pellera

THREAT INTEL REPORT 2025

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

AUGUST

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 August 2025

Three parallel threat developments from late 2024 reveal how cybercriminals and state actors are systematically exploiting the fundamental transformation of enterprise IT infrastructure. The Vietnamese-operated "**Ghost in the Zip**" campaign demonstrates how threat actors now weaponize legitimate cloud platforms—Telegram, Cloudflare Workers, and Dropbox—to create resilient command-and-control ecosystems that frustrate traditional takedown efforts. By **compromising over 4,000 victims across 62 countries and stealing 200,000 unique passwords** through sophisticated DLL sideloading techniques, this operation showcases how attackers have moved beyond simple malware distribution to establishing sustainable criminal business models with real-time data monetization through underground marketplaces.

The browser has emerged as the new primary battleground, with **95% of organizations** experiencing browser-based attacks as enterprises complete their migration to SaaS-first infrastructure. This represents a fundamental paradigm shift where traditional endpoint and network security controls become increasingly irrelevant as business operations occur entirely within browser environments. Attackers are exploiting this transformation by targeting the 10,000+ SaaS applications that modern enterprises typically manage, using sophisticated techniques like **ClickFix CAPTCHA spoofing** and **ChainLink phishing** that bypass conventional email security while leveraging trusted platforms for multi-step authentication mimicry.

Simultaneously, the emergence of the Russian-aligned "**Curly COMrades**" group introduces a novel persistence mechanism that exploits Microsoft's .NET Framework through COM object hijacking—a technique with universal applicability to any Windows environment globally. This advancement represents more than a new attack vector; it signals the evolution of state-sponsored groups toward techniques that can scale beyond geopolitical targets to affect any organization running standard enterprise infrastructure. The group's sophisticated use of compromised legitimate websites as traffic relays demonstrates how modern threat actors are building infrastructure that appears entirely benign while maintaining persistent access.

These convergent developments signal a maturation in the threat landscape where technical sophistication, economic sustainability, and operational resilience have reached unprecedented levels. Organizations can no longer assume that legitimate platforms are safe, that browsers are merely productivity tools, or that standard Windows environments provide adequate security through default configurations. Success now requires recognition that every cloud service, every browser session, and every .NET application represents a potential attack vector for adversaries who have fundamentally reimagined how cyber operations are conducted, funded, and sustained.

Executive Overview

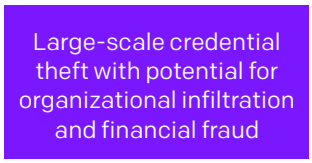
PXA STEALER "GHOST IN THE ZIP" CAMPAIGN

Audience

- CISO
- IT Operations Managers & Teams
- Risk Management Professionals
- Security Operations Team
- IT Security Managers
- Threat Intelligence Analysts

RISK

GEOGRAPHIC SCOPE



BUSINESS IMPACT

Vietnamese-speaking threat actors have conducted a sophisticated information stealer campaign since October 2024, utilizing the Python-based PXA Stealer malware to compromise over 4,000 victims across 62+ countries. The "Ghost in the Zip" operation demonstrates advanced evasion capabilities through DLL sideloading techniques with legitimate signed software (Haihaisoft PDF Reader, Microsoft Word 2013) and multi-stage deployment chains concealing payloads as image and PDF files. The campaign leverages a Telegram-powered ecosystem for automated data exfiltration and monetization, successfully stealing over 200,000 unique passwords, hundreds of credit card records, and 4+ million browser cookies. The operation targets financial platforms, cryptocurrency exchanges, and FinTech applications while feeding stolen data into underground marketplaces like Sherlock through subscription-based criminal services. The exclusive use of legitimate cloud infrastructure (Telegram, Cloudflare Workers, Dropbox) creates resilient command-and-control capabilities that frustrate traditional detection and takedown efforts.

READ MORE: PXA STEALER "GHOST IN THE ZIP" CAMPAIGN

SAME WAR, NEW BATTLEFRONT

Audience

- CISO
- IT Security Managers
- Security Operations Teams
- Compliance & Regulatory Affairs Teams

Browser-based attacks have emerged as the dominant threat vector, exploiting

RISK

GEOGRAPHIC SCOPE

INDUSTRY IMPACT

the fundamental shift to SaaS-based enterprise infrastructure. Attackers are systematically bypassing traditional security controls by targeting the browser environment where modern work occurs. Organizations face a critical security blind spot as 95% have experienced browser-based attacks while traditional defensive tools lack adequate visibility into browser-layer threats.

READ MORE: SAME WAR, NEW BATTLEFRONT

Audience

- CISO
- Board of Directors & Executive Leadership
- IT Security Managers
- Incident Response Teams
- Threat Intelligence Analysts
- Risk Management Professionals
- Network Operations Center (NOC) Personnel

