Doppel PUBLIC

DOPPEL THREAT INTELLIGENCE BRIEF

Never-Ending November

Six weeks of outages, breaches, and a ground stop. The lures changed with every headline. The infrastructure behind them was already built.

SCOPE	PUBLISHED	CLASSIFICATION	PREPARED BY
Oct to Nov 2026 headline events	18NOV2026	PUBLIC	DJ Peterson Doppel SECR

October refused to end

Between 01OCT2026 and 18NOV2026 the news produced a multi-region Azure outage, a breach of Denmark's national population register, ransomware across a SoftBank-group cloud platform in Japan, remotely sabotaged supermarket refrigeration, a ConnectWise backup credential opening hundreds of Microsoft 365 tenants, the $6.3 billion Binance theft, the largest cryptocurrency theft on record, an Optimizely script that turned 178 major websites into card skimmers for most of a day, an FBI warning about an autonomous AI intrusion framework, a day-long Microsoft 365 outage, a nationwide ground stop, a software bug at one of the largest US banks that slowed transactions across the financial system, and a critical Java flaw on the same day an NSA classified network went dark for maintenance. Each one handed someone a reason to message a lot of people at once.

Doppel watched what actors did with each headline. Threat actors played the sequence on repeat. Within hours, a domain named for the event. Within a day, a page built to take personal or financial details from people looking for a refund, a status update, or a way back into an account. Within two days of the Microsoft 365 outage, Microsoft itself confirmed a credential-phishing campaign dressed as its own service-health notice.

What did not happen matters just as much. The daily supply of sign-in phishing, fake support numbers, and bank-themed lookalikes did not rise in Doppel telemetry after any of these events, because it did not have to. That supply runs every day regardless of the news, and what a headline changes is how it lands, turning background noise into the exact message a worried person is already expecting to receive. The infrastructure was in place before any of these events broke, and the news simply raised its hit rate.

HEADLINE EXPOSURE
ELEVATED

Hours to a squat, a day to a harvesting page, no new supply required

Event-named domains appear within hours of a headline and harvesting pages within a day. The everyday phishing supply does not need to grow, because the event makes its standing lures believable.

- **6 h 20 min** FIRST EVENT-NAMED DOMAIN AFTER MICROSOFT 365 OUTAGE
- **23 h** FIRST HARVESTING PAGE AFTER THE MICROSOFT 365 OUTAGE
- **Under 48 h** MICROSOFT-CONFIRMED LURE CAMPAIGN
- **None observed** LIFT IN DAILY PHISHING SUPPLY, ALL EVENTS

DOPPEL SOCIAL ENGINEERING ATTACK CHAIN

- STAGE 1 — SETUP: Event-named domains in hours; support-number pages seeded a day early
- STAGE 2 — LAUNCH: Service-health, refund, and failed-transfer lures
- STAGE 3 — CONTACT: Email, search results, forum posts, texts
- STAGE 4 — ENGAGEMENT: Refund forms, sign-in clones behind bot checks, phone agents
- STAGE 5 — COMPROMISE: Credentials, card and identity details, phone-only payments

Every event in this brief maps to the same chain. Setup is a domain named for the headline, or a support-number page seeded into search results before the news breaks. Launch is the message that borrows the event, whether a service-health notice, a cancellation text, or a failed-transfer alert. Contact and Engagement are a refund form, a support line that answers, or a sign-in page that looks like the one a person was already expecting. Compromise is the credential, the card, or the identity details handed over.

Black October

October's largest incidents shared a shape. The decisive access was something the victim already trusted. A supplier's standing consent, a developer's package installer, a job candidate's take-home repository, and a key left in a partner's configuration file each opened a door. The intrusions that followed moved at machine speed, and in at least two of them the acceleration came from an AI framework that chains reconnaissance, exploitation, and privilege escalation with little human input.

30SEP to 01OCT
An Azure multi-region outage ran five hours and 45 minutes after paused gateway updates resumed at once and overloaded the networking control plane.

05OCT
Denmark disclosed unauthorized access to its national population register, about 8.8 million people, through a private company's legitimate lookup access.

07OCT
Ransomware took down IDC Frontier's IDCF Cloud, a SoftBank-group platform in Japan, disrupting 495 companies and local governments.

11 to 12OCT
Attackers forced refrigeration controllers at French supermarkets into defrost cycles for six hours, causing fires and spoiled stock; the national CERT issued an alert the next day.

15 to 16OCT
A ConnectWise Cloud Backup credential, holding standing consent into customers' Microsoft 365 tenants, was used to attempt sign-ins to about 1,000 tenants and succeed in more than 300. In at least two, a related app assigned itself the global administrator role.

