FLASHPOINT

2024

Global Threat Intelligence Report

Data, Insights, and Strategies for Navigating Today's Cyber, Physical, and Geopolitical Threat Landscape

Table of Contents

Foreword: On Resilience and Security in 2024

In the evolving landscape of global security, where cyber and physical threats increasingly converge, the *Flashpoint 2024 Global Threat Intelligence Report* offers a critical examination of the current threat environment. This year's analysis goes beyond traditional threat intelligence, incorporating Flashpoint's unparalleled data and insights to shed light on cyber threats, geopolitical turmoil, and escalating physical conflicts around the world. The goal: help your organization to strengthen its defenses, ensure operational resilience, and proactively confront multifaceted threats—thereby safeguarding critical assets, preventing financial losses, and protecting lives.

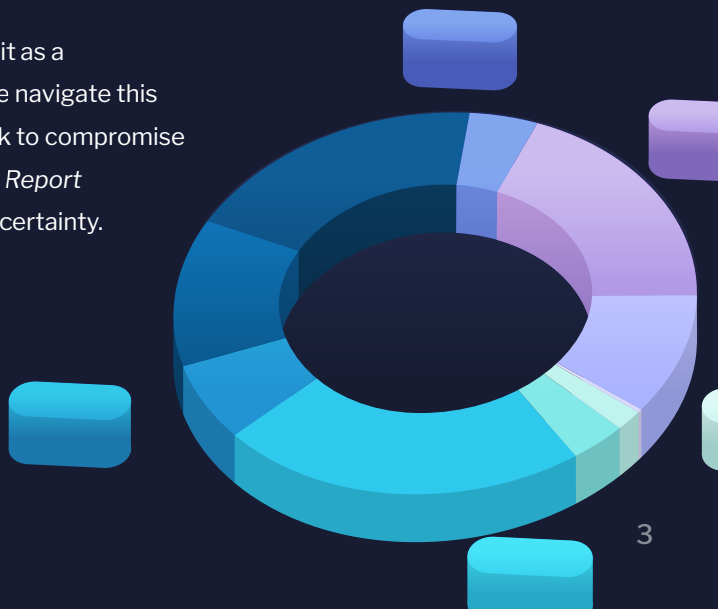
Cyber threats remain at the forefront of global security challenges, as opportunistic and resilient adversaries exploit vulnerabilities through sophisticated tactics. Our annual report details the continuing surge of ransomware attacks, data breach trends, and the exploitation of vulnerabilities, underscoring the evolving nature of cyber risks. Sectors rich in sensitive and confidential data continue to be prime targets, emphasizing the critical need for robust cybersecurity measures and actionable intelligence to counter threats and protect assets.

Looking ahead through 2024, we see the ongoing convergence of cyber and physical threats exacerbated by escalating geopolitical unrest. These include crucial elections, the continuous conflict between Russia and Ukraine, the Israel-Hamas War, and strategic tensions in the Taiwan Strait, each adding layers of complexity to the global threat landscape.

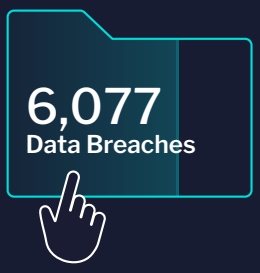
A notable highlight of our annual report is its focus on the central role of open-source intelligence (OSINT) in addressing not only cyber threats but also physical security challenges. In these pages, Flashpoint Executive Director of Global Security, Andrew Borene, provides his perspective on the next evolution of OSINT. The importance of OSINT is further detailed through a case study about its role in an investigation of fentanyl precursor sales. This investigation reveals the complex networks behind illicit activities, showcasing the effectiveness of integrated intelligence in dismantling such operations to enhance public safety and national security.

I invite you to explore the insights provided in the report and to utilize it as a cornerstone for constructing a more resilient and secure future. As we navigate this complex landscape, reinforcing our defenses against threats that seek to compromise our collective security, the *Flashpoint 2024 Global Threat Intelligence Report* illuminates the path forward, offering a beacon of clarity in a sea of uncertainty.

Josh Lefkowitz
Flashpoint CEO



Executive Overview: Cyber Threats at a Glance



Data Breaches Rose 34.5% in 2023.

