomware leak sites, underground forums, stealer logs and Fenestra honeypot sensors (Sep–Oct 2026).
https://fenestra-ti.com

17. gCaptain — Romania Blames Russia For Drone That Sinks Cargo Ship; 1 Killed, 3 Missing (25 Oct).
https://gcaptain.com/romania-blames-russia-for-drone-that-sinks-cargo-ship-1-killed-3-missing/

18. BleepingComputer — Germany arrests alleged core Qilin ransomware member after extradition (9 Oct).
https://www.bleepingcomputer.com/news/security/germany-arrests-alleged-core-qilin-ransomware-member-after-extradition/

19. CISA — Known Exploited Vulnerabilities Catalog (accessed 1 Nov).
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

20. Security Affairs — U.S. CISA adds Ivanti Connect Secure flaws to its Known Exploited Vulnerabilities catalog (31 Oct).
https://securityaffairs.com/202175/security/u-s-cisa-adds-ivanti-connect-secure-flaws-to-its-known-exploited-vulnerabilities-catalog.html

21. The Record (Recorded Future News) — Cyberattack disrupts refrigeration at hundreds of French supermarkets (11 Oct).
https://therecord.media/cyberattack-disrupts-refridgeration-in-france

22. Arab News — Investigators hunt French supermarket fridge hackers, no claim of responsibility (13 Oct).
https://www.arabnews.com/world/investigators-hunt-french-supermarket-fridge-hackers-no-claim-of-responsibility-3006133

23. Dark Web Informer — RT @DarkWebInformer: Many forums are down due to PHP2Shell. Threat feed is working, just not many alerts. (21 Oct).
https://x.com/DarkWebInformer/status/2112949108763975724

24. BleepingComputer — Binance links $6.3 billion crypto theft to compromised DevOps laptop (30 Oct).
https://www.bleepingcomputer.com/news/security/binance-links-63-billion-crypto-theft-to-compromised-devops-laptop/

25. Dawn — Binance to resume withdrawals after covering bulk of stolen $6.3bn (1 Nov).
https://www.dawn.com/news/2041364/binance-to-resume-withdrawals-after-covering-bulk-of-stolen-63bn

26. AeroTime — Lithuania suspects Russian sabotage after attempt to burn Starlink site in Vilnius (19 Oct).
https://www.aerotime.aero/articles/lithuania-starlink-arson-russian-sabotage

27. AeroTime — Drones breach no-fly zone over Toulon, home to France's main naval base (21 Oct).
https://www.aerotime.aero/articles/france-toulon-military-sites-drone-incursions-investigation

28. Hespress English (AFP) — Macron condemns 'racist terrorist attack' after deadly shooting near Paris (24 Oct).
https://en.hespress.com/147891-macron-condemns-racist-terrorist-attack-after-deadly-shooting-near-paris.html

29. National Post — 'Violence, clashes and damage': Student protests in France leave hundreds injured, about 2,000 arrested (1 Oct).
https://nationalpost.com/news/world/violence-clashes-and-damage-student-protests-in-france-leave-hundreds-injured-about-2000-arrested

30. France 24 — France closes 400 high schools as teens protests escalate (2 Oct).
https://www.france24.com/en/video/20261002-france-closes-400-high-schools-as-teens-protests-escalate

31. Arab News — Paris police chief says student protest movement out of control, urges peaceful action (3 Oct).
https://www.arabnews.com/world/paris-police-chief-says-student-protest-movement-out-of-control-urges-peaceful-action-3004436

32. BBC News — France promises 3,000 extra teachers in first step to calm student protests (9 Oct).
https://www.bbc.co.uk/news/articles/c6vg98lw017po?at_medium=RSS&at_campaign=rss

33. Al Jazeera — Macron condemns violence after riots lead to looting and mass arrests (18 Oct).
https://www.aljazeera.com/video/newsfeed/2026/10/18/macron-condemns-violence-after-riots-lead-to-looting-and-mass-arrests

34. France 24 — French PM blames 'ultra-left' groups for weekend riots, promises 'massive' security deployment (20 Oct).
https://www.france24.com/en/france/20261020-french-pm-blames-ultra-left-groups-for-weekend-riots-promises-massive-security-deployment