21OCT
PHP2Shell, two unauthenticated remote code execution flaws in PHP core, was exploited before the patch existed, with 1.3 to 1.9 million exposed hosts.

22OCT
Capcom disclosed 11.77 million account records exposed through its membership service.

23 and 27OCT
Two network-wide Cloudflare outages of about three hours each.

29OCT
Binance lost about $6.3 billion from hot wallets in roughly 20 minutes, the largest cryptocurrency theft on record and the end of a months-long campaign that began with a tampered developer installer in June and a fake job interview in September.

The Binance theft is the clearest case. Public reporting traces it to a tampered installer and a fake job interview that planted a malicious repository on an engineer's workstation, months before any wallet moved. The ConnectWise breach began with a consent grant customers had given years earlier. These were social engineering and trust abuse first, and intrusion second. The AI framework the FBI would name in November shortened what came after the door opened; it did not open the door.

November did not stop

01 to 02NOV
Barracuda's cloud environment was accessed for 44 hours through a cloud key a third-party AI vendor had left in a repository configuration file; the attacker hunted for cryptocurrency secrets.

03NOV
US midterm elections, with the FBI warning in October of donation, merchandise, and voter-registration fraud themed on the vote.

12NOV
Microsoft 365, including Exchange Online, Outlook, and Teams, went down for most of a business day. Microsoft attributed it to servers failing automated health checks, not an attack.

13NOV
A nationwide FAA ground stop held departures for about four and a half hours after a newly installed router flooded the air traffic network; operators canceled about 12,462 flights that day.

13NOV
The FBI published a FLASH on ARTEX, an open-source autonomous penetration-testing framework weaponized since August, with intrusions reaching privileged access in under three hours and more than 1,600 consoles exposed to the internet.

14NOV
Microsoft confirmed a high-volume credential-phishing campaign using the outage as its lure, detected the day after the outage began.

16NOV
A software bug at one of the largest US banks slowed transactions for most of a day, with ripple effects at peer banks and on Zelle. Not cyber-related, by the bank's account.

16NOV
Optimizely's web-experimentation script, served from the company's own CDN with its own certificate, carried an injected loader on the sites of 178 organizations for about 19 hours, including Zoom, the BBC, CNN, Salesforce, GitLab, HSBC, and IKEA. The second stage swapped cryptocurrency wallet addresses, skimmed card numbers typed into the sites' own forms, stole cookies and screenshots, and routed iPhones to exploit kits. None of the 178 was breached itself; Optimizely traced the entry to a flaw in its account signup flow.

17NOV
Infoblox confirmed a supply-chain breach in which a data-migration contractor's access to its SharePoint instance was used to take employee identity and payroll details and customers' network configuration backups. The company warned staff to expect phishing and vishing.

17NOV
Java4Shell, CVE-2026-114938, a memory-corruption flaw in the Java runtime's Base64 decoder that gives unauthenticated remote code execution against common enterprise applications in default configurations; CISA urged immediate patching.

17 to 18NOV
NSANet, the NSA's classified internal network, degraded during what the agency called routine maintenance. The next morning Apple confirmed an internal update had taken Apple Pay, iCloud, and support systems down, while users also reported problems with Gmail and Marriott's app. No evidence connects any of them.

18NOV
Rakuten Securities disclosed that login IDs and branch codes for 11.25 million accounts, and personal, bank, and income details for 4.47 million, may have been exposed through a test environment, with access traced to 11NOV.

19NOV
Grand Theft Auto VI launches, on PlayStation 5 and Xbox Series X|S only. Fake betas, leaked builds, nonexistent PC and mobile versions, cloned Rockstar login pages, and crypto-paid "early access" have been running for months, several carrying infostealers that land on the same laptops people use for work; login and purchase problems on the PlayStation Network were reported hours before release.

