INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-04 06:08 UTC

Dutch Ministry of Finance Treasury Portal Taken Offline After Cyber Breach

DATA BREACH | HIGH | CVSS 7.5

SCC Item ID	SCC-DBR-2026-0078
Type	Data Breach
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Dutch Ministry of Finance, Schatkistbankieren (treasury banking portal)
Discovery Source	Gemini

Executive Summary

The Dutch Ministry of Finance confirmed a cyber breach affecting Schatkistbankieren, its treasury banking portal serving Dutch public sector entities, and took the system offline to contain the incident. Government institutions dependent on the portal for treasury and banking operations lost access; the duration of disruption and scope of data exposure remain undisclosed. The incident signals active targeting of government financial infrastructure and warrants review of similar portal access controls and business continuity plans across public sector organizations.

Technical Analysis

The Dutch Ministry of Finance's Schatkistbankieren portal, a centralized treasury banking system for Dutch public sector entities, was taken offline following confirmation of a cyber incident. No CVE has been assigned. No CWE identifiers have been publicly linked. The ministry has not disclosed the attack vector, threat actor, or technical methodology. Two MITRE ATT&CK techniques are associated with this incident class based on pattern analysis: T1078 (Valid Accounts) and T1190 (Exploit Public-Facing Application). These are assessed as plausible vectors for government portal compromises, not confirmed techniques for this specific incident. CVSS base score is estimated at 7.5 (High) reflecting impact to government financial operations; no vendor CVSS vector has been published. EPSS data is not applicable, no CVE exists. Patch status, affected software versions, and exploitation details are not publicly available as of the item date. Attribution to a specific threat actor has not been made. Confidence in core facts (breach confirmed, portal offline, investigation active) is HIGH; all technical specifics remain LOW confidence pending official disclosure from the ministry or Dutch NCSC.

Action Checklist

1. Containment: If your organization operates public-facing government financial portals or shared treasury systems, review current access logs for anomalous authentication events. Temporarily restrict administrative and privileged access to those systems pending verification. Evaluate whether emergency offline procedures or alternate payment channels are available if a similar takedown becomes necessary.
2. Detection: Query authentication logs for unusual patterns consistent with T1078 (Valid Accounts): off-hours logins, logins from unfamiliar IPs or geolocations, multiple failed authentications followed by success, or service account activity outside normal baselines. For T1190 (Exploit Public-Facing Application), review web application and WAF logs for unexpected payloads, error spikes, or scanning activity against portal endpoints. No specific IOCs have been publicly released for this incident.
3. Eradication: No patch, CVE, or vendor advisory exists for this incident. If you identify suspicious access consistent with T1078, rotate credentials for all affected accounts, revoke active sessions, and audit privilege assignments. If web application exploitation is suspected (T1190), review application logs for injection patterns and validate that WAF rules are current. Await official disclosure from the Dutch Ministry of Finance or Dutch NCSC for specific remediation guidance.
4. Recovery: Before restoring any analogous portal to full operation, validate that authentication controls are functioning as expected, MFA enforcement is confirmed for all privileged accounts, and access logging is intact and centralized. Confirm no unauthorized accounts or backdoors were introduced during the incident window. Monitor for re-exploitation attempts in the 30 days following restoration.
5. Post-Incident: This incident exposes two recurring control gaps in government financial portal environments: insufficient monitoring of valid account misuse (T1078) and inadequate hardening of public-facing application attack surfaces (T1190). Review your organization's controls against NIST SP 800-53 AC-2 (Account Management), AC-17 (Remote Access), SI-10 (Information Input Validation), and SC-7 (Boundary Protection). If a formal business continuity plan for critical financial portal outages does not exist, initiate one. Track Dutch NCSC and ministry disclosures for updated technical details.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if forensic review of authentication logs confirms unauthorized access to treasury transaction records, account balances, or inter-governmental payment data affecting public sector entities, as this would trigger mandatory breach notification obligations under the Dutch Data Protection Act (Wet bescherming persoonsgegevens successor GDPR-NL) and potential reporting to De Nederlandsche Bank (DNB) under DORA financial sector incident notification requirements.

