FLASHPOINT

2025 Global Threat Intelligence Report

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

FLASHPOINT

Table of Contents

Introducing the GTIR: A Letter from Josh Lefkowitz, Flashpoint CEO

Organizations are facing an unprecedented barrage of sophisticated threats that are more complex, interconnected, and higher-stakes than ever before. From the rapid proliferation of information-stealing malware—a gold mine for threat actors—to the exploitation of vulnerabilities, and the rise of ransomware attacks and data breaches, the threat landscape is evolving at a breakneck pace.

We created the 2025 Global Threat Intelligence Report (GTIR) to provide leaders from across the security spectrum—including cyber threat intelligence (CTI), vulnerability management, and physical security, all the way to the CISO office—with the critical data and insights needed to navigate this complex cyber threat landscape. The report is powered by Flashpoint's best-in-class collection of over 3.6 petabytes of data sourced from the Internet's open and hardest-to-reach spaces, providing a comprehensive and timely view of the threats that will have the most impact in 2025 and beyond.

Read on and you will gain:

1. **A clear understanding of converging threats.**
   See how digital threats intertwine and impact the cyber threat landscape, such as the reemergence of information-stealing malware, the effect of the "New Cold War" on security, and the rise of data breaches and ransomware attacks.

2. **Insight into the tactics, techniques, and procedures (TTPs) of today's most prolific threat actors.**
   Learn about the complex, multi-stage, and converging TTPs being employed by the most prolific threat actors including LockBit, RansomHub, and Judische.

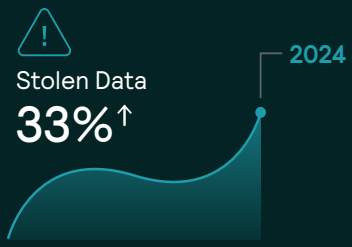
3. **Actionable intelligence to strengthen your security posture.**
   Leverage the latest trends, in-depth analysis, and data-driven insights to bolster your security posture by identifying and proactively defending against rising attack vectors.

Protecting organizations, industries, and communities is a shared mission. We must be one team that unites in the common intention to make the world a safer place. 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: Cyber Threats at a Glance

Flashpoint Identified Four Critical Trends from 2024 That Are Shaping the 2025 Threat Landscape

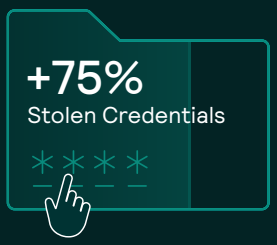


Compromised Credentials Spiked 33% to 3.2 Billion

Flashpoint found that threat actors compromised **over 3.2 billion credentials** in 2024, a **33% increase** from the year prior. This stolen data dominates illicit marketplaces and is used to fuel a number of illegal campaigns such as ransomware or other types of malware. Examining 2025, **over 200 million credentials have already been stolen.**

Infostealers Continued Their Meteoric Rise as a Primary Threat Vector

Of 2024's 3.2 billion stolen credentials, **75% or 2.1 billion**, were sourced from information-stealing malware, a dangerous new twist on an older threat that has infected over **23 million devices worldwide**. The simplicity, effectiveness, vast availability, and low overhead costs of infostealers has propelled them to become a primary vector for ransomware and high-impact data breaches that all organizations should be proactively monitoring for in 2025.



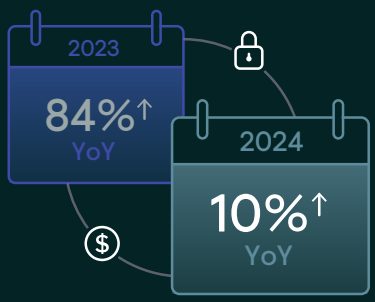
Vulnerabilities Grew by over 12%, More than 39% Have Known Exploits

Flashpoint aggregated **37,302 vulnerabilities** in 2024 and **over 39%** of them had publicly available exploit code. Leveraging exploits, threat actors can force their way into exposed systems to gain illegal access. As attack surfaces continue to grow, so too does the number of potential exposures. As a result, it's more critical than ever for security teams to prioritize based on exploitability, instead of adopting a top-down, or severity-narrowed approach for patching.

Ransomware Attacks Increased by 10%, Data Breaches by 6% Across All Sectors

Once access is gained either through compromised credentials, infostealers, or breaches, financially motivated threat actors use stolen credentials and other illegally-obtained information to complete various objectives that put organizations at greater risk, such as moving laterally within systems, installing ransomware, or exfiltrating and selling data.

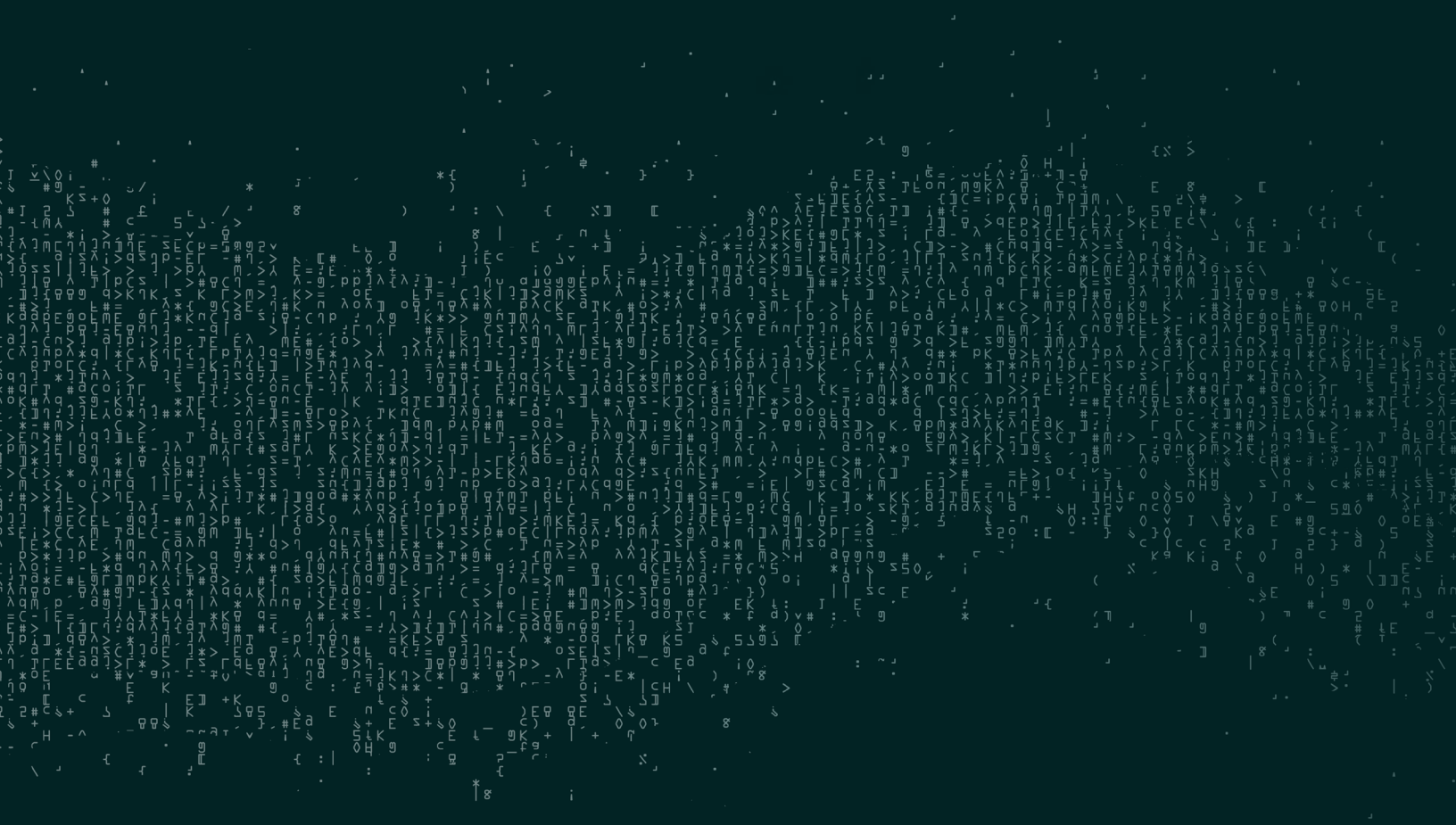
Flashpoint identified a **10% increase** in ransomware attacks across all sectors in 2024, following a tremendous 84% increase from the previous year. In addition, the five most prolific ransomware-as-a-service (RaaS) groups—Lockbit, Ransomhub, Akira, Play, and Qilin—were responsible for **over 47%** of 2024's reported attacks. Data breaches saw a year-over-year increase of approximately **6%**. All of this highlights the need for organizations to maintain strong defenses and incident response plans.



2025 Threat Landscape

DATA BREACHES

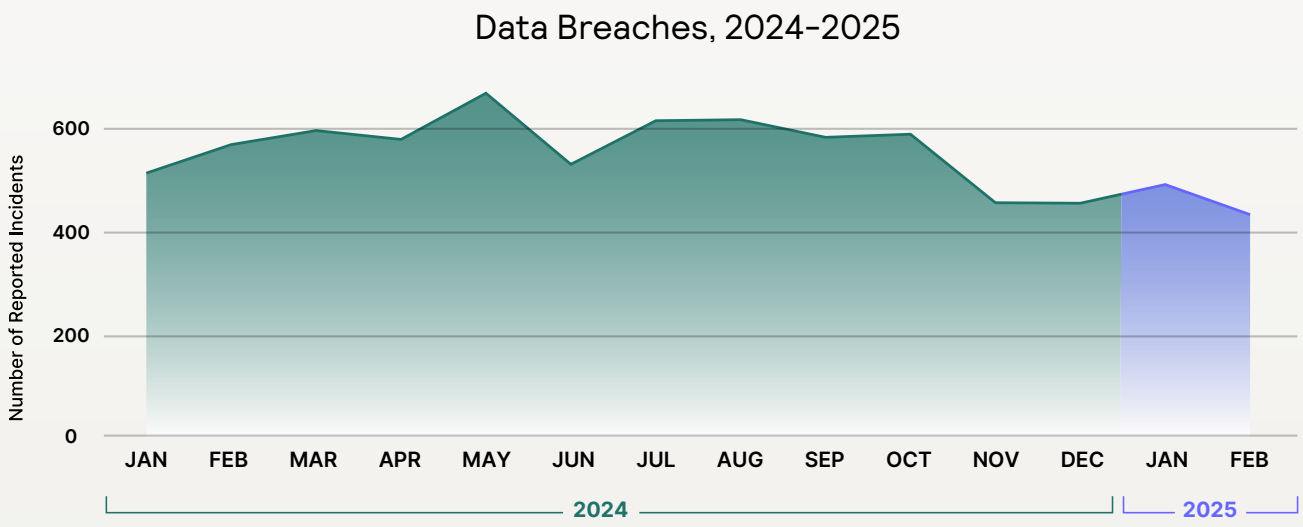
Flashpoint breach data and intelligence, as detailed in this section, comprises the Deep and Dark Web and open sources—including public attorney general reports, ransomware blogs, and Freedom of Information Act (FOIA) requests. Data is current from January 1, 2024 to February 28, 2025.



