CYBER OPERATIONS

WEEKLY INTELLIGENCE

SUPPLY-CHAIN INTELLIGENCE

Issue #001: Beyond The Headlines

Of the organisations named this period, 100 left no public trace of it at all.

20 – 24 July 2026

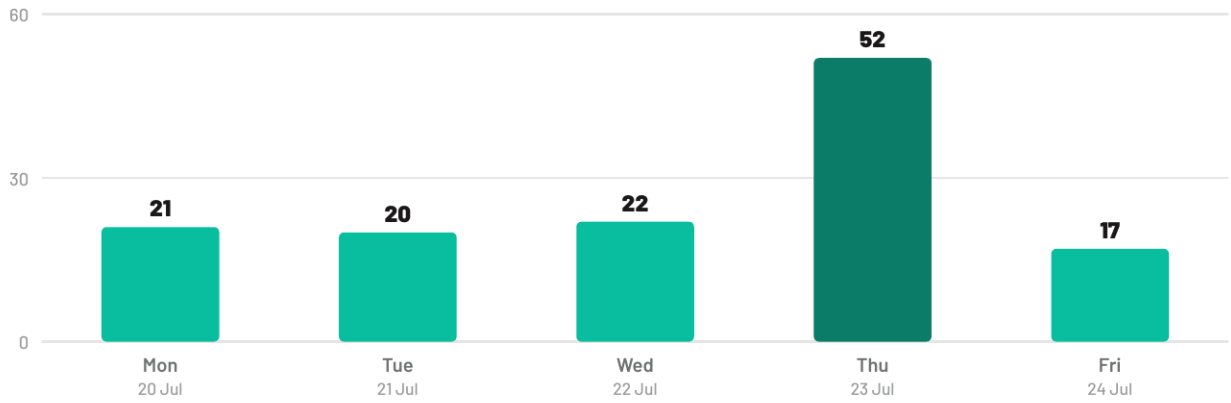
Contents

01 Executive summary

20 – 24 July 2026

Averro Weekly Intelligence is an outside-in assessment of the threat to enterprise supply chains. Each issue is built from six layers: the organisations publicly named as victims by ransomware and extortion groups; whether anyone outside those organisations — a customer, a regulator, you — could find out it happened; the credential exposure those organisations were carrying before they were named; the tradecraft of the groups responsible, mapped against the controls that address it; the malware infrastructure in active use; and the vulnerabilities newly confirmed as exploited.

129	28	51%	78%
ORGANISATIONS NAMED AS VICTIMS BY RANSOMWARE AND EXTORTION GROUPS	SEPARATE RANSOMWARE AND EXTORTION GROUPS BEHIND THEM	OF THE ORGANISATIONS WE COULD CHECK WERE ALREADY CARRYING STOLEN CREDENTIALS	OF THOSE NAMED LEFT NO PUBLIC TRACE OF THE INCIDENT



Organisations named per day. Thursday carried 52 — more than double any other day in the period.

WHAT STOOD OUT

The most exposed on employee credentials — the only category that is an entry route — were universities and a school district.

