INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-01 07:10 UTC

April 2026 Threat Pulse: Supply Chain Poisoning, 3.4M Exposed Remote Access Servers, and Infostealer Market Reshuffling Demand Immediate SOC Attention

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0248
Type	Threat Campaign
CVE ID	CVE-2019-0708, CVE-2026-24908, CVE-2026-23627
Severity	CRITICAL
CVSS Base Score	9.5
EPSS Score	0.9445 (100th percentile)
Affected Products	TanStack npm package ecosystem, Windows RDP/VNC/RPC servers (including end-of-life Windows versions), OpenEMR, Komari agent, Chrome and Edge browser extensions, VNC servers (unauthenticated exposure)
Published	2026-04-30T09:55:00
Discovery Source	Rss

Executive Summary

In the final week of April 2026, three simultaneous threats converge across developer pipelines, remote access infrastructure, and credential security. A malicious npm package actively exfiltrates environment variables from CI/CD systems; over 3.4 million RDP and VNC servers remain directly internet-exposed, many running unpatched or end-of-life Windows with CVE-2019-0708 (BlueKeep), an unauthenticated remote code execution vulnerability; and Vidar Stealer 2.0 has emerged to fill the operational gap left by disrupted infostealer operations, continuing active credential theft campaigns. Organizations running exposed remote access services, public-facing developer toolchains, or unpatched Windows endpoints face immediate breach risk from all three attack vectors.

Technical Analysis

Three distinct threat vectors are active concurrently:

1. Supply Chain Poisoning, Malicious npm Package (TanStack Brandsquatting)

A threat actor registered an npm package impersonating the legitimate TanStack ecosystem. The package executes environment variable exfiltration at install time, targeting CI/CD pipeline secrets, API keys, and credentials stored in shell environments. MITRE techniques: T1195.002 (Compromise Software Supply Chain), T1552.001 (Credentials in Files), T1071.001 (Web Protocols for C2). CWE-494 (Download of Code Without Integrity Check) is the core weakness. Confirmed affected scope: any developer or automated pipeline that installed the malicious package. No CVE assigned to this package at analysis time.

2. Mass Remote Access Exposure, RDP/VNC Internet-Facing Servers

Internet-exposed RDP and VNC servers number in the millions according to public scanning reports (Shadowserver, Shodan, Censys). A material subset runs unauthenticated VNC or end-of-life Windows versions. CVE-2019-0708 (BlueKeep), CVSS 9.8 per NVD, is an unauthenticated RCE vulnerability via RDP on Windows 7, Windows Server 2008 R2, and earlier systems. Exploitation is wormable with no user interaction required (AV:N/AC:L/PR:N/UI:N). MITRE techniques: T1190 (Exploit Public-Facing Application), T1021.001 (Remote Desktop Protocol), T1021.005 (VNC), T1068 (Exploitation for Privilege Escalation). CVE-2026-24908 and CVE-2026-23627 are referenced in source material but technical details are not yet available in NVD at analysis time. Organizations should monitor NVD updates for these 2026-series CVEs. Recommendations in this brief focus on CVE-2019-0708, which is confirmed and actively exploited.

3. Infostealer Ecosystem Reshuffling, Vidar Stealer 2.0

Following law enforcement disruption of Lumma Stealer and Rhadamanthys operations in early 2026, Vidar Stealer 2.0 has emerged as the dominant commodity infostealer in active use. Vidar is distributed via phishing (T1566.002), browser extension abuse (T1176), and malvertising. It targets browser-stored credentials (T1555), session cookies (T1539), and keylogging (T1056). CWE coverage: CWE-613 (Insufficient Session Expiration), CWE-285 (Improper Authorization). The transition to a new dominant stealer increases detection gap risk for SOC teams tuned to Lumma/Rhadamanthys IOC signatures and infrastructure.

CVE Verification Status:

- CVE-2019-0708 (BlueKeep): CVSS 9.8, confirmed in NVD, patched May 2019 via Microsoft Security Advisory.

- CVE-2026-24908 and CVE-2026-23627: Referenced in source data; specific technical details pending NVD publication. Do not rely on these CVEs for detection or containment guidance until NVD details are published.

