CYBER OPERATIONS

WEEKLY INTELLIGENCE

SUPPLY-CHAIN INTELLIGENCE

Issue #004: Beyond The Headlines

Of the 237 organisations we could assess, 16 produced any public account of it.

10 – 16 August 2026

Contents

01 Executive summary

10 – 16 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.

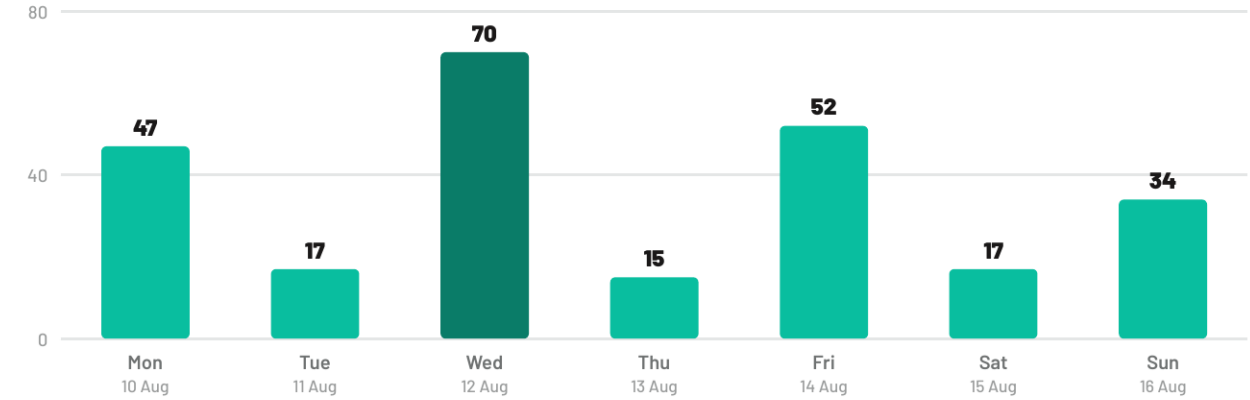
249
ORGANISATIONS LISTED AS VICTIMS BY RANSOMWARE AND EXTORTION GROUPS, ACROSS 252 LISTINGS

44
SEPARATE RANSOMWARE AND EXTORTION GROUPS BEHIND THEM

93%
OF THE 237 WE COULD ASSESS PRODUCED NO STATEMENT, NO JOURNALISM AND NO LEGAL ACTIVITY

42%
OF THE 221 DOMAINS WE COULD CHECK WERE CARRYING EXPOSED CREDENTIALS; 10% HELD CREDENTIALS TO THEIR OWN SYSTEMS

LISTINGS PER DAY



Organisations listed per day. Wednesday carried 70 and Thursday 15, a 4.6-fold spread across the period.

WHAT STOOD OUT

Listing slows at the weekend but does not stop: 51 organisations were listed on Saturday and Sunday, 25.5 a day against 40.2 on weekdays.

Wednesday's 70 is the largest bar on the chart and it is mostly one re-post: 40 of it is Clop republishing names it had masked a week earlier. Friday's 52 is the week's real peak.

WHAT THIS ISSUE COVERS

249 organisations across 252 listings, by 44 ransomware and extortion groups · 237 assessed for public disclosure · 221 domains checked for credential exposure · 5 groups with assessed tradecraft · 5,570 indicators of compromise · 3 vulnerabilities newly confirmed as exploited

HOW WE WORK

Every figure is derived from public sources observable without a supplier's cooperation: listings from ransomware.live, disclosure checked against Google News, credential exposure from LeakRadar, indicators from ThreatFox, and vulnerabilities from the CISA known-exploited catalogue with severity from NVD and exploitation forecasts from FIRST EPSS. Listings are reported as listings, not confirmed breaches. Where we interpret rather than measure, we say so. No client data appears in this report.

