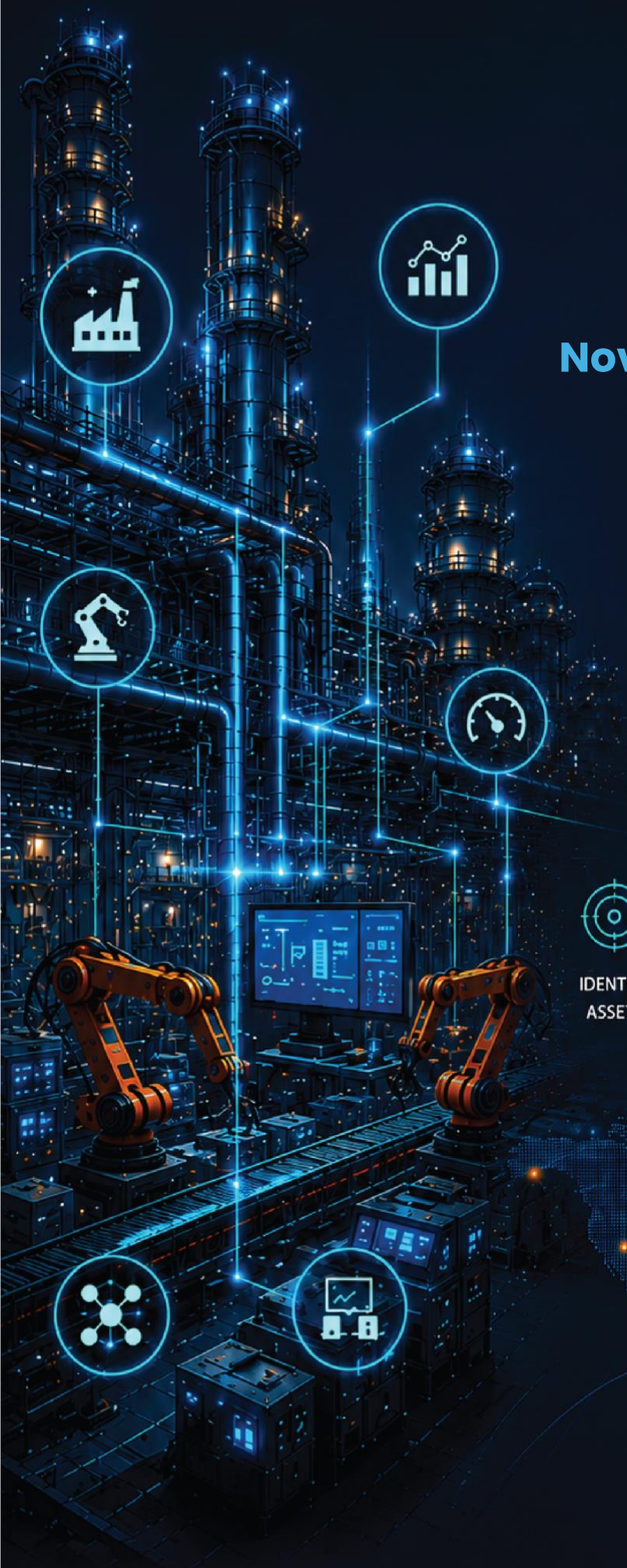
SHIELDWORKZ

Novo Nordisk Cyber Incident

Data-Theft Extortion, Clinical Trial and AI Asset Exposure



This page has been intentionally left blank

Table of Contents

1. Executive Summary

1.1 Overview

On 11 June 2026, Danish pharmaceutical company Novo Nordisk A/S publicly disclosed an IT security incident involving unauthorized access to a limited number of internal IT systems, resulting in the external, unauthorized copying of non-public data, including personal data associated with certain clinical trial participants and healthcare professionals (HCPs). [CONFIRMED — Novo Nordisk]

Within days of the disclosure, a cyber-extortion group calling itself FulcrumSec claimed responsibility on its dark web leak site, asserting it had exfiltrated approximately 1.3 terabytes of data across more than 700,000 files, including clinical trial records, source code repositories, proprietary drug compound data, and internal artificial intelligence (AI) and machine learning (ML) model assets used in drug discovery. FulcrumSec claims it demanded a US$25 million ransom, which Novo Nordisk did not pay, after which the group began publishing samples of the stolen data on 15–16 June 2026. A second, less-established actor, self-identified as "TheUSERS007," separately claimed a distinct intrusion and demanded a US$50 million ransom; this second claim has not been corroborated or confirmed by Novo Nordisk. [CLAIMED — threat actor(s)]

Novo Nordisk has confirmed that pseudonymized clinical trial data (patient ID, sex, year of birth, biomarker/health/immunogenicity data, and lifestyle factors such as BMI and smoking status) and identifiable contact information for certain healthcare professionals (names, registration numbers, email addresses, phone numbers, WhatsApp details, and office locations) were copied without authorization. The company states this data cannot be used on its own to identify individual patients by name. Novo Nordisk has explicitly stated that its core business operations, including manufacturing and distribution, were not impacted and remained fully operational throughout the incident. [CONFIRMED — Novo Nordisk]

1.2 Incident Severity

SEVERITY ASSESSMENT: HIGH (DATA CONFIDENTIALITY) — LOW-TO-NONE (OPERATIONAL/OT)

Confidentiality impact: HIGH. Confirmed exposure of clinical trial participant data and HCP contact data; threat-actor claims of substantially broader exposure (source code, drug compound data, AI/ML models) remain unverified but, if accurate, would represent a severe intellectual property loss.

Integrity impact: UNCONFIRMED. No public evidence of unauthorized data modification; however, independent security commentators have noted that any system accessed for exfiltration should also be evaluated for potential tampering.

Availability impact: LOW. No file encryption or destructive activity has been confirmed or claimed by any party. Novo Nordisk proactively took a limited number of systems offline as a precaution, and stated core operations continued without disruption.

This is assessed as a data-theft extortion event, not a ransomware-encryption event, and — based on all currently available public evidence — not an OT/ICS or manufacturing-control-system security incident.

1.3 Business Impact

The confirmed business impact centers on data confidentiality and the associated regulatory, notification, and reputational obligations rather than operational disruption. Novo Nordisk has stated it is in contact with relevant authorities (implicating GDPR notification obligations to the Danish Data Protection Agency, Datatilsynet, given the company's Danish domicile) and has begun direct notification to affected clinical trial participants and healthcare professionals. If the threat actor's claims regarding source code, proprietary compound data, and AI model theft are substantiated, the strategic and competitive impact could extend well beyond the currently confirmed personal-data exposure, given Novo Nordisk's position as one of the world's largest developers of GLP-1 and insulin therapies.

1.4 Strategic Implications

- The incident is a data-theft extortion attack, part of a broader 2026 trend in which cyber-extortion groups increasingly bypass encryption entirely and monetize stolen data directly — a model that reduces attacker operational complexity while retaining strong leverage over victims.
- The threat actor's claimed initial access vector — credentials and access tokens embedded in client-side JavaScript on public-facing development/staging subdomains — if accurate, illustrates a class of exposure that traditional code-scanning and secret-scanning tooling (which typically inspects source repositories, not deployed client-side assets) frequently does not cover.
- The incident illustrates an emerging targeting pattern in which AI/ML training data, model weights, and drug-discovery pipelines are treated by threat actors as high-value intellectual property comparable to — or exceeding — traditional clinical and compound data.
- No evidence currently links this incident to any compromise of Novo Nordisk's manufacturing or OT/ICS environments; the company's explicit, repeated statement that core business operations were unaffected is corroborated across all reviewed independent reporting.