Action Checklist

1. Step 1: Containment, Immediately audit all npm packages installed in CI/CD pipelines and developer environments over the past 30 days. Flag any package name resembling 'tanstack' that is not the verified @tanstack scope on npmjs.com. Revoke and regenerate all secrets, API keys, and credentials that were stored in pipeline environment variables and may have been exfiltrated. Block outbound connections from build systems to unrecognized external IPs at the network boundary.
2. Step 2: Detection, Run Shadowserver's RDP/VNC exposure check against your external IP ranges (https://www.shadowserver.org/what-we-do/network-reporting/). Query firewall and SIEM logs for inbound TCP 3389 (RDP) and TCP 5900 (VNC) connections from external sources NOT in your allowlisted VPN or jump-box IP ranges; establish a baseline to avoid false positive fatigue. Search EDR telemetry for event IDs 4624/4625 (logon success/failure) on RDP with external source IPs. For Vidar Stealer 2.0: review browser process trees for unexpected child processes, check for PowerShell execution (T1059.001) spawned from browser processes, and update threat intelligence feeds, existing Lumma/Rhadamanthys signature sets will not reliably detect Vidar 2.0 variants.

3. Step 3: Eradication, For BlueKeep (CVE-2019-0708): apply Microsoft Security Update KB4499175 (Windows 7 and Windows Server 2008 R2) or KB4499164 (Windows Server 2008 SP2), available via Microsoft Update Catalog. For end-of-life systems that cannot be patched: isolate immediately and begin decommission or upgrade planning. Disable RDP on all systems that do not require it. Enable Network Level Authentication (NLA) on all RDP-enabled systems as a compensating control. For exposed VNC: require authentication on all VNC instances or take offline. For the malicious npm package: remove from package.json, clear npm cache, purge node_modules, and rerun install from verified lock files only.

4. Step 4: Recovery, After patching, re-scan exposed IP ranges to confirm RDP/VNC ports are no longer directly reachable. Validate NLA is enforced via Group Policy (Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services). Rotate all secrets and tokens exposed to CI/CD pipeline environments. Re-run build pipelines from clean environments using verified package hashes. Monitor authentication logs for 30 days post-remediation for anomalous RDP logon patterns. For Vidar Stealer 2.0 exposure: assume browser-stored credentials are compromised and force password resets for any accounts accessible from affected endpoints.

5. Step 5: Post-Incident, This convergence exposes three recurring control gaps: (a) lack of npm package integrity verification in CI/CD pipelines, implement Sigstore or npm provenance attestation; (b) unmanaged internet-facing remote access, enforce zero-trust remote access (ZTNA) or VPN-gating for RDP/VNC, eliminating direct internet exposure; (c) signature lag on commodity stealer transitions, establish a process to refresh infostealer detection content within 72 hours of major law enforcement disruption events. Map these gaps to NIST CSF PR.AC (Access Control), PR.DS (Data Security), and DE.CM (Continuous Monitoring) and include in next GRC review cycle.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and legal counsel immediately if: evidence of successful BlueKeep (CVE-2019-0708) RCE is confirmed on any internet-facing host (kernel crash dumps with MS_T120 channel artifacts + subsequent unauthorized service installation Event ID 7045), if CI/CD environment variable exfiltration by the malicious TanStack npm package included secrets granting access to production systems or customer data (triggering breach notification assessment under applicable regulations including HIPAA if OpenEMR is in scope per the affected systems list), or if Vidar Stealer 2.0 credential theft is confirmed on endpoints with access to privileged accounts or PII/PHI repositories.
Recovery Notes	Post-containment, treat all CI/CD-derived secrets as fully compromised regardless of confirmed exfiltration evidence — the malicious npm postinstall hook had access to the full process environment, and absence of observed exfiltration does not equal absence of exfiltration given the 30-day exposure window. For BlueKeep-patched systems, conduct a post-patch authenticated vulnerability scan using OpenVAS or Nessus Essentials (free tier) within 24 hours of patch application to confirm KB4499175/KB4499164 resolved the CVE-2019-0708 finding, and retain scan results as compliance evidence. Monitor RDP authentication (Event ID 4624 LogonType=10) and new service installation (Event ID 7045) for a minimum of 30 days post-remediation, with particular attention to off-hours logons from previously observed external source IP ranges, as BlueKeep exploitation may have established persistence mechanisms that survive patching.

