CYBER OPERATIONS

WEEKLY INTELLIGENCE

SUPPLY-CHAIN INTELLIGENCE

Issue #002: Beyond The Headlines

Of the 196 organisations we could assess, 4 produced any public account of it.

27 July – 2 August 2026

Contents

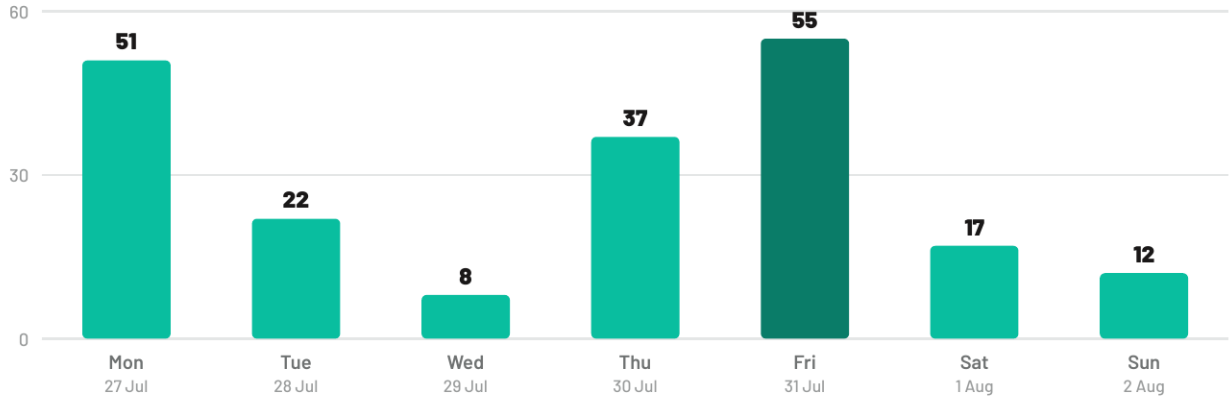
01 Executive summary

27 July – 2 August 2026

This is an outside-in assessment of the threat to enterprise supply chains. Each issue is built from six layers: the organisations publicly listed 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 listed; 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.

202	34	98%	28%
ORGANISATIONS LISTED AS VICTIMS BY RANSOMWARE AND EXTORTION GROUPS	SEPARATE RANSOMWARE AND EXTORTION GROUPS BEHIND THEM	OF THE 196 WE COULD ASSESS PRODUCED NO STATEMENT, NO JOURNALISM AND NO LEGAL ACTIVITY	OF THE ORGANISATIONS WE COULD CHECK WERE ALREADY CARRYING STOLEN CREDENTIALS

ORGANISATIONS LISTED PER DAY



Organisations listed per day. Friday carried 55 and Wednesday 8, a 7-fold spread across the period.

WHAT STOOD OUT

Activity did not stop at the weekend: 29 organisations were listed on Saturday and Sunday.

This is the first seven-day issue. A Monday-to-Friday window would have missed all 29.

WHAT THIS ISSUE COVERS

202 organisations listed by 34 ransomware and extortion groups · 196 assessed for public disclosure · 188 domains checked for credential exposure · 8 groups with assessed tradecraft · 7,804 indicators of compromise · 3 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.

