3C-INT — OPERATIONAL REPORT

Chronus Team

Hunting Playbook

Classification: TLP:WHITE

Origin: Mexico

Associated with: Hacktivist Group — Hacktivism

Playbook updated: 2026-03-27 04:18

PDF generated: 2026-03-27 17:19

Hunting Playbook

> This report translates analytical findings into operational hunting guidance. It is intended to support defenders and analysts in moving from actor context to concrete investigative priorities, review tasks, and environment-specific detection work.

Why This Matters

CHRONUS TEAM represents a practical and disruptive threat to public-sector and institutionally exposed organizations across Latin America. The actor’s apparent focus on government, judicial, health, education, and politically sensitive entities—combined with opportunistic intrusion, data leakage, and public amplification—creates a risk profile where relatively unsophisticated access can still produce significant reputational, operational, and privacy impact.

Who Should Use This Playbook

This playbook is intended for SOC teams, incident responders, threat hunters, CTI analysts, and security leaders supporting public-sector, healthcare, education, judicial, and government-adjacent environments, especially in Latin America. It may also be useful to private organizations exposed to politically motivated leak, defacement, or opportunistic intrusion activity.

What This Playbook Helps Detect

The hunts in this document are designed to support detection and investigation of CHRONUS TEAM-style activity, including abuse of exposed public-facing applications, web compromise and defacement preparation, archive staging, credential misuse, suspicious outbound transfer, and public claim correlation. The objective is not to attribute every alert directly to CHRONUS TEAM, but to identify behaviors and conditions consistent with the actor’s known or assessed operating pattern.

OPERATIONAL NOTE

This edition is focused on practical hunting and investigative follow-through. Broader analytical context, executive framing, and supplementary evidence may be available through the actor profile and related reports within the platform.

Hunting Playbook — Chronus Team

Priority: HIGH (LATAM public-sector) / MEDIUM elsewhere.

Chronus Team is modeled as a **hacktivist / doxing-oriented public-sector cluster**. Hunts focus on **public-facing application abuse, web-content tampering, archive staging, credential misuse, and leak-oriented data movement**, not on niche malware-specific behaviors.

Hunt 1 — Initial access via exposed admin panels and civic portals

Goal: Detect suspicious authentication and access activity on public-sector web applications and admin panels.

Scope: Web access logs, reverse proxy logs, IAM/SSO, VPN, admin portal authentication logs.

Detection logic: Look for repeated failures followed by success, logins from new IP ranges, or successful access to admin paths outside normal maintenance windows.

Example query (Splunk SPL):

```
index=web OR index=auth
| eval uri=coalesce(uri_path, url, request)
| eval outcome=lower(coalesce(status, result, action))
| where like(uri, "%/admin%") OR like(uri, "%/login%") OR like(uri, "%/ckan%")
| stats count values(src_ip) as src_ips values(user) as users values(outcome) as outcomes min(_time) as
first_seen max(_time) as last_seen by host, uri
| where count >= 10
```

Action: Validate whether access is expected, rotate credentials if compromised access is suspected, and inspect follow-on changes to web content and attached storage.

Hunt 2 — Web-shell or scripted execution on internet-facing servers

Goal: Detect command or script execution on public web servers and application hosts.

Scope: EDR, Sysmon, Windows/Linux process logs, web server telemetry.

Detection logic: Flag shell, PowerShell, cmd, bash, python, php, or scripting activity spawned by web-facing processes such as apache, nginx, httpd, php-fpm, w3wp, or IIS worker processes.

Example query (KQL-style):

```
DeviceProcessEvents
| where InitiatingProcessFileName in~ ("w3wp.exe","httpd.exe","nginx.exe","php-cgi.exe","php-
fpm","apache2")
| where FileName in~ ("cmd.exe","powershell.exe","pwsh.exe","bash","sh","python.exe","php.exe")
| project Timestamp, DeviceName, InitiatingProcessFileName, FileName, ProcessCommandLine, AccountName
```

Action: Treat hits as high-priority on internet-facing hosts. Triage for web-shell placement, unauthorized file modifications, and data staging directories.

Hunt 3 — Defacement content deployment

Goal: Identify unauthorized modification of public-facing HTML, template, or CMS content.

Scope: FIM, EDR file events, web deployment logs, source-control and CMS audit trails.

Detection logic: Alert on changes to index files, templates, homepages, or landing pages outside approved release windows, especially where content includes attacker slogans or unusual Spanish-language threat text.

Example query (Splunk SPL):

```
index=fim OR index=edr
| eval file=lower(file_path)
| where like(file, "%index%") OR like(file, "%.html%") OR like(file, "%.php%") OR like(file, "%.tpl%")
| bin _time span=10m
| stats count values(file_path) as paths values(user) as users by host, _time
| where count >= 5
```

Action: Validate against authorized deployments. If unauthorized, take the site into controlled maintenance mode, preserve artifacts, and review concurrent access logs and admin sessions.