Flashpoint recorded 6,077 data breach incidents in 2023. More than 70% of these stolen records—which include everything from financial data to personal health records—stemmed from direct compromise or via an affected third-party.

17Bn Records Stolen in 2023.

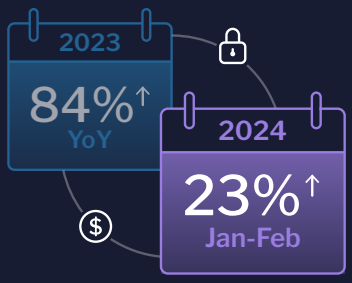
From January 1 to February 29, 2024, the number of stolen or leaked personal data spiked more than 4X compared to the same period last year. Unauthorized access and ransomware remain the primary culprits behind data breaches, accounting for over half of the incidents impacting major industries.

35% of Vulnerabilities in 2023 Had Known Public Exploits.

Prioritization continues to be challenging as the number of new technologies is introduced into the market, with 2023 marking a significant peak of 33,137 issues. Of those issues, 35% had known public exploits. Moving into 2024, Flashpoint continues to observe similar trends in vulnerability totals, disclosure rates, and exploitability.

Ransomware Attacks Rose by 84% in 2023.

After leveraging both zero-day and disclosed vulnerabilities to gain illegal access, financially motivated threat actors take additional actions on objectives, like installing ransomware. Flashpoint identified a significant increase in ransomware attacks across all sectors in 2023, resulting in an increase of 84% YoY. In the first two months of 2024 alone, the number of public ransomware attacks has grown nearly 23% compared to the same period in 2023.

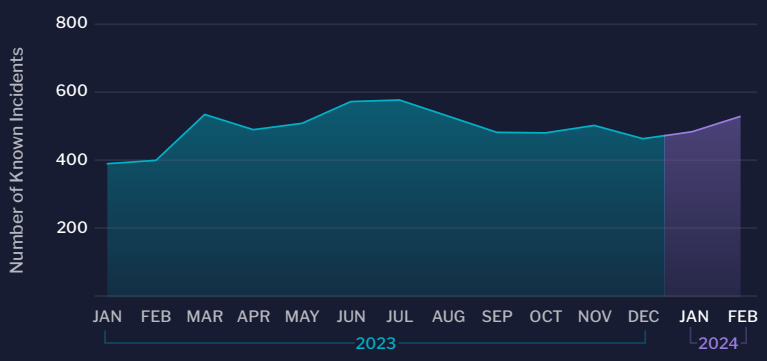


Key Threat Landscapes: Data and Insights

Data Breaches

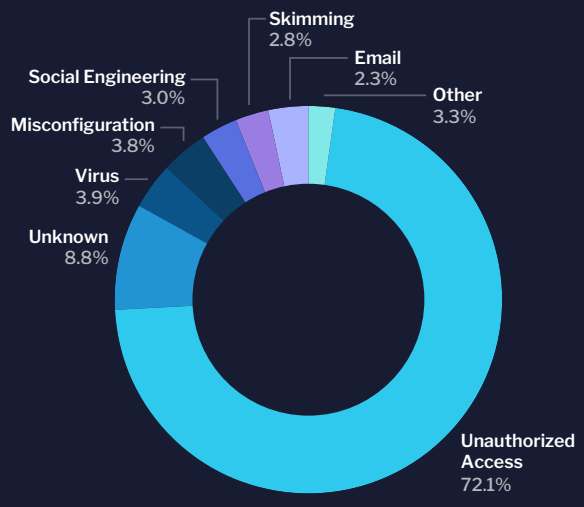
Flashpoint breach data and intelligence, as detailed in this section, comprises the Deep and Dark Web and open sources, including public attorney general reports, ransomware blogs, and Freedom of Information Act (FOIA) requests. Data is current to the date of publishing.

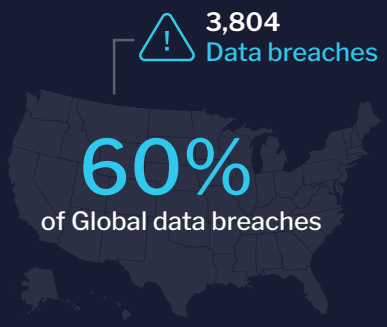
Data Breaches 2023-24



Flashpoint observed a significant uptick in data breach activity in 2023, with our analysts recording 6,077 publicly reported data breaches—**a 34.5% increase compared to 2022.** Data breaches are responsible for leaking over **17 billion personal records** that included sensitive information such as names, social security numbers, and financial data. Over 70% of these incidents were the result of unauthorized access that stemmed from outside the affected organization.

