FLASHPOINT

2026 Global Threat Intelligence Report

Data, Insights, and Strategies for Navigating Today's Hybrid Threat Landscape

Table of Contents

Introduction

In 2026, the cybersecurity landscape has reached a point of total convergence, where the silos that once separated malware, identity, and infrastructure have collapsed into a single, high-velocity threat engine. Simultaneously, the threat landscape is shifting from human-led attacks to machine-speed operations as a result of agentic AI, which acts as a force multiplier for the modern adversary. Meanwhile, this same technology has become a growing risk for defenders who, in a race to keep pace, have integrated AI into production workflows without fully grasping the new vulnerabilities it introduces.

Flashpoint's 2026 Global Threat Intelligence Report (GTIR) was developed to anchor security leaders — from threat intelligence and vulnerability management teams to physical security professionals and the CISO's office — with the data required to navigate this year's greatest threats, rife with infostealers, vulnerabilities, ransomware, and malicious insiders.

This report is powered by Flashpoint's Primary Source Collection (PSC), a specialized operating model that collects intelligence directly from original sources, driven by an organization's unique Priority Intelligence Requirements (PIR) — not a vendor's fixed feed. PSC preserves context and provenance to provide a ground-truth view of the trends, tactics, and adversary behaviors that will define 2026.

Read on and you will gain:

1. **A Clear Understanding of the New Convergence Between Identity and AI**
   Discover how threat actors are preparing to transition from generative tools to sophisticated agentic frameworks. Learn how 3.3 billion compromised credentials are being weaponized via automated orchestration to bypass legacy defenses and exploit the connective tissue of modern corporate APIs.

2. **Intelligence on the "Franchise Model" of Global Extortion**
   Gain deep insight into the professionalized operations of today's most prolific threat actors. From the industrial efficiency of RaaS groups like RansomHub and Clop to the market dominance of the next generation of infostealer malware, we break down the economics driving today's cybercrime ecosystem.

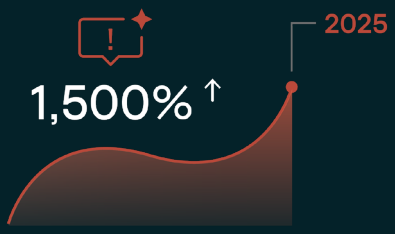
3. **A Blueprint for Proactive Defense and Risk Mitigation**
   Leverage the latest trends, in-depth analysis, and data-driven insights driven by Primary Source Collection to bolster your security posture by identifying and proactively defending against rising attack vectors.

Protecting organizations, industries, and communities is a shared mission that requires us to work together as one team. With that in mind, I'm proud to provide our customers and the larger community with the insights they need to fortify defenses and proactively manage risk in the face of an ever-evolving threat landscape.

Josh Lefkowitz
Flashpoint Co-Founder and CEO

Executive Summary: The Top Threats at a Glance

Flashpoint Identified Four Driving Themes Shaping the 2026 Threat Landscape

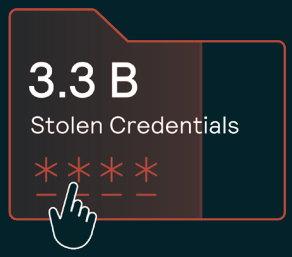


2026 is the Era of Agentic-Based Cyberattacks

Flashpoint identified a **1,500%** rise in AI-related illicit discussions between November and December 2025, signaling a rapid transition from criminal curiosity to the active development of malicious frameworks. Built on data pulled from criminal environments and shaped by fraud use cases, these systems scrape data, adjust messaging for specific targets, rotate infrastructure, and learn from failed attempts without the need for constant human involvement.

Identity is the New Exploit

Flashpoint observed over **11.1 million** machines infected with infostealers in 2025, fueling a massive inventory of **3.3 billion** stolen credentials and cloud tokens. The fundamental mechanics of cybercrime have shifted from breaking in to logging in, as attackers leverage stolen session cookies to behave like legitimate users.

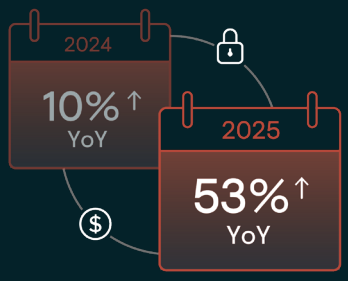


The Patching Window is Rapidly Closing

Vulnerability disclosures surged by **12%** in 2025, with **1 in 3 (33%)** vulnerabilities having publicly available exploit code. The strategic gap between discovery and weaponization is increasingly vanishing, as evidenced by mass exploitation of zero-day vulnerabilities in as little as 24 hours after discovery.

Ransomware is Hacking the Person, Not the Code

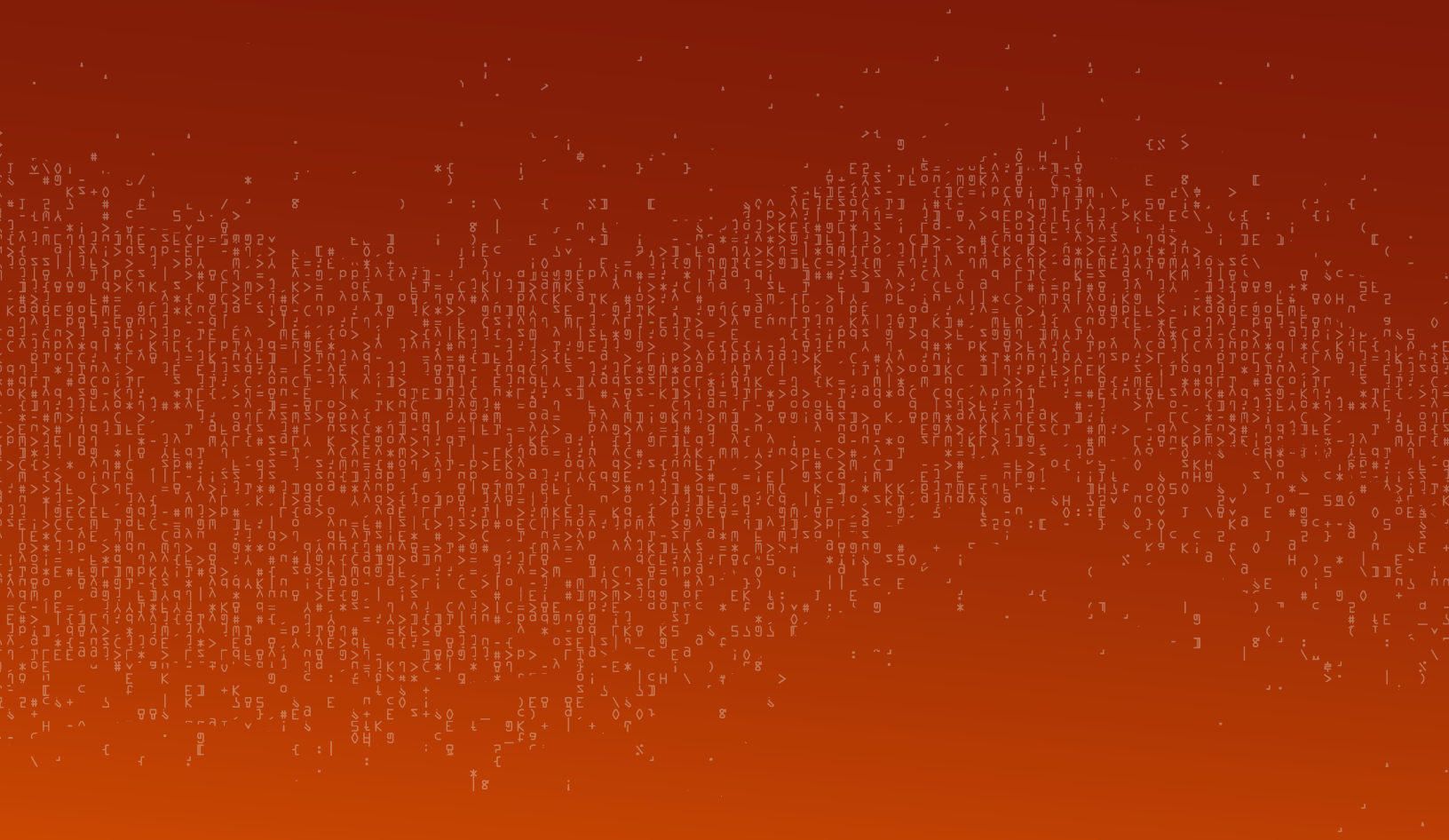
As technical defenses against encryption harden, ransomware groups are pivoting to the path of least resistance: human trust. This approach has led to a **53%** increase in ransomware, with RaaS groups being responsible for over **87%** of all ransomware attacks.



2026 Threat Landscape

ARTIFICIAL INTELLIGENCE

Flashpoint's AI collections are derived from Flashpoint's extensive coverage of forums and chat services datasets, including threat actor activity based on content or tactics, techniques, and procedures (TTPs).



AI Threats Overview: Data and Insights

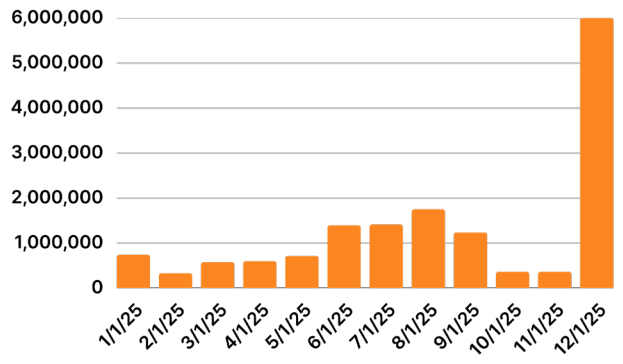
Artificial Intelligence (AI) is acting as a force multiplier, amplifying the scale and potency of nearly every component of the threat landscape. From information-stealing malware to vulnerabilities and ransomware, Flashpoint is observing threat actors improve their processes and expand their capabilities via generative AI and malicious LLMs.

