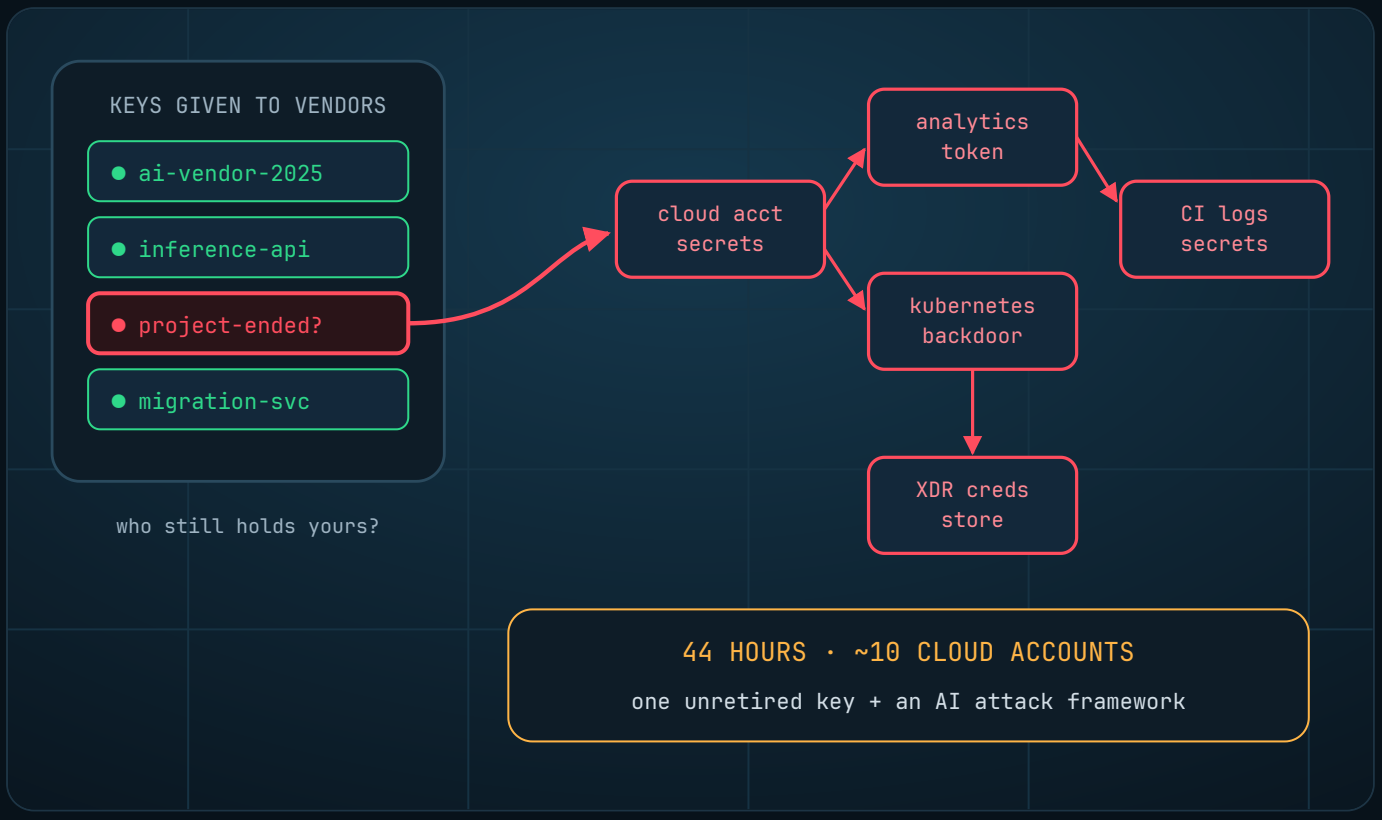
MAG212
CYBER

DAILY

Tuesday, 17 November 2026

DAILY CYBER INTELLIGENCE · CUTOFF 6:00 AM PT



THIRD-PARTY ACCESS / NOV 14-17

Keys that outlived the job

Barracuda left a cloud key with an AI vendor after the project ended. Fireworks AI's breach spilled into Uber, Cursor and Notion. Infoblox lost data through a SharePoint migration firm. Today's breaches all started with access someone else held.

03 Barracuda: one forgotten key, 44 hours, ARTEX

05 Fireworks AI breach reaches Uber, Cursor, Notion

06 Infoblox: migration vendor exposes NIOS backups

07 Google: AI agents turn patches into exploits

09 Copeland XWEB EVO: 14 flaws, probed in 2 hours

10 Briefs: Telegram widgets, Retadup, SANSAR, BIS

What matters today

Developments published or updated 14–17 November. Fireworks and Copeland follow earlier coverage; each article says what changed.

Vendor credentials are the new perimeter

Barracuda's intruder used a key issued to an AI vendor and never retired. Uber's driver data, Cursor's traces and Notion chats leaked through Fireworks AI. Infoblox's SharePoint data left through a migration vendor. [1][9][14]

AI agents run the intrusion

Barracuda matched its 44-hour intrusion to ARTEX. Google's GTIG found exploit_agent, which diffs patches, writes exploits and runs them with no human step. [1][17][19]

Refrigeration controllers, again

VulnCheck published 14 CVEs in Copeland XWEB EVO; scanners hit one within about 1 hour 40 minutes. Five flaws in the latest firmware will never be fixed: the product is end-of-support. [21]

Policy and platforms

Commerce's BIS now requires overseas data centres serving China and others to identify end users. Telegram's new widgets drew RCE demos and a malware warning in their first week. [27][24]