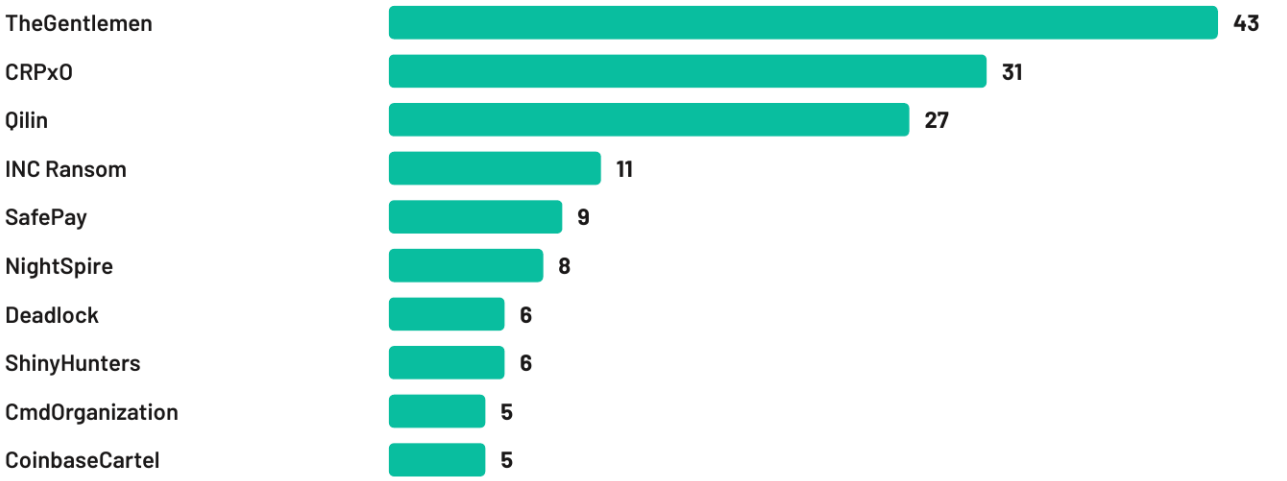
READING THIS AGAINST OTHER ISSUES

Only rate fields may be compared across issues of differing window length. Issue 001 covered five days; this covers seven, so raw counts will misread as trend.

02 Who was listed

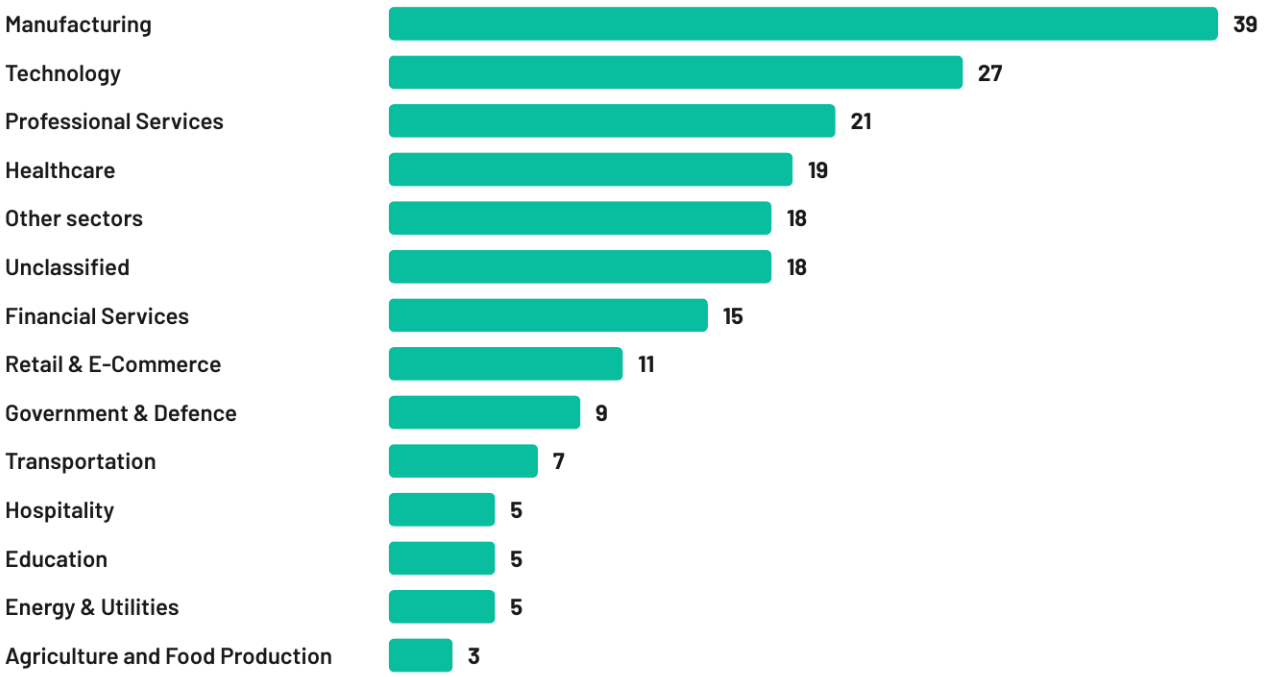
202 organisations · 45 countries · 28.9 a day

ORGANISATIONS LISTED PER GROUP



The 10 groups listing the most organisations. TheGentlemen and CRPxO account for 37% of the period between them. A further 24 groups listed the remaining 51 between them.