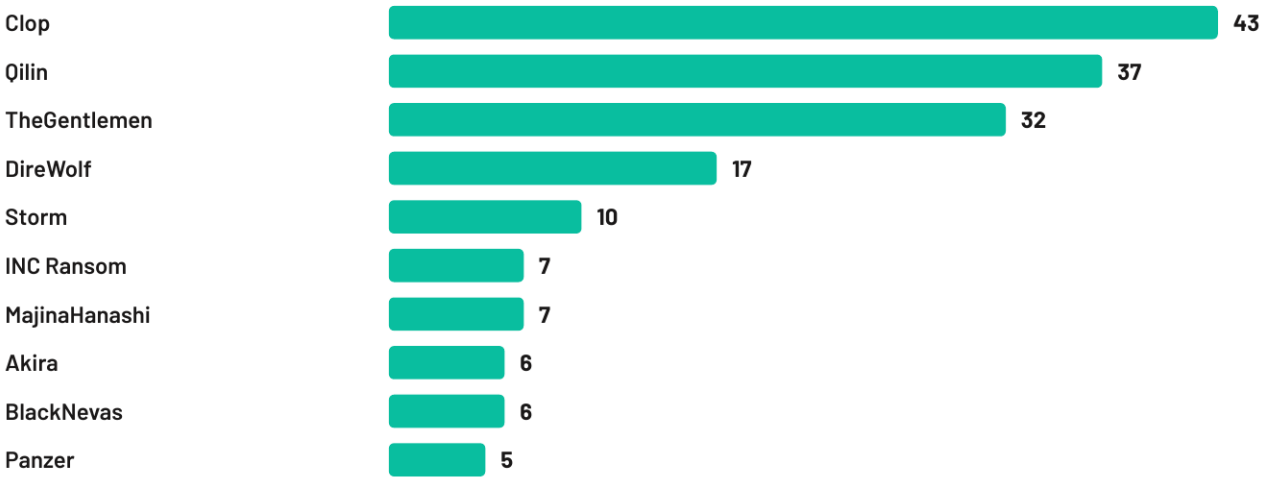
READING THIS AGAINST OTHER ISSUES

Only rate fields may be compared across issues. Issues 002, 003 and 004 all cover seven days. Three cautions this period. 40 of the 252 listings are organisations already listed in issue 003 as name fragments, so the two issues' totals must not be added. This is the first issue to count organisations rather than listings — 249 against 252 — so the headline count is not comparable with earlier issues, though the rates are. And genuine visibility moved from 5.0% to 6.8% on a corrected method rather than a changed world: the first sweep searched leak-site strings such as PHILIPS.COM and missed four large organisations' statements. Credential exposure rose from 34% to 42% and tradecraft coverage fell from 69% to 50%.

02 Who was listed

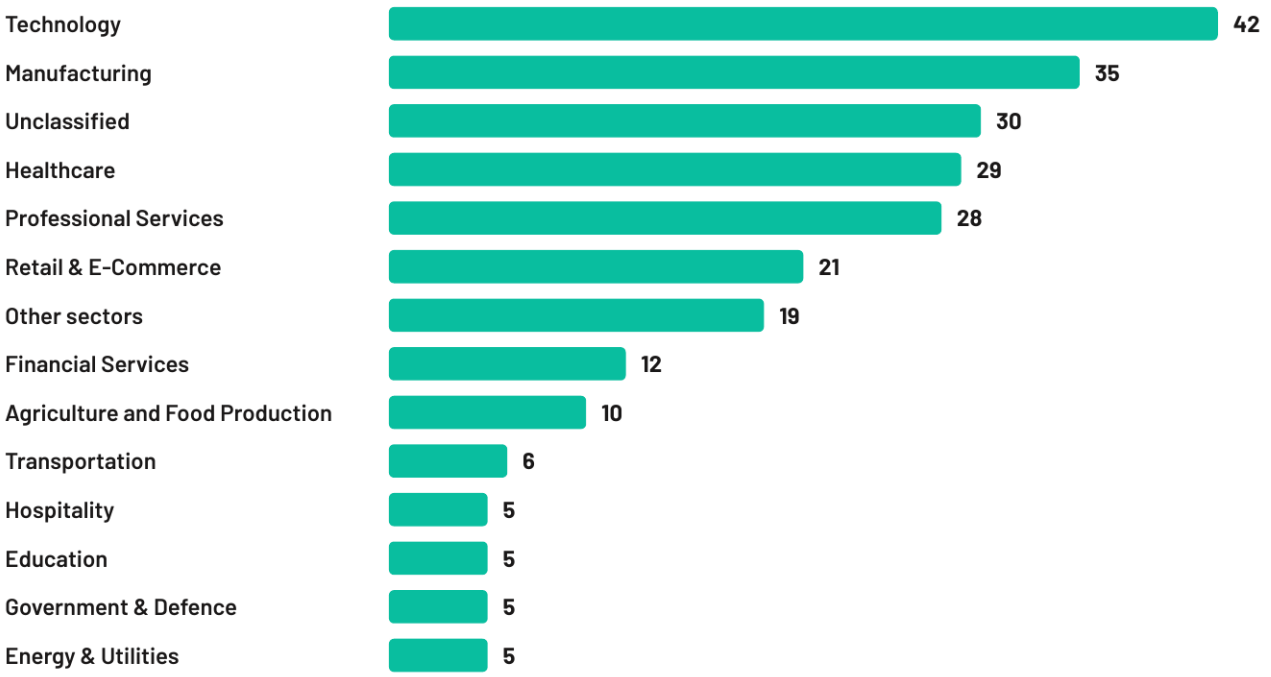
249 organisations across 252 listings · 43 countries · 36.0 a day