THE THREE PRIORITY ACTIONS

1. **Inventory and kill every credential a vendor holds.**
   List keys, service principals and tokens issued to third parties; check last use; revoke anything tied to a finished project. Barracuda's own advice: no standing, long-lived vendor credentials. [1][28]
2. **If you were notified by Barracuda, Fireworks, Uber or Infoblox, act on it today.**
   Recreate Barracuda XDR/Monitored Endpoint integration credentials; rotate keys Cursor emailed you; Infoblox customers should ask what NIOS data was taken and rotate secrets stored in grid configuration. [2][8][16]
3. **Take XWEB EVO off the internet and plan its replacement.**
   No fixes are coming. Block inbound access, hunt for config.lua and xwconsole.cgi requests, and budget for XWEB Pro or another supported controller. [21][23]

CONTENTS

03 Barracuda: anatomy of a 44-hour intrusion
04 Barracuda: hunt your own vendor keys
05 Fireworks AI: one vendor, many breaches
06 Infoblox: the migration vendor door
07 GTIG: exploit_agent and patch-to-exploit
08 GTIG: Claude Code hook backdoor, LLMjacking
09 Copeland XWEB EVO: 14 CVEs, no fixes
10 Briefs
11 Defender's Action Desk
12 Awareness: the key you forgot
13 Sources

CONFIRMED BY BARRACUDA | ENTRY: VALID VENDOR KEY | TOOLING: ARTEX (METHOD, NOT ACTOR)

Barracuda: one forgotten key, 44 hours inside

KEY FACT **What Barracuda says.** The intruder did not exploit Barracuda software. It used a valid cloud access key Barracuda had issued to an AI vendor for an earlier project and never retired; the vendor's own development environment was breached in October. Barracuda's words: “That is on us.” [1][4]

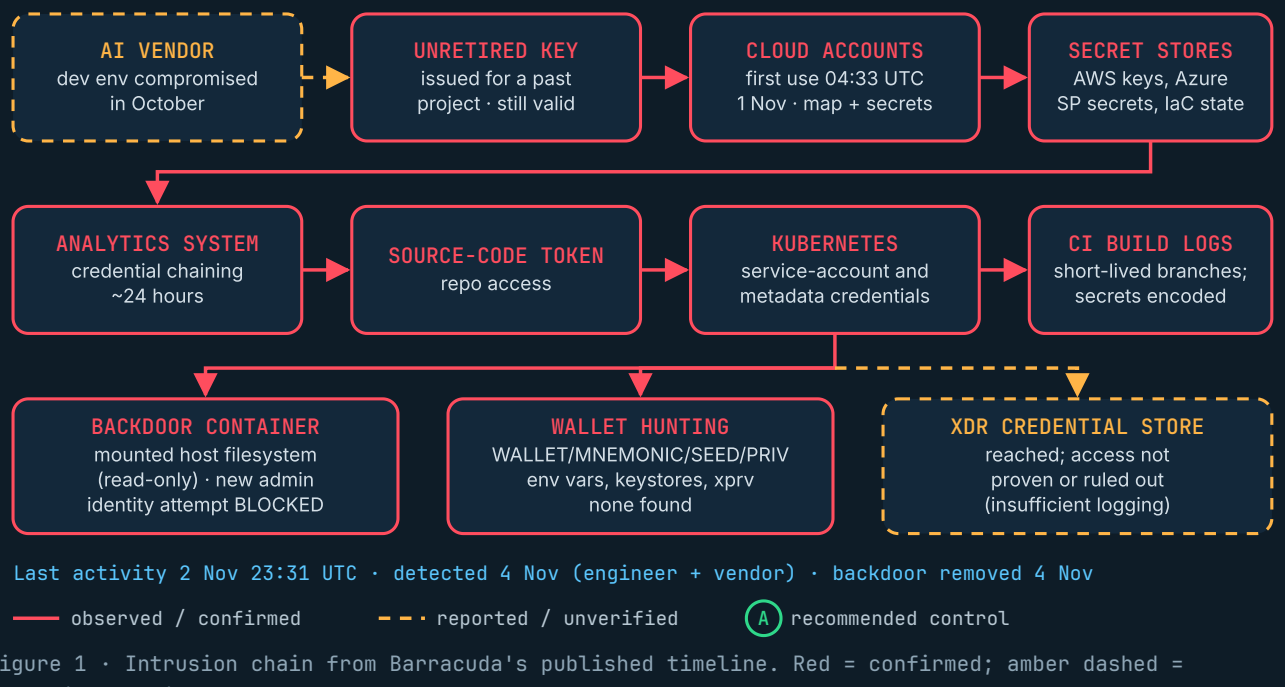


Figure 1 · Intrusion chain from Barracuda's published timeline. Red = confirmed; amber dashed = unconfirmed. Diagram: MAG212 CYBER.

HOW THE ATTACK WORKED

After mapping what the key could reach, the attacker chained credentials: cloud accounts to a data analytics system, that system to a source-code token, the token to Kubernetes clusters. It decrypted infrastructure-as-code state files and pulled credentials from server metadata services and Kubernetes service accounts. In about four hours on 2 November it pushed short-lived branches so a build workflow printed secrets to job logs, encoded to beat log masking. [1]

WHY ARTEX

Machine-style resource labels (“i” plus digits), task ordering and credential and wallet-hunting routines matched ARTEX, the open-source agentic pentest framework the FBI warned about on 13 November. Many groups use it, so Barracuda names the method, not the actor. [1][3][5]

WHO IS AFFECTED

Customers of **Barracuda Managed XDR Cloud** and **Monitored Endpoint** whom Barracuda contacted: their API integration credentials sat in a store the attacker reached. Others need no action, per Barracuda. [1][2]