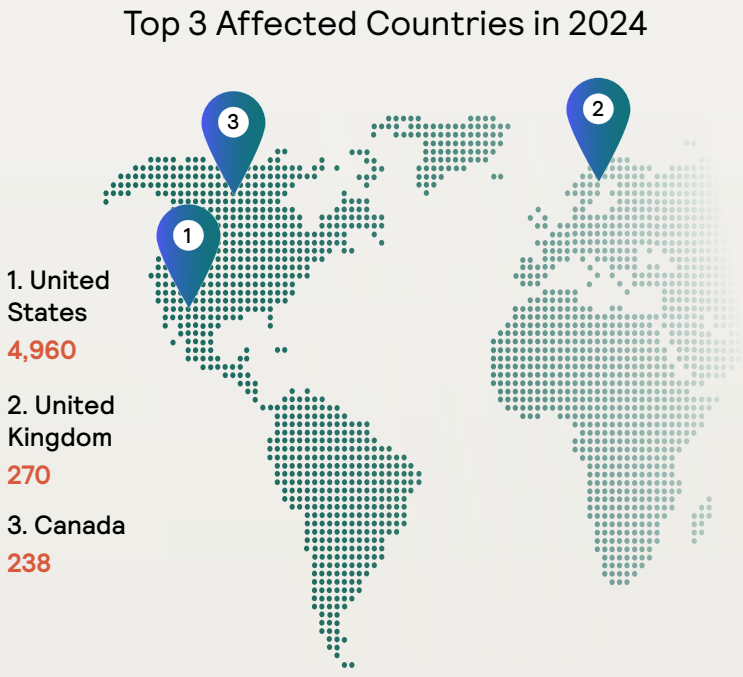
Data Breach Overview: Data and Insights

Data breaches continue to pose a significant threat to organizations worldwide by fueling the cybercrime ecosystem. Flashpoint observed an **approximately 6% increase in data breach activity** in 2024, with our analysts recording **6,670 publicly reported data breaches**. These breaches were responsible for **exposing over 16.8 billion records**, or "rows"—individual data points extracted from compromised systems—that included personally identifiable information (PII) such as names, social security numbers, and financial data.

This exposed PII represents an incredible risk for organizations, as threat actors use the information in various ways including leveraging artificial intelligence (AI) to create large-scale phishing campaigns, or sifting through stolen data for account credentials to power brute-force attacks and account takeover attempts.



The **United States represented more than 63% of the global data breach total** (6,670), reporting 4,260 breaches—a 12% increase compared to 2023. However, Flashpoint notes that both totals could be higher as these figures comprise publicly reported breach events which are often under reported. In some cases, organizations may not be aware that they have been compromised until their data is listed for sale on illicit marketplaces. Additionally, others may choose not to disclose a breach event until they are legally required to. So far, Flashpoint has collected **924 data breaches in 2025**, with **616 (66%) of them affecting organizations in the United States.**



Who is most at risk? Flashpoint data shows that the following five economic sectors, as defined by the North American Industry Classification System (NAICS), reported the most data breaches:

15.9%

Professional, Scientific, and Technical Services

This industry encompasses a wide range of businesses providing specialized knowledge and expertise. These organizations often handle sensitive client data, intellectual property, and financial information, making them attractive targets for cybercriminals seeking to exploit confidential information.

14.8%

Healthcare and Social Assistance

Includes a wide range of healthcare providers, hospitals, social services, and assisted living facilities. This sector often handles highly sensitive personal and medical information, which is valuable for threat actors.

14%

Finance and Insurance

Includes banks, credit unions, insurance companies, and investment firms. Organizations in this sector manage vast amounts of financial data and PII. Using this information, threat actors can attempt to brute-force to take over bank accounts and drain funds.

12.4%

Information

This sector covers a broad range of activities related to the creation, dissemination, and management of information. The data handled by this business group is critical for information flow and communications, making this sector a significant target for disruption and data theft.

11.9%

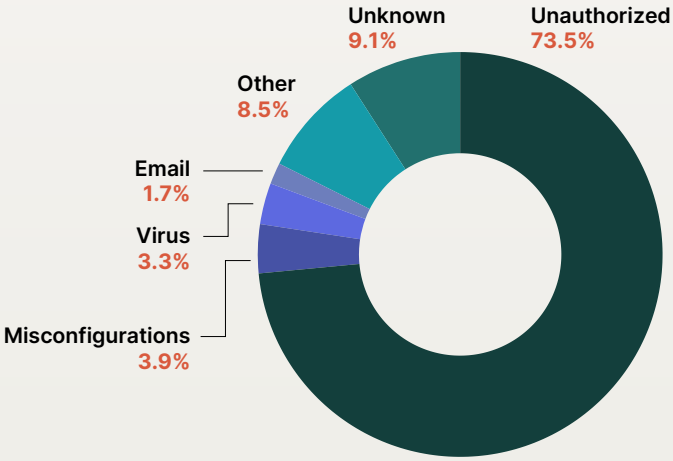
Public Administration

Includes government agencies at the federal, state, and local levels. These organizations hold vast amounts of sensitive data, including citizen information, infrastructure details, and national security information which attackers can sell to advanced persistent threat groups.

Unauthorized Access: From Background Checks to the Kremlin

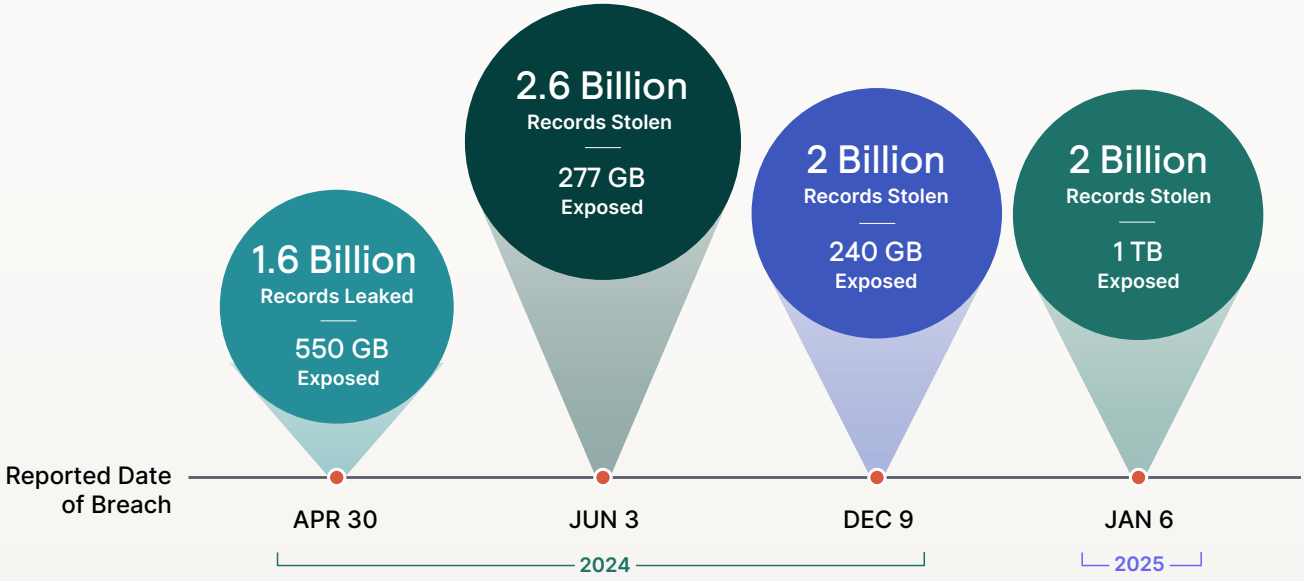
Unauthorized access is the number one cause of data breaches, with over 73% of all 2024 breach events stemming from an unwanted outsider gaining access. The highest number of records lost in this manner was 2.6 billion, when a US-based background check company failed to secure its database containing names, addresses, emails, and social security numbers, which were then listed for sale on illicit marketplaces.

Breakdown of Data Breaches by Type, 2024



This trend is not isolated to 2024. **In the first few months of 2025, over 2.18 billion records have already been exposed**. While the number is staggering, the more interesting development is a new and unusual breach target—Russia. Traditionally, threat actors have avoided compromising Russian organizations, let alone the Russian government. Most malware strains even have built-in code that prevents installation on Windows systems with Russian virtual keyboards installed. The ongoing Ukraine-Russia conflict has significantly impacted the cyber threat landscape, creating divisions between Ukrainian and Russian threat actor groups and leading to increased targeting of Russian entities. This highlights the direct influence of geopolitical dynamics on cyber activity.

2024-2025 Data Breaches Responsible for Exposing the Most Records



The Effect of Data Breaches on the Cyber Threat Landscape

Beyond the immediate reputational, financial, and legal repercussions for organizations, data breaches also contribute to the long-term growth and sophistication of the cyber threat landscape. Most threat actors are financially motivated, selling billions of stolen data records on illicit marketplaces and forums, which further fuels the cycle of cybercrime.

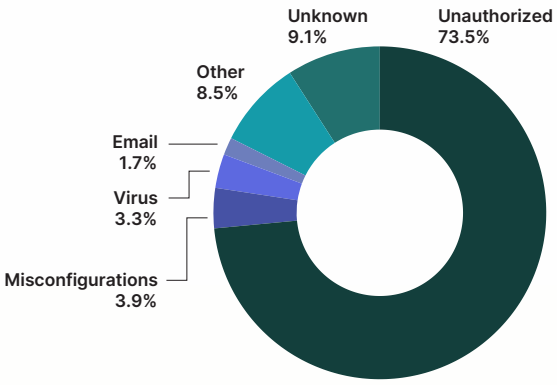
Leveraging this stolen data, threat actors harvest actionable information, often in the form of credentials—particularly account details such as usernames and passwords. This, in combination with other sensitive data and PII, provides attackers with what they need to operationalize their illegal campaigns. **Overall, Flashpoint found that threat actors compromised over 3.2 billion credentials in 2024, a 33% increase from the year prior.** Examining 2025, over 200 million credentials have already been stolen highlighting the pervasiveness of this threat.

Data Breach Quickview

JANUARY 2024-DECEMBER 2024

6,670	16.8 Billion	3.2 Billion
TOTAL DATA BREACHES	STOLEN RECORDS	STOLEN CREDENTIALS

Breakdown of Data Breaches by Type



Top 3 Affected Countries

1. United States
   4,260
2. Canada
   270
3. United Kingdom
   238

Key Takeaways

1 **Data breach activity is escalating, with a significant impact on sensitive data:**
The 6% increase in data breaches in 2024, resulting in 16.8 billion exposed records, demonstrates a steadily growing trend. This massive exposure of sensitive information such as social security numbers, financial data, and account information poses a substantial risk to both individuals and organizations.

2 **Unauthorized access remains the primary driver of data breaches:**
Exacerbated by geopolitical tensions, 73% of breaches stem from unauthorized access, which underscores the critical importance of robust access controls. The convergence of cyber and geopolitical factors has also resulted in a shift in targeting against Russian entities in 2025.

3 **Data breaches fuel the broader cybercrime ecosystem:**
The sale of stolen data on illicit marketplaces and the subsequent use of compromised credentials to launch further attacks create a self-perpetuating cycle of cybercrime. Organizations must recognize that data breaches are not isolated incidents but contribute to a larger, interconnected web of cyber threats.