35. G1 (Globo) — França vai mobilizar polícia antiterrorismo para conter novos protestos (20 Oct).
https://g1.globo.com/jornal-nacional/noticia/2026/10/20/franca-vai-mobilizar-policia-antiterrorismo-para-conter-novos-protestos.ghtml

36. France 24 — Curfew imposed in certain areas of Paris every night until Monday morning (22 Oct).
https://www.france24.com/en/curfew-imposed-in-certain-areas-of-paris-every-night-until-monday-morning

37. France 24 — 'France has fallen': Far-right figures fuel Islamophobic claims with false student protest videos (5 Oct). https://www.france24.com/en/france-has-fallen-far-right-figures-fuel-islamophobic-claims-with-false-student-protest-videos-1

38. France 24 — Macron says world leaders have made 'stupid' comments on France riots based on fake AI videos (21 Oct). https://www.france24.com/en/france/20261021-macron-says-world-leaders-have-made-stupid-comments-on-france-riots-based-on-fake-ai-videos

39. France 24 — France: Far right leader Marine Le Pen gains popularity amid nationwide riots (21 Oct). https://www.france24.com/en/france-far-right-leader-marine-le-pen-gains-popularity-amid-nationwide-riots

40. Rio Times — Court Bars Paris Union March From Bastille (31 Oct). https://www.riotimesonline.com/paris-union-march-barred-council-of-state/

41. The Guardian — Police clash with masked rioters after largely peaceful protests across France (31 Oct). https://www.theguardian.com/world/2026/oct/31/police-clash-rioters-after-largely-peaceful-protests-across-france

42. Al Jazeera — Cost of living protests hit Belgium, Italy, Portugal and France (17 Oct). https://www.aljazeera.com/news/2026/10/17/cost-of-living-protests-hit-belgium-italy-portugal-and-france

43. Infobae — Ola de protestas en Europa: casi 200 personas fueron detenidas en Bélgica tras los enfrentamientos con la policía (18 Oct). https://www.infobae.com/america/mundo/2026/10/18/ola-de-protestas-en-europa-casi-200-personas-fueron-detenidas-en-belgica-tras-los-enfrentamientos-con-la-policia/

44. The Guardian — Italy to deploy 500 troops to Milan after days of protests and looting (20 Oct). https://www.theguardian.com/world/2026/oct/20/milan-luxury-shops-close-italy-to-deploy-troops-youth-protests-europe

45. Infobae — Siete aeropuertos del sur de Italia alertan sobre falta de combustible por las protestas de camioneros (22 Oct). https://www.infobae.com/espana/2026/10/22/siete-aeropuertos-del-sur-de-italia-alertan-sobre-falta-de-combustible-por-los-protestas-de-camioneros/

46. The Guardian — Why are people protesting across Europe? (19 Oct). https://www.theguardian.com/world/2026/oct/18/europe-protests-france-spain-portugal-2026-explainer

47. France 24 — Greece: Protesters draw inspiration from demonstrations in France (21 Oct). https://www.france24.com/en/video/20261021-greece-protesters-draw-inspiration-from-demonstrations-in-france

48. Dawn — Germans join Europe's wave of 'Gen Z' protests; police fire water cannon on demonstrators (31 Oct). https://www.dawn.com/news/2041157/germans-join-europes-wave-of-gen-z-protests-police-fire-water-cannon-on-demonstrators

49. Euronews — France and Italy blame foreign powers for riots – but where's the evidence? (21 Oct). https://www.euronews.com/2026/10/21/france-and-italy-blame-foreign-powers-for-riots-but-wheres-the-evidence

50. Kyiv Post — Italy Investigates Russia's Possible Role in Violent Protests (21 Oct). https://www.kyivpost.com/post/87788

51. The Guardian — Violent street protests in France and Italy trigger stock and bond sell-off and send euro lower – as it happened (19 Oct). https://www.theguardian.com/business/live/2026/oct/19/exports-lift-china-economic-growth-french-protests-pressure-euro-bonds-latest-business-live-updates

52. Euronews — Disappointed after meeting, French unions call for 5 November action (21 Oct). https://www.euronews.com/2026/10/21/disappointed-after-meeting-french-unions-call-for-5-november-action

53. France Bleu — Mobilisation sociale : la CGT appelle à la grève à partir du 5 novembre (21 Oct). https://www.ici.fr/infos/societe/mobilisation-sociale-la-cgt-appelle-a-la-greve-a-partir-du-5-novembre-8412444