1.5 Key Takeaways for Executives

#	Takeaway
1	This was a confirmed data confidentiality breach with confirmed clinical trial and HCP data exposure — not a confirmed ransomware/encryption or OT/ICS incident.
2	The threat actor's claimed scope (source code, compound data, AI models) is significantly broader than what Novo Nordisk has confirmed; boards should expect the confirmed scope to evolve as forensic investigation continues.
3	The claimed initial access vector — secrets exposed via client-side JavaScript on forgotten or under-reviewed subdomains — is a blind spot for many organizations' existing secret-scanning and attack-surface-management programs.

#	Takeaway
4	Data-theft extortion (no encryption) is increasingly the dominant model among financially motivated groups in 2026; recovery planning built solely around ransomware/encryption scenarios is incomplete.
5	Organizations building AI/ML capability into R&D or manufacturing pipelines should treat model weights, training data, and pipeline infrastructure as crown-jewel assets requiring the same protection rigor as production and clinical systems.

2. Company Overview

2.1 About Novo Nordisk

Novo Nordisk A/S is a Danish multinational pharmaceutical company headquartered in Bagsværd, Denmark, founded in 1923. The company describes its purpose as driving change to defeat serious chronic diseases, built on its heritage in diabetes care. Novo Nordisk employs approximately 67,900 people across 80 countries and markets its products in approximately 170 countries. [CONFIRMED — Novo Nordisk corporate disclosure, June 2026]

The company is best known globally for its GLP-1 receptor agonist therapies — semaglutide, marketed as Ozempic (type 2 diabetes) and Wegovy (chronic weight management) — as well as its long-standing global leadership position in insulin production for diabetes care. Novo Nordisk's product portfolio also spans treatments for hemophilia and other rare chronic and blood disorders. [CONFIRMED — public company disclosures]

2.2 Global Operations and Manufacturing Footprint

Novo Nordisk operates a globally distributed manufacturing and R&D footprint anchored by significant production capacity in Denmark. Its Kalundborg, Denmark facility — established in 1969 — is described by the company as the world's largest insulin manufacturing site and covers approximately 1.6 million square meters with around 4,400 employees, producing active pharmaceutical ingredients (API) and finished biopharmaceutical products for diabetes and obesity care. Novo Nordisk has announced tens of billions of Danish kroner in additional manufacturing investment in Denmark (including Kalundborg and a new multi-product facility in Hillerød) to expand capacity for GLP-1 and related therapies. [CONFIRMED — Novo Nordisk corporate disclosures]

Beyond Denmark, Novo Nordisk operates additional manufacturing, R&D, and commercial sites internationally as part of its global supply chain for insulin, GLP-1 therapies, and other biopharmaceutical products, reflecting the scale required to serve patients in around 170 countries. This report does not enumerate the company's complete global site list, as a comprehensive, current inventory was not required to assess this incident and is not material to the confirmed facts of the breach.

2.3 Business Segments and Critical Digital Assets

Category	Description	Relevance to This Incident
Clinical R&D / Trials Infrastructure	Systems supporting clinical trial data collection, management, and analysis across Novo Nordisk's global trial portfolio	Confirmed source of exposed pseudonymized patient data
Corporate IT / Collaboration Systems	Internal IT systems, code repositories, cloud infrastructure (including Azure-hosted services)	Confirmed as the access point; claimed as the primary systems accessed by the threat actor

Category	Description	Relevance to This Incident
AI/ML Drug Discovery Infrastructure	Machine learning models, training datasets, and HPC/GPU infrastructure supporting computational drug discovery (Novo Nordisk has publicly discussed investment in AI-driven R&D, including support for a Danish national AI supercomputer initiative)	Claimed (not confirmed) as an exposed asset category; if substantiated, represents the most strategically significant claimed loss
Healthcare Provider (HCP) Relationship Systems	Systems holding contact and engagement records for healthcare professionals involved in clinical trials and commercial engagement	Confirmed source of exposed HCP contact data
Manufacturing / OT-ICS Environment	Industrial control and production systems at sites such as Kalundborg supporting insulin and GLP-1 manufacturing	No confirmed impact; explicitly stated by Novo Nordisk to be unaffected

2.4 Why operational resilience matters here

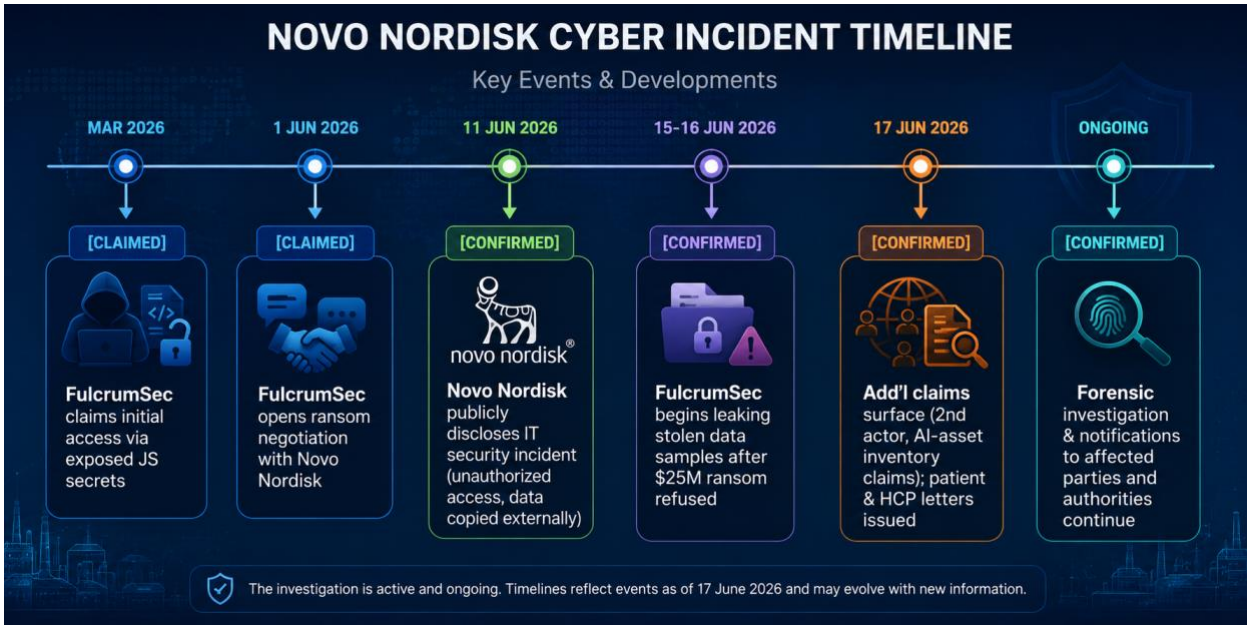
Novo Nordisk's products, including insulin and GLP-1 therapies, are life-sustaining and life-improving medicines used by millions of patients globally for chronic disease management. Any disruption to manufacturing or supply continuity carries direct patient-safety and public-health consequences, which is why Novo Nordisk's repeated, explicit statement that core business operations remained unaffected throughout this incident is a materially significant fact for this report — both as a confirmed positive outcome and as a benchmark against which the company's segmentation between IT and production environments can be assessed.

3. Incident overview

3.1 Summary

The following section summarizes the confirmed disclosure timeline based on Novo Nordisk's own statements and corroborating reputable press reporting. Threat-actor-claimed dates (e.g., claimed initial access date, claimed dwell time) are presented separately in Section 4 and Section 5 and are clearly marked as claims.

