



Darknet and deep web intelligence engine,
specialised in company documents.

SPECIMEN
fictitious data

Specimen. ACME and every organisation, person, address and value in this document are fictitious. It shows the form and level of detail of a statement delivered to a client.

Darknet exposure statement: ACME

Recipient: ACME Aérostructures SAS and ACME Aero Belgium SRL

Domains covered: acme-aero.example, acme-aerostructures.example, acme-aero-be.example

Delivery date: 1 October 2026

Prepared by: SitinCloud, publisher of OwlyScan

Nature of the statement: passive collection. No access to your systems, no scan of your infrastructure, no attempt to use the credentials or keys found. We have read only what is already exposed.

Executive summary

ACME is not itself the target of any ransomware claim. No ACME file share has been published in bulk, and no group names it as a victim.

Yet ACME secrets are circulating in clear text, and two call for action today. Four publications concern ACME directly: 119 documents, 12 of them rated high criticality. Their origins have nothing in common: infostealer logs (credential-stealing malware) taken from 14 employee workstations, six pastes on a public text-sharing service since 21 September 2026, your accounting firm's files published by a ransomware group, and forum threads describing your network. A wider search across your suppliers brings the total to seven sources, indexed between 12 May 2023 and 29 September 2026.

Requested heading	Finding	Severity
Trade secrets	Relationship with your machine shop reconstructed (quantities, deliveries, machine time, a quality defect), 14 suppliers with bank details and payment schedule	Medium, high when combined
Technical and industrial data	No drawing read, but the inspection file for a titanium part and the drawing index, with their export classes, published at a subcontractor	High
Sensitive defence information	No classified document, no marking, no defence programme. Drawings classified for export (<code>9E991</code> , <code>EAR99</code>)	Low, to be monitored
HR data	14 employees whose workstation is infected, 6 finance staff named with their direct line, the payment approval workflow	Medium
Cyber entry points	A VPN login for accounts payable, a billing key and a database password pasted on 27 September 2026	High
Entry points for a physical approach	Schedule, dock and contents of shipments to your assembly line, night security at Lavaur	Medium

The four points that call for a decision.

- Two ACME secrets were pasted in clear text on 27 September 2026.** The billing API key `acme_bill_[...]` and the password of the `billing_prod` database. This is the most direct item in the statement: rotating both secrets closes this scenario.

2. **A VPN login for accounts payable is in infostealer logs.** The `slemaitre` account, stolen on 22 July 2026 at Lavour. It combines with the gateway described by a forum and the finance names published with your accounting firm's files: three publications, none of which shows it alone. What is missing is the second-factor enrolment list, which we cannot see.
3. **ACME's part documentation is in the Globex Machining share.** First article inspection, purchase order, non-conformity, drawing index, load plan: 312 GB published on 2 June 2026, after a sale announcement. ACME's name does not appear in it; the customer code `AC-0092` is enough.
4. **Your accounting firm's files are published.** Invoices with their real numbers, bank details of 14 suppliers, payment schedule, names and direct lines of the finance team: enough to write a fake bank-details change letter that looks like a real one.

The overall reading. What ACME risks is not first of all the disclosure of its know-how: it is that someone gets in with its own keys and speaks to its teams in its own words. Three items from three unrelated sources complement each other: the key, the door and the person. Of the five attack scenarios OwlyScan computes for ACME, two are of high severity (logging in to the VPN, calling the billing API), two medium (phishing the finance team, diverting a payment) and one low (mapping the network). The hardening to carry out concerns secrets, VPN authentication and the supply chain, where your part documentation circulates outside your walls, under a customer code.

1. Summary

ACME appears in no ransomware claim. Yet ACME documents and secrets are circulating, coming from four unrelated places: infected workstations, an operating habit (dropping working files on a public service), an accounting firm and, one step further out, a machine shop and its freight forwarder. **Seven distinct sources** have been identified, and 55% of dated documents are less than a year old: the exposure is recent, not historical.

The mechanism is that of proximity leaks: it is not your information system that gives way, it is neighbouring links that hand over what they know about you. Each holds a piece of ACME, none has the whole, and it is the assembly that becomes usable. Four points call for a decision on your part.

