JANUARY

pellera

THREAT INTEL REPORT 2026

Prepared by: Pellera Threat Intel Team
pellera.com | 800.747.8585

Driving Momentum. Accelerating Change. Empowering IT Transformation.

Pellera Technologies was born out of the combined expertise of Converge Technology Solutions and Mainline Information Systems, two industry leaders with over 35+ years of experience and a shared vision for innovation. Together, we empower businesses to achieve greater efficiency, adaptability, and growth for today and tomorrow.

Our commitment is to reshape what's possible with IT, offering advanced solutions in digital infrastructure, cloud, cybersecurity, and AI. We don't just deliver technology—we partner with you to build tailored strategies designed to simplify complexities, unlock opportunities, and drive transformational outcomes.

At Pellera, momentum builds here through collaborative, people-first technology designed to fuel progress and deliver measurable impact.

pellera

Observations for January 2026

January 2026 delivered a clear message to defenders: **the threat environment is being shaped by state action**, **new automation layers inside enterprise systems, and mature APT tradecraft that continues to succeed against common weaknesses**.

This month's reporting shows how quickly geopolitical shocks convert into real targeting, how "assistive" technology can become an access path, and how adversaries are increasingly using other organizations as infrastructure to extend their reach.

The Venezuela operation marked a shift from conventional deterrence into direct action backed by cyber and space capabilities. Indicators tied to the operation, including reported BGP anomalies and rapid follow-on activity, are consistent with cyber access being used to enable real-world effects and then immediately exploited for influence and retaliation. In the near term, organizations should expect an **elevated volume of themed phishing, disinformation, and opportunistic intrusion attempts** aligned to Russian, Chinese, and Iran-linked objectives, with early activity already observed from China-nexus actors.

The second major trend is the speed at which enterprises are granting AI agents access to high-value systems and workflows without mature guardrails. Recent research and incident patterns show these tools create **privilege pathways that can be abused** through weak policy, over-broad permissions, and trusted agent-to-agent action chains. ServiceNow's patch of a critical AI Platform vulnerability that enabled user impersonation reinforces that agent-integrated platforms must be treated as production attack surface, not experimental tooling.

Finally, the Ink Dragon campaign reflects a disciplined model for persistence and operational scaling. By converting compromised IIS servers into relay nodes, the actor reduces attribution clarity and turns **victim infrastructure into a forwarding layer for downstream attack**s. Their continued reliance on ViewState deserialization and SharePoint exploit chains remains effective because exposed systems stay unpatched, secrets remain recoverable, and segmentation gaps still allow movement after initial access.

For MSSP customers, the **practical takeaway is unchanged**: harden and monitor public-facing Microsoft stacks, assume compromise is possible even without "new" vulnerabilities, and scope incidents with the expectation that internal systems may be used to target third parties.

Executive Overview

GEO-POLITICAL CLIMATE

Audience

- **CISO**
- **Project Managers**
- **Cybersecurity Analysts**
- **Risk Management Professionals**
- **IT Managers**

HIGH
RISK

GLOBAL
GEOGRAPHIC SCOPE

ALL ORGANIZATIONS
BUSINESS IMPACT

The U.S. operation that removed Nicolás Maduro from power is a historic precedent in combined military-cyber power projection and has triggered regional instability with long-term geopolitical consequences. Russia and China, both formal or de facto allies of Venezuela, now face public credibility tests after years of economic and strategic engagement. The attack also confronts BRICS with the question of whether it is a symbolic bloc or a platform capable of deterrence. As retaliatory pressures mount, U.S. organizations—especially in the government, energy, infrastructure, and policy sectors—should anticipate persistent targeting from motivated, state-aligned actors.

READ MORE

AI AGENTS AND THE MATRIX

Audience

- **CISO**
- **IT Operations Managers & Teams**
- **Risk Management Professionals**
- **Security Operations Team**
- **IT Security Managers**
- **Incident Response Teams**
- **System Administrators**

HIGH
RISK

GLOBAL
GEOGRAPHIC SCOPE

ARTIFICIAL INTELLIGENCE AGENTS
BUSINESS IMPACT

AI agents are no longer experimental tools; they are autonomous entities operating across enterprise environments. Their ability to ingest instructions, invoke external tools, and maintain state introduces an attack surface that fuses LLM-specific threats with legacy application security issues. Unit42's nine-category attack framework and CyberArk's production exploit analysis reveal that adversaries are now targeting these systems via SSRF, RCE, BOLA, and indirect prompt injection, often without needing to circumvent traditional security boundaries. Security teams that treat agents as "just another LLM" risk missing critical misconfigurations and privilege exposures.