3.2 Visual Incident Timeline



3.3 Timeline of public disclosures

Date	Event	Source	Status
11 Jun 2026	Novo Nordisk publicly discloses an IT security incident involving unauthorized access to a limited number of internal IT systems; states certain non-public data, including personal data, was copied externally	Novo Nordisk press release; Reuters; BNN Bloomberg	CONFIRMED
12 Jun 2026	BleepingComputer and other outlets report additional detail from Novo Nordisk on affected clinical trial data categories and HCP data exposure	BleepingComputer	CONFIRMED

Date	Event	Source	Status
15 Jun 2026	FulcrumSec begins publishing sample data on its dark web leak site after alleged ransom negotiations fail	SecurityAffairs; BankInfoSecurity; Ransomnews	CONFIRMED (leak activity observed) / CLAIMED (attacker narrative)
16 Jun 2026	FulcrumSec publicly claims responsibility and publishes a claimed data inventory (1.3TB / 700,000+ files); SecurityWeek and other outlets report the claim	SecurityWeek; HIPAA Journal; BankInfoSecurity	CLAIMED — threat actor
On/around 16-18 Jun 2026	A second actor, "TheUSERS007," separately claims an earlier, distinct breach (claimed 5-7 Jun 2026) via databreaches.net; demands separate ransom	HIPAA Journal; FiercePharma (via databreaches.net)	CLAIMED — unconfirmed by Novo Nordisk
Late Jun 2026	Novo Nordisk issues direct notification letters to affected clinical trial participants and healthcare professionals; industry press (Industrial Cyber, others) reports on notification content	Novo Nordisk incident update page	CONFIRMED

3.4 Timeline of recovery activities

- Novo Nordisk stated it took a limited number of internal IT systems offline as a containment measure immediately upon discovery. [CONFIRMED]
- The company stated it is working to bring affected systems back online "in a controlled and safe manner," acknowledging that this process takes time. [CONFIRMED]
- Novo Nordisk engaged external cybersecurity forensics experts to lead the investigation; the identity of the specific incident response firm(s) engaged has not been publicly disclosed as of this report's publication. [CONFIRMED engagement / firm identity UNCONFIRMED]
- The company stated it is in contact with relevant authorities, consistent with GDPR breach notification obligations applicable to a Danish-headquartered data controller. [CONFIRMED]
- As of publication, Novo Nordisk had not disclosed a specific date for full restoration of all affected systems, nor a final, validated count of affected individuals. [UNCONFIRMED / ONGOING]

3.5 Present status

STATUS AS OF THIS REPORT'S PUBLICATION DATE (1 JULY 2026)

Novo Nordisk's forensic investigation and data review remain ongoing; the company has not published a final tally of affected individuals.

Core business operations, including manufacturing and distribution, remain confirmed as unaffected and fully operational.

FulcrumSec's leak site continues to reference the Novo Nordisk listing; the group has stated it is withholding a portion of the allegedly stolen data (including patient, employee, and claimed OT-related data) while reportedly seeking a private buyer for other portions.

The second claimed actor, TheUSERS007, and its claims remain unconfirmed by Novo Nordisk and are not corroborated by independent forensic reporting reviewed for this report.

4. What happened?

4.1 Initial compromise

Novo Nordisk has not publicly disclosed the technical initial access vector for this incident. [UNCONFIRMED by victim organization]

FulcrumSec has claimed, via statements to the cybersecurity/breach-notification outlet DataBreaches.net and via its own leak-site postings, that it gained initial access as early as March 2026 through secrets embedded in client-side JavaScript served on two separate, unrelated Novo Nordisk subdomains. According to the group's claims, this included an Azure container registry credential "baked into" a client-side JavaScript bundle, and a GitHub personal access token (PAT) with access to hundreds of private repositories. The group further claims these initial credentials allowed it to locate additional API tokens, database credentials, and service account passwords within accessed repositories, enabling lateral "spidering" through Novo Nordisk's environment. [CLAIMED — FulcrumSec, reported by SecurityWeek, BankInfoSecurity, SecurityAffairs, CybelAngel]

KEY FINDING — DISTINCT FROM STANDARD SECRET-SCANNING BLIND SPOTS

If FulcrumSec's account is accurate, the exposure mechanism was not a secret accidentally committed to a public source-code repository (the scenario most commonly covered by commit-time secret scanning and pre-commit hooks). Instead, the claimed exposure involved credentials embedded in JavaScript actually served to any visitor's browser from public-facing development or staging subdomains — a distinct and frequently under-monitored class of exposure.

4.2 Attack progression (as Claimed by the Threat Actor)

The following progression reflects FulcrumSec's own public claims and has not been independently verified through forensic evidence published by Novo Nordisk or a named third-party incident response firm. It is presented for threat-intelligence context, not as an established fact pattern.

Stage	Claimed Activity	Confirmation Status
1. Reconnaissance	Identification of public-facing development/staging subdomains not intended for production access	CLAIMED
2. Initial Access	Extraction of an Azure container registry credential and a GitHub PAT embedded in client-side JavaScript	CLAIMED
3. Credential Access / Discovery	Use of the GitHub PAT to access hundreds of private repositories; discovery of additional API tokens, database credentials, and service account passwords within repository contents	CLAIMED

Stage	Claimed Activity	Confirmation Status
4. Lateral Movement	"Spidering" through additional internal systems using harvested credentials, reportedly over a claimed ~2.5 month dwell time	CLAIMED
5. Collection	Access to a collaborative drug discovery database, clinical trial data, employee/HCP data, AI/ML model repositories, and HPC/infrastructure configuration data	CLAIMED
6. Exfiltration	Low-and-slow, continuous data exfiltration over an extended period, claimed to total approximately 1.3TB / 700,000+ files	CLAIMED
7. Extortion	Direct ransom negotiation with Novo Nordisk beginning around 1 June 2026, demanding US$25 million	CLAIMED (negotiation contact acknowledged indirectly by Novo Nordisk's awareness of leak claims, per statements to ISMG/BankInfoSecurity)
8. Leak / Monetization	Publication of data samples on the group's leak site beginning 15-16 June 2026 following non-payment; stated intent to seek a private buyer for remaining data	CONFIRMED (leak site activity observed by multiple independent outlets) / CLAIMED (buyer-seeking intent)

4.3 Systems and data affected

4.3.1 Confirmed

- A limited number of internal IT systems were accessed without authorization. [Novo Nordisk]
- Pseudonymized clinical trial participant data was copied externally, including patient ID, sex, year of birth, biomarker/health/immunogenicity data, and lifestyle factors (e.g., smoking status, alcohol use, BMI). [Novo Nordisk]
- Healthcare professional (HCP) data was exposed, including names, registration numbers, email addresses, phone numbers, WhatsApp details, and office locations. [Novo Nordisk, as reported by BleepingComputer, Industrial Cyber, HIPAA Journal]

4.3.2 Claimed (Not Confirmed by Novo Nordisk)

- Approximately 4,750 source code repositories.
- More than 41,000 proprietary drug compound structures/records.
- More than 30 trained AI/ML models, including a claimed 16.7GB multimodal (text/image/transcriptomic) model checkpoint.
- Approximately 407MB of proprietary biological/chemical training datasets and 73 additional datasets.