Two secrets pasted in clear text. The billing API key and the `billing_prod` database password were posted on 27 September 2026 on a public text-sharing service, with the database server address. The six pastes in the series are new since 21 September.

A VPN access in three parts. The account of an accounts payable accountant at Lavour appears in a batch of infostealer logs (workstation infected on 22 July). The gateway comes from a forum, the identity and role of the account holder from your accounting firm's files. One element is missing, which only your team can see: the second factor.

Your part documentation, in your machine shop's share. The Globex Machining files, 312 GB, were published on 2 June 2026, four days after a sale announcement. Your references appear in them under a customer code, with the inspections, the order and the drawing index. The manifests of its freight forwarder, Initech Freight, show the same parts on their way to your assembly line.

Your accounting firm's files. Those of Contoso Expertise Comptable, published on 24 March 2026, deliver for ACME invoices, the bank details of 14 suppliers, the payment schedule, the named finance team and the approval workflow. Nothing classified, no drawing read, no source code: what you risk is entry through the right door, with the right key.

2. Scope, method and limits

What we queried. The OwlyScan index covers ransomware claim sites, exfiltration archives reachable through `.onion` addresses, infostealer log batches, text-pasting services and forums. Thirty-four queries were run on your domain names, your company names (ACME Aérostructures SAS, ACME Aero Belgium SRL), your executives, your IP address ranges and the part references you entrusted to us (prefix `7Q-4410-`). Sources are identified by a letter, from A to G (section 4).

Raw volumes.

Query	Occurrences	Observation
"acme-aero.example"	131	of which 36 duplicates (same file in several archives)
"acme-aerostructures.example"	9	
"acme-aero-be.example"	12	
"vpn.acme-aero.example"	19	of which 14 in forum threads
"ACME AEROSTRUCTURES"	87	of which 29 unrelated namesakes
"acme_bill_"	2	the key, and the variable name in the configuration file
"203.0.113.40"	17	VPN gateway
"198.51.100."	11	test servers and billing database
"7Q-4410-114"	21	14 at Globex Machining, 6 at Initech Freight, 1 sale announcement
"AC-0092"	11	5 at Globex Machining, 6 at Initech Freight

What we discarded. The string `acme` alone returns more than 3,000 results, almost all of them web server configurations containing an `acme-challenge` directory: no connection. Of the 87 occurrences of `ACME AEROSTRUCTURES`, 29 refer to namesakes (a structural steelwork company, a ladder manufacturer). Eighteen `@acme-aero.example` addresses appear in old credential compilations from third-party sites: they indicate no compromise of ACME. The 36 duplicates of the first domain were merged.

What we did not find, which matters just as much. No ransomware claim in ACME's name. No sale listing for VPN access, remote desktop or gateway on the marketplaces indexed. No source code. No drawing read: the Globex Machining drawing index is published, but no drawing file is in the part of the archive we read. No document from the integrator or the end customer. No payroll data, no employee file. No second-factor enrolment list.

How the link to ACME is established. ACME's name appears in no Globex Machining or Initech Freight file: they refer to their customer by a code, `AC-0092`. The link rests on three findings. The part references (`7Q-4410-114`, `-116`, `-120`) are yours, you entrusted them to us. In two sources that do not know each other, the Globex share and the Initech manifests, they are always associated with the same customer code, and the sale announcement cites them without it. Finally, order `P0-2026-0412` (240 brackets, 120 fittings, week 18) is found identically on manifest `MAN-55810`, and the accounting firm's 2025 purchase ledger (source C) lists Globex Machining among your machine shops. This is a solid inference, not proof: only your purchasing department can confirm that `AC-0092` is indeed your code.

Dating. The indexing date is that of OwlyScan's first read, not that of the leak. Of the 119 documents in sources A to D, 112 carry a usable date, and 62 of them are less than a year old, that is 55% of dated documents.

Limit of the exercise. A passive statement sees only what has been published and indexed: an exfiltration under negotiation remains invisible. The Globex Machining archive is read part by part. The 14 documents cited are all in part 07, and the other parts, still being processed, may contain more, drawings included. We tested no credential and no key, which may have been changed since their publication. This statement is current as of 30 September 2026.