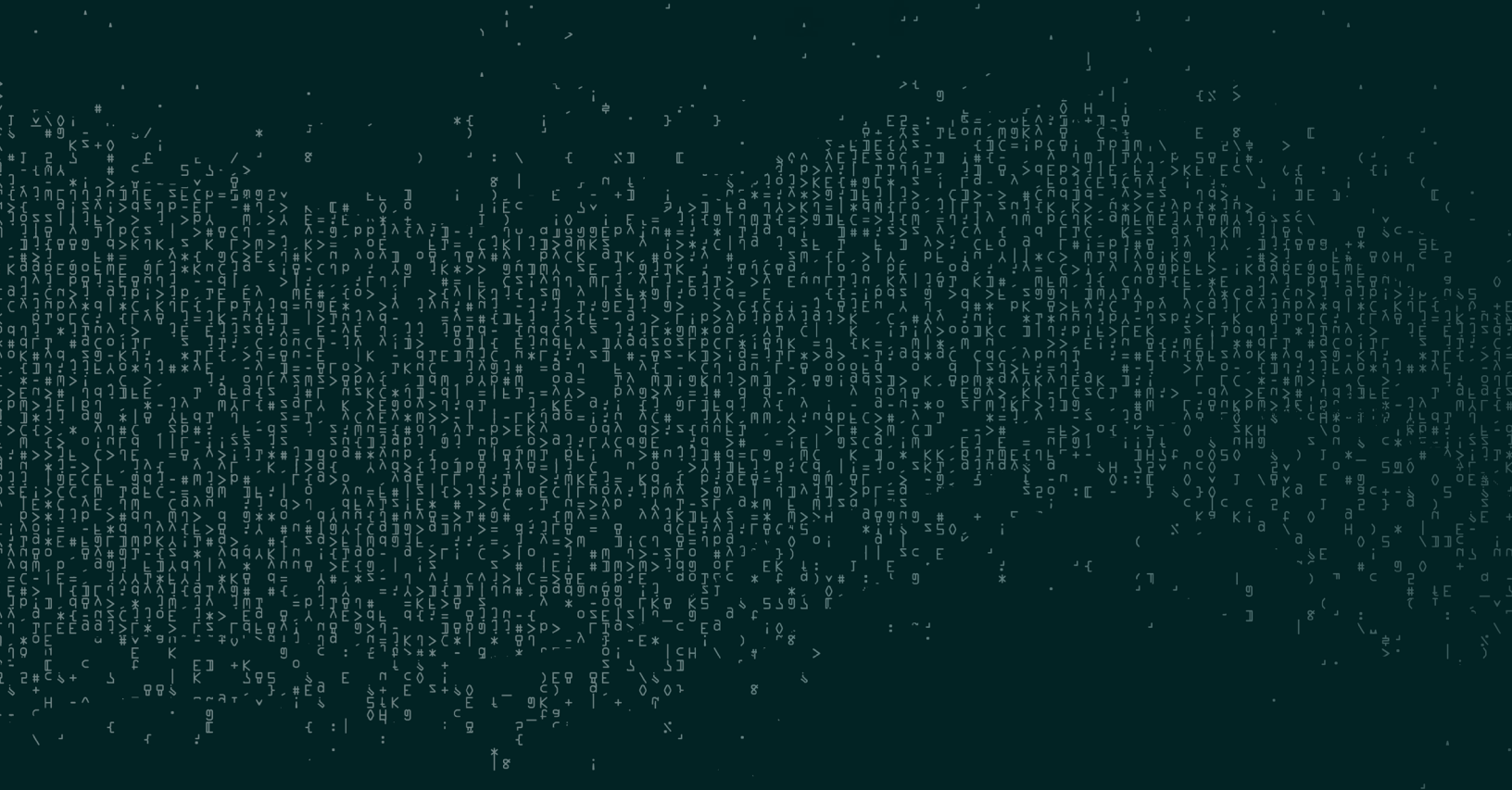
Threat Posture Assessment

- [ ] Is my organization operating in a highly-targeted economic sector? If so, can I vouch for where all of our critical data is being stored and secured?
- [ ] Are offline backups being tested regularly for integrity, and is it clear who their owners are?
- [ ] Are my security teams proactively tracking known illicit forums and marketplaces for any mentions of my organization and third-party partners?

2025 Threat Landscape

INFORMATION-STEALING MALWARE

Flashpoint infostealer data and intelligence, as detailed in this section, is derived from extensive monitoring of illicit online marketplaces, dedicated Telegram channels, and specialized bot shops where stealer logs and related services are traded. Data is current from January 1, 2024 to February 28, 2025.



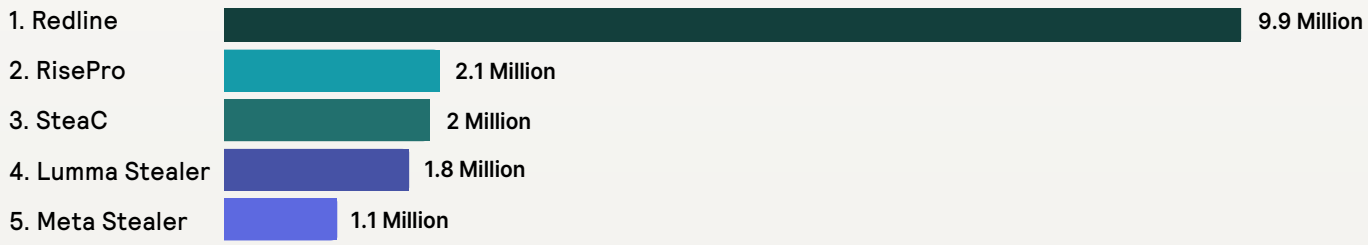
Infostealer Overview: Data and Insights

Information-stealing malware had a profound effect on the threat landscape, stealing **2.1 billion, or 75%, of 2024's 3.2 billion stolen credentials**. Also known as infostealers or stealers, their simplicity, vast availability, and low costs have made them incredibly popular among threat actors, with these malicious programs playing a pivotal role in many of 2024's most headline-grabbing data breaches.

Flashpoint analysts infiltrated threat actor communities and discussion groups, **tracking over 164 infostealer-related sales threads last year, finding a total of 24 unique stealer strains listed for sale on illicit marketplaces.** Each of these strains were specifically designed to circumvent specific security measures, employing a wide and diverse range of techniques—such as utilizing Telegram for exfiltration and command or control (C2) or preventing installation on virtual machines to avoid unnecessary detection and forensics.

Top 5 Most Prolific Infostealers in 2024

By Infected Hosts or Devices

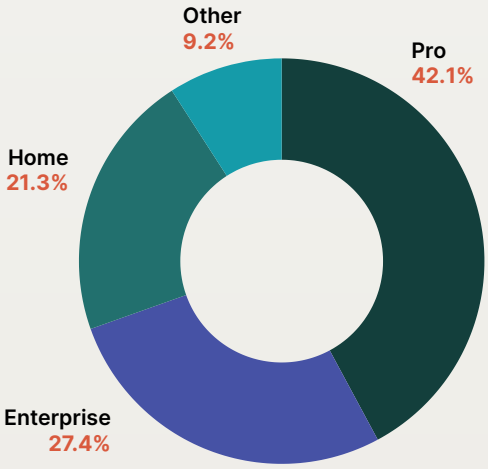


Infostealer Distribution: Corporate vs. Small Business

Infostealers compromised 23 million hosts and devices last year. Of those on Microsoft operating systems, data suggests **69% of infostealer infections likely targeted devices on corporate systems.** Conversely, 21.3% affected small businesses and personal devices. Regardless of size, organizations need to ensure that security teams are actively monitoring infostealer activity, in addition to being knowledgeable about prolific stealer strains such as RisePro, StealC, and Lumma.

Despite recent takedowns it is still likely for Redline and Meta to be repurposed, or duplicated as "new" strains. Being knowledgeable of infostealer tactics, techniques, and procedures (TTPs) is essential since every unique stealer has its own method of bypassing commonly used security measures, and can be used in combination with each other for maximum chances of success.

Windows OS Breakdown of Infected Host Data, 2024



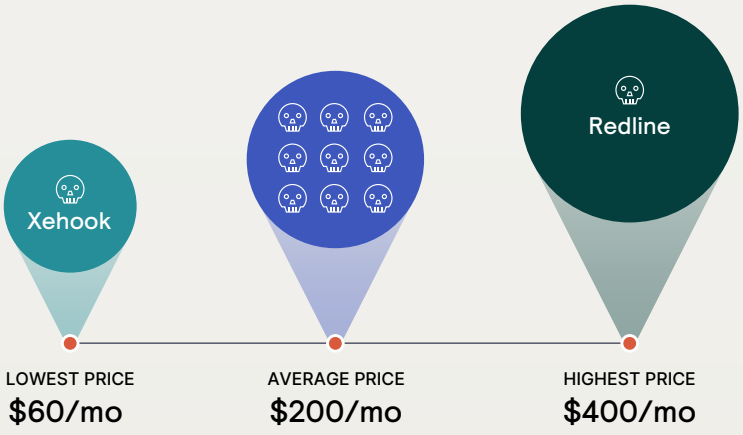
The Effect of Information-Stealing Malware's on the Cyber Threat Landscape

In April 2024, a data storage company suffered a breach that impacted over 165 organizations. Threat actors used stolen credentials obtained through various infostealers including Vidar, Risepro, Redline, Racoon, Lumma, and Meta Stealer to gain unauthorized access in order to compromise sensitive data belonging to multiple high-profile organizations.

Infostealers are inexpensive, costing threat actors $200 USD a month on average. They are also easy to use and are readily available on underground forums and dark web marketplaces. Stealers have been incredibly effective in carrying out crippling supply chain attacks and targeting critical infrastructure. As such, organizations working with third-parties should be extra vigilant in securing any shared sensitive data.

Top 5 Countries Affected by Information-Stealing Malware, 2024

While there have been attempts to hinder infostealers by implementing new app-bound cookie encryption updates, as well as other security improvements, stealer developers have been quick to respond. Furthermore, despite the takedown of Redline—the most prolific stealer of 2024—and Meta Stealer, the overall market and use of infostealers in 2025 continue to rise.



