INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-14 06:51 UTC

Nitrogen Ransomware Strikes Foxconn North America Amid Sustained Manufacturing Sector Campaign

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0311
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Foxconn North American manufacturing facilities (specific systems not disclosed publicly)
Published	2026-05-14T08:00:00
Discovery Source	Rss

Executive Summary

The Nitrogen ransomware group has confirmed an attack against Foxconn's North American manufacturing facilities, disrupting operations at one of the world's largest electronics contract manufacturers. Nitrogen is a ransomware-as-a-service operation that combines malvertising-based initial access with data exfiltration before encryption, meaning sensitive operational and business data may have been stolen before systems were locked. As a tier-one supplier to major global technology brands, Foxconn's disruption carries downstream supply chain risk that extends well beyond the company itself.

Technical Analysis

Nitrogen ransomware is a RaaS operation with documented initial access via malvertising and trojanized software installers (T1189, T1204.002), consistent with CWE-494 (Download of Code Without Integrity Check). Post-access tradecraft includes lateral movement via SMB and remote services (T1021, T1021.002), command execution (T1059), privilege escalation via valid account abuse (T1078), and persistence techniques. Data exfiltration (T1041) precedes encryption (T1486), following a double-extortion model. Shadow copy deletion (T1490) limits recovery options. CWE-284 (Improper Access Control) and CWE-269 (Improper Privilege Management) are consistent with observed lateral movement and privilege abuse patterns. No specific CVE is associated with this campaign; the CVSS base score referenced in source data is treated as a contextual severity indicator only, not a formally assigned vulnerability rating. Foxconn has acknowledged the incident; affected systems and full exfiltration scope are not publicly disclosed. Ransomware incidents targeting manufacturing represent a significant portion of 2026 threat activity. No patch is applicable, this is a

campaign-based intrusion, not a vulnerability-specific exploit chain.

Action Checklist

1. Isolate any systems with unexplained outbound connections or anomalous SMB lateral movement activity. Prioritize OT network segments and any systems accessible from the IT network. Disable unused remote access services (RDP, VNC, SMB) at the perimeter and between IT/OT network segments immediately.
2. Hunt for Nitrogen-associated TTPs: review endpoint logs for suspicious installer executions from user-writable directories (AppData, Temp), monitor for Volume Shadow Copy deletion (vssadmin delete shadows, wmic shadowcopy delete), and check for anomalous SMB connections between workstations. Review DNS and proxy logs for traffic to ad networks or domains associated with malvertising delivery. Reference MITRE ATT&CK techniques T1189, T1204.002, T1021.002, T1490.
3. Remove identified trojanized installers and any persistence mechanisms (scheduled tasks, registry run keys, services) dropped post-execution. Reset credentials for any accounts active during the suspected intrusion window. Enforce application allowlisting to block execution from user-writable paths.
4. Restore from clean, offline backups after verifying no persistence remains. Validate OT system integrity before resuming automated production processes. Monitor for re-infection attempts in the 30 days post-recovery, as ransomware operators frequently return to confirmed-access environments.
5. Review and segment IT/OT network boundaries; Nitrogen's manufacturing focus exploits flat or poorly segmented networks. Evaluate software installation controls to prevent user-initiated trojanized installer execution. Conduct a review of privileged account hygiene, CWE-269 exposure indicates privilege escalation paths existed that should not have.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if forensic evidence confirms pre-encryption data exfiltration (sustained large outbound transfers in network logs or Nitrogen's double-extortion leak site lists Foxconn data), as this triggers breach notification obligations under applicable data protection regulations and requires supply chain notification to downstream tier-one customers including major global technology brands.
Recovery Notes	Restore OT systems only after IT network persistence is fully eradicated and IT/OT segmentation controls are verified in place — Nitrogen's manufacturing sector targeting suggests operators understand OT system dependencies and may have staged persistence specifically to survive IT-layer recovery. Monitor all restored endpoints for 30 days post-recovery using Sysmon Event ID 1 alerts scoped to browser-spawned child processes in %AppData% and %Temp%, as Nitrogen RaaS operators are known to reuse confirmed-access environments for follow-on attacks. Validate that all credentials active during the intrusion window have been rotated before reconnecting restored systems to production networks, including service accounts used by OT automation processes.