- Complete logs from 113 claimed model training runs, HPC infrastructure maps, Slurm scheduler configuration, and SSH configuration data.
- Approximately 53GB of internal container images, developer identity information, and private GitHub repository URLs.
- Data belonging to approximately 11,500 pseudonymized clinical trial patients (a specific figure cited by the threat actor; Novo Nordisk has not confirmed a specific affected-individual count).

Note: FulcrumSec has also claimed it is deliberately withholding certain categories of data from publication, including employee and physician data, pseudonymized clinical trial patient data, and — notably for this report's audience — data the group describes as related to "operational technology and software used to interact with sensors and equipment" at Novo Nordisk production facilities. This is a threat-actor claim only; it has not been confirmed by Novo Nordisk, and no independent evidence of OT/ICS system access has been published. It is included here for completeness and OT-risk awareness, not as a confirmed finding. [CLAIMED — FulcrumSec, reported by HIPAA Journal]

4.4 Geographic and business function impact

Dimension	Status	Detail
Geographic scope	PARTIALLY CONFIRMED	Novo Nordisk is a Danish-headquartered global company; affected clinical trial and HCP data likely spans multiple countries given the company's ~170-market commercial footprint and multinational trial operations, though a country-by-country breakdown has not been published.
Corporate IT	CONFIRMED IMPACTED	Unauthorized access to internal IT systems confirmed; certain systems taken offline as a precaution.
Manufacturing / Production	CONFIRMED NOT IMPACTED	Novo Nordisk explicitly and repeatedly stated core business operations, including manufacturing and distribution, were not impacted and remained operational.
OT/ICS Environment	NO CONFIRMED IMPACT	No independently verified evidence of OT/ICS access; a threat-actor claim references withheld OT-adjacent data but this is unconfirmed (see Section 4.3.2 and Section 10).
Cloud Services	PARTIALLY CONFIRMED	Threat actor claims center on Azure-hosted container registry credentials and cloud-adjacent infrastructure; Novo Nordisk has not specifically confirmed or denied which cloud platforms were implicated.
Third Parties	UNCONFIRMED	No public evidence to date that the incident originated from or spread through a third-party vendor or supplier network; the claimed vector is Novo Nordisk's own public-facing web infrastructure.

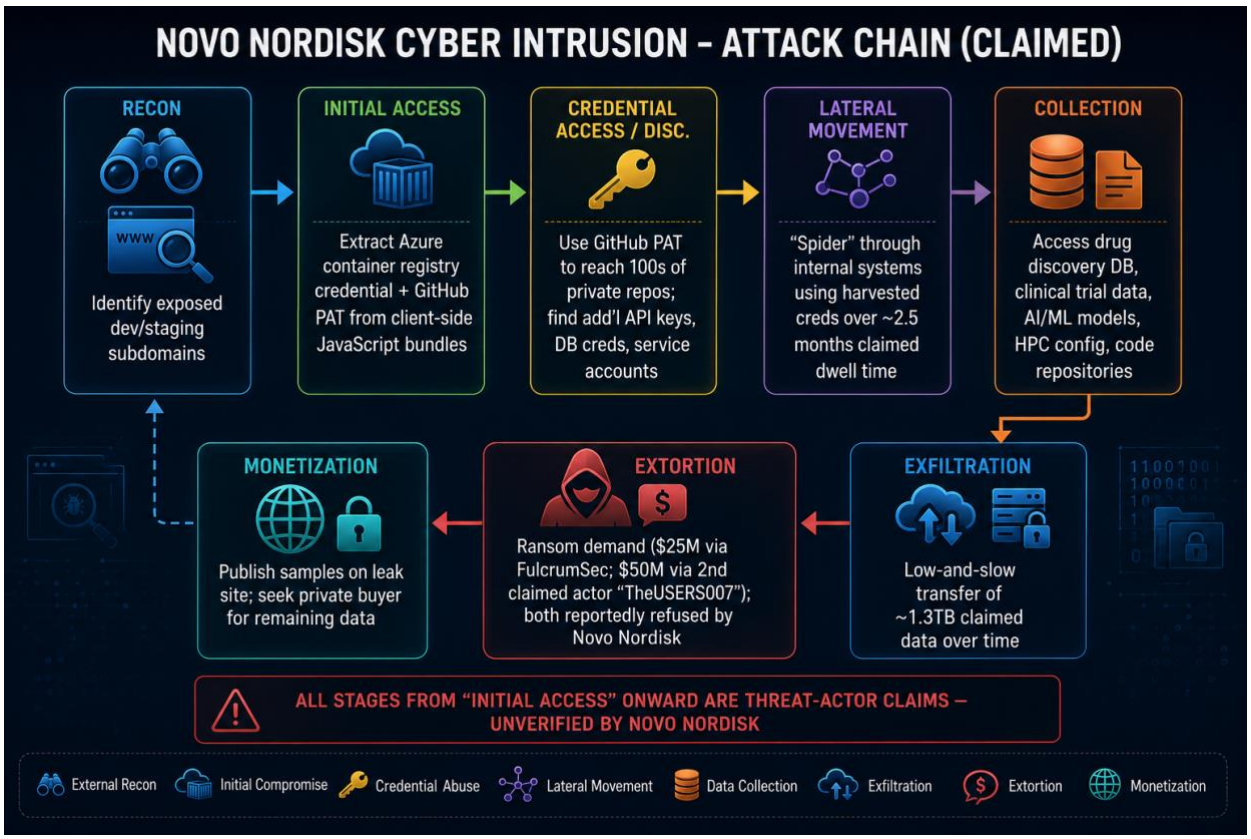
5. Technical analysis

Novo Nordisk has not published a technical forensic narrative of this incident. Everything in this section beyond Section 5.1 is derived from the threat actor's own public claims (via its leak site and statements to DataBreaches.net, as relayed by Shieldworkz, SecurityWeek, BankInfoSecurity, and SecurityAffairs) and must be read as unverified threat-actor reporting, not independently confirmed forensic fact. This section exists to give defenders a structured way to reason about the claimed technique set — not to assert that it is accurate.

5.1 Confirmed Technical Facts

- Unauthorized access occurred to a limited number of Novo Nordisk's internal IT systems. [CONFIRMED]
- Data was copied externally without authorization (i.e., exfiltration occurred in some form). [CONFIRMED]
- No file encryption, ransomware deployment, or destructive/wiper activity has been confirmed or even claimed by either threat actor. [CONFIRMED absence of encryption claims]
- Novo Nordisk took a limited number of systems offline as a precautionary containment measure. [CONFIRMED]

5.2 Claimed Attack Lifecycle



5.3 Technique summary table

Phase	Claimed / Confirmed Technique	Status
Initial Access	Harvesting of cloud (Azure container registry) and source-control (GitHub PAT) credentials embedded in publicly served client-side JavaScript	CLAIMED
Credential Access	Discovery of additional secrets (API tokens, DB credentials, service account passwords) inside accessed private repositories	CLAIMED
Discovery / Lateral Movement	Use of harvested credentials to enumerate and access additional internal systems and cloud resources over an extended dwell period	CLAIMED
Collection	Targeted access to clinical trial systems, drug-compound databases, source code, and AI/ML model and training infrastructure	CLAIMED
Exfiltration	Extended, low-volume/low-and-slow data transfer intended to evade detection thresholds; exact exfiltration channel not disclosed	CLAIMED

Phase	Claimed / Confirmed Technique	Status
Impact / Monetization	Data-theft extortion; no encryption; publication of samples on a dedicated leak site following non-payment	CONFIRMED (leak site activity) / CLAIMED (ransom amounts and negotiation detail)

5.4 MITRE ATT&CK Mapping (Based on Threat-Actor Claims — Not Forensically Confirmed)

MAPPING CAVEAT

The following mapping is provided strictly to support defensive planning and detection-engineering discussion. Because no independent forensic report has been published, this mapping should be treated as a hypothesis derived from the attacker's own narrative, not as a validated technique list. Analysts should not treat this table as equivalent to a vendor incident-response-confirmed ATT&CK mapping.

