INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-07-07 06:49 UTC

Armored Likho Targets Government and Energy Sectors Across Russia, Brazil, and Kazakhstan with BusySnake Infostealer

THREAT CAMPAIGN | CRITICAL | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0630
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	7.5
Affected Products	Government agencies and electrical power entities in Russia, Brazil, and Kazakhstan, specific products/versions not specified in available source material
Published	2026-07-06T17:37:56
Discovery Source	Rss

Executive Summary

A threat actor tracked as Armored Likho has conducted targeted intrusions against government agencies and electrical power sector entities in Russia, Brazil, and Kazakhstan, deploying an infostealer designated BusySnake to harvest credentials and exfiltrate sensitive data. The campaign's deliberate targeting of electrical power sector entities, with potential for OT-adjacent access, indicates an espionage-oriented operation rather than opportunistic financially motivated activity. Attribution and technical details currently rest on a single news outlet source; confidence is rated MEDIUM pending corroboration from a government advisory or vendor PSIRT.

Technical Analysis

Armored Likho is conducting targeted intrusions against government and electrical power sector entities across Russia, Brazil, and Kazakhstan using BusySnake, an infostealer with credential harvesting and data exfiltration capabilities. The campaign maps to multiple MITRE ATT&CK techniques: phishing for initial access (T1566), credential access via keylogging (T1056.001), browser session cookie theft (T1539), credential stores (T1555), and unsecured credentials (T1552), combined with screen capture (T1113) and exfiltration over C2 channel (T1041). Valid accounts (T1078) suggest harvested credentials are being reused for lateral movement or persistence. Relevant CWE weaknesses include insufficiently protected credentials (CWE-522), cleartext storage of sensitive information (CWE-312), and cleartext transmission of sensitive information (CWE-319). No CVE identifiers are associated with this campaign. No specific affected products or software versions are

identified in available source material. Attribution is sourced from Dark Reading (T2); no corroborating CISA advisory, government CERT, or vendor PSIRT has been identified. The CISA advisory listed in sources (aa25-141a) addresses Russian GRU targeting of Western logistics entities and does not directly corroborate this campaign. Technical confidence is MEDIUM.

Action Checklist

1. Preamble: The following steps reference NIST SP 800-53, CIS Controls, and the MITRE D3 Cyber Threat Response framework. Organizations should map these to their own control frameworks and incident response procedures.
2. Step 1: Containment, Audit privileged and service accounts across government and energy-sector systems for signs of unauthorized access or anomalous authentication events; enforce session termination for any accounts exhibiting suspicious behavior. Cross-reference against NIST AC-12 (Session Termination) and NIST AC-2 (Account Management).
3. Step 2: Detection, Hunt for BusySnake-associated behaviors: keylogging artifacts, browser credential store access, unusual outbound data transfers, and screen capture activity. Review endpoint logs for access to browser credential stores and Windows Credential Manager. Monitor for T1056.001, T1539, T1555, and T1113 indicators using available EDR telemetry. Enable and review audit logs per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). No confirmed IOCs are available from current source material.
4. Step 3: Eradication, Rotate all credentials on systems within the targeted sectors, prioritizing service accounts and accounts with access to OT-adjacent environments, per D3-CRO (Credential Rotation). Enforce MFA on all remote access and administrative accounts per NIST IA controls and CIS 6.3, 6.4, 6.5. Remove any unauthorized software identified during investigation per CIS 2.3 (Address Unauthorized Software).
5. Step 4: Recovery, Validate that credential rotation is complete and that no residual unauthorized sessions remain active (NIST AC-12). Confirm MFA is enforced across all externally exposed and administrative interfaces (CIS 6.3, 6.4, 6.5). Monitor for reappearance of anomalous outbound transfer patterns consistent with T1041. Retain audit logs for post-incident forensic review per NIST AU-11 (Audit Record Retention).
6. Step 5: Post-Incident, Assess whether credentials are transmitted or stored in cleartext in affected environments (CWE-312, CWE-319) and remediate per NIST SC controls. Review separation of duties for OT-adjacent roles (NIST AC-5). Evaluate credential protection posture against CWE-522 and implement D3-CH (Credential Hardening). Establish a process to monitor open-source threat intelligence for emerging corroboration of this campaign per NIST AU-13 (Monitoring for Information Disclosure).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISA (via cisa.gov/report) and organizational leadership immediately if BusySnake activity is confirmed on any OT-adjacent system, if exfiltrated data includes government PII or classified material triggering mandatory breach notification, or if the responding team lacks forensic capability to perform live memory acquisition on compromised critical infrastructure hosts.