54. Euronews — UEFA reschedules Europa League match amid planned French general strike (28 Oct). https://www.euronews.com/2026/10/28/uefa-reschedules-europa-league-match-amid-planned-french-general-strike

55. France Bleu — Mobilisation sociale : des syndicats lycéens et étudiants appellent à bloquer les établissements les 3 et 5 novembre (31 Oct). https://www.ici.fr/infos/societe/mobilisation-sociale-des-syndicats-lyceens-et-etudiants-appellent-a-bloquer-lycees-et-universites-les-3-et-5-novembre-2249248

56. gCaptain — Six Vessels Hit in Strait of Hormuz Since Sunday (2 Oct). https://gcaptain.com/six-vessels-hit-in-strait-of-hormuz-since-sunday/

57. The Maritime Executive — 12 Seafarers Injured in Attack on LR2 Tanker in Strait of Hormuz (6 Oct). https://maritime-executive.com/article/12-seafarers-injured-in-attack-on-lr2-tanker-in-strait-of-hormuz

58. gCaptain — Tanker Attack Off Qatar Signals Wider Threat Beyond Hormuz (8 Oct). https://gcaptain.com/tanker-attack-off-qatar-signals-wider-threat-beyond-hormuz/

59. MarineTraffic Maritime Security — Two Seafarers Missing After Drone Attack on Tanker at Sohar Anchorage off Oman (12 Oct). https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13295/two-seafarers-missing-after-drone-attack-on-tanker-at-sohar-

60. MarineTraffic Maritime Security — Tanker Temporarily Disabled After Small Boat Attaches Explosives to Hull Off Oman (30 Oct). https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13348/tanker-temporarily-disabled-after-small-boat-attaches-explos

61. MarineTraffic Maritime Security — Two Crude Tankers Attack in Hormuz, All 29 Indian Crew Members Safe (31 Oct). https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13352/two-crude-tankers-attack-in-hormuz-all-29-indian-crew-member

62. Seatrade Maritime News — Product tanker attacked in Red Sea as hostilities escalate (5 Oct). https://www.seatrade-maritime.com/security/product-tanker-attacked-in-red-sea-as-hostilities-escalate

63. MarineTraffic Maritime Security — Singapore-Flagged Containership Attacked by Armed Boat in Red Sea (8 Oct). https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13291/singapore-flagged-containership-attacked-by-armed-boat-in-re

64. MarineTraffic Maritime Security — Two Ships Attacked by Drones Off Bulgaria, One Sinks (7 Oct). https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13288/two-ships-attacked-by-drones-off-bulgaria-one-sinks

65. gCaptain — Seven Sailors Missing as Drones Strike Tankers Near Romania (15 Oct). https://gcaptain.com/two-ships-ablaze-off-romanian-black-sea-coast-7-sailors-missing/

66. The Maritime Executive — Romania Shoots Down Two Suspected Russian Drones in NATO Airspace (19 Oct). https://maritime-executive.com/article/romania-shoots-down-two-suspected-russian-drones-over-its-territorial-seas

67. MarineTraffic Maritime Security — Update: Containership Sank After Three Drones Strike in Black Sea off Bulgaria: All Crew Rescued (28 Oct). https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13343/update-containership-sank-after-three-drones-strike-in-black

68. MarineTraffic Maritime Security — Cyprus-Flagged Vessel Detained While Passing Through Russian Waters in the Gulf of Finland (2 Oct). https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13276/cyprus-flagged-vessel-detained-while-passing-through-russian

69. BBC News — 'I was not going to let others die' - pilot of Flydubai flight describes cockpit attack by co-pilot (2 Oct). https://www.bbc.co.uk/news/articles/c639m98gde00o

70. Al Jazeera — Saudi Arabia says Houthi attacks on airports killed three foreign nationals (7 Oct). https://www.aljazeera.com/news/2026/10/7/saudi-arabia-says-three-foreign-nationals-killed-in-attacks-on-airports?traffic_source=rss

71. AeroTime — King Fahd Airport death toll rises to two following latest attack (22 Oct). https://www.aerotime.aero/articles/king-fahd-airport-death-toll-rises-to-two-following-latest-attack

