pellera

THREAT INTEL REPORT 2025

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

NOVEMBER

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

CONVERGE TECHNOLOGY SOLUTIONS + Mainline®

Observations for November 2025

Geopolitical pressure in the Western Hemisphere continued to build this month as the U.S. increased its military posture in the Caribbean and moved forward with covert operations targeting Venezuela. At the same time, **Venezuela signaled a deeper alignment with BRICS**, positioning itself closer to a bloc that is working to challenge Western influence. These parallel developments—kinetic maneuvering on one side and geopolitical realignment on the other—create an environment where cyber retaliation becomes an expected extension of statecraft. The likelihood of spillover activity affecting global organizations grows as regional tensions harden and alliances set clearer boundaries.

Against this backdrop, Russia-aligned intrusion activity pushed further into hybrid operations that blur established defensive lines. **Curly COMrades** has continued refining its tradecraft by deploying lightweight Alpine Linux VMs within compromised Windows environments, leveraging native Hyper-V capabilities to sidestep traditional endpoint monitoring. This method gives the operator a covert execution layer with its own persistence and credential-theft pathways, making detection significantly more difficult for defenders who may assume Windows telemetry tells the full story. The campaign demonstrates how virtualization can be weaponized to mask activity while maintaining long-term access.

Meanwhile, **software supply chain** compromises gained momentum heading into Q4. Open-source ecosystems, particularly npm, saw a surge in coordinated attacks that exploited developer trust, automated CI/CD pipelines, and identity compromises to push malicious packages at scale. The **"Shai-Hulud" event**—affecting hundreds of npm packages—served as a reminder that attackers continue to favor the path of least resistance: poisoning upstream dependencies to reach thousands of downstream users in a single move. These incidents show how quickly a compromised developer account or tampered build step can ripple across global organizations.

These three trends show how quickly the threat landscape is shifting. Geopolitical tension, more inventive intrusion techniques, and upstream software compromises are now feeding into each other instead of appearing as isolated events. As a result, organizations should expect more pressure across multiple fronts at once, especially in areas where visibility is limited or trust is assumed. The environment is becoming less forgiving of security gaps, and staying ahead will require steady attention to identity controls, workload monitoring, and software integrity.

Executive Overview

VENEZUELA AND BRICS

Audience

- CISO
- C-Suite Executives
- Board of Directors Audity & Risk Committees
- General Counsel & Legal Teams
- Government Relations Directors
- Compliance Officers
- Project Managers
- Cybersecurity Analysts
- Risk Management Professionals
- IT Managers

RISK

GEOGRAPHIC SCOPE

Geopolitical Tensions, Economic Impact, Critical Infrastructure Targeting

BUSINESS IMPACT

The escalation between the United States and Venezuela has entered a critical phase, marked by kinetic military operations, intelligence activities, and growing digital risk. Venezuela, which faces mounting pressure from U.S. forces and CIA-authorized operations, has responded by expanding asymmetric military strategies and reinforcing diplomatic ties with the BRICS group. Although Brazil has yet to approve formal membership, President Maduro has publicly declared Venezuela part of BRICS—a bloc increasingly leveraged by member states to oppose Western influence in global institutions. This strategic pivot increases the likelihood of coordinated cyber operations against Western digital infrastructure, regardless of industry or geographic proximity.

READ MORE: VENEZUELA AND BRICS

CURLY COMRADES

Audience

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

RISK

GEOGRAPHIC SCOPE

Development environment compromise, credential theft, potential production system access through stolen cloud service tokens

INDUSTRY IMPACT

Curly COMrades has adopted a cross-platform persistence model exploiting Windows Hyper-V to deploy Linux VMs hosting stealth malware. The strategy enables long-term access while evading detection by host-based tools. With no reliance on kernel exploits, the operation reveals a strategic misuse of Linux environments as operational blind spots. Organizations with mixed infrastructures must reassess monitoring assumptions and align their detection efforts across hypervisors, endpoints, and guest OS telemetry to close exploitable security gaps.