Recovery Notes	Post-containment, validate recovery by monitoring all previously compromised accounts and hosts for re-infection indicators — specifically renewed access to browser credential stores and Windows Credential Manager — for a minimum of 14 days given Armored Likho's demonstrated persistence capability in espionage-oriented campaigns. Confirm that all OT-adjacent service accounts have completed credential rotation and that MFA enforcement has been verified on all externally exposed interfaces before declaring systems fully recovered. Given the absence of confirmed public IOCs for BusySnake at this time, maintain elevated logging verbosity (Sysmon + Windows Security Event Log at maximum audit policy) and re-evaluate IOC feeds weekly as the campaign is further analyzed by the threat intelligence community.
Forensic Artifacts	Browser credential store files: Chrome '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data', Firefox '%APPDATA%\Mozilla\Firefox\Profiles*.default\logins.json', and Edge '%LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Login Data' — accessed by BusySnake's T1555 credential harvesting module; file access timestamps and Security Event ID 4663 on these paths confirm harvesting activity | Windows Credential Manager vault files at '%LOCALAPPDATA%\Microsoft\Credentials\' and '%APPDATA%\Microsoft\Credentials\' — targeted by BusySnake for harvesting stored RDP, network share, and application credentials via CryptUnprotectData API calls visible in Sysmon Event ID 10 (ProcessAccess) against svchost.exe hosting VaultSvc | LSASS process memory dump — BusySnake's keylogging and credential harvesting requires interaction with LSASS; a memory acquisition via ProcDump or WinPmem will contain injected code artifacts, in-memory credential stores, and Kerberos ticket caches reflecting any pass-the-ticket lateral movement performed within the government or energy-sector environment | Windows Security Event Log entries for Event IDs 4624/4625/4648 (authentication events), 4688 (process creation with command-line logging enabled), and 4663 (object access on credential store paths) — correlate process creation events for any unsigned executable spawning from unusual parent processes consistent with BusySnake's initial access and execution chain | Firewall and DNS logs for outbound connections from compromised hosts — BusySnake exfiltration (T1041) would produce recurring outbound sessions with consistent data volumes to non-organizational external IPs; DNS query logs for unusual domain resolutions immediately prior to data transfer events can identify C2 infrastructure even without confirmed IOCs

Per-Action IR Details

Step 1: Containment — Audit privileged and service accounts across government and energy-sector systems for signs of unauthorized access or anomalous authentication events; enforce session termination for any accounts exhibiting suspicious behavior. Cross-reference against NIST AC-12 (Session Termination) and NIST AC-2 (Account Management).

NIST Phase: Containment

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

Controls: NIST AC-2 (Account Management), NIST AC-12 (Session Termination), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Run 'Get-ADUser -Filter * -Properties LastLogonDate,PasswordLastSet,Enabled | Export-Csv accounts.csv' to baseline all AD accounts; cross-reference against 'Get-ADUser -Filter {LastLogonDate -gt (Get-Date).AddDays(-7)}' to identify recently active accounts. For Linux service accounts, parse /var/log/auth.log or /var/log/secure for PAM authentication events. Use 'quser' or 'query session' on Windows Terminal Servers to enumerate and terminate suspicious live sessions via 'logoff '.