Tactic	Technique (ID)	Basis for Mapping
Reconnaissance	Search Victim-Owned Websites (T1594)	Claimed identification of exposed dev/staging subdomains
Credential Access	Unsecured Credentials: Credentials In Files (T1552.001)	Claimed extraction of Azure and GitHub credentials embedded in client-side JavaScript
Initial Access	Valid Accounts: Cloud Accounts (T1078.004)	Claimed use of the harvested Azure container registry credential to gain authenticated cloud access
Discovery	Cloud Service Discovery (T1526)	Claimed enumeration of cloud/container infrastructure following initial access
Credential Access / Discovery	Data from Information Repositories (T1213)	Claimed discovery of further API tokens and credentials within accessed GitHub repositories
Lateral Movement	Valid Accounts (T1078)	Claimed reuse of harvested credentials to move between internal systems
Collection	Data from Information Repositories (T1213); Data from Cloud Storage (T1530)	Claimed access to source code, compound databases, and AI/ML model repositories
Exfiltration	Exfiltration Over Web Service (T1567) [tentative]	Exfiltration mechanism not disclosed by the threat actor; this mapping is speculative and

		included only as the most common technique for this actor profile
Impact	Financial Theft (T1657)	Confirmed extortion attempt via ransom demand and leak-site publication

5.5 Recovery actions (Confirmed)

- Precautionary isolation of a limited number of internal IT systems.
- Engagement of external cybersecurity forensic experts (firm not publicly named).
- Phased, controlled restoration of affected systems.
- Direct notification to affected clinical trial participants and healthcare professionals.
- Ongoing engagement with relevant regulatory authorities consistent with GDPR obligations.

6. Threat actor analysis

6.1 Primary actor: FulcrumSec

ATTRIBUTION CONFIDENCE: MODERATE (SELF-CLAIMED, PARTIALLY CORROBORATED)

Attribution in this section reflects the actor's own public self-identification and leak-site activity, corroborated by multiple independent cybersecurity outlets observing the same leak-site listing and claims. It does not reflect law-enforcement attribution, victim-confirmed forensic linkage, or a named nation-state/criminal-group designation from a government agency.

Attribute	Assessment
Actor name	FulcrumSec (self-identified)
Type	Financially motivated cyber-extortion group
Observed operational model	Data-theft extortion without file encryption ("exfiltrate-and-extort"); publishes stolen data samples on a dedicated leak site to pressure non-paying victims
First observed activity	Reported by multiple outlets as active since approximately September 2025
Motivation	Financial gain via direct ransom payment and/or resale of stolen data to third-party buyers
Leak site	Dedicated Tor-based and clearnet-referenced leak site; group has publicly listed Novo Nordisk alongside other victim organizations
Confidence level	MODERATE — self-attribution corroborated by consistent, independent reporting of the same leak-site content across multiple reputable outlets; not confirmed via law enforcement or victim forensic disclosure

6.2 Secondary Claimed Actor: "TheUSERS007"

A separate individual or group self-identified as "TheUSERS007" claimed, via a submission to the breach-notification site DataBreaches.net, to have separately compromised Novo Nordisk between approximately 5-7 June 2026, asserting use of a self-described "self-learning AI-engine" tool referred to as "venomware," and demanding a US$50 million ransom. [CLAIMED]

ASSESSMENT: UNCORROBORATED CLAIM

This report treats the TheUSERS007 claim as unconfirmed. Novo Nordisk has not acknowledged a second, distinct intrusion, and no independent forensic or technical evidence has been published to substantiate the claimed "venomware" tooling or the claimed compromise timeline. It is included here for completeness because it appears in reputable secondary reporting (HIPAA Journal, FiercePharma via DataBreaches.net), but readers should not treat it as an established fact pattern

distinct from the FulcrumSec claims. It is possible, though unconfirmed, that this represents a second actor opportunistically claiming credit for aspects of the same underlying incident.

6.3 Industries and Geography Historically Targeted

Public reporting reviewed for this report did not identify a detailed, independently verified historical victim list or sector-targeting pattern for FulcrumSec beyond its general profile as a data-theft extortion group operating since approximately September 2025. Specific prior campaign details, additional named victims, and geographic targeting patterns have not been independently confirmed at the time of this report's publication and should be treated as an intelligence gap rather than inferred.

6.4 Attribution Summary

No government agency (e.g., CISA, NCSC, Europol) attribution statement regarding this incident had been publicly issued as of this report's publication date. This report makes no nation-state attribution and is aware of none being claimed by any party.

7. Indicators of Compromise (IOCs)

IMPORTANT NOTICE ON IOC QUALITY AND SOURCING

As of this report's publication, no forensic malware family, file hash, C2 (command-and-control) infrastructure, YARA rule, or Sigma rule associated with this incident has been published by Novo Nordisk, a named incident response firm, or a recognized threat-intelligence vendor (e.g., Mandiant, CrowdStrike, Microsoft, Recorded Future).

During research for this report, at least one secondary online source presented a purported technical IOC list containing a file hash that resolves to the SHA-256 value of an empty file (a well-known placeholder/test value, not a legitimate malware artifact). This is a strong indicator that the referenced list is fabricated, templated, or the product of unreliable automated content generation. That list has been deliberately excluded from this report and should not be relied upon by any organization for detection engineering purposes.

Because no malware payload (e.g., a ransomware encryptor) has been confirmed or claimed in this incident, the absence of a named malware family or binary hash is consistent with a credential-theft-and-data-exfiltration operation rather than a gap in reporting.

7.1 Threat actor infrastructure (Publicly Observable)

Indicator Type	Value / Description	Source	Confidence
Leak site (naming convention only — see note)	A dedicated leak site operated by the group self-identified as FulcrumSec, referenced across multiple cybersecurity news outlets covering the Novo Nordisk listing	SecurityAffairs; BankInfoSecurity; HIPAA Journal; Ransomnews	MODERATE — site existence and Novo Nordisk listing independently corroborated by multiple outlets; this report does not republish the live onion/clearnet address

This report deliberately does not reproduce the leak site's onion or clearnet address. Organizations with a legitimate operational need (e.g., for blocking, monitoring, or law-enforcement coordination) should obtain current, verified leak-site infrastructure indicators through a paid threat-intelligence provider or direct law-enforcement/CERT channel rather than an unvetted public report, given the rate at which such infrastructure changes and is spoofed or mirrored by unrelated parties.

7.2 Malware families

None publicly confirmed or named by any party at the time of publication. FulcrumSec's operational model, as reported, does not involve a file-encrypting payload; "venomware," referenced only by the uncorroborated second claimed actor (TheUSERS007), has not been

technically analyzed or confirmed by any independent source and is not listed here as a confirmed malware family.

7.3 File hashes

None have been published by a credible, named source as of this report's publication. (See the callout above regarding a fabricated hash observed in unreliable secondary reporting during research.)

7.4 Domains, IP addresses, and registry changes

No specific domains, IP addresses, or registry-key indicators tied to this incident have been published by Novo Nordisk or a named forensic firm as of this report's publication.