LISTINGS PER GROUP



The 10 groups listing the most organisations. Clop and Qilin account for 32% of the period between them. A further 34 groups listed the remaining 82 between them.

SECTOR OF EVERY LISTING



Every sector represented, summing to the 252 listings published this period. They sit in 43 countries, with 86 organisations in the United States.

252

252 listings named 249 organisations in seven days, by 44 separate groups — 36.0 a day.

40

40 of those listings are Clop republishing in full the names it masked a week earlier — Philips, Shell, GE, Fiserv and Toast among them. One actor, one drop, most likely one campaign. Reuters named the common factor on 14 August as PTC Windchill and FlexPLM, product-lifecycle software. The question is not 40 separate incidents but whether your suppliers run it.

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.

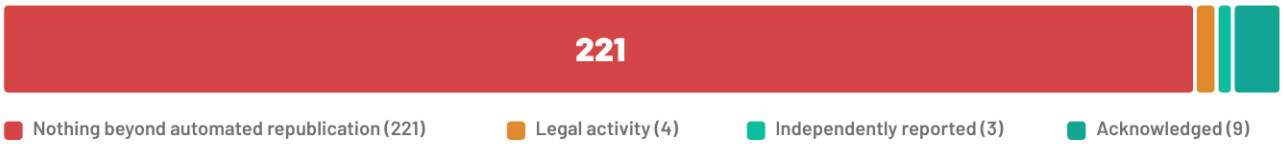
03 Can anyone find out?

All 252 listings · 237 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 listing is counted once, in the highest state it reached; a few organisations were listed by more than one group and appear more than once.

HOW EACH ORGANISATION'S INCIDENT SURFACED



221 of 237 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 or the name is too short to attribute. 15 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. Names are resolved before searching. This issue's first sweep queried the leak site's raw strings, missed four large organisations' statements, and was re-run. Credential counts arrive in buckets of twenty and none is exact to the record. A listing is a publication, not a break-in, so exposure recorded before one is not evidence of the route in.

WHERE IT DID SURFACE — 7 OF 16

ORGANISATION	HOW IT SURFACED	WHERE	DETAIL
Philips, Shell, GE and Fiserv	Acknowledged	each company's own statement; Reuters, BleepingComputer	All four had been name fragments a week earlier and said nothing. Once the full names appeared, Philips said it had contained an attempted compromise of an enterprise server, Fiserv said it had found no evidence that customer, banking or transaction data was compromised, and Shell and GE said they were assessing the position.
Metabase	Independently reported	Cybernews — not Metabase	Its 6 August advisory concerns the flaw in its product and predates its own listing. Metabase has said nothing about being listed, and one publication reported it. The wider coverage of the vulnerability is about its customers, not about Metabase being breached.
AnMed	Acknowledged	AnMed (statements to patients); The Record, HIPAA Journal, Healthcare Dive	Closed 83 of its 106 facilities at the peak and was still restoring services more than two weeks on. A group posting as TheGentlemen took over its Facebook page on 11 August and published the ransom demand there. AnMed says the posts are unverified and has not named the group.
Hong Kong Baptist University	Acknowledged	HKBU (public statement); The Standard	Said publicly that it had noted a webpage alleging a breach and was reviewing its systems, and told staff it had alerted police and commissioned forensics. It has published no figures of its own; the account numbers in circulation are a newspaper's reporting, not an HKBU disclosure.

The other nine are four class-action cases, two reported by journalists, and three further statements.

WHAT STOOD OUT

16 of the 237 organisations we could assess produced any public account of the incident — 6.8%. 9 issued a statement, 3 were brought to light by journalism alone, and 4 produced nothing but class-action advertising.