Artificial Intelligence Quickview

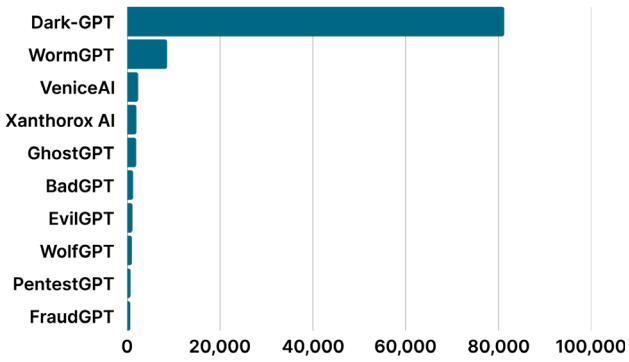
JANUARY 2025 - DECEMBER 2025

1.5 Billion
TOTAL AI MENTIONS

Total Mentions of AI and Illicit Activity, 2025



Top Mentioned Malicious LLMs, 2025



Source: Flashpoint Collections

Common Threat Actor Use Cases of Malicious AI

Jailbreaking

A method to find a loophole around an AI's safety nets and bypass regulations that could then be leveraged to make the AI system perform illicit activity.

Vishing

Threat actors impersonate IT support or security teams to gain remote access, leveraging generative AI such as deepfake technology.

Slopsquatting

Threat actors create fake software packages that mimic real ones, tricking AI coding assistants into recommending malware directly to developers.

AI Sidebar Spoofing

Attackers create a fake AI assistant sidebar to trick users to navigate to malicious sites, run illicit commands, or install backdoors and potentially other harmful applications.

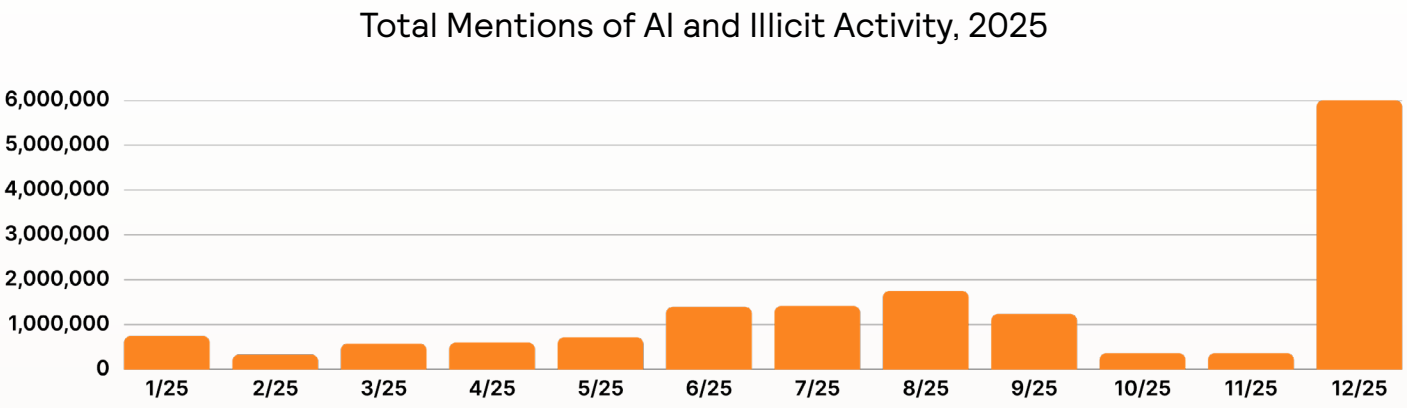
Prompt Injection

Threat actors hide malicious instructions within HTML or social media comments — thereby tricking AI assistants into following hidden commands and allowing the attacker to steal login information or access sensitive data from the user.

Steganographic Prompting

Threat actors hide secret instructions inside an AI model. When a user gives a normal command, the AI follows the hidden "sleeper" rules instead, performing a malicious task without the user ever knowing.

Infiltrating threat actor communities and discussion groups, Flashpoint identified over 1.5 billion illicit discussions and criminal activities centered around AI. Advancements in Flashpoint's AI capabilities also revealed that this activity peaked in December 2025 at a staggering 1,500% when compared to the prior month. This surge of 6M discussions focused heavily on weaponizing AI for high-impact vectors, including topics such as "deepfake", "KYC" (know-your-customer), "jailbreak prompts", "phish", and "malware".

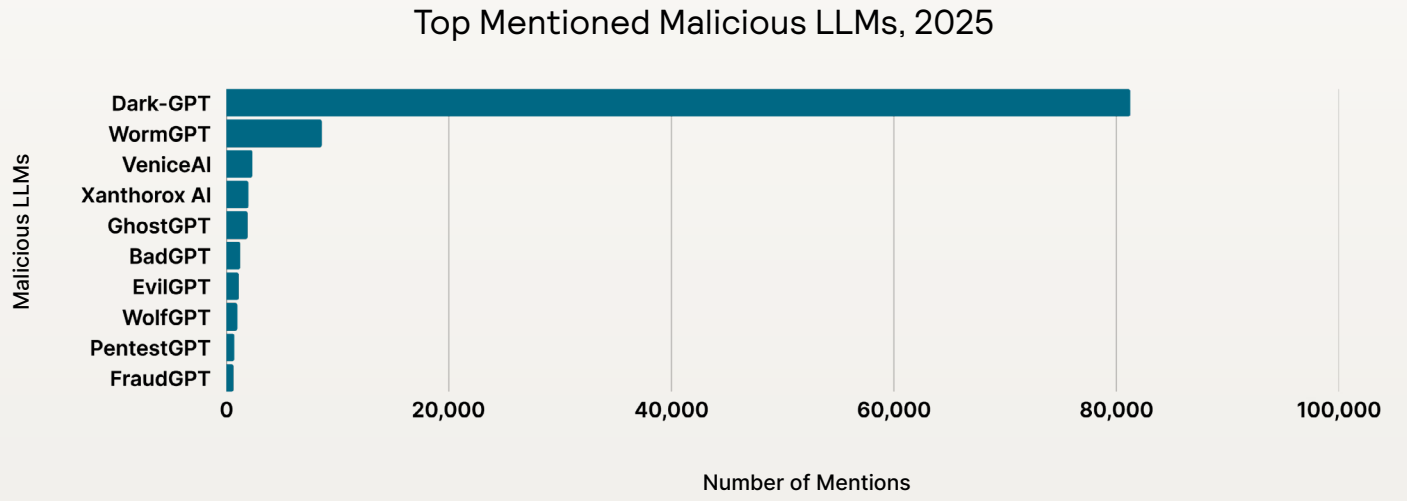


Source: Flashpoint Collections

The Rising Danger of Agentic AI

AI threats are undergoing a major transition: threat actors are moving beyond one-off uses of generative AI — such as creating phishing lures and deepfakes — in favor of building systems that automate the entire attack chain continuously.

Built on data pulled from criminal environments and shaped by fraud use cases, these systems scrape data, adjust messaging for specific targets, rotate infrastructure, and learn from failed attempts without constant human involvement. This shift is critical, not for its technological novelty, but for its potential of dramatically lowering the cost of experimentation for the attacker. When iteration becomes cheap, attackers can afford to fail repeatedly until any variation works.



Source: Flashpoint Collections

At the same time, attackers are taking note that defenders are increasingly connecting AI into production environments at a pace that outstrips their ability to understand its components or downstream risk. APIs, plugins, identity services, and internal tools are being linked together in ways that expand functionality and exposure at the same time. Many of these connections were never designed with adversarial pressure in mind.

The most concerning and potentially dangerous is the exploitation of agentic AI and browser AI assistants. Flashpoint analysts assess that in 2026, many incidents will involve exploiting how automation has been stitched together into everyday workflows.

Defending Against AI Threats in 2026

Incremental improvements to existing security models will not be enough. Attackers are adapting more quickly, leveraging automation, identity, and trusted relationships in ways that circumvent traditional controls. Intelligence programs built solely around static feeds and retrospective reporting will continue to lag behind.

The organizations that fare best will be those that focus on early visibility, contextual intelligence, and human-led analysis, that is supported by automation rather than replaced by it. As convergence and speed continues to define the threat landscape, foresight is a requirement.

Key Takeaways

1. **Attackers are pivoting to autonomous "agentic" attack chains.**
Threat actors are actively seeking agentic AI systems that manage the entire attack lifecycle independently. These autonomous systems will dramatically lower the cost of experimentation by scraping data and rotating infrastructure without human intervention, allowing attackers to iterate until they find a successful foothold.

2. **Adversaries are weaponizing organizational AI workflows and APIs against them.**
Attackers are aggressively targeting the connections between AI assistants and corporate environments, such as APIs and identity services, rather than the models themselves. By leveraging TTPs like slopsquatting and steganographic prompting, they trick automated systems into executing hidden commands or installing backdoors directly into a developer's workflow.

3. **2026 is ushering an explosive surge in specialized illicit AI discussion groups.**
Flashpoint data reveals a staggering 1,500% surge in illicit AI-related criminal activity within a single month. In November 2025, Flashpoint identified 362,000 discussions and illicit mentions of AI; by December 2025, that volume skyrocketed to a peak of 6M. Organizations will need to focus on early visibility, contextual intelligence, and human-led analysis, that is supported by automation.breaches are not isolated incidents but contribute to a larger, interconnected web of cyber threats.