DATE (UTC)	EVENT	SOURCE
Oct	AI vendor's development environment compromised; key likely taken there	Barracuda
1 Nov 04:33	First use of the key; ~10 accounts touched over ~44 h	Barracuda
2 Nov 23:31	Last recorded activity	Barracuda
4 Nov	Engineer reports anomaly; vendor reports its own incident; containment	Barracuda
10–16 Nov	Trust Center advisory (10th), blog (11th), press coverage (16th)	Barracuda, SW, BC

Hunt the keys you handed out

AWS CLI v2 | IAM read (iam:List*, Get*) | READ-ONLY | NOT TESTED BY MAG212

AWS · VENDOR KEY REVIEW

```
aws iam list-access-keys --user-name <VENDOR_USER>
aws iam get-access-key-last-used --access-key-id <ACCESS_KEY_ID>
aws cloudtrail lookup-events --max-results 50 \
  --lookup-attributes AttributeKey=AccessKeyId,AttributeValue=<ACCESS_KEY_ID>
```

Lists a vendor user's keys, shows when and where each was last used, and pulls recent management events for one key. A key with no business use in months is a candidate for removal. CloudTrail event history covers 90 days of management events only. [28][29]

Azure CLI + kubectl + jq | Entra read · cluster read | READ-ONLY | NOT TESTED BY MAG212

AZURE + KUBERNETES · BLAST-RADIUS CHECK

```
az ad sp credential list --id <APP_ID> --query "[].{id:keyId,end:endDateTime}"
kubectl get pods -A -o json | jq -r '.items[]
  | select(any(.spec.volumes[]?; .hostPath)) | "\(.metadata.namespace)/\(.metadata.name)"'
```

First line lists a service principal's secrets and expiry dates. The pipeline lists every pod that mounts a host path, the technique Barracuda's intruder used to read node credentials. Legitimate agents (CNI, logging, monitoring) also do this, so compare with a known list. [30][31][1]

WHAT TO LOOK FOR

- API calls from a vendor's key outside its project window or from new networks.
- Bulk secret-store reads (Secrets Manager, Key Vault) and IaC state-file downloads.
- Short-lived branches that trigger CI and are deleted; base64-looking strings in build logs.
- New pods with hostPath mounts; attempts to create admin identities.
- Resource names like “i” plus digits, which Barracuda tied to ARTEX. [1]

No IP addresses or hashes were published, so detection rests on behaviour.

CONTAIN AND REMEDIATE

1. Barracuda XDR customers who were contacted: revoke and recreate API integration credentials per the Trust Center steps. [2]
2. Revoke vendor keys tied to finished work; replace the rest with short-lived, narrowly scoped credentials. [1]
3. Assume the worst: treat every secret reachable from a compromised key as exposed and rotate it.
4. Remove unknown containers and identities; rebuild nodes from known-good images.
5. Mask and scan CI logs; block secrets in job output; require review for workflow changes.

VERIFY RECOVERY

- Old keys fail; new ones work only from expected sources.
- No hostPath pods outside the approved list.
- Secret-store and CI audit logs quiet.

UPDATE TO WEEKLY 14 NOV | CONFIRMED BY UBER, CURSOR, FIREWORKS | ATTACKER: UNKNOWN

Fireworks AI: one vendor, three customers' breaches

STATUS **What changed since our Weekly.** We covered Cursor's poisoned Claude Code extension. Since then Cursor named Fireworks AI as the starting point (13 Nov), Uber began notifying ~150,000 drivers whose data sat with Fireworks, Notion confirmed chat exposure, and Fireworks widened its own scope on 9 November. [8][9][10][33]