Forensic Artifacts	Windows kernel crash dump files (%SystemRoot%\Minidump*.dmp, %SystemRoot%\MEMORY.DMP) from internet-facing RDP hosts — BlueKeep (CVE-2019-0708) exploits a use-after-free in the MS_T120 channel of the RDP pre-authentication stack, frequently producing a BSoD with heap spray artifacts in pool memory before successful RCE; presence of crash dumps correlated with inbound TCP 3389 connection spikes is a primary BlueKeep exploitation indicator | CI/CD pipeline execution logs and npm postinstall script output from the build step that installed the malicious TanStack-named package — the exfiltration mechanism is a lifecycle hook that reads process.env and transmits environment variables via HTTP POST to a hardcoded C2; logs will contain the outbound HTTP request or DNS resolution if network logging was enabled on the build node | Chrome and Edge browser credential store SQLite files from Vidar Stealer 2.0-affected endpoints: '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data' and '%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Login Data' — Vidar accesses these files directly using SQLite queries; LastWriteTime and LastAccessTime metadata on these files will reflect unauthorized access timestamps that precede the stealer's process termination | Sysmon Event ID 1 (Process Create) and Event ID 3 (Network Connection) logs showing chrome.exe or msedge.exe spawning powershell.exe or cmd.exe child processes (MITRE T1059.001) with subsequent outbound connections to non-CDN external IPs — this process tree pattern is the primary Vidar Stealer 2.0 behavioral indicator given its use of browser process injection or malicious extension abuse as an initial execution vector | Firewall and perimeter flow logs for inbound TCP 3389 and TCP 5900 showing source IP volume, connection frequency, and connection duration distribution over the 72-hour window prior to detection — BlueKeep mass scanning produces high-frequency single-packet or short-duration connection attempts across sequential or randomized destination IPs, distinguishable from legitimate RDP sessions which establish sustained connections; unauthenticated VNC (TCP 5900) logs showing sessions with zero authentication exchange (no VNC handshake security-type negotiation) confirm unauthenticated exposure exploitation

Per-Action IR Details

Step 1: Containment — Immediately audit all npm packages installed in CI/CD pipelines and developer environments over the past 30 days. Flag any package name resembling 'tanstack' that is not the verified @tanstack scope on npmjs.com. Revoke and rotate all environment variables and secrets stored in affected pipeline environments. Block outbound connections from build systems to unrecognized external IPs at the network boundary.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems and prevent further damage while preserving evidence; CSF [RS] — execute IR plan, contain, communicate, mitigate

Controls: NIST IR-4 (Incident Handling) — implement containment as part of incident handling capability, NIST SI-3 (Malicious Code Protection) — detect and contain malicious code introduced via supply chain vector, NIST CM-3 (Configuration Change Control) — flag unauthorized package introductions as unapproved configuration changes, CIS 2.3 (Address Unauthorized Software) — ensure unauthorized packages (malicious TanStack typosquats) are removed from enterprise assets, CIS 4.4 (Implement and Manage a Firewall on Servers) — enforce outbound firewall rules on build servers to block C2 exfiltration channels

Compensating: Use 'npm ls --all 2>/dev/null | grep -i tanstack' across all pipeline nodes to enumerate installed packages; cross-reference against 'npm view @tanstack/ dist-tags' to confirm legitimate scoped publisher. For secret rotation without a secrets manager, use 'printenv | grep -iE "token|secret|key|password|api"' to enumerate exposed variables, then immediately update each upstream service credential. Block outbound build-server traffic using host-based iptables rules: 'iptables -A OUTPUT -p tcp --dport 80 -d <flagged_ip> -j DROP' for flagged IPs identified from 'ss -tnp' or 'netstat -tnp' captured at time of detection.

Evidence: Capture BEFORE rotating secrets or removing packages: (1) full 'npm ls --all' output and package-lock.json/yarn.lock snapshots from each affected pipeline node to document the malicious package's dependency chain; (2) CI/CD job execution logs (GitHub Actions logs, Jenkins build console output, GitLab CI job traces) showing the install step that introduced the malicious TanStack-named package — these logs will contain the exact npm registry URL resolved and any stderr output from postinstall hooks; (3) network flow logs or pcap from the build server's outbound interface during the last 30-day window, filtering on the build server IP as source — the exfiltration payload (environment variables) was transmitted outbound, so capture destination IPs/domains and payload size; (4) /proc//environ snapshots or OS-level process environment dumps for any node processes spawned by the malicious postinstall script; (5) shell history files (~/.bash_history, ~/.zsh_history) on build nodes for any commands executed by the malicious package's lifecycle hooks.

