CYBER OPERATIONS

WEEKLY INTELLIGENCE

SUPPLY-CHAIN INTELLIGENCE

Issue #003: Beyond The Headlines

Of the 181 organisations we could assess, 9 produced any public account of it.

3 – 9 August 2026

Contents

01 Executive summary

3 – 9 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.

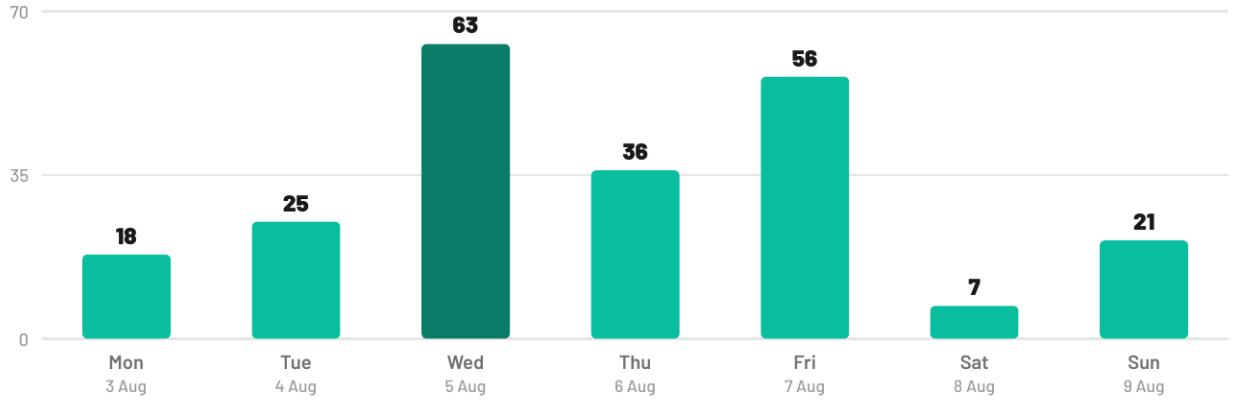
226
ORGANISATIONS LISTED AS VICTIMS BY RANSOMWARE AND EXTORTION GROUPS

38
SEPARATE RANSOMWARE AND EXTORTION GROUPS BEHIND THEM

95%
OF THE 181 WE COULD ASSESS PRODUCED NO STATEMENT, NO JOURNALISM AND NO LEGAL ACTIVITY

34%
OF THE 170 ORGANISATIONS WE COULD CHECK WERE ALREADY CARRYING STOLEN CREDENTIALS

ORGANISATIONS LISTED PER DAY



Organisations listed per day. Wednesday carried 63 and Saturday 7, a 9-fold spread across the period.

WHAT STOOD OUT

Activity did not stop at the weekend: 28 organisations were listed on Saturday and Sunday.

Wednesday 5 August carried 63 listings, more than any other day, and 40 of them came from one group in one drop.

WHAT THIS ISSUE COVERS

226 organisations listed by 38 ransomware and extortion groups · 181 assessed for public disclosure · 170 domains checked for credential exposure · 8 groups with assessed tradecraft · 3,546 indicators of compromise · 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.