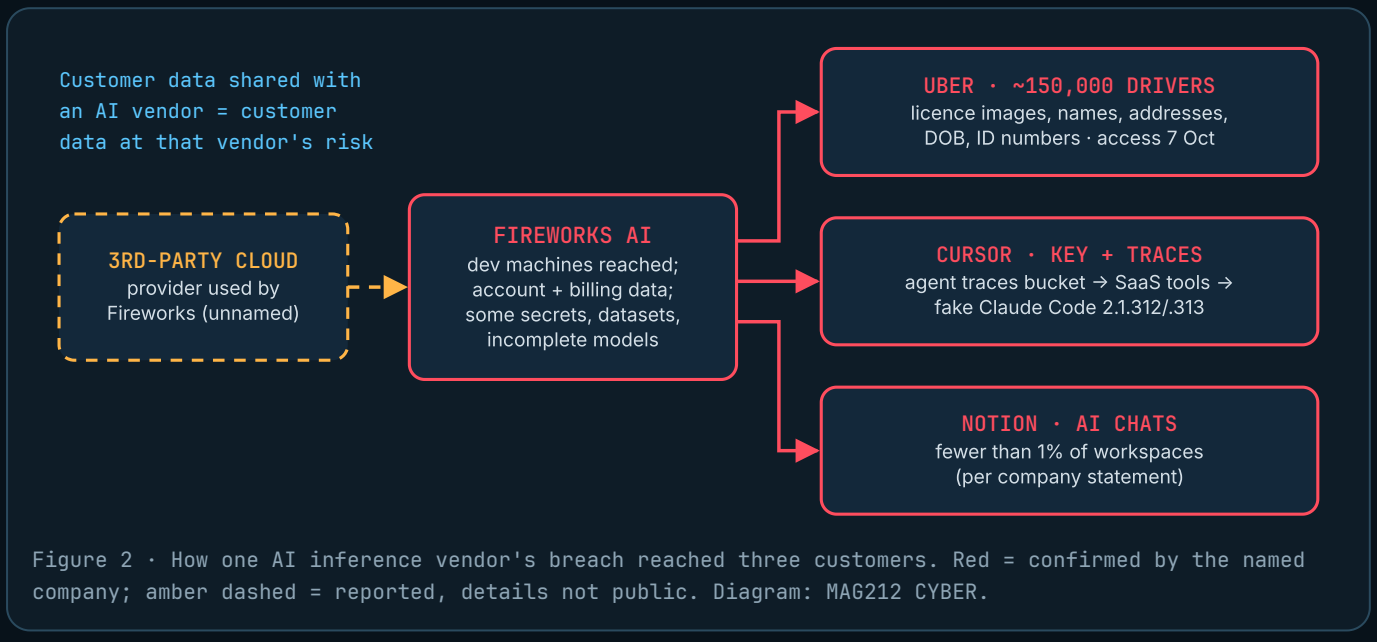


Figure 2 · How one AI inference vendor's breach reached three customers. Red = confirmed by the named company; amber dashed = reported, details not public. Diagram: MAG212 CYBER.

UBER

On 7 October attackers used the provider's compromised credentials to reach data Uber had shared with it; Uber learned on 9 October and confirmed misuse on 13 October. The data sat in an environment run by Uber's cloud security team; alerts were on but did not fire because the credentials were valid. Uber says they gave no access to other Uber systems and offers credit monitoring. A Texas filing reportedly lists 149,346 people. [9]

FIREWORKS

Its first bulletin found no evidence of access to customer models or datasets. The 9 November update says attackers reached development machines through a third-party cloud provider and touched account and billing data (not card numbers) and, for a limited set of accounts, secrets, datasets and incomplete models. [10][12]

CURSOR

A key Cursor issued to Fireworks, exposed by Fireworks, was used to copy a read-only bucket of mostly 2025 agent traces from non-Privacy-Mode sessions; under 0.01% of customers had API credentials in them. Those credentials led into SaaS tools and, on 29 October, to tampered Claude Code 2.1.312 and 2.1.313 builds served to at most 5,000 users for about 11 hours. [8]

WHAT TO DO

1. Cursor users who installed 2.1.312/.313 from Cursor's marketplace: follow the 30 October notice; uninstalling may not be enough. [8]
2. Rotate any key Cursor or Fireworks emailed you about. [8]
3. Uber drivers: enrol in the offered monitoring; watch for ID-based fraud.
4. Every org: list data shared with AI vendors and the credentials they hold for you.

CONFIRMED 16 NOV | DATA DETAIL: REPORTED, NOT CONFIRMED BY INFOBLOX | COUNTS: UNDISCLOSED

Infoblox: the migration vendor's door

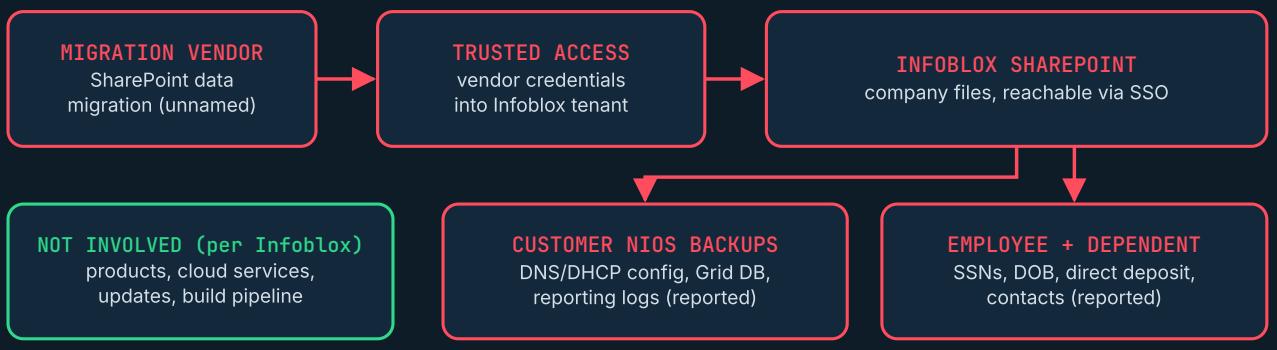


Figure 3 · Path as reported by TechCrunch and The Register. Red = confirmed or reported; green = Infoblox statement. Diagram: MAG212 CYBER.

WHAT HAPPENED

Infoblox, which sells DNS, DHCP and IP address management (DDI) and security services, confirmed on 16 November that it is investigating unauthorised access to company information through a compromised third-party data migration vendor. It activated incident response, contained the incident and brought in outside experts. [14]

A breach notification seen by TechCrunch's sources says the vendor provides SharePoint data migration services; one source said Infoblox ended work with the vendor. Infoblox says it has no indication its products, cloud services, software updates or build-and-release processes were involved. [14]

WHAT WAS REPORTEDLY TAKEN

According to The Register, sources say the data included NIOS configuration snapshots for some customers: saved copies of DNS and DHCP configuration, Grid databases and reporting logs that can rebuild an appliance or Grid. A CEO email it saw lists employee and dependent data: direct-deposit details, contact information, dates of birth and Social Security numbers. Infoblox declined to give data types or counts. [15][16]

WHY A NIOS BACKUP MATTERS · MAG212 ANALYSIS

A Grid backup is a blueprint of an organisation's core network: zones, subnets, DHCP scopes, server roles. Depending on configuration it may also hold secrets used by the Grid. Customers cannot yet know which of their items were in scope, so plan as if the snapshot is in hostile hands.