Step 2: Detection — Run Shadowserver's RDP/VNC exposure check against your external IP ranges (https://www.shadowserver.org/what-we-do/network-reporting/). Query firewall and SIEM logs for inbound TCP 3389 (RDP) and TCP 5900 (VNC) connections from external sources. Search EDR telemetry for event IDs 4624/4625 (logon success/failure) on RDP with external source IPs. For Vidar Stealer 2.0: review browser process trees for unexpected child processes, check for PowerShell execution (T1059.001) spawned from browser processes, and update threat intel feeds — existing Lumma/Rhadamanthys signature sets will not reliably detect Vidar 2.0 variants.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across log sources, prioritize incidents by scope and impact; CSF [DE] — monitor, detect, analyze, correlate, and triage adverse events

Controls: NIST SI-4 (System Monitoring) — monitor for BlueKeep exploitation attempts on RDP (TCP 3389) and unauthenticated VNC (TCP 5900) exposure, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review Windows Security Event Log for Event IDs 4624/4625 indicating external RDP authentication attempts, NIST AU-2 (Event Logging) — ensure RDP authentication events and network flow logs are captured for analysis, NIST IR-5 (Incident Monitoring) — track and document RDP/VNC exposure findings and Vidar Stealer 2.0 behavioral indicators across affected endpoints, CIS 8.2 (Collect Audit Logs) — ensure audit logs for RDP logon events and browser process telemetry are collected and centrally accessible, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — use Shadowserver exposure data as an input to identify unmanaged internet-facing RDP/VNC assets

Compensating: Without SIEM/EDR: on each Windows RDP-enabled host, run 'Get-WinEvent -LogName Security -FilterXPath "*[System[(EventID=4624 or EventID=4625)] and EventData[Data[@Name=\"LogonType\"]=\"10\"]]" | Select-Object TimeCreated, Message | Export-Csv rdp_logons.csv' — LogonType 10 is RDP-specific. For Vidar Stealer 2.0 browser process tree detection without EDR, deploy Sysmon with SwiftOnSecurity's base config and query Event ID 1 (Process Create) filtering ParentImage containing 'chrome.exe' or 'msedge.exe' with Image containing 'powershell.exe' or 'cmd.exe'. For VNC unauthenticated exposure, run 'nmap -sV -p 5900 --script vnc-info ' from an external vantage point to confirm authentication enforcement. Register for free Shadowserver organizational membership to receive automated daily reports on your ASN's exposed services.

Evidence: Capture BEFORE any blocking or isolation actions: (1) Windows Security Event Log exports (Event IDs 4624, 4625, 4648) from all internet-facing RDP hosts filtered to LogonType=10, preserving source IP fields — BlueKeep exploitation (CVE-2019-0708) targets the pre-authentication RDP protocol stack and may appear as anomalous connection attempts followed by system crashes or Event ID 7045 (new service installed) post-exploitation; (2) Windows System Event Log for Event ID 6008 (unexpected shutdown) and Application Log for Event ID 1000/1001 (application crash/Windows Error Reporting) on RDP hosts — BlueKeep causes a kernel-level use-after-free that frequently produces a BSoD/crash dump before achieving RCE; (3) for Vidar Stealer 2.0, collect browser credential store file paths before they are wiped — Chrome: '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data', Edge: '%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Login Data' — these SQLite files will show last-accessed timestamps indicating stealer activity; (4) Sysmon Event ID 3 (Network Connection) logs showing browser processes (chrome.exe, msedge.exe) making outbound connections to non-Google/Microsoft IPs, consistent with Vidar 2.0 C2 exfiltration; (5) firewall/perimeter logs showing inbound connection volume and source IP distribution for TCP 3389 and TCP 5900 over the prior 72 hours — mass BlueKeep scanning produces characteristic port-sweep patterns from known exploit framework source ranges.

Step 3: Eradication — For BlueKeep (CVE-2019-0708): apply Microsoft patch MS19-0708 (KB4499175 for Windows 7/2008 R2, KB4499164 for Windows 2008 SP2) — available via Microsoft Update Catalog. For end-of-life systems that cannot be patched: isolate immediately and begin decommission or upgrade planning. Disable RDP on all systems that do not require it. Enable Network Level Authentication (NLA) on all RDP-enabled systems as a compensating control. For exposed VNC: require authentication on all VNC instances or take offline. For the malicious npm package: remove from package.json, clear npm cache, purge node_modules, and rerun install from verified lock files only.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: remove threat from environment, remediate vulnerabilities that enabled the incident, verify eradication completeness; CSF [RS] — remove threat, verify eradication

