INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-17 13:50 UTC

Ransomware Attacks Claimed Against Italian Seed Producer PSB and Mexican Insurer Grupo 55

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0328
Type	Threat Campaign
Severity	HIGH
Affected Products	Società Produttori Sementi S.p.A. (PSB), Italian agricultural/seed production sector; Grupo 55, Mexican insurance brokerage sector
Published	2026-05-17
Discovery Source	Gemini

Executive Summary

Ransomware operators posted two new victims on May 17, 2026: Società Produttori Sementi S.p.A. (PSB), an Italian agricultural seed producer, and Grupo 55, a Mexican insurance brokerage. These claims originate from attacker-controlled leak sites aggregated by Ransomware.live and remain unverified by the affected organizations. If confirmed, both incidents carry significant risk of operational disruption, data exposure, and supply chain concern given the sectors involved.

Technical Analysis

Source: Ransomware.live, an attacker-operated leak aggregator (T3). Claims are unverified by affected organizations or independent corroboration. No CVE, CWE, CVSS, or EPSS data is available for this item. No ransomware family, threat actor attribution, ransom demand, or confirmed data exfiltration volume has been identified in available source data. MITRE ATT&CK techniques mapped based on ransomware campaign norms: T1486 (Data Encrypted for Impact), T1083 (File and Directory Discovery), T1005 (Data from Local System), T1657 (Financial Theft), T1041 (Exfiltration Over C2 Channel). These mappings reflect the general ransomware TTPs consistent with double-extortion operations; they are not derived from confirmed forensic evidence for these specific incidents. Affected organizations operate in agricultural seed production (PSB, Italy) and insurance brokerage (Grupo 55, Mexico). No patch, vendor advisory, or remediation guidance exists for this campaign at this time.

Action Checklist

1. Step 1: Containment. If your organization has business relationships with PSB or Grupo 55, audit data-sharing interfaces and third-party connections. Restrict inbound/outbound traffic to those partners pending confirmation of incident scope.
2. Step 2: Detection. Search SIEM and EDR telemetry for indicators consistent with double-extortion ransomware: large-scale file renaming events, bulk file reads from sensitive directories, anomalous outbound data transfers, and unexpected use of legitimate tools (e.g., rclone, 7-Zip, Cobalt Strike artifacts). No confirmed IOCs are available for this campaign.
3. Step 3: Eradication. No specific ransomware family or CVE is confirmed; eradication steps cannot be scoped to this campaign. Apply general ransomware hygiene: disable unused remote access paths, enforce MFA on all remote access, audit privileged accounts, and review backup integrity.
4. Step 4: Recovery. Verify backup integrity and offline backup availability for critical systems. If your organization is not a direct victim, validate that shared data with PSB or Grupo 55 has not been exfiltrated. Monitor for leak site updates confirming or expanding disclosed data.
5. Step 5: Post-Incident. Review third-party risk assessments for agricultural supply chain and financial sector partners. Assess whether vendor security questionnaires address ransomware preparedness. Document this event in your threat intelligence log for trend tracking across critical sector targeting.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal, privacy counsel, and executive leadership if internal review confirms your organization shared PII, PHI, financial records, or agricultural supply chain contracts with PSB or Grupo 55 within the past 12 months, as data appearing on the Ransomware.live leak site may trigger GDPR Article 33 (72-hour breach notification to Italian DPA / Garante) or Mexican LFPDPPP notification obligations for your organization as a data controller or processor in those relationships.
Recovery Notes	If your organization is not a direct victim, recovery focus is on validating the integrity of shared data and hardening third-party connection surfaces before resuming normal operations with PSB or Grupo 55. Monitor Ransomware.live and affiliated leak site aggregators daily for a minimum of 30 days post-claim (through mid-June 2026) for publication of exfiltrated data that may include your organization's information — ransomware operators in double-extortion campaigns typically publish data in tranches over days to weeks to maximize pressure. Reassess and formally close this event in your incident log only after both the affected organizations issue public statements confirming or denying the incident scope, or after 60 days with no leak site data publication implicating your organization.