Recovery Notes	Before restoring Schatkistbankieren-equivalent portals, require a signed attestation from system owners confirming MFA is enforced for all accounts, all privileged account passwords have been rotated, and centralized log forwarding is confirmed active and tamper-protected per NIST AU-9 (Protection of Audit Information). Monitor authentication logs daily for the first 30 days post-restoration, specifically watching for the same source IPs, user agents, or account combinations observed in the pre-breach window — adversaries frequently re-attempt access against restored government financial systems within weeks of initial discovery. Coordinate with Dutch NCSC for any threat intelligence on the specific actor or TTPs once official disclosure is made, and update detection rules accordingly before extending portal access back to the full population of dependent public sector entities.
Forensic Artifacts	Web application server access logs (IIS: '%SystemDrive%\inetpub\logs\LogFiles\W3SVC**.log' or Apache/nginx: '/var/log/apache2/access.log', '/var/log/nginx/access.log') — specific to T1190, look for anomalous POST request bodies to authentication and session management endpoints, repeated 400/500 error sequences from single IPs, and User-Agent strings associated with automated scanners (sqlmap, Nikto, Nuclei) in the 14-30 days preceding portal takedown. | Windows Security Event Log entries for Event IDs 4624, 4625, 4648, 4768, 4769 from domain controllers and portal-hosting servers — specific to T1078, the attack signature for valid account misuse in government portal environments is successful logins (4624) from IPs with no prior authentication history following a burst of failed attempts (4625), particularly targeting service accounts or shared administrative accounts used by multiple public sector entities for Schatkistbankieren access. | Active Directory object change logs (Event ID 4720 — account created, 4728/4732/4756 — member added to privileged group, 4738 — account changed) from the domain controller Security Event Log — these identify whether the attacker created backdoor accounts or escalated privileges within the treasury portal's AD tenant during the dwell period between initial access and detection. | WAF or reverse proxy logs in raw format (not aggregated) preserving full HTTP request headers including X-Forwarded-For, Referer, and Cookie fields — for a government financial portal breach, these logs are the primary evidence source to determine whether T1190 exploitation involved SQL injection, authentication bypass, or session token theft, and whether the attacker originated from infrastructure consistent with known threat actor TTPs targeting European government financial systems. | File system integrity artifacts from the web server document root and configuration directories: directory listings with creation and modification timestamps ('Get-ChildItem -Recurse | Select FullName,LastWriteTime,CreationTime'), SHA-256 hashes of all files in the web application root, and IIS applicationHost.config or Apache httpd.conf — these reveal web shell implantation (T1505.003) or configuration tampering that would persist across credential rotation and represent an eradication gap if missed before portal restoration.

Per-Action IR Details

Containment — If your organization operates public-facing government financial portals or shared treasury systems, review current access logs for anomalous authentication events. Temporarily restrict administrative and privileged access to those systems pending verification. Evaluate whether emergency offline procedures or alternate payment channels are available if a similar takedown becomes necessary.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For teams without PAM tooling: export active session data immediately using 'Get-PSSession | Export-Csv sessions.csv' (Windows) or 'who -a > active_sessions.txt' (Linux). Disable privileged accounts in bulk via Active Directory PowerShell: 'Get-ADGroupMember -Identity "Domain Admins" | Disable-ADAccount'. Block administrative interface IPs at the perimeter firewall using deny-all rules on management VLANs. Document all actions with timestamps for chain-of-custody.

Evidence: Before restricting access, capture a full export of active authentication sessions from the treasury portal's identity provider (SAML/OAuth logs if federated, or IIS/Apache auth logs if local). Preserve IIS logs at '%SystemDrive%\inetpub\logs\LogFiles\' or Apache logs at '/var/log/apache2/access.log' — look for admin-panel URI paths, session token reuse across distinct source IPs, and POST requests to authentication endpoints within the 72-hour pre-discovery window. For federated portals, export Azure AD or ADFS sign-in logs filtering on the treasury portal application ID before any account changes invalidate the baseline.