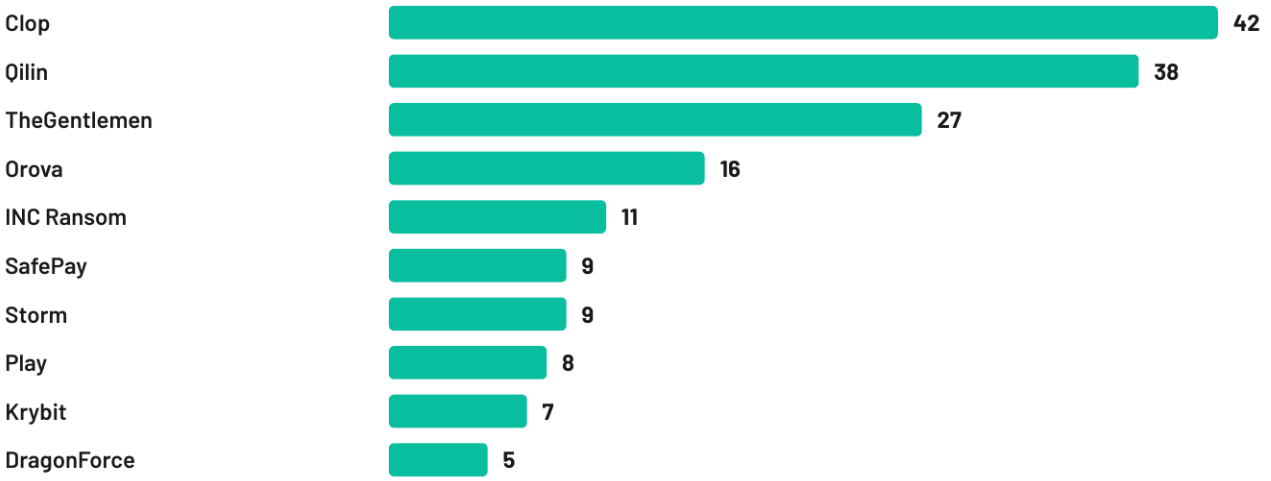
READING THIS AGAINST OTHER ISSUES

Only rate fields may be compared across issues. Issue 002 covered the same seven days, so counts are comparable with it but not with issue 001, which ran five. One rate moved materially: genuine visibility rose from 2.0% to 5.0%, on a corroboration sweep that used a single search engine throughout where issue 002's changed mid-sweep.

02 Who was listed

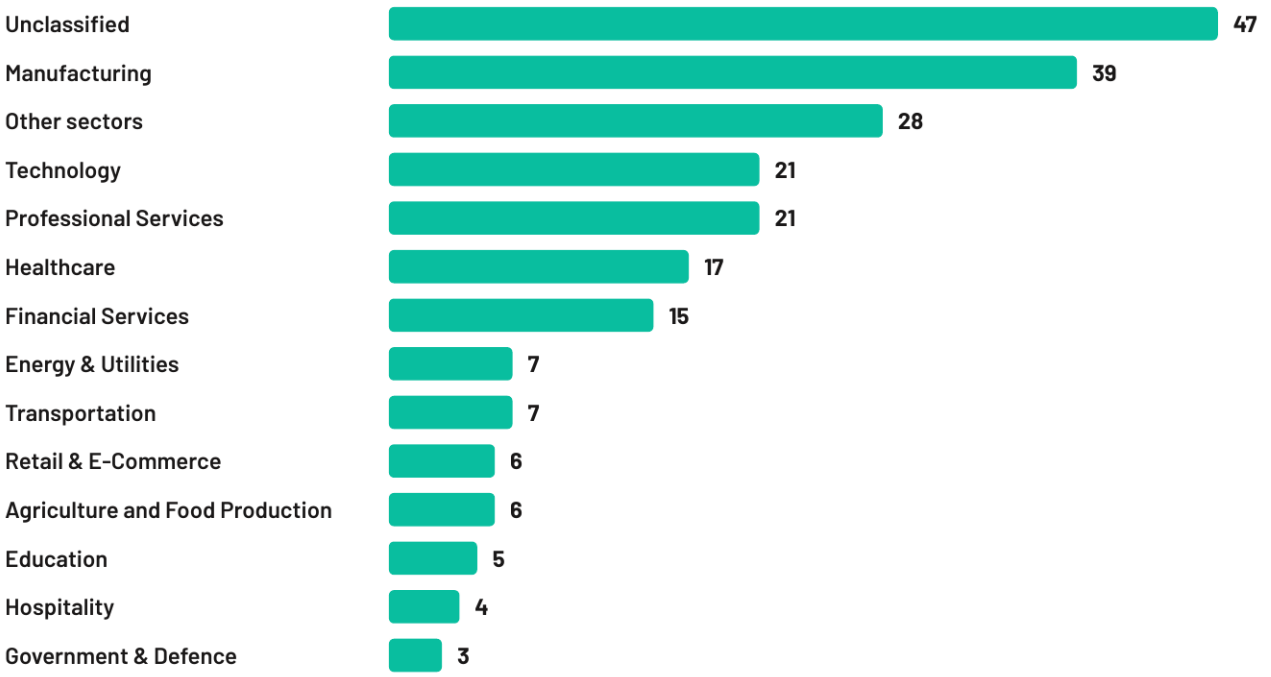
226 organisations · 39 countries · 32.3 a day

ORGANISATIONS LISTED PER GROUP



The 10 groups listing the most organisations. Clop and Qilin account for 35% of the period between them. A further 28 groups listed the remaining 54 between them.