Unauthorized access, continues to be the number one cause of publicly disclosed data breaches.





19.8%↑
2023 vs. 2022

30%↑
Jan-Feb vs. PP

The United States represented more than 60% of the global data breach total, reporting 3,804 data breaches—a 19.8% increase compared to 2022. **In the first two months of 2024 alone, data breaches have increased by an additional 30% compared to the previous year, within the same period.**

However, of all incidents recorded last year, one cyberattack in particular had a profound impact on the data breach landscape—Cl0p's exploitation of a vulnerability within the MOVEit file transfer application. By leveraging a vulnerability within the MOVEit Transfer file application (VulnDB ID: 322555, CVE 2023-34362), the ransomware group had compromised numerous organizations by the end of 2023, either directly or through third-party compromise. Looking specifically at public breach disclosures, Flashpoint analysts determined that **the MOVEit attack was responsible for 19.3% of all reported 2023 data breaches.** This figure includes affected third-parties, organizations who were not directly compromised by Cl0p, but had sensitive data stolen from vendors within their supply chain.

Vulnerability metadata for CVE 2023-34362

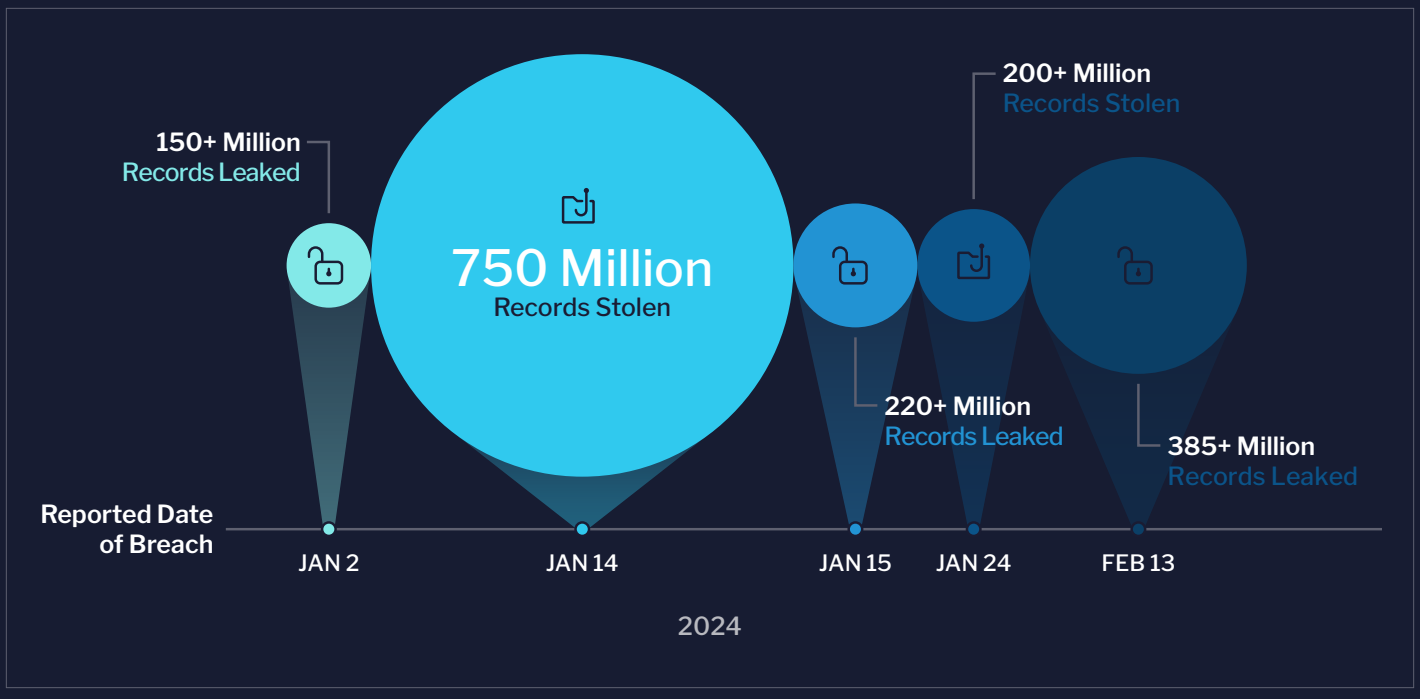
CVSS (v2 | v3)	7.5 | 9.8
Social Risk Score	Low
Location	Remote / Network Access
Exploit	Exploit Public
Ransomware Likelihood	Critical