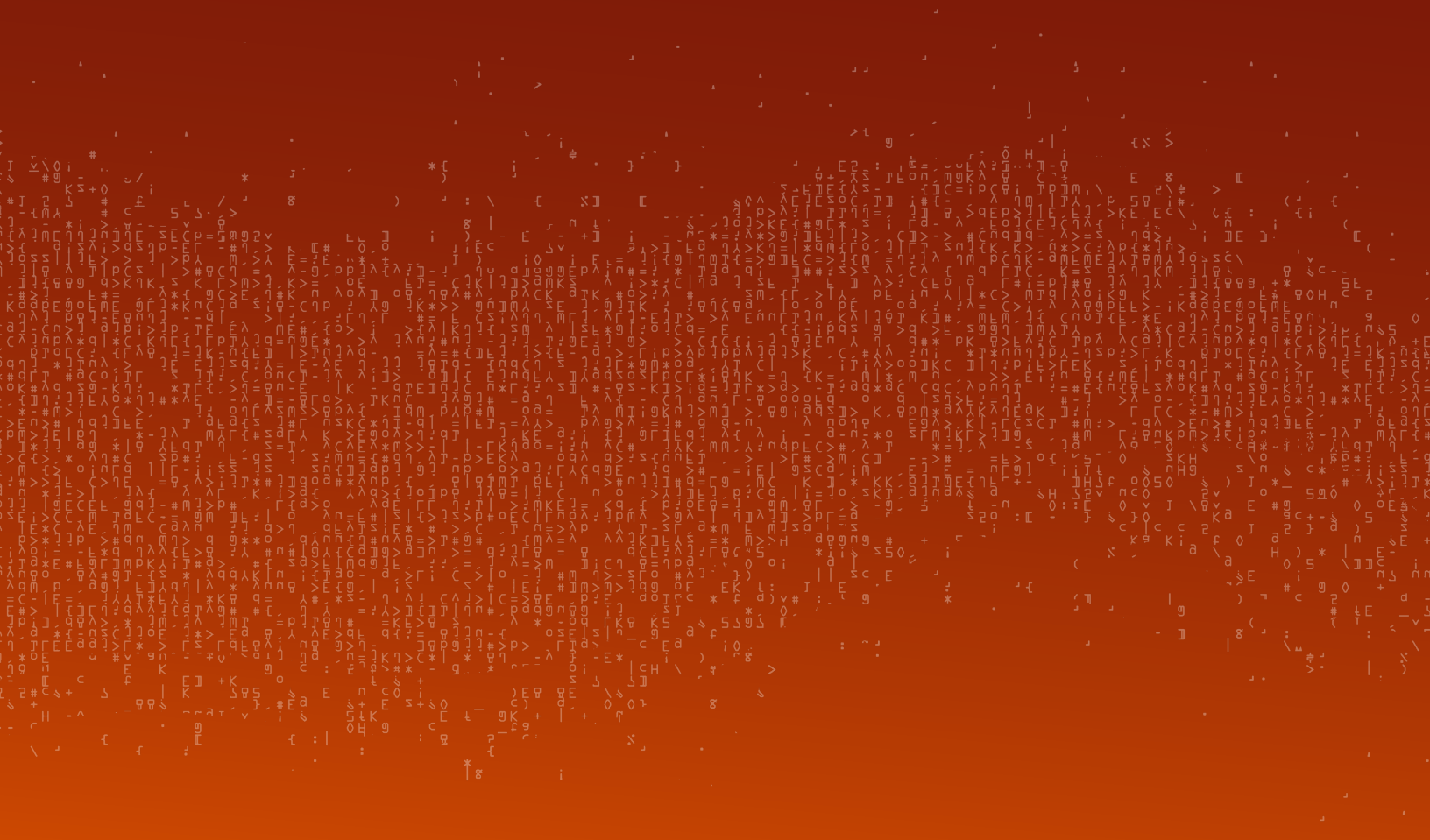
Threat Posture Assessment

- [ ] Is my organization aware of the processes involved between our AI agents and production environments?
- [ ] Are my security teams able to detect and neutralize steganographic prompting within our current workflows?
- [ ] Does my organization have direct visibility into the peak discussion cycles of illicit AI marketplaces and forums?

2026 Threat Landscape

INFORMATION-STEALING MALWARE

Flashpoint infostealer data and intelligence, as detailed in this section, is derived from extensive monitoring of illicit online marketplaces and specialized bot shops where stealer logs and related services are traded.



Infostealer Overview: Data and Insights

Information-stealing malware, AKA infostealers, has changed the cybercrime economics of access. Between January 1 to December 31, 2025, **Flashpoint observed over 11.1M machines infected with infostealers, culminating in over 3.3B stolen credentials, session cookies, cloud tokens, and personal data that has been openly sold on illicit forums and marketplaces.** As a result, Flashpoint has observed many instances in which attackers do not need to escalate privileges or deploy custom malware to gain access; they simply log in.

Infostealer Quickview

JANUARY 2025 - DECEMBER 2025

11.1 Million
INFECTED HOSTS AND DEVICES

3.3 Billion
STOLEN CREDENTIALS

Top 5 Most Prolific Infostealers in 2025
(By Infected Hosts or Devices)

1. Lumma — UP YOY
2. Acreed — NEW
3. Rhadamanthys — NEW
4. Vidar — UP YOY
5. StealC — DOWN YOY

Top 6 Countries Affected by Information-Stealing Malware, 2025

1. India | **2.** Brazil | **3.** Indonesia
4. Vietnam | **5.** Phillipines | **6.** United States

Source: Flashpoint Collections

The Hybrid Threat of AI-Driven Identity Exploitation

The true danger of infostealers lies in two inherent characteristics of identity data: its reusability for multiple attacks and its ability to bypass traditional defenses entirely. A single compromised identity can support fraud, espionage, extortion, or lateral movement depending on who buys it and when. If paired with a malicious agentic AI system, threat actors could soon have the capability to acquire, test, and compromise user credentials across a variety of platforms at an incredible velocity.

The AI-Driven Identity Exploitation Cycle

1. Harvesting
Infostealers drain credentials and session cookies from infected devices or Software-as-a-Service (SaaS).

2. Ingestion
Stolen logs are fed into agentic AI systems.

3. Automated Testing
The AI autonomously tests these credentials against thousands of endpoints, such as corporate VPNs, SaaS, cloud providers, simultaneously.

4. Monetization/ Escalation
The system identifies successful logins for immediate fraud or lateral movement.

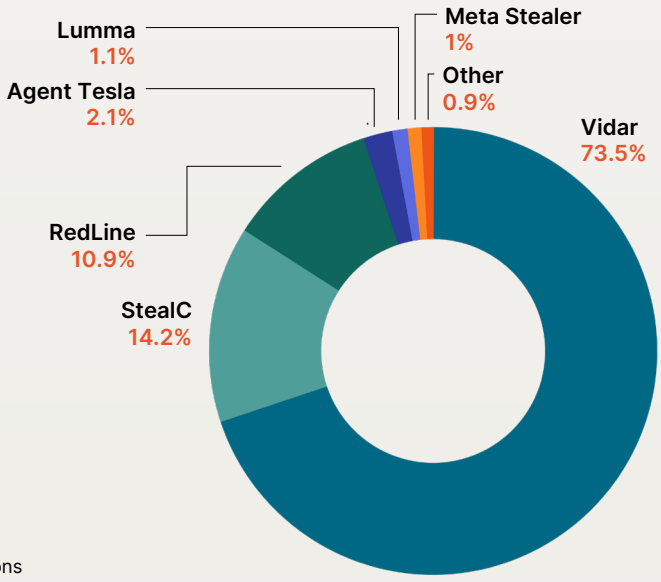
The reality of identity data and the potential for its automation necessitates a shift in how organizations must view their attack surface. Infostealers have shown that it is no longer limited to corporate infrastructure; it now includes employee browsers, personal devices, SaaS platforms, and third-party access.

Vidar Takes Center Stage Post-Lumma's Takedown

The infostealer ecosystem has undergone incredible volatility over the past year, with many infostealers vying for market share ever since Lumma's takedown in May 2025. Although Lumma still remains active, its developers suffered major setbacks, experiencing a centralized server wipe and having 2,500 domains seized by law enforcement. These events, in addition to Lumma administrators being doxxed in August 2025, created significant dissent with its customer base.

As such, Flashpoint observed the volume of uploaded Lumma logs severely drop over the course of 2025. In its place, various strains, such as Vidar and Rhadamanthys have taken over Lumma's market share. As of January 2026, the new generation of Vidar, Vidar 2.0, has gained popularity and is currently the most used infostealer by threat actors. This is likely due to many of its similar features and improvements to Lumma, combined with Rhadamanthys' takedown in November 2025.

Most Prolific Infostealers by Infected Hosts and Devices, January - February 2026



Source: Flashpoint Collections

Defending Against Infostealers in 2026

Intrusions using identity data will be difficult for defenders to catch, as systems will seemingly behave as expected. As such, it is essential that organizations have access to comprehensive threat intelligence that empowers security teams to proactively monitor when credentials are compromised and could be exploited.

However, organizations also need to ensure that their intelligence providers can enrich and structure raw log files into actionable intelligence that brings value. To be useful, logs need to be parsed, correlated, and enriched with metadata so they can provide contextual clues into inflection points, impact, and intent.

How Flashpoint Transforms Raw Logs Into Structured, Actionable Intelligence

1. Source Ingestion

Our expert analysts and technology actively monitor underground ecosystems – forums, marketplaces, paste sites, chat platforms, and malware repositories – to identify and ingest raw infostealer data the moment it becomes available.

2. Normalization and De-Duplication

Incoming logs are automatically reviewed and scored for uniqueness, freshness, and threat relevance. Duplicate files are removed, and data is routed through processing workflows designed to optimize signal extraction.