Controls: NIST SI-2 (Flaw Remediation) — apply KB4499175 and KB4499164 to remediate CVE-2019-0708 on Windows 7/2008 R2 and 2008 SP2 respectively; identify and remediate EoL systems that cannot receive patches, NIST CM-7 (Least Functionality) — disable RDP on systems that do not require it as part of reducing attack surface, NIST SI-3 (Malicious Code Protection) — purge malicious TanStack-named npm packages from all pipeline environments and verify clean reinstall from verified lock files, NIST IA-3 (Device Identification and Authentication) — enforce Network Level Authentication (NLA) on RDP to require device-level credential verification before session establishment, CIS 7.3 (Perform Automated Operating System Patch Management) — apply BlueKeep patches KB4499175/KB4499164 through patch management process; flag EoL systems as unmanageable via standard patching, CIS 7.4 (Perform Automated Application Patch Management) — enforce npm package integrity via verified lock files as part of application-level patch management, CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software) — audit VNC instances for default or null authentication configurations and enforce password requirements

Compensating: For EoL Windows systems that cannot receive KB4499175/KB4499164: implement host-based firewall rules to block all inbound TCP 3389 — 'netsh advfirewall firewall add rule name="Block RDP Inbound" dir=in action=block protocol=tcp localport=3389' — and place the host on an isolated VLAN with no internet routing. For NLA enforcement without Group Policy infrastructure, set the registry key directly: 'reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v UserAuthentication /t REG_DWORD /d 1 /f'. For npm eradication on CI/CD nodes without package management tooling, run 'npm cache clean --force && rm -rf node_modules package-lock.json && npm install --ignore-scripts' — the '--ignore-scripts' flag prevents malicious postinstall hooks from re-executing during the clean reinstall. Verify package integrity with 'npm audit' and cross-check each dependency's SHA-512 integrity hash in package-lock.json against npmjs.com registry entries.

Evidence: Capture BEFORE patching or removing packages — eradication destroys forensic state: (1) full memory dump from any RDP host suspected of BlueKeep exploitation using WinPmem ('winpmem_mini_x64.exe memdump.raw') — CVE-2019-0708 exploitation leaves artifacts in kernel memory pool allocations related to the MS_T120 channel use-after-free; (2) Windows crash dump files (%SystemRoot%\Minidump*.dmp and %SystemRoot%\MEMORY.DMP) from affected RDP hosts — BlueKeep frequently triggers BSoD prior to successful RCE, preserving heap spray artifacts; (3) registry export of 'HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server' to document current RDP configuration state, NLA setting, and any attacker-modified values before patching overwrites them; (4) for the malicious npm package, preserve the full contents of node_modules// including package.json, any .js files, and postinstall scripts — these contain the exfiltration logic and C2 destination hardcoded or obfuscated within the lifecycle hook; (5) npm-debug.log and CI/CD runner logs from the install step that introduced the malicious package, preserving the registry resolution URL and any HTTP requests made during postinstall execution.

Step 4: Recovery — After patching, re-scan exposed IP ranges to confirm RDP/VNC ports are no longer directly reachable. Validate NLA is enforced via Group Policy (Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services). Rotate all secrets and tokens exposed to CI/CD pipeline environments. Re-run build pipelines from clean environments using verified package hashes. Monitor authentication logs for 30 days post-remediation for anomalous RDP logon patterns. For Vidar Stealer 2.0 exposure: assume browser-stored credentials are compromised and force password resets for any accounts accessible from affected endpoints.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: execute recovery plan, restore systems to normal operations, verify integrity of restored systems, and monitor for recurrence; CSF [RC] — execute recovery plan, restore, verify, communicate

Controls: NIST SI-2 (Flaw Remediation) — verify patch application via post-remediation scan confirming CVE-2019-0708 is no longer exploitable on previously exposed RDP hosts, NIST AU-6 (Audit Record Review, Analysis, and Reporting) — monitor Windows Security Event Log for anomalous RDP Event ID 4624 (LogonType=10) patterns for 30 days post-remediation as indicator of persistent access or re-exploitation, NIST IA-5 (Authenticator Management) — force rotation of all CI/CD secrets, API tokens, and credentials exfiltrated by the malicious TanStack-named npm package; force password resets for all accounts accessible from Vidar Stealer 2.0-affected endpoints, NIST SI-7 (Software, Firmware, and Information Integrity) — verify npm package integrity via SHA-512 hash comparison in package-lock.json before re-running production build pipelines, NIST CP-4 (Contingency Plan Testing) — validate that recovery procedures restored systems to verified clean state, not merely operational state, CIS 7.2 (Establish and Maintain a Remediation Process) — document post-patch rescan results as evidence of remediation closure for BlueKeep-exposed systems, CIS 5.3 (Disable Dormant Accounts) — during 30-day monitoring window, identify and disable any RDP accounts showing no legitimate activity that may indicate attacker-created persistence