CURLY COMRADS

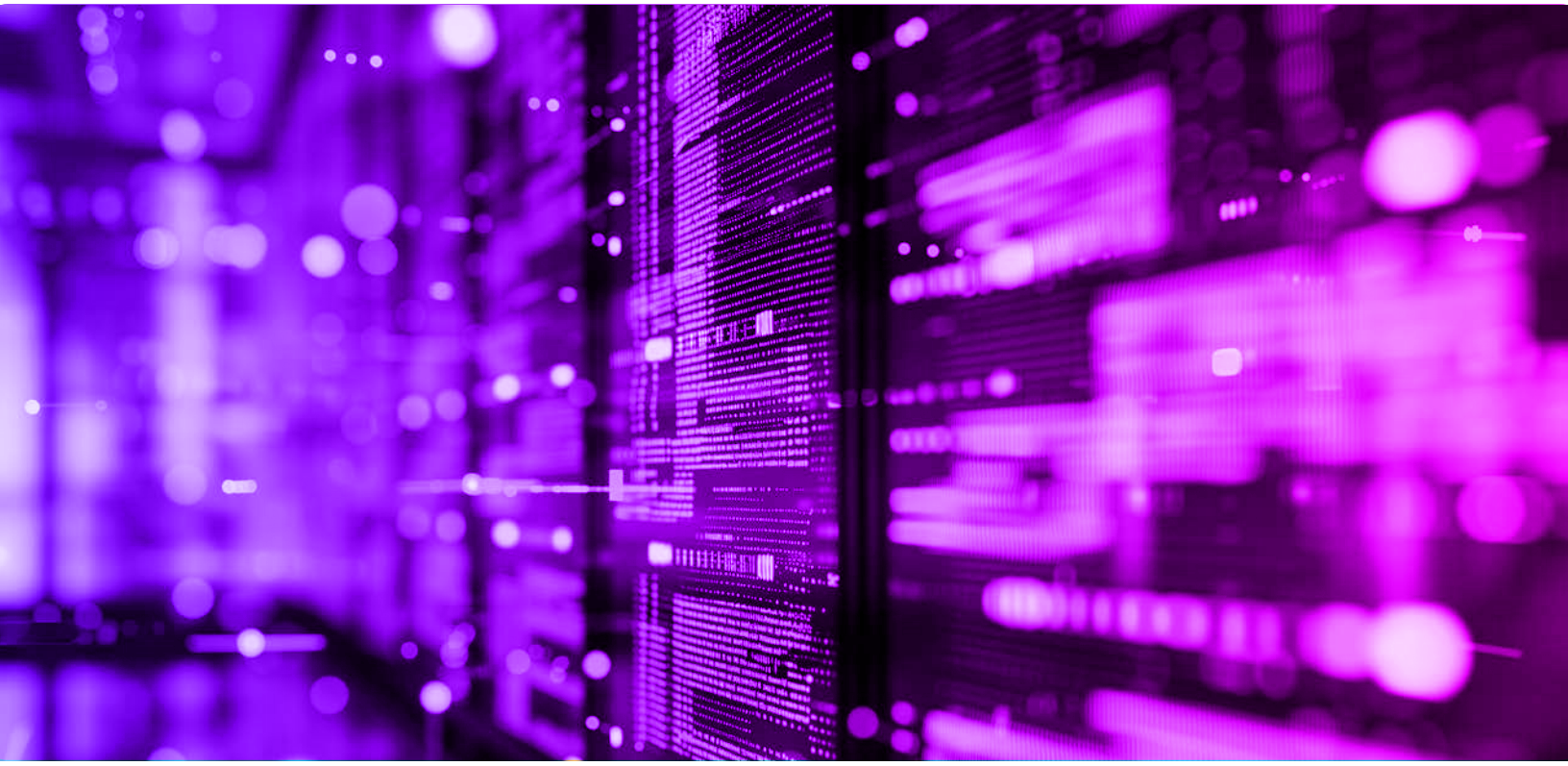
HIGH
RISK

GLOBAL
GEOGRAPHIC SCOPE

ALL SECTORS
INDUSTRY IMPACT

A previously unknown Russian-aligned Advanced Persistent Threat (APT) group designated "Curly COMrades" has been conducting sophisticated cyber espionage operations initially targeting government and energy infrastructure in Georgia and Moldova since mid-2024. The group employs a novel persistence mechanism exploiting Microsoft's .NET Framework Native Image Generator (NGEN) through COM object hijacking, representing an unprecedented technique with global implications for any organization running Windows/.NET environments. The campaign demonstrates advanced operational security with heavy reliance on legitimate compromised websites as traffic relays, custom malware toolsets, and strategic targeting methodologies that could be replicated against organizations worldwide involved in geopolitically sensitive sectors or supply chains.

READ MORE: CURLY COMRADS



Tactical Guidance

PXA STEALER "GHOST IN THE ZIP" CAMPAIGN

Overview & Impact

PXA Stealer campaign experienced sophisticated information theft operations targeting global victims since October 2024, utilizing advanced evasion techniques and legitimate software abuse. The campaign leveraged DLL sideloading with signed applications including Haihaisoft PDF Reader and Microsoft Word 2013, multi-stage Python deployment chains, and Telegram-powered infrastructure for automated data exfiltration. Vietnamese-speaking threat actors established resilient command-and-control capabilities through exclusive use of legitimate cloud platforms while monetizing stolen data through underground marketplaces.

- Complete compromise of over 4,000 victims across 62+ countries with concentrated targeting in South Korea, United States, Netherlands, Hungary, and Austria
- Theft of over 200,000 unique passwords, hundreds of credit card records, and 4+ million browser cookies from financial and cryptocurrency platforms
- Potential organizational infiltration through compromised employee credentials creating downstream business email compromise and lateral movement risks
- Extensive data monetization through Telegram-powered subscription services feeding criminal marketplaces like Sherlock for automated resale operations
- Regulatory compliance exposure under GDPR, PCI DSS, and regional data protection laws across multiple jurisdictions
- Supply chain implications from compromised VPN, cloud application, and financial platform credentials enabling secondary attacks against victim organizations

Attribution & Assessment

- **Threat Actor:** PXA Stealer Operators - Vietnamese-Speaking Cybercriminal Group
- **Assessed Attribution:** Sophisticated Vietnamese cybercriminal organization demonstrating advanced technical capabilities through legitimate software abuse, cloud infrastructure exploitation, and automated monetization systems with potential connections to broader Southeast Asian cybercrime ecosystem
- **Confidence Level:** High based on Vietnamese language artifacts in malware samples, operational timing patterns consistent with UTC+7 timezone, and documented attack infrastructure patterns matching known Vietnamese threat actor methodologies.