Infostealer Prices, 2024

Infostealer Quickview

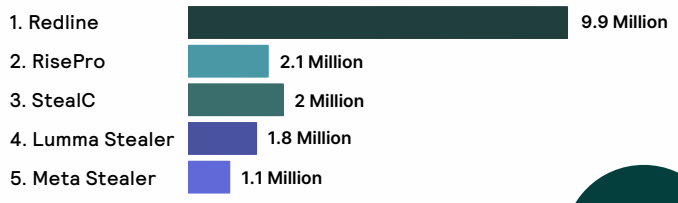
JANUARY 2024-DECEMBER 2024

23 Million
INFECTED HOSTS AND DEVICES

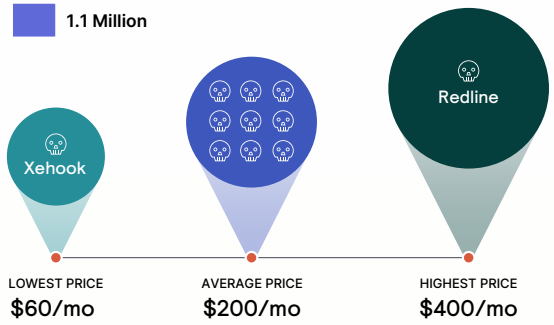
2.1 Billion
STOLEN CREDENTIALS

Top 5 Most Prolific Infostealers

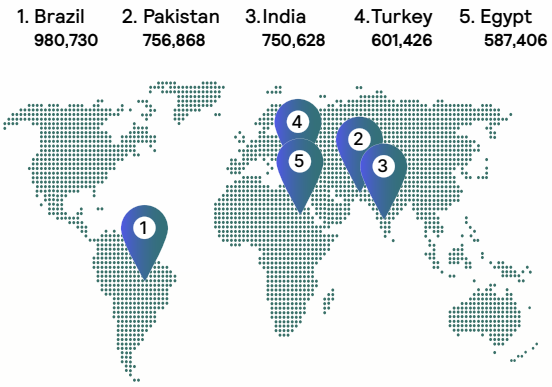
By Infected Hosts or Devices



Prices of Infostealers



Top 5 Countries Infected by Infostealers



Key Takeaways

1 **Information-stealing malware is a dominant, growing, and highly accessible threat:**
Infostealers are becoming a pivotal component in the modern cyberattack chain, acting as a gateway to broader compromises. Their success in 2024 stealing 2.1 billion credentials and infecting 23 million devices, coupled with their low cost and widespread availability, have elevated them to a primary threat vector that all organizations should be proactively monitoring in 2025.

2 **Corporate systems are particularly at risk:**
Flashpoint data suggests that 69% of infostealer infections impacted corporate hosts and devices, compared to 21.3% affecting small businesses. This highlights a critical exposure in enterprise security and demonstrates the need for security teams to be knowledgeable of existing, and emerging stealer strains—especially in regards to how they are designed to bypass security measures.

3 **The infostealer market is dynamic and resilient:**
The rapid emergence of new infostealer strains and the persistence of the market, even after the takedowns of Redline and Meta Stealer, indicates a highly adaptable and resilient threat landscape. Organizations must adopt a proactive security posture, continuously monitoring for new threats and adapting their defenses accordingly.

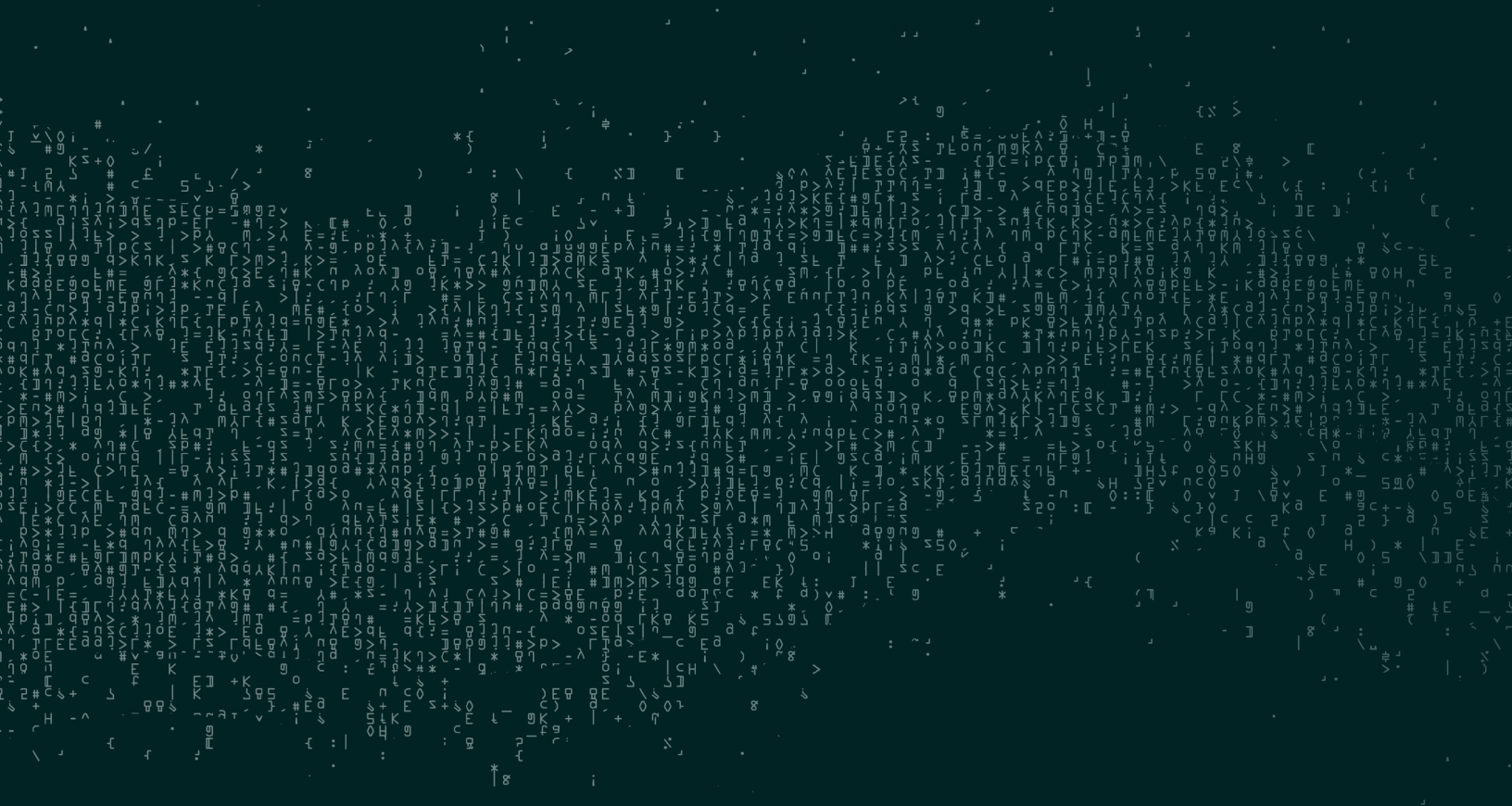
Threat Posture Assessment

- [ ] Is my organization actively monitoring online channels and communities where our stolen credentials are often shared?
- [ ] Do my security teams and third-party partners have plans in place to respond to infostealer infections and mitigate their impact?
- [ ] Is my Cyber Threat Intelligence team knowledgeable of the most prolific stealer strains and how they bypass security measures?

2025 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 enrichment provides full context into metadata such as EPSS, the MITRE ATT&CK framework, exploit intelligence, social risk, and ransomware likelihood. Data is current from January 1, 2024 to February 28, 2025.

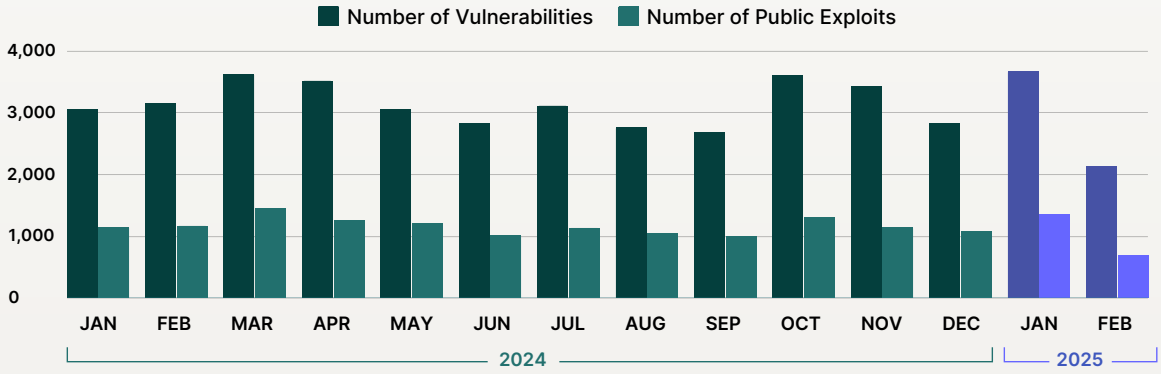


Vulnerability Overview: Data and Insights

Attack surfaces continue to grow each year as new software and hardware flaws, or vulnerabilities, are discovered in organizational technologies. According to Flashpoint's vulnerability intelligence data, there has been a **year-over-year increase of over 12%**, with our analysts aggregating **37,302 vulnerabilities in 2024**. Looking specifically at the **first two months of 2025, Flashpoint has already collected and detailed 5,784 vulnerabilities** with disclosures showing no signs of slowing down.

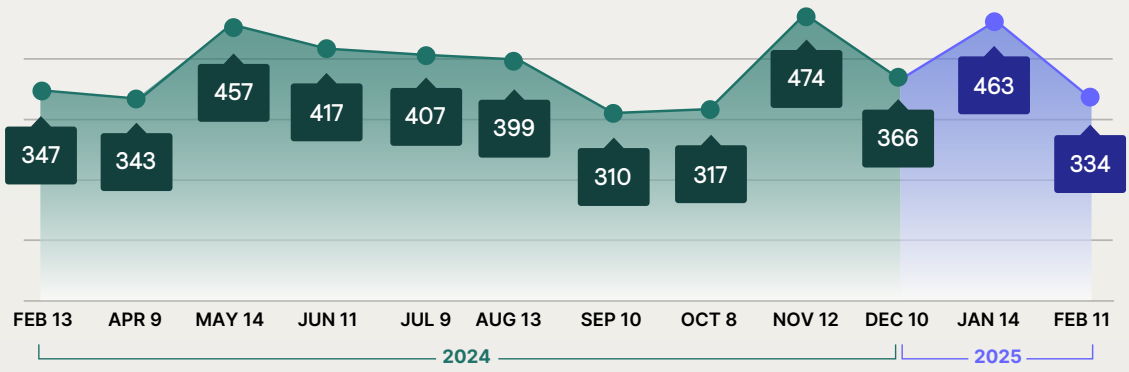
As vulnerability disclosures continue to steadily grow, organizations need to adapt their security strategies appropriately. Due to the sheer amount of resources and research required, it is unrealistic for the majority of organizations to triage, remediate, or mitigate every vulnerability. Instead, security leaders and vulnerability management teams need to implement a risk-based patching framework that is geared towards their unique needs and is based on relentless prioritization.

Vulnerability Disclosures and Exploits, 2024-2025



Examining disclosures on a daily level, hundreds of vulnerabilities are steadily being released throughout the year. Looking at the ten days with the most vulnerability disclosures, there is a consistent trend: they all are dominated by Microsoft's Patch Tuesday, when Microsoft releases updates and patches for its software products on the second Tuesday of each month.