COVERAGE

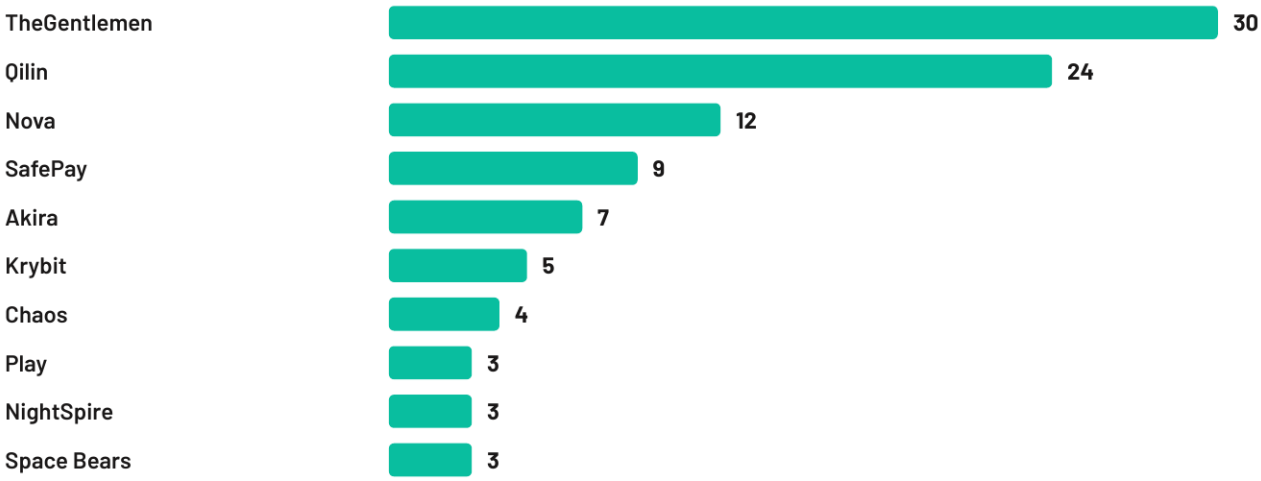
Week ending Friday 24 July 2026. 129 organisations named by 28 groups, of which 128 were assessed for public disclosure across 219 searches. 115 domains assessed for credential exposure. 229 attacker techniques mapped across the 9 groups with assessed tradecraft. 1,964 indicators of compromise identified. 6 vulnerabilities newly confirmed as exploited.

HOW WE WORK

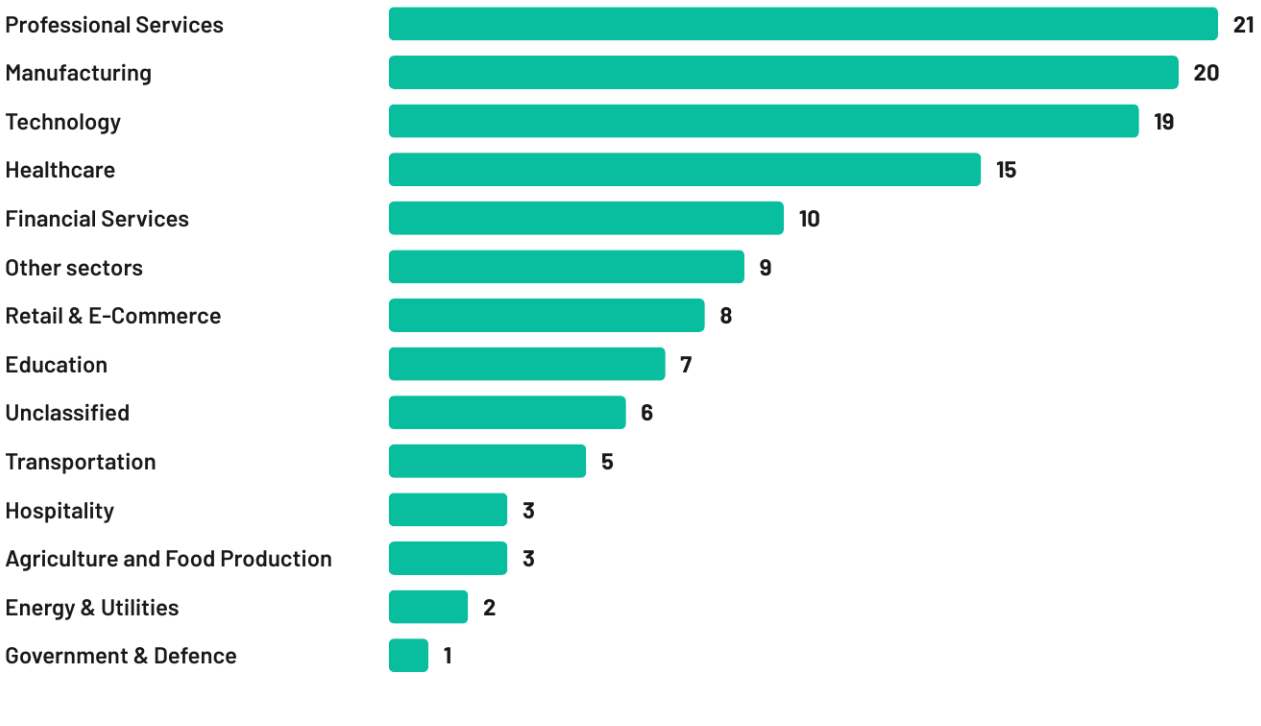
Every figure is derived from sources observable without a supplier's cooperation. Listings are reported as listings, not confirmed breaches. Where we interpret rather than measure, we say so. No client data appears in this report.