7.5 YARA / sigma rules

None have been published in connection with this incident as of this report's publication date. Given the credential-theft/exfiltration nature of the claimed attack, organizations may find general-purpose detection content more relevant than incident-specific signatures — see Section 11 for detection recommendations (e.g., anomalous GitHub PAT usage, anomalous Azure Container Registry pull activity, and outbound data-transfer volume anomalies).

8. Root Cause Analysis

Because Novo Nordisk has not published a root cause determination, this section separates the single technical claim made by the threat actor from broader analyst observations about the general risk pattern this incident illustrates, regardless of whether the actor's specific technical narrative is ultimately validated.

8.1 Claimed initial vulnerability

FulcrumSec's claim centers on cloud (Azure) and source-control (GitHub) credentials embedded directly in client-side JavaScript served from public-facing subdomains. If accurate, this would represent a secrets-management and secure development lifecycle gap rather than a classical software vulnerability (e.g., an unpatched CVE). [CLAIMED — not independently confirmed]

8.2 Analyst observations: Security gap patterns (General, Not Novo Nordisk-specific unless cited)

The following observations describe general risk patterns commonly associated with this class of claimed exposure across the industry. They are presented as analyst commentary for defensive planning purposes and are explicitly not asserted as confirmed findings about Novo Nordisk's specific environment or practices.

Risk Category	Analyst Observation
Secrets management	Credentials embedded in client-side, browser-delivered JavaScript are a well-documented but frequently under-addressed exposure class, distinct from — and often missed by — repository-focused secret scanning tools that inspect committed source code but not compiled/bundled client-side output actually served to end users.
Attack surface management	Development and staging subdomains that are internet-reachable but not intended for production use are commonly under-inventoried and under-monitored relative to primary production domains.
Least privilege / token scoping	A single GitHub personal access token reportedly providing access to "hundreds" of private repositories, if accurate, would indicate a token-scoping practice broader than the minimum necessary for its client-side use case.
Detection of long-dwell-time exfiltration	A claimed ~2.5 month dwell time with "low-and-slow" exfiltration is a well-known technique for evading volume- and rate-based data loss prevention (DLP) thresholds; this pattern is common across data-theft extortion incidents industry-wide, not specific to this case.
Third-party/software supply chain	No public evidence to date implicates a third-party vendor, managed service provider, or supply-chain compromise as the root cause of this specific incident.

8.3 Human and architectural factors

No Novo Nordisk-specific human-factor findings (such as phishing, social engineering, insider action) have been claimed by either threat actor or confirmed by Novo Nordisk in connection with this incident; the claimed vector is exclusively technical (exposed secrets in web assets). Any statement asserting a specific human-error root cause for this incident beyond what is stated here would exceed the currently available public evidence.

9. Business impact assessment

9.1 Financial impact

Novo Nordisk has not published a quantified financial impact estimate for this incident (e.g., incident response costs, regulatory fines, litigation reserves) as of this report's publication. The threat actor(s) have claimed ransom demands of US$25 million (FulcrumSec) and US$50 million (TheUSERS007, unconfirmed); Novo Nordisk's reported position is that it has not paid either demand. [Ransom amounts: CLAIMED; non-payment: consistent with reporting reviewed, treated as CONFIRMED based on continued leak-site activity]

9.2 Manufacturing disruption

KEY FINDING

Novo Nordisk has explicitly and consistently stated, across its public disclosure and subsequent updates, that core business operations — including manufacturing and product distribution — were not impacted by this incident and remained fully operational throughout. No independent reporting reviewed for this report contradicts this statement.

9.3 Supply chain impact

No public evidence indicates disruption to Novo Nordisk's supply chain, including raw material sourcing, API production, finished product distribution, or partner/distributor operations, as a result of this incident.

9.4 Customer and patient impact

The primary confirmed patient-facing impact is the exposure of pseudonymized clinical trial data for trial participants and, separately, identifiable contact data for healthcare professionals — not an impact to product availability, product safety, or ongoing patient care. Novo Nordisk has stated the exposed clinical trial data cannot on its own be used to identify individual patients by name, though the company and independent commentators have noted that combined with other information, re-identification risk cannot be entirely excluded for pseudonymized data of this kind.

9.5 Regulatory implications

Regulatory Dimension	Status
GDPR (EU/Denmark)	Novo Nordisk, as a Danish-domiciled data controller, is subject to GDPR breach notification obligations to the Danish Data Protection Agency (Datatilsynet) and, where applicable, to affected data subjects. The company has stated it is in contact with relevant authorities. [CONFIRMED engagement stated; specific regulatory findings or penalties UNCONFIRMED/pending]

Regulatory Dimension	Status
Clinical trial regulatory bodies	Given the exposure of clinical trial data, engagement with relevant clinical trial oversight and ethics bodies would be a standard expectation; no specific regulatory finding has been publicly disclosed.
U.S. state/federal privacy law	Given Novo Nordisk's significant U.S. commercial presence, exposure of any U.S.-linked HCP or trial participant data could trigger separate U.S. state breach-notification requirements; no U.S.-specific regulatory action had been publicly reported at the time of this report's publication.
Securities/market disclosure	As a company listed on Nasdaq Copenhagen (and with ADRs on the NYSE), Novo Nordisk's disclosure obligations under applicable securities regulations are a relevant consideration; the company's 11 June 2026 public statement is consistent with a market disclosure of a material event, though this report does not assess formal securities-law compliance.

9.6 Reputational damage and market reaction

Reputational impact is inherently difficult to quantify shortly after disclosure. The incident received substantial coverage across mainstream financial press (Reuters), pharmaceutical trade press (FiercePharma/FierceBiotech), and cybersecurity trade press, reflecting Novo Nordisk's global prominence as a top-tier pharmaceutical manufacturer. This report did not identify a specific, publicly reported, statistically significant Novo Nordisk share-price movement directly and solely attributable to this incident as of publication; broader Novo Nordisk share price dynamics in 2026 have been influenced by multiple unrelated commercial and competitive factors (e.g., GLP-1 market competition), and this report does not attempt to isolate an incident-specific market effect, as doing so would exceed the available evidence.

9.7 Business impact summary table

Impact Area	Severity	Status
Data confidentiality	High	CONFIRMED
Manufacturing/production continuity	None	CONFIRMED (unaffected)
Supply chain continuity	None identified	CONFIRMED (no evidence of impact)
Financial (direct costs/fines)	Undetermined	UNCONFIRMED / pending disclosure
Regulatory exposure	Moderate-to-High (pending outcome)	CONFIRMED engagement / outcome UNCONFIRMED

Impact Area	Severity	Status
Reputational	Moderate (assessed qualitatively)	ANALYST ASSESSMENT
Intellectual property (if threat-actor claims substantiated)	Potentially Severe	CLAIMED — unconfirmed

10. OT security perspective

HEADLINE FINDING FOR OT/ICS AND MANUFACTURING AUDIENCES

There is no confirmed evidence that this incident affected Novo Nordisk's operational technology (OT), industrial control systems (ICS), or manufacturing production environments. Novo Nordisk has explicitly and repeatedly stated that core business operations, including manufacturing, were not impacted and remained fully operational. This assessment should be read plainly: absence of confirmed OT impact, not absence of any OT-adjacent claim (see below).