Top 10 Days with Most Vulnerability Disclosures, 2024-2025



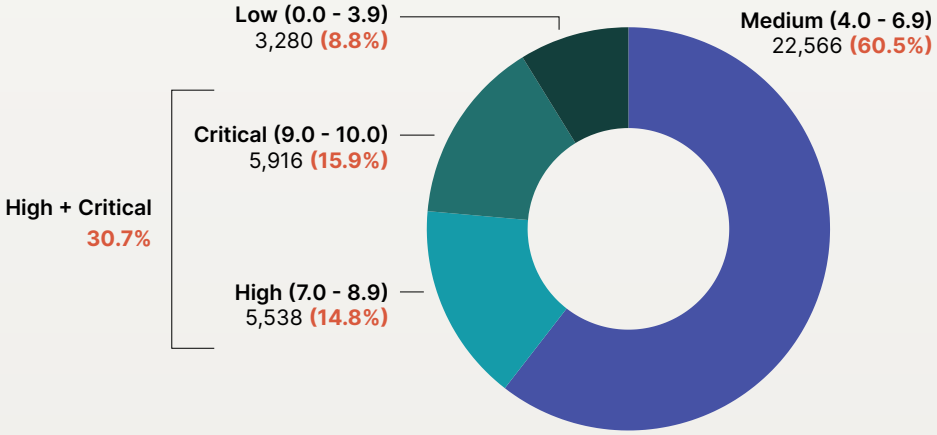
Since Patch Tuesday's introduction in 2003, Flashpoint has observed an overwhelming number of notable vendors adopting it for their own releases. This, coupled with the growth of Common Vulnerability and Exposures (CVE) Numbering Authorities (CNA)—organizations authorized to assign CVE IDs to vulnerabilities and publish CVE records—has caused disclosures to be grouped more tightly together, playing a major role in every year's rising totals.

Limitations of CVSS Severity Scores

Organizations have historically patched "top-down," focusing on vulnerabilities highly rated in severity. However, this approach has not brought meaningful results as too many vulnerabilities are rated high (7.0) to critical (10.0) using the Common Vulnerability Scoring System (CVSS). This is mainly due to CVSS specifications mandating to "score for the worst" if there are no details. 2024 was no exception as over 30% of all vulnerabilities fell between those ranges. As a result, prioritizing solely based on this characteristic will not result in effective or timely patching.

Security teams must remember that different versions of CVSS can drastically impact the score of a given vulnerability, especially for issues that borderline between "medium" and "high." An immediate shift in scoring guidelines could either drastically increase or decrease critical workloads. Regardless, Flashpoint includes up-to-date and corrected scores for CVSSv2, v3, and v4 for every newly disclosed vulnerability.

CVSS Breakdown for 2024 Vulnerabilities



Cut Critical Vulnerability Workloads by 83% Using Metadata

The most effective way to prioritize vulnerabilities is by filtering critical vulnerabilities leveraging metadata—particularly using exploit intelligence. **Examining 2024, over 39% of all vulnerabilities had publicly available exploit code, a 26% increase from the previous year.** These issues represent an immediate risk to organizations. However, remediating or mitigating every exploitable vulnerability in a timely manner is still an incredibly resource-taxing undertaking, and unrealistic for most organizations.

To make this timely, **organizations can cut their critical vulnerability workloads by 83% using additional metadata**. Security teams should further filter exploitable vulnerabilities by:

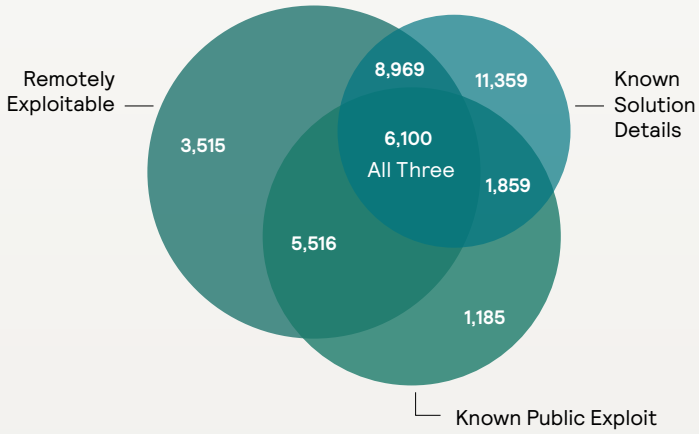
1. **Determining if any exploits are remotely exploitable:** Remote code executions (RCEs) allows threat actors to compromise affected systems regardless of where the attacker is located.
2. **Whether there is a documented solution for the exploit:** An existing solution saves time spent on vulnerability research, allowing organizations to immediately triage and patch issues.

Depending on any other organizational requirements, other considerations and metadata, such as Ransomware Likelihood scoring, social risk, or MITRE ATT&CK mapping can be added. Once applied, security teams can produce an actionable vulnerability report, and then secure the proper resources to remediate them. Then, once those issues are fully resolved, they can then focus on other flagged issues.

The Effect of Vulnerabilities on the Cyber Threat Landscape

Vulnerability exploits often serve as the initial access point in cyberattacks such as ransomware. Attackers actively scan for and target systems with known vulnerabilities, a process made easier by infostealers (see page 11). Once a vulnerability is identified, threat actors leverage publicly available exploits, develop their own, or solicit for exploit code to gain a foothold in the target network.

Breakdown of Actionable, High Severity Vulnerabilities, by Availability and Exploitation, Disclosed in 2024



Vulnerability Exploit Attack Chain

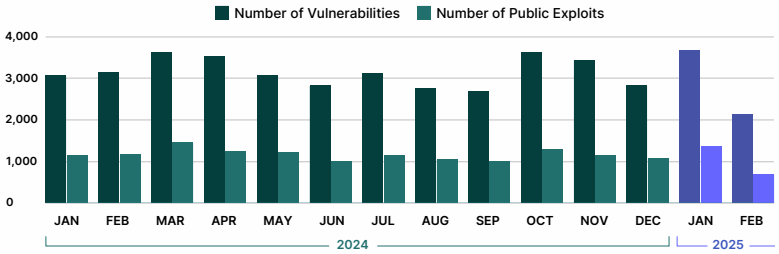
Vulnerability Quickview

JANUARY 2024-DECEMBER 2024

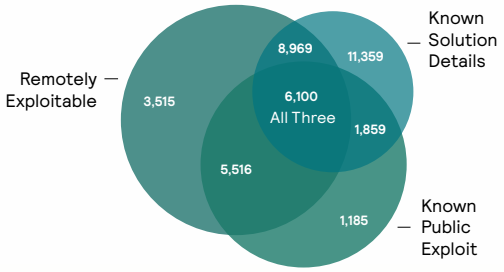
37,302
DISCLOSED VULNERABILITIES

14,660
VULNERABILITIES WITH PUBLICLY AVAILABLE EXPLOITS

Vulnerability Disclosures and Exploits



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



Key Takeaways

1 **Vulnerabilities are surging, creating an overwhelming challenge for vulnerability management (VM) teams:** The 12% year-over-year increase in vulnerability disclosures, with over 37,000 vulnerabilities in 2024, demonstrates the sheer volume of security flaws that organizations must contend with. This deluge, exacerbated by Patch Tuesday and the growing numbers of CNAs, makes it nearly impossible for VM teams to address every vulnerability, necessitating a strategic, risk-based approach to patching.

2 **Relying solely on CVSS scores for prioritization is ineffective; exploit intelligence and metadata are crucial:** The overabundance of high to critical CVSS scores renders them insufficient for effective vulnerability prioritization. Leveraging exploit intelligence and additional metadata, such as remote exploitability and known solutions, enables organizations to reduce their critical vulnerability workload by 83%. This focused approach allows security teams to concentrate on the most impactful threats, while maximizing their resources.

3 **Vulnerabilities are a prime attack vector for threat actors, emphasizing the need for proactive defense:** Vulnerability exploits allow threat actors to gain initial access to target networks for attacks like infostealers or ransomware. The increasing availability of exploit code and the ease of scanning for vulnerable systems underscore the need for proactive vulnerability management. Organizations must prioritize timely patching of exploitable vulnerabilities to minimize their attack surface.

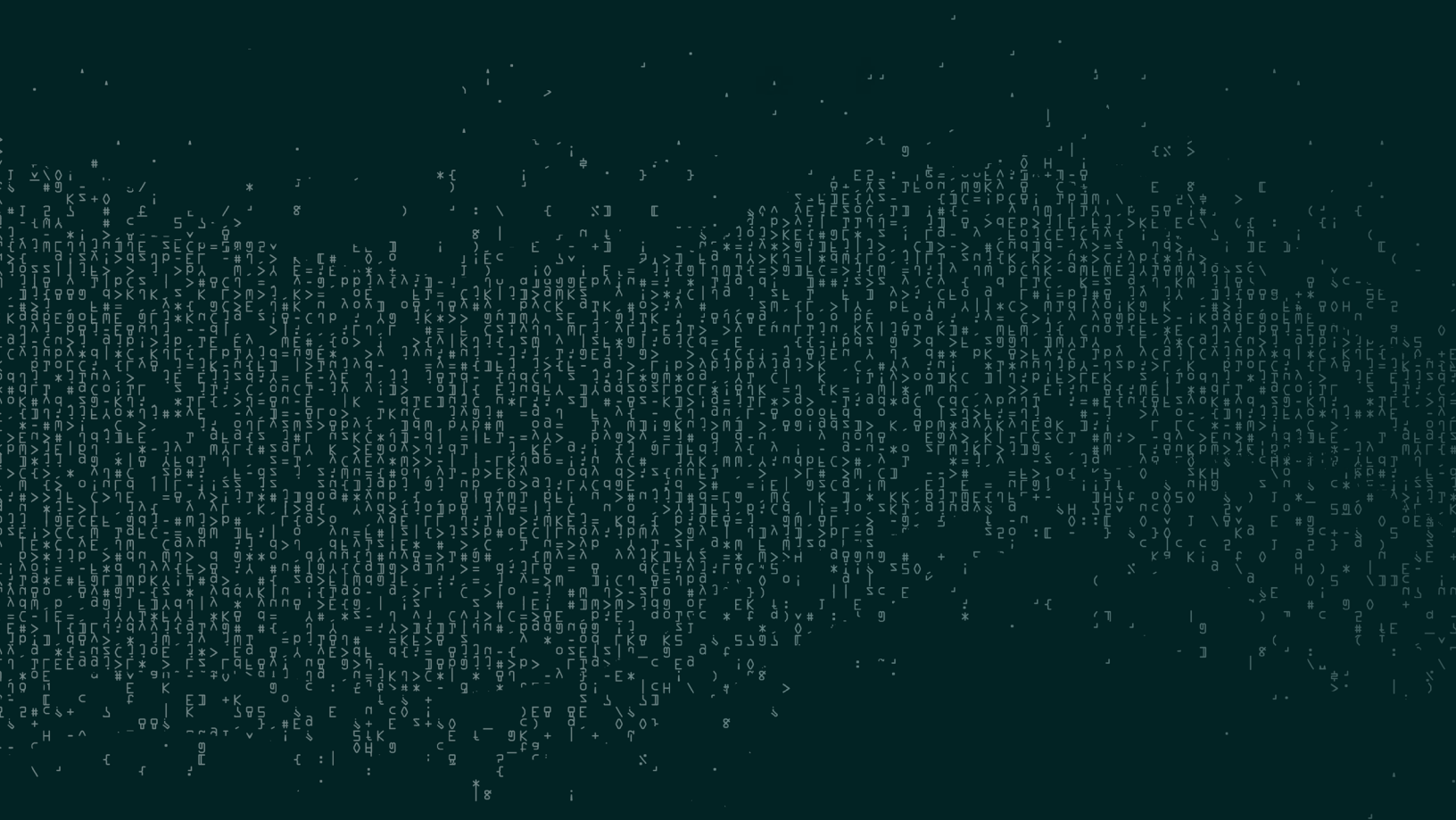
Threat Posture Evaluation

- [ ] Is my vulnerability management team prioritizing remediation based on risk and threat intelligence?
- [ ] Does my vulnerability management team have access to comprehensive metadata, such as Ransomware Likelihood and MITRE ATT&CK mapping?
- [ ] Is my IT team able to quickly patch vulnerable systems, or are they forced to research solutions themselves?