3. Automated Parsing and Enrichment

Flashpoint's enrichment engine dissects each log to extract and tag critical components, including:

- Credentials (usernames, passwords)
- Session cookies (often used in SSO and MFA bypass)
- Host metadata (operating system, IP, browser, ISP, device specs)
- Autofill PII (emails, names, phone numbers, saved forms)
- Application data (installed software, AV/EDR tools)
- Stealer attribution (identifying the malware family)

4. Structured Output

Parsed data is organized into a normalized format, mapped to known stealer strains, and indexed within Flashpoint's intelligence platform, Ignite. This structured dataset powers:

- Real-time alerts
- Searchable, filterable infostealer compromise views
- SIEM/SOAR integrations
- Correlation with broader threat actor infrastructure

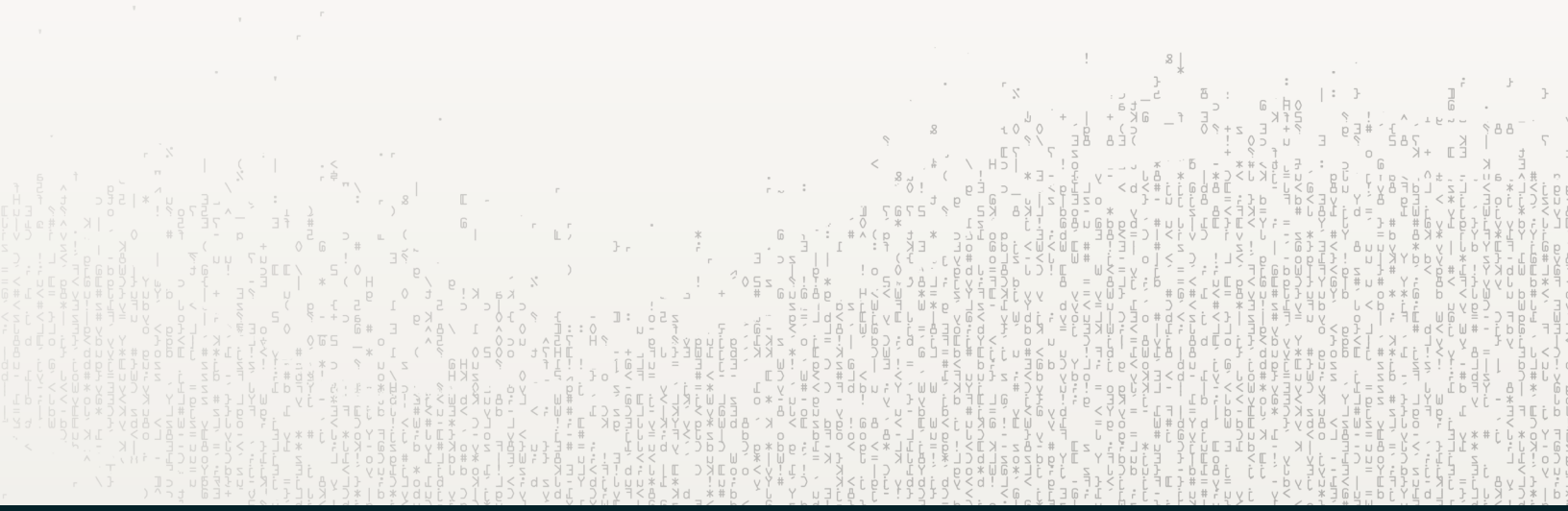
In addition, organizations will need to expand their attack surface even further to account for employee behavior — both online and offline — on their personal devices, Software-as-a-Service (SaaS) ecosystems, and all third-party and partner access. Treating digital identity compromise as an endpoint, rather than a starting point for attackers will result in security teams playing defense after all the damage is already done.

Key Takeaways

1. **Infostealers have expanded the attack surface to personal and SaaS ecosystems.**
   The modern attack surface has aggressively moved beyond corporate infrastructure to include employee browsers, personal devices, and third-party SaaS platforms. Because infostealers harvest data from these unmanaged endpoints, organizations must now treat digital identity compromise as a starting point for an attack.

2. **Identity is turning into the primary exploit vector.**
   The massive volume of available session cookies and cloud tokens has allowed attackers to bypass traditional security perimeters entirely, as they no longer need to escalate privileges but can instead behave as legitimate users within a network.

3. **Vidar 2.0 rapidly dominates the infostealer market following Lumma's decline.**
   Vidar 2.0 has aggressively seized market share to become the most utilized strain by threat actors as of January 2026. Defenders must maintain visibility into illicit marketplaces and forums to adapt to any potential improvements and new features.



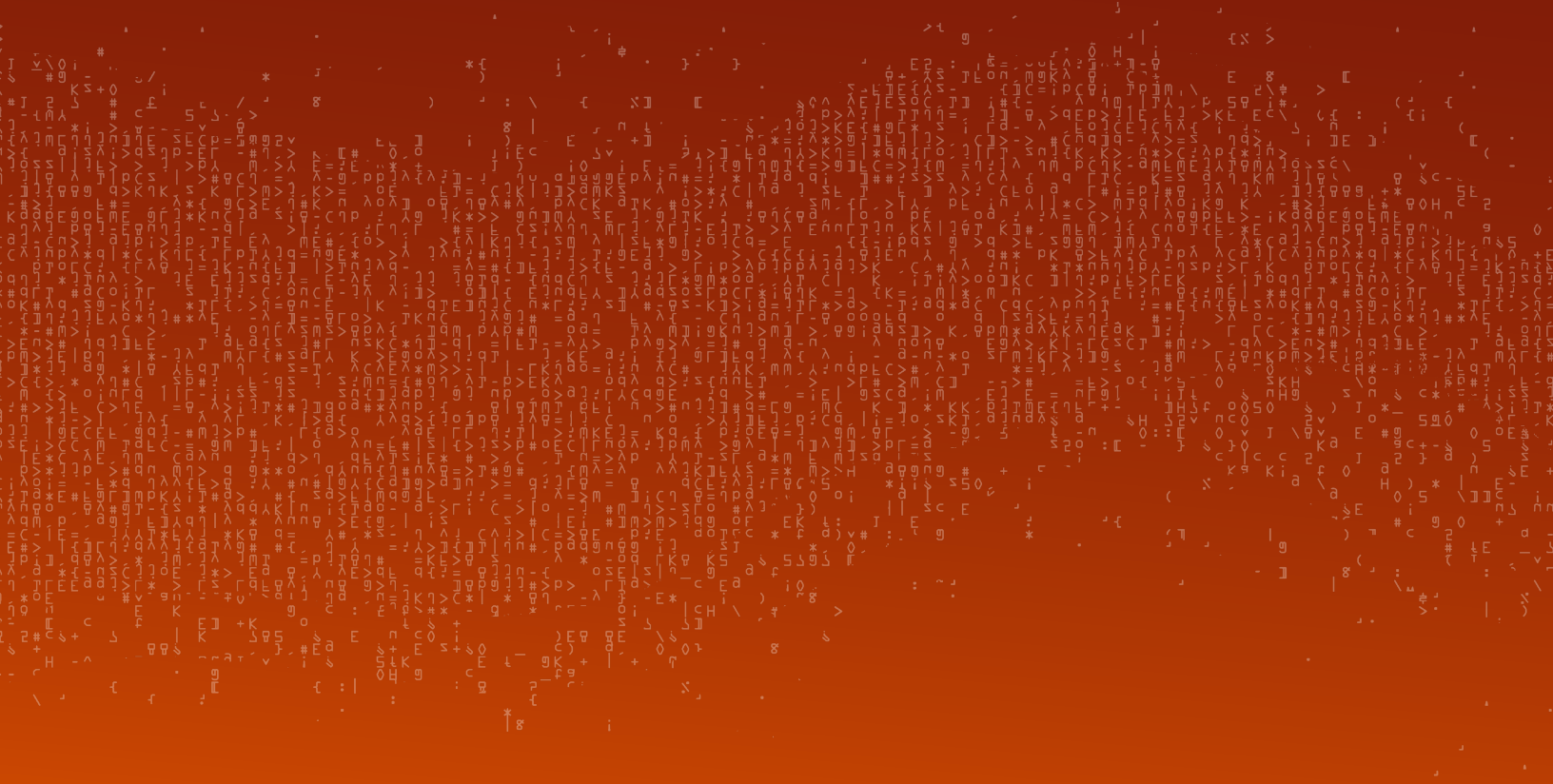
Threat Posture Assessment

- [ ] Am I relying on generic feeds for infostealer intelligence, or do I have direct access to the raw data from illicit forums and marketplaces?
- [ ] Is my threat intelligence data allowing me to actively monitor for potential compromises affecting me and my partners, or am I just waiting to respond to an attack?
- [ ] Is my Cyber Threat Intelligence team knowledgeable of the most prolific stealer strains and how they bypass security measures?

2026 Threat Landscape

VULNERABILITIES

The data in this section reflects Flashpoint's vulnerability intelligence, covering all attack surfaces — including vendors, endpoints, cloud, Internet of things (IoT), operational technology, open source software (OSS), and third-party libraries and dependencies. Flashpoint's vulnerability database abstracts differently from MITRE and provides full context into metadata such as EPSS, the MITRE ATT&CK framework, exploit intelligence, social risk, and ransomware likelihood.



Vulnerability Overview: Data and Insights

Vulnerability disclosures have continued to grow, **with Flashpoint seeing a year over year increase of over 12%, aggregating a total of 44,509 vulnerabilities in 2025.** Of those vulnerabilities, 466 were known to be exploited in the wild. Nearly 33% (14,593) of all vulnerabilities disclosed in 2025 had publicly available exploits.

