CYBER RESILIENCE INTELLIGENCE REPORT

CALDERWICK INDUSTRIES

WHO IS TARGETING YOU, HOW THEY GET IN, AND WHAT TO FIX FIRST.

An adversary-led threat assessment of the groups working US manufacturing, read against an external review of what Calderwick shows the internet. One question runs through both: which adversaries would come for this company, how they would arrive, and what stands in the way.

PREPARED FOR	PREPARED BY	DATE	CLASSIFICATION
Calderwick Industries	Alchemy Security	September 2026	Public sample

IN THIS REPORT

01 EXECUTIVE OVERVIEW 02
02 THE ADVERSARY PICTURE 05
03 EXTERNAL ATTACK SURFACE 06
04 PRIORITY ACTIONS 09
05 NEXT STEPS 10
06 METHODOLOGY 10

01 EXECUTIVE OVERVIEW

Most security budgets are set against a framework, which addresses what could happen. An adversary-led assessment starts from what is happening. Somewhere in the world a group publishes a new victim about once an hour, every hour of the day. Seven of the seventy-eight groups Alchemy tracks are documented working manufacturing this year, and the pages that follow are about those seven and the doors they use.

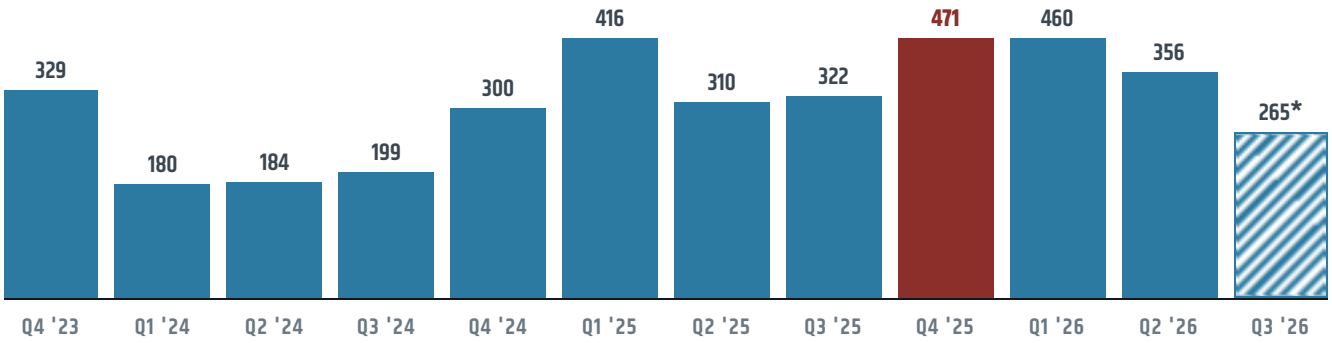
Calderwick makes parts other operations cannot run without: the precision bearings and couplings inside the pumps and rotating equipment of power stations, refineries, and water plants. Two things make it a target, and they pull in different directions: what it knows, and what it must keep shipping.

AT A GLANCE

7	1,675	159	4	8
ATTACK GROUPS NAMED	US MANUFACTURERS PUBLISHED	IN THE LAST 90 DAYS	LIKELY ATTACK PATHS	PRIORITY ACTIONS

MANUFACTURERS PUBLISHED BY QUARTER, WORLDWIDE

3,792 SINCE Q4 2023 · PEAK 471



From Athanor. Manufacturers published on adversary leak sites. * Quarter in progress.

ALCHEMY ASSESSMENT

DOUBLE-EXTORTION RANSOMWARE IS THE PRIMARY NEAR-TERM THREAT. THE LEVER IS THE OPERATIONAL HALT, NOT THE STOLEN FILES.

A manufacturer that stops making things loses money every day the line is down. That cost is visible, compounding, and easy for an extortionist to calculate. Manufacturing is the most heavily worked sector in the evidence: 1,608 US firms published since late 2023, and 159 in the last ninety days alone.

WHAT HAPPENED AT PEERS

THE CONSEQUENCES ARE DOCUMENTED, NOT HYPOTHESIZED

WEST PHARMACEUTICAL SERVICES

MAY 2026 · DISCLOSED TO INVESTORS · CONTRACT MANUFACTURER

Reported a cybersecurity incident under Item 1.05, the disclosure item reserved for material incidents, and amended the filing as its assessment developed.