3. Answers heading by heading

3.1 Trade secrets

A supply relationship is reconstructed, with its volumes and its schedule.

Globex Machining (sources E and G). Its file share, published on 2 June 2026, contains purchase order `P0-2026-0412`: 240 brackets `7Q-4410-114` revision C and 120 fittings `7Q-4410-116` revision B, delivery in week 18 at dock B of the “Plant 2” factory, quality clause `QC-7` (first article inspection required). The load plan `Plant2_Load_wk14-26.xlsx` adds the machine time: in week 18, 96 hours on machine `M4` for the brackets, or 24 minutes per part. The Initech Freight manifests (source F) give the pace: four shipments in April 2026 (40, 60, 80 and 100 parts), then, in May, a batch of samples and two crates (240 brackets, 120 fittings).

A quality defect, dated and explained. Non-conformity report `NCR-2026-031` records a bore at 12.06 mm against a dimension of 12.00 mm +0.05, the rework decided, the concession request sent to the quality department of customer `AC-0092` and the cause: wear of the machining fixture on machine 4.

What this gives a competitor: the name of your machine shop, the quantity and delivery week of each batch, the unit machining time, the ramp-up and the history of a defect on a titanium part. Enough to estimate your cost price and prepare a competing bid.

The accounting firm (source C). Its 38 documents list 14 recurring suppliers (including Globex Machining, Soy lent Matériaux for titanium, Wonka Traitements de Surface, Fabrikam Outillage, Umbrella Métrologie and Vandelay Sécurité), with invoices, amounts and due dates. The last six VAT returns, from August 2025 to January 2026, give the monthly turnover.

Severity: medium, high when combined. No framework contract, no customer invoice, no selling price was found. But the whole outlines your cost structure on one part, your delivery schedule, your suppliers and your cash flow rhythm.

3.2 Technical and industrial data

No drawing read, but the inspection file of a structural part. Everything comes from part 07 of the archive `globex_shares_part07.7z`, published on a ransomware group's claim site (host `mojzk4yj.onion`) on 2 June 2026.

The first article inspection report. File `globex/Shares/Quality/FAI/FAI_7Q-4410-114_revC.xlsx`, inspected on 14 March 2026 and approved on 16 March. At the top:

```
Part number;7Q-4410-114;Rev;C
Part name;Bracket, wing-to-pylon fairing
Customer;AC-0092;Purchase order;P0-2026-0412
Material;Ti-6Al-4V AMS 4928;Heat lot;H-22871
Drawing;7Q-4410-114 sheet 1-3;Export class;9E991
```

Eight characteristics follow with their dimension, tolerance and measured value. Characteristic 4, bore B, is marked `NOK`.

The drawing index. The file `globex/Shares/Engineering/Drawings/index.csv` lists 12 references for `AC-0092`. The first three:

```
drawing;rev;title;customer;export
7Q-4410-114;C;Bracket, wing-to-pylon fairing;AC-0092;9E991
7Q-4410-116;B;Fitting, fairing aft;AC-0092;9E991
7Q-4410-120;A;Shim set;AC-0092;EAR99
```

The other nine, from `7Q-4410-130` to `7Q-4410-146`, are the components that assemble onto the `7Q-4410-114`: each has its inspection report in the share. The assembly structure can be reconstructed without a drawing. The paste of 29 May 2026 (source G, `/p/8fd2c1`) puts the share up for sale and claims the drawings:

Globex Machining full share dump 312 GB, incl. engineering drawings for aerospace customers (7Q-4410-114, 7Q-4410-116...)

We can state neither that these drawings are in the archive nor that they are not: the part read contains none.

Severity: high. It is not a drawing, but it is the inspection file of a structural part of a commercial aircraft programme: material, heat lot, tolerances, export class. It came out of a tier 1 subcontractor where your confidentiality requirements now apply only on paper. ACME's name is not in the file, but the reference is yours.

3.3 Sensitive defence information

No classified document, no protective marking, no defence programme reference in the index for ACME. The scope covered is that of a commercial aircraft programme.