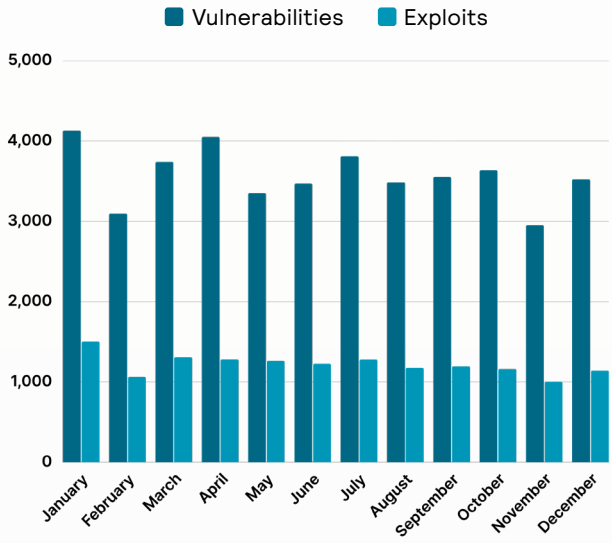
Vulnerability Quickview

JANUARY 2025 - DECEMBER 2025

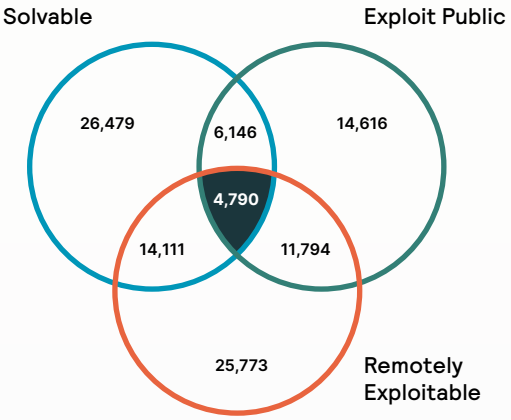
44,509
DISCLOSED VULNERABILITIES

14,593
VULNERABILITIES WITH PUBLICLY AVAILABLE EXPLOITS

Vulnerability Disclosures and Exploits, 2025



Breakdown of Actionable, High Severity Vulnerabilities by Availability and Exploitation, 2025



Source: Flashpoint Collections

Vulnerability Exploitation: Targeting High-Value Infrastructure

The 2025 vulnerability intelligence landscape has been defined by a zero-day to exploit window that has effectively vanished, as evidenced by the mass exploitation in the wild of vulnerabilities like Citrix Bleed 2 and React2Shell. Ransomware groups, most notably RansomHub, have moved with alarming speed to weaponize these flaws, prompting an unprecedented one-day remediation deadline from the Cybersecurity Infrastructure and Security Agency (CISA).

The strategic focus of vulnerability exploit attacks increasingly centers on high-value infrastructure and emerging technologies. Chinese Advanced Persistent Threat (APT) groups have pivoted quickly to leverage the ToolShell SharePoint vulnerabilities and React2Shell for both RCE (Remote Code Execution) and ransomware campaigns.

In addition to these flaws, Flashpoint analysts highlighted the following zero-days and highly publicized vulnerabilities that pose the most risk to organizations:

CVE ID	Title	CVSS Scores (v2, v3, v4)	Exploit Status	Ransomware Likelihood Score	Social Risk Score
CVE-2025-5777	CitrixBleed2	10.0 9.8 9.3	Exploited in the Wild	High	Low
CVE-2025-53770	ToolShell	10.0 9.8 9.4	Exploited in the Wild	Critical	Low
VulnDB ID: 419253	Shai-Hulud	5.0 9.8 9.3	Exploited in the Wild	Medium	N/A
VulnDB ID: 427979	Shai-Hulud 2.0	5.0 9.8 9.3	Exploited in the Wild	Medium	N/A
CVE-2025-14847	Mongobleed	5.0 7.5 8.7	Exploited in the Wild	High	Medium
CVE-2025-55182	React2Shell	10.0 10.0 10.0	Exploited in the Wild	Critical	High
CVE-2025-66478	Langflow	10.0 9.8 9.3	Exploited in the Wild	High	Medium

The Weaponization of AI Infrastructure

Additionally, Flashpoint is observing the weaponization of AI infrastructure, with the Langflow vulnerability being exploited in just days to form the backbone of the Flodrix Botnet, which targeted the massive user base of a tool designed for building AI-powered agents. Combined with the sophisticated, self-replicating Shai-Hulud supply chain attacks targeting the npm ecosystem, it is clear that state-sponsored and financially motivated actors are prioritizing the compromise of the modern development and AI pipeline to achieve maximum reach.

In addition to Langflow, Flashpoint cataloged the following critical vulnerabilities that impacted AI applications and technologies:

Vulnerability ID	Title
VulnDB ID: 385466 (No CVE ID)	Multiple Extensions Extension for Chrome Malicious Code Remote Information Disclosure
CVE-2025-31564	AI Auto Tool Content Writing Assistant Plugin for WordPress Unspecified SQL Injection
VulnDB ID: 395437 (No CVE ID)	Google Gemini Cloud Assist GCP Log Explorer HTTP Request Log Handling Arbitrary Prompt Injection
CVE-2025-54795	Claude Code Echo Command Handling Confirmation Prompt Bypass Unspecified Arbitrary OS Command Execution
CVE-2025-59828	Claude Code Yarn Plugin Autoloading Arbitrary Code Execution CVE-2025-62222: Microsoft Visual Studio Copilot Chat Extension Agentic AI Unspecified GitHub Issue Arbitrary Command Execution
CVE-2025-62222	Microsoft Visual Studio Copilot Chat Extension Agentic AI Unspecified GitHub Issue Arbitrary Command Execution
CVE-2025-11445	Kilo Code AI Agent Extension for VS Code webview/ClineProvider[.]ts ClineProvider Function Prompt Injection Arbitrary Code Execution
CVE-2025-11749	AI Engine Plugin for WordPress labs/mcp.php Meow_MWAI_Labs_MCP::rest_api_init() Function Improper Access Restriction Remote Bearer Token Disclosure
VulnDB ID: 416965 (No CVE ID)	Perplexity Comet Web Content Parsing Indirect Prompt Injection Arbitrary Browser Instruction Execution
VulnDB ID: 415420 (No CVE ID)	OpenHands Content Parsing Prompt Injection Arbitrary Code Execution

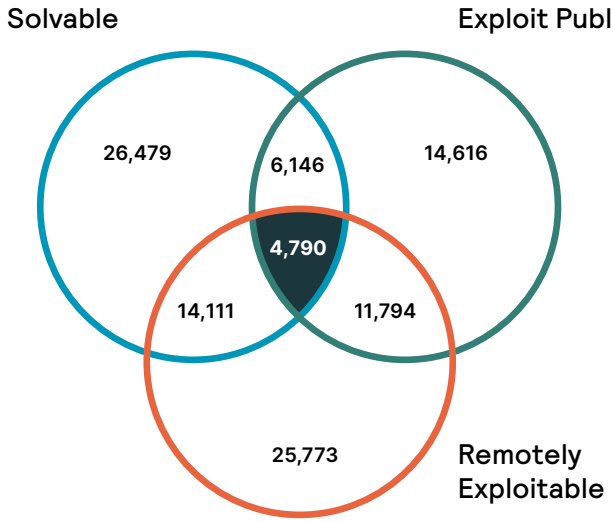
Defending Against Vulnerabilities in 2026

Vulnerability management teams that struggle with disclosure volumes will find 2026 to be even more challenging. Despite the power and popularity of LLMs, the vulnerability intelligence industry has not seen widescale adoption of LLMs in sourcing vulnerabilities. With vulnerability disclosures still rising to record highs even without this technology, it is only a matter of time until security teams are inundated with potentially tens of thousands of AI-sourced disclosures.

To stay focused, security teams should prioritize vulnerabilities that meet the following criteria:

- Have a known solution
- Are remotely exploitable
- Have a publicly available exploit

Breakdown of Actionable, High Severity Vulnerabilities, by Availability and Exploitation, 2025



Source: Flashpoint Collections

Following this methodology can potentially allow organizations to cut their higher-risk vulnerability workloads by nearly 90%.

Additionally, depending on any other organizational requirements, other considerations and metadata such as if known to be exploited in the wild, MITRE ATT&CK mapping, Ransomware Likelihood, or social risk can be added. This provides the capability to produce actionable vulnerability reports to leadership that could help secure the proper resources to remediate them. Then, once those issues are resolved, vulnerability management teams can shift to other key issues.

Modern vulnerability management is currently contending with the increasing fragility of publicly available vulnerability intelligence. Organizations that rely solely on the Common Vulnerabilities and Exposures (CVE) program or the National Vulnerability Database (NVD) face increasing systemic risk as 2026 progresses due to massive backlogs and degraded data quality. However, organizations leveraging security vendors that employ dedicated vulnerability research teams, such as Flashpoint, will be unaffected.

Business leaders that were proactive in finding a supplemental or complete replacement for CVE data will be better positioned for this volatility going into 2026. Organizations that have not prepared for this possibility will need to quickly pivot into finding a comprehensive source of vulnerability intelligence.

Key Takeaways

1. **Zero-day exploit windows are increasingly vanishing.**
   The mass exploitation of vulnerabilities like Citrix Bleed 2 and React2Shell within hours of discovery shows that the window for remediation is rapidly closing.

2. **Attackers are pivoting to weaponize the AI development pipeline.**
   Adversaries are strategically targeting modern AI infrastructure. By compromising tools used to build AI agents, threat actors are achieving maximum reach by poisoning the very foundation of the enterprise's automation strategy.

3. **Potential CVE volatility mandates intelligence redundancy.**
   With the CVE program contract set to expire in March 2026, organizations face catastrophic downstream risks if public vulnerability databases experience a complete operational stop. This systemic instability makes it a business requirement to move beyond generic feeds and adopt dedicated research teams that can provide continuous, independent vulnerability enrichment even if public systems fail.