Evidence: Before terminating any suspicious session, capture volatile state: run 'Get-NetTCPConnection | Where-Object {$_.State -eq "Established"}' and 'netstat -ano' to record all active connections associated with the

suspect account. Collect Windows Security Event Log Event ID 4624 (successful logon), 4625 (failed logon), 4648 (explicit credential use), and 4779 (session disconnect) filtered on the flagged account names. Export live session tokens and Kerberos ticket state via 'klist' before any session termination — BusySnake's credential harvesting may have produced pass-the-ticket or pass-the-hash lateral movement artifacts visible only in live session state. Preserve LSASS memory via Task Manager protected dump or ProcDump ('procdump.exe -ma lsass.exe lsass.dmp') before any credential rotation or session kill.

Step 2: Detection — Hunt for BusySnake-associated behaviors: keylogging artifacts, browser credential store access, unusual outbound data transfers, and screen capture activity. Review endpoint logs for access to browser credential stores and Windows Credential Manager. Monitor for T1056.001, T1539, T1555, and T1113 indicators using available EDR telemetry. Enable and review audit logs per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). No confirmed IOCs are available from current source material.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config and add rules for: Event ID 10 (ProcessAccess targeting lsass.exe), Event ID 11 (FileCreate in %APPDATA%\Local\Google\Chrome\User Data\Default\Login Data or equivalent browser credential paths), and Event ID 3 (NetworkConnect for unusual outbound connections on non-standard ports). Write a YARA rule scanning for BusySnake behavioral hallmarks — in-memory keylogger hooks, GDI-based screen capture API calls (BitBlt, GetDC), and Windows Credential Manager API access (CredEnumerateW, CryptUnprotectData). Use Osquery query 'SELECT * FROM processes WHERE name LIKE "%.exe" AND path NOT LIKE "C:\\Windows\\%"' to identify unsigned or anomalously pathed executables consistent with BusySnake staging.

Evidence: This step is observational and does not alter live state, but if suspicious processes are identified during hunting, capture process memory ('procdump.exe -ma ') and the full process tree ('Get-CimInstance Win32_Process | Select-Object ProcessId,ParentProcessId,Name,CommandLine | Export-Csv proctree.csv') before any remediation action. Key artifact paths for BusySnake credential harvesting: Chrome Login Data at '%LOCALAPPDATA%\Google\Chrome\User Data\Default\Login Data', Firefox logins.json at '%APPDATA%\Mozilla\Firefox\Profiles*.default\logins.json', and Windows Credential Manager vault at '%LOCALAPPDATA%\Microsoft\Credentials\'. Examine Windows Security Event ID 4663 (object access) and 4656 (handle request) on these file paths. For screen capture activity, look for GDI handle exhaustion anomalies or repeated desktop window station access in Sysmon Event ID 10 targeting 'explorer.exe'. Capture outbound NetFlow or firewall logs for sustained connections to non-organizational IPs on ports 443, 80, or custom ports indicative of BusySnake C2 exfiltration channels before blocking.

Step 3: Eradication — Rotate all credentials on systems within the targeted sectors, prioritizing service accounts and accounts with access to OT-adjacent environments, per D3-CRO (Credential Rotation). Enforce MFA on all remote access and administrative accounts per NIST IA controls and CIS 6.3, 6.4, 6.5. Remove any unauthorized software identified during investigation per CIS 2.3 (Address Unauthorized Software).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 2.3 (Address Unauthorized Software)

Compensating: For credential rotation without enterprise PAM tooling, use 'Set-ADAccountPassword' in bulk via PowerShell iterating a CSV of flagged accounts: 'Import-Csv accounts.csv | ForEach-Object { Set-ADAccountPassword -Identity $_.SamAccountName -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "" -Force) }'. For OT-adjacent service accounts that cannot tolerate immediate rotation due to operational dependency, document and schedule a maintenance window, then disable interactive logon via GPO ('Deny log on locally' policy) as an interim compensating measure. For unauthorized software removal, use 'Get-WmiObject Win32_Product | Where-Object {$_.Name -like "**"} | Invoke-WmiMethod -Name Uninstall' and verify removal with Sysmon Event ID 1 process creation logs post-removal.