WHAT IT SHOWS

Disclosure turns an IT event into a market event, on the company's timetable rather than the adversary's.

SIGMA PLASTICS GROUP

AUGUST 2026 · PUBLISHED BY PLAY · PRIVATE MANUFACTURER

Play published one of the largest privately held plastic film manufacturers in the US. Its documented route in is compromised VPN credentials and unpatched perimeter infrastructure.

WHAT IT SHOWS

Private ownership removes the disclosure obligation, not the adversary.

CLUTCH INDUSTRIES

JANUARY 2025 · PUBLISHED BY LYNX · ENGINEERING MATERIAL NAMED

Lynx took roughly 350 GB from an Australian clutch manufacturer and named employee, purchasing, engineering, and financial records among the material.

WHAT IT SHOWS

Engineering material is now advertised as worth stealing. Treat design repositories as a target.

KEYTRONIC

MAY 2024 · PUBLISHED BY BLACK BASTA · CONTRACT ELECTRONICS

Disclosed a two-week production stoppage to the SEC after a ransomware intrusion.

WHAT IT SHOWS

The number that follows the company is the downtime, not the ransom.

1.1 ADVERSARY-LED DEFENSE

Adversary-Led Defense starts from the adversaries the evidence shows, follows them to the vectors they use, and tests those vectors against what the company exposes. Coverage is measured against that named set, which keeps the work short enough to finish and specific enough to verify.

01 · EVIDENCE	02 · ADVERSARIES	03 · VECTORS	04 · SURFACE	05 · CONTROLS	06 · MEASURE
1,675 SECTOR PUBLICATIONS	7 GROUPS NAMED	4 LIKELY ROUTES	WHAT THE FIRM SHOWS	8 PRIORITY ACTIONS	COVERAGE, NOT OPINION

THE OPERATING LOOP · EVERY CONTROL TRACES BACK TO A NAMED ADVERSARY

The single highest-return item is coverage: a second factor on every remote-access path, because one VPN account without it is the opening move in the highest-likelihood scenario.

02 THE ADVERSARY PICTURE

Seven groups are named on observed activity against US manufacturing specifically, and all are financially motivated. Counts are US publications since January 2025. No state-aligned actor is named, because espionage succeeds by going unreported. The seven resolve into four paths, ranked by likelihood.

IMPACT	LIKELIHOOD	ADVERSARIES · RECENT VICTIMS	PATH
THE LINE STOPPED A remote-access login becomes the virtualization platform encrypted and the backups destroyed in the same event.	●●●●● HIGHEST	**AKIRA** 199 Albers Mechanical (Aug '26) · Plumley Engineering (Jul '26) **QILIN** 159 AUM Construction (Aug '26) · Teikoku USA (Aug '26)	**A remote-access login without a second factor** Virtualization and backups encrypted; the plant stops.
THE EDGE EXPLOITED An internet-facing gateway exploited before a patch lands, then data taken first and systems locked second.	●●●●○ HIGH	**PLAY** 145 · **DRAGONFORCE** 64 **INC RANSOM** 38 · **THE GENTLEMEN** 27 KRC Machine Tool · Sigma Plastics · RUS Industrial · Kewaunee Scientific	**An unpatched perimeter service** Exploited in a broad campaign, not a targeted siege.
THE DESIGNS COPIED Bearing geometries and process knowledge copied out quietly, surfacing years later in a competitor's catalog.	●●●○○ MODERATE Highest consequence	**QILIN · INC RANSOM · THE GENTLEMEN** Teikoku USA · Trulite Glass & Aluminum · ESCON Group	**The engineering and formulation store** Copied out quietly; nothing is encrypted.
THE SUPPLIER BREACHED Reached through a supplier's software, with the notification decision made on someone else's timetable.	●●●○○ MODERATE TO HIGH	**CLOP** 39 Named on method: one flaw, many firms at once	**A file-transfer product the company does not operate** Drawings and shipping data taken at the vendor.

AKIRA

A joint CISA advisory records its primary access as remote access without MFA, the control this assessment returns to most often.