Four of the 9 statements came from one campaign and all four followed the name being published, not the listing a week earlier. The ones that answered were the large ones. We do not measure severity, so we cannot say it played any part.

04 Exposed before they were listed

93 of 221 domains we could check

Each figure counts stolen credential pairs recovered from infostealer dumps: an account name and the site it was used to log into. The source reports these in buckets of twenty, so every credential figure here is a multiple of 20 and none is exact to the record.

42%	10%	4,780	917,460
CARRYING EXPOSED CREDENTIALS	CARRYING CREDENTIALS TO THEIR OWN SYSTEMS	EMPLOYEE CREDENTIALS, IN BUCKETS OF 20	CUSTOMER CREDENTIALS, NOT A ROUTE IN

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 exposure is more evenly spread this period than last: the largest single organisation, Philips, accounts for 39% of the total against 91% last period. The figure is a distribution with a long tail, not an average, and it is reported in buckets of twenty.

Customer — Philips and Zanichelli carry 39% of the customer figure between them. It is the weakest of the three measures: other people's accounts, not a route in.

THE 14 WITH THE MOST EXPOSED EMPLOYEE CREDENTIALS, OF THE 22 CARRYING ANY

ORGANISATION	LISTED BY	SECTOR	EMPLOYEE	THIRD PARTY	CUSTOMER
Philips	Clop	Healthcare	1,880	6,140	209,580
Hong Kong Baptist University	TheGentlemen	Education	660	2,620	7,700
Shell	Clop	Energy & Utilities	580	2,000	79,340
Columbia University Information (Dental)	Global Secret Group	Healthcare	540	16,920	20,420
Baxter International	ShinyHunters	Healthcare	300	13,800	940
GE	Clop	Technology	180	23,660	56,560
IRCO	Clop	Unclassified	160	620	1,140
Statista	DireWolf	Professional Services	80	80	112,680
The Courier Guy	MedusaLocker	Transportation	60	20	4,160
Zebra Technologies	Clop	Manufacturing	40	580	31,380
Carhartt	ShinyHunters	Retail & E-Commerce	40	120	5,900
Starkey	Clop	Healthcare	40	100	60
Cook Medical	ShinyHunters	Healthcare	40	40	40
Zanichelli	Qilin	Education	20	220	148,800

WHAT STOOD OUT

93 of the 221 domains we could check were already carrying exposed credentials when the organisation was listed — 42%.

The number that describes a way in is smaller. 22 of the 221 — 10% — were carrying credentials to their own systems. The rest qualify on customer or third-party records, which are somebody else's accounts and not a route in.

Retail and e-commerce carried the highest rate, 75% of 20 checked, against 54% of 24 in healthcare.

20 organisations is not a sector finding, and consumer-facing retail brands accumulate infostealer records for reasons that have nothing to do with who attacked them.

One caution on the timing. These credentials were exposed before the organisation was listed, and a listing is a publication, not a break-in. The intrusion behind it usually happened weeks earlier, so this is not proof the credentials were the way in.

05 · THIS PERIOD'S FINDING

Trezor lost 13,689 customers' home addresses to a flaw reportedly two suppliers away.

13,689	2	5	10.0
CUSTOMERS EXPOSED	SUPPLIERS BETWEEN THE FLAW AND THEM	OF METABASE'S CUSTOMERS DISCLOSED A BREACH	SEVERITY, THE MAXIMUM

On 6 August, Metabase published a security update for a flaw in its business-intelligence platform. It scored the maximum 10.0: an unauthenticated attacker could inject arbitrary SQL through the password-reset endpoint and take administrator control — including the live credentials for every database the customer had connected to it.

Over the following four days, five companies told their customers they had been breached through it: Framework, Tally, n8n, Kilo Code and ChecklyHQ. Those are the ones that said so by 16 August. Metabase has published no figure, so the real number is unknown. Public exploit code was open-sourced on 10 August and the vulnerability entered the US exploited-vulnerabilities catalogue on 11 August with three days to fix it.

On 10 August the fulfilment company ShipMonk told Trezor that systems holding Trezor's order data had been accessed. ShipMonk told its customers the route was the Metabase flaw; that is the only account of the link, and Trezor has never named Metabase itself.