SECTOR OF EVERY ORGANISATION LISTED



Every sector represented, summing to the 226 organisations listed this period. They sit in 39 countries, with 84 organisations in the United States.

226

226 organisations were listed by 38 separate groups in seven days — 32.3 a day.

47

Manufacturing was the largest identified sector at 39. But 47 organisations — more than any named sector — arrived with no sector recorded at all.

A supplier does not have to be large or well known to appear here. Most of these organisations are small, and most of them supply somebody bigger.

03 Can anyone find out?

All 226 listed · 181 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

172 of 181 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 or a regulatory filing.

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 — Nothing but the listing itself, whether reprinted by a tracker or nowhere to be found. The two are reported together because the split between them measures our search recall rather than the world.

Excluded — Organisations we could not search reliably, because the group published only part of the name. 45 were set aside and 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. 45 organisations could not be searched because the group published only part of the name; they are excluded from the denominator rather than counted as invisible. One search engine and one query form were used throughout, correcting the mid-sweep change that made issue 002's finer splits unreliable. Every acknowledgement was then verified individually.

WHERE IT DID SURFACE

ORGANISATION	HOW IT SURFACED	WHERE	DETAIL
Sawyer Savings Bank	Acknowledged	Sawyer Savings Bank (statement); Daily Freeman, Hudson Valley press; Claim Depot (class-action advertising)	Kept four Ulster County branches shut from Monday 3 August, brought in outside cybersecurity specialists, and stated the incident is believed to be linked to a vulnerability at one of its vendors. Customers lost counter service for the week.
Stade Français Paris	Acknowledged	Stade Français (statement); The Record, Eurosport, City AM	The Top 14 rugby club confirmed an attack on part of its information system, notified the authorities and filed a criminal complaint. Qilin listed it on 5 August with a countdown and published identity documents for 18 players as proof.
HIWIN	Acknowledged	Hiwin Technologies Corp (Taiwan Stock Exchange filing); MarketScreener	The Taiwanese motion-control manufacturer disclosed to the Taiwan Stock Exchange that its Italian subsidiary had detected a cyberattack. Shares fell 6%. TheGentlemen listed it 7 August.
Loyalist College	Acknowledged	Loyalist College (statement); Quinte News, InQuinte, Napanee Today	Confirmed that an unauthorised third party had accessed files containing personal information. The incident was discovered on 9 July; INC Ransom listed the college four weeks later.
Winn-Dixie	Legal activity	ClassAction.org; Migliaccio & Rathod LLP	Anubis listed the southeastern US grocery chain on 3 August. Within a day two US law firms were advertising for claimants. The first public account of the incident is an advertisement.

WHAT STOOD OUT

9 of the 181 organisations we could assess produced any public account of the incident — 5.0%. 4 issued a statement or a regulatory filing, 5 produced nothing but class-action advertising, and not one was brought to light by journalism alone.

Three of the four acknowledgements were forced: closed branches, a stock exchange filing, a countdown clock and 18 published passports. Disclosure followed visible disruption, not the breach. If watching the news is your control, it caught 5% of this period.

04 Exposed before they were listed

58 of 170 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.