10.1 The One OT-Adjacent Claim, and Why It Should Be Treated Cautiously

As referenced in Section 4.3.2, FulcrumSec has claimed it is withholding certain stolen data described as relating to "operational technology and software used to interact with sensors and equipment" at Novo Nordisk production facilities. This is the only OT-adjacent claim identified in public reporting for this incident, and it carries several important caveats:

- It is a claim made by a financially motivated extortion actor with a direct incentive to maximize perceived leverage and asset value — including by asserting access to categories of data (like OT/ICS-related material) that are known to be highly sensitive to industrial operators.
- It describes possession of data or software related to OT, not confirmed access to, control over, or manipulation of live production control systems, sensors, or equipment.
- Novo Nordisk has not confirmed this claim, and no independent forensic evidence of OT/ICS system access has been published.
- The claim is consistent with — and does not exceed — the broader confirmed narrative that the accessed environment was corporate IT and cloud/development infrastructure, from which engineering documentation, configuration files, or software related to OT equipment could plausibly have been stored without those systems constituting live production control-system access.

10.2 Assessed implications for operational resilience

Even without confirmed OT/ICS compromise, this incident offers instructive considerations for pharmaceutical and other critical-infrastructure manufacturers regarding the IT/OT boundary:

- Engineering documentation, equipment configuration files, sensor interface software, and similar OT-adjacent artifacts are frequently stored and version-controlled within corporate IT/cloud/developer environments (source code repositories, file shares, collaboration platforms) rather than exclusively within the OT environment itself — meaning an IT-only breach can still expose OT-relevant intellectual property even when no OT network boundary is crossed.
- Novo Nordisk's apparent success in preventing operational disruption despite a confirmed, multi-week (or longer, per threat-actor claims) IT compromise is consistent with — though not proof of — effective segmentation between corporate IT/cloud environments and

production control systems. This is a positive resilience indicator worth noting for the sector, even though it cannot be fully verified from public information alone.

- Manufacturers should independently verify, rather than assume, that OT-relevant engineering data stored in IT/cloud/developer repositories is subject to the same data-classification and access-control rigor as clinical and financial data, since this incident illustrates that such artifacts may reside in more broadly accessible corporate systems than commonly assumed.

10.3 Lessons for Pharmaceutical and Critical Infrastructure Manufacturers

Lesson	Applicability
IT/OT segmentation is a resilience control, not just a compliance checkbox	The apparent containment of this incident to IT/cloud environments — with production continuing unaffected — illustrates the practical value of maintaining a hardened boundary between corporate IT and production control environments.
OT-relevant intellectual property can be exposed without an OT network being touched	Equipment configuration data, sensor/interface software, and similar artifacts stored in developer/collaboration platforms warrant the same data classification rigor applied to core OT systems.
Extortion actors will assert OT-related claims for leverage regardless of actual access	Organizations and incident responders should have a pre-established, calm process for verifying (or ruling out) OT-related claims during extortion negotiations, rather than treating every claim at face value under pressure.
Confirmed operational continuity should still trigger a full OT risk review	Even absent confirmed OT compromise, a significant IT breach affecting a manufacturer should prompt an internal review of what OT-relevant data or credentials may be reachable from the compromised IT scope.

11. Defensive lessons learned

The following recommendations are derived from the general risk patterns this incident illustrates (per Section 8.2) and represent standard industry best practice for organizations seeking to reduce exposure to similar data-theft extortion scenarios. They are Shieldworkz analyst recommendations, not statements about specific gaps confirmed within Novo Nordisk's environment.

11.1 Immediate priority (0-30 Days)

Identity, Secrets, and Endpoint

- Audit all public-facing web assets (including development, staging, and "forgotten" subdomains) for embedded secrets in client-side JavaScript, configuration files, and source maps — this class of exposure is typically missed by repository-only secret scanning.
- Rotate and re-scope any credentials discovered through this audit; enforce least-privilege scoping for all API tokens, personal access tokens (PATs), and service account credentials, with expiration and narrow repository/resource scope by default.
- Review outbound data-transfer monitoring thresholds for sensitivity to low-and-slow exfiltration patterns rather than only high-volume anomalies.

11.2 Short-term priority (1-3 Months)

Network, Vulnerability, and Access Management

- Extend attack-surface-management coverage to include all internet-reachable subdomains and cloud assets, not only production-designated domains.
- Implement or strengthen just-in-time, time-bound privileged access for source-control and cloud administration accounts, with mandatory MFA and session monitoring.
- Establish or refresh a formal vulnerability and exposure management process specifically covering exposed secrets and misconfigurations in cloud and CI/CD (continuous integration/continuous deployment) pipelines.
- Review third-party and vendor access to code repositories, cloud environments, and AI/ML infrastructure for excessive standing privilege.

11.3 Medium-term priority (3-9 Months)

Monitoring, Detection, and Backup/Recovery

- Deploy or mature user and entity behavior analytics (UEBA) capability specifically tuned to detect anomalous GitHub/source-control API usage, anomalous cloud container registry pull activity, and unusual repository access patterns.
- Validate that backup and recovery capability for both IT and AI/ML infrastructure (training data, model weights, pipeline configuration) is tested and does not assume a ransomware-only threat model — data-theft extortion requires a different response posture (containment and negotiation strategy) than encryption-recovery scenarios.

- Conduct a tabletop exercise specifically modeling a data-theft extortion scenario (no encryption), including decision-making around ransom negotiation, regulatory notification timing, and public communications — distinct from a standard ransomware tabletop.
- Extend security monitoring and data classification rigor explicitly to AI/ML development environments (training data stores, model registries, HPC/GPU scheduling infrastructure), treating these as crown-jewel assets comparable to clinical and financial systems.

11.4 Long-term priority (9+ Months)

Governance, OT Boundary, and Third-Party Risk

- Institute an ongoing, board-level governance review of the organization's IT/OT segmentation architecture and its effectiveness at limiting business-continuity impact from IT-originated incidents, using this incident's apparent successful containment as a benchmark to validate against, not assume.
- Establish a formal, cross-functional (legal, communications, security, executive) extortion-response playbook that includes a defined process for independently verifying threat-actor claims (including OT-related claims) before they inform public statements or negotiation posture.
- Build sustained investment in secure development lifecycle practices specifically covering AI/ML pipelines and infrastructure, given the increasing targeting of these assets by financially motivated threat actors.
- Formalize third-party and supply-chain risk management specifically for cloud, source-control, and AI/ML tooling providers, given the centrality of these platforms to the claimed attack path in this incident.

12. Key takeaways for critical infrastructure organizations

While Novo Nordisk operates in the pharmaceutical manufacturing sector, the risk patterns this incident illustrates are broadly applicable across critical infrastructure sectors that combine large-scale production operations with extensive digital R&D, engineering, and cloud/AI infrastructure.

Sector	Applicable Lesson
Manufacturing (general)	Corporate IT/cloud environments frequently store engineering and equipment-configuration data with direct relevance to production systems; classify and protect this data with the same rigor as OT systems themselves, even when it never crosses the OT network boundary.
Pharmaceuticals / Life Sciences	Clinical trial data, drug compound structures, and AI-driven drug discovery infrastructure are now explicit, high-value targets for extortion actors; data governance programs should extend equal rigor to research/discovery data as to patient-facing clinical systems.
Energy	The claimed initial access vector (secrets in client-side web assets) applies equally to energy sector organizations' customer portals, field-service applications, and partner-facing web platforms; attack-surface management should explicitly include non-production and legacy subdomains.
Water and Wastewater	As in the OT Security Perspective (Section 10), water utilities should verify that SCADA/HMI configuration data and engineering documentation are not exposed via loosely governed IT file shares or developer repositories, even where the OT network itself is well segmented.
Transportation	Organizations with extensive fleet-management, logistics, or scheduling software development functions should apply the same secrets-management and CI/CD security scrutiny recommended in Section 11 to reduce exposure to credential-harvesting-based initial access.