72. gCaptain — US Blockade Bottles Up Dozens of Iranian Tankers, Nonprofit Says (6 Oct). https://gcaptain.com/us-blockade-bottles-up-dozens-of-iranian-tankers-nonprofit-says/

73. gCaptain — Fog of War Deepens in Hormuz as UKMTO Says Most Ship Attacks Go Unreported (16 Oct). https://gcaptain.com/fog-of-war-deepens-in-hormuz-as-ukmto-says-most-ship-attacks-go-unreported/

74. Splash247 — Hormuz attacks overwhelm UKMTO (19 Oct). https://splash247.com/hormuz-attacks-overwhelm-ukmto/

75. MarineTraffic Maritime Security — US Forces Strike and Disable Vessel Attempting to Cross Blockade on Iran (12 Oct). https://www.marinetraffic.com/en/maritime-news/15/maritime-security/2026/13297/us-forces-strike-and-disable-vessel-attempting-to-cross-bloc

76. gCaptain — Iran Claims More Tankers Hit Mines in Hormuz, But Evidence Remains Elusive (20 Oct). https://gcaptain.com/iran-claims-more-tankers-hit-mines-in-hormuz-but-evidence-remains-elusive/

77. gCaptain — Oil Spill Off UAE Widens, Satellite Images Show, Prompting More Beach Closures (26 Oct).
https://gcaptain.com/oil-spill-off-uae-widens-satellite-images-show-prompting-more-beach-closures/

78. gCaptain — IEA Moves to Accelerate Oil Reserve Releases as Hormuz Crisis Drags On (16 Oct).
https://gcaptain.com/iea-moves-to-accelerate-oil-reserve-releases-as-hormuz-crisis-drags-on/

79. The Maritime Executive — Tanker Hit by Limpet Mine Attack in Strait of Hormuz (30 Oct).
https://maritime-executive.com/article/tanker-hit-by-limpet-mine-attack-in-strait-of-hormuz

80. gCaptain — Qatar LNG Cargo Makes Rare Red Sea Journey to Get Gas to Europe (19 Oct).
https://gcaptain.com/qatar-lng-cargo-makes-rare-red-sea-journey-to-get-gas-to-europe/

81. Seatrade Maritime News — Gulf of Aden piracy warning as US issues Iran blockade update (28 Oct).
https://www.seatrade-maritime.com/security/gulf-of-aden-piracy-warning-us-issues-iran-blockade-update

82. The Maritime Executive — NATO Discusses Black Sea After More Vessel Strikes Leave Seven Crew Missing (15 Oct).
https://maritime-executive.com/article/nato-discusses-black-sea-after-more-vessel-strikes-leave-seven-crew-missing

83. gCaptain — France Seizes Another 'Shadow Fleet' Tanker; Russia Decries 'Piracy' (13 Oct).
https://gcaptain.com/france-seizes-another-shadow-fleet-tanker-russia-decries-piracy/

84. Splash247 — Former Ukrainian officer goes on trial over Nord Stream sabotage (16 Oct).
https://splash247.com/former-ukrainian-officer-goes-on-trial-over-nord-stream-sabotage/

85. gCaptain — Hackers Breached Propulsion System of US-Bound Oil Tanker (5 Oct).
https://gcaptain.com/hackers-breached-propulsion-system-of-us-bound-oil-tanker/

86. The Record (Recorded Future News) — Coast Guard, FBI boarded tanker after attack by 'foreign cyber actors' (16 Sep).
https://therecord.media/oil-tanker-cyberattack-coast-guard-fbi

87. FlightGlobal — EASA broadens Saudi airspace conflict warning to Riyadh and Dammam (9 Oct).
https://www.flightglobal.com/ops-safety/2026/10/easa-broadens-saudi-airspace-conflict-warning-to-riyadh-dammam-and-madinah/

88. Middle East Eye — Lufthansa, Air India suspend flights to Riyadh airport after Houthi attacks (8 Oct).
https://www.middleeasteye.net/live-blog/live-blog-update/lufthansa-air-india-suspend-flights-riyadh-airport-after-houthi-attacks

89. Middle East Eye — Etihad and Qatar Airways suspend flights to Saudi cities (13 Oct).
https://www.middleeasteye.net/live-blog/live-blog-update/etihad-and-qatar-airways-suspend-flights-saudi-cities