2025 Threat Landscape

RANSOMWARE

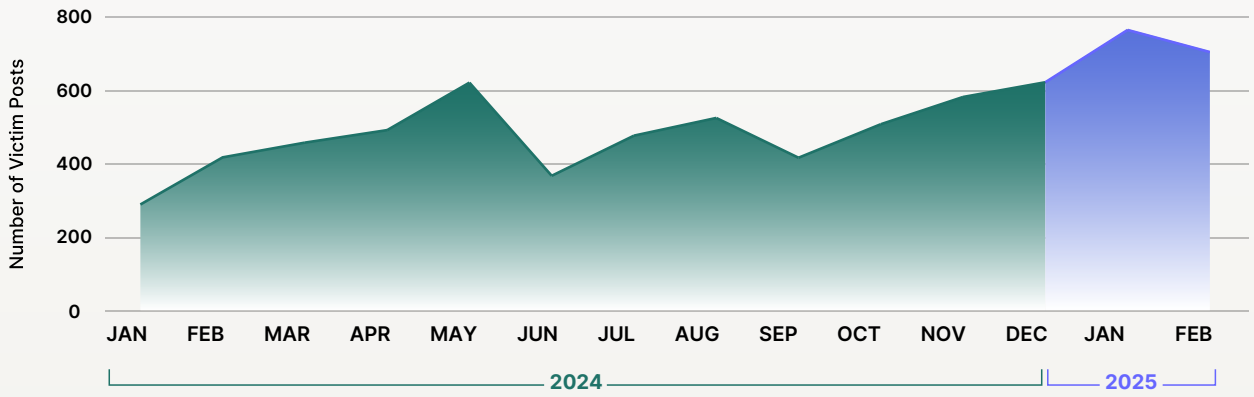
The data in this section comprises victimized organizations that have been announced on ransomware blogs and leak sites. Data is current from January 1, 2024 to February 28, 2025.



Ransomware Overview: Data and Insights

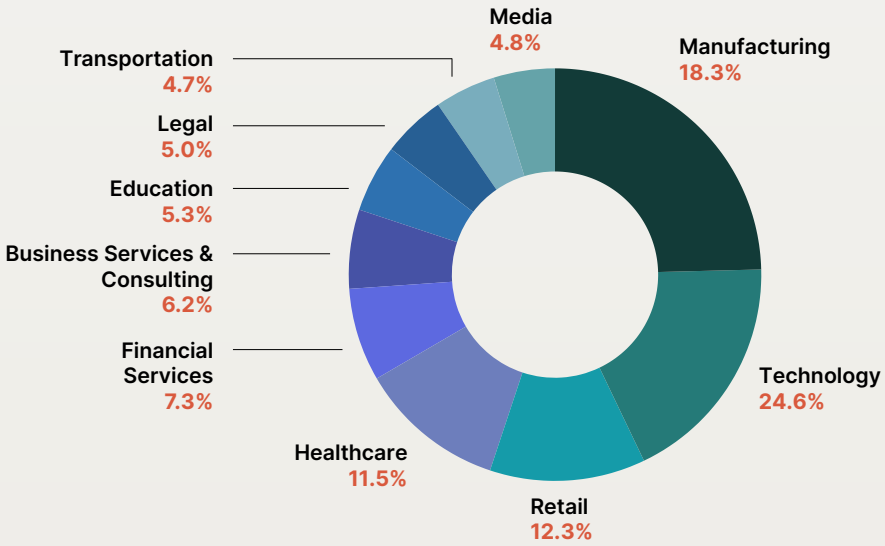
Ransomware attacks, in which malicious actors encrypt an organization's data and demand a ransom for its release, continue to plague organizations. Flashpoint identified **5,742 ransomware attacks—approximately a 10% year-over-year increase—across all sectors, with technology (24.6%), manufacturing (18.3%), and retail (12.2%) experiencing the most ransomware attacks**. This 10% increase follows a tremendous 84% year-over-year increase the previous year, showing that ransomware still remains an alarmingly high and dangerous threat.

Reported Ransomware Attacks, 2024–2025



While ransomware attacks occur globally, the vast majority of them affect the United States, due to the value of the data its organizations maintain and their demonstrated high willingness to pay. Flashpoint analysts found that the **United States experienced over 51% of 2024's total ransomware attacks. 1,462 ransomware attacks have been reported in 2025, with 805 (55%) of them affecting US-based organizations**.

Breakdown of Ransomware Attacks by Industry, 2024



Top 10 Countries Affected by Ransomware, 2024

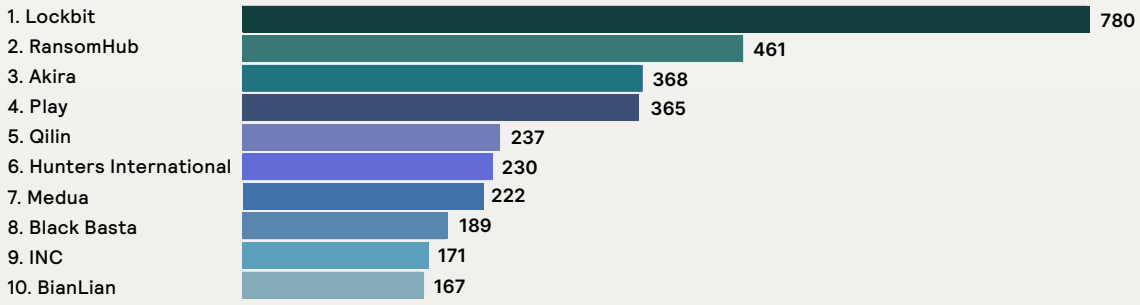
1. United States 2,977
2. United Kingdom 263
3. Canada 259
4. Germany 170
5. Italy 145
6. Brazil 131
7. France 129
8. India 125
9. Spain 115
10. Australia 96

Ransomware-as-a-Service: Fueling the Growth of the Ransomware Ecosystem

The staggering availability of ransomware-as-a-service (RaaS) plays a massive role in ransomware's continued growth. RaaS, combined with other malware, such as infostealers, creates a force-multiplier effect that greatly lowers the barrier to entry, allowing unsophisticated attackers to leverage these complex tools as long as they can afford an illicit monthly subscription, on average costing $200 USD.

RaaS has a direct effect on the ransomware landscape, with **just five of 2024's most prolific RaaS groups—Lockbit, Ransomhub, Akira, Play, and Qilin—being responsible for over 47% of the year's ransomware attacks.**

Top 10 Most Prolific Ransomware-as-a-Service Groups in 2024

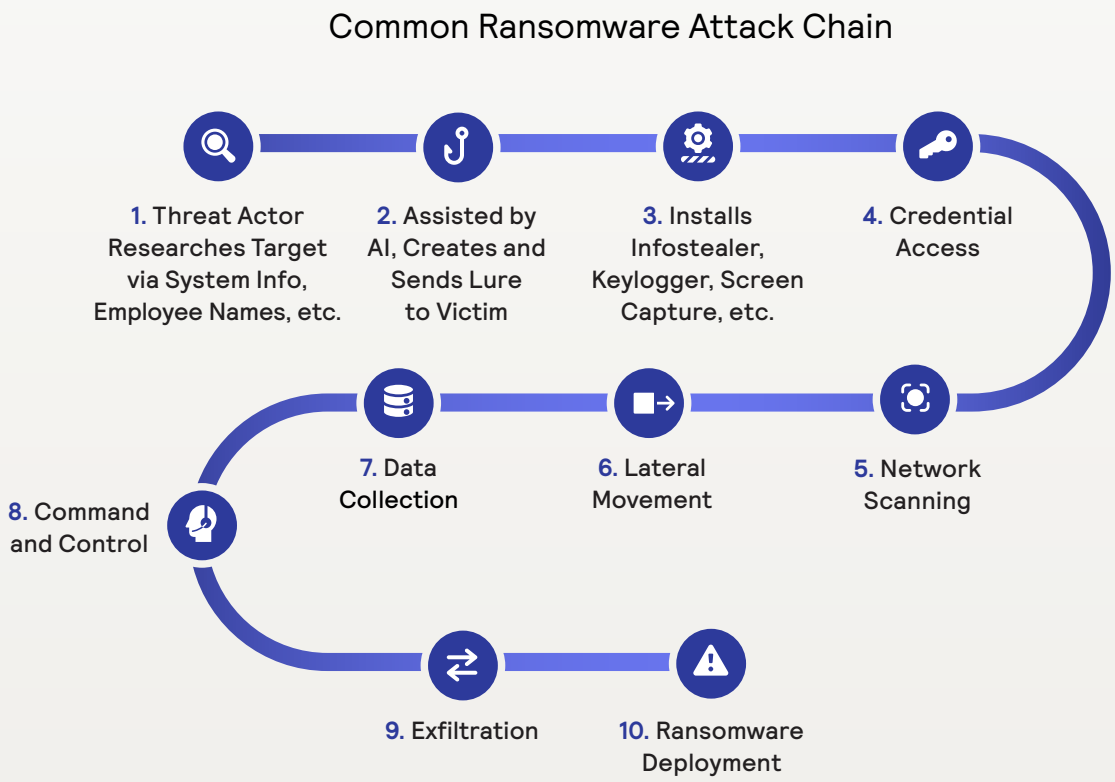


Flashpoint recorded several hierarchy changes within the landscape as high-profile ransomware groups discontinued operations and newly emerged groups filled the void. One of the most notable changes to the top 10 RaaS list in 2024 was the absence of ALPHV/BlackCat, the second most active RaaS group last year. Their absence on the list can be attributed to the December 2023 seizure of their leak site by global law enforcement agencies. Taking their place on the list is RansomHub, a group that first appeared in February 2024. The group quickly gained notoriety due to their high-profile attack on a major healthcare organization. It is highly likely that RansomHub is composed of former members of ALPHV/BlackCat.

Lockbit continued their place as the most prolific RaaS group, listing 780 victims on their leak site in 2024, despite facing several upheavals. In February 2024, the group lost thirty-four servers, 14,000 rogue accounts, and 200 cryptocurrency accounts due to Operation Cronos, a collaborative global law enforcement takedown. Then in May 2024, the United Kingdom's National Crime Agency identified and coordinated sanctions against Lockbit's founder, Russian national Dmitry Yuryevich Khoroshev. However, Lockbit continues to operate, albeit posting lower numbers of victims compared to previous years.

The Effect of Ransomware on the Cyber Landscape

The commoditization of RaaS has created a challenging environment for security teams, **with over 42% of all reported data breaches explicitly citing ransomware**. Developments in the cyber threat landscape continue to show that ransomware attacks are not isolated incidents.