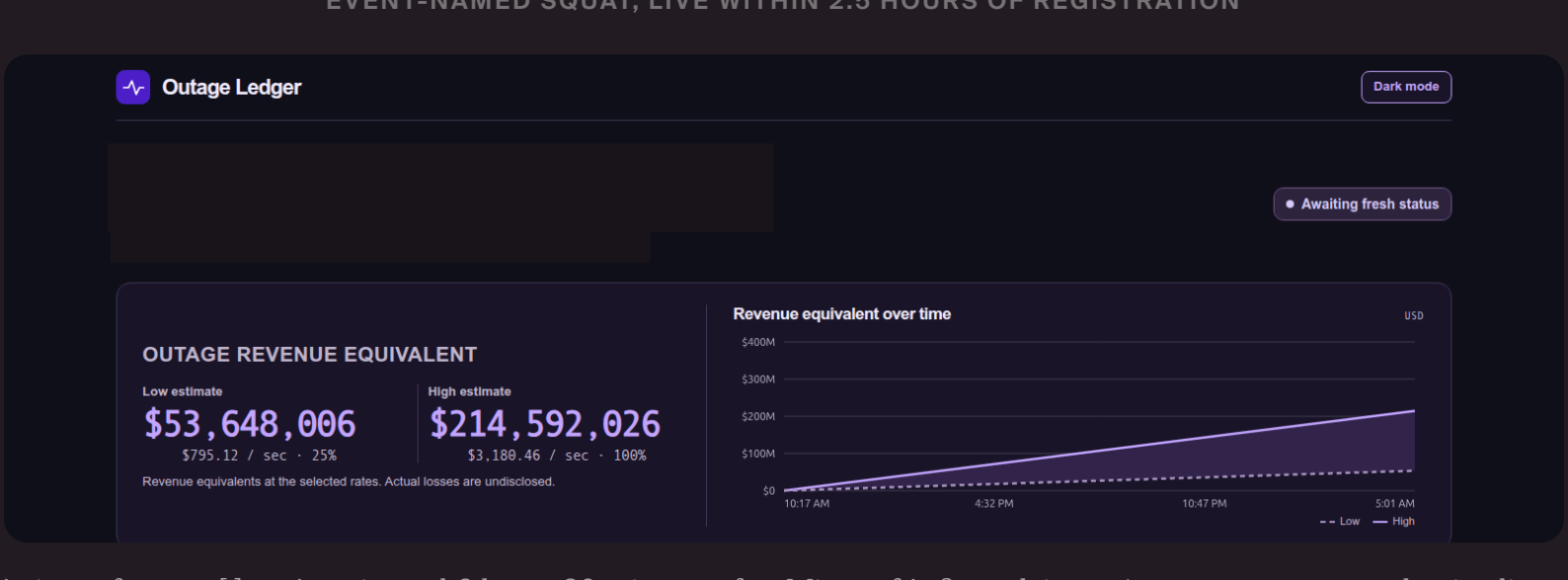
27NOV
Black Friday. Doppel confirmed the season's first Black Friday-named lookalike page on 01SEP2026, a month or more ahead of last year's ramp.

What actors built on each headline

The Microsoft 365 outage, 12NOV

Microsoft's first advisory went out at 16:17 UTC. The first domain named for the outage, `microsoftoutage[.]com`, was registered six hours and 20 minutes later through a mainstream registrar with privacy protection, and had live content within two and a half hours of registration. The content was a revenue-loss counter with no forms and no inputs, a traffic play. A second, `outlookoutage[.]com`, followed at ten hours and 24 minutes, hosting a "community forum" with its own account registration. Neither harvested credentials or were verified as malicious, but both show how fast the name space around an event is claimed.