Trezor disclosed on 13 August: 11,742 customers with name, email, phone number and shipping address exposed and 1,947 partially, 13,689 in total across seven countries, for orders received between 10 May and 8 August. Trezor notes the 1,947 may include older orders and is still verifying the window with ShipMonk.

Trezor's own systems and devices were not compromised. The flaw was not in anything Trezor ran — it was in software its fulfilment partner had connected to the database holding Trezor customers' home addresses.

WHAT IT MEANS

That is two suppliers between the flaw and the customer. The vendor questionnaire that would have caught this is not the one you send ShipMonk; it is the one ShipMonk would have to send Metabase. Almost no supplier-risk programme reaches that far, and the ones that do reach it by name, not by dependency. One control appears to have limited it, and it was contractual rather than technical. Trezor requires fulfilment partners to delete or anonymise order data 90 days after delivery, and the exposed set is roughly three months of orders rather than every order it has shipped — though Trezor's own note says some records may be older, so the clause may not have held everywhere. Retention terms are the cheapest supply-chain control there is, and the only one that limits damage in a system you cannot see. For a hardware wallet company the exposed field that matters is the home address. Customers known to hold cryptocurrency, matched to where they live, is a physical-security problem, not a privacy one — and it was created two companies away from the brand the customer trusted. This is also the week's exception, and it is worth saying so. Every party in this chain disclosed, quickly, which is the only reason it can be described at all. The 93% on page 5 are the weeks where there is no chain to follow — and the credential check on page 6 would not have found this one either, because the exposure was never on Trezor's domain.

06 The route in

5 of 44 groups assessed · 50% 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 are on record as using — and the next section turns them into the questions.

These are techniques a public catalogue attributes to each group, not observations of what they did this period, and not MITRE ATT&CK group profiles — ATT&CK carries entries for only two of these five. The technique identifiers and names are ATT&CK's; the group mapping is community-maintained and historical, which is why Clop's entry for exploiting internet-facing applications still cites 2021 vulnerabilities. Read it as what each group is known to do, and the questions opposite as the ones worth asking whoever your supplier is.

HOW AN ATTACKER GETS IN

The entry techniques, and how many of the 5 assessed groups use each. Red because these are the ones short enough to close.

WHAT STOOD OUT

5 of the 44 groups listing organisations this period have enough tradecraft on public record to map. Those 5 listed 125 of the 252 — 50%.

123 technique identifiers across those groups, 88 once sub-techniques are folded into their parent — which is how the counts opposite are taken. Entry is the narrow part: all 5 use valid accounts and all 5 exploit an internet-facing application. On a set of 5 that is a small-sample result, but it is the same two doors every period.

7 of the twelve groups that listed most organisations this period have no usable technique record in the catalogue we use, DireWolf among them — the fourth largest total of the week.

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 are recorded as doing, and the question that separates a supplier who has covered it from one who says they have.

PREVENT

Valid Accounts 5/5 · Exploit Public-Facing Application 5/5 · Phishing 4/5 · Valid Accounts: Domain Accounts 2/5

93 of the 221 domains we could check were carrying exposed credentials when the organisation was 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 4/5 · Windows Management Instrumentation 3/5 · Command and Scripting Interpreter 5/5 · Command and Scripting Interpreter: PowerShell 3/5

4 of 5 assessed groups disable or modify security tooling, and 5 of 5 run their tooling through a command interpreter, mostly PowerShell.

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

DETECT

Remote System Discovery 3/5 · Network Service Discovery 3/5 · System Information Discovery 3/5 · OS Credential Dumping: LSASS Memory 2/5

3 of 5 scan the network from inside once they are in, and 3 dump operating-system credentials, 2 of them from LSASS specifically. *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 4/5 · Lateral Tool Transfer 4/5 · Remote Services: SMB/Windows Admin Shares 3/5 · Application Layer Protocol 4/5

4 of 5 move by remote desktop and 3 by Windows admin shares; counted together, all 5 use remote services.

> ASK A SUPPLIER
> **Can anything in your environment reach ours over RDP, SMB or a site-to-site link, and what leaves your estate to a destination you do not manage?**

RECOVER

Data Encrypted for Impact 5/5 · Inhibit System Recovery 4/5 · Financial Theft 2/5 · Service Stop 1/5

4 of 5 destroy the recovery points before they encrypt. But 3 exfiltrate to cloud storage and 3 over non-command channels: this period's finding involved no encryption at all.