Some compliance information is nonetheless exposed. The drawing index classifies each reference for export (`9E991` for the first two, `EAR99` for the third), and manifest `MAN-55794` carries the note "export-controlled, keep paperwork with the crate". These are not defence markings, they are export control classifications: they indicate that your parts fall under an export regime and that their movement is governed by a paperwork file (see 3.6).

Severity: low today, to be monitored. The risk is not the disclosure of a defence secret, it is that an export-controlled document circulates outside the authorised chain.

Specific recommendation: have your export compliance officer check that these classes are those you declared, and whether this circulation calls for informing the integrator.

3.4 HR data

Two sources name your teams: the infostealer logs and the accounting firm's file. No payslip or individual file was found.

The infected workstations (source A). The logs come from 14 workstations (8 at Lavour, 3 at Castres, 3 at Ath), infected between 2 February 2024 and 9 August 2026, ten of them since October 2025. Each workstation yields two credential files (one per browser) and a system sheet: workstation name, user, country, installed software. To this is added an SSH host list, `ssh_hosts.txt`, found on the administration workstation `LAV-PC009`, making 43 documents. Workstations follow the `SITE-PCnnn` convention (`LAV-PC114`, `CAS-PC027`, `ATH-PC031`). Of the 28 credential files, 8 are of high criticality: they contain a login for an ACME service (VPN, webmail, ERP, purchasing portal). The other 20 mix private and professional use.

The finance team, named (source C). The contact sheet of the ACME file, dated 20 November 2025:

Name	Role	Direct contact exposed
Marianne Chauvet	Chief Administrative and Financial Officer	<code>+33 5 36 49 02 08</code>
Nathalie Vasseur	Accounting and Treasury Manager	<code>+33 5 36 49 02 21</code>
Sylvie Lemaitre	Accounts payable accountant	<code>+33 5 36 49 02 17</code> , <code>+33 6 39 98 41 52</code>
Arnaud Barbier	Accounts receivable accountant	<code>+33 5 36 49 02 19</code>
Étienne Brossard	Management accountant	<code>+33 5 36 49 02 24</code>
Charlotte Morel	Accounting assistant	<code>+33 5 36 49 02 26</code>

Also listed are Quentin Wauters, head of the Ath site, and Aurélie Hanot, administrative and financial officer. On the firm's side, the engagement letter names Mathieu Roche, partner chartered accountant, and Inès Navarro, who handles the file.

Why this cross-referencing matters. A finance team can be guessed from professional networks. What cannot be guessed is who holds which authority: the accounts payable accountant prepares payments, the accounting and treasury manager approves them, the Chief Administrative and Financial Officer countersigns above €20,000 (point 3.5.d). The stolen VPN account (point 3.5.a) is that of the first, the person best placed to trigger a payment.

Severity: medium. No health or payroll data. But a name, a role, a direct line and an approval right are enough to make a call or an email credible.

3.5 Entry points for a cyber attack

a. A VPN access in the name of accounts payable

Source: host `x4hq7p2d...onion`, archive `FR_FREEPACK_2026-08.zip`, infostealer log batch showcased by a reseller, indexed on **14 August 2026**. Workstation `LAV-PC114`, infected on **22 July 2026**. The entry saved by the browser:

```
URL: https://acces.acme-aerostructures.example/  
Login: slemaitre  
Password: [...]
```

Analysis. The address is an alias of the gateway on the old domain, and the login follows the original convention of first initial plus surname. On its own, the entry says neither whether the alias still responds nor who `slemaitre` is. Two other publications answer. The forum (source D) establishes that this alias and `vpn.acme-aero.example` point to the same address, `203.0.113.40`, and that the login page was still responding on 3 July 2026. The accounting firm (source C) gives the name, role and direct line of Sylvie Lemaitre, accounts payable accountant. Evidence gathered: **3 out of 4**. We did not find the list of accounts enrolled in the second factor.

No publication shows this scenario alone: it is their assembly that composes it. A password stolen on 22 July 2026 is ten weeks old at the date of this statement: if the account does not require a second factor, it may be enough. It must be considered burnt, the sessions of `LAV-PC114` revoked and the workstation reinstalled.

b. A billing key and a database password, pasted on 27 September 2026

Source: host `dmp5cnzx...onion`, text-pasting service. Six pastes by the same anonymous author, indexed from **21 to 29 September 2026**, all new since 21 September.

