INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-16 18:52 UTC

Nitrogen Ransomware Group Claims Breach of Foxconn North American Operations; Client Data Allegedly Exfiltrated

DATA BREACH | HIGH | CVSS 9.1

SCC Item ID	SCC-DBR-2026-0127
Type	Data Breach
Severity	HIGH
CVSS Base Score	9.1
Affected Products	Foxconn North American manufacturing facilities; client data allegedly belonging to Apple, Google, Nvidia, Dell, Intel, and AMD
Published	2026-05-15
Discovery Source	Gemini

Executive Summary

The Nitrogen ransomware group has claimed responsibility for a cyberattack against Foxconn's North American manufacturing operations, with Foxconn confirming the incident occurred around May 12-13, 2026. Threat actors allege exfiltration of proprietary data belonging to major technology clients including Apple, Google, Nvidia, Dell, Intel, and AMD, though the full scope of stolen data has not been independently confirmed. The primary business risk is indirect: client organizations may have had product specifications, supply chain logistics, or confidential business data exposed through their contract manufacturing relationship with Foxconn, without any direct breach of their own networks.

Technical Analysis

Nitrogen is a ransomware-as-a-service (RaaS) operation with a documented history of using malvertising and SEO poisoning for initial access delivery, techniques mapped to MITRE ATT&CK T1566 (Phishing) and T1190 (Exploit Public-Facing Application). Once inside, the group typically pursues credential abuse (T1078), data exfiltration (T1041), and ransomware deployment (T1486). The Foxconn incident represents a supply chain compromise vector (T1195), where a tier-1 contract manufacturer is targeted to access downstream client data without directly breaching client organizations. Relevant CWEs include CWE-284 (Improper Access Control), CWE-359 (Exposure of Private Personal Information), and CWE-693 (Protection Mechanism Failure). No CVE is associated with this incident. The specific initial access vector used against Foxconn has not been publicly confirmed. Specific technical intrusion details and confirmed data contents remain at medium confidence

pending official disclosure from Foxconn or affected clients. Ransom demand figures have not been publicly reported as of this writing. Sources: TechCrunch, The Register, The Manufacturer.

Action Checklist

1. Step 1: Containment. Nitrogen group claims exfiltration of data from major technology clients (per TechCrunch, The Register); Foxconn has confirmed the attack but not the full scope. If your organization has a direct manufacturing or supply relationship with Foxconn North American operations, immediately engage your vendor risk management team to determine what data Foxconn holds on your behalf. Assess whether data sharing agreements, NDAs, or supply chain contracts cover the categories of data alleged to be exfiltrated (product specs, logistics, business intelligence). Do not wait for Foxconn confirmation before initiating internal review.
2. Step 2: Detection. Review your threat intelligence feeds and SIEM for any indicators associated with the Nitrogen group. Monitor for anomalous outbound connections, unexpected data transfers, or lateral movement patterns from systems with Foxconn-adjacent integrations (EDI systems, supplier portals, procurement platforms). Check for Nitrogen-associated TTPs: malvertising-delivered payloads, SEO-poisoned software installers, and credential abuse against VPN or remote access infrastructure. No confirmed IOCs for this specific campaign have been publicly released as of this writing.
3. Step 3: Eradication. No patch applies to this incident. Eradication focus should be on third-party access: audit and revoke any Foxconn-held credentials or API keys that grant access to your internal systems or data repositories. Review and tighten supplier portal access controls. If Nitrogen TTPs suggest malvertising as initial access, enforce application allowlisting and block unauthorized software installation vectors on endpoints.
4. Step 4: Recovery. Validate that no Foxconn-connected systems or integrations in your environment show signs of compromise. Monitor for anomalous access attempts against accounts or systems that interact with Foxconn supply chain infrastructure. Confirm your data classification policies accurately reflect what was shared with Foxconn, and document findings for regulatory and legal review.
5. Step 5: Post-Incident. This incident exposes a common third-party risk gap: sensitive client data held by contract manufacturers often sits outside the client's direct security controls. Conduct a formal third-party risk assessment of all tier-1 contract manufacturers. Verify that vendor contracts require breach notification within defined timeframes, mandate minimum security controls, and limit data retention to operational necessity. Map what proprietary data each manufacturing partner holds and ensure it is captured in your data inventory.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if: (1) your organization's proprietary data (product roadmaps, unreleased specifications, or customer data) is confirmed in scope of Foxconn NA exfiltration, triggering breach notification obligations under applicable state laws or sector regulations; (2) forensic evidence indicates Nitrogen actors used Foxconn-adjacent credentials or integrations to pivot into your internal environment; or (3) you cannot account for data shared with Foxconn NA within 24 hours of initiating internal review, indicating a data inventory gap that itself constitutes a compliance finding.