Threat Implications

- **Technical Sophistication Evolution:** Vietnamese cybercriminal groups transitioning from commodity malware distribution to advanced persistent operations with custom tooling and legitimate platform abuse
- **Infrastructure Resilience:** Exclusive use of legitimate cloud platforms (Telegram, Cloudflare, Google Drive) provides operational durability and complicates traditional blocking approaches
- **Monetization Scalability:** Real-time data processing and marketplace integration through subscription services enables sustainable criminal business model with rapid victim-to-revenue conversion
- **Geographic Targeting Precision:** Concentrated focus on financially valuable regions (South Korea, Netherlands) indicates strategic victim selection based on economic intelligence
- **Supply Chain Risk Multiplication:** Compromised credentials from VPN, cloud applications, and financial platforms create cascading organizational vulnerabilities beyond initial victim impact
- **Regulatory Compliance Weaponization:** Multi-jurisdictional victim distribution creates complex compliance obligations under GDPR, PCI DSS, and regional data protection frameworks

RETURN >>>

Tactical Guidance

Notable Campaigns

- **PXA Stealer "Ghost in the Zip" (October 2024-Present):** Primary campaign utilizing DLL sideloading with Haihaisoft PDF Reader and Microsoft Word 2013 targeting 4,000+ victims across 62 countries
- **ChainLink Phishing Operations:** Multi-step authentication mimicry campaigns using trusted cloud services to bypass traditional email security controls
- **ClickFix CAPTCHA Spoofing:** Sophisticated interface replication attacks tricking users into executing PowerShell commands through fake CAPTCHA interfaces
- **Telegram Marketplace Integration:** Automated data monetization through "Sherlock" criminal marketplace with subscription-based access to stolen credentials and financial data

MITRE ATT&CK Framework Mapping

- **T1574.002 (Hijack Execution Flow: DLL Side-Loading):** Exploitation of legitimate signed applications including Microsoft Word 2013 and Haihaisoft PDF Reader for malicious DLL execution from user directories
- **T1036 (Masquerading):** Python interpreter process masquerading as legitimate system processes (svchost.exe) to evade behavioral detection and process monitoring
- **T1027 (Obfuscated Files or Information) :** Multi-stage deployment chains utilizing encrypted archives and file extension masquerading to bypass static analysis and sandbox environments
- **T1555 (Credentials from Password Stores):** Systematic browser credential harvesting targeting financial platforms, cryptocurrency services, and enterprise authentication systems
- **T1041 (Exfiltration Over C2 Channel):** Automated data exfiltration via Telegram Bot API with Cloudflare Workers relay infrastructure for command and control resilience
- **T1102 (Web Service):** Legitimate platform abuse including Google Drive, Dropbox, and AWS for malware hosting and command and control communications
- **T1566.001 (Phishing: Spearphishing Attachment):** Archive-based phishing campaigns delivering legitimate software bundled with malicious DLL components through email vectors
- **T1055 (Process Injection):** Browser injection techniques targeting encryption mechanisms and credential storage systems for real-time data collection
- **T1547.001 (Boot or Logon Autostart Execution: Registry Run Keys):** Persistence establishment through Windows Registry Run key modifications with deceptive service names

Observations

- Attackers exploit legitimate platforms (Google Drive, Dropbox, AWS) to host malicious content and evade reputation-based filtering
- ChainLink Phishing employs multi-step authentication mimicry using trusted services to bypass traditional email security
- ClickFix attacks replicate legitimate CAPTCHA interfaces to trick users into executing PowerShell commands
- Malware reassembly techniques like ClearFake and SocGolish dynamically construct malicious code within browser environments
- Traditional security tools (EDR, email gateways, network filters) lack visibility into browser Document Object Model (DOM) manipulation
- Browser extensions present an largely unmonitored attack surface with deep system access privileges

RETURN >>>

Guidance

Strategic Intelligence

- **Trend**
  - Information stealer campaigns evolving toward cloud-native infrastructure abuse with automated monetization ecosystems replacing traditional malware distribution models
  - Vietnamese cybercriminal groups demonstrating increasing technical sophistication and organizational maturity with potential evolution toward advanced persistent threat capabilities
  - Legitimate platform abuse becoming primary attack vector with Telegram, Cloudflare Workers, and cloud storage services weaponized for malware operations
  - Subscription-based criminal services enabling lower-barrier entry for downstream threat actors through real-time data processing and marketplace integration
  - DLL sideloading vulnerabilities in widely-deployed legitimate software creating systemic risk across enterprise environments
- **Business Risk Context**
  - Employee credential compromises create cascading organizational risks through business email compromise and lateral movement attack opportunities
  - Financial platform targeting exposes direct monetary theft risks and regulatory compliance violations under multiple jurisdictional frameworks
  - Supply chain implications from compromised VPN and cloud application credentials enabling secondary attacks against organizational infrastructure
  - Board-level concerns regarding third-party risk management and employee security awareness program effectiveness
  - Regulatory compliance exposure requiring immediate assessment under GDPR, PCI DSS, and regional data protection laws
- **Security Enhancements**
  - Application control policies requiring immediate implementation to prevent unauthorized DLL loading and Python interpreter abuse
  - Behavioral monitoring capabilities for cloud service abuse patterns and non-standard process execution from user directories
  - Credential monitoring and rotation programs for employees in heavily affected geographic regions
  - Threat intelligence integration for real-time monitoring of organizational domain exposure in criminal marketplaces