Detection — Query authentication logs for unusual patterns consistent with T1078 (Valid Accounts): off-hours logins, logins from unfamiliar IPs or geolocations, multiple failed authentications followed by success, or service account activity outside normal baselines. For T1190 (Exploit Public-Facing Application), review web application and WAF logs for unexpected payloads, error spikes, or scanning activity against portal endpoints. No specific IOCs have been publicly released for this incident.

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-2 (Event Logging), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without SIEM, run these targeted queries: (1) PowerShell against Windows Security Event Log — 'Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4625,4648,4768,4769)} | Export-Csv auth_events.csv' — then filter in Excel for after-hours timestamps and source IPs outside your known government network ranges. (2) For web logs, use 'grep -E "(40[0-9]|500)" /var/log/apache2/access.log | awk "{print $1}" | sort | uniq -c | sort -rn' to surface IP addresses generating abnormal error rates against portal endpoints. (3) Deploy the public Sigma rule 'win_susp_failed_logon_reasons.yml' via Sigma's standalone converter to generate raw log queries if Splunk/Elastic is unavailable.

Evidence: Preserve the following before any log rotation occurs: Windows Security Event IDs 4624 (successful logon), 4625 (failed logon), 4648 (explicit credential use), 4768/4769 (Kerberos TGT/service ticket requests) from all systems hosting or authenticating to the Schatkistbankieren-equivalent portal. For T1190, capture WAF logs in raw format (not summarized) covering at least 14 days pre-detection, specifically preserving HTTP request bodies, User-Agent strings, and X-Forwarded-For headers — these reveal whether a scanning tool (e.g., Nuclei, SQLMap) or a custom exploit was used against portal login or API endpoints.

Eradication — No patch, CVE, or vendor advisory exists for this incident. If you identify suspicious access consistent with T1078, rotate credentials for all affected accounts, revoke active sessions, and audit privilege assignments. If web application exploitation is suspected (T1190), review application logs for injection patterns and validate that WAF rules are current. Await official disclosure from the Dutch Ministry of Finance or Dutch NCSC for specific remediation guidance.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST AC-2 (Account Management), NIST SI-10 (Information Input Validation), CIS 5.3 (Disable Dormant Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Credential rotation without enterprise PAM: use 'net user /domain' for AD accounts, and script bulk rotation with 'Get-ADUser -Filter * -SearchBase "OU=PortalAdmins,DC=domain,DC=gov" | Set-ADAccountPassword'. For session revocation in web applications without SSO tooling, restart application pools (IIS: 'Restart-WebAppPool -Name ') to invalidate all server-side sessions simultaneously. For WAF rule validation without a commercial WAF, deploy ModSecurity with the OWASP Core Rule Set (free) on an nginx reverse proxy in front of the portal and run OWASP ZAP against a staging clone to verify rule coverage against injection payloads.

Evidence: Before rotating credentials or revoking sessions, snapshot the current state of all privileged account objects in Active Directory using 'Get-ADUser -Filter * -Properties * | Select-Object SamAccountName,LastLogonDate,PasswordLastSet,MemberOf | Export-Csv ad_snapshot.csv' — this preserves pre-eradication privilege assignments for forensic comparison. If web exploitation occurred, extract application memory dumps or capture web server process handles using ProcDump ('procdump.exe -ma w3wp.exe worker_dump.dmp') before restarting IIS, as in-memory artifacts of injected payloads or web shells would be lost on service restart.

Recovery — Before restoring any analogous portal to full operation, validate that authentication controls are functioning as expected, MFA enforcement is confirmed for all privileged accounts, and access logging is intact and centralized. Confirm no unauthorized accounts or backdoors were introduced during the incident window. Monitor for re-exploitation attempts in the 30 days following restoration.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-9 (Protection of Audit Information), NIST AU-11 (Audit Record Retention), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Validate MFA enforcement on the portal without enterprise tooling: attempt login with a privileged test account from a clean browser session and confirm MFA challenge fires before access is granted — document with screen recording. For backdoor detection on web servers, run 'find /var/www/ -name "*.php" -newer /var/www/index.php -mtime -30' (Linux) or use SysInternals Autoruns to check for new IIS ISAPI filters or HTTP modules registered since the estimated compromise date. Establish a 30-day osquery schedule on portal hosts using the 'listening_ports' and 'startup_items' packs to detect new persistence mechanisms introduced post-recovery.