02 Who was named

129 organisations · 39 countries · 25+ a day



The 10 groups naming the most organisations. TheGentlemen and Qilin account for 42% of the period between them. A further 18 groups named the remaining 29, one or two each.



Every sector represented, summing to the 129 organisations named this period. They sit in 39 countries, with 41 organisations in the United States.

42%

2 groups accounted for 42% of the period between them.

60 of 129

Professional services, manufacturing and technology together account for 60 of 129 — the sectors most likely to sit inside another organisation's supply chain.

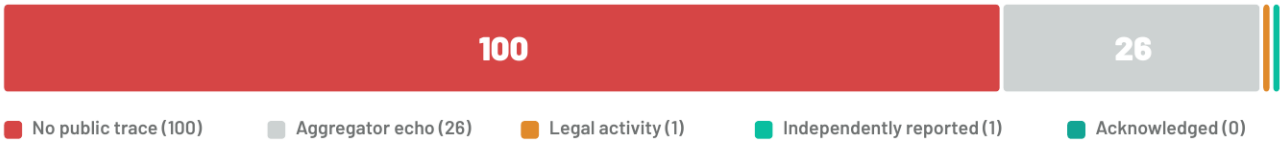
03 Can anyone find out?

All 129 named · 128 assessed

If one of these is your supplier, no amount of watching the news will tell you.

For every organisation named this period, whether anyone outside it — a customer, a regulator, you — could find out the incident happened at all.

HOW EACH ORGANISATION'S INCIDENT SURFACED



26 more appear only as the leak-site listing reprinted automatically — the listing repeating, not anyone confirming it.

WHAT EACH STATE MEANS

Acknowledged — The organisation has issued a public statement.

Independently reported — A journalist investigated and published.

Legal activity — Law firms advertising for claimants. Not confirmation, but a signal that someone believes the listing.

Aggregator echo — Automated republication of the leak-site listing. This is the listing repeating, not corroborating it.

No public trace — Nothing found.

WHERE IT DID SURFACE

ORGANISATION	HOW IT SURFACED	WHERE	DETAIL
HBS Group	Independently reported	Cyber Daily	Australian heritage restoration and construction firm, Alphington, Victoria. Listed 23 July. No statement from the company.
Kean University	Legal activity		Class-action solicitation within a day of the listing. No statement from the university.

WHAT STOOD OUT

Of 128 organisations assessed, one attracted independent reporting and one attracted class-action advertising. None issued a statement.

100 have no public trace of the incident at all — 78%.

Most of what looks like coverage is the leak-site listing being reprinted automatically, which corroborates nothing.

04 · THIS PERIOD'S FINDING

Half the organisations named by ransomware groups already had stolen credentials

129	115	59	51%	18	1,041
ORGANISATIONS NAMED	DOMAINS WE COULD CHECK	ALREADY CARRYING STOLEN CREDENTIALS	OF THOSE WE COULD CHECK	CARRYING CREDENTIALS TO THEIR OWN SYSTEMS	EMPLOYEE CREDENTIALS IN TOTAL

59 of the 115 organisations we could check were already carrying stolen credentials at the point a ransomware group named them.