QILIN

Works VPN and RDP on bought or stolen credentials, then encrypts the hypervisor to stop many systems at once.

PLAY

Favors compromised VPN credentials and unpatched perimeter gear, with documented Fortinet and Exchange exploitation.

CLOP

Exploits one widely used file-transfer product and works every victim as a batch, repeated across four platforms since 2020.

03 EXTERNAL ATTACK SURFACE

A HACKER'S VANTAGE POINT · NO LOGINS, AGENTS, OR ACCESS REQUIRED

The review enumerated 109 names from certificate transparency, passive DNS, and internet-scan data, the way an adversary sizes up a target. 54 resolved to 43 addresses. Each was tested across service ports: twenty-three hosts answered, two answered as a provider's content-delivery edge, eighteen stayed silent, and a reverse-DNS sweep recovered one more host no name had surfaced.

109	43	23	2 / 25
NAMES ENUMERATED	ADDRESSES	HOSTS ANSWERED	CRITICAL / HIGH VULNS

STRENGTHS

- SPF, DKIM, and DMARC are all published, so enforcement is a policy change.
- Part of the public web estate sits behind Cloudflare.
- No company address was seen sending scan traffic.
- No Calderwick listing appears on any tracked leak site.

AREAS OF CONCERN

- 2 critical and 25 high vulnerabilities on exposed builds.
- MySQL and PostgreSQL answer the open internet on a shared host.
- A dangling DNS record points at a claimable Azure service.
- Four mail hosts answer on plaintext POP3 and IMAP.
- IIS on Windows Server 2012 R2, past end of support, on three hosts.
- DMARC is set to quarantine rather than reject.

3.1 EMAIL AUTHENTICATION

SPF	DKIM	DMARC	POLICY
● PRESENT	● PRESENT	● PRESENT	■ QUARANTINE

Quarantine sorts failing mail into spam rather than refusing it, so a forgery in the company's name still reaches the recipient, one folder away. Move to reject once legitimate senders are aligned. Lookalike domains and taken-over mailboxes sit outside DMARC; monitoring and identity controls answer those.

3.2 THE ESTATE, HOST BY HOST

Ordered by what each system's presence would cost, not by name. Excerpt: two of fourteen entries.

SYSTEM	WHAT IT IS	STATE	WHY IT MATTERS

`7b3e.calderwick.example`
`blog.calderwick.example`
21 22 25 53 80 110 143 443 465 587 993 995 2083 2086 2087 2095 2096 2222 3306 5432
Shared cPanel host · 198.18.29.113
	Twenty ports open, including MySQL and PostgreSQL on the open internet, cPanel and WHM consoles, webmail, FTP, and two SSH services. 36 version-inferred vulnerabilities.	REACHABLE
		Both answered
			The most serious exposure on the estate. A database answering the internet invites attack on it and everything behind it. Take the database ports and control panels off the internet first.

`mail.calderwick.example`
`regulatory · cwk · serviceawards`
21 22 26 80 110 143 465 544 587 993 995 40005
One estate · 198.18.89.46
	Self-operated mail stacks on plaintext POP3 and IMAP alongside FTP, SSH, and SMTP submission. One host serves a sign-in prompt over unencrypted HTTP.	REACHABLE
		All four answered
			Where Qilin and Akira get credentials. Plaintext protocols carry passwords reusable against the Microsoft tenant; FTP and SSH turn one into a foothold.

Host-level detail for every name and port: companion External Attack Surface report, 24 September 2026.

3.3 COVERAGE ACROSS THE FIVE ATTACK VECTORS

Nearly every intrusion enters through software vulnerabilities, patching practice, social engineering, misconfiguration, or credential failure. Three of the five resolve to identity, and for this company the credential vector is sharpest.

MANAGED

ATTACK SURFACE DISCOVERY & MANAGEMENT

A continuous inventory surfaces drift first: the unsupported web server, the takeover candidate, the inherited estate.

MANAGED

VULNERABILITY & EXPOSURE MANAGEMENT

Prioritized by whether the named actors exploit a flaw, not by score alone. The direct answer to Play.

ASSESSMENT

CYBER RESILIENCE ASSESSMENT FOR MICROSOFT CLOUD

Mail, files, and identity in one tenant: a concentrated target where a stolen credential does the most work.