Recovery Notes	Before restoring any Foxconn-adjacent EDI, supplier portal, or procurement integrations to full operational status, require Foxconn NA to provide written confirmation of eradication and a summary of their forensic findings — do not restore trust unilaterally. Implement a 30-day enhanced monitoring period on all systems that communicate with Foxconn NA infrastructure, specifically alerting on authentication anomalies, unexpected data volumes, and any new outbound connections from integration middleware. Given Nitrogen's use of Cobalt Strike and extended dwell-time tactics common to ransomware operators conducting pre-exfiltration reconnaissance, treat the May 12-13 breach date as a last-known-bad date, not a first-known-bad date — expand forensic review to at least 60 days prior.
Forensic Artifacts	EDI transaction logs (X12 850/855/856 purchase order and ASN messages) from the 60-day window preceding May 12, 2026 — establish what product specification and logistics data transited Foxconn NA systems and could have been in scope for exfiltration | Supplier portal and procurement platform authentication logs — specifically OAuth token issuance logs, SAML assertion logs, and session duration records for Foxconn-associated accounts — to identify any unauthorized access or token abuse by Nitrogen actors using stolen credentials | Windows Prefetch files (C:\Windows\Prefetch\) and browser download history on endpoints used by supply chain and procurement staff — Nitrogen's malvertising campaigns deliver SEO-poisoned installers (disguised as AnyDesk, WinSCP, Advanced IP Scanner) that leave execution artifacts in Prefetch and download directories | Sysmon Event ID 1 (Process Create) and Event ID 3 (Network Connection) logs from EDI servers and supplier-portal-facing hosts — specifically processes spawned from browser temp or AppData directories and outbound connections to non-approved external IPs, consistent with Nitrogen's IDAT loader or Cobalt Strike stager execution chain | API gateway and SFTP server transfer logs showing data volume and file type metadata for all outbound transfers to Foxconn NA endpoints in the 90-day pre-breach window — establishes the maximum possible data exposure scope for regulatory disclosure and legal hold purposes

Per-Action IR Details

Step 1: Containment — If your organization has a direct manufacturing or supply relationship with Foxconn North American operations, immediately engage your vendor risk management team to determine what data Foxconn holds on your behalf. Assess whether data sharing agreements, NDAs, or supply chain contracts cover the categories of data alleged to be exfiltrated (product specs, logistics, business intelligence). Do not wait for Foxconn confirmation before initiating internal review.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy (CSF RS.MA-01: Execute IR plan in coordination with relevant third parties)

Controls: NIST IR-4 (Incident Handling), NIST IR-6 (Incident Reporting), NIST SA-9 (External System Services) — enforce contractual requirements for third-party security controls and breach notification, CIS 3.2 (Establish and Maintain a Data Inventory) — identify what proprietary data (product specs, logistics, BI) was shared with Foxconn NA, CIS 6.2 (Establish an Access Revoking Process) — initiate review of any access Foxconn holds into your systems

Compensating: Without a vendor risk platform, build a manual data-sharing matrix in a spreadsheet: columns for system name, data classification (e.g., product roadmap, NDA-covered specs), Foxconn-facing interface (EDI, SFTP, portal), and contractual notification SLA. Use your legal team's contract repository to pull executed NDAs and data processing agreements for Foxconn NA specifically. Run: `grep -ri 'foxconn' /path/to/contracts/` if contracts are stored locally, to surface relevant agreements quickly. A 2-person team should divide: one owns the data inventory pull, one owns contract review.