12.1 The core cross-sector principle

BOTTOM LINE FOR CRITICAL INFRASTRUCTURE LEADERSHIP

Operational continuity and data confidentiality are separate risk dimensions that require separate — though coordinated — defensive strategies. This incident demonstrates that an organization can experience a serious, high-profile confidentiality breach while maintaining full operational continuity, provided IT/OT segmentation and incident containment practices function as intended. Critical infrastructure organizations should resist the temptation to treat 'no operational impact' as equivalent to 'incident contained' — the confidentiality and intellectual-property consequences of a breach like this can be severe and long-lasting even when production never stops.

13. Timeline appendix: Complete chronology

This appendix consolidates every dated event referenced throughout this report into a single chronological reference table.

Date	Event	Status
~Mar 2026	Claimed initial access date per FulcrumSec's account (exposed credentials in client-side JavaScript on Novo Nordisk subdomains)	CLAIMED
~5-7 Jun 2026	Claimed date of a separate intrusion asserted by second actor "TheUSERS007"	CLAIMED / UNCONFIRMED
~1 Jun 2026	Claimed start of ransom negotiation between FulcrumSec and Novo Nordisk ($25M demand)	CLAIMED
11 Jun 2026	Novo Nordisk publicly discloses the IT security incident via official statement	CONFIRMED
11-12 Jun 2026	Reuters, BNN Bloomberg, and BleepingComputer report on the disclosure, including confirmed data categories exposed	CONFIRMED
15 Jun 2026	FulcrumSec begins publishing sample stolen data on its leak site	CONFIRMED (leak activity)
16 Jun 2026	FulcrumSec publicly claims responsibility with a detailed (claimed) data inventory; SecurityWeek, HIPAA Journal, and BankInfoSecurity report the claims	CLAIMED
~16-18 Jun 2026	TheUSERS007 claim surfaces via DataBreaches.net; reported by HIPAA Journal and FiercePharma	CLAIMED / UNCONFIRMED
Late Jun 2026	Novo Nordisk sends direct notification letters to affected clinical trial participants and healthcare professionals	CONFIRMED
Late Jun 2026	Industrial Cyber and other trade press publish sector-focused analysis of the incident	CONFIRMED (reporting activity)
1 Jul 2026	Publication date of this Shieldworkz intelligence report	N/A
Ongoing	Novo Nordisk's forensic investigation, regulatory engagement, and system restoration continue; final affected-individual count not yet published	ONGOING / UNCONFIRMED

14. References and bibliography

This report draws exclusively on the following publicly available sources. In-text references throughout this document correspond to the organizations named below; specific article URLs are provided here for verification.

14.1 Primary Sources

- Novo Nordisk A/S — "Incident update" and related corporate disclosures. novonordisk.com/news-and-media/latest-news/incident-update.html

14.2 Wire and Financial News

- Reuters — reporting on Novo Nordisk's disclosure of unauthorized IT system access and data copying, 11-12 June 2026.
- BNN Bloomberg — syndicated Reuters coverage of the Novo Nordisk disclosure.

14.3 Cybersecurity Trade Press and Threat Intelligence Commentary

- BleepingComputer — coverage of Novo Nordisk's confirmed data categories and incident details, June 2026.
- SecurityWeek — reporting on FulcrumSec's claim of responsibility and claimed data inventory.
- SecurityAffairs — reporting on the leak-site publication timeline and threat actor claims.
- BankInfoSecurity (ISMG) — reporting on ransom negotiation claims and threat actor profile.
- HIPAA Journal — reporting on healthcare-data-specific aspects of the breach, including HCP data exposure and the second claimed actor, TheUSERS007.
- Shieldworkz — Incident analysis, threat actor TTPs and lessons
- Ransomnews — coverage of leak-site activity and claimed data categories.
- FierceBiotech / FiercePharma — pharmaceutical trade press coverage, including reporting on the TheUSERS007 claim via DataBreaches.net.

14.4 Company Background Sources

- Novo Nordisk A/S — corporate "About" and investor-relations disclosures regarding employee count, global footprint, and manufacturing sites (including Kalundborg, Denmark).

14.5 Sources Consulted but Excluded

During research, this report's authors identified at least one secondary online source presenting purported technical indicators of compromise, including a file hash matching the known SHA-256 value of an empty file — a strong indicator of fabricated or low-quality automated content. That source, and any claims unique to it (including a threat actor name not corroborated elsewhere),

have been deliberately excluded from this report's findings and are noted here only to document the exclusion and the reasoning behind it, consistent with this report's sourcing discipline.

14.6 Disclaimer

This report reflects publicly available information as of 1 July 2026. Threat-actor-sourced claims are inherently unverified and may be inaccurate, exaggerated, or fabricated in whole or in part; they are presented for intelligence and defensive-planning awareness, not as established fact. This report will be superseded by any official findings subsequently published by Novo Nordisk, relevant regulators, or law enforcement. Shieldworkz recommends monitoring Novo Nordisk's official incident update page and relevant regulatory disclosures for authoritative updates.

About Shieldworkz

Shieldworkz is a specialist OT/ICS cybersecurity firm with an NDR solution and AI-based tools for securing SCADA, PLCs and Cyber Physical Systems. We serve critical infrastructure operators, industrial organisations, and government entities across the energy, oil and gas, manufacturing, utilities, transport, and defence sectors.

Our service areas include OT security assessments (powered by OThello Assess with sub-24-hour assessment cycles), NIS2 and IEC 62443 compliance programmes, OT threat intelligence advisories, OT SOC design and implementation, and regulatory readiness engagements for NCA (Saudi OTCC/ECC), NERC CIP, SOCI, and Singapore Cybersecurity Act obligations.

NDR Solution: shieldworkz.com/products/ot-security-platform **| Media Scan:** shieldworkz.com/products/ot-security- **| Othello Assess:** shieldworkz.com/othello/assess **| Patch Management:** shieldworkz.com/products/patch-management-solution **| Regulatory Playbooks:** shieldworkz.com/regulatory-playbooks **| Remediation Guides:** shieldworkz.com/remediation-guides **| Reports:** shieldworkz.com/reports

About Shieldworkz

ISOC and Honeypot Locations

Honeypot Locations

Security Operations Center

Shieldworkz is a global OT security company founded by top industry experts to protect critical infrastructure using proprietary technology and a leading consulting platform, we partner with businesses to secure assets, networks, and programs across industries. Our services are tailored to each client's cyber risks and backed by the world's largest OT and IoT threat intelligence facility and a global research team.

Secure Your Industrial Future

Talk to us today!

From OT security assessments covering NIS2, IEC 62443, NERC CIP and other regional requirements to an OT security platform, Shieldworkz covers all compliance and industrial cybersecurity enhancement needs. Talk to us to learn how you can enhance your security posture in 7 easy steps.

Contact Us

Fritz-Schäffer-Street 1,
4th floor

Bonn, 53113, Germany

+49 (0) 228 / 929 39210

europe@shieldworkz.com

396 Old Colony Road
Richmond Hill,
ON L4E 5A5 Canada

+1 (437) 223-7770

americas@shieldworkz.com

Tenth floor,

Abu Dhabi,
United Arab Emirates,
FAB Business Center

+971 56 660 5200

middleeast@shieldworkz.com

Gopalan Signature Tower,
No 6, 2nd Floor, Old Madras
Road, Benniganahalli

Bengaluru,
Karnataka 560093

+91 9059620557

apac@shieldworkz.com