18 of those held credentials for their own systems — the category that is directly an entry route, rather than reuse on somebody else's platform.

The sharpest instance is education: 4 universities and school districts carry 415 of the 1,041 exposed employee credentials — 40% — and 3 of the 6 most exposed organisations this period are education institutions.

WHAT IT MEANS

Exposure came first. We cannot say it caused any of these incidents, and we do not claim it did. What matters is the sequence: it was visible from outside, before the listing appeared, without the organisation's cooperation and without anyone reporting it. That makes it the one thing you can check about a supplier yourself. Universities and colleges supply research, training and placements across every sector, and vendor registers are built from procurement records — so they rarely sit in one.

05 Exposed before they were named

59 of 115 organisations we could check

Each figure counts a stolen credential pair recovered from infostealer dumps: an account name and the site it was used to log into.

51%	1,041	11,322	534,215
CARRYING EXPOSED CREDENTIALS	EMPLOYEE CREDENTIALS	THIRD-PARTY CREDENTIALS	CUSTOMER CREDENTIALS

WHAT EACH FIGURE COUNTS

Employee — The account belongs to the organisation and was used to log into the organisation's own systems. The most direct route in, and the number that matters most.

Customer — An outside account used to log into the organisation's systems. Exposure the organisation carries on behalf of other people, not a route into it.

Third party — An organisation account used to log into an external service. Measures credential reuse and unmanaged SaaS across the workforce. It does NOT count supplier relationships.

READING THE CUSTOMER FIGURE

Customer totals are heavily concentrated. One organisation accounts for most of the period's figure, so the total is reported for completeness rather than as a measure of spread.

THE 14 CARRYING THE MOST, OF THE 59 WITH ANY EXPOSURE

ORGANISATION	GROUP	SECTOR	EMPLOYEE	THIRD PARTY	CUSTOMER
EFU Life Assurance	Qilin	Financial Services	239	304	3,710
Highline Community College	Qilin	Education	174	1,564	1,901
Colliers Real Estate	CoinbaseCartel	Professional Services	163	1,932	313
Universidad Nacional de Mar del Plata	Nova	Education	136	1,234	28,330
Sunway Berhad	Qilin	Hospitality	122	699	2,441
Kean University	Qilin	Education	91	3,544	2,936
Raben Group	TheGentlemen	Transportation	30	188	561
BH Security (brinkshome.com)	ShinyHunters	Professional Services	19	256	1,098
upland.k12.ca.us	SafePay	Education	14	328	81
Tikona Infinet	TheGentlemen	Technology	13	170	87,904
metrabyte.cloud	APT73	Technology	7	5	1,915
Ejército Argentino	Qilin	Government & Defence	0	47	393,103
Record Go Alquiler	Play	Hospitality	0	47	5,735
Restaurant Depot	Play	Retail	0	0	3,166

WHAT STOOD OUT

Of the 115 organisations whose domains we could check, 59 were already carrying stolen credentials.

Employee credential reuse on external services is an order of magnitude larger than exposure on their own systems, at 11,322 against 1,041.

06 The route in

9 of 28 groups assessed · 64% of organisations named

You cannot audit a supplier's estate. You can ask questions only a supplier with working controls can answer well. These are the techniques the groups naming victims this period actually use — and the next section turns them into the questions.

The entry techniques, and how many of the 9 assessed groups use each. Red because these are the ones short enough to close. Techniques are MITRE ATT&CK identifiers. Technique names are reproduced as ATT&CK publishes them.

WHAT STOOD OUT

9 of the 28 groups naming victims this period have tradecraft assessed in enough depth to map. Those 9 named 83 of the 129 organisations — 64%.