Evidence: Before engaging the vendor risk team, preserve a timestamped snapshot of all active data-sharing configurations with Foxconn NA — SFTP transfer logs, EDI transaction logs (X12 850/856/810 message logs), API gateway access logs showing Foxconn-associated tokens or service accounts, and any supplier portal session logs.

Capture these before any access revocation actions that could overwrite or rotate credentials and destroy audit trail. Document exact data categories transmitted in the 90 days prior to May 12, 2026 — the alleged breach window.

Step 2: Detection — Review your threat intelligence feeds and SIEM for any indicators associated with the Nitrogen group. Monitor for anomalous outbound connections, unexpected data transfers, or lateral movement patterns from systems with Foxconn-adjacent integrations (EDI systems, supplier portals, procurement platforms). Check for Nitrogen-associated TTPs: malvertising-delivered payloads, SEO-poisoned software installers, and credential abuse against VPN or remote access infrastructure. No confirmed IOCs for this specific campaign have been publicly released as of this writing.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis (CSF DE.AE-02: Analyze adverse events using CTI; DE.AE-07: Integrate threat intelligence into detection; DE.CM-09: Monitor common attack vectors including malvertising and credential abuse)

Controls: NIST SI-4 (System Monitoring) — monitor endpoints and network for Nitrogen TTP signatures including malvertising delivery and SEO-poisoned installer execution, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review logs on EDI systems, VPN concentrators, and supplier portal access for anomalous activity bracketing May 12-13, 2026, NIST IR-5 (Incident Monitoring) — track and document all Nitrogen-related indicators as they become available from CISA, threat intel vendors, and ISAC feeds, CIS 8.2 (Collect Audit Logs) — ensure EDI platforms, procurement portals, and VPN infrastructure are logging at sufficient verbosity to support retrospective analysis, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — monitor for Nitrogen-specific IOC releases from CISA and sector ISACs

Compensating: Without a SIEM, execute targeted log queries manually: (1) On Windows endpoints, query Sysmon Event ID 1 (Process Create) for processes spawned from browser temp directories or AppData — a hallmark of Nitrogen's malvertising-delivered IDAT loader or similar stagers. Command: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1 -and $_.Message -match 'AppData\\Local\\Temp'}`. (2) On VPN concentrators, extract authentication logs for the May 12-13 window and flag accounts with successful logins from unexpected geolocations or at unusual hours — Nitrogen has used credential abuse as a pivot post-initial-access. (3) Use Sigma rule 'proc_creation_win_malware_nitrogen' (available in SigmaHQ repository) converted to PowerShell or grep for offline log analysis. (4) Check DNS query logs (Windows DNS debug log or Pi-hole if deployed) for domains matching Nitrogen's known C2 infrastructure patterns — high-entropy subdomains or newly registered domains queried from supply-chain-facing workstations.

Evidence: Collect the following before any remediation actions alter system state: (1) Windows Security Event Log Event ID 4624/4625 (logon success/failure) and 4648 (explicit credential use) from VPN-connected and supplier-portal-facing systems for the May 10-15 window. (2) Sysmon Event ID 3 (Network Connection) logs showing outbound connections from EDI or procurement systems to non-approved external IPs. (3) Browser download history and Windows Prefetch files (`C:\Windows\Prefetch\`) on endpoints used by procurement or supply chain staff — Nitrogen's SEO-poisoned installers (masquerading as legitimate tools like AnyDesk, WinSCP) leave prefetch artifacts. (4) PowerShell ScriptBlock logs (Event ID 4104) for encoded or obfuscated commands executed on supplier-portal-adjacent hosts. (5) NetFlow or firewall connection logs showing large outbound data transfers (>100MB) from internal systems to external destinations in the breach window.