34%	8,220	21,040	105,780
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 dominated by one organisation. Surakarta University accounts for 91% 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 concentrated too: Surakarta University and Price Shoes account for half 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 58 WITH ANY EXPOSURE

ORGANISATION	GROUP	SECTOR	EMPLOYEE	THIRD PARTY	CUSTOMER
Surakarta University	Panzer	Education	7,460	11,660	33,000
Universitatea de Vest Vasile Goldiș	Qilin	Education	260	260	1,540
Keysight	Everest	Technology	200	580	7,840
Pushidrosal	INC Ransom	Other sectors	100	0	440
Mindray	Clop	Healthcare	80	300	3,780
Université Libre de Bruxelles	Qilin	Education	40	4,120	8,720
Clinton Health Access Initiative	INC Ransom	Healthcare	40	280	20
Price Shoes	Qilin	Retail & E-Commerce	20	200	19,380
LCC Group	INC Ransom	Professional Services	20	0	80
Winn-Dixie	Anubis	Retail & E-Commerce	0	0	11,040
Brainhunter	Dark Project	Professional Services	0	0	9,360
Cesmac University Centre	Krybit	Education	0	760	5,220
DHC	TheGentlemen	Unclassified	0	40	2,420
Loyalist College	INC Ransom	Education	0	1,280	0

WHAT STOOD OUT

58 of the 170 organisations whose domain we could check were already carrying exposed credentials when they were listed — 34%.

9 were carrying credentials to their own systems, 8,220 employee records in total.

Education is 5 of the 226 organisations listed this period, and two of the three most exposed. Surakarta University alone accounts for 7,460 of the 8,220 employee credentials found.

One institution carrying 91% of the employee total is a distribution with a tail of one, not a sector finding. Universities run large, long-lived, loosely federated account estates, which produces more infostealer records for reasons that have nothing to do with who attacked them.

The useful part is the timing, not the ranking. Every one of these records was visible from outside before the organisation was listed. It is the one thing you can check about a supplier without asking the supplier.

05 · THIS PERIOD'S FINDING

Clop listed 40 organisations in one day and named none of them.

42	40	226	19%
LISTED BY THE GROUP	LISTED WITH THE NAME MASKED	ORGANISATIONS LISTED	OF ALL LISTINGS THIS PERIOD

Clop listed 42 organisations this period, 40 of them in a single drop on Wednesday 5 August. Every one of the 40 was published as a fragment — 'net*******', 'fis*******', 'jpm*******' — with no domain, no country and, for 33 of them, no sector.

Across the whole period 43 of the 226 listings carried a masked name, 19% of everything published. 40 of those 43 were Clop's.

Those are the organisations we could not search, could not check for exposed credentials and could not count: 45 dropped out of this issue's corroboration denominator and 40 out of its exposure sweep.

WHAT IT MEANS

This is not a gap in the data. It is the tactic. Clop has published partial names for years, and the practice is well documented: organisations that have not opened negotiations are listed as fragments, with the full name threatened within about 48 hours if they still do not. It is a negotiating clock. The clock runs against the organisation. It does not run for you. While it lasts, the only parties who know which supplier was breached are that supplier and the people who breached it — and an organisation that engages may never have to tell anyone at all. The practical consequence is that any supplier-monitoring control keyed on a company name is blind to a fifth of this period. Ours included; we have reported the gap rather than quietly shrinking the denominator around it.

06 The route in

8 of 38 groups assessed · 69% 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 38 groups listing organisations this period have tradecraft assessed in enough depth to map. Those 8 listed 156 of the 226 organisations — 69%.

219 distinct techniques across those groups. Entry is the narrow part: valid accounts are used by 7 of the 8 and exploiting an internet-facing application by 6.

Qilin's recorded tradecraft names the route directly: its affiliates phished managed service provider administrators through a remote support tool to reach the customers underneath. The supplier was the door, not the target.

What happens after entry is 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

Valid Accounts 7/8 · Exploit Public-Facing Application 6/8 · Phishing 3/8 · Develop Capabilities: Malware 3/8

58 of the 170 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, service accounts and any managed service provider that administers your estate?**

PROTECT

Impair Defenses: Disable or Modify Tools 6/8 · Indicator Removal: File Deletion 5/8 · Boot or Logon Autostart Execution 5/8 · Obfuscated Files or Information 4/8

6 of 8 assessed groups disable or modify 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 · System Information Discovery 4/8 · File and Directory Discovery 4/8 · Account Discovery: Domain Account 4/8

5 of 8 scan the network from inside once they are in, and 3 dump operating-system credentials. *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 5/8 · Remote Services 4/8 · Application Layer Protocol: Web Protocols 4/8

5 of 8 move by remote desktop, and 5 also by Windows 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 6/8 · Service Stop 3/8 · Disk Wipe: Disk Content Wipe 2/8

6 of 8 destroy the recovery points before they encrypt, and 3 stop the services holding the data open first.