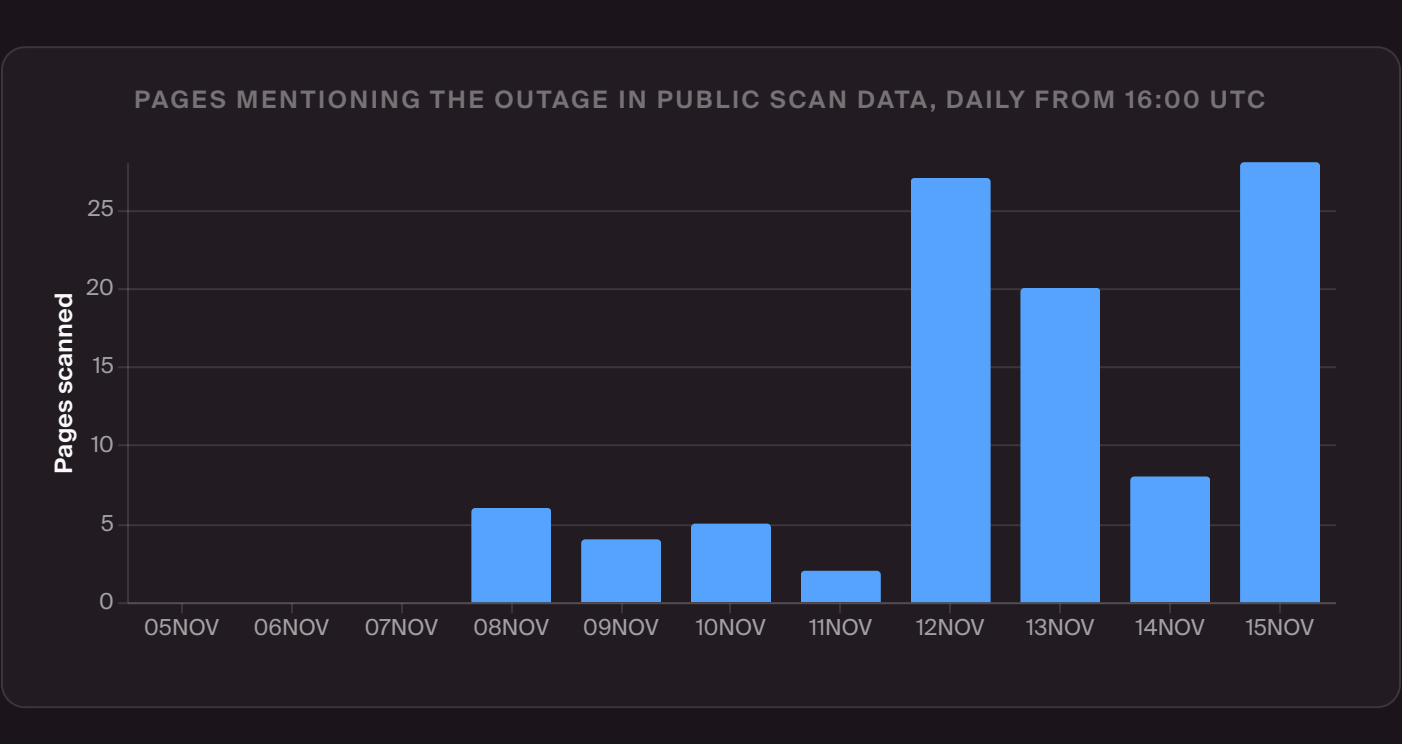
EVENT-NAMED SQUAT, LIVE WITHIN 2.5 HOURS OF REGISTRATION



`microsoftoutage[.]com`, registered 6 hours 20 minutes after Microsoft's first advisory. A revenue counter and a timeline, no inputs.

In public scan data, pages mentioning the outage ran at about two a day in the week before and 27 in the first 24 hours after onset, roughly ten times the run rate. Sixteen of the 27 were news coverage. Eight were opportunistic, meaning the two new domains above (four scans between them) and four unofficial status pages on free hosting. None of the 27 collected a credential. Over the same 26 hours, Microsoft sign-in impersonation pages on third-party hosting ran at about 40, below the prior week's daily range of 43 to 163. Actors did not build new sign-in phishing for the outage. The existing supply was already the message more than 400 million Microsoft 365 users expected to receive as service came back.