Source: VulnDB®

Unauthorized Access Is Up In 2024.

As we move forward into 2024, the data breach landscape is seeing a significant spike in stolen or leaked personal data. From January 1 - February 29, 2024, threat actors compromised 1.897 billion personal records and credentials—a 429% increase compared to the same period last year. Five data breach incidents have had an outsized impact:

> **From January 1 - February 29, 2024, threat actors compromised 1.897 billion personal records and credentials—a 429% increase compared to the same period last year.**



The Effect of Ransomware and Unauthorized Access on Key Industries

To gain context into potential risks, organizations need to be aware of how the data breach landscape specifically affects their industry. How are threat actors gaining access into systems? Understanding the answer to this question is critical to forming safeguards and response plans.

	Manufacturing	Healthcare	Government	Financial	Retail	Technology
Number of breaches	754	735	582	530	291	134
Percentage of overall breaches caused by unauthorized access and ransomware	**86.2%**	**65.3%**	**54.1%**	**52.6%**	**54.6%**	**85.8%**
Total data stolen	6M	92M	1.3Bn	375M	78M	3.5Bn

Ransomware and Unauthorized Access Are the Top Two Causes of Data Breaches in 2023.

Together, they are responsible for more than half of all incidents experienced by major sectors. However, for the manufacturing and technology industries, ransomware and unauthorized access accounted for more than 85% of all publicly disclosed breach incidents. This data further illustrates the need for robust threat intelligence and vulnerability management programs that can help reduce risk, prevent losses, and maintain day-to-day operations.

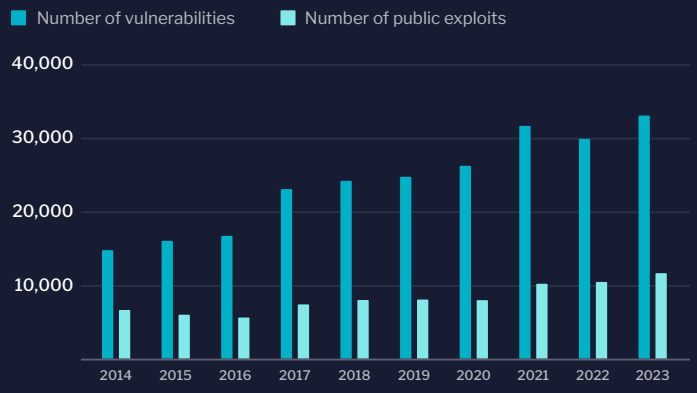
Vulnerabilities

> The data in this section comprises 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, exploit intelligence, social risk, and ransomware likelihood. Data is current to the date of publishing.

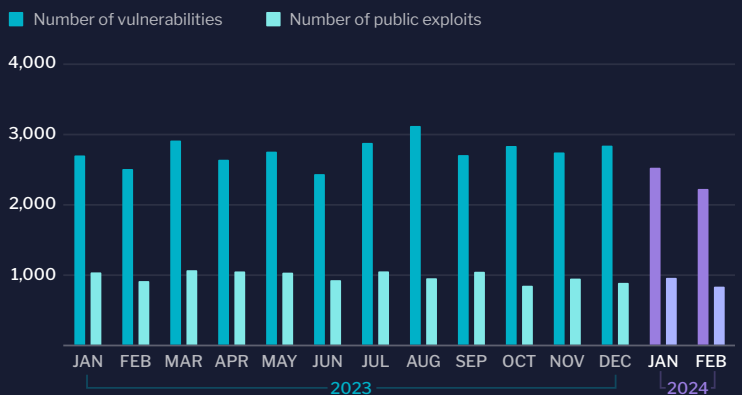
From a threat actor's perspective, unpatched vulnerabilities are opportunities to gain access into an organization. By exploiting them, vulnerabilities allow malicious actors to spread through compromised networks—allowing them to perform a wide variety of actions that may ultimately result in data loss or exposure. However, due to the increasing disclosure of vulnerabilities from an expanded digital ecosystem, organizations may be unaware of vulnerabilities within their networks. One major blind spot occurs when enterprises strictly rely on the Common Vulnerabilities and Exposure (CVE) database, which is missing over 100,000 vulnerabilities—nearly a third of known vulnerability risk.