> 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. These are techniques a public catalogue attributes to each group, not observations of what they did this period, and not MITRE ATT&CK group profiles — ATT&CK carries entries for only two of these five. The technique identifiers and names are ATT&CK's; the group mapping is community-maintained and historical, which is why Clop's entry for exploiting internet-facing applications still cites 2021 vulnerabilities. Read it as what each group is known to do, and the questions opposite as the ones worth asking whoever your supplier is. Data Encrypted for Impact is recorded against every group in the source catalogue, so a full count on that row distinguishes nothing and nothing here rests on it. A count covers a technique and its sub-techniques together, so a figure in the text can be higher than the single sub-technique shown beside it. The denominator is 5 groups. A technique used by all 5 is a small-sample result, not a universal one, and the counts are shown rather than converted to percentages for that reason.

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

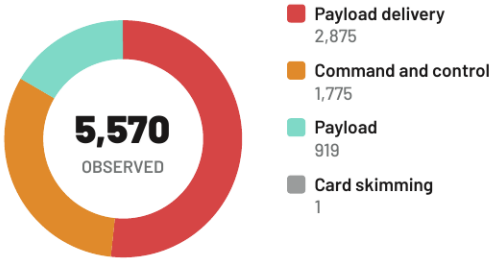
08 What to look for

5,570 indicators observed this period

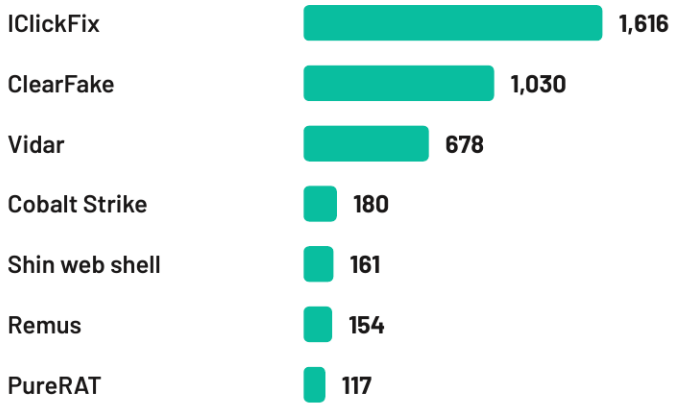
A domain, address or file signature seen in use by attacker infrastructure during the period.

5,570	3,218	2,875	1,775
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 1,634 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

5,570 indicators were observed in seven days, 3,218 of them high-confidence network addresses. A further 281 carry no family attribution at all.

1,616 belong to IClickFix and 1,030 to ClearFake — two families that do the same thing: a fake update or verification prompt on a website the visitor already trusts, which ends with the visitor pasting a command into their own machine.

14 of the 29 in the sample are hosts somebody else already owned — legitimate sites and accounts taken over, not infrastructure the attacker built. Search for them. Do not block them without looking first.

This is how the credential exposure in section 04 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

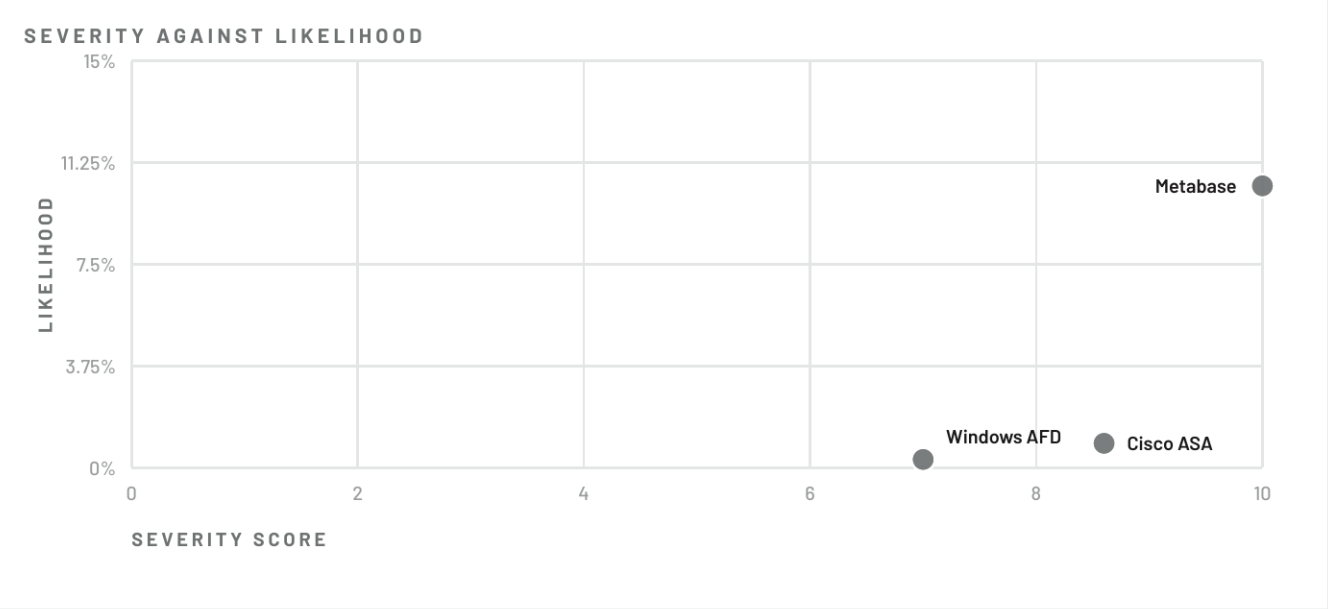
29 of the 5,570 indicators observed this period — the highest-confidence entries at each stage of an intrusion, with no single malware family allowed to dominate. A sample, not the full set. Search them against your own logs.