Operational Intelligence

- **Threat Vectors**
  - DLL sideloading attacks targeting legitimate signed applications creating bypass opportunities for traditional endpoint protection platforms
  - Multi-stage deployment chains utilizing encrypted archives and file extension masquerading to evade static analysis and sandbox detection
  - Telegram Bot API automation for command-and-control communications requiring enhanced network monitoring and behavioral analysis
  - Python interpreter abuse from user-accessible directories necessitating process execution monitoring and application allowlisting
  - Browser injection techniques targeting encryption mechanisms requiring enhanced endpoint detection and response capabilities
- **Monitoring & Detection Gaps**
  - Insufficient behavioral detection for legitimate tool abuse including certutil, WinRAR, and Python interpreter misuse

RETURN >>>

- Limited visibility into Telegram API communications and Cloudflare Workers traffic patterns indicating malware command-and-control
- Inadequate process parent-child relationship analysis for detecting signed application abuse and DLL sideloading attempts
- Missing correlation between archive extraction activities and subsequent network communications to known malicious infrastructure
- Limited threat intelligence integration for real-time monitoring of organizational credential exposure in criminal data markets

- **Response Actions**
  - Deploy expanded IOC monitoring across all security platforms with focus on Vietnamese threat actor infrastructure and Telegram bot tokens
  - Implement enhanced email security controls to detect phishing campaigns delivering archive-based malware with legitimate software components
  - Activate credential monitoring services for organizational domains and employee email addresses across commercial threat intelligence feeds
  - Coordinate with legal teams for regulatory compliance assessment and potential law enforcement cooperation regarding credential theft

Tactical Intelligence

- **Mitigation Strategies**
  - Implement application control policies preventing execution of Python interpreters from user-accessible directories (%TEMP%, %PUBLIC%, Downloads)
  - Deploy strict DLL loading policies for Microsoft Office applications and PDF readers preventing sideloading from non-system directories
  - Configure network monitoring for Telegram Bot API traffic patterns with automated alerting for large POST requests and file uploads
  - Establish behavioral analytics for process execution anomalies including renamed system processes and unusual parent-child relationships
  - Reset credentials for employees in heavily affected regions (South Korea, Netherlands, Hungary, Austria) within 24-hour response window

- **Preventive Measures**
  - Deploy user education programs focused on archive-based phishing attacks and legitimate software bundled with malicious components
  - Implement email security controls detecting suspicious attachment combinations including signed applications with DLL files
  - Establish endpoint detection rules for certutil decoding operations targeting files with non-executable extensions
  - Configure SIEM alerting for WinRAR/7-Zip execution with password parameters and extraction to system directories
  - Deploy network segmentation preventing direct internet access from critical systems and implementing proxy-based web filtering

RETURN >>>

Threat Hunting Hypotheses

DLL Sideloading via Legitimate Applications

Hypothesis: PXA Stealer gains initial access through DLL sideloading attacks targeting legitimate signed applications including Microsoft Word 2013 and Haihaisoft PDF Reader.

Investigation Steps

- Review Windows process creation events for signed applications (winword.exe, PDF readers) with unusual command-line parameters or working directories
- Correlate DLL load events with process creation to identify non-Microsoft DLLs (msvcr100.dll) loaded by Microsoft applications
- Analyze file hash reputation for DLL files loaded from user-accessible directories (%TEMP%, %PUBLIC%, Downloads)
- Monitor for Windows Registry Run key modifications with suspicious service names like "Windows Update Service"
- Cross-reference signed application execution with subsequent Python interpreter launches from user directories

Python Interpreter Masquerading as System Processes

Hypothesis: Attackers rename Python interpreters as svchost.exe and execute obfuscated scripts from user directories to evade detection.

Investigation Steps

- Search for python.exe or renamed Python interpreter executions from non-standard installation paths (%PUBLIC%, %TEMP%)
- Monitor command-line arguments for Python scripts with suspicious names (images.png, Photos) or encoded content execution
- Correlate Python process creation with network connections to Telegram API endpoints (api.telegram.org)
- Analyze parent-child process relationships for Python interpreters spawned by Microsoft Office applications
- Review file system artifacts for Python libraries extracted to Windows system directory impersonation folders

Telegram Bot API Data Exfiltration

Hypothesis: PXA Stealer uses automated HTTP POST requests to Telegram Bot API endpoints for data exfiltration, potentially relayed through Cloudflare Workers.

Investigation Steps

- Monitor outbound HTTPS traffic to api.telegram.org with large POST request bodies containing ZIP archive uploads
- Correlate Telegram API communications with local ZIP archive creation patterns in user directories
- Analyze HTTP User-Agent strings for Python requests library patterns and non-standard Telegram client behaviors
- Review DNS queries for workers.dev domains (lone-none-1807.workers.dev pattern) indicating Cloudflare Workers relay usage
- Check network traffic for specific bot token patterns (7414494371:AAHsrQDkPrEVyz9z0RoiRS5fJKI-ihKJpzQ)

RETURN >>>

Tactical Guidance

Sources

- **Ghost in the Zip:** New PXA Stealer and Its Telegram-Powered Ecosystem
- Ghost in the Zip Reveals Expanding Ecosystem Behind PXA Steal

SAME WAR, NEW BATTLE FRONT

Overview & Impact

The cybersecurity threat landscape has undergone a fundamental transformation as attackers systematically abandon traditional endpoint and network attack vectors in favor of sophisticated browser-based techniques. This strategic shift directly corresponds to enterprise IT's comprehensive migration to cloud and SaaS platforms, where web browsers have evolved from simple productivity tools into the primary interface for all business-critical operations.

Traditional cyber attack methodology relied on a consistent pattern: compromise endpoints through software exploits or malware deployment, establish lateral movement within internal networks, and target privileged systems for data theft or ransomware deployment. However, the SaaS-ification of enterprise infrastructure has rendered this approach increasingly ineffective. With core business systems no longer locally deployed and centrally managed, attackers have adapted by targeting the browser environment where digital identities are created, managed, and utilized.