Date	Content	Criticality
21 September	deployment script, hard-coded API key labelled "test"	medium
23 September	seven test servers, from <code>198.51.100.11</code> to <code>198.51.100.17</code>	medium
24 September	application log excerpt: five business addresses	low
27 September	configuration file with the login and password of the <code>billing_prod</code> database	high
27 September	billing API key <code>acme_bill_...</code>	high
29 September	description of the backup, no secret	low

The configuration file, secrets masked:

```
db_host: 198.51.100.23  
db_name: billing_prod  
db_password: [...]
```

Analysis. The key pasted on 27 September does not have the `_test` marker of the test key in the 21 September script: everything points to a production key. We do not probe the network: we do not know whether `198.51.100.23` is reachable from the Internet. If it is, the password opens the billing database directly; if not, it helps whoever is already getting in by other means, through the VPN of point a for example. Nothing indicates an intrusion at your end: the series has the profile of working files dropped from a development workstation. But the service is public, read by automated collectors, and we cannot say who else read these pastes. The seven test servers also appear in the SSH host list of source A, along with a bastion (`198.51.100.5`): the two sources confirm each other.

This is the most direct item in the statement. Rotating the key and the password closes this scenario and by itself justifies action today.

c. ACME's network, described by a forum

Source: Russian-language forum, host `f2tn5vby...onion`, 32 messages from **11 May 2023** to **3 July 2026**, indexed from **12 May 2023**. Three members, in threads exchanging target lists for European aerospace. No message offers access for sale.

Machine	IP	First mention	Function
<code>vpn.acme-aero.example</code> (and <code>acces.acme-aerostructures.example</code>)	203.0.113.40	11 May 2023	remote access
<code>webmail.acme-aero.example</code>	203.0.113.41	11 May 2023	webmail
<code>erp.acme-aero.example</code>	203.0.113.44	2 February 2024	production management
<code>portail.acme-aero.example</code>	203.0.113.46	14 October 2024	supplier document drop
<code>vpn.acme-aero-be.example</code>	192.0.2.18	9 April 2025	remote access, Belgian site

The messages also give the account convention (first initial plus surname) and that of workstations (`SITE-PCnnn`).

Analysis. Nothing usable on its own: no account, no announced vulnerability, no password. But the inventory is established: the `203.0.113.0/24` block did not change from 2023 to 2026, the gateway is known under two names, the account convention is public. Anyone preparing an operation against ACME starts from these five machine names, with no need to search. It is worth checking that each of these services must be reachable from the Internet, and under which authentication.

Severity: low in itself. But this reconnaissance has been done and shared for more than three years, and it provides the door for the scenario of point a.

d. The supplier payment workflow, with its template documents

Source: ACME file of the firm Contoso Expertise Comptable, published by a ransomware group (host `h6wk3zr5...onion`) on **24 March 2026**, indexed on **25 March 2026**. Of nearly 6,400 files, all clients combined, 38 concern ACME:

Document type	Number	Criticality
Supplier bank details register (<code>RIB_fournisseurs_2026.xlsx</code>)	1	high
2026 payment schedule (<code>calendrier_reglements_2026.xlsx</code>)	1	high
Bank-details change letters (scans)	3	medium
Supplier invoices (scans)	17	medium
Purchase ledgers 2023, 2024 and 2025	3	medium
Finance team contact sheet	1	medium
Engagement letter, amendment, VAT returns, miscellaneous letters	12	low

The workflow. The amendment of 18 December 2025 to the engagement letter describes the procedure. Payments go out on the 5th and the 20th of each month. The accounts payable accountant prepares them, the accounting and treasury manager approves them, the Chief Administrative and Financial Officer countersigns above €20,000. A change of bank details is accepted on a letter signed by the supplier, scanned and sent to the firm, which updates the register. No call-back to the supplier on a known number is provided for before this update.