Forensic Artifacts	Firewall and NetFlow logs filtered to PSB (Italian ASN, seed production sector IP ranges) and Grupo 55 (Mexican insurance sector IP ranges) for the 90 days prior to May 17, 2026 — establishes the data exchange window and identifies any anomalous inbound connections from potentially compromised partner infrastructure during the ransomware operator's dwell time. | Windows Security Event ID 4624/4625 (Logon Success/Failure) and 4648 (Explicit Credential Use) filtered to service accounts and API credentials used for B2B integrations with PSB or Grupo 55 — double-extortion operators harvesting credentials from a compromised partner may attempt to pivot into your environment using stolen integration credentials. | DNS query logs and proxy/web gateway logs for resolution of known double-extortion exfiltration infrastructure: Mega.nz (api.mega.co.nz), Rclone-compatible endpoints, and any newly registered domains with agricultural or insurance sector lures — these are staging destinations commonly used by ransomware operators before publishing on leak sites. | Sysmon Event ID 1 (Process Create) and Event ID 3 (Network Connection) logs for rclone.exe, winscp.exe, and WinRAR/7-Zip invocations with command-line arguments referencing sensitive directory paths (e.g., \\finance\, \\contracts\, \\seeds\, \\policies\) — these artifact patterns are specific to the data-staging phase of double-extortion ransomware prior to encryption deployment. | Application integration and API gateway logs (REST API call logs, EDI transaction logs, SFTP transfer logs) documenting all bidirectional data exchanges with PSB and Grupo 55 — these establish the data scope for breach notification assessment under GDPR Article 33 and Mexican LFPDPPP and serve as the factual basis for any regulatory disclosure regarding what organizational data may have been present on compromised partner systems.

Per-Action IR Details

Step 1: Containment — If your organization has business relationships with PSB or Grupo 55, audit data-sharing interfaces and third-party connections. Restrict inbound/outbound traffic to those partners pending confirmation of incident scope.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected third-party connections to prevent lateral propagation from a potentially compromised partner environment into your network.

Controls: NIST IR-4 (Incident Handling), NIST SC-7 (Boundary Protection), NIST CA-3 (Information Exchange), 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 (netsh advfirewall) or iptables/ufw to create explicit DENY rules for PSB IP ranges (seed production B2B integrations often use static IPs — enumerate via DNS lookup on known partner hostnames) and Grupo 55 insurance portal endpoints. On pfSense or OPNsense (free), create an alias for partner CIDRs and toggle to block. Document rule change with timestamp for audit trail. Two-person task: one implements, one verifies with traceroute/ping.

Evidence: Before blocking, capture current NetFlow or firewall connection state logs showing active sessions to PSB and Grupo 55 IP ranges. Export firewall state tables (e.g., 'netstat -an > connections_pre_block.txt' on Windows; 'ss -tulpn > connections_pre_block.txt' on Linux). Preserve DNS query logs (Windows DNS debug log or /var/log/syslog on Linux) for partner FQDNs to establish what your systems were communicating with and when. Screenshot or export any EDR network connection telemetry filtered to partner IP ranges before rule changes alter visibility.

Step 2: Detection — Search SIEM and EDR telemetry for indicators consistent with double-extortion ransomware: large-scale file renaming events, bulk file reads from sensitive directories, anomalous outbound data transfers, and unexpected use of legitimate tools (e.g., rclone, WinRAR, Cobalt Strike artifacts). No confirmed IOCs are available for this campaign.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate behavioral indicators of double-extortion ransomware activity (exfiltration staging followed by encryption) using available telemetry in the absence of confirmed campaign-specific IOCs.

Controls: NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with the SwiftOnSecurity or Olaf Hartong modular config to capture Event ID 1 (Process Create) for rclone.exe, wrar.exe, or any process with 'cobalt' or 'beacon' in the image path. Query with: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Message -match "rclone|wrar|7z"}'. For bulk file rename detection, enable Windows File System auditing (auditpol /set /subcategory:"File System" /success:enable /failure:enable) and query Security Event Log Event ID 4663 (Object Access) filtered on .bak, .sql, .docx renamed to unknown extensions in bulk. Use Sigma rule 'proc_creation_win_rclone_exec.yml' (SigmaHQ) converted to a PowerShell query for no-SIEM environments. For outbound exfiltration detection, run Wireshark or tcpdump on egress points filtering for large sustained flows to cloud storage endpoints (Mega.nz, SFTP to unknown IPs) common in double-extortion staging.

Evidence: Capture Sysmon Event ID 1 logs for process creation of tools used in double-extortion staging: rclone (used to sync data to attacker-controlled cloud storage), WinRAR/7-Zip (used to archive sensitive data pre-exfil), and any process executing from %TEMP%, %APPDATA%, or ProgramData that is not in your software baseline. Collect Windows Security Event ID 4688 (Process Creation with command line) filtered on cmd.exe, powershell.exe, and wscript.exe spawned by network-facing services (IIS, RDP session processes). Export network proxy or DNS logs showing resolution of cloud storage domains (api.mega.co.nz, transfer.sh, or unknown SFTP endpoints) in the 48–72 hours prior to discovery, as double-extortion actors typically exfiltrate before deploying the encryption payload.