READ MORE: CURLY COMRADES

Audience

- **CISO**
- **IT Operations Managers & Teams**
- **Risk Management Professionals**
- **Security Operations Team**
- **Ai/Ml Development Teams**
- **Cloud Security Teams**
- **Software Development Teams**

SOFTWARE SUPPLY CHAIN

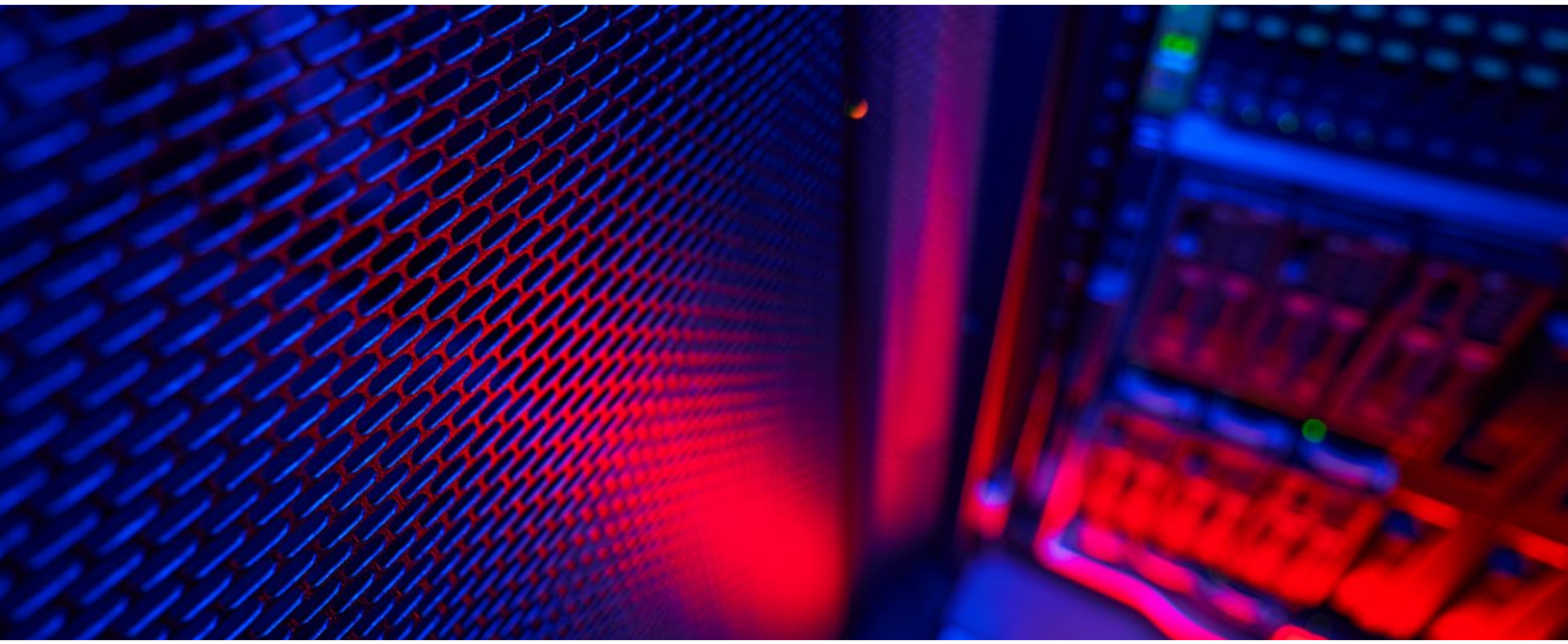
MEDIUM
RISK

GLOBAL
GEOGRAPHIC SCOPE

Open Source Tool Impact, Vendor Tools that rely on Open Source Technology, Internal Tooling
INDUSTRY IMPACT

The "Shai-Hulud" worm represents a critical escalation in software supply chain compromise, exploiting developer ecosystems to automate malware propagation via compromised npm tokens and GitHub Actions workflows. This event, alongside a surge in token farming and delayed-activation logic bombs, signals a transition in attacker behavior toward long-tail, infrastructure-embedded threats. These attacks exploit core assumptions of trust in package management systems, threatening development pipelines and downstream application security across sectors.