90. FlightGlobal — Delta delays Saudi Arabia service until 2027 after deadly Riyadh airport strikes (12 Oct).
https://www.flightglobal.com/delta-air-lines/2026/10/delta-delays-saudi-arabia-service-until-2027-after-deadly-riyadh-airport-strikes/

91. FlightGlobal — Saudi airspace restrictions come at 'a bad time' for Europe-Asia flights (16 Oct).
https://www.flightglobal.com/airlines/2026/10/saudi-airspace-restrictions-come-at-a-bad-time-for-europe-asia-flights/

92. AeroTime — Japan scrambles fighters as Chinese drones fly near Okinawa during Keen Sword (20 Oct).
https://www.aerotime.aero/articles/chinese-drones-japan-okinawa-keen-sword-27

93. The Guardian — Flydubai co-pilot used crash axe to attack captain, says UAE (3 Oct).
https://www.theguardian.com/world/2026/oct/03/flydubai-co-pilot-used-crash-axe-to-attack-captain-says-uae

94. Al Jazeera — 12 minutes of madness: How Flydubai pilot, passengers saved plane midfall (2 Oct).
https://www.aljazeera.com/news/2026/10/2/12-minutes-of-madness-how-flydubai-pilot-passengers-saved-plane-midfall

95. The Guardian — Netanyahu says too early to tell who was behind plane incident as flydubai halts all flights to Israel (1 Oct).
https://www.theguardian.com/world/2026/oct/01/netanyahu-flydubai-halts-all-flights-to-israel

96. Euronews — Flydubai co-pilot planned suicide attack in Tel Aviv airport inspired by 9/11 (9 Oct).
https://www.euronews.com/2026/10/09/flydubai-co-pilot-planned-suicide-attack-in-tel-aviv-airport-inspired-by-911

97. The Guardian — Flydubai co-pilot originally planned attack for July, investigators believe (5 Oct).
https://www.theguardian.com/world/2026/oct/05/flydubai-co-pilot-originally-planned-attack-for-july-investigators-believe

98. NDTV — 'War Isn't Over': Al-Qaeda Praises flydubai Co-Pilot, Calls For More Attacks (4 Oct).
https://www.ndtv.com/world-news/al-qaeda-praises-flydubai-co-pilot-calls-for-similar-attacks-on-us-israel-12137276

99. ADL — Within 48 Hours of FlyDubai Incident, at Least 25,000 X Posts Pushed Conspiracy Theories (2 Oct).
https://www.adl.org/resources/article/within-48-hours-flydubai-incident-least-25000-x-posts-pushed-conspiracy-theories

100. AeroTime — Cyberattack triggers partial shutdown at French aerospace supplier (14 Oct).
https://www.aerotime.aero/articles/egide-cyberattack-french-aerospace-defense-supplier

101. Security Affairs — FBI and CISA Warn of SafePay Ransomware Attacks on 600 Organizations (22 Oct).
https://securityaffairs.com/201464/cyber-crime/fbi-and-cisa-warn-of-safepay-ransomware-attacks-on-600-organizations.html

102. Huntress — Up a Creek Without a Command Line: Mapping an Akira Ransomware Attack (6 Oct).
https://www.huntress.com/blog/mapping-akira-ransomware-attack

103. Group-IB — Stray Cat, Open Doors: How k0t Wanders Through the Network Edge (21 Oct).
https://www.group-ib.com/blog/stray-cat-network-edge/

104. CISA Cybersecurity Advisories — CISA Urges Patching Newly Exploited Vulnerability in Ivanti Connect Secure (13 Oct).
https://www.cisa.gov/news-events/alerts/2026/10/13/cisa-urges-patching-newly-exploited-vulnerability-ivanti-connect-secure

105. Unit42 (Palo Alto Networks) — Threat Brief: Active Exploitation of PAN-OS CVE-2026-0257 (Updated October 19) (19 Oct).
https://unit42.paloaltonetworks.com/active-exploitation-of-pan-os-cve-2026-0257/

106. Google Threat Intelligence (Mandiant) — ARMORY CASTLE Exploits BeyondTrust (15 Oct).
https://cloud.google.com/blog/topics/threat-intelligence/armory-castle-exploits-beyondtrust/

107. Security Affairs — U.S. CISA adds GitLab and Cisco flaws to its Known Exploited Vulnerabilities catalog (30 Oct).
https://securityaffairs.com/202133/security/u-s-cisa-adds-gitlab-and-cisco-flaws-to-its-known-exploited-vulnerabilities-catalog.html