> ASK A SUPPLIER
> **Where are your backups held, who can delete them, and when did you last restore from them rather than test that they exist?**

> 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.

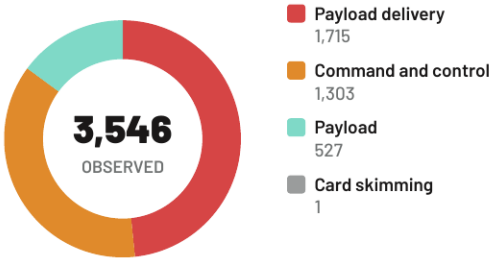
08 What to look for

3,546 indicators observed this period

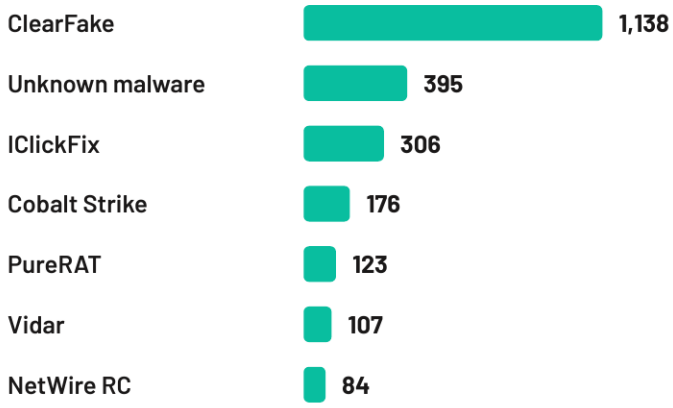
A domain, address or file signature seen in use by attacker infrastructure during the period.

3,546	1,910	1,715	1,303
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 1,217 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.

Payload — The malware file itself, identified by signature.

WHAT STOOD OUT

3,546 indicators were observed in seven days, 1,910 of them high-confidence network addresses you can search your own logs for.

1,138 belong to ClearFake and 306 to IClickFix — two families that do the same thing: a fake update or verification prompt on a website the visitor already trusts.

Look at the delivery domains in the sample. They are ordinary small-business websites — a lash salon, a food shop, a puzzle site. The lure is not a domain anyone would blocklist; it is a real site somebody else failed to patch.

This is how the credential exposure in the previous section is manufactured. The stealer runs on an employee's machine, and the password appears in a leak set months before anyone is listed.