PAGES MENTIONING THE OUTAGE IN PUBLIC SCAN DATA, DAILY FROM 16:00 UTC

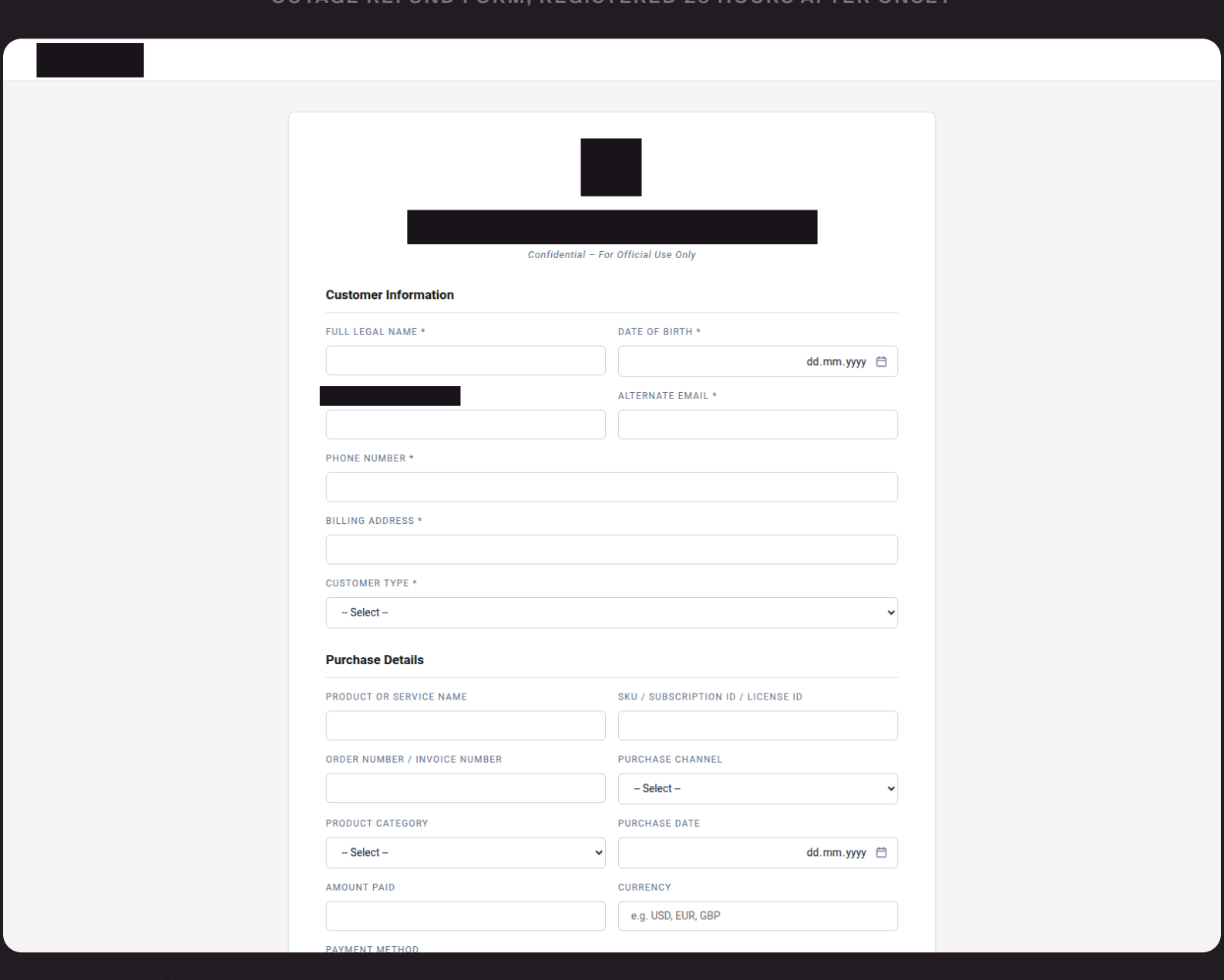


The campaign Microsoft confirmed on 14NOV is the model of an event lure. Emails posed as service-health notices, cited the real incident identifier, EX1550543, and warned that mail held during the outage would be deleted within 24 hours unless the recipient clicked to restore it. Display names took the form of the recipient's own organization followed by "Outage Notification" or "Service Health". Links were per-recipient and routed through a legitimate email delivery service, then a redirector that showed a decoy blog to anyone who was not a target, then a landing page on a random subdomain behind a bot check, the shape of an adversary-in-the-middle sign-in proxy. The infrastructure was four aged domains bought through two registrars, three sharing one CDN account, two sharing one cloud host, and all three senders sharing one mail provider. The delivery service disabled the links and the sender domains stopped resolving by 16NOV. Microsoft assesses the activity as likely credential phishing and has not confirmed credential capture or account compromise.

A second campaign, reported on 17NOV and still being detected that day, took a different shape. Subject line "disconnected after the outage", a verification code in the body, and a link to a sign-in clone that walks the visitor through entering an account name, requesting a new code, and entering it, with a "use your password" fallback at every step. The flow fits either a device-join attempt or a plain credential theft, and the same "outage" banner sits on the sign-in page regardless of the lure, which is the signature of a kit built to be reused for the next event.

The first outage-themed harvesting page came from a different operator. Registered 23 hours after onset on a Bahamas-based registrar and hosted on a mainstream cloud provider, `winrefrequests[.]com` presented a "Microsoft Refund Request Form" marked confidential and asked for full legal name, date of birth, Microsoft account, alternate email, phone, billing address, purchase channel, payment method, bank name, and refund amount. The form rendered client-side and posted to a relay script on a second domain. Nothing about its registrar, hosting, or DNS connects it to the service-health campaign. Two crews worked one headline with two different asks. One wanted a credential. The other wanted an identity and a bank relationship.

OUTAGE REFUND FORM, REGISTERED 23 HOURS AFTER ONSET



`winrefrequests[.]com`. Identity, contact, billing, and payment details, posted to a relay on a second domain. First public scan 16NOV2026. Microsoft marks redacted in the capture.