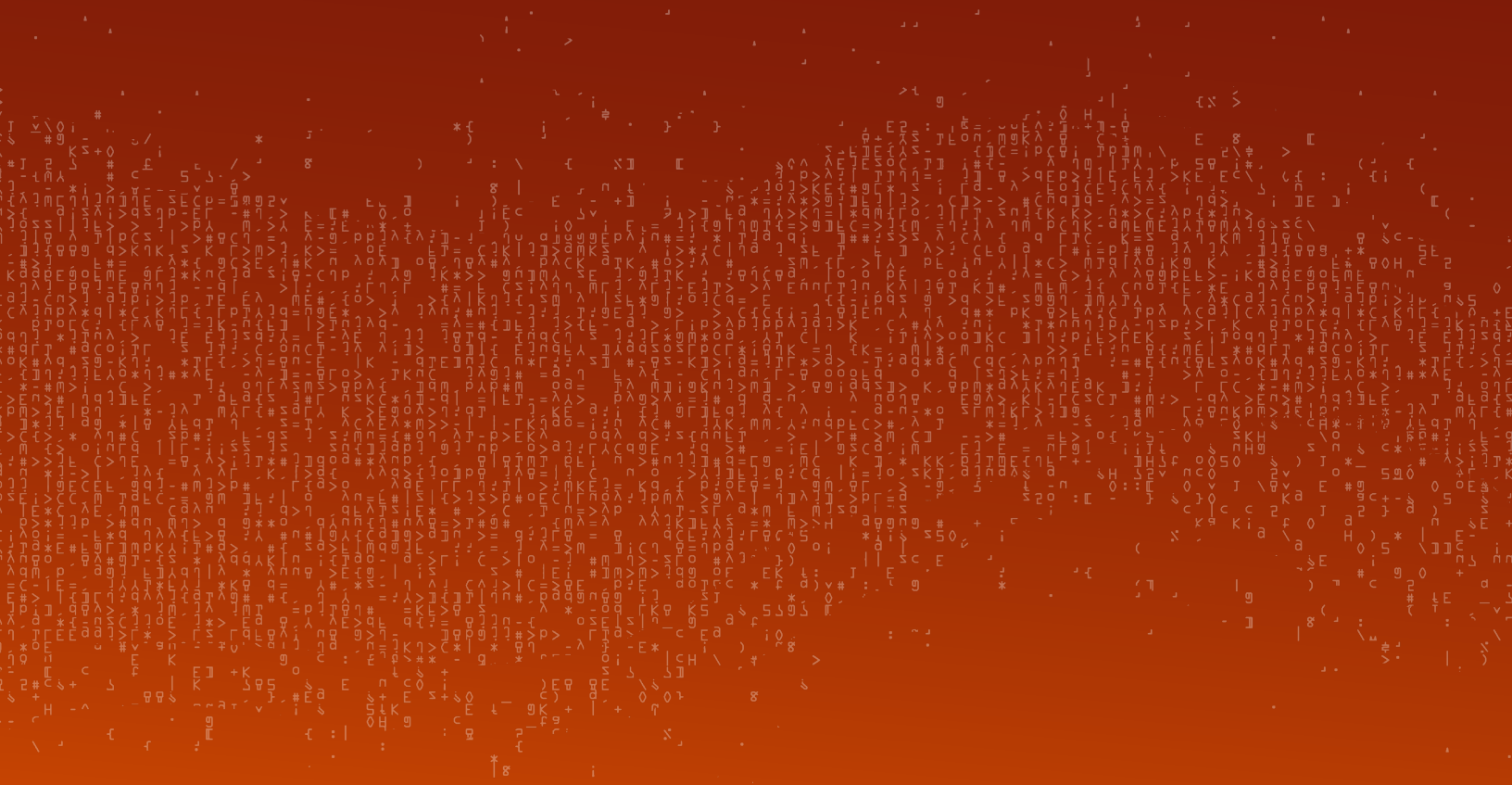
Threat Posture Evaluation

- [ ] Does my security team have the capability of identifying zero-day vulnerabilities?
- [ ] Is my organization auditing the security of any agentic AI dependencies or third-party libraries?
- [ ] What is my organization's response if publicly available vulnerability intelligence program funding and oversight remain volatile?

2026 Threat Landscape

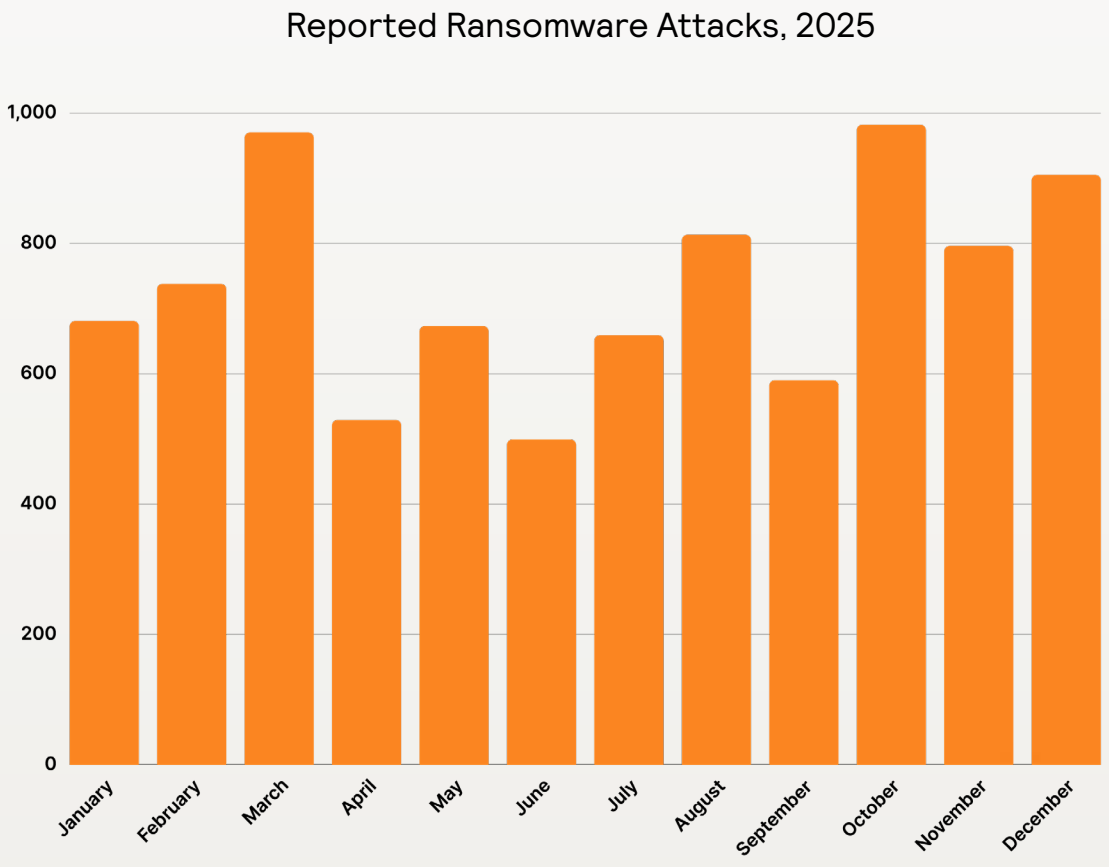
RANSOMWARE

The data in this section comprises victimized organizations that have been announced on ransomware blogs and leak sites. The intelligence presented here reflects activity directly observed as part of Flashpoint's proprietary collections.



Ransomware Overview: Data and Insights

Ransomware continues to thrive and evolve, primarily fueled by ransomware-as-a-service (RaaS) distribution and the interconnectedness of adjacent threats such as infostealers and vulnerability exploits. **Flashpoint observed a year-over-year 53% increase in ransomware attacks.** The vast majority of these attacks impacted the United States, which accounted for nearly 53% of all named victim organizations. This is attributed to the value of US data and demonstrated high willingness to pay.



Source: Flashpoint Collections

Flashpoint also found that RaaS groups were responsible for over 87% of all ransomware attacks in 2025. Ransomware operators have been extremely proficient in using vulnerability exploits, targeting digital supply chains and SaaS infrastructure to circumvent security defenses instead of attacking them head on. RaaS groups such as Clop have been particularly effective in leveraging zero-days such as CVE-2025-61882, which have allowed them to victimize multiple organizations, especially within the financial sector.

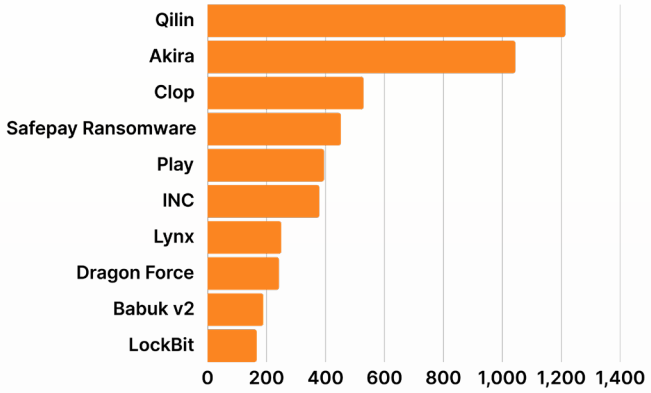
Ransomware Quickview

JANUARY 2025 - DECEMBER 2025

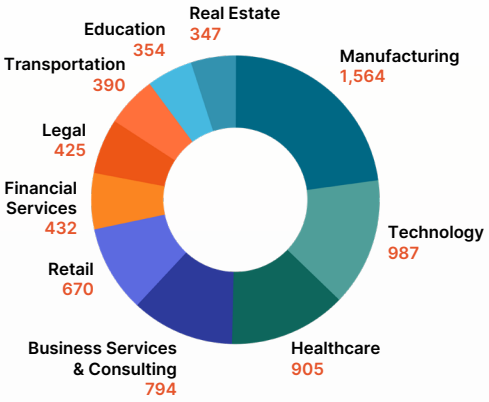
8,835

TOTAL RANSOMWARE ATTACKS

Top 10 Most Prolific Ransomware-as-a- Service Groups, 2025



Top 10 Industries Targeted by Ransomware, 2025



Top 10 Countries Affected by Ransomware, 2025

1. United States
2. Canada
3. Germany
4. U.K.
5. France
6. Italy
7. Spain
8. Brazil
9. India
10. Australia

Source: Flashpoint Collections

Shift in Ransomware Tactics: The Identity and Human Frontier

Flashpoint intelligence is observing an undeniable and fundamental evolution taking place: ransomware extortion groups are strategically moving away from the technical exploits they used earlier in 2025 to attack the most critical layer of the modern enterprise — human trust and identity.