INDICATOR	FIRST SEEN	TYPE	FAMILY	ROLE
DELIVERY — HOW THE VICTIM IS REACHED				**10**
moniskk[.]live	2026-08-11	Domain	IClickFix	Fake verification prompt that gets a user to paste a command
verif-key-code[.]info	2026-08-11	Domain	IClickFix	Fake verification prompt that gets a user to paste a command
leappoploaderinstantly[.]monster	2026-08-11	Domain	IClickFix	Fake verification prompt that gets a user to paste a command
getignitra[.]com	2026-08-10	Domain	ClearFake	Fake-update lure delivering a stealer
get--ignitra[.]com	2026-08-10	Domain	ClearFake	Fake-update lure delivering a stealer · **compromised host**
bypraqr[.]get--ignitra[.]com	2026-08-10	Domain	ClearFake	Fake-update lure delivering a stealer
hxxps://yelahaye[.]surf/api/v1/status	2026-08-11	URL	KongTuke	Fake verification prompt that gets a user to paste a command · **compromised host**
hxxps://mathiuu[.]surf/api/v1/verify	2026-08-12	URL	KongTuke	Fake verification prompt that gets a user to paste a command · **compromised host**
herndndes[.]beer	2026-08-12	Domain	KongTuke	Fake verification prompt that gets a user to paste a command · **compromised host**
488e038d75bd71a749dcb98ca5f0006d	2026-08-15	MD5	KongTuke	Fake verification prompt that gets a user to paste a command
CREDENTIAL THEFT — STEALERS AND LOADERS				**7**
its[.]sm188auto[.]top	2026-08-10	Domain	Vidar	Infostealer harvesting browser-saved passwords and session cookies · **compromised host**
its[.]beras1[.]com	2026-08-10	Domain	Vidar	Infostealer harvesting browser-saved passwords and session cookies · **compromised host**
goo[.]bercak4d[.]org	2026-08-10	Domain	Vidar	Infostealer harvesting browser-saved passwords and session cookies · **compromised host**
7a933fff468a55cfe086b1939080127d	2026-08-12	MD5	Vidar	Infostealer harvesting browser-saved passwords and session cookies
72[.]62[.]195[.]74:2536	2026-08-11	IP:port	Remus	Stealer collecting credentials from an infected machine
64[.]176[.]12[.]165:8811	2026-08-14	IP:port	Remus	Stealer collecting credentials from an infected machine
209[.]38[.]82[.]72:9048	2026-08-15	IP:port	Remus	Stealer collecting credentials from an infected machine
POST-COMPROMISE — CONTROL ONCE INSIDE				**12**
154[.]12[.]86[.]154:8002	2026-08-10	IP:port	Cobalt Strike	Post-compromise command and control framework · **compromised host**
192[.]252[.]179[.]24:443	2026-08-10	IP:port	Cobalt Strike	Post-compromise command and control framework · **compromised host**
192[.]252[.]179[.]24:80	2026-08-10	IP:port	Cobalt Strike	Post-compromise command and control framework · **compromised host**
89[.]125[.]244[.]131:80	2026-08-10	IP:port	VShell	Cross-platform command and control implant · **compromised host**
8[.]147[.]56[.]196:8084	2026-08-11	IP:port	VShell	Cross-platform command and control implant · **compromised host**
180[.]76[.]53[.]183:80	2026-08-11	IP:port	VShell	Cross-platform command and control implant · **compromised host**
rx7brabo[.]ddns[.]com[.]br	2026-08-13	Domain	PureRAT	Remote access tool used once a machine is controlled
combustu[.]bingbaochow[.]cam	2026-08-11	Domain	AsyncRAT	Remote access tool used once a machine is controlled
updatewindows[.]gotdns[.]ch	2026-08-11	Domain	AsyncRAT	Remote access tool used once a machine is controlled
158[.]94[.]208[.]101:8808	2026-08-11	IP:port	AsyncRAT	Remote access tool used once a machine is controlled · **compromised host**
1bb0a4abcc83dd82f0c7da52ce5d9e8a	2026-08-13	MD5	AsyncRAT	Remote access tool used once a machine is controlled
812abe43796f6b78922fc9228e422465	2026-08-12	MD5	Kuiper	Ransomware payload