SECTOR OF EVERY ORGANISATION LISTED



Every sector represented, summing to the 202 organisations listed this period. They sit in 45 countries, with 88 organisations in the United States.

37%

TheGentlemen and CRPxO accounted for 37% of the period between them.

87 of 202

Manufacturing, technology and professional services together account for 87 of 202 — the sectors most likely to sit inside another organisation's supply chain.

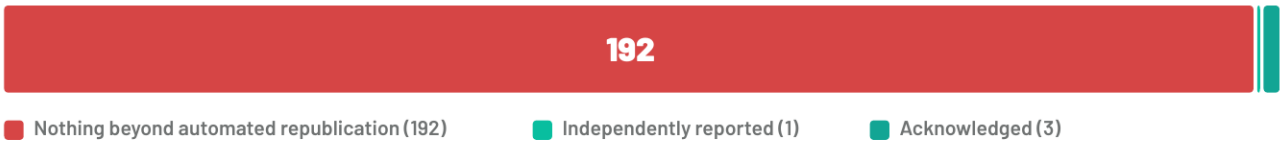
03 Can anyone find out?

All 202 listed · 196 assessed

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

For every organisation listed this period, whether anyone outside it — a customer, a regulator, you — could find out the incident happened at all. Each organisation is counted once, in the highest state it reached.

HOW EACH ORGANISATION'S INCIDENT SURFACED



192 of 196 produced nothing but the 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.

Automated republication — A tracker or feed reproducing the leak-site listing. This is the listing repeating, not anyone confirming it.

Excluded — Organisations whose name is too generic or too short to attribute search results reliably. 6 were set aside this period and are excluded from the denominator.

HOW THIS WAS MEASURED

Listings are assertions made by the groups themselves and are not independently verified. Where we interpret rather than measure, it is marked as interpretation. English-language search only; a third of organisations sit outside the main English-speaking markets. Search engines were changed mid-sweep when a quota was exhausted, and different engines returned different amounts of tracker material. The count of organisations with a public statement, journalism or legal activity is unaffected; any finer split within the remainder is not reliable.

WHERE IT DID SURFACE

ORGANISATION	HOW IT SURFACED	WHERE	DETAIL
Ernst & Young	Acknowledged	EY (statement); BleepingComputer, SecurityWeek, Hackread, SecurityAffairs, Cybernews	EY publicly confirmed unauthorised access to a third-party IT service management platform between 28 March and 12 April 2026 affecting client tax documents, and the ShinyHunters extortion listing was reported independently by BleepingComputer, SecurityWeek and others from 27 July 2026.
Brinks Home	Acknowledged	Brinks Home (statement); BleepingComputer, SC Media	Brinks Home confirmed a breach it identified on 20 July 2026 involving Salesforce and support systems after ShinyHunters listed 'BH Security, LLC (brinkshome.com)', with independent coverage by BleepingComputer and SC Media.
Craneware	Acknowledged	Craneware plc RNS (20 Jul 2026); also TechCrunch, Infosecurity Magazine, IT Pro; class-action solicitation by ClassActionU and ClaimDepot	Craneware plc issued a formal Notice of Cyber Security Incident on 20 Jul 2026 confirming unauthorised access and data copying, notified the ICO and FBI, and the incident drew substantial independent reporting and US class-action advertising ahead of the Chaos leak-site listing on 28 Jul.
Mairie de Drancy	Independently reported	Le Parisien / Ouest-France / Actu.fr / Le Journal Toulousain	Multiple French national and regional titles reported the cyberattack on the town hall, its disrupted municipal services and probable resident-data leak, and the mairie publicly urged residents to change passwords.

WHAT STOOD OUT

Of 196 organisations assessed, 4 produced a public statement, a piece of journalism or any legal activity.

The other 192 produced none of those three — 98% with nothing a customer could act on.

The four exceptions are a Big Four firm, a listed software company, a US consumer brand and a French town hall. Coverage tracks how large an organisation is, not how serious the incident was.

Trackers auto-generate a page for most listings, but a search for the supplier's name does not return it. Where that holds, the page exists without being findable — which is the same as not existing, to a customer.