FOR INFOBLOX NIOS CUSTOMERS

1. Check for an Infoblox notification; ask whether your Grid's backups were in scope and from which date.
2. If yes, rotate secrets your Grid configuration stores: admin and API accounts, TSIG and DNSSEC keys, directory/RADIUS/SNMP integration credentials.
3. Review Grid admin audit logs for unknown logins since the snapshot date.
4. Expect targeted phishing that uses accurate internal hostnames and IP ranges.

FOR EVERYONE

- Migration vendors get broad, temporary access: time-box it, scope it to the data being moved, and revoke it on completion.
- Do not leave appliance backups in collaboration sites.

GOOGLE GTIG + MANDIANT · 16 NOV | FIRST OBSERVED IN THE WILD

FULL REPORT NOT READABLE AT CUTOFF

exploit_agent: from patch to attack with no human

Google's Threat Intelligence Group says attackers now run LLM pipelines that watch software updates, work out which flaw was fixed and build an attack for it. Its centrepiece is a framework it calls exploit_agent, which GTIG describes as the first fully autonomous patch-to-attack chain it has seen outside a lab. [17][19]

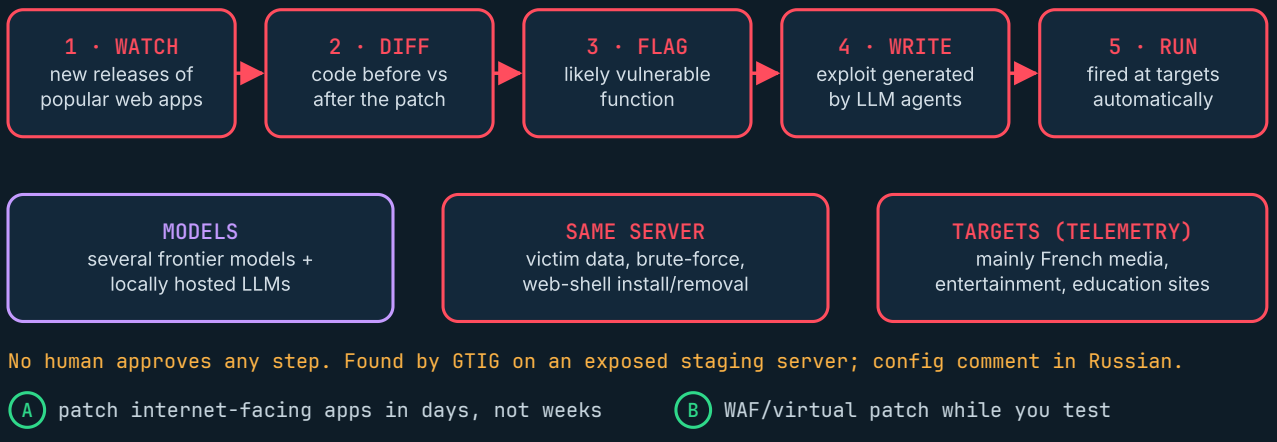


Figure 4 · exploit_agent workflow as reported from GTIG's findings. All red steps are GTIG observations. Diagram: MAG212 CYBER.

FINDING (GTIG Q4 AI THREAT TRACKER)	DETAIL
Frameworks in use	ARTEX, CAIRN (US aerospace breach), CyberStrikeAI, PentAGI (Asia scanning, late Aug–early Oct); HexStrike AI under test
Patch race example	PaperCut NG/MF: two flaws chained as zero-days in late August; working exploits within a day; mass campaign four days after disclosure
LLMjacking	Stolen LLM and cloud keys resold through 'LLM mixers' (APIMart, JetNight); Mandiant saw over $100,000 in fraudulent charges in one day
Phishing	Chinese-language Jieyou kit added an LLM chatbot so affiliates build lures in plain language

WHY PATCHES, NOT ZERO-DAYS

GTIG's reasoning: a patch diff, release notes and any proof of concept narrow the search to a few functions, which is cheaper than hunting new bugs. Defenders' patch window is what the agents are racing. [19][20]

WHAT GOOGLE DID

Disabled the implicated accounts and assets, fed findings into model classifiers, released Google SecOps detection rules for ARTEX and pointed to a Mandiant hardening guide. [19]

Details come from Google's summary post and press coverage of the report; MAG212 could not load the full GTIG report before cutoff.

Backdoors in the AI coding config, and stolen AI keys for sale

UNC6836: A BACKDOOR THAT LAUNCHES WITH THE TOOL

GTIG reports that UNC6836, which coverage describes as a suspected North Korean group, edited `.claude/settings.json` files in internal code repositories so that Claude Code downloaded a backdoor, SOMBERMEME, every time a developer started it. [19]

The lesson is general. AI coding tools read project-level settings that can run commands (Claude Code calls them hooks). Anyone who can commit to a repository can therefore make every developer who opens it run their code. [32]

WHAT TO LOOK FOR

- Commits to `.claude/`, `.cursor/`, `.vscode/` or similar folders by unusual authors or without review.
- Hooks or tasks that fetch remote content (curl, wget, PowerShell download).
- Developer machines making new outbound connections right after an AI tool starts.