Step 3: Eradication — No patch applies to this incident. Eradication focus should be on third-party access: audit and revoke any Foxconn-held credentials or API keys that grant access to your internal systems or data repositories. Review and tighten supplier portal access controls. If Nitrogen TTPs suggest malvertising as initial access, enforce application allowlisting and block unauthorized software installation vectors on endpoints.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication (CSF RS.MA-01: Mitigate incident; remove threat actor footholds and revoke compromised access paths)

Controls: NIST AC-2 (Account Management) — immediately disable or rotate all service accounts, API keys, and shared credentials associated with Foxconn NA integrations, NIST CM-7 (Least Functionality) — restrict supplier portal

access to minimum required functions; disable any Foxconn-associated accounts that cannot be immediately verified as uncompromised, NIST SI-2 (Flaw Remediation) — while no CVE applies, treat credential exposure as a flaw requiring remediation through rotation and access policy update, NIST SI-7 (Software, Firmware, and Information Integrity) — deploy application allowlisting to block Nitrogen's malvertising-delivered installers from executing on endpoints used by supply chain personnel, CIS 4.6 (Securely Manage Enterprise Assets and Software) — enforce software restriction policies or AppLocker rules to block execution from user-writable paths, CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) — verify no Foxconn-associated service accounts hold elevated privileges beyond operational necessity

Compensating: Without an enterprise PAM tool: (1) Use PowerShell to enumerate and disable Foxconn-associated AD service accounts: `Get-ADUser -Filter {Description -like '*foxconn*' -or Name -like '*foxconn*'} | Disable-ADAccount`. (2) Rotate all API keys and SFTP credentials associated with Foxconn NA integrations immediately — document old and new credential metadata with timestamps for the audit trail. (3) Deploy Windows AppLocker (built-in, no cost) in audit mode first, then enforce: block execution from `%TEMP%`, `%APPDATA%`, and `%USERPROFILE%\Downloads` — directories where Nitrogen's malvertising payloads land. (4) Use OSQuery to identify any non-standard software installed on supply-chain-facing endpoints since May 10: `SELECT name, install_date FROM programs WHERE install_date > '2026-05-10' ORDER BY install_date DESC;`. (5) For supplier portal access, manually review the portal's active session list and force-terminate all Foxconn-associated sessions.

Evidence: Before revoking credentials, preserve: (1) A full export of the Identity Provider (IdP) or Active Directory access logs showing all authentications by Foxconn-associated accounts or service principals in the 30 days prior to May 12 — rotation destroys the ability to correlate future forensic findings to these identities. (2) API gateway access logs showing all API calls made using Foxconn-associated keys, including endpoints accessed, data volumes, and response codes — critical for scoping what data was accessible. (3) A snapshot of current ACLs on all data repositories (SharePoint, S3 buckets, SFTP directories) accessible to Foxconn NA accounts, timestamped before any permission changes are made. (4) If any Nitrogen-delivered malware is suspected on an endpoint, acquire a full memory image using WinPmem (free) before remediation — Nitrogen's IDAT loader and Cobalt Strike variants are memory-resident and will not survive a reboot.

Step 4: Recovery — Validate that no Foxconn-connected systems or integrations in your environment show signs of compromise. Monitor for anomalous access attempts against accounts or systems that interact with Foxconn supply chain infrastructure. Confirm your data classification policies accurately reflect what was shared with Foxconn, and document findings for regulatory and legal review.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery (CSF RC: Execute recovery plan, restore integrity of supply chain integrations, verify no residual attacker presence, communicate findings to legal and regulatory stakeholders)

Controls: NIST IR-4 (Incident Handling) — execute the recovery phase of the incident response plan, verifying eradication before restoring Foxconn-adjacent integrations to operational status, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — implement enhanced monitoring on all systems that had Foxconn-facing integrations for a minimum 30-day post-incident observation window, NIST CA-7 (Continuous Monitoring) — establish baseline behavioral metrics for EDI, supplier portal, and procurement systems and alert on deviations, NIST SI-4 (System Monitoring) — deploy targeted detection rules for Nitrogen-associated post-exploitation behaviors (Cobalt Strike beaconing, lateral movement via SMB) on supply-chain-facing network segments, CIS 3.2 (Establish and Maintain a Data Inventory) — update data inventory to accurately reflect what proprietary data categories were shared with Foxconn NA, supporting regulatory disclosure decisions, CIS 7.2 (Establish and Maintain a Remediation Process) — document remediation actions with timestamps, evidence references, and responsible parties for legal and regulatory review