READ MORE: SOFTWARE SUPPLY CHAIN



VENEZUELA AND BRICS

Overview & Impact

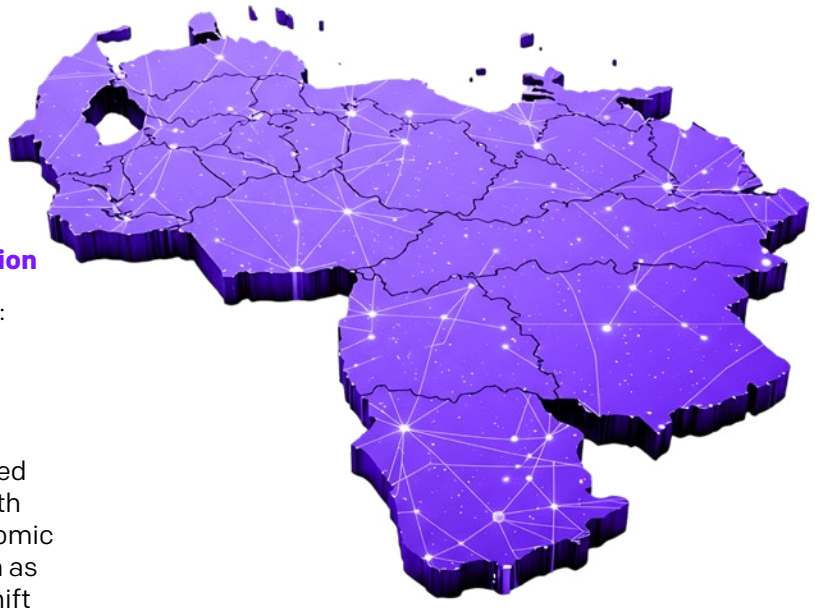
The deployment of U.S. naval and intelligence assets near Venezuela—including the USS Gerald R. Ford and CIA authorization for covert actions—has escalated the regional security crisis. Venezuela, militarily overmatched in conventional terms, is relying on asymmetric strategies: guerrilla defense, urban destabilization ("anarchization"), and broader information warfare. Concurrently, Maduro's government has proclaimed its integration into BRICS, a coalition aimed at reducing reliance on U.S.-led institutions and promoting multipolar governance.

The BRICS bloc, comprising Brazil, Russia, India, China, South Africa, and newer members (e.g., Iran, Egypt, UAE), enables member states to coordinate economic policy, develop parallel financial systems (via the New Development Bank), and push geopolitical agendas counter to the West. This realignment could activate state or proxy cyber actors in defense of BRICS-aligned states, especially amid perceived Western aggression.

- Increased targeting of critical infrastructure, finance, and telecom sectors in Western countries through APT-aligned operations
- Potential for coordinated disinformation campaigns and digital sabotage, particularly as retaliation for U.S. strikes
- Elevated operational risk for multinational organizations operating across BRICS-aligned regions
- Threat escalation through parallel proxy activity by groups ideologically or financially supported by BRICS members

Observations

- Venezuela claims de facto BRICs membership, reflecting a strategic pivot toward anti-Western alliances
- BRICS enables member support through diplomatic cover, alternative financing, and non-dollar trade infrastructure
- U.S. intelligence and military activities in the region have already triggered lethal force use; cyber retaliation is a plausible extension



Guidance

Strategic Intelligence

- **Trend Analysis and Threat Landscape Evolution**
  - Escalating Global Geopolitical Polarization: The situation involving Venezuela reflects an accelerating division between Western-aligned coalitions and an emerging bloc of nations seeking to challenge U.S.-centric governance structures. Venezuela's declared integration into BRICS occurs in parallel with an increase in support for alternative economic and security frameworks by countries such as Iran, Russia, and China. This geopolitical shift increases the risk of coordinated non-military responses, including economic disruption and cyber operations targeting strategic sectors.

RETURN >>>

- Multipolar Conflict Theater Expanding Beyond Conventional Boundaries: As conventional confrontation intensifies in localized regions, associated digital activity is extending globally. Adversarial cyber campaigns are increasingly conducted through indirect or unattributed methods, originating from or in support of politically aligned states. Organizations operating across multiple jurisdictions should consider the expanded threat landscape, including secondary targeting of Western entities viewed as strategically significant by state or proxy actors.
- Diminishing Influence of Western-Led Institutions: Venezuela's move toward BRICS corresponds with a broader effort by emerging economies to reduce dependency on the U.S. dollar and Western-led financial systems. This trend includes the use of alternative development banks, bilateral trade in local currencies, and shared strategic initiatives. As more states engage in parallel governance structures, the risk environment becomes more fragmented, with increasing divergence in regulatory enforcement, threat actor motivations, and incident attribution.
- Elevated Use of Asymmetric Cyber Capabilities in Support of Political Objectives: As kinetic and diplomatic avenues reach operational limits, cyber operations offer a low-cost, high-impact means to impose costs or signal resolve. Venezuela's alignment with BRICS-affiliated nations—several of which possess advanced offensive cyber capabilities—may enable coordinated or opportunistic operations aimed at Western critical infrastructure, finance, or information systems. Entities with operations or exposure in aligned countries should reassess control efficacy against state-linked threats.