Flashpoint vulnerability intelligence shows that disclosed vulnerabilities have displayed a consistent upward trend, with 2023 marking a significant peak at 33,137 disclosures. This progressive increase underscores the escalating challenge for cybersecurity defenses, as it is unfeasible for any organization, regardless of maturity, to triage and remediate all of these issues in a timely manner.

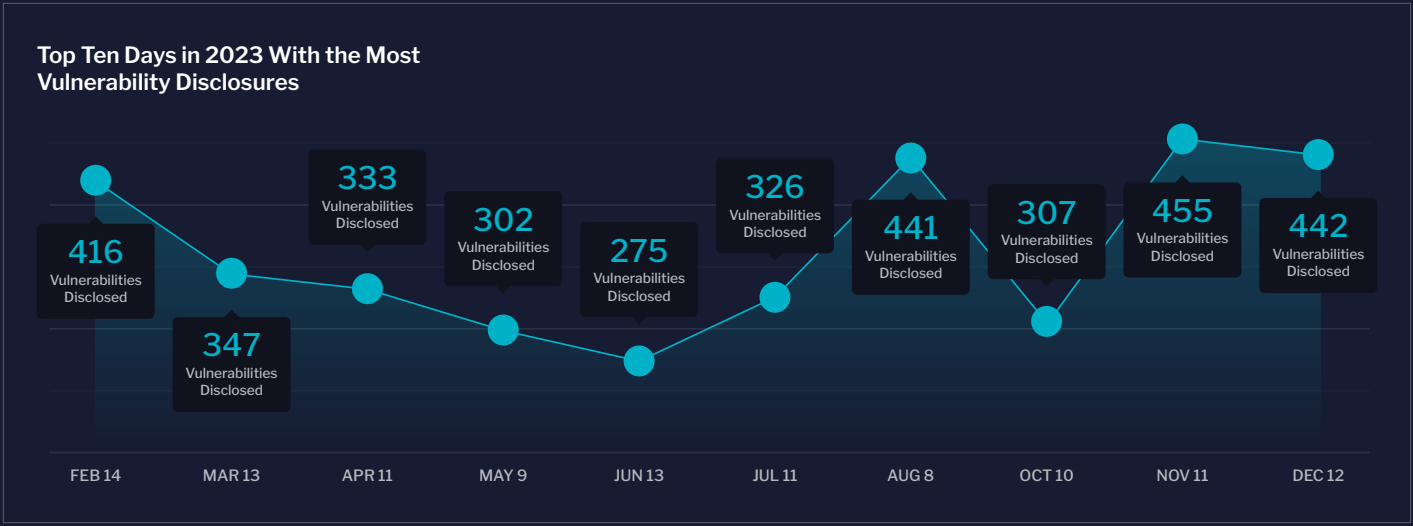
Vulnerability Disclosures Reported by Year, 2014-23