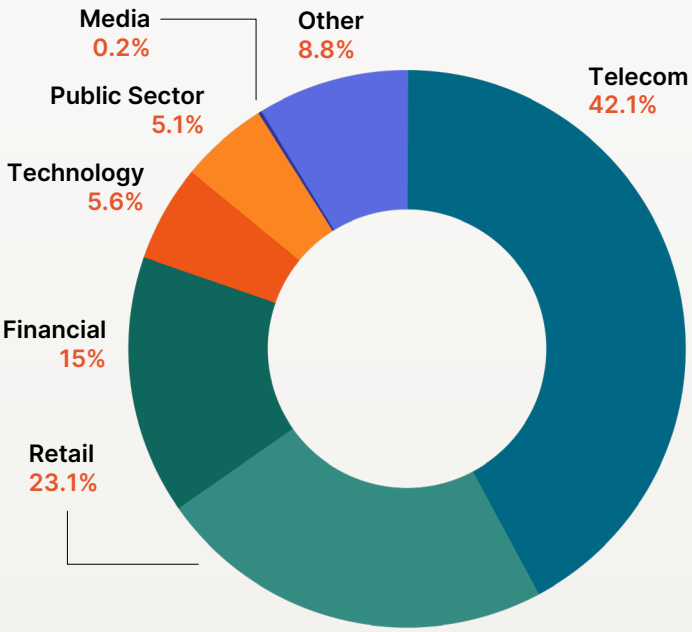
RaaS groups are realizing that organizational firewalls are getting stronger, but the human element offers the path of least resistance. This strategic pivot is clearly demonstrated by the TTPs of groups like LAPSUS$, Scattered Spider, and the various distinct offshoots of them, such as Sp1d3rHunters and Scattered Lapsus$ Hunters.

Threat actor groups have been seen eschewing traditional ransomware for a pure-play extortion model driven by social engineering. This often involves gaining access through trusted relationships: third-party vendors, help desks, identity systems, and employees under pressure. Once access or sensitive data is obtained, extortion becomes a negotiation rather than a technical challenge.

Shift in Ransomware Tactics: Increasing Reliance on Insider Threats

In addition to increased social engineering, Flashpoint is seeing RaaS groups like Scattered Spider augment their efforts in recruiting malicious insiders. **In 2025, Flashpoint observed 91,321 instances of insider recruiting, advertising, and threat actor discussions involving insider-related illicit activity.** This change in tactics is far more efficient for attackers, as it is cheaper to recruit an insider to circumvent multi-million dollar security stacks than it is to develop a complex exploit from the outside.

Insider Threats by Industry, 2025

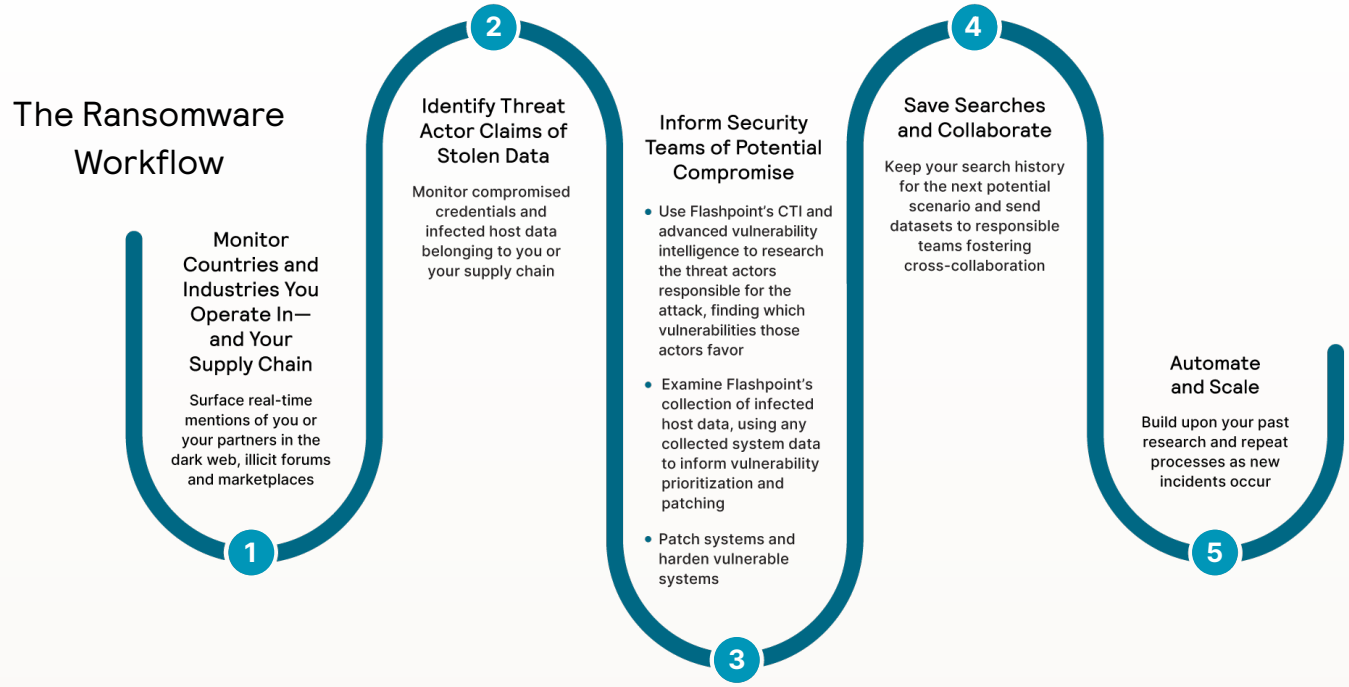


Source: Flashpoint Collections

Throughout 2025, Flashpoint has observed a variety of prominent insider-related cases, ranging from intentional fraud to massive technical oversights. Incidents include military contractors being bribed by threat actors to pass confidential information, North Korean threat actors posing as legitimate employees to steal funds and proprietary information, and an insider at a well-known cybersecurity organization sharing screenshots of internal dashboards with the Scattered Lapsus$ Hunters group.

Defending Against Ransomware in 2026

Organizations need to establish and implement a robust ransomware workflow that includes both preventative and responsive measures. This includes continuous monitoring for real-time mentions of relevant compromised organizations, potential malicious insiders, and supply chains. Additionally, security teams will need to have the capability to monitor for compromised credentials and infected host data sourced from information-stealing malware.



In addition to preventative measures, organizations should also regularly conduct tabletop exercises and create cyber extortion playbook reviews to ensure readiness and meet compliance requirements.

Key Takeaways

1 **Ransomware is shifting into pure-play identity extortion.**

Despite overwhelming success, threat actors are actively pivoting away from complex encryption toward a pure-play extortion model that targets human trust and identity rather than software flaws.

2 **Adversaries are weaponizing malicious insiders to bypass security stacks.**

Flashpoint data shows an aggressive surge in insider recruitment, with over 91,000 instances of threat actors discussing or advertising for malicious insiders in 2025. This tactical shift allows RaaS groups to circumvent multi-million dollar security investments by simply bribing or social engineering employees, contractors, or partners to provide direct, authorized access to sensitive dashboards and data.

3 **US critical infrastructure remains the epicenter of global ransomware attacks.**

The United States accounted for nearly 53% of all named ransomware victims in 2025, driven by the high perceived value of U.S. data and a demonstrated willingness to pay. RaaS groups like Qilin and Akira are prioritizing high-leverage sectors — specifically manufacturing, technology, and healthcare — where operational downtime has the most immediate and severe financial consequences.

Threat Posture Evaluation

- [ ] Have we expanded our defense beyond "encryption protection" to include social engineering and "pure extortion" playbooks?
- [ ] How are we monitoring for signs of insider recruiting or unauthorized dashboard access within our internal communications?
- [ ] Is our Help Desk a hardened security gate or a potential access point?

The Flashpoint Advantage: Driving Mission-Critical Outcomes

Following the preceding analysis and assessment of your organization's threat posture, the subsequent step is to provide your teams with the tools and intelligence required to address identified exposures. From real-time threat intelligence to proactive vulnerability management, discover how Flashpoint empowers organizations to strengthen their defenses and enhance resilience in the face of today's dynamic threat landscape. Certainly no one can summarize the positive mission impact, risk avoidance, and ROI of Flashpoint than our customers — we are proud to share their conclusions here.

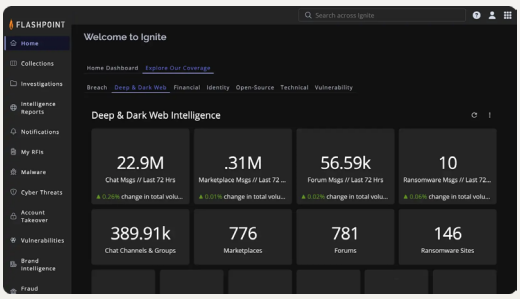
We sought more than just an intelligence provider. We wanted a strategic partner who could acutely understand our security challenges and seamlessly integrate with our team. Flashpoint provided that — and then some.

Director of Security Intelligence
Global Financial Services Company

Intelligence Platform

Flashpoint Ignite

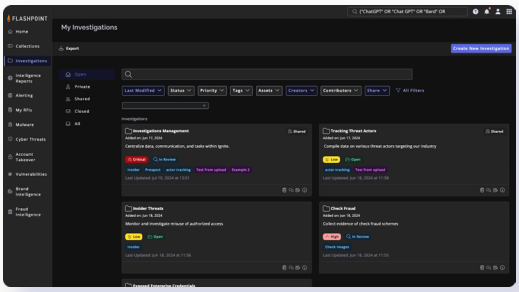
Our award-winning Flashpoint Ignite platform empowers security teams by providing direct access to our unparalleled primary-source collections. We combine automated analysis and integrated AI with deep human expertise to provide a holistic view of risk, enabling organizations to identify and remediate threats with rapid, decisive action. By gathering data from open and difficult-to-access online spaces, we offer a comprehensive solution that transcends the limitations of conventional approaches. This ensures your team has the high-fidelity intelligence required to reduce risk, optimize operations, and improve resilience across the entire enterprise.