108. Security Affairs — PHP Warns of New Code Execution Flaw Days After PHP2Shell Patches (23 Oct).
https://securityaffairs.com/201595/security/php-warns-of-new-code-execution-flaw-days-after-php2shell-patches.html

109. SecurityWeek — Drupal Commerce Core Vulnerability Exploited Against Online Stores (30 Oct).
https://www.securityweek.com/drupal-commerce-core-vulnerability-exploited-against-online-stores/

110. South China Morning Post — France supermarkets say cyberattack forced defrosting of refrigerators in over 200 stores (12 Oct).
https://www.scmp.com/news/world/europe/article/3370633/france-supermarkets-say-cyberattack-forced-defrosting-refrigerators-over-200-stores

111. Dhaka Tribune — Saudi says no Houthi truce until Yemen govt regains territory (9 Oct).
https://www.dhakatribune.com/world/middle-east/421683/saudi-says-no-houthi-truce-until-yemen-govt

112. Arab News — Houthis target Madinah power station supplying Prophet's Mosque, coalition says (1 Oct).
https://www.arabnews.com/saudi-arabia/houthis-target-madinah-power-station-supplying-prophets-mosque-coalition-says-3004131

113. South China Morning Post — Flames, smoke seen at Aramco facility south of Saudi capital (3 Oct).
https://www.scmp.com/news/world/middle-east/article/3369667/flames-smoke-seen-aramco-facility-south-saudi-capital?utm_source=rss_feed

114. Middle East Eye — At least one plane severely damaged as Houthis claim third Riyadh airport attack (8 Oct).
https://www.middleeasteye.net/live-blog/live-blog-update/least-one-plane-severely-damaged-houthis-claim-third-riyadh-airport

115. Dawn — Pilot among 3 Saudi nationals killed in attacks on Riyadh airport, authorities say (9 Oct).
https://www.dawn.com/news/2035905/pilot-among-3-saudi-nationals-killed-in-attacks-on-riyadh-airport-authorities-say

116. Al Jazeera — Saudi Arabia says 1 dead, 11 injured in latest attack on Riyadh airport (12 Oct).
https://www.aljazeera.com/news/2026/10/12/saudi-arabia-says-1-dead-11-injured-in-latest-attack-on-riyadh-airport?traffic_source=rss

117. South China Morning Post — Aramco facility hit as Houthis and Saudi coalition exchange attacks (14 Oct).
https://www.scmp.com/news/world/middle-east/article/3370793/aramco-facility-hit-houthis-and-saudi-coalition-exchange-attacks?utm_source=rss_feed

118. Dhaka Tribune — Saudi forces say intercepted two Houthi missiles targeting Yanbu, Taif (24 Oct).
https://www.dhakatribune.com/world/middle-east/422798/saudi-forces-say-intercepted-two-houthi-missiles

119. The Maritime Executive — Yemen's Houthi Rebels Strike Saudi Aramco's Ras Tanura Oil Terminal (27 Oct).
https://maritime-executive.com/article/yemen-s-houthi-rebels-strike-saudi-aramco-s-ras-tanura-oil-terminal

120. The Hindu — Oil rises over 1% after Saudi Arabian refinery attack reignites supply risk (28 Oct).
https://www.thehindu.com/news/international/oil-rises-after-saudi-arabian-refinery-attack-reignites-supply-risk/article71634583.ece

121. Arab News — Coalition intercepts Houthi drones over Riyadh and Madinah, missile in south (30 Oct).
https://www.arabnews.com/saudi-arabia/coalition-intercepts-houthi-drones-over-riyadh-and-madinah-missile-in-south-3009043

122. Middle East Eye — Saudi-led coalition forces intercept Houthi drone over Riyadh region (31 Oct).
https://www.middleeasteye.net/live-blog/live-blog-update/saudi-led-coalition-force-intercepts-houthi-drone-over-riyadh-region

123. The Independent (Uganda) — Saudi-led coalition: 17 killed, over 330 injured in attacks on Riyadh airport since Oct (16 Oct).
https://www.independent.co.ug/saudi-led-coalition-17-killed-over-330-injured-in-attacks-on-riyadh-airport-since-oct/