Entry is the narrow part. Valid accounts and internet-facing applications are each used by 7 of the 9, and phishing and external remote services by 4 — a short, shared list.

Nothing new entered the shared route this period. The same 2 entry techniques and the same lateral movement as the groups' established tradecraft.

What happens after entry is far more varied, and every group is different. You cannot cover all of it. The entry list is short enough to close.

One group named this period takes data without encrypting anything. Immutable backups and continuity testing do not answer that.

07 What to ask a supplier

Five questions, one per control layer

Prevent, Protect, Detect, Respond and Recover are the five things a control estate has to do. Below each is what the assessed groups actually did this period, and the question that separates a supplier who has covered it from one who says they have.

PREVENT

Valid Accounts 7/9 · Exploit Public-Facing Application 7/9 · External Remote Services 4/9 · Phishing 4/9

51% of the organisations we could check — 59 of 115 — were already carrying stolen credentials when a ransomware group named them.

> ASK A SUPPLIER
> **Is MFA enforced on every remote path, including contractors and service accounts, and what is your help desk's verification procedure for an MFA re-enrolment?**

PROTECT

Impair Defenses: Disable or Modify Tools 7/9 · Obfuscated Files or Information 5/9 · Command and Scripting Interpreter: PowerShell 5/9 · Masquerading: Match Legitimate Name or Location 4/9

7 of 9 disable security tooling, and 5 of 9 obfuscate what they run.

> ASK A SUPPLIER
> **Is tamper protection enforced, and does anyone get alerted when an agent stops reporting?**

DETECT

Network Service Discovery 6/9 · System Information Discovery 5/9 · File and Directory Discovery 5/9 · OS Credential Dumping: LSASS Memory 4/9

Internal scanning appears across two thirds of the groups. *Internal scanning is rarely legitimate and is the cheapest activity to alert on.*

> ASK A SUPPLIER
> **Do you alert on internal network scanning, and who sees it?**

RESPOND

Remote Services: Remote Desktop Protocol 7/9 · Remote Services: SMB/Windows Admin Shares 5/9 · Archive Collected Data: Archive via Utility 5/9 · Lateral Tool Transfer 4/9

7 of 9 move by RDP, 5 also by SMB admin shares.

> ASK A SUPPLIER
> **Can anything in your environment reach ours over RDP, SMB or a site-to-site link?**

RECOVER

Data Encrypted for Impact 9/9 · Inhibit System Recovery 5/9 · Exfiltration Over Web Service: to Cloud Storage 5/9 · Financial Theft 4/9

All 9 encrypt. 5 destroy the recovery path first. *Some also wipe disk content, which is destruction rather than leverage.*

> ASK A SUPPLIER
> **Are backups immutable, offline and restore-tested, and when did you last prove it?**

> ABOUT THIS FRAMING
>
> Prevent, Protect, Detect, Respond and Recover are our own grouping of what a control estate has to do. They are not the NIST CSF functions, which begin with Identify rather than Prevent. Techniques are MITRE ATT&CK identifiers. Technique names are reproduced as ATT&CK publishes them.

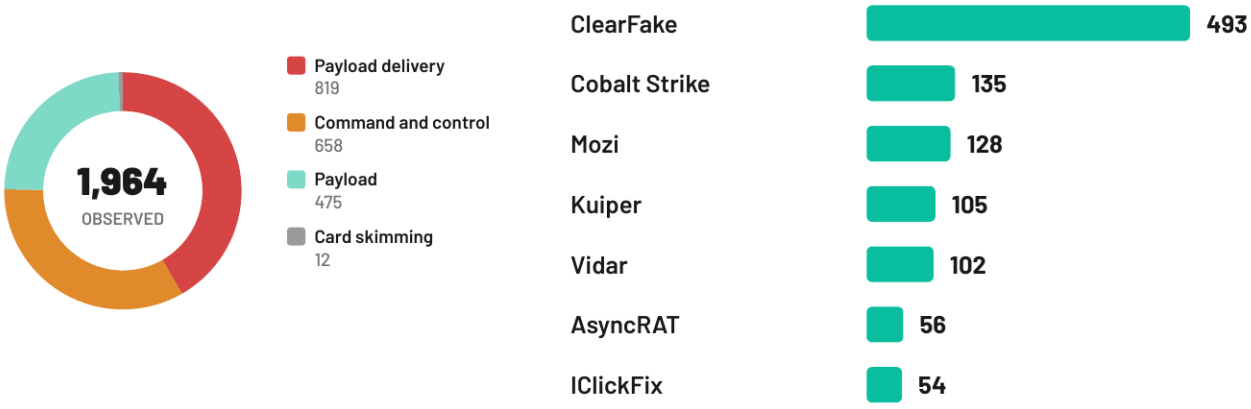
A further five questions, for your own team rather than a supplier, are on page 13.