What to look for

A sample of this period's indicators

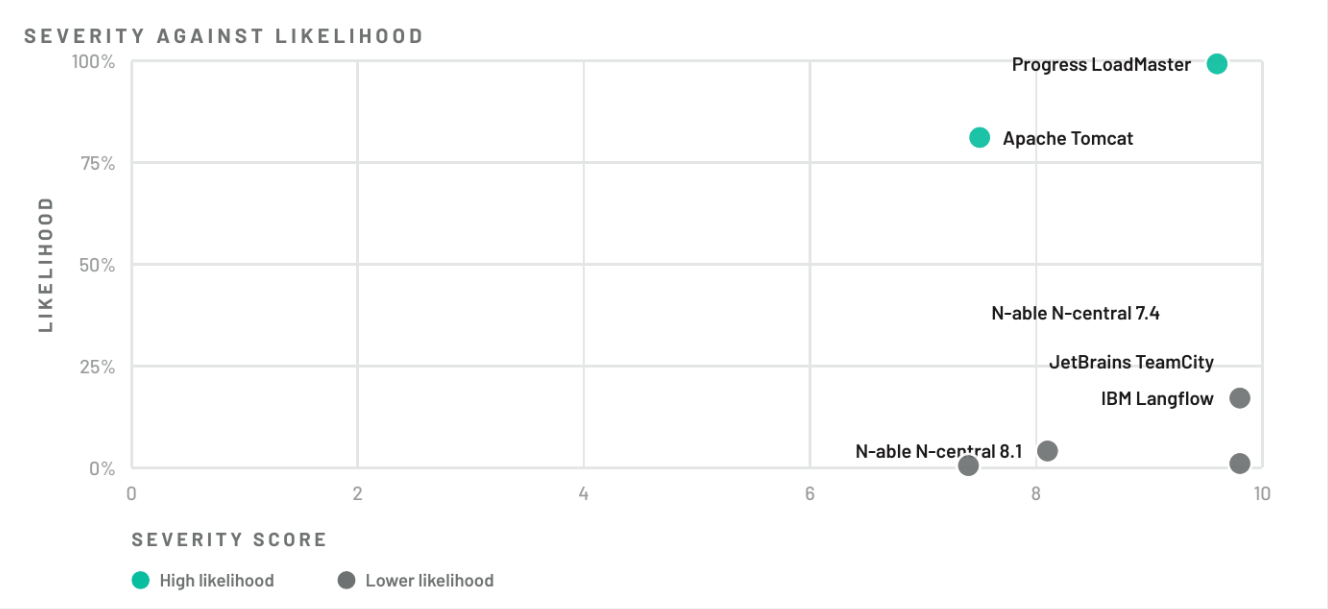
42 of the 3,546 indicators observed this period — the highest-confidence entries at each stage of an intrusion, with no single malware family allowed to dominate. A sample, not the full set. Search them against your own logs.

INDICATOR	TYPE	FAMILY	ROLE
DELIVERY — HOW THE VICTIM IS REACHED			**17**
khqcst.latinmarketmana.com	Domain	ClearFake	Fake-update lure delivering a stealer
lashextensionsdowney.com	Domain	ClearFake	Fake-update lure delivering a stealer
latinmarketmana.com	Domain	ClearFake	Fake-update lure delivering a stealer
letterboxedsolved.com	Domain	ClearFake	Fake-update lure delivering a stealer
nxpdrg.lashextensionsdowney.com	Domain	ClearFake	Fake-update lure delivering a stealer
svohxwo.letterboxedsolved.com	Domain	ClearFake	Fake-update lure delivering a stealer
assessoriamusicalsalvador.com.br	Domain	IClickFix	Fake-update lure delivering a stealer
176.65.148.145:2	IP:port	Mirai	Attacker infrastructure
http://glentraverse.com/kos	URL	SmartApeSG	Fake-update lure delivering a stealer
https://ivyprologue.top/legacy/throttle-theme.js	URL	SmartApeSG	Fake-update lure delivering a stealer
https://slatebeacon.top/legacy/identity-build	URL	SmartApeSG	Fake-update lure delivering a stealer
https://slatebeacon.top/legacy/throttle-theme.js	URL	SmartApeSG	Fake-update lure delivering a stealer
https://slatebeacon.top/legacy/version-validator.js	URL	SmartApeSG	Fake-update lure delivering a stealer
slatebeacon.top	Domain	SmartApeSG	Fake-update lure delivering a stealer
guestsafeimage.info	Domain	TonRAT	Attacker infrastructure
photolog-hotel.top	Domain	TonRAT	Attacker infrastructure
safeimageandphoto.info	Domain	TonRAT	Attacker infrastructure
CREDENTIAL THEFT — STEALERS AND LOADERS			**7**
https://nonobody123.com/a85e9a98b9364c5d8f74.php	URL	Stealc	Attacker command and control
https://jbb.cau777.org/	URL	Vidar	Attacker command and control
https://jbb.popi999.net/	URL	Vidar	Attacker command and control
https://slu.popi999.net/	URL	Vidar	Attacker command and control
jbb.cau777.org	Domain	Vidar	Attacker command and control
jbb.popi999.net	Domain	Vidar	Attacker command and control
slu.popi999.net	Domain	Vidar	Attacker command and control
POST-COMPROMISE — CONTROL ONCE INSIDE			**18**
173.199.70.174:443	IP:port	AdaptixC2	Attacker command and control
173.199.70.174:80	IP:port	AdaptixC2	Attacker command and control
173.199.70.174:8080	IP:port	AdaptixC2	Attacker command and control
46.16.34.50:8001	IP:port	Aisuru	Attacker command and control
85.120.81.167:8001	IP:port	Aisuru	Attacker command and control
85.120.81.167:8080	IP:port	Aisuru	Attacker command and control
91.208.162.129:8001	IP:port	Aisuru	Attacker command and control
91.208.162.129:8443	IP:port	Aisuru	Attacker command and control
91.208.162.129:9035	IP:port	Aisuru	Attacker command and control
108.165.147.244:80	IP:port	Cobalt Strike	Attacker command and control
151.244.243.42:7443	IP:port	Cobalt Strike	Attacker command and control
156.224.18.21:143	IP:port	Cobalt Strike	Attacker command and control
156.224.18.21:587	IP:port	Cobalt Strike	Attacker command and control
156.224.18.21:8010	IP:port	Cobalt Strike	Attacker command and control
39.106.183.67:8080	IP:port	Cobalt Strike	Attacker command and control
141.94.121.162:2222	IP:port	DCRat	Attacker command and control
101.33.45.136:8084	IP:port	VShell	Attacker command and control
http://autumn-mountain-e855.erinbraumbachlianebl.workers.dev/	URL	ValleyRAT	Attacker command and control