- **Contextual Insights and Historical Comparisons**
  - Patterns from Prior Interstate Conflicts: Comparable geopolitical confrontations—such as those involving Ukraine, Iran, and Israel—have demonstrated consistent patterns of cyber activity preceding, paralleling, or extending beyond physical engagements. These have included disruptive attacks on government systems, energy infrastructure, and media platforms. The Venezuela scenario exhibits similar conditions, particularly in its reliance on asymmetric deterrence and external alliance structures.
- **Outlook**
  - Cross-Domain Risk Amplification Across International Enterprises: As nations deepen strategic ties through BRICS or similar groupings, private-sector organizations are increasingly exposed to politically motivated threats. This includes not only direct attacks but also regulatory pressure, supply chain compromise, and reputational targeting. Firms with digital, operational, or financial interdependencies in contested regions should account for heightened exposure across geopolitical fault lines, especially in sectors linked to energy, defense, media, and telecommunications.

Operational Intelligence

- **Threat Vectors**
  - APT-linked spear phishing, wiper malware, disinformation, and destructive OT campaigns targeting Western infrastructure
- **Monitoring & Detection Gaps**
  - Lack of cross-border intelligence sharing between enterprises operating in BRICS and non-BRICS jurisdictions
  - Gaps in visibility across hybrid cloud systems common to international firms

RETURN >>>

Tactical Guidance

- **Response Actions**
  - Revalidate cross-region incident response coordination, especially for BRICS-linked operational zones
  - Monitor for increased activity linked to groups such as APT29 (Russia), APT10 (China), and Iranian-linked actors
- **Mitigation Strategies**
  - Block IOCs tied to known BRICS-aligned APTs
  - Harden access controls on cross-border data sharing platforms
- **Preventive Measures**
  - Conduct cyber readiness assessments for business units exposed to BRICS-related supply chains or subsidiaries
  - Expand internal threat intelligence capability to monitor BRICS-centric geopolitical triggers

Tactical Intelligence

- **Mitigation Strategies**
  - Block IOCs tied to known BRICS-aligned APTs
  - Harden access controls on cross-border data sharing platforms
- **Preventive Measures**
  - Conduct cyber readiness assessments for business units exposed to BRICS-related supply chains or subsidiaries
  - Expand internal threat intelligence capability to monitor BRICS-centric geopolitical triggers

Sources

- **Reuters: Trump confirms CIA authorization in Venezuela**
- **Guardian: US military escalation in Caribbean raises stakes with Venezuela**
- **Mehr News: Venezuela's BRICS membership is a reality**
- **Council on Foreign Relations: What Is the BRICS Group and Why Is It Expanding?**
- **BBC: Maduro accuses US of fabricating war**
- **Reuters: Venezuela prepares guerrilla response to US attack**

CURLY COMRADES

Overview & Impact

Curly COMrades enabled Hyper-V on targeted Windows 10 hosts to install Alpine Linux virtual machines that run ELF-based implants CurlyShell and CurlCat. CurlyShell operates as an encrypted reverse shell, while CurlCat functions as a traffic proxy via SSH tunneling. These lightweight VMs serve as isolated execution environments, masking malicious traffic as legitimate host-originated activity.

Additional components included PowerShell-based Kerberos ticket injection into LSASS for remote authentication, and creation of local user accounts across domain-joined machines for persistence. Despite operating within native functionality, these actions enable stealthy lateral movement and long-term control.

From a Linux security standpoint, the campaign did not target kernel vulnerabilities but exploited operational lapses: weak logging, insufficient VM telemetry, and default Linux service configurations. The VM instances ran data handlers and C2 components, treating Linux not as a primary attack vector but as a concealed subsystem for persistence and exfiltration.