08 What to look for

1,964 indicators observed this period

A domain, address or file signature seen in use by attacker infrastructure during the period.

1,964	1,177	819	658
INDICATORS OBSERVED THIS PERIOD	HIGH-CONFIDENCE NETWORK INDICATORS	PAYLOAD DELIVERY INFRASTRUCTURE	COMMAND-AND-CONTROL INFRASTRUCTURE



Indicators by role in the intrusion, and the families they belong to.

WHAT EACH ROLE MEANS

Payload delivery — Infrastructure used to place malware on a machine, typically the first step toward stealing a credential.

Command and control — Infrastructure an attacker uses to control a machine once inside it.

WHAT STOOD OUT

819 of the 1,964 indicators observed were delivery infrastructure — how an infostealer gets onto a device in the first place.

ClearFake accounts for a quarter of everything observed, at 493 of 1,964.

An infostealer that lands writes a stealer log — the account names and sites typed on that device. Those logs are where the exposed credentials counted earlier in this issue come from. Delivery infrastructure this week is credential exposure in a fortnight.

That is the same route the assessed groups rely on to get in, seen from the other end.

What to look for

A sample of this period's indicators

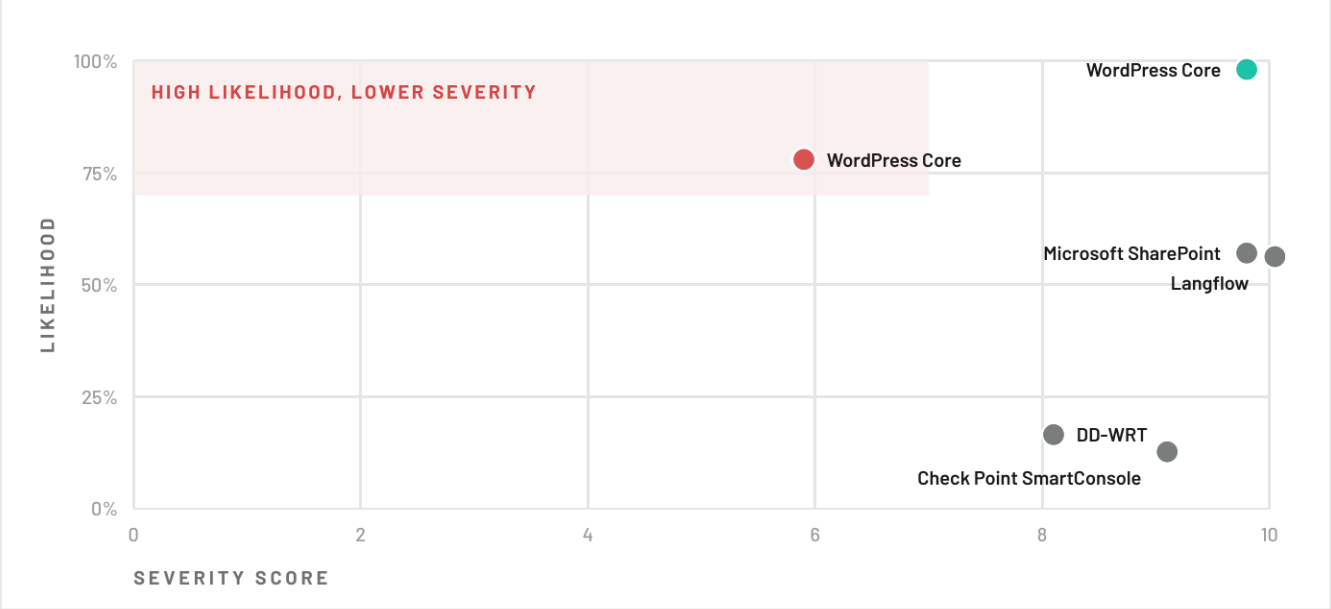
40 of the 1,964 indicators observed this period — the highest-confidence entries at each stage of an intrusion, with no single malware family allowed to dominate. A sample, not the full set. Search them against your own logs.