Step 3: Eradication — No specific ransomware family or CVE is confirmed; eradication steps cannot be scoped to this campaign. Apply general ransomware hygiene: disable unused remote access paths, enforce MFA on all remote access, audit privileged accounts, and review backup integrity.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: in the absence of confirmed family attribution or IOCs for this campaign, eradication focus shifts to hardening the attack surface exploited by the ransomware kill chain common to agricultural and financial sector targeting — specifically exposed remote access and privileged credential abuse.

Controls: NIST SI-2 (Flaw Remediation), NIST IA-5 (Authenticator Management), NIST AC-6 (Least Privilege), NIST CM-7 (Least Functionality), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Audit exposed remote access with Shodan Community (free) or Censys free tier — search your ASN for RDP (3389), VNC (5900), and SMB (445) exposure, as ransomware operators targeting agricultural and insurance sectors frequently gain initial access via exposed RDP or VPN appliances with weak credentials. Disable RDP via GPO or 'Set-ItemProperty -Path HKLM:\System\CurrentControlSet\Control\Terminal Server -Name fDenyTSConnections -Value 1' on all non-jump-host systems. Audit local administrator accounts with 'net localgroup administrators' on each host and compare against your CIS 5.1 account inventory. Use the free Microsoft LAPS (Local Administrator Password Solution) if not already deployed to eliminate shared local admin passwords that ransomware uses for lateral movement.

Evidence: Before disabling remote access paths, extract Windows Security Event ID 4624 (Successful Logon) and 4625 (Failed Logon) filtered to Logon Type 10 (RemoteInteractive/RDP) and Type 3 (Network) for the past 30 days to establish a baseline of remote access activity and identify anomalous accounts. Pull Active Directory last-logon timestamps for all privileged accounts ('Get-ADUser -Filter {AdminCount -eq 1} -Properties LastLogonDate | Select Name, LastLogonDate') to identify dormant privileged accounts consistent with CIS 5.3 (Disable Dormant Accounts) violations that ransomware operators harvest. Capture VPN authentication logs (if applicable) for the 30 days prior to the partner incident claim date (May 17, 2026) to identify any anomalous authentication from PSB or Grupo 55 network ranges.

Step 4: Recovery — Verify backup integrity and offline backup availability for critical systems. If your organization is not a direct victim, validate that shared data with PSB or Grupo 55 has not been exfiltrated. Monitor for leak site updates confirming or expanding disclosed data.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: verify the integrity of systems and data shared with confirmed ransomware victims (PSB, Grupo 55) before restoring or continuing data exchange, and establish a monitoring cadence for the Ransomware.live leak site to detect disclosed organizational data.

Controls: NIST CP-9 (System Backup), NIST SI-7 (Software, Firmware, and Information Integrity), NIST IR-4 (Incident Handling), NIST AU-11 (Audit Record Retention), CIS 3.4 (Enforce Data Retention), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Verify backup integrity using built-in tools: on Windows, 'wbadmin get versions' and test-restore a non-production file to confirm backup chain is intact and unencrypted. On Linux, verify backup archive hashes against stored checksums ('sha256sum -c backup.sha256'). For leak site monitoring without a commercial threat intel subscription, use RSS feeds from Ransomware.live (free, aggregates leak site posts) or configure a free IFTTT/RSS-to-email alert on Ransomware.live filtered for 'PSB', 'Produttori Sementi', 'Grupo 55', and your own organization's name. Check Have I Been Pwned's organizational lookup for email domains associated with either victim company to detect credential exposure that may affect shared authentication systems.

Evidence: Before resuming any data exchange with PSB or Grupo 55, document the last known-clean data transfer timestamps from firewall logs and application integration logs (EDI, API gateway logs, or SFTP transfer logs) to establish a data exposure window. If your organization shared sensitive data (seed supply contracts, insurance policy data, financial records) with either victim, create an inventory of that data per NIST AU-11 (Audit Record Retention) and assess it against applicable breach notification thresholds — GDPR Article 33 for PSB (Italian entity, EU regulation) and Mexican LFPDPPP (Ley Federal de Protección de Datos Personales en Posesión de los Particulares) for Grupo 55. Preserve any API access logs or partner portal authentication logs showing bidirectional data flow as potential evidence of exfiltrated data scope.