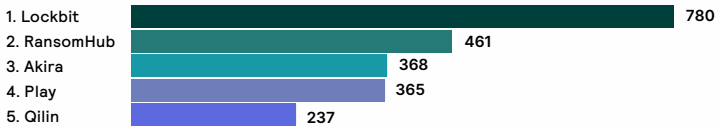


Ransomware is often part of a complex, multi-stage operation that can weave together infostealers, AI-powered phishing lures or other AI-assisted attacks, vulnerability exploits, in addition to other various tactics, tools, and procedures. Therefore, organizations need comprehensive intelligence that also monitors ransomware-adjacent threats. This can equip teams to identify potential attacks, prevent them, and respond swiftly during incidents, ensuring quick recovery with minimal disruption.

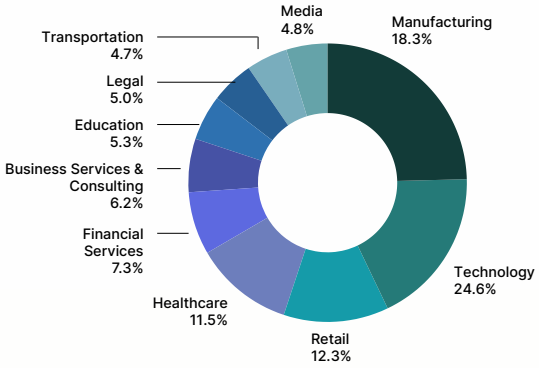
Ransomware Quickview

JANUARY 2024-DECEMBER 2024

Top 5 Most Prolific Ransomware-as-a-Service Groups



Breakdown of Ransomware Attacks by Industry



Top 10 Targeted Countries

1. United States: **2,977**
2. United Kingdom: **263**
3. Canada: **259**
4. Germany: **170**
5. Italy: **145**
6. Brazil: **131**
7. France: **129**
8. India: **125**
9. Spain: **115**
10. Australia: **96**

Key Takeaways

1 **Ransomware remains a significant, pervasive, and evolving threat:**

There was a 10% increase in ransomware attacks in 2024, totaling 5,742 incidents. This follows a 84% YoY increase experienced in the previous year. The continued prevalence of ransomware, particularly in the technology, manufacturing, and retail sectors, highlights the need for organizations to maintain strong defenses and incident response plans.

2 **RaaS is lowering the barrier of entry, enabling a wider range of attackers:**

The accessibility of RaaS offerings, combined with other malware like infostealers, is lowering the barrier to entry for cybercriminals. This 'force-multiplier effect' allows less sophisticated attackers to launch complex ransomware attacks, increasing the overall risk for organizations of all sizes.

3 **Ransomware attacks are often part of a larger, multi-faceted operation:**

Ransomware is rarely an isolated incident. It is often integrated into complex attack chains involving various tactics, techniques, and procedures, such as AI-powered phishing, vulnerability exploitation, and data exfiltration. This underscores the need for a holistic security approach that addresses the interconnectedness of cyber threats.

Threat Posture Evaluation

- [ ] Do my security teams have a process for proactively monitoring RaaS leak sites and illicit marketplaces to detect potential mentions of the organization?
- [ ] Is my security team aware of the latest TTPs being employed by the most prolific RaaS groups such as Lockbit, Ransomhub, Akira, Play, and Qilin?
- [ ] Do we have a ransomware response team or playbook that includes negotiation protocols, is easily accessible, up to date, and based upon actual resources?

Commentary

May You Live in Interesting Times: The Rise and Fall of Threat Actors

By Ian Gray
Vice President of Intelligence, Flashpoint

We live in interesting times, where technology is both a blessing and a curse. 2025 is following a year of significant upheaval in the cybercrime landscape, marked by high-profile arrests, platform policy changes, and the rise and fall of prominent threat actors. The aforementioned risks—compromised credentials, infostealers, and vulnerabilities—served as an undercurrent for the many cyberattacks and extortion events that took place throughout the year. In cybersecurity, curses typically come in threes:

1. May You Live in Interesting Times: The volatility and change that comes with progress
2. May You Come to the Attention of Those in Authority: Success, notoriety, and its eventual consequences
3. May You Find What You're Looking For: The desire to take and protect

As you will see, the solution is not a talisman but intelligence, preparedness, and the foresight to recognize that curses might just be opportunities in disguise.

May You Come to the Attention of Those in Authority: Government Takedowns

2024's cyberattacks did not occur without impunity, with law enforcement notably cracking down on ALPHV/BlackCat, LockBit, and BreachForums. In these interventions, multiple global law enforcement agencies seized cybercriminal infrastructure, arrested high-profile individuals, and attempted to disrupt parts of their cybercrime operations.

Law enforcement also shuttered multiple marketplaces, disrupted infrastructure for botnets, malware droppers, infostealers, and attempted to interrupt the attack chain of multiple campaigns. Despite law enforcement's wins in 2024, many of these venues continued to operate, albeit with setbacks:

ALPHV/BlackCat Splinters into RansomHub

The December 2023 law enforcement seizure of ALPHV/Blackcat's, one of the largest ransomware groups, spilled into 2024 as the group struggled to maintain its infrastructure and extort Change Healthcare. The ensuing $22M USD ransom payment led to a power struggle between operators and affiliates that played out on Deep and Dark Web forums. ALPHV/Blackcat resolved the issue by claiming that the FBI re-seized their infrastructure, as a front for an exit scam. RansomHub accepted its affiliate refugees, becoming one of the largest ransomware groups of 2024 and extorting Change Healthcare a second time.

LockBit "Taken Down" by Operation Cronos

In February 2024, LockBit's infrastructure was seized by law enforcement in Operation Cronos, led by the UK's National Crime Agency. The disruption led to a decline in the total number of victims and affected LockBit's ability to recruit affiliates. An ensuing phase of Operation Cronos further pressured LockBit to close, including sanctions, asset seizures, and travel bans for their administrator. Despite the reduced capacity, Lockit claimed to be unphased and continued its operations, even resorting to recycling its victims on its leak site to appear operational.

BreachForums Heavily Disrupted

In May 2024, the FBI and DOJ disrupted BreachForums, the largest English-language data breach forum, following a shutdown of its predecessor Raid Forums in 2022, and the original Breach Forums in 2023. Following a short period of reorganization, BreachForums (with a slightly different spelling) re-appeared albeit with rumors of the arrest of one of its administrators. The site owners, "ShinyHunters" appeared to step down while other threat actors began to take more prominent roles in the forum's operation. Meanwhile, some of the largest breaches of the year continued to play out on BreachForums. High-profile members such as the threat actor "Judische" were arrested for infecting multiple victims through info stealer logs on infected victims of a cloud data warehouse platform. Then, "USDoD," who was responsible for the compromise of a large US data broker and multiple other companies, was arrested in Brazil.

These incidents don't happen in a vacuum. These vignettes are only a portion of last year's interventions, all of which continue to impact the 2025 landscape—including threat actors migrating to new venues or infrastructure. For example, Lumma and Vidar have likely already replaced infostealer activity from RedLine and Meta Stealer's takedown. There is increasing opportunity within the cybercrime realm, and the absence of one prominent individual or group leads to others vying to take the top spot.

Hubris often comes before the fall. As many of these cybercrime venues were created with the intent to skirt sanctions or amass illicitly obtained profits, they often attract the exact intention they sought to avoid. While 2024 was an interesting year, 2025 is already off to an explosive start with Clop's exploitation of Cleo file transfer application echoing 2023's MOVEit attacks.

May You Find What You Are Looking For

As we navigate 2025's threat landscape, perhaps the final curse is the most fitting to transform into a blessing. Organizations seeking security will indeed find what they're looking for—in the form of endless vulnerabilities, evolving threats, and persistent adversaries. It is important to understand that while these are tools for adversaries, we have the ability to mitigate them through vulnerability management, proactive management of cybercrime communities, and strategic intelligence thereby transforming these "curses" into opportunities for resilience.

The cybersecurity community will find new challenges in AI-augmented attacks, expanding attack surfaces, and increasingly sophisticated social engineering. Threat actors will find not just the opportunities they seek, but also the heightened scrutiny, improved defenses leveraging AI-tools shepherded by human intelligence, coordinated law enforcement actions, and inevitable consequences that follow.

In this digital landscape of action and reaction, of curses disguised as opportunities and opportunities disguised as curses, one thing remains constant: we will continue to live in interesting times. And that may be the most reliable curse of all.

Navigating the New Hybrid Cold War

By Andrew Borene
Executive Director of Global Security and International Markets, Flashpoint

Rising geopolitical tensions are reshaping the global threat environment. Adversaries like Russia, China, Iran, and North Korea are employing hybrid warfare strategies that destabilize international alliances and create unprecedented security challenges. This era of heightened competition—what Flashpoint calls the "New Cold War"—is defined by its convergence across digital, physical, and geopolitical domains. Unlike the Cold War of the 20th century, today's battlefield is asymmetric, decentralized, and constantly shifting. To navigate this reality, security professionals must adapt, using intelligence-driven strategies that anticipate and mitigate threats before they escalate into crises.

Just a few recent examples illustrate this new hybrid Cold War landscape:

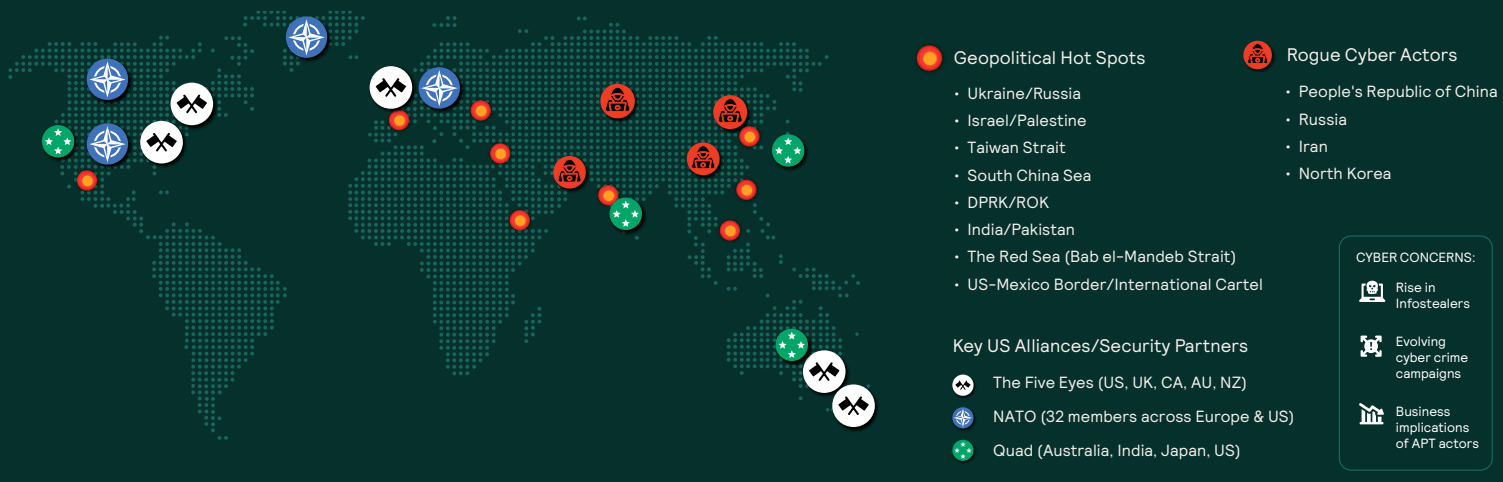
1. Before boots first touched the ground in Ukraine, Russian cyber operations targeted Ukraine's power grid, financial sector, and critical government systems confirming what intelligence agencies long suspected: cybercriminals and state actors are working in lockstep.