LLMJACKING: YOUR AI BILL AS LOOT

Attackers steal LLM API keys and cloud credentials from compromised companies, then resell access through 'LLM mixers' such as APIMart and JetNight. Mandiant saw more than $100,000 in fraudulent charges in a single day and estimates up to $1 million in the worst case. This matches Amazon's ARTEX key-theft findings we covered yesterday. [19][20][35]

CONTROLS

1. Require code-owner review for AI tool config folders (CODEOWNERS or branch protection).
2. Turn on secret scanning; keep LLM keys out of repos, CI logs and agent traces.
3. Set provider spend alerts and per-key quotas; rotate keys on a schedule.
4. Patch internet-facing web apps within days; virtual-patch where you cannot.

git (any OS) | repo read | READ-ONLY | NOT TESTED BY MAG212

REPOS · CLAUDE CODE SETTINGS REVIEW

```
git log --all --oneline -- '.claude/settings.json' '*/.claude/settings.json'
git grep -n -E '"hooks"|curl |wget |Invoke-WebRequest|bash -c' \
  -- '*.claude/settings*.json'
```

Run in each repository. The first command shows every commit that touched a Claude Code project settings file; the second finds hook definitions and download commands inside them. Hooks are a documented feature, so a match is a lead to review, not proof of compromise. [32][19]

ARTEX IN THE WILD · AS REPORTED THIS MONTH

WHO	WHAT	SOURCE
Vapor Panda (China, espionage)	Used ARTEX in October against 200+ organisations in 14 countries	SentinelOne via SW
Storm-0940 / Storm-3358	State-sponsored and financially motivated groups using ARTEX	Cisco Talos via SW
Exposed consoles	About 1,500 internet-facing ARTEX consoles in early November	Censys
Barracuda, Railway	Cloud intrusions matched to ARTEX-like harnesses	Barracuda, Railway

Vendor attributions as reported by SecurityWeek [3]; Censys [6]; Railway [7]. Not independently verified by MAG212.

FOLLOWS DANFOSS, 16 NOV | 14 CVEs · 2 EXPLOITED | END OF SUPPORT · 5 NEVER FIXED

Copeland XWEB EVO: probed within two hours

SPEED Timeline. CVE records went live 12 November at 20:18 UTC; VulnCheck's canaries saw the first config.lua write attempt at 22:00 UTC, with no public proof of concept. One Tokyo-geolocated VPS sent 125 requests overnight; a Hong Kong host probed xwconsole.cgi from 03:41 UTC on 13 November, running only `id`. VulnCheck calls both opportunistic, not the October campaign. [21][22]

CVE	FIRMWARE	ISSUE	STATUS
CVE-2026-124010	Legacy	Unauth GET to setuid-root xwconsole.cgi runs a command	EXPLOITED
CVE-2026-124014	Legacy	Unauth write of system config file via config.lua	EXPLOITED
CVE-2026-124002 / -007	Legacy	Command injection in login.lua (user / password field)	—
CVE-2026-124004	Legacy	Hardcoded Administrator backdoor password	—
CVE-2026-124005 / -012	5.8.8	Daily admin password derived from MAC + date; login with it	NO FIX
CVE-2026-124011	5.8.8	sysinfo.lua leaks MAC and clock without auth	NO FIX
CVE-2026-124006	5.8.8	Root password rebuilt daily from fixed prefix + code	NO FIX
CVE-2026-124013	5.8.8	Authenticated command injection (api.lua import)	NO FIX

Selected CVEs from VulnCheck's disclosure of 13 November [21]. Legacy = pre-2021 Lua-era builds (tested 5.2.3); 5.8.8 = current firmware.

WHO IS AFFECTED

Dixell XWEB EVO supervisory controllers, now sold as Copeland, used to run refrigeration in supermarkets and cold stores. Copeland ended software support on 16 March 2026 and recommends XWEB Pro. Onyphe counts about 1,960 exposed EVO hosts against 108 XWEB Pro. CERT-FR named XWEB controllers among those hit in October's French attacks. [21][22][23]

WHY THE CURRENT FIRMWARE FALLS

The daily admin and root passwords come from the MAC address and date, and an unauthenticated page discloses both. An attacker can compute the password offline, enable SSH and log in as root. [21][22]

CONTAIN AND REMEDIATE

1. Block all internet access to XWEB EVO; allow access only over VPN.
2. Hunt for the request patterns below; if found, treat the controller as compromised and rebuild from a known configuration.
3. Check setpoints, defrost schedules, users and SSH status, as for Danfoss.
4. Budget and schedule replacement: there will be no fixes. [23][34]

Linux · zgrep | log read | READ-ONLY | NOT TESTED BY MAG212

XWEB EVO · ATTEMPT HUNT

```
zgrep -E 'POST [^ ]*config\.lua|GET [^ ]*xwconsole\.cgi' <PROXY_OR_FW_LOG>*
zgrep -E '202\.61\.138\.117|177\.4\.12\.11' <FIREWALL_LOG>*
```

Looks for the two request patterns VulnCheck saw exploited and the two scanning IPs it recorded. Only works if your logs capture HTTP paths to the controller; a match shows an attempt, not success. [21]

Also today

MESSAGING · DISPUTED

Telegram widgets: RCE demos and a malware warning in week one

Telegram's new widgets, promoted on 10 November, let messages act as apps; researchers say they run the QuickJS engine without a sandbox. A researcher posted a video of a bot interaction opening Calculator on Android. On 13 November Kaspersky said a widget flaw may have been used to deliver WebRAT (Salat Stealer) via PowerShell, without technical details. Durov says a user had to start a third-party service first and that the issue is fixed server-side; the Android fix is deployed, a Windows claim is unconfirmed. Kaspersky advises not launching widgets until fixed. [24]

MALWARE · WINDOWS

Retadup worm returns with CoffeeLoader

The USB worm taken down by French police in 2019 is back after someone re-registered its old C2 domains. Kaspersky says the new chain drops a tampered 7-Zip library (7z.dll) into a temp folder, runs it with rundll32, persists via a Run key with an eight-hex-digit name and injects into processes such as dllhost.exe and WerFault.exe. About 15,000 infections were blocked, mostly in Peru, Angola, Russia and Bolivia. Hunt for 7z.dll outside the 7-Zip folder. [25]