INDICATOR	TYPE	FAMILY	ROLE
DELIVERY — HOW THE VICTIM IS REACHED			**13**
grace-tung.com	Domain	ClearFake	Fake-update lure delivering a stealer
exywujgzhhueysauy.gentletouchchiropracticclinicauroracol.com	Domain	ClearFake	Fake-update lure delivering a stealer
gentletouchchiropracticclinicauroracol.com	Domain	ClearFake	Fake-update lure delivering a stealer
xdkrrektzqqrsjsae.fidipodiatry.com	Domain	ClearFake	Fake-update lure delivering a stealer
https://bouoher.lol/api/v1/status	URL	KongTuke	Compromised-site lure
https://tommy-ee.top/f	URL	KongTuke	Compromised-site lure
tommy-ee.top	Domain	KongTuke	Compromised-site lure
http://59.180.156.235:42443/Mozi.m	URL	Mozi	IoT botnet control
http://182.123.165.64:33331/Mozi.m	URL	Mozi	IoT botnet control
https://sagearcade.top/alias/signup-stylesheet	URL	SmartApeSG	Fake-update lure delivering a stealer
sagearcade.top	Domain	SmartApeSG	Fake-update lure delivering a stealer
https://sagearcade.top/alias/proxy-worker.js	URL	SmartApeSG	Fake-update lure delivering a stealer
popelkar.pro	Domain	Unattributed	Delivery infrastructure
CREDENTIAL THEFT — STEALERS AND LOADERS			**13**
168.144.135.136:8080	IP:port	Aisuru	Attacker infrastructure
168.144.135.136:9035	IP:port	Aisuru	Attacker infrastructure
195.20.115.53:2004	IP:port	DCRat	Remote access trojan control server
47.129.159.160:8888	IP:port	DCRat	Remote access trojan control server
12.187.175.73:7878	IP:port	DCRat	Remote access trojan control server
js-sec.seketafrica.org	Domain	FakeUpdates	Attacker infrastructure
111.170.148.134:80	IP:port	Unattributed	Delivery infrastructure
175.43.223.202:7443	IP:port	Unattributed	Delivery infrastructure
111.170.148.134:443	IP:port	Unattributed	Delivery infrastructure
82.156.166.227:22	IP:port	Unattributed	Delivery infrastructure
http://103.80.135.19:8880/getinstall64	URL	ValleyRAT	Loader delivering remote access
27.124.10.162:4452	IP:port	ValleyRAT	Loader delivering remote access
https://sup.merahsm188.top/	URL	Vidar	Information stealer control server
POST-COMPROMISE — CONTROL ONCE INSIDE			**14**
87.251.64.204:63812	IP:port	AdaptixC2	Post-compromise framework
111.230.238.243:443	IP:port	Cobalt Strike	Post-compromise framework
111.230.238.243:80	IP:port	Cobalt Strike	Post-compromise framework
111.228.62.67:8000	IP:port	Cobalt Strike	Post-compromise framework
43.144.19.224:53	IP:port	Cobalt Strike	Post-compromise framework
119.29.21.84:80	IP:port	Cobalt Strike	Post-compromise framework
47.96.154.174:443	IP:port	Havoc	Post-compromise framework operating on HTTPS
103.101.85.111:4747	IP:port	Quasar RAT	Remote administration tool used after access
162.19.139.33:5553	IP:port	Quasar RAT	Remote administration tool used after access
101.96.224.108:50005	IP:port	VShell	Post-compromise control server
103.149.93.150:8084	IP:port	VShell	Post-compromise control server
115.159.210.123:8088	IP:port	VShell	Post-compromise control server
146.56.205.231:8084	IP:port	VShell	Post-compromise control server
206.238.123.117:8080	IP:port	VShell	Post-compromise control server