Step 5: Post-Incident — Review third-party risk assessments for agricultural supply chain and financial sector partners. Assess whether vendor security questionnaires address ransomware preparedness. Update threat intelligence log for trend tracking across critical sector targeting.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: integrate the PSB and Grupo 55 ransomware claims into your third-party risk program as a trigger event for reassessing agricultural and insurance sector vendor security posture, and update threat intelligence records to track ransomware operator targeting patterns against these sectors.

Controls: NIST IR-8 (Incident Response Plan), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), NIST CA-3 (Information Exchange), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory)

Compensating: Use free TPRM tooling: the Shared Assessments SIG Lite questionnaire (free download) includes ransomware-specific questions under Domain I (Incident Management) that can be sent to agricultural supply chain and insurance sector vendors. Log this event in a structured threat intelligence register using MISP (free, open-source threat intelligence platform) or a simple STIX 2.1-formatted JSON file tagging the campaign with sectors 'agriculture' and 'insurance', threat type 'ransomware', and actor 'unknown' pending attribution — this enables trend analysis if additional agricultural or insurance sector victims appear on leak sites. Cross-reference against MITRE ATT&CK Enterprise matrix for double-extortion ransomware TTPs: T1486 (Data Encrypted for Impact), T1567.002 (Exfiltration to Cloud Storage), T1078 (Valid Accounts), and T1190 (Exploit Public-Facing Application) to assess detection coverage gaps in your current controls.

Evidence: Compile a post-incident evidence package including: (1) screenshots of the Ransomware.live leak site posts for PSB and Grupo 55 dated May 17, 2026, preserved with URL, timestamp, and hash of the page content as legal-hold artifacts per NIST AU-10 (Non-Repudiation); (2) your organization's third-party data-sharing inventory entries for both entities, establishing what data your organization may have shared; (3) the firewall and DNS log exports from Steps 1 and 2 retained per your AU-11 (Audit Record Retention) policy for a minimum of 1 year given the regulatory exposure (GDPR, LFPDPPP) associated with these victim entities. Document all actions taken in an incident timeline per NIST IR-5 (Incident Monitoring) even if your organization was not directly compromised, as this record supports future regulatory inquiries and third-party risk program audits.

Detection Guidance

No confirmed IOCs are available for this campaign. Detection should focus on behavioral indicators consistent with double-extortion ransomware TTPs. Key signals: (1) T1005/T1083, bulk file enumeration and reads from sensitive directories in short timeframes; query EDR process telemetry for tools like Everything (Windows filesystem search utility), Robocopy, or rclone operating outside normal business hours. (2) T1041, anomalous outbound data transfers, particularly to cloud storage endpoints or uncommon geographies; review firewall and proxy logs for large POST requests or DNS queries to newly registered domains. (3) T1486, file extension mass-change events or shadow copy deletion (vssadmin delete shadows); monitor Windows Event Log 4663 (object access) and PowerShell logs for VSS manipulation. (4) T1657, relevant primarily to Grupo 55 (insurance sector); monitor for unauthorized access to financial records, policyholder databases, or claims systems. Organizations with direct relationships to PSB or Grupo 55 should also monitor for credential-based lateral movement originating from partner network segments.

Framework Mappings

MITRE-ATTACK

- **T1486** — Data Encrypted for Impact
- **T1083** — File and Directory Discovery
- **T1005** — Data from Local System
- **T1657** — Financial Theft
- **T1041** — Exfiltration Over C2 Channel

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

NIST-CSF-2

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

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.34** — Privacy and protection of personal information

- **A.5.21** — Managing information security in the ICT supply chain

SOC2-TSC

- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1486	Data Encrypted for Impact	Impact
T1083	File and Directory Discovery	Discovery
T1005	Data from Local System	Collection
T1657	Financial Theft	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
Ransomware.live	https://www.ransomware.live/	T3
[PDF] PRIVACY POLICY - SOCIETÀ PRODUTTORI SEMENTI S.p.A.	https://www.psbsementi.it/pdf/Privacy_Notice_PSB.pdf	T3
[PDF] The complex regulation of wheat grain storage protein ... - Hal Inrae	https://hal.inrae.fr/hal-02743144v1/file/2014_Ravel_Eucarpia_1.pdf	T3
[PDF] Genetics and Breeding of Durum Wheat - ResearchGate	https://www.researchgate.net/profile/Federico-Vita/publication/2805...	T3
[PDF] Value creation in corporate divestments - Research@CBS	https://research-api.cbs.dk/ws/portalfiles/portal/68334314/1155567_...	T3

Generated 2026-05-17 13:50 UTC by TJS Security Command Center