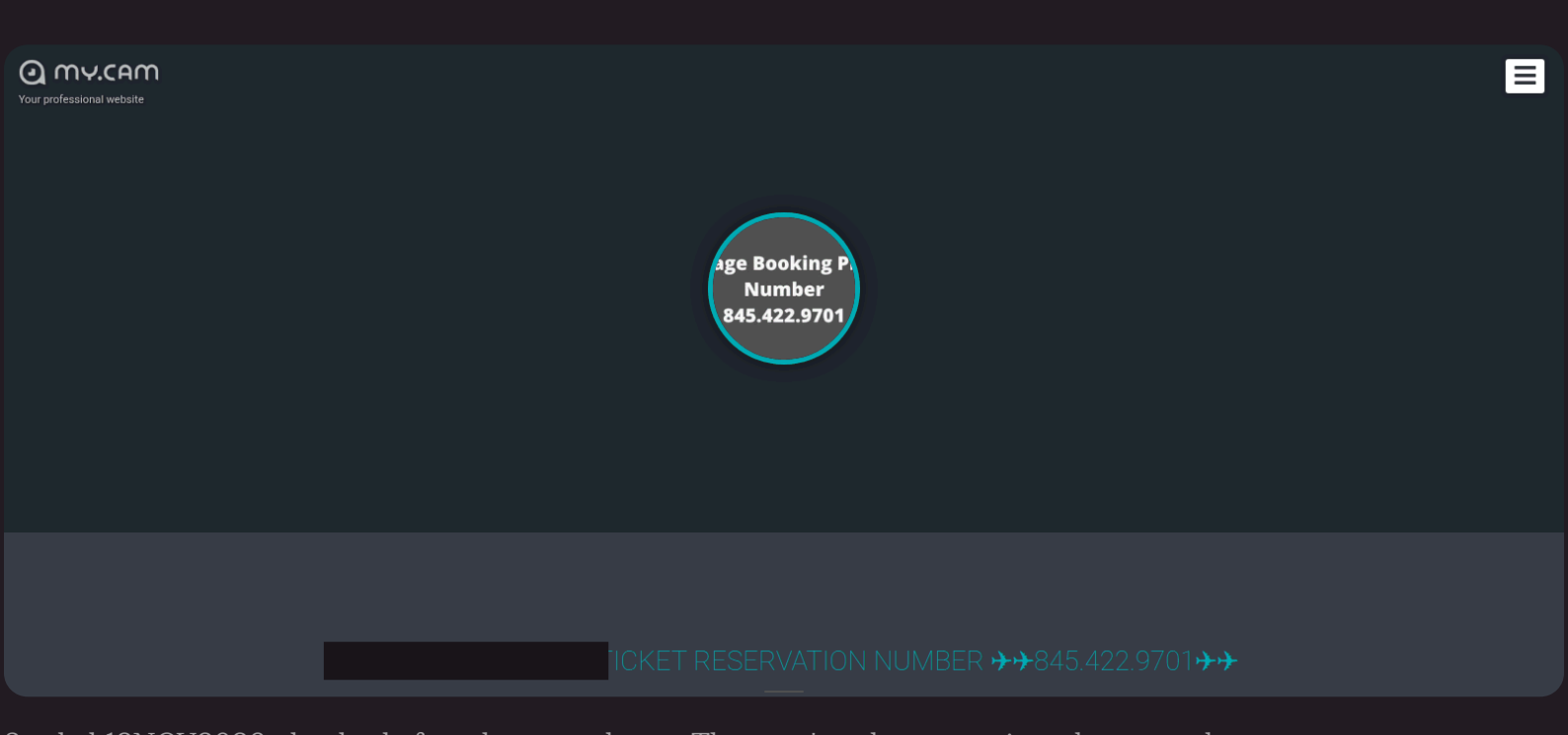
The ground stop, 13NOV

About 12,462 flights were canceled on the day of the ground stop, airlines issued waivers, and every major outlet published refund guidance over the weekend. Within a day a software startup launched a refund-claims intermediary. A traveler uploads the cancellation email or booking confirmation, or texts a screenshot to a number, and the service pursues the airline for a small case fee. It is a legitimate business with published terms and a real payment processor. Its intake form also asks for what a scam would ask for, meaning name, record locator, fare paid, and the last four digits of the card. For a traveler, the legitimate opportunist and the fraudulent one look the same at the point of contact.

Two days after the ground stop a "travel agency" domain appeared on a budget host. Visitors search fares online, an agent calls back, and payment is by phone only. Its registered address is a registered-agent mail drop shared with other fake online travel agencies, its route guides carry the logos of seven carriers, and the phone number has no footprint anywhere else. We assess with moderate confidence that it is a phone-fee operation of the kind that has run against airline customers for years.