- Bypassed host EDR through malware isolation within Linux VMs, circumventing standard detection techniques.
- Leveraged virtualization layers to conceal outbound C2 traffic behind legitimate host IP addresses.
- Shifted persistence and control into Linux environments that lacked active monitoring or hardened configurations.
- Introduced stealth paths via systemd overrides, .so preloading, and cron-based persistence inside Linux VMs.
- Expanded threat surface by transforming virtualization from infrastructure utility into attacker advantage.

Observations

- Use of Windows Hyper-V to deploy minimalistic (120MB) Alpine Linux VMs.
- Operation of CurlyShell and CurlCat malware entirely within Linux VMs.
- PowerShell-based Kerberos ticket injection and unauthorized local account creation.
- VM-based persistence survives Windows resets and reboots without triggering alerts.
- No exploitation of Linux kernel flaws—focus was on operational security weaknesses and misconfigurations.

Guidance

Strategic Intelligence

- **Trends**
  - Hybrid intrusion models are maturing, with threat actors embedding cross-platform persistence in virtual machines.
  - Linux systems—particularly guest VMs—are increasingly leveraged as covert operational environments within Windows networks.
  - Virtualization misuse is emerging as a durable tactic in long-term espionage operations, particularly where host monitoring is assumed to be comprehensive.

RETURN >>>

Operational Intelligence

- **Threat Vectors**
  - Hyper-V-enabled deployment of Linux VMs as covert execution environments.
- **Monitoring & Detection Gaps**
  - Lack of telemetry from guest OS activity and insufficient correlation between virtualization and endpoint logs.
- **Response Actions**
  - Audit all endpoints for unauthorized VM installations and Hyper-V role activations.
  - Review domain-wide creation of local accounts and investigate recent LSASS access patterns.
  - Inspect virtualization and container logs for unexpected activity or persistent processes.

Tactical Intelligence

- **Mitigation Strategies**
  - Disable Hyper-V on systems that do not require virtualization capabilities.
  - Monitor for unexpected VM deployment activity and analyze virtual switch logs for irregular traffic patterns.
  - Deploy logging agents within guest VMs and enforce visibility parity across host and virtual OS.
- **Preventive Measures**
  - Harden Linux environments with enforced SELinux/AppArmor policies and auditd-based event tracking.
  - Align Linux telemetry with Windows event data to detect hybrid persistence chains.
  - Map behaviors to MITRE ATT&CK v17 for both Linux and Windows to identify gaps in defensive coverage.

Threat Hunting Hypotheses

Linux VM Deployed as Persistent Execution Layer in Windows Hosts

Hypothesis: Curly COMrades deployed Alpine Linux VMs via Hyper-V for covert operations.

Investigation Steps

- Search Windows Event Logs for Hyper-V installation (Event ID 14000–15000).
- Identify VHD/VHDX files with minimal size and recent activity in unusual locations.
- Correlate network activity originating from host IPs with Linux-like traffic signatures (e.g., SSH, curl-based requests).
- Inspect for ELF binaries named CurlyShell or CurlCat within VM disk images.
- Confirm by mapping VM lifecycle events to suspicious outbound traffic or authentication anomalies.

Tactical Guidance

MFA Bypass Through Social Engineering

Hypothesis: PowerShell scripts injected Kerberos tickets and created persistent local accounts.

Investigation Steps

- Review PowerShell logs for encoded or obfuscated scripts invoking LSASS or kerberos APIs.
- Examine Security Event Logs (4720, 4732) for unapproved user creation.
- Cross-reference process creation logs for PowerShell spawning access to memory injection routines.
- Validate hypothesis through replay of TTPs in controlled environments.

Sources

- The Hacker News: Hackers Weaponize Windows Hyper-V to Hide Linux VM and Evade EDR Detection
- Dark Reading: Pro-Russian Hackers Use Linux VMs to Hide in Windows
- The Record: Russia-linked 'Curly COMrades' turn to malicious virtual machines for digital spy campaigns
- LinuxSecurity.com: Linux Kernel Security 2025 – Curly COMrades Exploits and Risks Exposure
- Security Affairs: Curly COMrades Exploit Windows Hyper-V to Evade EDRs