09 What crossed the line

6 confirmed exploited · 6 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-2026-8037	**Progress** LoadMaster Load balancer and application delivery controller, sits in front of a supplier's applications and terminates their traffic.	9.6	99.3%	3d
CVE-2026-34486	**Apache** Tomcat Application server. Runs a very large share of the internet-facing Java applications suppliers operate.	7.5	81.2%	3d
CVE-2026-9198	**IBM** Langflow Low-code platform for building AI agents, increasingly wired directly into business systems.	9.8	17.1%	3d
CVE-2026-18577	**N-able** N-central Remote monitoring and management platform used by managed service providers to administer their customers' estates.	8.1	4.1%	3d
CVE-2026-63077	**JetBrains** TeamCity Continuous integration server. It holds the credentials that sign and ship a supplier's software.	9.8	1.0%	3d
CVE-2026-18556	**N-able** N-central Remote monitoring and management platform used by managed service providers to administer their customers' estates.	7.4	0.5%	3d

WHAT EACH COLUMN MEANS

Fix in — The window recommended for fixing each one, counted from the date exploitation was confirmed. 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.

WHAT STOOD OUT

6 vulnerabilities crossed from theoretical to confirmed exploitation this period, and all 6 of them carried a three-day remediation window.

Every one sits in software that stands between a supplier and its customers: a load balancer, a build server, an application server, an AI agent platform, and twice a managed service provider's remote administration console.

Two exceeded an 80% chance of exploitation within 30 days: Progress LoadMaster at 99.3% and Apache Tomcat at 81.2%. Last period nothing exceeded 1.3%.

N-able N-central appears twice, added on consecutive days, both authentication bypasses — the console a managed service provider uses to reach into every customer it administers. This is equipment your supplier runs, not you: you cannot patch it, you will not be told when it is patched, and by the time you could ask, the recommended window has closed.

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?

226 organisations were listed in seven days by 38 separate groups, and 47 of them arrived with no sector recorded at all. Would we know if one of them were ours?

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

58 of the 170 organisations we could check were already carrying stolen credentials when they were listed. What is our number, and when did we last look?

3 Who administers our estate remotely, and what did they patch this week?

Two authentication bypasses in N-able N-central — the console a managed service provider uses to reach into every customer it administers — were confirmed as exploited on consecutive days, both with three-day windows. Who would have told us?

4 What is our plan for the day a supplier's breach is announced by a law firm?

Anubis listed a US grocery chain on 3 August. Within a day two law firms were advertising for claimants and the company had said nothing. Who fields that call here, and what do we say?

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

95% of the 181 organisations we could assess produced no statement, no journalism and no legal activity, and a further 45 could not be identified at all. 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.