Evidence: Credential rotation and software removal alter live system state irreversibly — complete all volatile evidence capture from Steps 1 and 2 before proceeding. Specifically for OT-adjacent environments: document all active service account sessions using 'Get-WmiObject Win32_LoggedOnUser' before rotation, and snapshot the Windows Registry hive HKLM\SECURITY\Cache (cached domain credentials) and HKCU\Software\Microsoft\Windows\CurrentVersion\Run (persistence mechanisms) via 'reg export'. Identify unauthorized software artifacts left by BusySnake: check for executables in '%TEMP%', '%APPDATA%\Roaming', and '%PROGRAMDATA%' with creation timestamps correlating to the suspected compromise window. Hash all identified suspect files with 'Get-FileHash -Algorithm SHA256' before removal to support future threat intelligence correlation once public IOCs for BusySnake become available.

Step 4: Recovery — Validate that credential rotation is complete and that no residual unauthorized sessions remain active (NIST AC-12). Confirm MFA is enforced across all externally exposed and administrative interfaces (CIS 6.3, 6.4, 6.5). Monitor for reappearance of anomalous outbound transfer patterns consistent with T1041. Retain audit logs for post-incident forensic review per NIST AU-11 (Audit Record Retention).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-12 (Session Termination), NIST AU-11 (Audit Record Retention), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Validate session cleanliness using 'quser /server:' and 'Get-NetTCPConnection -State Established' across all in-scope hosts, comparing against a known-good session baseline. For outbound transfer monitoring without SIEM, configure Windows Firewall audit logging ('netsh advfirewall set allprofiles logging droppedconnections enable') and review %SystemRoot%\System32\LogFiles\Firewall\pfirewall.log daily for high-volume outbound connections — BusySnake exfiltration would produce repeated connections to the same external IP with consistent byte-count patterns. Use Wireshark captures at the network perimeter for 72-hour post-recovery monitoring, filtering on 'tcp.len > 1000 && ip.dst != ' to catch residual exfiltration.

Evidence: Recovery validation requires confirming that no new credential harvesting artifacts appear post-rotation. Re-run Sysmon Event ID 10 checks against lsass.exe process access and browser credential store file access (Event ID 11) for 48–72 hours post-recovery to confirm BusySnake is not re-executing via a missed persistence mechanism. Archive all collected logs — Windows Security Event Logs, Sysmon logs, firewall logs, and any captured memory dumps — to write-protected offline storage per NIST AU-11 before rotating or purging production log storage. For OT-adjacent environments, verify that no new authentication events appear from the rotated service account credentials by querying Event ID 4624 with the old account SIDs for 24 hours post-rotation.

Step 5: Post-Incident — Assess whether credentials are transmitted or stored in cleartext in affected environments (CWE-312, CWE-319) and remediate per NIST SC controls. Review separation of duties for OT-adjacent roles (NIST AC-5). Evaluate credential protection posture against CWE-522 and implement D3-CH (Credential Hardening). Establish a process to monitor open-source threat intelligence for emerging corroboration of this campaign per NIST AU-13 (Monitoring for Information Disclosure).

NIST Phase: Post Incident

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

Controls: NIST AC-5 (Separation Of Duties), NIST SC (System And Communications Protection) — specifically SC-8 (Transmission Confidentiality and Integrity) and SC-28 (Protection of Information at Rest), cited from knowledge base family reference, NIST AU-13 (Monitoring For Information Disclosure)

Compensating: Assess cleartext credential exposure using Wireshark captures on internal segment traffic filtered for 'http contains "password"' or FTP/Telnet protocol use — particularly relevant for OT-adjacent networks where legacy protocols are common. For credential hardening without enterprise PAM, enable Windows Credential Guard via GPO (Device Guard settings) on all Windows 10/11 and Server 2016+ hosts to prevent LSASS credential extraction of the type BusySnake performs. For OSINT monitoring of Armored Likho campaign corroboration, configure free RSS/Atom feeds from CISA advisories (cisa.gov/news-events/cybersecurity-advisories), MITRE ATT&CK group updates, and VirusTotal Intelligence community reports, reviewed weekly by a designated analyst.