The standing supply was ready before the stop. Fake airline support-number pages on free subdomain hosts and edge-hosting platforms, mass-seeded into forums and classifieds to rank for "airline reservation number" searches, were seeded in bulk on 12NOV, the day before. One number appeared on 17 hosts in Doppel telemetry that day alone; a second operator's series for another carrier had been running since early November. The pages are templates. On one, the headline names one carrier and the body text names another. When a stranded traveler searched for a number to call on 13NOV, these pages were already indexed.

FAKE AIRLINE SUPPORT-NUMBER PAGE ON A FREE SUBDOMAIN HOST



Seeded 12NOV2026, the day before the ground stop. The page's only content is a phone number.

Confirmed and actioned impersonation posts of a US carrier on one social platform rose from 76 a day on 12NOV to 261 a day on 17NOV. Doppel has not tied the post content to the ground stop; the lift coincides with it and with the start of holiday travel booking.

The bank slowdown, 16NOV

A transaction slowdown at one of the largest US banks is the ideal pretext for a text or a call saying a transfer did not go through and the account must be verified to release it. Public warnings to that effect went out within hours. In Doppel telemetry, newly surfaced lookalike hosts carrying the names of the largest US banks ran at 18 on 16NOV and 14 on 17NOV, inside the prior month's daily range of 2 to 46, and none of the 32 was confirmed as live impersonation. None carried Zelle's name. Text and call activity against financial-services brands on 16NOV sat inside its range for the month.

The absence is the finding. The bank-themed phishing supply already produces a steady run of new lookalike hosts every day. An actor who wanted to exploit the slowdown did not need to register anything; the next scheduled smishing wave went out as it would have anyway, into an audience that had just seen "some services aren't available" on a banking app.

The breaches started with trust

The three largest breaches of the period did not start with an exploit. The Binance theft began with a tampered installer and a job candidate's repository, the ConnectWise compromise with a consent grant customers had given the vendor's application years earlier, and the Barracuda intrusion with a cloud key a partner had left in a configuration file. The FBI's ARTEX FLASH describes what followed each of those footholds. AI agents chained reconnaissance, password spraying, consent abuse, lateral movement, and exfiltration, and some intrusions reached privileged access in under three hours.

The newest case did not need a breach at all. On 16NOV Optimizely's experimentation script, loaded by 178 organizations from the company's own CDN, carried an injected loader for about 19 hours. Every visitor to those sites ran it. It swapped wallet addresses on the page and in the clipboard, skimmed card numbers from the sites' own checkout forms, and on iPhones loaded exploit kits by iOS version. The sites' own infrastructure was untouched. Public reporting puts verified cryptocurrency losses in the thousands of dollars by that evening and Optimizely had the code removed within the day. The second-stage host has not appeared against protected brands in Doppel telemetry, and its DNS now points to a private address. The lesson defenders will be asked about is that a trusted third-party script is a dependency with write access to every page it loads on, the week before the heaviest card-entry days of the year.

Large thefts also feed a second wave. After every major exchange incident, recovery and refund scams target the people who lost money or fear they did. In Doppel telemetry, lookalike hosts carrying Binance's name ran at one to twelve a day before and after 29OCT with no rise in the two weeks following, so the second wave has not yet surfaced against protected brands. We assess, with low confidence given the short window, that it will arrive on Binance's own support channels and on social platforms before it arrives on lookalike domains, because that is where recovery scams after prior exchange incidents first appeared.

Black Friday is already open

Doppel confirmed the first lookalike page carrying Black Friday in its address on 01SEP2026, a month or more ahead of the 2025 ramp. This season's fake deals rarely name the holiday, mostly wear a non-retail brand (software, payments, travel, crypto), and sit in social groups or on borrowed hosting platforms rather than on lookalike domains. Public reporting now says the same about the early ramp, including a network of more than 10,000 fake stores imitating 166 fashion and luxury brands across 26 countries, tuned to rank in search results and already surfacing in AI shopping assistants. Black Friday falls on 27NOV2026 and Cyber Monday on 30NOV2026, and Grand Theft Auto VI lands on 19NOV with its own fake-download economy already in place, which Doppel documented earlier this month. The ground stop refund guidance, the Microsoft 365 sign-in prompts, and the holiday deal are now competing for the same inbox.

Doppel's view

Speed is the actor's advantage, and it is measured in hours. The first event-named domain appeared six hours after Microsoft's first advisory, the first harvesting page within a day, and the campaign Microsoft confirmed was detected the day after onset. Fake support-number pages were seeded the day before the ground stop, which means the actors did not predict the event; they maintain the pages continuously and the event found them ready.

The supply is standing, and the headline changes the hit rate. None of the events produced a measurable rise in sign-in phishing, bank lookalikes, or exchange lookalikes in Doppel telemetry. A "sign back in to your account" email that goes out at the same volume every day becomes the most credible message in the inbox on the day 400 million people are waiting for exactly that. Defenders who look for a spike will not see one. The exposure is in the match between standing lures and a population primed to act on them.