MALWARE · GPU / LINUX

SANSAR hides crypto-mining from nvidia-smi

Elastic found attackers entering GPU hosts through an exposed Ray job agent, then adding an SSH key. The Rust toolkit takes orders over Tor and runs XMRig or SRBMiner. A modified NVML wrapper makes nvidia-smi show 0% use with fake temperature and power, a DKMS kernel rootkit reloads at boot, and a backdoor reads its C2 address from an Ethereum contract. Audit who can submit Ray jobs and check GPU libraries for tampering. [26]

POLICY · EXPORT CONTROLS

BIS targets remote access to US AI chips

Commerce's Bureau of Industry and Security issued a rule on 16 November, effective immediately: overseas data centres serving companies in countries such as China, Russia, Iran and Cuba must identify their end users. Chip sales to Indonesia, Malaysia, Singapore, Thailand and Brazil face case-by-case licensing. Cloud and GPU-hosting providers should review know-your-customer processes. [27]

STILL OPEN FROM EARLIER ISSUES

ITEM	STATUS ON 17 NOV	SEE
Danfoss AK-SM800A six pre-auth flaws	No fix or CVE published	Daily 16 Nov
UnrealIRCd and Check Point KEV	Federal deadline passed 16 Nov	Daily 16 Nov
ARTEX key theft (Amazon)	IoCs and lockdown steps unchanged	Daily 16 Nov

Your work list for today

Ordered by urgency. Each row points to the page with evidence, commands and verification steps.

WHEN	TEAM	ACTION	SEE
TODAY	Cloud / IAM	List every key, service principal and token issued to vendors; revoke those for finished work.	p.04
TODAY	Barracuda XDR	If contacted, revoke and recreate Managed XDR / Monitored Endpoint integration credentials.	p.04
TODAY	OT / facilities	Block internet access to Copeland XWEB EVO and Danfoss AK-SM800A; hunt config.lua / xwconsole.cgi hits.	p.09
48 H	Network (Infoblox)	Ask Infoblox if your Grid backups were in scope; rotate Grid-stored secrets if so.	p.06
48 H	Developers	Check for Claude Code 2.1.312/.313 from Cursor's marketplace; rotate keys you were emailed.	p.05
48 H	Platform	Review hostPath pods, CI log masking and secret-store access logs.	p.04
THIS WEEK	Engineering	Code-owner review on .claude/, .cursor/, .vscode/; secret scanning on all repos.	p.08
THIS WEEK	Vuln mgmt	Set patch targets in days for internet-facing web apps; virtual-patch the gap.	p.07
THIS MONTH	Procurement	Contract clauses: credential expiry, scope, breach notice for AI and migration vendors.	p.12

ONE-PAGE HUNT SHEET

AWS	`get-access-key-last-used` on vendor keys; CloudTrail by AccessKeyId.
Azure	`az ad sp credential list`: long-lived secrets on vendor apps.
Kubernetes	Pods with hostPath volumes; new admin identities; unknown containers.
Repos / CI	Commits to `.claude/settings.json`; secrets in job logs.
OT	POST to `config.lua`, GET `xwconsole.cgi`; IPs 202.61.138.117, 177.4.12.11.

BEFORE YOU CLOSE A TICKET

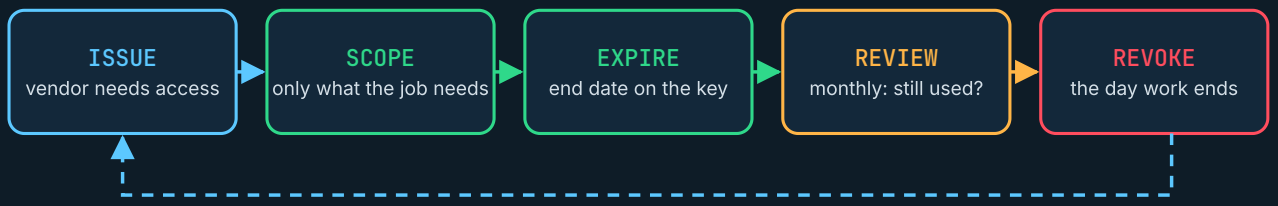
- Confirm revoked keys fail; test from outside.
- Rotate every secret the compromised identity could read.
- Keep logs and images before cleaning.
- Record vendor, scope and expiry for every credential you issue.

COMMAND SAFETY

Every command in this issue is read-only and checked against vendor documentation, but none was run by MAG212. Test on one system first, use the least privilege shown, and replace <PLACEHOLDERS> with your values.

The key you forgot to take back

A five-minute lesson for managers, project leads and anyone who works with outside vendors.



Barracuda's key skipped the last step. That was enough.

Uber, Cursor, Notion and Infoblox trusted a vendor's own security with their data.

Figure 5 · Vendor access lifecycle. Conceptual illustration, MAG212 CYBER.

FOR BUSINESS LEADERS AND PROJECT OWNERS

- Every vendor project should end with a checklist item: revoke the access we gave them.
- Ask suppliers where your data lives with them, who can reach it, and how fast they will tell you about a breach.
- AI vendors often hold copies of your data for training or evaluation. Treat them like any other processor of sensitive data.
- Fund short-lived credentials and an inventory of who holds what; it is cheaper than a breach notice.

FOR EMPLOYEES

- Never paste passwords, keys or tokens into support tickets, chats or AI tools. Cursor's attacker reached credentials users had sent to support.
- If you created an access key for a supplier, tell IT when the project ends.
- Report odd activity on your own account at once. That is how Barracuda caught its intruder.
- Expect phishing that quotes real breaches: Uber, Infoblox or Barracuda in the subject line.