The browser has emerged as both the primary attack surface and the gateway to organizational assets. Modern enterprises typically utilize approximately 10,000 SaaS applications, each accessed through browser interfaces, creating an expansive and complex attack surface that traditional security controls cannot adequately monitor or protect. This transformation represents a paradigm shift comparable to the transition from physical to digital infrastructure, requiring entirely new defensive approaches.

Impact

- 95% of surveyed organizations experienced browser-based attacks within the past 12 months
- 94% suffered successful phishing incidents specifically targeting browser environments
- 752,000 browser-based phishing attempts were observed in 2024, representing a 140% year-over-year increase
- 98% of organizations reported BYOD policy violations that create browser-based security gaps
- 65% of organizations have minimal or no control over sensitive data shared in GenAI applications accessed through browsers
- 64% of encrypted web traffic remains uninspected due to business operational requirements
- 70% of multi-step phishing campaigns specifically impersonate Microsoft, OneDrive, or Office 365 applications

Attack Lifecycle

- **Phase 1:** Initial access via trusted platforms (Google Drive, Dropbox, Microsoft services)
- **Phase 2:** Multi-step redirection through legitimate domains to avoid detection

RETURN >>

- **Phase 3:** Credential harvesting or session token theft through spoofed interfaces
- **Phase 4:** Account takeover and lateral movement through compromised identities

Attribution & Assessment

- **Threat Actor:** Browser-Based Attack Ecosystem
- **Assessed Attribution:** Global cybercriminal ecosystem including state-aligned groups, financially motivated actors, and commodity threat groups with demonstrated browser-targeting capabilities
- **Confidence Level:** High based on widespread adoption across threat actor categories and documented attack campaigns.

Threat Implications

- **Technique Democratization:** Browser-based attack methods are accessible to low-sophistication actors through readily available toolkits and services
- **Cross-Platform Scalability:** Attack techniques function universally across Windows, macOS, and Linux environments through standardized browser interfaces
- **Operational Resilience:** Multi-step attack chains using legitimate platforms provide built-in redundancy and detection evasion
- **Economic Viability:** High success rates and low infrastructure costs drive continued investment in browser-based attack development
- **Global Reach Potential:** SaaS-first business models create universal attack surfaces independent of geographic location or organizational size

Notable Campaigns

- **Scattered Spider (2025):** Advanced social engineering campaigns targeting help desk systems and browser-based identity theft
- **Snowflake Breach Campaign (2024):** Mass credential reuse attacks leveraging infostealer-harvested browser data dating to 2020
- **ClearFake/SocGolish Operations:** Ongoing malware reassembly campaigns utilizing JavaScript injection in legitimate websites
- **ClickFix Campaign Operators:** Sophisticated CAPTCHA spoofing attacks targeting enterprise browser environments

MITRE ATT&CK Framework Mapping

- **T1566.002 (Phishing: Spearphishing Link):** Universal technique applicable across all browser platforms and SaaS environments
- **T1539 (Steal Web Session Cookie):** Cross-platform session hijacking methodology targeting browser-stored authentication tokens
- **T1185 (Browser Session Hijacking):** Browser-agnostic technique for maintaining persistent access to authenticated sessions
- **T1176 (Browser Extensions):** Platform-independent malicious extension deployment affecting Chrome, Firefox, Safari, and Edge browsers
- **T1566.001 (Phishing: Spearphishing Attachment):** Malicious file delivery through browser downloads circumventing email security controls
- **T1204.001 (User Execution: Malicious Link):** Social engineering technique exploiting user trust in browser-presented content
- **T1056.003 (Input Capture: Web Portal Capture):** Credential harvesting through spoofed authentication interfaces in browser environments
- **T1583.001 (Acquire Infrastructure: Domains):** Domain registration and compromise for hosting browser-based attack infrastructure

RETURN >>>

- **T1102 (Web Service):** Legitimate platform abuse (Google Drive, Dropbox, AWS) for command and control communications
- **T1190 (Exploit Public-Facing Application):** Third-party script compromise affecting websites visited through corporate browsers

Observations

- Attackers exploit legitimate platforms (Google Drive, Dropbox, AWS) to host malicious content and evade reputation-based filtering
- ChainLink Phishing employs multi-step authentication mimicry using trusted services to bypass traditional email security
- ClickFix attacks replicate legitimate CAPTCHA interfaces to trick users into executing PowerShell commands
- Malware reassembly techniques like ClearFake and SocGolish dynamically construct malicious code within browser environments
- Traditional security tools (EDR, email gateways, network filters) lack visibility into browser Document Object Model (DOM) manipulation
- Browser extensions present an largely unmonitored attack surface with deep system access privileges

Guidance

Strategic Intelligence

Trend

- Browser-based attacks represent a fundamental shift in threat landscape as traditional perimeter defenses become less effective against SaaS-first infrastructure
- Identity compromise has become the primary attack objective, with browsers serving as both the target and delivery mechanism

Risk Context

- Organizations face regulatory compliance challenges as PCI DSS 4.0 introduces stricter browser security requirements
- The average large organization manages approximately 10,000 SaaS applications, creating vast attack surfaces through browser interfaces
- Business continuity risks increase as attackers target the browser environment where most productivity occurs

Compliance Impact

- PCI DSS 4.0 enforcement in March 2025 requires enhanced client-side security controls
- Financial services and healthcare sectors face heightened scrutiny for browser-based data protection