Vulnerability Disclosures Reported by Month, 2023-24



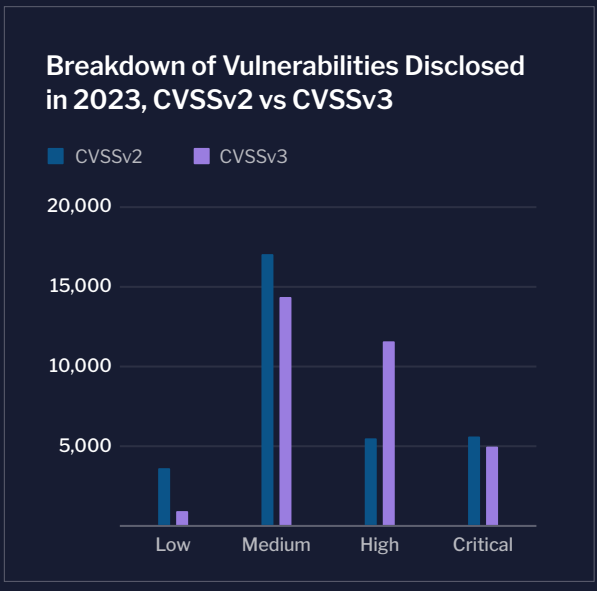
The efficient identification, prioritization, and remediation of vulnerabilities are crucial in preventing or mitigating the impact of breaches and cyber attacks. However, security teams will continue to face challenges as the total number of vulnerabilities increases and new issues are disclosed at a consistent rate. Throughout 2023, the distribution of vulnerabilities per month has seen little fluctuation, with the number of vulnerabilities being disclosed ranging from 2,425 to 3,111. Moving into 2024, Flashpoint is observing similar disclosure totals.



Further examining the rate of vulnerability disclosures, looking at the top 10 days in 2023 with the most reported vulnerabilities, there is a consistent trend: they all take place on the second Tuesday of each month. This is no coincidence as Microsoft's Patch Tuesday has always played a major role in every year's rising totals. As more vendors adopt Microsoft's monthly disclosure schedule, organizations will need a timely and actionable source of vulnerability intelligence to help reduce the need for lengthy manual research.

Severity's effect on prioritization

Flashpoint vulnerability intelligence shows that nearly 52% of all vulnerabilities disclosed in 2023 are scored high to critical (7.0 to 10.0) in severity, according to CVSSv3. For most organizations, vulnerabilities scored between 7.0 to 10.0 are considered to be a major risk, but if more than half of the year's total meet this criteria, which ones should be prioritized? Remediation is a timely process, and if vulnerability management teams are expected to triage all of these issues, it is highly possible that many of these issues will go unpatched.



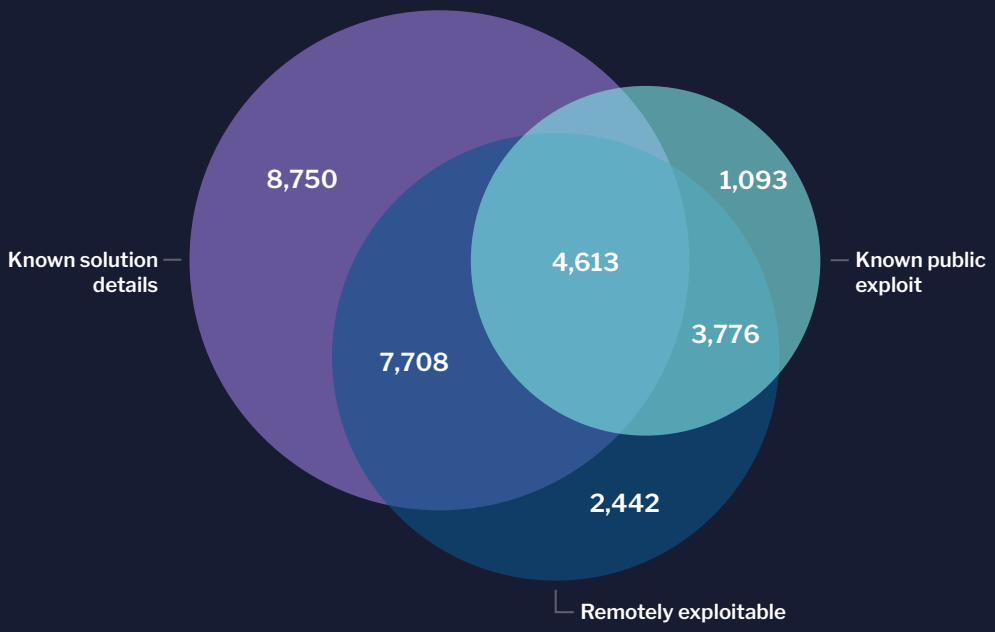
Organizations should also be aware that the National Vulnerability Database (NVD) no longer provides base scores for CVSSv2, and has instead opted to score using CVSSv3. This is significant for three reasons.