READ MORE

Audience

- CISO
- IT Operations Managers & Teams
- Risk Management Professionals
- Security Operations Team
- IT Security Managers
- Incident Response Teams
- System Administrators

INK DRAGONS

HIGH

RISK

GLOBAL

GEOGRAPHIC SCOPE

IIS TECHNOLOGY STACK

BUSINESS IMPACT

Ink Dragon has escalated its operational capability by deploying a custom ShadowPad IIS module that reconfigures compromised infrastructure into command-and-control relay nodes. This tactic converts victim networks into transparent intermediaries for attacking other targets, complicating attribution and raising legal exposure risks. The group exploits misconfigured or unpatched IIS/SharePoint servers and employs credential harvesting, sideloading, and cloud-native C2 via FinalDraft to sustain access and expand its footprint. The campaign presents a high-impact threat to public sector and telecom organizations in Southeast Asia, South America, and increasingly Europe.

READ MORE

GEO-POLITICAL CLIMATE

Overview & Impact

The capture of Venezuelan President Nicolás Maduro represents a marked departure from past U.S. actions designed to constrain adversary capabilities without directly removing leadership. This operation signals a shift from traditional deterrence toward assertive regime change enforcement in the Western Hemisphere. Secretary of State Marco Rubio's post-raid framing of the region as a U.S. strategic domain—the so-called "Rubio Doctrine"—sets a new policy baseline, directly challenging China's long-held assertion that Latin America is "not anyone's backyard."

As a result, the raid has intensified geopolitical fault lines:

- **Pressure on Russia:** Moscow's credibility is at risk given its October 2025 10-year Strategic Partnership Treaty with Venezuela. Failure to respond decisively could be interpreted as weakness by allies and rivals alike.
- **Exposure for China:** Beijing faces potential financial and diplomatic fallout. Decades of financing and oil-backed loan arrangements with Venezuela are at risk, and Chinese supertankers reportedly aborted oil pickups in the immediate aftermath, underscoring economic repercussions.
- **BRICS Credibility Test:** Venezuela's pursuit of BRICS membership has elevated the bloc's strategic profile. The attack tests whether BRICS can function as a deterrent for aspiring members or remains an aspirational alignment without collective security mechanisms.

This episode also marks a qualitative escalation compared with the 2025 U.S. strikes on Iranian nuclear facilities. Unlike the Iran strikes, which targeted infrastructure while leaving leadership intact, the Venezuelan operation resulted in the actual removal of a sitting head of state. Combined with the apparent pre-raid cyber and space coordination—such as power grid disruption and internet routing anomalies observed hours beforehand—this indicates a more integrated U.S. operational approach. Adversaries are therefore confronted with both a heightened sense of risk and a more complex retaliation calculus.

- Likely retaliatory cyber operations from Russian, Chinese, and Iranian actors, either directly or via proxies.
- Increased targeting of U.S. critical infrastructure sectors, particularly OT environments and energy supply chains.
- Surge in geopolitical-themed phishing tied to Mustang Panda's rapid post-raid malware deployment.
- Proxy and hacktivist campaigns driving alert fatigue through low-sophistication noise (DDoS, defacement).
- Financial exposure through fraud schemes leveraging disinformation campaigns (e.g., "Crypto Maduro").
- Economic ripple effects
  - China holds an estimated $50B in oil-for-debt loans to Venezuela, now at risk of default.
  - At least two Chinese supertankers turned away post-raid, halting crude transfer operations.
  - Regional uncertainty disrupting over $500B in China-Latin America trade volume.

Observations

- Coordinated power disruption in Caracas occurred precisely at 2:00 a.m., with helicopters landing at 2:01 a.m.
- Public internet routing anomalies (BGP shifts) detected 14 hours prior to raid; lacked adequate visibility by defenders.
- Disinformation campaigns included AI-generated images and deepfakes, with over 140 fraudulent domains registered.
- Proxy activity likely to increase, modeled after Iran 2025 precedent, with defacements and opportunistic ransomware.
- China's Mustang Panda campaign was operational within hours, exploiting interest in Venezuela policy outcomes.

Guidance

Strategic Intelligence

The Venezuela operation is not likely to be a standalone event. Secretary of State Rubio's invocation of the Western Hemisphere as a protected strategic domain suggests additional flashpoints may follow, with Cuba explicitly mentioned as a failing state that "should be concerned." This signals continuity in U.S. policy toward adversarial influence in Latin America and increases the likelihood of further action targeting states aligned with Russia, China, or Iran in the region.