Security Enhancements

- Budget allocation toward Browser Detection & Response (BDR) capabilities
- Integration of browser security controls with existing SASE and Zero Trust architectures
- Identity security enhancement focusing on phishing-resistant authentication methods

Operational Intelligence

Threat Vectors

Multi-channel phishing campaigns utilizing email, instant messaging, social media, and malicious advertisements

RETURN >>>

- Third-party script compromise affecting legitimate websites visited by employees
- Browser extension exploitation through malicious or compromised add-ons

Monitoring & Detection Gaps

- Limited visibility into browser DOM manipulation and JavaScript execution
- Insufficient monitoring of credential input patterns and session behavior
- Lack of real-time analysis of web page modifications and script behavior

Response Actions

- Implement browser-based telemetry collection for security operations centers
- Establish incident response procedures specific to browser-based credential compromise
- Develop threat hunting capabilities focused on browser session anomalies

Tactical Intelligence

Mitigation Strategies

- Deploy browser isolation technologies for high-risk browsing activities
- Implement DNS-layer filtering to block known malicious domains before browser access
- Establish real-time monitoring of PowerShell execution from browser contexts
- Configure browser extension allowlisting to limit attack surface

Preventive Measures

- Enforce phishing-resistant authentication methods (FIDO2, WebAuthn) across critical applications
- Implement continuous monitoring of employee accounts for credential reuse and weak passwords
- Deploy secure browser solutions with built-in threat protection for sensitive operations

Security Enhancement

- Configure browser security policies through enterprise management platforms (Chrome Enterprise, Microsoft Edge for Business)
- Integrate browser-based threat detection with existing security orchestration workflows
- Establish automated response procedures for detected browser-based credential theft attempts

Validation and Testing

- Conduct phishing simulation exercises targeting browser-based attack scenarios
- Test browser security controls against known attack techniques (ClickFix, ChainLink Phishing)
- Validate incident response procedures through tabletop exercises focused on browser-based compromises

RETURN >>>

Threat Hunting Hypotheses

Credential Harvesting Through Spoofed Authentication Pages

Hypothesis: Employees are entering credentials into spoofed authentication pages that mimic legitimate corporate applications

Investigation Steps

- Monitor browser navigation patterns for unusual redirect chains leading to authentication pages
- Analyze credential input events for timing patterns inconsistent with normal user behavior
- Correlate authentication failures with subsequent successful logins from different geographic locations
- Examine browser extension activity during authentication events

Malicious Browser Extension Installation and Activity

Hypothesis: Users have installed malicious or compromised browser extensions that are exfiltrating data or credentials

Investigation Steps

- Audit installed browser extensions across enterprise endpoints
- Monitor extension permission requests and data access patterns
- Analyze network traffic for unusual data exfiltration during browser sessions
- Correlate extension installation events with subsequent security incidents

Sources

- **Palo Alto Networks:** Is Your Browser Ground Zero for Cyberattacks?
- **The420.in:** Here Is Why Your Browser Is the New Battleground for Phishing Attacks
- **BleepingComputer: The Browser Blind Spot:** Why Your Browser is the Next Cybersecurity Battleground
- **LNGFRM: The Browser:** Cybersecurity's Next Battleground
- **Security Buzz: ClickFix and the New Face of Phishing:** Why Your Browser Is the Next Battleground
- **Security Boulevard:** Why the Browser Is Becoming a Prime Security Battleground
- **Push Security:** How the Browser Became the Main Cyber Battleground

CURLY COMRADS

Overview & Impact

Curly COMrades represents a sophisticated cyber espionage campaign with demonstrated capabilities that pose significant risks to organizations globally. While initially focused on specific geopolitical targets, the technical methodologies and operational patterns indicate scalable approaches applicable to diverse international targets across multiple sectors.

Impact

- **Multinational Corporations:** Supply chain infiltration through subsidiaries in targeted regions
- **Critical Infrastructure:** Energy, telecommunications, and financial services operators with international presence

RETURN >>>

- **Government Contractors:** Defense and intelligence sector suppliers regardless of geographic location
- **Technology Companies:** Organizations developing or maintaining .NET Framework applications globally
- **International NGOs:** Humanitarian and development organizations operating in geopolitically sensitive regions

Attack Lifecycle

- **Initial Access:** Adaptable vectors including spear-phishing, supply chain compromise, or third-party service exploitation
- **Persistence:** CLSID hijacking applicable to any Windows/.NET environment globally
- **Privilege Escalation:** Credential dumping techniques effective across international Windows deployments
- **Defense Evasion:** Compromised website relay methodology scalable to any geographic region
- **Collection:** Data harvesting techniques applicable to organizations with Active Directory infrastructure worldwide
- **Exfiltration:** Automated exfiltration capabilities adaptable to global compliance and regulatory environments

Attribution & Assessment

- **Threat Actor:** Curly COMrades (newly designated)
- **Assessed Attribution:** Russian Federation intelligence services or aligned proxy group with global operational capability
- **Confidence Level:** High based on technical sophistication and operational methodology

Threat Implications

- **Scalable TTPs:** Technical approaches demonstrated are platform-agnostic and geographically transferable
- **Operational Adaptability:** Campaign methodology suggests capability for rapid target diversification
- **Infrastructure Sophistication:** Use of compromised legitimate websites indicates global reach potential

MITRE ATT&CK Framework Mapping

- T1055 (Process Injection) - Globally applicable to Windows environments
- T1547.001 (Boot or Logon Autostart Execution) - Universal Windows persistence technique
- T1087 (Account Discovery) - Standard enterprise network reconnaissance
- T1003 (OS Credential Dumping) - Cross-platform credential theft methodology
- T1090 (Proxy) - Infrastructure technique applicable worldwide
- T1041 (Exfiltration Over C2 Channel) - Universal data theft approach