04 Exposed before they were listed

52 of 188 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.

28%	10,320	33,720	335,160
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 THESE FIGURES

Employee — Employee totals are heavily concentrated. Pertamina accounts for 63% of the period's figure on its own, so the total is reported for completeness rather than as a measure of spread.

Customer — The customer figure is more concentrated still: Pertamina and RingCentral account for 55% of it between them. It is also the weakest of the three — it counts other people's accounts and is not a route into the organisation.

THE 14 WITH THE MOST EXPOSED EMPLOYEE CREDENTIALS, OF THE 52 WITH ANY EXPOSURE

ORGANISATION	GROUP	SECTOR	EMPLOYEE	THIRD PARTY	CUSTOMER
Pertamina	TheGentlemen	Energy & Utilities	6,500	4,540	100,400
Ernst & Young	ShinyHunters	Professional Services	2,180	6,140	22,860
Johnson & Johnson	CRPxO	Healthcare	1,060	16,900	33,480
RingCentral	ShinyHunters	Technology	320	1,860	84,600
Lumenis	ShinyHunters	Technology	120	360	80
Brinks Home	ShinyHunters	Professional Services	40	280	800
Malaysian Nuclear Agency	TheGentlemen	Government & Defence	40	160	460
Boyum IT Solutions	Genesis	Technology	20	0	80
Hyundai	CRPxO	Manufacturing	20	220	35,220
Kuveyt Türk	CRPxO	Financial Services	20	440	10,840
Tesco Engineer	Deadlock	Retail & E-Commerce	0	0	20
Hardware Asesorías Software	Deadlock	Technology	0	180	40
Marketech	CRPxO	Technology	0	0	120
Katathani Phuket Beach Resort	DragonForce	Hospitality	0	0	20

WHAT STOOD OUT

Of the 188 organisations whose domains we could check, 52 were already carrying stolen credentials.

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

Employee credential reuse on external services is more than three times larger than exposure on their own systems, at 33,720 against 10,320.

05 · THIS PERIOD'S FINDING

ShinyHunters listed 6 organisations. 4 already had stolen credentials.

6	4	67%	188	5%
LISTED BY THE GROUP	ALREADY CARRYING STOLEN CREDENTIALS	OF THEM ALREADY EXPOSED	ORGANISATIONS WE COULD CHECK	THE BASE RATE ACROSS ALL OF THEM

ShinyHunters listed 6 organisations this period. 4 of them were already carrying exposed employee credentials.

Across all 188 organisations we could check, 10 were carrying employee credentials — 5%. The next-highest rates were CRPx0 at 3 of 31 and TheGentlemen at 2 of 43; Qilin's 27 included none.

The four were Ernst & Young, RingCentral, Lumenis and Brinks Home — professional services and technology firms, which is to say suppliers to everybody else.

WHAT IT MEANS

Read that comparison carefully. All six are large multinationals, while the 5% base rate comes from 188 organisations that are mostly small. A bigger workforce produces more infostealer records whatever an attacker is doing, so size alone could account for the gap. What we can say is narrower, and still useful: this group's recorded method is credential-led throughout — voice phishing, stolen private keys, stolen application access tokens — and the organisations it listed were among the most credential-exposed we found. On six organisations that is worth watching, not banking. Whatever selects them, exposure is visible from outside before the listing appears — and it is the one thing you can check about a supplier without asking them.

06 The route in

8 of 34 groups assessed · 56% of organisations listed

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 listing victims this period actually use — and the next section turns them into the questions.

HOW AN ATTACKER GETS IN

The entry techniques, and how many of the 8 assessed groups use each. Red because these are the ones short enough to close.

WHAT STOOD OUT

8 of the 34 groups listing victims this period have tradecraft assessed in enough depth to map. Those 8 listed 113 of the 202 organisations — 56%.

218 distinct techniques across those groups. Entry is the narrow part: exploiting an internet-facing application and valid accounts are each used by 5 of the 8.

Nothing new entered the shared route this period. The same entry techniques and the same lateral movement as these 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.

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

Exploit Public-Facing Application 5/8 · Valid Accounts 5/8 · Phishing 4/8 · Phishing: Spearphishing Voice (Vishing) 4/8

52 of the 188 organisations we could check were already carrying stolen credentials when they were listed.