Compensating: Without enterprise NDR or EDR: (1) Deploy Sysmon with a hardened configuration (SwiftOnSecurity or Olaf Hartong templates) on all supply-chain-facing endpoints if not already present — this provides the Event ID 1/3/7/10 telemetry needed for retrospective analysis. (2) Set up a free Elastic Stack (ELK) instance to ingest Windows Event Logs from EDI and procurement systems for the 30-day monitoring window — Winlogbeat ships logs at no cost. (3) Create a daily cron job or scheduled task to run `netstat -ano` on Foxconn-adjacent servers and diff the output against a known-good baseline — flag any new persistent outbound connections. (4) Use Wireshark or tcpdump in scheduled capture mode on the network segment hosting supplier portal integrations to capture a 1-hour baseline daily

— inspect for beaconing patterns (regular interval outbound connections) consistent with Cobalt Strike's default 60-second beacon.

Evidence: Before declaring recovery complete, document: (1) Output of integrity verification on configuration files for EDI translation software and supplier portal connectors — compare file hashes against vendor-provided baselines to rule out Nitrogen implanting persistence in integration middleware. (2) Full export of authentication logs for the 30-day post-incident monitoring window, retained per your log retention policy (NIST AU-11) for potential regulatory disclosure. (3) Written confirmation from Foxconn (when available) of the scope of data confirmed exfiltrated — required for breach notification threshold assessment under applicable state breach notification laws and, if Apple/Google/Nvidia/Dell/Intel/AMD data is confirmed exfiltrated, potentially sector-specific regulatory frameworks. (4) Data classification audit output confirming what data categories were shared with Foxconn NA, mapped against your data inventory — this is the evidentiary record for any regulatory filing.

Step 5: Post-Incident — This incident exposes a common third-party risk gap: sensitive client data held by contract manufacturers often sits outside the client's direct security controls. Conduct a formal third-party risk assessment of all tier-1 contract manufacturers. Verify that vendor contracts require breach notification within defined timeframes, mandate minimum security controls, and limit data retention to operational necessity. Map what proprietary data each manufacturing partner holds and ensure it is captured in your data inventory.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (CSF GV, ID: Update policies, conduct lessons learned, improve third-party risk controls based on incident findings; DE.AE-07: Integrate intelligence findings into future detection improvement)

Controls: NIST IR-4 (Incident Handling) — update the incident handling capability to include third-party breach scenarios, incorporating lessons learned from the Nitrogen/Foxconn incident, NIST IR-8 (Incident Response Plan) — revise the IR plan to explicitly address supply chain and contract manufacturer breach scenarios, including third-party notification workflows, NIST SA-9 (External System Services) — enforce contractual requirements mandating breach notification SLAs, minimum security controls (e.g., MFA, encryption at rest), and data retention limits for all tier-1 contract manufacturers, NIST RA-3 (Risk Assessment) — conduct a formal third-party risk assessment of all tier-1 contract manufacturers using findings from the Foxconn incident as a case study for data exposure scope, NIST SI-12 (Information Management and Retention) — require contract manufacturers to demonstrate data minimization — retain only data operationally necessary for manufacturing execution, with documented destruction schedules, CIS 3.2 (Establish and Maintain a Data Inventory) — extend the data inventory to explicitly track proprietary data held by each manufacturing partner, including data type, classification, and contractual basis, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate third-party security posture assessments into the vulnerability management program for all tier-1 contract manufacturers

Compensating: Without a GRC platform or dedicated vendor risk team: (1) Build a manufacturer data exposure register in a spreadsheet: rows for each tier-1 contract manufacturer, columns for data categories shared (product specs, roadmaps, logistics, customer data), contractual notification SLA, and minimum security control requirements documented in the contract. Populate it using the data inventory work from Step 4. (2) Draft a standard vendor security addendum (freely modelable from NIST SP 800-161 supply chain risk management guidance) requiring MFA on all systems handling client data, encryption at rest and in transit, and 72-hour breach notification — attach to all contract renewals. (3) Use the CISA Third-Party Risk Management resources (freely available at cisa.gov) as a framework for assessing contract manufacturers without purchasing a TPRM platform. (4) Assign one team member to subscribe to manufacturing sector ISAC (e.g., MFG-ISAC) alerts and Nitrogen group tracking via free sources (CISA advisories, Recorded Future community feed, OTX AlienVault) to maintain awareness of future campaigns targeting contract manufacturers.