Compensating: Post-patch RDP/VNC exposure validation without commercial scanner: use 'nmap -sV -p 3389,5900 --script rdp-enum-encryption,vnc-info -oN rdp_vnc_postscan.txt' from an external IP to confirm ports are unreachable or NLA-enforced. For 30-day RDP authentication monitoring without SIEM, schedule a daily PowerShell task on each RDP host: 'Get-WinEvent -LogName Security -FilterXPath '*[System[(EventID=4624) and TimeCreated[@SystemTime >= \"$(Get-Date (Get-Date).AddDays(-1) -Format s)Z\"]]]' | Where-Object {$_.Message -match "Logon Type:\s+10"} | Export-Csv -Append daily_rdp_monitor.csv'. For Vidar Stealer 2.0 credential compromise scope assessment without EDR, run 'Get-ChildItem -Path "$env:LOCALAPPDATA\Google\Chrome\User Data\Default" -Filter "Login Data" | Select-Object LastWriteTime' to identify recent stealer access timestamps on affected endpoints.

Evidence: Capture during recovery to establish clean baseline and support post-incident review: (1) post-patch Nmap scan output confirming TCP 3389 and TCP 5900 are no longer exposed or are NLA-enforced — this becomes the documented remediation evidence artifact for compliance records (NIST AU-11); (2) Group Policy Results report ('gpresult /H gpo_report.html') from representative RDP-enabled hosts confirming NLA policy application under 'Computer Configuration > Windows Components > Remote Desktop Services'; (3) npm 'package-lock.json' integrity diff between pre-incident and post-clean-install states, capturing the SHA-512 hash change for the removed malicious package and its dependency subtree; (4) CI/CD pipeline execution logs from the first clean post-incident build run, confirming '--ignore-scripts' flag enforcement and absence of unexpected outbound network connections during install; (5) password reset completion audit log from IAM/IdP system (Active Directory event ID 4723/4724 or equivalent) documenting forced resets for all accounts accessible from Vidar Stealer 2.0-compromised endpoints, establishing a documented remediation timeline.

Step 5: Post-Incident — This convergence exposes three recurring control gaps: (a) lack of npm package integrity verification in CI/CD pipelines — implement Sigstore or npm provenance attestation; (b) unmanaged internet-facing remote access — enforce zero-trust remote access (ZTNA) or VPN-gating for RDP/VNC, eliminating direct internet exposure; (c) signature-lag on commodity stealer transitions — establish a process to refresh infostealer detection content within 72 hours of major law enforcement disruption events. Map these gaps to NIST CSF PR.AC (Access Control), PR.DS (Data Security), and DE.CM (Continuous Monitoring) and include in next GRC review cycle.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review, update IR plan and detection capabilities, share intelligence, and implement improvements to prevent recurrence; CSF [GV, ID] — update policies, improve detection, share intelligence

Controls: NIST IR-4 (Incident Handling) — update incident handling procedures to address supply chain package poisoning, mass RDP/VNC exposure, and commodity stealer variant transitions as distinct incident categories, NIST IR-8 (Incident Response Plan) — revise IR plan to incorporate 72-hour detection content refresh SLA triggered by major infostealer law enforcement disruption events (e.g., LockBit, Lumma takedowns precipitating Vidar 2.0 market entry), NIST SI-7 (Software, Firmware, and Information Integrity) — implement npm Sigstore provenance attestation or

package integrity verification (SHA-512 hash pinning in package-lock.json) as a preventive control for future supply chain poisoning attempts targeting CI/CD pipelines, NIST SI-5 (Security Alerts, Advisories, and Directives) — establish process to receive and act on CISA KEV additions and threat intel feeds within defined SLAs, specifically for commodity stealer variant transitions, NIST RA-3 (Risk Assessment) — document residual risk from EoL Windows systems unable to receive CVE-2019-0708 patches and include in formal risk register with compensating control documentation, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — update vulnerability management process to include internet-facing service exposure scanning (RDP TCP 3389, VNC TCP 5900) as a recurring discovery control, not a reactive measure, CIS 2.2 (Ensure Authorized Software is Currently Supported) — formally designate EoL Windows versions (7, 2008 R2, 2008 SP2) as unsupported in the software inventory and initiate decommission or upgrade tracking, CIS 6.3 (Require MFA for Externally-Exposed Applications) — include RDP/VNC gateway enforcement of MFA as a post-incident improvement action item for the next GRC review cycle