> 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 5/8 · Boot or Logon Autostart Execution 4/8 · Obfuscated Files or Information 4/8 · Exploitation for Privilege Escalation 3/8

5 of 8 assessed groups disable security tooling, and 4 of 8 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 5/8 · File and Directory Discovery 4/8 · Account Discovery: Domain Account 3/8 · OS Credential Dumping 3/8

5 of 8 scan the network from inside once they are in. *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 5/8 · Remote Services: SMB/Windows Admin Shares 4/8 · Windows Management Instrumentation 4/8 · Exfiltration Over Web Service: Exfiltration to Cloud Storage 4/8

5 of 8 move by RDP, 4 of 8 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 8/8 · Inhibit System Recovery 3/8 · Service Stop 2/8 · Disk Wipe: Disk Content Wipe 2/8

Encryption for impact is recorded against all 8 assessed groups. A technique carried by every group tells you nothing about any of them — read it as the catalogue default it is, and look at the layers above. *One group listed this period takes data and never encrypts. Immutable backups and continuity testing answer none of that.*

> 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 is our own grouping of what a control estate has to do. It is deliberately not the NIST CSF functions — those begin with Identify, which is asset and risk discovery and is not what this section measures. Techniques are MITRE ATT&CK identifiers, reproduced as ATT&CK publishes them.

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

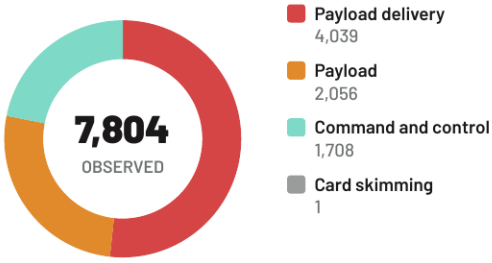
08 What to look for

7,804 indicators observed this period

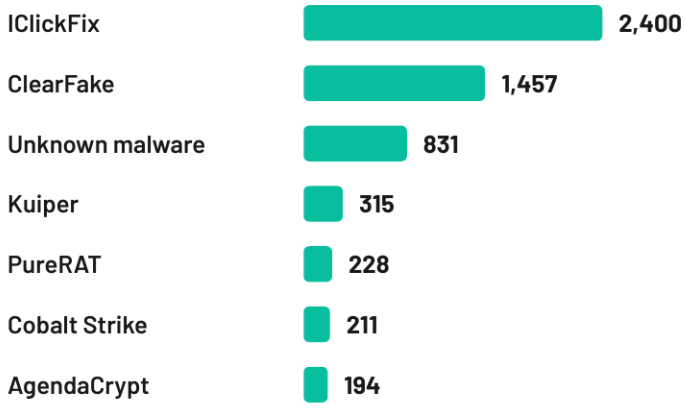
A domain, address or file signature seen in use by attacker infrastructure during the period.

7,804	4,397	4,039	1,708
INDICATORS OBSERVED THIS PERIOD	HIGH-CONFIDENCE NETWORK INDICATORS	PAYLOAD DELIVERY INFRASTRUCTURE	COMMAND-AND-CONTROL INFRASTRUCTURE

INDICATORS BY ROLE



TOP 7 MALWARE FAMILIES



Indicators by role in the intrusion, and the 7 largest families. A further 2,168 indicators belong to families outside the seven.

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

4,039 of the 7,804 indicators observed were delivery infrastructure — how an infostealer gets onto a device in the first place.

Two fake-update families, IClickFix and ClearFake, account for 3,857 of everything observed — nearly half.

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.