69B+ Stolen Credentials	**22.3B+** Chat Services Messages	**975M+** Illicit Forum Posts	**435K+** Vulnerabilities (105K+Pre-CVE)
1B+ News Articles	**2.6B+** Unique Media	**1.9B+** Illicit Marketplace Items	**9.3B+** Stolen Credit Cards

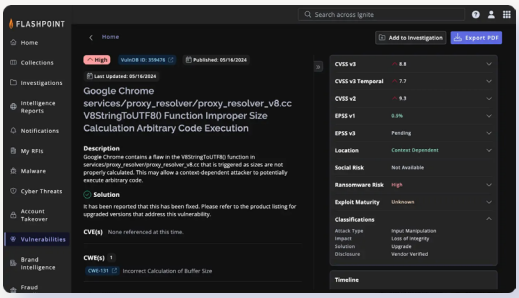
Core Packages

Flashpoint Cyber Threat Intelligence



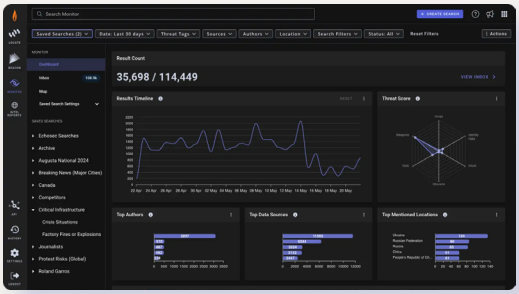
Protect your organization from evolving cyber threats, including ransomware, emerging malware, account takeovers, fraud, and exploited vulnerabilities with Flashpoint Cyber Threat Intelligence (CTI). Flashpoint combines unrivaled primary-source collections with AI-driven analysis and expert human validation to deliver contextual, actionable intelligence. Security teams gain clear visibility into the threats that matter most, accelerate investigations, and operationalize insights directly within their workflows to reduce risk and protect the business with confidence.

Flashpoint for Vulnerability Management (Built on VulnDB®)



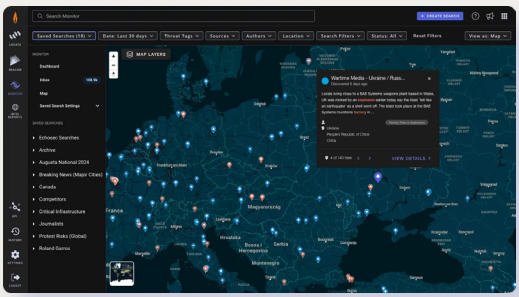
Gain timely awareness of new vulnerabilities with attribution to affected products/versions, packages, and libraries, severity scoring, and exploit intelligence. Flashpoint Vulnerability Intelligence is the most comprehensive vulnerability database and timely source of intelligence available. It allows organizations to search for and be alerted to the latest vulnerabilities, both in end-user software and third-party libraries and dependencies.

Flashpoint Physical Security Intelligence (Built on Echosec)



Enhance your situational awareness with Flashpoint Physical Security Intelligence (PSI), which provides real-time, geo-enriched data and expert intelligence insights. Amidst ever-expanding online chatter, PSI helps security and intelligence teams cut through the noise by providing access to a wide range of global open sources, including social media, messaging apps, defense forums, and underground networks. Integrated AI and granular filtering allow practitioners to effectively identify and analyze significant events, geopolitical risks, executive threats, and public sentiment, transforming overwhelming volumes of data into actionable intelligence.identify mission-critical risk and take rapid, decisive action.

Flashpoint National Security Intelligence



Flashpoint National Security Intelligence provides government agencies with rapid, secure access to the critical data and technology needed to accelerate intelligence cycles. By streamlining the collection of vast open-source information across diverse networks, we deliver the contextual understanding required for effective mission support. This a-la-carte catalog offers Flashpoint platform access for deep and dark web investigations and geospatial social media. It also provides Data as a Service (DaaS) for raw API access and specialized managed services, ensuring government teams gain the insight necessary to drive informed investigations and decisive action.

Additional Capabilities

Managed Attribution

Flashpoint Managed Attribution provides a secure, isolated virtual environment to conduct advanced digital research and interact with malicious content without risking your organization's network. This turnkey solution eliminates the resource-intensive overhead of self-hosting virtual machines, allowing teams to focus on their core mission. Users can safely download files, engage in illicit communities, and obfuscate their digital footprint by choosing from 187 global points of presence. Protect your infrastructure from malware and tracking while following investigations directly to the source.

Brand Intelligence

Flashpoint Brand Intelligence transforms how you protect your brand in the ever-evolving digital landscape. It empowers you to proactively oversee critical assets like domains, logos, social media, and mobile applications. Swiftly identifying misuse or impersonation enables effective neutralization of threats, ensuring your brand's integrity and consumer trust remain intact. Navigate the complex web of digital dangers, from fraudulent domains to social media impersonations and mobile app scams, with confidence and ease.

Firehose API

The Flashpoint Firehose delivers a fast and reliable stream of data from Flashpoint's unique collections. With Firehose access, users can pull key segments of Flashpoint data into their own infrastructure without the need to query APIs. This allows users to build high-quality data and AI tools that help enhance global situational awareness, generate timely intelligence, and advance national security initiatives.

Fraud Intelligence

Flashpoint Fraud Intelligence helps security and fraud teams detect indicators of fraud across the cybercriminal economy, assess exposure, investigate potential risks, and take action before monetary loss or reputational damage occurs. It offers deep insights into how fraudsters operate, revealing stolen credit cards, payment methods, account credentials for sale, and suspicious cryptocurrency transactions. With powerful search and analytics, you can search for fraud indicators with or without bank or customer identifiers, effectively identifying and investigating deceptive activities targeting your organization.

Flashpoint Services

Threat Readiness & Response

Our Threat Readiness & Response service equips organizations with comprehensive tools and insights to proactively prepare for, swiftly assess, and effectively counteract ransomware or cyber extortion attacks. By focusing on rapid evaluation and strategic response planning, it ensures minimal impact and swift recovery from cybersecurity threats.

Threat Actor Engagement and Procurement

Flashpoint anonymously and securely engages with threat actors on other organizations' behalf. This may include coordinating an engagement to identify the possible source of material or data, validate information, purchase or obtain data, and arrange for any communications with malicious actors.

Curated Alerting

Receive timely, relevant alerts based on your intelligence requirements and achieve continual monitoring of illicit communities and social media. Flashpoint analysts provide hand-crafted risk assessments that are unique to your organization. This streamlined approach ensures that you receive actionable and pertinent intelligence, improving the decision-making process and overall operational efficiency.

Analyst Support

Force multiply your team (staff augmentation) with onsite or virtual staff providing full-time intelligence analyst support. Allow Flashpoint to produce in-depth intelligence assessments to rapidly identify threats and mitigate your most critical security risks.

Tailored Reporting

Flashpoint Tailored Reporting Service (TRS) provides a tailored weekly or monthly deliverable that addresses specific intelligence requirements and highlights relevant threats with further assessments, saving analyst time and equipping teams with the resources to stay informed of your organization's threat landscape.

Extortion Monitoring

Flashpoint's Extortion Monitoring Service delivers real-time automated alerts of identified leaked assets as a result of an extortion incident, providing teams with the necessary insight into the extent of exposure and damage.

Request for Information (RFI)

Flashpoint intelligence analysts field questions and conduct specific research inside closed illicit online communities and open sources to provide original, unique analysis.

Proactive Acquisitions

With Proactive Acquisitions, Flashpoint analysts actively monitor your organization's standing portfolio of digital assets that must remain safe. If compromised, Flashpoint analysts will proactively acquire solicited data on your behalf, ensuring that it doesn't become a potential vector for serious cyber attacks.

Proactive Security in 2026 and Beyond

Organizations are facing an unprecedented barrage of sophisticated threats that are more complex, interconnected, and higher-stakes than ever before. Flashpoint's 2026 Global Threat Intelligence Report shows that organizations will soon be defending against an adversarial ecosystem — one where malicious Agentic AI autonomously seeks to exploit the gaps in digital systems. Ultimately, this landscape will be defined by the convergence of autonomous AI, commoditized identity, and a vanishing window of response.

The shift from generative lures to Agentic AI means that our adversaries will soon operate at a velocity that human-only teams cannot match. Accounting for the staggering volume of 3.3 billion stolen credentials and record-high numbers of vulnerabilities and ransomware attacks, intelligence programs built solely around static feeds and retrospective reporting will lag behind. To confront this reality, three key imperatives have emerged:

Prioritize Context Over Volume:

Organizations must pivot to a risk-based intelligence model that filters out the noise, focusing resources exclusively on exposures that demonstrate a high likelihood of weaponization and active exploitation in the wild.

Harden the Human and Machine Identity Layer:

The modern attack surface is defined by trust — whether it is the trust placed in an AI agent's API or the trust placed in a help desk employee. Security teams must treat every digital identity as a potential breach point, requiring constant, real-time monitoring of illicit markets and behavioral anomalies.

Build Resilience Against Systemic Intelligence Failures:

2026 demands a redundant intelligence posture, one that leverages proprietary, dark and deep web research to maintain visibility and operational continuity even when public databases and established security standards experience catastrophic disruptions.

The organizations that fare best will be those that focus on early visibility, contextual intelligence, and human-led analysis, supported by automation rather than replaced by it. As convergence and speed continue to define the threat landscape, foresight is a critical requirement. Flashpoint remains committed to empowering its clients with the intelligence and expertise necessary to confidently confront threats and safeguard their critical assets.

About Flashpoint

Flashpoint is the leader and largest private provider of threat data and intelligence. We empower mission-critical businesses and governments worldwide to decisively confront complex security challenges, reduce risk, and improve operational resilience amid fast-evolving threats. Powered by Flashpoint Primary Source Collection, our proprietary approach to collecting intelligence directly from the digital spaces where threats originate, the Flashpoint Ignite platform delivers unmatched depth, speed, and relevance from open and hard-to-reach sources, enriched by human expertise and scaled by AI. Our solutions span cyber threat intelligence, vulnerability intelligence, geopolitical risk, physical security, fraud, and brand protection. The result: our customers safeguard critical assets, avoid financial loss, and protect lives. Discover more at **flashpoint.io.**

Join the Conversation

LinkedIn | X | Threat Intel Blog

See Flashpoint Ignite in Action

https://flashpoint.io/demo/