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 how probable exploitation was thought to be. This period they rank the same way, which is unusual.

REFERENCE	PRODUCT	SEVERITY	LIKELIHOOD	FIX IN
CVE-2026-72898	Metabase Business-intelligence platform, usually a supplier's rather than yours. It holds live credentials for every database connected to it, which is what made this a supply-chain event rather than a single breach.	10.0	10.4%	3d
CVE-2026-20349	**Cisco** Secure Firewall ASA and Threat Defense Remote-access VPN on a firewall — almost certainly on your own estate as well as your suppliers'. This flaw crashes the device rather than giving an attacker a way through it.	8.6	0.9%	3d
CVE-2026-68820	**Microsoft** Windows Ancillary Function Driver for WinSock Core Windows networking driver, on effectively every Windows machine you and your suppliers run. Local privilege escalation: the step after a stolen credential.	7.0	0.3%	14d

WHAT EACH COLUMN MEANS

Fix in — The deadline CISA sets US federal agencies, counted from the date it confirmed exploitation. It is not an obligation on you; it is the best public read on urgency, and 3 days is at the sharp end.

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

Likelihood — A forecast of the chance a flaw will be exploited in the next 30 days, published before exploitation is observed. Every entry here is already being exploited, so read it as how predictable each one was, not as how likely it is.

WHAT STOOD OUT

3 vulnerabilities crossed from theoretical to confirmed exploitation this period, 2 of them with a three-day remediation window.

None of the three was predicted. On 11 August, the day CISA confirmed exploitation, the Metabase flaw's forecast was 0.7% — the 49th percentile, the middle of the distribution. It reached the 95th on 17 August, after the fact. The other two are still below 1%.

The Metabase entry is the same vulnerability as this period's finding. A catalogue entry and a customer notification, 11 and 13 August, are the same event seen from two ends.

Two of these are almost certainly on your own estate as well as your suppliers' — a firewall VPN and a Windows driver — and the analytics platform is the one you cannot reach. Check the first two this week; ask about the third.

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 Who are our suppliers' suppliers, for the ten that matter most?

13,689 Trezor customers lost their home addresses through a flaw in software Trezor never bought — two suppliers out from any contract it holds. Could we name the second link for any of our top ten?

2 Do we run Cisco ASA or Secure Firewall, and is CVE-2026-20349 closed?

Two of this period's three confirmed-exploited flaws sit on your own estate as well as your suppliers': a firewall VPN, where the flaw crashes the device rather than opening it, and a Windows driver. Their deadlines are CISA's, not yours — 14 August and 25 August — and the first has passed.

3 Which of our suppliers connect a reporting tool to a live customer database?

The Metabase flaw handed over the credentials for every database connected to it. The exposure was not in the analytics tool; it was in what the analytics tool could reach.

4 What do our contracts say about deleting our data when the work is done?

A 90-day retention clause is the reason Trezor's exposure was three months of orders rather than every order it had ever shipped. Which of our supplier contracts carries one, and has anyone checked it is honoured?

5 If a supplier of ours were listed tomorrow, would we hear it from them or from a wire?

93% of the 237 organisations we could assess produced no account we could find in English. The ones that did speak were the household names, and they spoke after a news agency published.

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.