Forensic Artifacts	Trojanized installer binary in %AppData% or %Temp% with SHA-256 hash — the direct forensic artifact of Nitrogen's malvertising-delivered fake software installer (T1204.002); compute hash and check against VirusTotal before deletion | Sysmon Event ID 1 logs showing process creation chain: browser (chrome.exe/msedge.exe) → installer in %Temp% → post-exploitation tooling — documents the Nitrogen initial access kill chain from malvertising click to payload execution (T1189) | Windows Security Event Log Event ID 4688 (Process Creation) or Sysmon Event ID 1 entries for 'vssadmin delete shadows' and 'wmic shadowcopy delete' — the definitive forensic indicator of Nitrogen's pre-encryption VSS destruction (T1490), with timestamps establishing encryption event timing | DNS debug logs and browser history/cache from patient-zero endpoint — identifies the specific malvertising domain and fake software title (e.g., trojanized AnyDesk, WinSCP, or similar legitimately-named installer) used by Nitrogen for initial delivery, enabling downstream IOC generation and blocklisting | Network firewall and NetFlow session logs showing sustained high-volume outbound transfers prior to encryption event — forensic evidence of Nitrogen's pre-encryption data exfiltration stage, critical for determining breach notification scope and identifying which data sets were stolen from Foxconn's manufacturing systems

Per-Action IR Details

Containment — Isolate any systems with unexplained outbound connections or anomalous SMB lateral movement activity. Prioritize OT network segments and any systems accessible from the IT network. Disable unused remote access services (RDP, VNC, SMB) at the perimeter and between IT/OT network segments immediately.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST AC-17 (Remote Access), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Use Windows Firewall with Advanced Security (netsh advfirewall firewall add rule name='Block SMB Outbound' protocol=TCP dir=out remoteport=445 action=block) to block SMB laterally between workstation subnets. For OT isolation, physically disconnect IT-facing switches or null-route the IT/OT VLAN trunk via managed switch CLI. Use Wireshark on a TAP or SPAN port to capture and confirm active SMB session establishment (filter: smb2.cmd == 1) before cutting connectivity so you preserve evidence of lateral movement paths.

Evidence: Before isolating, capture full packet captures of active SMB sessions (Wireshark/tcpdump filter: port 445 or port 139) to document lateral movement source and destination IPs. Pull Windows Security Event Log Event ID 4648 (Explicit Credential Logon) and Event ID 4624 Type 3 (Network Logon) from affected hosts to map which accounts Nitrogen operators used during SMB traversal. Export NetFlow or firewall session logs showing outbound connections — Nitrogen exfiltrates prior to encryption, so large sustained outbound transfers to non-business IPs are key evidence of pre-encryption data theft.

Detection — Hunt for Nitrogen-associated TTPs: review endpoint logs for suspicious installer executions from user-writable directories (AppData, Temp), monitor for Volume Shadow Copy deletion (vssadmin delete shadows, wmic shadowcopy delete), and check for anomalous SMB connections between workstations. Review DNS and proxy logs for traffic to ad networks or domains associated with malvertising delivery. Reference MITRE ATT&CK techniques T1189, T1204.002, T1021.002, T1490.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity's config (github.com/SwiftOnSecurity/sysmon-config — search-retrieved, validate before use) and hunt using Event ID 1 (Process Create) filtering on Image paths containing

\AppData\ or \Temp\ with ParentImage of a browser process (chrome.exe, msedge.exe, firefox.exe) — this directly maps to Nitrogen's malvertising-to-trojanized-installer chain (T1189, T1204.002). For VSS deletion, query Sysmon Event ID 1 for CommandLine containing 'vssadmin' OR 'shadowcopy delete'. For DNS hunting without a SIEM, export Windows DNS debug log (enable via: dnscmd /config /logLevel 0x6101 /logFilePath C:\dns.log) and grep for known ad-network TLDs or newly registered domains. Use Sigma rule 'proc_creation_win_vssadmin_delete_shadows' mapped to T1490 to query collected Sysmon logs with grep or PowerShell: Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Message -match 'vssadmin.*delete'}.