- **Trend**
  - Military operations now tightly integrated with cyber and space assets.
  - Regime-change operations setting precedents for adversary escalation.
  - BRICS bloc facing coherence test; potential fragmentation under stress.
  - Proxy and hacktivist surges predictable post-conflict flashpoints.
  - Retaliation timeline likely phased over 90+ days.
- **Retaliation Timeline:**
  - **Week 1–2:** Confirmed Mustang Panda phishing, disinformation surge, fraud domains, CISA alert posture.
  - **Week 2–4:** Likely increase in hacktivism, opportunistic ransomware, and poorly coordinated APT activity.
  - **Month 1–3: Strategic operations mature:** CNI probing, BGP anomalies, supply chain compromise.
  - **Ongoing:** Venezuela becomes persistent lure; long-term prepositioning by Volt Typhoon-type actors.

Operational Intelligence

- **Proxy and Hacktivist Layer**
  - Post-raid conditions mirror the aftermath of the 2025 Iran strikes, which triggered a 300% surge in hacktivist noise targeting U.S. and allied infrastructure.
  - Typical tactics include DDoS attacks, website defacements, and recycled ransomware strains.
  - These operations tend to cluster in Weeks 2–4 post-trigger and persist for 4–8 weeks.
  - SOCs should expect elevated alert volume, primarily from unsophisticated actors attempting symbolic retaliation.
- **Threat Vectors**
  - Geopolitically themed phishing campaigns and .zip payload delivery.
  - OT/IT convergence exploitation with focus on energy and telecoms.
  - Social engineering leveraging BRICS rhetoric and Maduro political imagery.
- **Monitoring & Detection Gaps**
  - Inability to detect pre-attack configuration changes and BGP anomalies.
  - Reduced disinformation analysis capacity within CISA under recent reforms.

- **Response Actions**
    - Proactive monitoring of identity systems for drift and shadow admin creation.
    - SOC tuning to detect event-tied phishing and reconnaissance traffic.
    - Alert suppression strategy for anticipated low-tier hacktivist noise.

Tactical Intelligence

- **Mitigation Strategies**
    - Geo-event content filtering on mail gateways (.zip files, "Venezuela", "Maduro").
    - Enhanced behavioral sandboxing for geopolitical lures.
    - Triage logic for distinguishing high-signal campaigns from disinformation noise.
- **Preventive Measures**
    - Correlate internet routing anomalies with geopolitical escalation.
    - Red team OT network edge with Venezuela methodology scenarios.
    - Pre-emptively tag and block likely phishing lure terms and related fraudulent domain variants.

Threat Hunting Hypotheses

Prepositioned Campaign Infrastructure (Mustang Panda)

Hypothesis: Adversary infrastructure was primed for use immediately following a geopolitical catalyst.

Investigation Steps

- DNS logs and WHOIS history analysis of newly active geopolitical-themed domains.
- Email and proxy logs filtered for event-specific lures or suspicious .zip attachments.
- Endpoint detections for behaviors tied to Mustang Panda historical TTPs.
- Lateral movement correlation with compromised policy or think tank identities.

CNI Environment Shaping (Russia/China Aligned)

Hypothesis: OT/IT systems were reshaped in energy and telecom sectors to enable future short-duration disruptions.

Investigation Steps

- Historical audit of firewall changes and route table modifications over last 90 days.
- Identity logs reviewed for privilege escalation and conditional access bypass.
- OT telemetry reviewed for intermittent logic interference or test patterns.
- Cross-reference with geopolitical developments and strategic statements.
- **Success criteria:** Detection of pattern alignment with 3-phase CNI attack model.

Sources

- Reuters: Chinese-linked hackers target US entities
- Chatham House: US-China Rivalry in Latin America
- TV BRICS: Venezuela-Russia Treaty
- BankInfoSecurity: CISA Warns of Retaliation Risk
- Nextgov: Disinformation Tracking Post-Raid
- Dark Reading: Cyber Role in Venezuela Operation
- SecurityBrief UK: CNI Vulnerability Analysis
- Digital One Agency: BRICS at a Crossroads
- BBC: World Leaders React

AI AGENTS AND THE MATRIX

Overview & Impact

AI agents inherit LLM vulnerabilities while introducing new threat dimensions due to their tool access and autonomy. The Unit42 study found framework-agnostic attack success across diverse techniques: tool schema enumeration, server-side request forgery (SSRF), mounted volume exploitation, token exfiltration from metadata services, SQL injection, and BOLA. These attack paths require no novel exploits—only poorly scoped instructions and permissive access. CyberArk's financial agent scenario confirms these are not theoretical, while the ServiceNow compromise demonstrates that attacker access to agent execution paths can lead to full platform takeover.