09 What crossed the line

6 confirmed exploited · 5 with three-day windows

Vulnerabilities confirmed as being exploited in real attacks during the period. This is a deliberately high bar: not everything published, and not everything rated critical, but the small number each week that crosses from theoretical to actively used.



Severity says how damaging a flaw is. Likelihood says how probable exploitation is. They disagree.

REFERENCE	PRODUCT	SEVERITY	LIKELIHOOD	FIX IN
CVE-2026-63030	**WordPress** Core website platform	9.8	98.1%	3d
CVE-2026-60137	**WordPress** Core website platform	5.9	78.0%	14d
CVE-2026-50522	**Microsoft** SharePoint document collaboration platform	9.8	57.1%	3d
CVE-2026-0770	Langflow AI application builder	9.8	56.3%	3d
CVE-2021-27137	DD-WRT router firmware	8.1	16.5%	3d
CVE-2026-16232	**Check Point** SmartConsole firewall management console	9.1	12.7%	3d

WHAT EACH COLUMN MEANS

Fix in — The window recommended for fixing each one, counted from the date exploitation was confirmed. A short window signals how quickly the exploitation was judged to be spreading. 3 days is at the sharp end.

Severity — How damaging the flaw is if exploited, on the standard 0–10 scale.

Likelihood — The probability the flaw will be exploited in the next 30 days. Severity says how bad it would be; likelihood says how likely it is.

WHAT STOOD OUT

6 vulnerabilities crossed from theoretical to confirmed exploitation this week.

5 of the 6 carried three-day remediation recommendations.

1 is rated medium on severity — 5.9 — but carries a 78% chance of exploitation, higher than four of the five rated critical.

1 had been public since 2021 before being confirmed as exploited this week. It is router firmware, the kind of equipment that sits in a small supplier's office and is rarely touched after installation.

10 Questions to take to your team

5 questions for your own team, grounded in this period's data

Page 9 gave you five questions for your suppliers. These five are for your own team, and each is answerable from this issue.

1 Does our supplier register include the organisations that got hit?

Universities and school districts carried 40% of the exposed employee credentials this period. Does our supplier programme include research partners, training providers and public bodies, or only commercial suppliers?

2 Is MFA enforced on every path a supplier uses to reach us?

Valid accounts and internet-facing applications were each used by 7 of the 9 groups we assessed. Is MFA enforced on every remote path a supplier uses to reach us, and how would we know if it lapsed?

3 What is our credential exposure, and our top ten suppliers'?

59 of the 115 organisations we could check were already carrying stolen credentials when a ransomware group named them. What is our number, and our top 10 suppliers' numbers?

4 Who is asking which suppliers run these products?

5 of the 6 vulnerabilities confirmed as exploited this period carried three-day remediation recommendations, including a firewall management console and a document platform. Who owns asking which suppliers run them?

5 What evidence do we hold beyond a supplier's own attestation?

19 of the 28 groups naming victims this period have no publicly documented methods. What evidence do we hold that a supplier's controls work, beyond their own attestation?