The breaches started with trust, not exploits. A job candidate, an installer, a supplier's consent grant, a key in a partner's repository, a contractor's document access, a marketing script every page already loaded. AI frameworks shortened the time from foothold to privileged access, and that shortening is real, but the foothold in each case was a person or a relationship. The due diligence that matters is on who and what is trusted into the environment, and on what a standing consent or a long-lived key is allowed to reach.

DURING AN OUTAGE OR INCIDENT IN THE NEWS

1. **Say where the real status lives before the first lure lands.** Publish the one status page, the one support channel, and the one refund route, through channels already established with employees and customers, and say that no other message about the event will ask for a login, a payment, or identity details.
2. **Treat "sign back in" and "your mail will be deleted" as the expected lure.** After any service disruption, brief help desks and employees that a message offering to restore access is the standing phish of the week, and route sign-ins through the application directly, never through a link in a notice.
3. **Never take a support number from a search result or a forum post.** Fake support-number pages are seeded continuously and rank within a day. The number on the card, in the app, or on the carrier's own site is the only one to call, especially during a disruption.

BEFORE THE HOLIDAY WINDOW

4. **State whether the organization runs holiday promotions, and where.** Brands that never run a sale still draw sale-themed lookalikes. Customer-facing teams need to know which promotions, domains, and ad accounts are real so they can say so when asked.
5. **Expect the refund intermediary and the scam to look alike.** Legitimate claims services and fraudulent ones ask for the same booking and card details within the same day of an event. Verify the operating company, its terms, and its payment processor before handing over a record locator or card digits.

STANDING POSTURE

6. **Inventory standing consents and long-lived keys.** The ConnectWise and Barracuda intrusions ran on access granted long before the event. Review which third-party applications hold consent into email and identity tenants, which keys live in partner repositories, and what each is allowed to reach.
7. **Treat recruiting and developer tooling as attack surface.** A take-home assignment, a package installer, and an internal AI assistant were each a step in the Binance theft. Isolate candidate code, verify installer provenance, and scope internal AI tools away from signing and secrets services.
8. **Know what third-party scripts run on customer-facing pages, and what they can reach.** One Optimizely snippet skimmed cards on 178 brands' own checkout pages without touching their servers. Inventory every external script on pages that take a login or a payment, pin what can be pinned, and set a content security policy that names the hosts allowed to load code.

Indicators

Indicators from the activity above.

INDICATOR	ROLE	FIRST SEEN
`microsoftoutage[.]com`	Event-named squat, revenue counter, no inputs	12NOV2026 22:37 UTC (registration)
`outlookoutage[.]com`	Event-named "outage forum" with its own account registration	13NOV2026 02:41 UTC (registration)
`winrefrequests[.]com`	Outage refund form, identity and payment harvesting	13NOV2026 15:12 UTC (registration)
`julliesite[.]xyz`	Relay endpoint receiving the refund form submissions	28JUL2026 (registration)
`mivorantul[.]com`	Service-health campaign landing, random subdomain behind a bot check	04AUG2026 (registration); first scanned 13NOV
`reallifeaccounting[.]com`	Campaign redirector serving a decoy blog to non-targets	15NOV2026 (first public scan)
`moments-notice[.]com`, `planetmaison[.]com`, `newbooker[.]com`	Service-health campaign sender domains, published by Microsoft	13NOV2026
`flighthelp24[.]com`, +1 844-480-0252	Assessed phone-fee travel agency, payment by phone only	15NOV2026 (registration)
+1 845-422-9701, +1 716-351-6210, +1 802-392-0167	Fake airline support numbers, one operator cluster	12NOV2026 (bulk seeding)
+1 833-253-7012, +1 833-341-3142	Fake airline support numbers, second carrier	03 to 13NOV2026
`1688360[.]cc` (`/track.js`, `/card.php`)	Second stage of the 16NOV Optimizely injection (wallet swap, card skimmer, exploit-kit router)	16NOV2026 04:21 UTC

Findings are based on Doppel telemetry across a global customer base, with strongest coverage in North America.

Doppel

Our mission is to protect the world from social engineering attacks every day. Our AI-native defense anticipates deception and eliminates threats.

1B+ INDICATORS ANALYZED DAILY **300+** TRUSTED CUSTOMERS doppel.com

Prepared by Doppel SECR - Social Engineering Counterintelligence & Research

© Doppel Inc. 2026. All Rights Reserved.