Evidence: Before bringing the portal back online, generate a cryptographic baseline of all web application files and configuration files using 'Get-FileHash -Algorithm SHA256 -Path "C:\inetpub\wwwroot*" -Recurse | Export-Csv baseline_hashes.csv' — this enables integrity verification if re-compromise is suspected post-recovery. Preserve the full directory listing with timestamps ('Get-ChildItem -Recurse | Select-Object FullName,LastWriteTime,CreationTime | Export-Csv file_timeline.csv') to support timeline reconstruction if a web shell was introduced during the incident window.

Post-Incident — This incident exposes two recurring control gaps in government financial portal environments: insufficient monitoring of valid account misuse (T1078) and inadequate hardening of public-facing application attack surfaces (T1190). Review your organization's controls against NIST SP 800-53 AC-2 (Account Management), AC-17 (Remote Access), SI-10 (Information Input Validation), and SC-7 (Boundary Protection). If a formal business continuity plan for critical financial portal outages does not exist, initiate one. Track Dutch NCSC and ministry disclosures for updated technical details.

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 AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST AC-2 (Account Management), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: For teams without a formal GRC platform: conduct the lessons-learned review within 5 business days using a structured after-action template (CISA's free Post-Incident Review template is suitable). Map control gaps directly to CIS Controls v8.1 IG1 safeguards — at minimum validate CIS 6.3 (MFA for external apps), CIS 8.2 (audit log collection), and CIS 4.4 (server firewall) are implemented before the portal class is considered remediated. Subscribe to Dutch NCSC advisories (ncsc.nl) and CISA's Government Facilities Sector alerts for disclosure updates without requiring a threat intelligence platform.

Evidence: Compile the full incident timeline from preserved log artifacts — authentication event exports, WAF logs, AD snapshot CSVs, and file integrity baselines — into a single chronological record before evidence retention windows expire. Retain all raw logs for a minimum of 12 months per NIST AU-11 (Audit Record Retention) to support any regulatory inquiry by Dutch financial supervisory authorities (DNB — De Nederlandsche Bank) given the public-sector financial nature of Schatkistbankieren. Document specifically whether T1078 or T1190 (or both) were confirmed, as

this determination drives whether the root cause was a credential compromise requiring identity controls review or an application vulnerability requiring code-level remediation.

Detection Guidance

No IOCs have been publicly released for this incident. Detection should focus on behavioral indicators consistent with the associated MITRE techniques. For T1078 (Valid Accounts): monitor SIEM for authentication events outside business hours, logins from new or foreign IPs, rapid sequential logins across accounts, and privilege escalation by standard user accounts. For T1190 (Exploit Public-Facing Application): review WAF and application server logs for HTTP 4xx/5xx error spikes, unusual URI patterns, large or malformed POST bodies, and scanning signatures against portal login and API endpoints. If your organization uses Schatkistbankieren or has direct integration with Dutch Ministry of Finance financial systems, treat any anomalous portal activity as potentially related and escalate for investigation. Watch Dutch NCSC (ncsc.nl) and ministry communications for official IOC releases.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
Dutch Ministry of Finance takes treasury systems offline amid cyber ...	https://securityaffairs.com/190204/hacking/dutch-ministry-of-financ...	T3
Could Your Institution Handle a Treasury Cyberattack Like the Dutch ...	https://www.cloaked.com/post/could-your-institution-handle-a-treasu...	T3
Dutch Finance Ministry takes treasury banking portal offline after ...	https://www.bleepingcomputer.com/news/security/dutch-finance-minist...	T3
Dutch Ministry of Finance portal offline after cyberattack | brief	https://www.scworld.com/brief/dutch-ministry-of-finance-portal-offl...	T3
The Dutch Ministry of Finance took some of its systems offline ...	https://www.instagram.com/p/DWjPBoylRzU/	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-04-04 06:08 UTC by TJS Security Command Center