SOFTWARE SUPPLY CHAIN

Overview & Impact

The technical sophistication of deepfake attacks in 2025 encompasses three primary vectors: video, audio, and hybrid multi-modal operations. Video deepfakes utilize generative adversarial networks (GANs) trained on publicly available footage to create photorealistic impersonations. Audio deepfakes leverage neural voice synthesis, requiring minimal input data - as little as 3-5 seconds for basic cloning or 20-30 seconds for high-fidelity reproduction. Hybrid attacks combine both technologies, exemplified by the Hong Kong incident where criminals created an entire fake video conference with multiple deepfaked participants. The infrastructure supporting these attacks includes cloud-based rendering farms, distributed C2 networks, and cryptocurrency money laundering chains that can move funds within minutes of successful fraud.

- **Trust Erosion in Open Source:** Hundreds of trusted npm packages were used as distribution vectors, undermining confidence in community-maintained dependencies.
- **Credential Exposure:** Stolen GitHub PATs, npm tokens, and cloud API keys exposed organizational environments to lateral movement, cloud service abuse, and downstream compromise.
- **Operational Disruption:** NuGet logic bombs threaten delayed sabotage of critical systems, complicating incident response and potentially disrupting industrial operations years after compromise.
- **Regulatory and Compliance Risk:** These attacks increase the likelihood of non-compliance with software assurance, SBOM, and third-party risk mandates.

RETURN >>>

Observations

- Use of self-replicating worms leveraging GitHub Actions
- Deployment of AI-assisted scripts containing obfuscated code and emojis
- Public data exposure via automated GitHub repo creation (e.g., "Shai-Hulud")
- Widespread abuse of package.json post-install scripts • Discovery of over 150,000 non-functional token-farming packages targeting blockchain incentives

Guidance

Strategic Intelligence

- **Trend**
  - Automation abuse and persistent identity compromise are now baseline tactics in software supply chain attacks.
  - CI/CD workflows and package managers are primary threat vectors.
  - Logic bombs introduce time-shifted threats, complicating forensics and response timelines.

Operational Intelligence

- **hreat Vectors**
  - Phishing campaigns and GitHub Action misconfigurations (e.g., pull_request_target abuse)
  - Package metadata abuse and circular dependencies in npm
- **Monitoring & Detection Gaps**
  - Limited validation on publishing workflows and artifact updates
  - Insufficient auditability of long-lived developer credentials
- **Response Actions**
  - Revoke and rotate all developer tokens and PATs immediately
  - Audit CI/CD workflows for unauthorized publishing activity
  - Remove or downgrade affected packages and rebuild with verified artifacts

Tactical Intelligence

- **Mitigation Strategies**
  - Block webhook[.]site domains and known IOCs at egress points
  - Detect unauthorized repo creation and credential exfiltration scripts
- **Preventive Measures**
  - Mandate hardware-backed 2FA (e.g., FIDO2) for registry and SCM accounts
  - Implement SBOM enforcement and dependency age gating in CI pipelines
  - Disable auto-install scripts and enforce review of new package additions

Tactical Guidance

Threat Hunting Hypotheses

Compromised SCM Token Propagation via GitHub Actions

Hypothesis: Malicious packages used automated CI workflows to exfiltrate secrets and create new malware-laden packages.

Investigation Steps

- Search GitHub audit logs for public repo creation with names containing "Shai-Hulud"
- Review CI pipeline logs for unexpected publishes and YAML workflows
- Inspect package.json and install scripts for credential-harvesting behavior
- Correlate installation timestamps with outbound DNS or HTTP(S) traffic to known C2s
- Validate incident scope by comparing to package-lock or yarn.lock references

Sources

- Palo Alto Networks: "Shai-Hulud" Worm Compromises npm Ecosystem
- Dark Reading: 150,000 Packages Flood NPM Registry in Token Farming Campaign
- CISA: Widespread Supply Chain Compromise Impacting npm Ecosystem
- Socket: Ongoing Supply Chain Attack Targets CrowdStrike npm Packages
- The Hacker News: Hidden Logic Bombs in Malware-Laced NuGet Packages
- Datadog: Learnings from Recent npm Supply Chain Compromises
- Industrial Cyber: Supply Chain Attacks Escalate Against Industrial Sectors
- Cyble: Record Surge in Software Supply Chain Attacks

RETURN >>

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

pellera.com

A PELLERA PODCAST

Edge of I.T.