Observations

- **Platform Universality:** NGEN COM hijacking technique affects all Windows environments with .NET Framework globally
- **Scalable Infrastructure:** Compromised website relay approach demonstrates capability for worldwide operations
- **Adaptable Targeting:** Methodologies applicable beyond initial geopolitical focus to any high-value targets
- **Enterprise-Grade TTPs:** Techniques sophisticated enough to threaten major multinational corporations

RETURN >>>

- **Cross-Border Operations:** Evidence of infrastructure spanning multiple countries indicates global operational capability
- **Supply Chain Implications:** Targeting patterns suggest potential for third-party and vendor compromise affecting global supply chains

Guidance

Strategic Intelligence

Trend

- ORB networks represent the evolutionary advancement of traditional botnets, prioritizing stealth and persistence over volume
- Increasing adoption expected across threat actor spectrum, expanding beyond state-sponsored groups to cybercriminal enterprises
- Growing commoditization of ORB infrastructure indicates potential for "infrastructure-as-a-service" business models

Business Risk Context

- **Technology Sector:** Organizations developing or maintaining .NET applications face universal vulnerability.
- **Multinational Operations:** companies with subsidiaries or operations geopolitically sensitive regions at elevated risk.
- **Supply Chain Networks:** Global suppliers and vendors may serve as entry points for targeting primary objectives.
- **Critical Infrastructure:** Energy, Telecommunications, Financial services, and transportation sectors vulnerable regardless of location.

Security Enhancements

- **Unified Threat Detection:** Enterprise-wide visibility across all geographic locations and subsidiaries
- **International Incident Response:** Capabilities for coordinating response across multiple countries and legal jurisdictions
- **Supply Chain Security:** Enhanced third-party risk assessment and monitoring for global vendor networks
- **Cross-Border Threat Intelligence:** Information sharing partnerships with international cybersecurity organizations

Operational Intelligence

Threat Vectors

- **Universal Persistence:** NGEN COM hijacking effective against any Windows/.NET environment worldwide
- **Scalable Infrastructure:** Compromised website approach adaptable to any geographic region or language
- **Cross-Platform Applicability:** Core techniques transferable to cloud environments and hybrid infrastructure
- **Supply Chain Vectors:** Third-party compromise potential affects organizations regardless of direct targeting

Monitoring & Detection Gaps

- **Geographic Blind Spots:** Organizations may lack visibility into subsidiary or regional office security posture
- **Cross-Border Traffic:** International network communications may evade detection in globally distributed environments
- **Multi-Tenant Environments:** Cloud and shared infrastructure complicates attribution and detection
- **Third-Party Networks:** Limited visibility into vendor and partner security controls creates detection gaps

RETURN >>>

Response Actions

- **Enterprise-Wide Hunting:** Deploy detection capabilities across all geographic locations and business units
- **International Coordination:** Establish incident response protocols for multi-country operations
- **Supply Chain Assessment:** Enhanced security evaluation of all third-party vendors and partners globally
- **Cross-Border Monitoring:** Implement network monitoring for international data flows and communications

Tactical Intelligence

Mitigation Strategies

- Hunt for MucorAgent indicators across all Windows/.NET environments worldwide
- Monitor CLSID {de434264-8fe9-4c0b-a83b-89ebeebff78e} hijacking attempts in all regional Active Directory environments
- Block known malicious IP addresses at all international network perimeters and cloud environments
- Implement PowerShell execution monitoring across all global Windows deployments

Preventive Measures

- **Global LSASS Protection:** Deploy credential guard and protected process configurations across all Windows endpoints
- **International Network Segmentation:** Isolate critical systems from general network access in all geographic locations
- **Cross-Border Application Control:** Implement consistent application whitelisting policies across all international offices
- **Universal Logging Enhancement:** Standardize security logging configurations across all global infrastructure

Technical Implementation

Registry Monitoring

- **Deploy Across:** All Windows systems in all geographic locations
- **Monitor:** HKEY_USERS*\SOFTWARE\Classes\CLSID*\InprocServer32
- **Alert:** CodeBase modifications pointing to non-standard locations
- **Correlation:** Cross-reference with known compromise indicators globally

Network Detection

- **Coverage:** All network perimeters, cloud environments, and VPN connections
- **Monitor:** HTTP/HTTPS traffic with suspicious encoding patterns
- **Alert:** Data transfers to recently registered domains across all TLDs
- **Correlation:** Aggregate suspicious traffic patterns across all regions

Process Monitoring

- **Scope:** All Windows endpoints across enterprise
- **Monitor:** NGEN service executions outside maintenance windows
- **Alert:** PowerShell execution via System.Management.Automation without standard process
- **Correlation:** Pattern analysis across time zones and business units

RETURN >>>

Threat Hunting Hypotheses

MucorAgent Distribution

Hypothesis: MucorAgent or similar .NET-based malware is present in the environment using NGEN COM hijacking for persistence

Investigation Steps:

- **Registry Hunting:** Search for CLSID {de434264-8fe9-4c0b-a83b-89ebeebff78e} and {613fba38-a3df-4ab8-9674-5604984a299a} hijacking in HKEY_USERS*\SOFTWARE\Classes\CLSID*\InprocServer32
- **File System Analysis: Hunt for TaskLauncher.dll and related files in these locations:**
  - C:\ProgramData\Intel\Logs\Data\TaskLauncher.dll
  - C:\ProgramData**\AppConfig files
  - C:\Windows\Microsoft.NET\Framework64\v4.0.30319\ASP.NETWebAdminFiles\AppConfig\
- **Scheduled Task Investigation:** Examine ".NET Framework NGEN v4.0.30319 Critical" task for unusual execution patterns or modifications
- **PowerShell Execution Analysis:** Search for System.Management.Automation namespace usage without powershell.exe process execution
- **Encrypted Payload Detection: Look for PNG files without proper headers in:**
  - C:\Users*\AppData\Roaming\Microsoft\Windows\Templates\Curl\index.png
  - C:\ProgramData\Canon\OIPPESP\icon.png