MANAGED

IDENTITY INTELLIGENCE ANALYTICS

Anomalous authentication, unusual access to engineering material, and privilege change made visible.

PROGRAM

DETECTION MAPPED TO ADVERSARY ATTACK PATTERNS

Built against the MITRE ATT&CK techniques these actors use, and measured against this actor set.

3.4 DETECTION REQUIREMENTS FOR THESE ADVERSARIES

DETECTION REQUIREMENT	WHAT IT WOULD CATCH	ADVERSARIES
Remote-access authentication and sessions	Valid-account entry through VPN and RDP without a second factor	AKIRA · QILIN · PLAY
Virtualization access and bulk encryption	The hypervisor encrypted to stop many systems at once	QILIN · AKIRA
Backup deletion or encryption	Recovery copies removed in the same event as the servers	AKIRA · QILIN · PLAY
Exploitation of public-facing applications	Perimeter gateway and file-transfer compromise	PLAY · CLOP · AKIRA
Defensive-tooling interference	Endpoint protection disabled before the noisy work begins	AKIRA · QILIN · PLAY
Documents leaving over web services	Engineering and commercial data copied out ahead of encryption	CLOP · QILIN · AKIRA · PLAY

04 PRIORITY ACTIONS

Ordered by the paths they close, not by cost or convenience. Each stands on its own.

1 **PUT A SECOND FACTOR ON EVERY REMOTE-ACCESS PATH** BUDGET — AKIRA · QILIN · PLAY

Closes the highest-likelihood path in full. Start with the paths engineers and maintenance partners use.

2 **PUT THE BACKUPS BEYOND THE INTRUDER'S REACH** PROJECT — AKIRA · QILIN · PLAY

One copy that production cannot delete, separate credentials, and a restore measured in hours.

3 **CLOSE THE EXPOSED EDGE ON A SET SCHEDULE** NO COST — PLAY · CLOP · AKIRA

Agree a maximum patch window. Retire the Windows Server 2012 R2 hosts before 13 October 2026.

4 **REMOVE THE LIVE TAKEOVER CANDIDATE** PROJECT — ALL GROUPS

Delete the dangling Azure record and reconcile every inherited name against the asset register.

ACTIONS 5–8 CONTINUE: SEGMENTATION · DESIGN-DATA ACCESS · SUPPLIER PLATFORMS · DMARC TO REJECT

05 NEXT STEPS

This report summarizes two assessments delivered separately: the Adversary-Led Threat Assessment and the External Attack Surface Assessment. Those carry the actor profiles, technique mapping, host inventory, and the remediation behind each finding.

WALK THROUGH THE FINDINGS WITH US

A working session on the findings and actions above. The findings are freshest now and describe your posture as it stands today.

SCHEDULE THE DEBRIEF

06 METHODOLOGY

THE INTELLIGENCE BEHIND EVERY REPORT · FROM ATHANOR

32,243 PUBLISHED BREACHES TRACKED	**420** THREAT ACTORS TRACKED	**155** ATT&CK TECHNIQUES MAPPED	**342** LEAK SITES MONITORED
78 FULL ATT&CK DOSSIERS	**737** TECHNIQUE PROCEDURES	**162** INDUSTRIES PROFILED	**196** COUNTRIES

Actors are selected on observed activity against US manufacturing, not general prominence. Sector figures come from Athanor, Alchemy's adversary intelligence platform: the sector total and quarterly chart cover late 2023 onward, per-actor counts cover 1 January 2025 onward, and the ninety-day figure runs from 9 June 2026. The external review enumerated names from certificate transparency, passive DNS, and internet-scan data, then tested every host from an unrestricted vantage.

TO LEARN MORE

AKIRA	Joint Advisory AA24-109A: Akira Ransomware · CISA / FBI / EC3 / NCSC-NL
QILIN	Qilin Ransomware · Trend Micro Research
PLAY	Joint Advisory AA23-352A: #StopRansomware: Play Ransomware · CISA / FBI / ASD ACSC
CLOP	Joint Advisory AA23-158A: CL0P exploits CVE-2023-34362 MOVEit · CISA / FBI