What to look for

A sample of this period's indicators

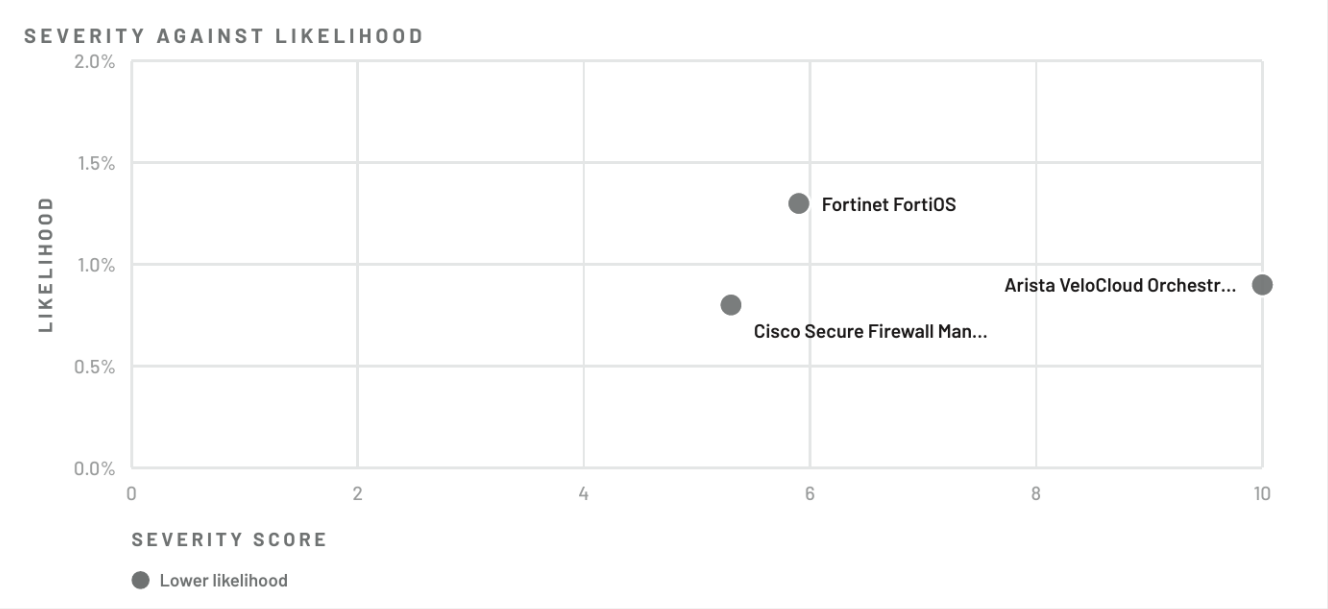
40 of the 7,804 indicators observed this period — the highest-confidence entries at each stage of an intrusion, with no single malware family allowed to dominate. A sample, not the full set. Search them against your own logs.