Compensating: For organizations without a formal threat intel program to achieve 72-hour Vidar 2.0 detection refresh: subscribe to free OSINT feeds — abuse.ch URLhaus, Feodo Tracker (for C2 IOCs), and the MITRE ATT&CK STIX feed — and create a weekly cron job to pull updated YARA rules from the Malpedia Vidar family page into local detection tooling. For npm supply chain integrity without Sigstore infrastructure, enforce 'npm ci' (instead of 'npm install') in all CI/CD pipelines — 'npm ci' requires a committed package-lock.json and fails if the lock file is inconsistent with package.json, preventing opportunistic package substitution. For ZTNA without budget, implement SSH tunneling or WireGuard (free, open-source) as a VPN gateway in front of all RDP endpoints, removing direct TCP 3389 internet exposure entirely: 'wg-quick up wg0' with a config restricting AllowedIPs to the RDP host subnet.

Evidence: Collect for lessons-learned documentation and GRC review: (1) timeline artifact mapping the three convergent threats — malicious npm package introduction date from CI/CD logs, Shadowserver first-alert date for RDP/VNC exposure, and Vidar Stealer 2.0 first detection date from threat intel feeds — to quantify mean time to detect (MTTD) for each threat vector; (2) asset inventory gap report identifying all EoL Windows systems (Windows 7, Server 2008/2008 R2) still in production that cannot receive CVE-2019-0708 patches, as direct input to NIST RA-3 risk register update; (3) npm package audit history from the CI/CD platform showing all packages installed in the 30-day window prior to detection, preserving the supply chain attack entry point for root cause documentation; (4) Vidar Stealer 2.0 IOC set (C2 domains, process tree patterns, credential store access timestamps) collected during detection phase, formatted as STIX 2.1 for sharing with sector ISACs and updating internal detection rules; (5) GRC control gap mapping document cross-referencing the three identified gaps (npm integrity, RDP exposure, stealer signature lag) against current control inventory, quantifying the delta between existing control state and target state for the next audit cycle.

Detection Guidance

RDP/VNC Exposure (CVE-2019-0708/BlueKeep):

- External exposure: query Shadowserver exposure reports for your ASN or IP ranges; cross-reference with Shodan or Censys scans for port 3389/5900 on your public IPs.

- SIEM query: filter firewall logs for inbound ACCEPT on TCP/3389 or TCP/5900 from src_ip NOT in [RFC1918 ranges] AND NOT in [allowlisted VPN/jump-box IP ranges]. Baseline noise before alerting to avoid false positive fatigue.

- Windows Security Event Log: Event ID 4625 (failed logon) with Logon Type 10 (RemoteInteractive) from non-RFC1918 source addresses at high frequency signals BlueKeep scanning activity.

- EDR: flag MS-RDPEUDP or RDP pre-authentication traffic patterns from external hosts against unpatched Windows 7/2008 endpoints.

Malicious npm Package (TanStack Brandsquatter):

- Audit npm install logs for package names closely resembling tanstack (e.g., tanstakc, tan-stack, @tanstak/query). Verify all @tanstack/* installs match official registry checksums.

- CI/CD pipeline: alert on unexpected outbound HTTPS POST from build agents to non-allowlisted domains immediately following npm install steps.

- Behavioral: watch for env variable access (process.env enumeration) followed by outbound network calls during build, this is not typical build behavior.

Vidar Stealer 2.0:

- Browser process trees: flag chrome.exe or msedge.exe spawning cmd.exe, powershell.exe, or wscript.exe.

- File system: monitor for creation of .zip or .7z archives in %APPDATA%\Local\Temp containing browser profile directories (Login Data, Cookies, Web Data filenames are Vidar targets).

- Network: alert on POST requests from browser-spawned processes to non-Google/Microsoft domains, particularly to Telegram API endpoints (T1102, Web Service for C2 is a known Vidar exfiltration channel).

- Update threat intelligence IOC feeds immediately; signatures tuned to Lumma Stealer or Rhadamanthys infrastructure will not reliably match Vidar 2.0 C2 domains or hashes.