- Privilege misuse via tools enabled lateral movement, data theft, and infrastructure compromise.
- Metadata service access in code interpreters led to token exfiltration, risking cloud environment integrity.
- Mounted volume read access enabled theft of plaintext secrets and credentials.
- Absence of agent scoping allowed indirect prompt injection via user input fields.
- ServiceNow's universal credential and email-only auth led to enterprise-wide exposure.

Observations

- Tool misuse did not require prompt injection; excessive permissions were sufficient.
- Code interpreters lacked sandboxing, enabling RCE and host access.
- Multi-agent systems allowed attacker-pivot through trust chains between agents.
- Schema enumeration provided attackers with system maps to plan lateral movement.

Guidance

Strategic Intelligence

- **Threat Context**
  - Poorly scoped AI agents can be exploited without traditional prompt injection.
  - Multi agent trust relationships enable privilege escalation chains attackers can abuse.
- **Trends Analysis**
  - Shift from prompt injection attacks to systemic exploitation of tool permissions.
  - Memory context and metadata access are emerging as preferred abuse vectors.

Operational Intelligence

- **Threat Vectors**
  - Server-Side Request Forgery (SSRF) via web scraping tools.
  - Cloud metadata token theft from code interpreter runtimes.
  - Unvalidated tool inputs leading to backend exploitation.
- **Monitoring & Detection Gaps**
  - Limited telemetry on agent tool invocations.
  - No enforcement of privilege boundaries across agents.

RETURN

- **Response Actions**
    - Restrict agent tool access and privileges.
    - Rotate secrets and enforce scoped execution policies.
    - Sandbox code interpreters with strict syscall and volume controls.

Tactical Intelligence

- **Mitigation Strategies**
    - Apply least privilege to agent tools and enforce tight prompt boundaries.
    - Enable syscall filtering and volume restrictions within interpreter environments.

- **Detection Engineering**
    - Monitor agent logs for access to internal IP ranges.
    - Alert on interpreter output containing credential-like strings or cloud tokens.
    - Correlate agent interactions for signs of indirect prompt manipulation or trust abuse.

Threat Hunting Hypotheses

Memory Poisoning via Indirect Prompt Injection

Hypothesis: Adversaries are using indirect prompts to manipulate long-term memory.

- **Investigation Steps**
    - Scan web content inputs for hidden instructions (e.g., base64 or whitespace obfuscation)
    - Match external data inputs with later memory-based actions by agent
    - Isolate agent memory snapshots before and after trigger
    - Cross-reference changes with attacker-controlled domains
    - Monitor for repeated behaviors matching exfiltrated data flows

Privilege Escalation via Inter-Agent Trust

Hypothesis: One compromised agent can escalate privileges by delegating tasks to trusted agents.

- **Investigation Steps**
    - Review agent-to-agent task delegation logs
    - Flag commands where low-scope agents issued high-impact instructions
    - Detect unusual task sequences indicating orchestration bypass
    - Analyze response behavior changes after upstream agent compromise
    - Confirm privilege boundaries on agent role definitions

Sources

- Unit42: AI Agents Are Here. So Are the Threats
- CyberArk: AI Agents and Identity Risks
- Dark Reading: Most Severe AI Vulnerability to Date Hits ServiceNow
- USCSI: AI Agent Security Plan 2026
- Legit Security: OWASP’s Agentic AI Top 10

INK DRAGON

Overview & Impact

Ink Dragon, operating under aliases such as Earth Alux and REF7707, exploits persistent misconfigurations in IIS/SharePoint to deploy a ShadowPad IIS module that silently intercepts HTTP traffic. The module uses the HttpAddUrl API to register dynamic listeners and builds a distributed relay network for lateral and external communications. SharePoint CVEs CVE-2025-49706, -53771, -49704, and -53770 are actively exploited. The actor also employs FinalDraft malware for stealthy C2 via Microsoft Graph API and routinely harvests service credentials for lateral movement across IIS farms.

Ink Dragon's infrastructure-first approach weaponizes victim servers for upstream and downstream attacks, bypassing traditional network controls. The attack lifecycle includes:

- Initial access via ViewState deserialization or ToolShell SharePoint exploits
- Deployment of a modular ShadowPad IIS listener for C2 relay operations
- Credential theft from IIS app pools and lateral movement using RDP tunneling
- Persistence through scheduled tasks and masqueraded services
- FinalDraft deployment for cloud-native C2 leveraging Outlook drafts and OAuth tokens
- Compromised IIS servers act as transparent relays in a C2 mesh, raising liability and complicating IR scoping
- CVE exploitation enables unauthenticated RCE in SharePoint environments
- Credential reuse across IIS farms enables rapid lateral movement
- FinalDraft usage complicates detection due to use of trusted Microsoft services