Evidence: Capture Sysmon Event ID 1 logs showing process creation chains originating from browser processes spawning installer executables in %AppData% or %Temp% — this is the forensic signature of Nitrogen's trojanized installer delivery via malvertising (T1204.002). Preserve DNS query logs and browser history/cache from suspected patient-zero endpoints to identify the malvertising domain that delivered the fake installer. Collect Windows System Event Log Event ID 7045 (New Service Installed) and Event ID 4698 (Scheduled Task Created) to identify Nitrogen's post-execution persistence mechanisms. Export VSS snapshot inventory pre-deletion if any snapshots survive: vssadmin list shadows > vss_inventory.txt.

Eradication — Remove identified trojanized installers and any persistence mechanisms (scheduled tasks, registry run keys, services) dropped post-execution. Reset credentials for any accounts active during the suspected intrusion window. Enforce application allowlisting to block execution from user-writable paths.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-7 (Least Functionality), CIS 2.3 (Address Unauthorized Software), CIS 5.3 (Disable Dormant Accounts)

Compensating: Use Autoruns (Sysinternals) to enumerate all persistence locations — export baseline via autorunsc.exe -a * -c -h -o autoruns_output.csv, then diff against a known-clean system to identify Nitrogen-dropped scheduled tasks, registry Run keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run), and services. For application allowlisting without enterprise tooling, use Windows Software Restriction Policies (SRP) or AppLocker (available on Windows 10/11 Pro and Server) to create a deny rule for execution paths matching %APPDATA% and %TEMP% — run gpedit.msc > Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies. Credential reset scope must include all accounts that logged in during the intrusion window per Event ID 4624 logs, not just known-compromised accounts.

Evidence: Before removal, forensically image or copy the trojanized installer binary from %AppData% or %Temp% and compute its SHA-256 hash for IOC sharing and YARA rule development. Export the full registry hive (reg export HKCU\Software\Microsoft\Windows\CurrentVersion\Run runkeys_backup.reg) to document persistence keys before deletion. Preserve scheduled task XML definitions (schtasks /query /fo LIST /v > schtasks_full.txt) to document Nitrogen's persistence mechanism and execution trigger. Capture memory (using WinPmem or similar) from any actively running suspicious processes before termination to recover in-memory payloads, C2 configuration, or encryption keys.

Recovery — Restore from clean, offline backups after verifying no persistence remains. Validate OT system integrity before resuming automated production processes. Monitor for re-infection attempts in the 30 days post-recovery, as ransomware operators frequently return to confirmed-access environments.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Verify backup integrity by restoring to an isolated VM first and running Sysmon + ClamAV (free AV) full scan before promoting to production — ClamAV signatures should be updated immediately prior: freshclam && clamscan -r /path/to/restored/system. For OT system integrity validation without commercial OT security tooling, use file integrity baselines: generate SHA-256 hashes of critical OT application binaries and configuration files pre-incident

(from backup manifest) and compare against restored system using PowerShell: Get-FileHash -Algorithm SHA256 -Path 'C:\OTApp*' | Export-Csv ot_integrity_check.csv. For re-infection monitoring, configure Sysmon Event ID 1 alerting specifically for browser-spawned child processes in user-writable directories — this is the exact chain Nitrogen uses for re-entry via malvertising.

Evidence: Before restoring any system to production, verify that Windows VSS snapshots used as recovery source predate the Nitrogen intrusion by cross-referencing snapshot timestamps against the earliest Sysmon evidence of trojanized installer execution. Confirm no Nitrogen persistence artifacts survive in restored images by running Autoruns against the restored offline registry hive: autorunsc.exe -z -s . Document backup restoration timestamps and the verification checksums used — this supports both operational continuity evidence and any future regulatory or insurance reporting requirements given Foxconn's tier-one supplier status.

Post-Incident — Review and segment IT/OT network boundaries; Nitrogen's manufacturing focus exploits flat or poorly segmented networks. Evaluate software installation controls to prevent user-initiated trojanized installer execution. Conduct a review of privileged account hygiene — CWE-269 exposure indicates privilege escalation paths existed that should not have.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST AC-6 (Least Privilege), NIST SC-7 (Boundary Protection), NIST CM-6 (Configuration Settings), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: For IT/OT segmentation without a commercial micro-segmentation platform, implement VLAN separation at the managed switch layer and enforce firewall ACLs that whitelist only documented, business-required IT-to-OT communication flows — document all rules in a change-controlled spreadsheet. For software installation control, enforce Standard User accounts (remove local admin rights from all non-IT staff) via Group Policy: Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment — remove 'Load and unload device drivers' and restrict 'Install software' to SYSTEM/Administrator only. Conduct privileged account audit using PowerShell: Get-LocalGroupMember -Group 'Administrators' on all endpoints, then cross-reference against HR-approved admin list to identify CWE-269 exposures (accounts with excess privileges that enabled Nitrogen's escalation).