124. Arab News — Houthi missile debris damages kindergarten and medical center in Riyadh (8 Oct).
https://www.arabnews.com/saudi-arabia/houthi-missile-debris-damages-kindergarten-and-medical-center-in-riyadh-3005295

125. Africanews — Iran denies being behind Houthi attacks as Aden airport hit (17 Oct).
http://www.africanews.com/2026/10/17/iran-denies-being-behind-houthi-attacks-as-aden-airport-hit/

126. BBC News — Houthi missile strike on Yemen camp kills 50 security recruits, local authorities say (19 Oct).
https://www.bbc.co.uk/news/articles/cv0ld6lrr2zeo?at_medium=RSS&at_campaign=rss

127. African Manager — Les Houthis ont ciblé le palais présidentiel et l'aéroport international d'Aden (30 Oct).
https://africanmanager.com/les-houthis-ont-cible-le-palais-presidentiel-et-laeroport-international-daden/

128. Middle East Eye — Turkey to deploy troops and air defence systems to Saudi Arabia amid Houthi attacks (6 Oct).
https://www.middleeasteye.net/news/turkey-to-deploy-troops-and-air-defence-systems-saudi-arabia

129. The Siasat Daily — Egypt approves sending troops to Saudi amid Houthi attacks (18 Oct).
https://www.siasat.com/egypt-approves-sending-troops-to-saudi-amid-houthi-attacks-3560586/

130. Al Jazeera — UK to deploy Typhoon jets to help defend Saudi Arabia from Houthi attacks (20 Oct).
https://www.aljazeera.com/news/2026/10/20/uk-to-deploy-raf-fighter-jets-to-defend-saudi-arabia-from-houthi-attacks?traffic_source=rss

131. BBC World News — US orders some diplomats to leave Saudi Arabia as Houthi attacks escalate (22 Oct).
https://www.bbc.co.uk/news/articles/c6×2vpk93770o?at_medium=RSS&at_campaign=rss

132. The Siasat Daily — Saudi Arabia postpones major events amid Houthi attacks (15 Oct).
https://www.siasat.com/saudi-arabia-postpones-major-events-amid-houthi-attacks-3558902/

133. Middle East Eye — France, Saudi Arabia weigh military options to protect Yanbu oil terminal, army chief says (8 Oct).
https://www.middleeasteye.net/live-blog/live-blog-update/france-saudi-arabia-weigh-military-options-protect-yanbu-oil-terminal

134. SecurityWeek — PHP2Shell Exploitation Started Days Before Patches (22 Oct).
https://www.securityweek.com/php2shell-exploitation-started-days-before-patches/

135. BleepingComputer — Amazon says PHP2Shell exploitation began 4 days before patches (22 Oct).
https://www.bleepingcomputer.com/news/security/amazon-says-php2shell-exploitation-began-4-days-before-patches/

136. CISA Cybersecurity Advisories — Critical Vulnerabilities in PHP Require Immediate Patching (21 Oct).
https://www.cisa.gov/news-events/alerts/2026/10/21/critical-vulnerabilities-php-require-immediate-patching

137. SANS Internet Storm Center — Critical PHP Vulnerability (CVE-2026-109618, CVE-2026-109619) [infocon yellow], (Wed, Oct 21st) (21 Oct).
https://isc.sans.edu/diary/rss/33440

138. Patchstack — Major security alert: PHP vulnerable to critical RCE, attacks ongoing (21 Oct).
https://patchstack.com/articles/php-major-vulnerability-alert-10-2026/

139. Check Point Blog — PHP2Shell Update: One in ten organizations impacted as Europe bears the brunt (22 Oct).
https://blog.checkpoint.com/ai-security/php2shell-one-in-ten-organizations-impacted-as-europe-bears-the-brunt/

140. CrowdStrike Blog — Obstacles to Weaponizing PHP2Shell Likely Constrain Immediate Widespread Exploitation (23 Oct).
https://www.crowdstrike.com/en-us/blog/obstacles-to-weaponizing-php2shell-likely-constrain-exploitation/

141. SecurityWeek — China-Linked Hackers Exploit PHP2Shell to Root Firewalls (28 Oct).
https://www.securityweek.com/china-linked-hackers-exploit-php2shell-to-root-firewalls/