Evidence: Post-incident this step does not alter live forensic state, but catalog all retained artifacts for long-term reference: SHA-256 hashes of all BusySnake-suspect binaries, exported registry hives (HKCU\Software\Microsoft\Windows\CurrentVersion\Run, HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run), browser credential store copies (Login Data, logins.json), and LSASS memory dumps collected during the investigation. These artifacts should be retained under chain-of-custody documentation for potential future attribution analysis or law enforcement referral given the espionage-oriented nature of the Armored Likho campaign targeting government and critical infrastructure sectors. Note that CWE-312, CWE-319, and CWE-522 are weakness classifiers, not controls — remediation actions should cite the NIST SC control family (SC-8 for transmission, SC-28 for storage) for auditability.

Detection Guidance

Detection should focus on behaviors consistent with BusySnake's reported capabilities: credential harvesting, screen capture, and data exfiltration. Hunt for the following: (1) Access to browser credential stores and Windows Credential Manager from non-browser, non-OS processes (T1555, T1539). (2) Keylogging artifacts or low-level input capture processes running under user-space accounts (T1056.001). (3) Screen capture activity from unexpected processes (T1113). (4) Anomalous outbound data transfers, particularly to unfamiliar external destinations, consistent with C2 exfiltration (T1041). (5) Authentication events using valid accounts from unexpected source IPs or geolocations (T1078). (6) Phishing-related email artifacts in mail gateway and endpoint logs (T1566). Review endpoint detection and response (EDR) telemetry, Windows Security Event Logs (Event IDs 4624, 4625, 4648, 4663, 4688), and network flow data for these behavioral patterns. No confirmed IOCs (hashes, IPs, domains) are available from current source material; monitor for updated advisories from CISA, relevant national CERTs, or the original reporting outlet for IOC enrichment. Pending IOC release, organizations may request detection signatures from their EDR vendor or consult MITRE ATT&CK for behavioral detection patterns aligned with T1056.001, T1539, T1555, and T1113. Enable logging per NIST AU-2 and CIS 8.2 if not already active.

Framework Mappings

MITRE-ATTACK

- **T1056.001** — Keylogging
- **T1539** — Steal Web Session Cookie
- **T1555** — Credentials from Password Stores
- **T1113** — Screen Capture
- **T1552** — Unsecured Credentials
- **T1078** — Valid Accounts
- **T1041** — Exfiltration Over C2 Channel
- **T1566** — Phishing

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **SC-8** — Transmission Confidentiality and Integrity

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures
- **A02:2021** — Cryptographic Failures

CIS-V8

- **5.2** — Use Unique Passwords
- **3.10** — Encrypt Sensitive Data in Transit
- **6.3** — Require MFA for Externally-Exposed Applications

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(e)(1)** — Transmission Security
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC7.4** — Responds to identified security incidents
- **CC9.2** — Manages risks associated with vendors and business partners

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1056.001	Keylogging	Collection
T1539	Steal Web Session Cookie	Credential-Access
T1555	Credentials from Password Stores	Credential-Access
T1113	Screen Capture	Collection

Technique ID	Technique Name	Tactic
T1552	Unsecured Credentials	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1041	Exfiltration Over C2 Channel	Exfiltration
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/busysnake-in...	T2
Russian Harmful Foreign Activities Sanctions	https://ofac.treasury.gov/faqs/topic/6626	T1
Russian GRU Targeting Western Logistics Entities and Technology ...	https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a	T1
Sanctions to Degrade Russia's Energy Sector	https://2021-2025.state.gov/office-of-the-spokesperson/releases/202...	T1
New Executive Order Expands Sanctions Risk in Russia; Targets ...	https://www.millerchevalier.com/publication/trade-compliance-flash-...	T3

Generated 2026-07-07 06:49 UTC by TJS Security Command Center