Hunt 4 — Large archive creation on public-sector servers

Goal: Detect collection and staging of large data packages prior to publication or exfiltration.

Scope: EDR, Sysmon, Linux audit, file servers, application servers.

Detection logic: Search for zip, rar, 7z, tar, or export utilities creating large archives on servers that do not normally build distribution packages.

Example query (Sigma-style pseudo):

```
selection:
  Image|endswith:
    - '\\7z.exe'
    - '\\rar.exe'
    - '\\tar.exe'
    - '\\powershell.exe'
  CommandLine|contains:
    - '.zip'
    - '.rar'
    - 'Compress-Archive'
condition: selection
```

Action: Review the source directories and file contents. Correlate with outbound connections, admin access, and any public claims made within the same time window.

Hunt 5 — Bulk outbound transfer from government or municipal portals

Goal: Detect exfiltration of staged archives or sensitive datasets to external destinations.

Scope: NetFlow, proxy, firewall, cloud egress logs.

Detection logic: Focus on file/application servers sending unusually large volumes to new destinations over HTTPS, SSH, or web APIs.

Example query (Splunk SPL):

```
index=netflow OR index=proxy
| where dest_port IN (22,80,443)
| eval bytes_out=coalesce(bytes_out, bytes)
| stats sum(bytes_out) as total_out values(dest_ip) as dest_ips values(dest_domain) as dest_domains by
src_ip
| where total_out >= 200000000
```

Action: Validate the destination, block if needed, and inspect the source host for archive creation or export jobs.

Hunt 6 — Unusual database export or bulk query activity

Goal: Detect abnormal data extraction from administrative systems.

Scope: DB logs, SIEM, application audit logs.

Detection logic: Look for off-hours exports, SELECT * patterns against high-value tables, or bulk dump utilities run by unusual accounts.

Example query (KQL-style pseudo):

```
DatabaseAuditLogs
| where Statement has_any ("SELECT *","mysqldump","pg_dump","bcp","EXPORT")
| summarize count(), min(TimeGenerated), max(TimeGenerated) by Account, ClientIP, DatabaseName
```

Action: Confirm whether the account is authorized for bulk export. If not, suspend access and investigate data lineage and destination.

Hunt 7 — Public-sector credential misuse

Goal: Identify likely compromised or shared administrative credentials.

Scope: IAM, VPN, admin portals, local authentication logs.

Detection logic: Detect new geographies, unusual hours, multiple hosts accessed by the same account in short periods, or authentications after long dormancy.

Example query (Splunk SPL):

```
index=auth
| stats values(src_ip) as src_ips values(host) as hosts min(_time) as first_seen max(_time) as last_seen
count by user
| where count >= 5 AND mvcount(hosts) >= 3
```

Action: Force reset and MFA review for suspicious accounts. Pivot to server-side changes and data access activity.

Hunt 8 — Actor-specific defacement or leak-language indicators

Goal: Catch public web content or files containing Chronus-themed strings.

Scope: Web content scanning, WAF logs, FIM, snapshot comparison.

Detection logic: Search for strings such as “HACKED BY CHRONUS”, “Chronus Team”, or Spanish-language mass-leak phrasing in public pages and newly created text files.

Example query (pseudo-code):

```
index=web_content OR index=fim
| where body LIKE "%HACKED BY CHRONUS%"
   OR body LIKE "%Chronus Team%"
   OR body LIKE "%megafiltraci%"
   OR body LIKE "%seguridad%ineficiente%"
```

Action: Confirm compromise, preserve evidence, and review for deeper data theft or archive exposure beyond the visible defacement.

Hunt 9 — External leak monitoring and claim correlation

Goal: Correlate internal anomalies with public leak or defacement claims.

Scope: OSINT monitoring, brand protection, incident response intake.

Detection logic: Monitor public posts, preserved pages, and analyst trackers for references to your organization or peer institutions alongside Chronus Team branding.

Example query (pseudo-code):

```
search_osint("Chronus Team" AND ("[ORG_NAME]" OR "[SECTOR]" OR "[COUNTRY]"))
```

Action: Treat public claims as investigation triggers even when technical confirmation is pending. Start integrity checks and internal breach validation immediately.

Building Block B1 — Tagging sensitive public datasets

Goal: Maintain a reusable list of citizen, employee, police, health, judicial, and tax-linked datasets that must trigger higher-priority alerts.

- Police rosters, personnel records, armament or assignment files.
- Citizen registration, tax, and health-affiliation datasets.
- Municipal open-data backends and administrative export repositories.

Building Block B2 — Baseline for approved web and data operations

Goal: Establish normal release windows, approved export jobs, and expected admin access paths so Chronus-style anomalies stand out quickly.

- Normal deployment windows for public websites and civic platforms.
- Expected volumes and destinations for legitimate data export processes.
- Usual geographies and source systems for public-sector administrators.