IOC Availability Notice: IOCs for Vidar 2.0 and the 2026-series CVEs are not provided in primary sources at analysis time. Supplement with live threat intelligence feeds (CrowdStrike, Mandiant, CISA, Shodan) before deploying detection rules.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Not confirmed at analysis time`	Vidar Stealer 2.0 C2 infrastructure — current domains not independently verified in primary sources. Update from live threat intel feeds (e.g., abuse.ch, MISP communities).	LOW
URL	`Not confirmed at analysis time`	Malicious TanStack-brandsquatting npm package exfiltration endpoint — specific URL not disclosed in available sources.	LOW
HASH	`Not confirmed at analysis time`	Vidar Stealer 2.0 payload hashes — not independently verified in primary sources at analysis time. Cross-reference with VirusTotal and threat intel feeds using 'Vidar 2.0' family tag.	LOW

Framework Mappings

MITRE-ATTACK

- **T1176** — Software Extensions
- **T1552.001** — Credentials In Files
- **T1059** — Command and Scripting Interpreter
- **T1539** — Steal Web Session Cookie

- **T1056** — Input Capture
- **T1588.002** — Tool
- **T1059.001** — PowerShell
- **T1566.002** — Spearphishing Link
- **T1071.001** — Web Protocols
- **T1021.001** — Remote Desktop Protocol
- **T1543** — Create or Modify System Process
- **T1555** — Credentials from Password Stores
- **T1195.002** — Compromise Software Supply Chain
- **T1068** — Exploitation for Privilege Escalation
- **T1111** — Multi-Factor Authentication Interception
- **T1548.002** — Bypass User Account Control
- **T1078** — Valid Accounts
- **T1195.001** — Compromise Software Dependencies and Development Tools
- **T1190** — Exploit Public-Facing Application
- **T1021.005** — VNC
- **T1102** — Web Service

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **SA-9** — External System Services
- **SR-3** — Supply Chain Controls and Processes
- **AC-6** — Least Privilege
- **SI-2** — Flaw Remediation
- **AC-2** — Account Management
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-10** — Information Input Validation
- **CM-3** — Configuration Change Control
- **AC-3** — Access Enforcement
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A03:2021** — Injection
- **A08:2021** — Software and Data Integrity Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **16.12** — Implement Code-Level Security Checks
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **15.1** — Establish and Maintain an Inventory of Service Providers

ISO-27001-2022

- **A.8.28** — Secure coding
- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1176	Software Extensions	Persistence
T1552.001	Credentials In Files	Credential-Access
T1059	Command and Scripting Interpreter	Execution
T1539	Steal Web Session Cookie	Credential-Access
T1056	Input Capture	Collection
T1588.002	Tool	Resource-Development
T1059.001	PowerShell	Execution
T1566.002	Spearphishing Link	Initial-Access
T1071.001	Web Protocols	Command-And-Control

Technique ID	Technique Name	Tactic
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1543	Create or Modify System Process	Persistence
T1555	Credentials from Password Stores	Credential-Access
T1195.002	Compromise Software Supply Chain	Initial-Access
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1111	Multi-Factor Authentication Interception	Credential-Access
T1548.002	Bypass User Account Control	Privilege-Escalation
T1078	Valid Accounts	Defense-Evasion
T1195.001	Compromise Software Dependencies and Development Tools	Initial-Access
T1190	Exploit Public-Facing Application	Initial-Access
T1021.005	VNC	Lateral-Movement
T1102	Web Service	Command-And-Control

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/threatsday-bulletin-sms-blaster-b...	T3
CVE-2019-0708 Details - NVD	https://nvd.nist.gov/vuln/detail/cve-2019-0708	T1
Customer guidance for CVE-2019-0708 | Remote Desktop Services ...	https://support.microsoft.com/en-us/topic/customer-guidance-for-cve...	T1
CVE-2019-0708 Vulnerability: Analysis, Impact, Mitigation | Huntress	https://www.huntress.com/threat-library/vulnerabilities/cve-2019-0708	T3
Exploitation of Windows RDP Vulnerability CVE-2019-0708 ...	https://unit42.paloaltonetworks.com/cve-2019-0708-bluekeep/	T3
NVD	https://nvd.nist.gov/vuln/detail/CVE-2019-0708, CVE-2026-24908, CVE...	T1

Generated 2026-05-01 07:10 UTC by TJS Security Command Center