Proxy Infrastructure Deployment

Hypothesis: Discovery of hijacked CLSIDs, suspicious .NET assemblies, or evidence of encrypted PowerShell payload execution

Investigation Steps

- **Network Service Discovery:** Scan for listening services on ports 55333, 55334, 443, 8443, 3000, and 52437
- **Process Analysis: Hunt for proxy tools masquerading as legitimate software:**
  - GoogleUpdate.exe in non-standard locations
  - chrome.exe in C:\Program Files (x86)\Google\
  - DRM.exe, java.exe, vmtools.exe in C:\ProgramData\ subdirectories
- **Network Flow Analysis: Examine outbound connections to known C2 infrastructure:**
  - 91.107.174.190
  - 96.30.124.103
  - 194.87.31.171
  - 75.127.13.136
  - 94.131.109.91
  - 207.180.194.109
- **SSH Configuration Hunt: Search for SSH configs and tunneling in:**
  - C:\ProgramData\Microsoft\UEV\Templates\SettingsLocationTemplate2013C.xsd
  - C:\Windows\System32\Config\SystemProfile\.ssh\
- **Custom Tool Detection:** Look for CurlCat variants and encoding/decoding tools with base64 substitution alphabets

RETURN >>>

Credential Harvesting Activity

Hypothesis: Evidence exists of NTDS database extraction, LSASS memory dumping, or browser credential theft

Investigation Steps

- **Volume Shadow Copy Analysis:** Search Windows Event Logs for unauthorized VSS snapshot creation (Event ID 8193, 8194)
- **Credential Dump Detection: Hunt for these artifacts in staging locations:**
  - NTDS.dit and SYSTEM files in C:\Users\Public\Documents\
  - LSASS dump files (lss.dmp, lsass.dmp) in C:\ProgramData\
  - Password-protected RAR archives with patterns like *J347Hw* or *B6uqLX3*
- **LSASS Dumping Tools: Search for custom credential dumping tools:**
  - TB.exe, TSB.exe, TBD.exe (TrickDump variants)
  - Results.exe with embedded shellcode
  - Procdump.exe usage targeting LSASS PID
- **DCSync Activity:** Analyze security logs for replication requests (Event ID 4662) with unusual source systems
- **Browser Data Theft: Look for copied browser credential files:**
  - Chrome Login Data files in C:\ProgramData\L
  - Firefox key4.db files in C:\ProgramData\k

Data Staging and Exfiltration

Hypothesis: Attackers have established data collection and exfiltration capabilities using curl.exe and custom scripts

Investigation Steps

- **Staging Directory Analysis: Examine C:\Users\Public\Documents\ for:**
  - Unusual file accumulation patterns
  - RAR archives with suspicious naming conventions
  - Recently created or modified sensitive files
- **Curl Usage Patterns: Hunt for suspicious curl.exe executions:**
  - POST requests with --upload-file parameters
  - Custom User-Agent strings: "Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0"
- **PowerShell Exfiltration Scripts: Search for run.ps1 variants containing:**
  - RAR file enumeration and upload loops
  - Sleep timers between upload attempts
  - Automatic file deletion after upload
- **Batch Script Analysis: Look for rar.bat and similar archiving scripts that:**
  - Compress files from staging directories
  - Use password protection with high compression levels
  - Split archives into specific volume sizes (2048k, 1024k)
- **Network Traffic Analysis:** Examine for encoded data transfers disguised as legitimate image files (PNG headers/footers)

RETURN >>>

Living-off-the-Land Binary (LOLBin) Abuse

Hypothesis: Attackers are using legitimate Windows tools and processes for malicious purposes

Investigation Steps

- **Command Line Analysis: Search command history and logs for suspicious usage of:**
  - netstat -anob, tasklist /v, systeminfo executed in rapid succession
  - wmic commands targeting logicaldisk, process information
  - reg query targeting HKLM\Security\Policy\Secrets
- **PowerShell Activity: Hunt for Active Directory enumeration commands:**
  - Get-ADTrust, Get-ADDomain, Get-ADUser with unusual parameters
  - PowerShell execution with -ep bypass flags
- **File System Tools: Look for suspicious usage of:**
  - icacls.exe modifying permissions on SSH keys or configuration files
  - vssadmin creating shadow copies outside maintenance windows
  - rundll32.exe loading comsvcs.dll for LSASS dumping
- **Network Discovery: Analyze for reconnaissance commands:**
  - arp -a, route print, ipconfig /all executed by non-admin users
  - ping commands targeting domain controllers
  - curl ipinfo.io for external IP verification
- **Persistence Mechanisms: Search for legitimate tools used for persistence:**
  - schtasks creating tasks with suspicious names or execution paths
  - sc create establishing services with misleading names

Sources

- **Bitdefender Business Insights: Curly COMrades:** A New Threat Actor Targeting Geopolitical Hotbeds
- **The Hacker News:** New 'Curly COMrades' APT Using NGEN COM Hijacking in Georgia, Moldova Attacks
- **CSO Online:** Russian APT group Curly COMrades employs novel backdoor and persistence tricks
- **COE Security:** Curly COMrads Cyber Spy Threat
- **BetterWorld Technology:** New 'Curly COMrades' APT Targets Eastern Europe with Stealthy NGEN COM Hijacking

RETURN >>>

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

pellera.com

A PELLERA PODCAST

Edge of I.T.