INDICATOR	TYPE	FAMILY	ROLE
DELIVERY — HOW THE VICTIM IS REACHED			**14**
patrins.com	Domain	5.t Downloader	Attacker infrastructure
feather-24.com	Domain	AMOS	Attacker infrastructure
https://feather-24.com/curl/50919cfb07265cc6116b5ced7fbdb9c8f5e214445eea436e93e2c88d70da7e43	URL	AMOS	Attacker infrastructure
https://feather-24.com/2kqYRM0DCrnyJgoS4gVLI_FHJRRdTUhGCbjyuYwpZ6c/code3/update	URL	AMOS	Attacker infrastructure
iyxadrf.jbgkito21.xyz	Domain	ClearFake	Fake-update lure delivering a stealer
huscms.kanganjeweller.com	Domain	ClearFake	Fake-update lure delivering a stealer
kanganjeweller.com	Domain	ClearFake	Fake-update lure delivering a stealer
602kigvy.hanovereyephotography.com	Domain	ClearFake	Fake-update lure delivering a stealer
uzyjmjoqveovvvbfxo.gamestwists.com	Domain	ClearFake	Fake-update lure delivering a stealer
mhkkzdp.jasperstays.com	Domain	ClearFake	Fake-update lure delivering a stealer
comunitel.de	Domain	IClickFix	Fake-update lure delivering a stealer
agrandelephant.com	Domain	IClickFix	Fake-update lure delivering a stealer
dann-sommer.dk	Domain	IClickFix	Fake-update lure delivering a stealer
darethebook.com	Domain	IClickFix	Fake-update lure delivering a stealer
CREDENTIAL THEFT — STEALERS AND LOADERS			**13**
haven-vibe.com	Domain	AMOS	Attacker infrastructure
https://haven-vibe.com/api/metrics/run?event=pasted	URL	AMOS	Attacker infrastructure
198.98.53.100:12345	IP:port	Aisuru	Attacker infrastructure
206.189.81.41:34567	IP:port	Aisuru	Attacker infrastructure
167.172.71.69:34567	IP:port	Aisuru	Attacker infrastructure
kieronellisonhikslumberparty.ru	Domain	Aisuru	Attacker infrastructure
143.198.206.191:8080	IP:port	Aisuru	Attacker infrastructure
137.184.199.120:9035	IP:port	Aisuru	Attacker infrastructure
d3qx7quq68rdce.cloudfront.net	Domain	AstarionRAT	Attacker infrastructure
185.157.46.242:8808	IP:port	AsyncRAT	Attacker infrastructure
157.20.182.22:6666	IP:port	AsyncRAT	Attacker infrastructure
86.106.119.24:8808	IP:port	AsyncRAT	Attacker infrastructure
157.20.182.22:1992	IP:port	AsyncRAT	Attacker infrastructure
POST-COMPROMISE — CONTROL ONCE INSIDE			**13**
65.49.220.29:443	IP:port	AdaptixC2	Attacker infrastructure
65.49.220.29:80	IP:port	AdaptixC2	Attacker infrastructure
65.49.220.29:8080	IP:port	AdaptixC2	Attacker infrastructure
95.216.94.101:8080	IP:port	AdaptixC2	Attacker infrastructure
95.216.94.101:443	IP:port	AdaptixC2	Attacker infrastructure
95.216.94.101:80	IP:port	AdaptixC2	Attacker infrastructure
156.224.18.21:22	IP:port	Cobalt Strike	Post-compromise framework
151.244.243.42:22	IP:port	Cobalt Strike	Post-compromise framework
151.244.243.42:8443	IP:port	Cobalt Strike	Post-compromise framework
151.244.243.42:443	IP:port	Cobalt Strike	Post-compromise framework
151.244.243.42:80	IP:port	Cobalt Strike	Post-compromise framework
14.103.214.233:80	IP:port	Cobalt Strike	Post-compromise framework
104.248.185.92:22	IP:port	Havoc	Attacker infrastructure

09 What crossed the line

3 confirmed exploited · 2 with three-day windows

Vulnerabilities confirmed as being exploited in real attacks during the period. A deliberately high bar: not everything published, and not everything rated critical, but the small number each period 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-2025-68686	**Fortinet** FortiOS	5.9	1.3%	14d
CVE-2026-16812	**Arista** VeloCloud Orchestrator	10.0	0.9%	3d
CVE-2026-20316	**Cisco** Secure Firewall Management Center (FMC)	5.3	0.8%	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

3 vulnerabilities crossed from theoretical to confirmed exploitation this period.

All 3 sit in network edge and management equipment — a firewall management console, a VPN operating system and an SD-WAN orchestrator.

2 of the 3 carried three-day remediation recommendations, and none exceeded a 1.3% chance of exploitation in the next 30 days.

This is the equipment a supplier runs at its perimeter. You cannot patch it, you will not be told when it is patched, and a low likelihood score is no comfort when the exploitation is already confirmed.

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 Do we know which of our suppliers were listed this period?

202 organisations were listed in seven days, including a Big Four firm, a global vehicle manufacturer and a Danish software vendor with 12,000 customers. Would we know if one of them were ours?

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

52 of the 188 organisations we could check were already carrying stolen credentials when they were listed. What is our number?

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

Exploiting an internet-facing application and using valid accounts were each used by 5 of the 8 groups we assessed. Is MFA enforced on every remote path, and how would we know if it lapsed?

4 Who owns asking which suppliers run this edge equipment?

All 3 vulnerabilities confirmed exploited this period were in firewall management, VPN and SD-WAN equipment. Who owns asking which suppliers run them, and on what patch cadence?

5 What would we learn if a supplier were listed tomorrow?

98% of the 196 organisations we could assess this period produced no statement, no journalism and no legal activity. If watching the news is our control, what exactly is it detecting?

WHERE THIS COMES FROM

Everything in this issue was produced from outside, without any organisation's cooperation — and none of it is specific to your suppliers. Averro is the Cyb3r Operations platform that runs the same checks against your own supplier estate, continuously: who has been listed, who is already carrying exposed credentials, and what changed this week.

To see your own estate against this period's data, talk to us at cyb3roperations.com.