Analysis (scenarios 3 and 4, medium severity). The invoices carry real numbers, amounts and due dates: **SM-2026-01877** (Soylent Matériaux, 14 January 2026), **F0-2026-03317** (Fabrikam Outillage), **WTS-26-0315** (Wonka Traitements de Surface). A reminder about one of them, addressed to the accounts payable accountant, is credible (scenario 3). The three bank-details change letters provide a complete template: letterhead, wording, signatory. With the register and the schedule of the 5th and 20th, a fake letter arrives at the right time and to the right person (scenario 4). These scenarios remain of medium severity: they require a careful forgery and the right timing, but the workflow described has no step that would stop them.

Severity: high. Two accesses are within reach (points a and b): the billing key, which depends only on its validity, and the VPN, which depends on a second factor we cannot see. Both can be closed in under 24 hours.

3.6 Entry points for a physical approach

Source: Initech Freight manifests (source F), folder **initech/Ops/Manifests**, host **ynm3mex5...onion**, published on **21 May 2026**, 6 documents; invoices and contact sheet of the accounting firm (source C).

Manifest	Folder	Content
MAN-55700 , -55709 , -55718 , -55727	2026-04	consignee AC-0092 , 7Q-4410-114 ; 40, 60, 80 then 100 parts
MAN-55794	2026-05	5 parts for a new first article inspection, presumably after the rework of NCR-2026-031 ; "export-controlled, keep paperwork with the crate"
MAN-55810	2026-05	shipper Globex Machining Plant 2, consignee AC-0092 (final assembly line), 2 crates, 240 brackets and 120 fittings, declared value €71,400

Analysis. Whoever prepares a physical approach knows, before setting foot on the site: when the crates leave (week 18, dock B of "Plant 2"), what they contain and are worth, that the accompanying paperwork is authoritative, and at which line they arrive. The firm adds the Lavaur switchboard (**+33 5 36 49 02 00**), goods reception (**+33 5 36 49 02 31**) and security: invoice **VS-2026-0311** from Vandelay Sécurité (28 February 2026) describes two night guards, seven nights a week, and one daytime guard at weekends. No site plan, access code, badge list or visitor instruction is exposed. Castres and Ath expose nothing physical: only their workstations and, for Ath, a gateway.

Point to note: the manifest is the paper a fake carrier would try to imitate in order to collect a batch, and six real copies are published.

Severity: medium, through logistics. Nothing gives access to the site: what is exposed is the timing, place, contents and paperwork of a transfer of export-controlled parts.

3.7 What an adversary deduces by cross-referencing with public information

None of the elements above is decisive in isolation. Combined, and cross-referenced with what can be published about ACME (website, job postings, professional profiles), they make up five scenarios, from most to least severe.

#	Scenario	Severity	What is gathered
1	Log in to ACME's VPN as the accounts payable accountant	High	3 evidence items out of 4: credentials (A), gateway (D), finance names (C). Missing: second-factor enrolment

#	Scenario	Severity	What is gathered
2	Call the billing API with the pasted key	High	a single publication (B): the key and the database password, pasted on 27 September 2026. Rotating both closes the scenario
3	Phish the finance team with real invoice numbers	Medium	invoices, contacts, schedule (C)
4	Divert a payment with a fake bank-details change letter	Medium	register, template letters, approval workflow (C)
5	Map ACME's network from a forum	Low	inventory and naming conventions (D)

First line of reasoning: the key, the door and the person come from three places. The infostealer logs give the key, the forum the door (the gateway, its address, its two names), the accounting firm the person (name, role, direct line, place in the approval workflow). Three origins with no link between them, and none shows the scenario alone. Public information has almost nothing to add: a job posting is enough to confirm that an accounts payable accountant position exists at Lavaur.

Second line of reasoning: ACME's value is also at its suppliers. The Globex Machining share proves that an inspection file for your part **7Q-4410-114** is circulating, without your name appearing in it. The link is made effortlessly by anyone who knows your references: the accounting firm lists Globex among your machine shops, and Globex's public website boasts of its titanium machining capabilities and its aerospace customers. The 29 May announcement shows that your parts served as a selling point. The reasoning is immediate: reading a subcontractor's file costs less than targeting its principal, and it is less well guarded.

Third line of reasoning: the vocabulary is available. Invoices, amounts and due dates give the content of a fake email, the bank-details change letters the template, the schedule the timing, the approval workflow the names and the €20,000 threshold. On the quality side, **P0-2026-0412**, **NCR-2026-031**, heat lot **H-22871** and clause **QC-7** make a fake "concession granted" email to your purchasing or quality department credible.