Evidence: Lessons learned documentation should capture and preserve: (1) Timeline reconstruction of when Foxconn NA received data from your organization versus the alleged breach window (May 12-13, 2026) — establishes exposure duration for regulatory and legal purposes. (2) Inventory of all data categories confirmed shared with Foxconn NA, mapped to sensitivity classification — this becomes the baseline for any future breach notification scope determination if exfiltration is confirmed. (3) Gap analysis output comparing your current vendor contract requirements against the controls that would have been required to detect or limit this breach — specifically: Was breach notification required?

Was MFA required on Foxconn systems handling your data? Was data retention limited? (4) Documentation of any proprietary data categories alleged in the Nitrogen group's claims (product specs for Apple, Google, Nvidia, Dell, Intel, AMD) cross-referenced against what your organization shares with Foxconn — required for both internal risk decisions and potential regulatory disclosure.

Detection Guidance

No confirmed IOCs for this specific Foxconn campaign have been publicly released as of this writing, treat all IOC fields accordingly. For Nitrogen group TTPs generally, focus detection on: (1) Malvertising and SEO poisoning delivery, monitor endpoint telemetry for software installers downloaded from non-allowlisted domains, particularly mimicking legitimate tools (AnyDesk, WinSCP, Notepad++, Python installers); (2) Credential abuse, alert on authentication anomalies against VPN, RDP, and remote access systems, particularly off-hours logins or logins from unfamiliar geographies; (3) Exfiltration patterns, monitor for large outbound data transfers, use of legitimate cloud storage services (MEGA, rclone) for staging, and unusual access to file shares containing sensitive documents; (4) Ransomware precursors, watch for volume shadow copy deletion (vssadmin delete shadows), disabling of backup services, and lateral movement via PsExec or WMI. MITRE techniques to hunt: T1195 (Supply Chain Compromise), T1078 (Valid Accounts), T1041 (Exfiltration Over C2 Channel), T1486 (Data Encrypted for Impact), T1566 (Phishing), T1190 (Exploit Public-Facing Application). If your organization has direct supply chain exposure to Foxconn North America, escalate monitoring priority on EDI and supplier portal integrations immediately.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`none confirmed`	No IOCs for this specific Foxconn-Nitrogen campaign have been publicly released as of this writing. Monitor threat intelligence feeds for Nitrogen group infrastructure updates.	LOW

Framework Mappings

MITRE-ATTACK

- **T1195** — Supply Chain Compromise
- **T1657** — Financial Theft
- **T1078** — Valid Accounts
- **T1486** — Data Encrypted for Impact
- **T1041** — Exfiltration Over C2 Channel
- **T1566** — Phishing
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **SA-9** — External System Services

- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **AC-3** — Access Enforcement
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1195	Supply Chain Compromise	Initial-Access
T1657	Financial Theft	Impact
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration
T1566	Phishing	Initial-Access
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Ransomware hackers claim breach at Foxconn, a major electronics ...	https://techcrunch.com/2026/05/13/ransomware-hackers-claim-breach-a...	T2
Foxconn Attack Highlights Manufacturing's Cyber Crisis	https://www.darkreading.com/cyberattacks-data-breaches/foxconn-atta...	T3
Foxconn confirms cyber attack on North American facilities	https://www.themanufacturer.com/articles/foxconn-confirms-cyber-att...	T3
Foxconn confirms cyberattack after Nitrogen claims Apple, Nvidia ...	https://www.theregister.com/cyber-crime/2026/05/12/foxconn-confirms...	T3
data from Intel, Google, Dell, Nvidia and AMD were stolen. - Reddit	https://www.reddit.com/r/AMD_Stock/comments/1tbybvl/cyberattack_aga...	T3

DISCLAIMER

Generated 2026-05-16 18:52 UTC by TJS Security Command Center