THREE QUESTIONS FOR YOUR NEXT TEAM MEETING

1. Which vendors hold keys or accounts into our systems today?
2. Which of those projects have already ended?
3. What customer or employee data have we sent to an AI vendor, and is it still there?

LESSONS BARRACUDA PUBLISHED ABOUT ITS OWN BREACH

- Remove standing, long-lived credentials, especially those held by third parties.
- Use short-lived, narrowly scoped credentials so one key cannot open the next system.
- Plan for compromise: be able to rotate secrets at scale and rebuild from known-good states.
- Share indicators early, even before impact is confirmed.

Paraphrased from Barracuda's post [1].

Sources

[1] Barracuda · 11 Nov · Anatomy of a machine-speed intrusion

[2] Barracuda Trust Center · 10 Nov · Barracuda XDR integration credentials advisory

[3] SecurityWeek · 16 Nov · Barracuda hacked amid surge in Artex-powered cyberattacks

[4] BleepingComputer · 16 Nov · Barracuda links cloud breach to ARTEX AI-powered cyberattack

[5] FBI · 13 Nov · Cybersecurity advisory on ARTEX (FLASH, PDF)

[6] Censys · Nov · ARTEX: agentic asbestos (exposed consoles)

[7] Railway · Oct · Incident report: October security incident

[8] Cursor · 13 Nov · Security incident update

[9] SecurityWeek · 16 Nov · Uber data breach impacts 150,000 people

[10] PYMNTS (citing TechCrunch) · 16 Nov · Hackers breach Fireworks AI and steal data from Uber, Notion and Cursor

[11] Tech Times · 15 Nov · Uber data breach: hackers compromised AI vendor Fireworks

[12] CybersecurityNews · 10 Nov · Hackers breach Fireworks AI through third-party cloud provider

[13] The Hacker News · 15 Nov · Cursor says stolen Fireworks AI key led to trojanized Claude Code extension incident

[14] TechCrunch · 16 Nov · Cyber giant Infoblox confirms security incident after hackers access company information

[15] SC Media (citing The Register) · 16 Nov · Infoblox investigates data breach involving third-party vendor

[16] The Register (via SecOpsNews) · 16 Nov · Infoblox customer and staff data exposed in SharePoint breach

[17] Google (GTIG) · 16 Nov · The era of autonomous attacks has arrived

[18] Google Cloud (GTIG) · 16 Nov · Agentic threat activity crosses a significant threshold (full report; not readable at cutoff)

[19] ITdaily · 16 Nov · Google sees AI agent turn patches into exploits without human intervention

[20] The Hacker News · 16 Nov · Google finds hackers using AI agents to build and run exploits from software patches

[21] VulnCheck · 13 Nov · Copeland XWEB EVO: unauthenticated root (14 CVEs)

[22] SecurityWeek · 16 Nov · Hackers probe newly disclosed flaws in Copeland refrigeration controllers

[23] Copeland · Mar · XWEB EVO end-of-software-support product bulletin (PDF)

[24] SecurityWeek · 16 Nov · Telegram widgets hit by RCE demos, malware warning days after launch

[25] The Hacker News · 16 Nov · Retadup worm resurfaces 7 years after takedown to spread CoffeeLoader

[26] The Hacker News · 16 Nov · SANSAR Linux cryptomining malware uses modified NVIDIA library

[27] SecurityWeek · 16 Nov · Trump administration moves to block China from indirect access to American AI technology

[28] AWS CLI reference · docs · iam get-access-key-last-used

[29] AWS CLI reference · docs · cloudtrail lookup-events

[30] Microsoft Learn · docs · az ad sp credential list

[31] Kubernetes · docs · Volumes: hostPath

[32] Anthropic · docs · Claude Code settings and hooks

[33] MAG212 CYBER · 14 Nov · Cursor extension backdoor and the Fireworks AI vendor key (Weekly)

[34] MAG212 CYBER · 16 Nov · Danfoss AK-SM800A: six unpatched pre-login flaws

[35] MAG212 CYBER · 16 Nov · ARTEX agents stole AI keys to pay for more attacks

[36] The Hacker News · 16 Nov · Weekly recap: N-able 0-days, Windows 0-days, Chrome 0-days, fridge 0-days

HOW WE VERIFIED THIS ISSUE

- Primary sources read: Barracuda's blog post, Cursor's incident update, VulnCheck's disclosure and Google's GTIG summary post.
- Google's full GTIG report would not load before cutoff; exploit_agent, UNC6836 and LLMjacking details come from press coverage of it (ITdaily, The Hacker News) and are labelled.
- Infoblox data types come from The Register's sources and a CEO email it saw, via SC Media and a news aggregator; Infoblox has not confirmed them. Uber figures come from SecurityWeek and state filings it cites.
- No command in this issue was executed by MAG212. Older items (GPUStack KEV of 9 Nov, Maersk of 11 Nov) were left out as more than 72 hours old.

Read.
Verify.
Defend.

Free daily intelligence, CVE explainers and practical defensive guidance from MAG212 CYBER.

SUBSCRIBE FREE

Get every issue in your inbox

cyber.mag212.com/subscribe-free

MAG212 ATLAS · LIVE DEMO

Map every network before you test it

demo.atlas.mag212.com

WORK WITH MAG212 CYBER

Penetration testing
Find the forgotten edge before someone else does.

Network & security consulting
Inventory, segmentation and remote-access design.

Training
For staff, IT teams, leaders and schools.

cyber.mag212.com/services

Watch the Atlas walkthrough: youtu.be/j27B5g3viKw

MAG212 CYBER

Daily · 17 November 2026
Understand the threat. Build the defense.