Evidence: Compile the full attack timeline from Sysmon, Windows Security Event Logs, DNS logs, and firewall session logs to document the complete Nitrogen kill chain — from malvertising-delivered installer execution through lateral SMB movement to VSS deletion and encryption — to support lessons-learned, supply chain notification obligations (given Foxconn's role as tier-one supplier), and insurance/regulatory reporting. Preserve all collected forensic artifacts (disk images, memory captures, log exports, network PCAPs) in write-protected, chain-of-custody storage for a minimum of 12 months in case of downstream customer breach notification investigations or legal proceedings.

Detection Guidance

Key behavioral indicators for Nitrogen intrusions: (1) Process execution of legitimate-looking installers (AnyDesk, WinSCP, Notepad++, Python) from user-writable paths (C:\Users*\AppData, C:\Users*\Downloads), cross-reference against software inventory. (2) Scheduled task creation or registry run key modifications following installer execution within the same user session. (3) Lateral SMB connections from non-server workstations, particularly to OT-adjacent segments (T1021.002). (4) Volume Shadow Copy deletion via vssadmin.exe or wmic.exe, high-fidelity indicator, treat as confirmed ransomware staging (T1490). (5) Unusual outbound data transfers to cloud storage or file-sharing endpoints prior to encryption (T1041). SIEM query focus: Windows Event ID 4688 (process creation) filtered for installer names executing from AppData/Temp; Event ID 4624/4625 for credential-based lateral movement; Event ID 7045 for new service installations.

Open-source IOCs may be available through CISA alerts, VirusTotal, and abuse.ch if a formal CISA advisory is issued; commercial threat intelligence feeds are the primary real-time source for Nitrogen indicators. Cross-reference any published indicators against proxy, DNS, and EDR telemetry.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`[not publicly disclosed at time of writing]`	Nitrogen malvertising delivery infrastructure — check commercial threat intelligence feeds for current IOC sets associated with Nitrogen RaaS campaigns	LOW

Framework Mappings

MITRE-ATTACK

- **T1021.002** — SMB/Windows Admin Shares
- **T1204.002** — Malicious File
- **T1059** — Command and Scripting Interpreter
- **T1189** — Drive-by Compromise
- **T1486** — Data Encrypted for Impact
- **T1041** — Exfiltration Over C2 Channel
- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1195** — Supply Chain Compromise
- **T1021** — Remote Services
- **T1490** — Inhibit System Recovery

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)

- **IA-5** — Authenticator Management
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **SA-9** — External System Services
- **SR-2** — Supply Chain Risk Management Plan
- **SR-3** — Supply Chain Controls and Processes
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-3** — Configuration Change Control
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **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
- **CC7.4** — Responds to identified security incidents
- **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
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

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.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1204.002	Malicious File	Execution
T1059	Command and Scripting Interpreter	Execution
T1189	Drive-by Compromise	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access
T1195	Supply Chain Compromise	Initial-Access
T1021	Remote Services	Lateral-Movement
T1490	Inhibit System Recovery	Impact

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/foxconn-atta...	T3
Foxconn confirms cyberattack affecting some North American facilities	https://www.yahoo.com/news/articles/foxconn-confirms-cyberattack-af...	T3
Foxconn Ransomware Attack Shows Nothing Is Safe Forever - WIRED	https://www.wired.com/story/foxconn-ransomware-attack-shows-nothing...	T2

Source	URL	Tier
Foxconn confirms cyberattack impacting North American factories	https://therecord.media/foxconn-confirms-cyberattack-north-american...	T3
Foxconn confirms cyberattack on North American facilities	https://m.economictimes.com/news/international/world-news/foxconn-c...	T3

Generated 2026-05-14 06:51 UTC by TJS Security Command Center