Observations

- Use of HttpAddUrl for dynamic listener registration
- Custom traffic decryption routines within IIS module
- Graph API misuse and OAuth refresh token abuse for C2
- Common persistence via SYSCHECK tasks and WindowsTempUpdate services
- DLL sideloading with legitimate vendor signatures (AMD, Realtek, NVIDIA)

Guidance

Strategic Intelligence

- **Threat Context**
  - Ink Dragon (aka Earth Alux, REF7707) is a PRC-aligned espionage group emphasizing stealth, infrastructure repurposing, and long-term access across public sector and telecom targets.
  - Victims are not only targeted for data exfiltration but are repurposed as infrastructure for downstream attacks — creating geopolitical, legal, and reputation risk.
- **Trends Analysis**
  - Continued success exploiting known misconfigurations (e.g., machineKey reuse) over novel zero-days signals persistent weaknesses in web-tier hygiene.
  - Modular ShadowPad components reflect a shift toward distributed, peer-to-peer C2 infrastructure to obscure operator origin and enhance operational resilience.
  - Cloud-native C2 through FinalDraft using Microsoft Graph API shows growing reliance on legitimate services to bypass perimeter monitoring.

Operational Intelligence

- **Threat Vectors**
  - Initial access via ViewState deserialization using leaked/predictable machineKeys.
  - **SharePoint exploitation via ToolShell chain:** CVE-2025-49706, -53771, -49704, -53770.
  - Lateral movement via RDP tunneling, credential harvesting, and config file decryption.
- **Monitoring & Detection Gaps**
  - Lack of monitoring for HttpAddUrl dynamic listener registration leaves ShadowPad implants undetected.
  - OAuth and Graph API activity from non-standard processes (e.g., w3wp.exe) often escapes notice.
  - Debug logs from ShadowPad relay modules are written silently and blend with legitimate IIS activity.
- **Response Actions**
  - Immediately patch all SharePoint instances and rotate machineKeys on IIS servers.
  - Audit for wildcard URL listeners and abnormal IIS behavior.
  - Investigate for credential harvesting artifacts, RDP tunneling, and unauthorized OAuth activity.

Tactical Intelligence

- **Mitigation Strategies**
  - Apply patches for CVE-2025-49706, -53771, -49704, -53770.
  - Rotate and secure machineKey configurations across all IIS/SharePoint deployments.
  - Revoke and reissue OAuth tokens suspected of compromise.
- **Detection Engineering**
  - Monitor for abnormal HttpAddUrl API usage and wildcard listener registrations.
  - Alert on outbound Microsoft Graph API calls from non-browser processes.
  - Detect DLL sideloading with mismatched OriginalFileName vs. binary name.
  - Flag w3wp.exe spawning interactive shells or credential dumpers.
  - Correlate RDP session tunneling with authentication anomalies and config file access.

Threat Hunting Hypotheses

Compromised IIS Servers Used as Relay Nodes

Hypothesis: ShadowPad IIS module is forwarding external C2 traffic to internal implants

Investigation Steps

- Review w3wp.exe process network traffic for uncharacteristic destinations
- Identify custom URL listeners registered via HttpAddUrl
- Cross-reference server logs with observed debug strings detailing byte transfers
- Compare internal traffic flow with known peer IPs from Check Point telemetry

Credential Reuse Across IIS Farms

Hypothesis: IIS service account credentials reused across multiple web servers

Investigation Steps

- Audit local service account usage across IIS fleet
- Examine authentication logs for lateral logins using IIS credentials
- Identify matching hashes or passwords in IIS config files across hosts
- Correlate with SMB, RDP session data for pivoting behavior

Cloud IAM Abuse Post Appliance Compromise

Hypothesis: Cloud-hosted devices compromised by misconfiguration were used to pivot into IAM services.

Investigation Steps

- Review access to metadata IPs (169.254.169.254) from compromised hosts.
- Check cloud audit logs for new API token issuance or credential escalation.
- Confirm timeline correlation between appliance compromise and IAM actions.

Sources

- Check Point Research: Ink Dragon Expands With New Tools and a Growing Victim Network
- The Hacker News: China-Linked Ink Dragon Hacks Governments Using ShadowPad and FINALDRAFT Malware
- Cyberpress.org: Turning Servers Against Themselves Inside a ShadowPad-Driven Campaign
- GovInfoSecurity: Chinese Hackers Hijack European Networks for Espionage

pellera

Contact the Pellera Threat Intel Group at getsecure@pellera.com

pellera.com