Important caveat. Nothing says that any of these scenarios is being played out: we tested no access and cannot see inside ACME. We observe that the pieces needed for each are online, some for more than three years (the gateway), others for four days (the secrets). The response addresses first what expires (secrets, passwords, sessions), then the workflows (who approves what, with which call-back), and finally what your suppliers hold about you.

4. The seven sources, dated

#	Source	Indexing date	Documents	What it exposes about ACME
A	infostealer logs, x4hq7p2d...onion	14 August 2026	43	14 employee workstations, credentials including an accounting VPN login, SSH hosts
B	text-pasting service, dmp5cnzx...onion	21 to 29 September 2026	6	billing key, database password , deployment script, test servers
C	Contoso Expertise Comptable, h6wk3zr5...onion	25 March 2026	38	invoices, bank details of 14 suppliers, payment schedule, finance team
D	Russian-language forum, f2tn5vby...onion	12 May 2023	32	VPN gateway, host names, naming conventions
E	Globex Machining, ransomware group, mojzk4yj...onion	2 June 2026	14	first article inspection, order, non-conformity, drawing index, load plan
F	Initech Freight, ynm3mex5...onion	21 May 2026	6	shipments to AC-0092 : contents, pace, value
G	sale announcement, dmp5cnzx...onion	29 May 2026	1	7Q-4410-114 and 7Q-4410-116 cited in the Globex share offer

Sources A to D are those of the OwlyScan dashboard: 119 documents, 12 of them of high criticality (8 for A, 2 for B, 2 for C). Sources E to G come from a search widened to your suppliers and are not counted in these 119; their count is that of the documents citing `7Q-4410-114`. An eighth corpus, the list of registrants at a trade show, mentions ACME as an exhibitor. Not relevant.

Method point to remember. Sources A and B are not attacks against ACME: they are proximity leaks, an employee workstation and an operating habit. Sources C, E and F are three distinct ransomware victims, published on three sites within ten weeks (24 March, 21 May, 2 June 2026): the accounting firm, the freight forwarder, the machine shop. None has ACME as its target, and each nonetheless delivers a piece of ACME.

5. Appendix: inventory of addresses found

@acme-aero.example

adminsyst, anne-laure.pons, arnaud.barbier, charlotte.morel, claire.bessiere, david.rouquette, didier.salles, etienne.brossard, facturation.clients, gaetan.pinel, gilles.peyrac, helene.cazals, isabelle.delmas, karim.benaissa, laurent.roussel, lucie.arnal, marianne.chauvet, mathilde.sabatier, nathalie.vasseur, olivier.marty, pascal.fabre, qualite, romain.duplessis, sandrine.cros, service.achats, sylvie.lemaitre, thierry.lacombe, yann.combes

@acme-aerostructures.example

comptabilite, nathalie.vasseur, qualite, reception, secretariat, sylvie.lemaitre

@acme-aero-be.example

aurelie.hanot, bernard.lambotte, comptabilite, expéditions, maxime.pirotte, nathalie.collard, quentin.wauters, sabine.dewaele

That makes 42 distinct addresses, 14 of them present in the infostealer logs (source A).

6. Next steps

This statement is delivered to you alone. It contains no password or key value: secrets are masked in it.

Today. Renew the key `acme_bill_...` and the `billing_prod` password, then review the access logs since 27 September 2026. Reset the password of `slemaitre`, revoke its sessions, require a second factor on the VPN gateway, treat in the same way the accounts in the 8 high-criticality files, and reinstall the 14 infected workstations.

This week. Ask Globex Machining, Initech Freight and Contoso Expertise Comptable for the list of ACME documents contained in their leak. Require a call-back to the supplier on a known number before any change of bank details. Have your export compliance officer review the `9E991` and `EAR99` classes.

Three questions remain open, and only you can answer them:

- Does the `slemaitre` account require a second factor, and is `acces.acme-aerostructures.example` still in service?
- Is the address `198.51.100.23` reachable from the Internet?
- Is `AC-0092` indeed your customer code at Globex Machining?