142. BleepingComputer — PHP2Shell security flaws now sucessfully exploited in the wild (26 Oct).
https://www.bleepingcomputer.com/news/security/php2shell-security-flaws-now-sucessfully-exploited-in-the-wild/

143. Marcus Hutchins — Seeing some anecdotal reports of successful php2shell exploitation in the wild, but also seeing a lot of peopl... (24 Oct).
https://x.com/MalwareTechBlog/status/2114077217261334609

144. Dark Web Intelligence — UPDATE: UNIT 42 RETRACTS PHP2SHELL EXPLOITATION UPDATE Unit 42 has retracted its Oct 23 update that tied a Eur... (26 Oct).
https://x.com/DailyDarkWeb/status/2114561172124926387

145. Security Affairs — PHP2Shell: Suspected North Korean campaign targets 216 vulnerable PHP hosts (26 Oct).
https://securityaffairs.com/201748/hacking/php2shell-suspected-north-korean-campaign-targets-216-vulnerable-php-hosts.html

146. BleepingComputer — CISA confirms PHP2Shell vulnerabilities now exploited in attacks (27 Oct).
https://www.bleepingcomputer.com/news/security/cisa-confirms-php2shell-vulnerabilities-now-exploited-in-attacks/

147. Check Point Blog — PHP2Shell: Log4Shell at AI Speed — A CISO's Perspective (22 Oct).
https://blog.checkpoint.com/ai-security/php2shell-log4shell-at-ai-speed-a-cisos-perspective/

148. The Record (Recorded Future News) — Reports of PHP bug exploitation attempts grow as experts downplay viability of exploits (23 Oct).
https://therecord.media/php-php2shell-exploitation-attempts-pocs

149. SANS Internet Storm Center — (Reliable)? php2shell exploitability, (Fri, Oct 23rd) (23 Oct).
https://isc.sans.edu/diary/rss/33452

150. SecurityWeek — Mirai Botnet Operators Join PHP2Shell Attacks as ASLR Bypass Exploits Emerge (23 Oct).
https://www.securityweek.com/mirai-botnet-operators-join-php2shell-attacks-as-aslr-bypass-exploits-emerge/

151. Premium Times (Nigeria) — Binance reserves $6.34bn to cover stolen assets after cyberattack – CEO (30 Oct).
https://www.premiumtimesng.com/business/business-news/921592-binance-reserves-6-34bn-to-cover-stolen-assets-after-cyberattack-ceo.html

152. SecurityWeek — $6 Billion Binance Hack Bears Hallmarks of North Korea's TraderTraitor (30 Oct).
https://www.securityweek.com/6-billion-binance-hack-bears-hallmarks-of-north-koreas-tradertraitor/

153. Folha de S.Paulo — Binance Brasil suspende saques após ataque hacker de US$ 6,3 bilhões (30 Oct).
https://c-level.folha.uol.com.br/financas/2026/10/binance-brasil-suspende-saques-apos-ataque-hacker-de-us-63-bilhoes.shtml

154. CNN Brasil — Criptomoedas têm forte queda após ataque hacker contra a Binance (30 Oct).
https://www.cnnbrasil.com.br/economia/money/mercado/criptomoedas-bitcoin-ethereum-30-outubro-2026/

155. BBC News — Why North Korea's 'elite' hackers are the prime suspect in major Binance hack (31 Oct).
https://www.bbc.co.uk/news/articles/ck9dz3v7z7v3o

156. The Hill — Trump says US looking into Binance hack: 'We don't know' if North Korea responsible (30 Oct).
https://thehill.com/policy/technology/6185518-trump-binance-crypto-hack-north-korea/

157. CNN Brasil — FBI e Serviço Secreto dos EUA colaboram com Binance após ataque cibernético (30 Oct).
https://www.cnnbrasil.com.br/economia/money/negocios/fbi-e-servico-secreto-dos-eua-colaboram-com-binance-apos-ataque-cibernetico/

158. Euronews — How the Binance hack happened and who was behind it (30 Oct).
https://www.euronews.com/2026/10/30/how-the-binance-hack-happened-and-who-was-behind-it

159. BleepingComputer — Polymarket halts trading after crypto-draining script breach, $2.5M traced (29 Oct).
https://www.bleepingcomputer.com/news/security/polymarket-halts-trading-after-crypto-draining-script-breach-25m-traced/



contact@fenestra-ti.com