2. North Korea's Lazarus Group is funding the regime through sophisticated cyber campaigns, siphoning billions from financial institutions and cryptocurrency platforms to fuel its weapons program and bypass international sanctions. Iran, China, and Russia are leveraging AI-generated deepfakes, fake social media personas, and information warfare to manipulate public perception, disrupt democratic institutions, and influence global discourse, presenting a direct challenge to intelligence and security professionals trying to distinguish fact from fiction.

3. Adversaries don't use a single method of attack—they employ them all. This new hybrid reality highlights the urgent need for a security approach that is proactive, intelligence-led, and deeply integrated across domains.

The New Cold War is Hybrid

A convergence of threats across geopolitical, cyber, and physical domains



Open Source Intelligence as the First Line of Defense

Open-source intelligence (OSINT) has become indispensable in this New Cold War environment. Recognized by the Director of National Intelligence as the "INT of first resort," OSINT enables security teams to detect early warning signs, monitor online sentiment, and neutralize risks before they materialize into real-world threats. Unlike classified intelligence, OSINT is accessible to both government agencies and the private sector, making it a critical tool for decisionmakers across international borders and sector boundaries.

By leveraging OSINT, organizations can:

- Gain real-time insights from publicly available data to understand adversary tactics and intent.
- Enhance transparency in intelligence operations, ensuring credibility and verifiability.
- Operationalize intelligence at scale, connecting cyber, physical, and geopolitical threats into a single, actionable picture.

For professionals in national security, OSINT provides visibility into adversary movements, supply chain vulnerabilities, and emerging threat vectors. In the private sector, OSINT is essential for protecting intellectual property, security supply chains, and safeguarding executives from targeted threats.

OSINT in Action: The Ukraine War as a Case Study

The war in Ukraine has demonstrated OSINT's mission-critical role in modern intelligence operations. While classified intelligence informs high-level strategy, real-time, verifiable OSINT has provided key insights into battlefield developments, allowing OSINT practitioners to:

- **Track Russian troop movements** using satellite imagery, geolocation data, and social media analysis.
- **Identify and disrupt logistical networks** supporting mercenary groups soliciting donations, purchasing military equipment, and supplying Russian forces in Ukraine.
- **Expose disinformation campaigns** by studying propaganda efforts aimed at justifying the invasion and shaping public perception.
- **Document war crimes** through collection and verification of evidence, including unique identifiers such as patches, license plates, road signs, and landmarks, to track the movement of troops and supplies.

Flashpoint analysts have leveraged OSINT tools such as optical character recognition (OCR) and global social media monitoring to map illicit fundraising activity, track arms shipments, and monitor key personnel involved in the conflict. These insights have proven invaluable in countering hybrid warfare tactics and strengthening resilience across sectors.

Security professionals who fail to adapt will be left reacting to threats rather than anticipating them. OSINT is no longer just a tool, it is a strategic necessity for delivering actionable insights that shape real-world security outcomes.

The stakes are too high for complacency. This moment calls for OSINT professionals to become New Hybrid Cold Warriors who collaboratively operate across shared private sector and government interests to defend the whole of society.

The Best Data for The Best Intelligence

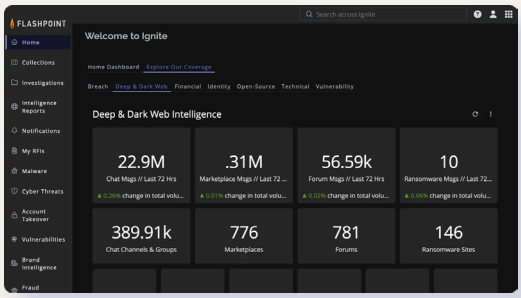
Following the preceding analysis and assessment of your organization's threat posture, the subsequent step is to provide your teams with the tools and intelligence required to address identified exposures. From real-time threat intelligence to proactive vulnerability management, discover how Flashpoint 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 places the power of our data, intelligence expertise, and automated analysis into the hands of security teams, enabling them to identify and remediate risk and take rapid, decisive action. By combining the skills of our analysts with cutting-edge technology, we offer a comprehensive solution that transcends the limitations of conventional approaches, giving our customers the intelligence they need to reduce risk, optimize operations, and improve resilience.

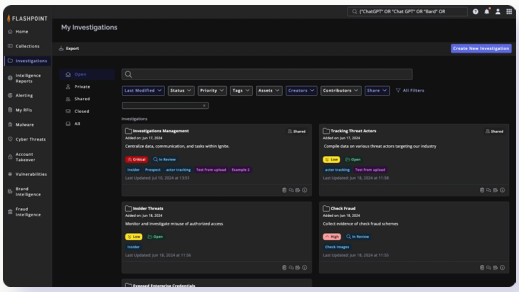


41B+	5.2B+	138B+	349K+
Stolen Credentials	Chat Service Messages	Stolen Accounts	Vulnerabilities (100K+Pre-CVE)
64M	212M+	1.2B+	2.1B+
Paste Site Articles	Unique Media Assets Collected	Illicit Marketplace Elements	Stolen Credit Cards

Core Packages

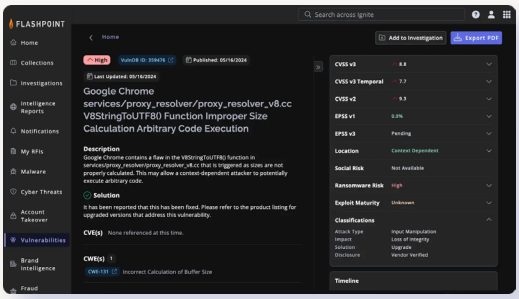
Flashpoint Cyber Threat Intelligence

Secure your organization from evolving cyber threats such as cybercrime, emerging malware, ransomware, account takeovers, and vulnerabilities with Flashpoint Cyber Threat Intelligence (CTI). Seamlessly integrating automated data collection and human analysis, it provides a precise understanding of evolving threat landscapes. Flashpoint CTI delivers high-quality, actionable intelligence, enabling security teams to identify mission-critical risk and take rapid, decisive action.



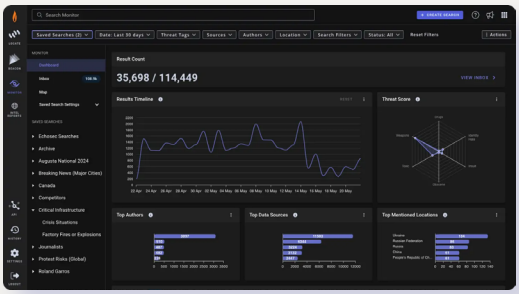
Flashpoint for Vulnerability Management (Built on VulnDB®)

Gain timely awareness of new vulnerabilities with attribution to affected products/versions, packages, and libraries, severity scoring, and exploit intelligence. VulnDB 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.



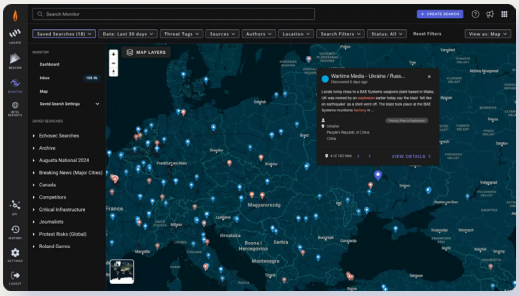
Flashpoint Physical Security Intelligence (Built on Echosec)

Secure your organization from evolving cyber threats such as cybercrime, emerging malware, ransomware, account takeovers, and vulnerabilities with Flashpoint Cyber Threat Intelligence (CTI). Seamlessly integrating automated data collection and human analysis, it provides a precise understanding of evolving threat landscapes. Flashpoint CTI delivers high-quality, actionable intelligence, enabling security teams to



Flashpoint National Security Intelligence

Today's digital communication landscape generates an unprecedented amount of open-source intelligence across a myriad of networks, presenting a significant challenge in harvesting pertinent information and disseminating it to the appropriate teams. This process is crucial for expediting and enriching intelligence cycles. Flashpoint National Security Intelligence offers rapid and secure access to essential data, advanced technology, and critical insights, empowering government agencies with the necessary knowledge, oversight, and contextual understanding to effectively propel their missions forward.



Additional Capabilities

Managed Attribution

Empower your security team to delve into threat intelligence like never before with Flashpoint's Managed Attribution. This turnkey virtual environment allows you to safely conduct advanced digital operations and research, liberating you from the overhead associated with building and maintaining virtual machines.

Fraud Intelligence

Flashpoint Fraud Intelligence helps security and fraud teams detect indicators of fraud across the cybercriminal economy to evaluate exposure, investigate potential risk, and take action before monetary loss and 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 have the flexibility to search for fraud indicators with or without bank or customer identifiers, effectively identifying and investigating deceptive activities aimed at your organization.

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.

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. By identifying misuse or impersonation swiftly, it 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.

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.

The Path Forward: Proactive Security in 2025 and Beyond

The data and analysis in the *Flashpoint 2025 Global Threat Intelligence Report* exposes a hybrid, interconnected cyber threat landscape that demands a proactive and holistic security approach. This extensive collection of data and analysis provides organizations with in-depth insights into the cyber threat landscape, enabling them to make informed security decisions and build a more resilient security posture.

Three themes emerge as critical takeaways to navigate this challenging environment:

The Hybrid Nature of Cyber Threats:

Cyber threats are converging, with data breaches, information-stealing malware, vulnerabilities, and ransomware taking center stage in 2025. Cybercriminals and nation-state actors are carrying out complex campaigns against organizations, supply chains, and critical infrastructure—weaving together various tactics, tools, and procedures (TTPs).

Adapting to the Evolving Threat Landscape:

Organizations need to move beyond siloed intelligence teams and adopt an integrated security strategy. The cyber threat landscape is dynamic and constantly evolving. Throughout 2024 and 2025, infostealer strains and various RaaS offerings have emerged regularly, while existing threats adapt their TTPs to evade defenses.

Proactive Defense Through Foresight:

Leverage the latest trends, in-depth analysis, and data-driven insights to bolster your security posture by identifying and proactively defending against rising attack vectors.

The Flashpoint 2025 Global Threat Intelligence Report serves as an indispensable resource for organizations navigating today's complex and interconnected cyber threat landscape. By embracing the report's findings and recommendations, organizations can proactively defend against evolving threats, adapt to the dynamic nature of cybercrime, and build a more secure and resilient future. Flashpoint remains committed to empowering its clients with the intelligence and expertise necessary to confidently confront cyber risks 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. Through the Flashpoint Ignite platform, we deliver unparalleled depth, breadth and speed of data from highly relevant sources, enriched by human insights. 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 Coversation

LinkedIn | X | Threat Intel Blog | Intelligence-101

See Flashpoint in Action

https://flashpoint.io/demo/