- Many organizations still currently choose to rely on CVSSv2 for prioritization.
- Due to differences in scoring methodologies, a vulnerability scored in CVSSv2 can vary greatly from CVSSv3, which can have a major impact on prioritization.
- CVSSv4 was released in November 2023.

Flashpoint has found that categorizing high severity vulnerabilities based on the following criteria can have massive benefits for vulnerability management teams:

- Remotely exploitable
- Known public exploit
- Known solution details

Breakdown of Actionable, High Severity Vulnerabilities, by Availability and Exploitation, Disclosed by 2023

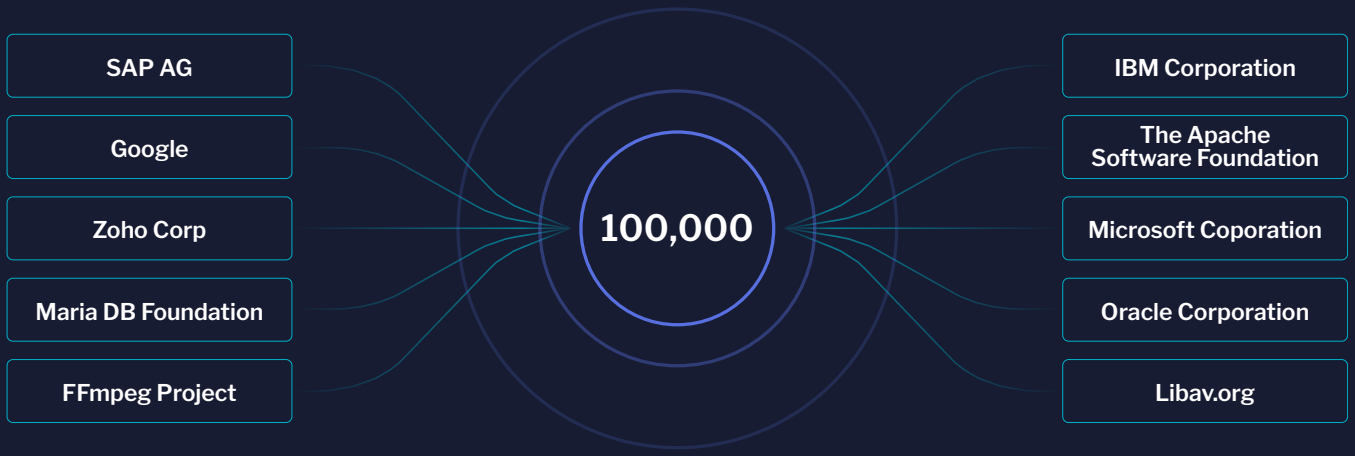


Adopting this model can allow vulnerability management teams to cut their critical workloads by nearly 85%.

By shifting immediate attention to issues that are remotely exploitable that have public exploits, with known solution information, organizations can maximize their resources. Once those issues are fully triaged and taken care of, they can then focus on less severe issues.

Beyond CVE: Uncovering the Hidden Vulnerability Landscape

Organizations strictly relying on CVE are likely unaware of nearly a third of known vulnerability risk. Flashpoint has documented over 100,000 vulnerabilities that CVE has failed to report, many of which affect major vendors such as Google and Microsoft. Flashpoint's non-CVE coverage has also identified a significant number of issues affecting numerous third-party libraries—in addition to zero-day and in-the-wild exploits that are being used by threat actors.



As of February 2024, Flashpoint analysts have cataloged 330 vulnerabilities that were discovered being exploited in the wild, that still do not have a CVE ID. These include vulnerabilities in:

- Adobe Reader
- Apple iOS
- Apple macOS
- Google Android
- Microsoft SQL Server
- Siemens SIMATIC
- Solarwinds Orion Platform

As of February 2024, the following have been exploited in some form of malware, yet do not have a CVE ID:

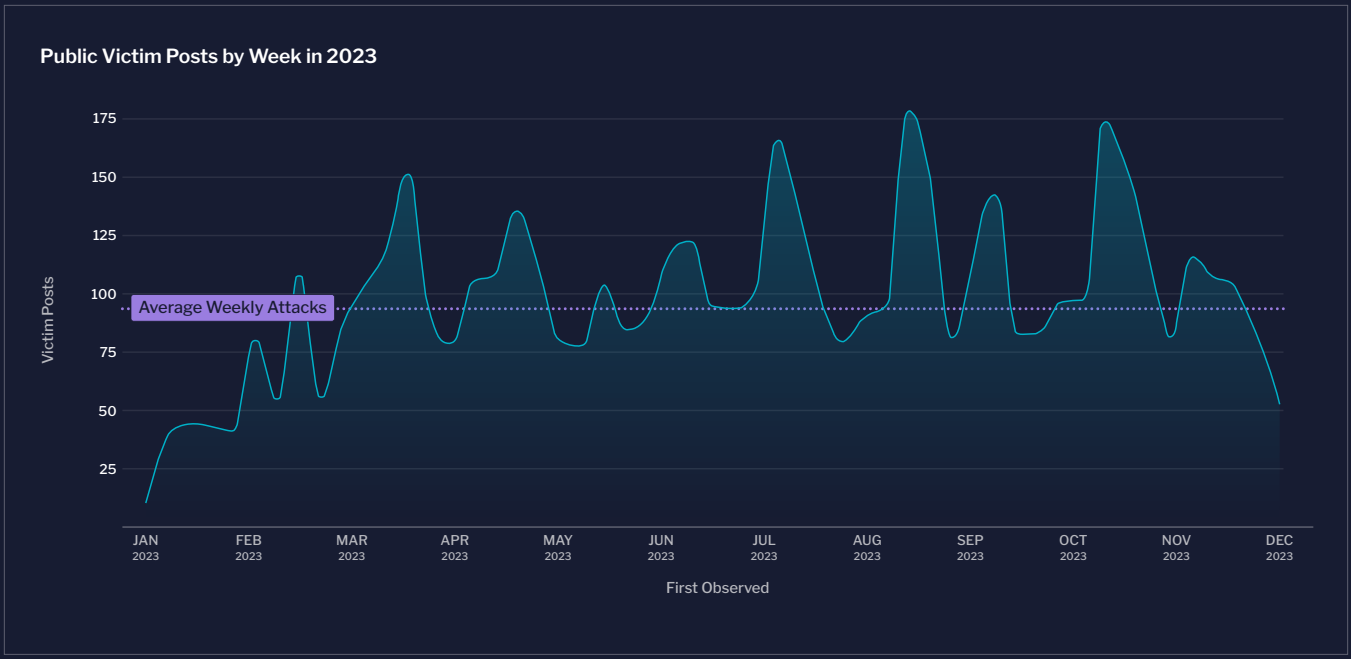
- Apache Hadoop
- Google Authenticator for Android
- PHP

Any vulnerability management team that feels underserved by their current coverage needs visibility into non-CVE issues—especially if they are leveraging legacy or end-of-life software. Having immediate access to actionable data empowers security teams to address issues, sometimes as fast as two weeks compared to CVE.

Ransomware

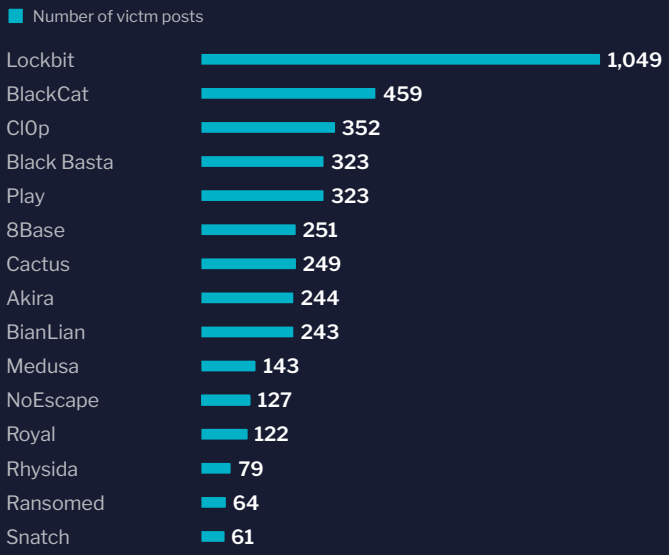
> The data in this section comprises victimized organizations that have been announced on ransomware blogs and leak sites. Data is current to the date of publishing.

Ransomware plays a massive role within the threat intelligence landscape. **Flashpoint identified a significant escalation in ransomware attacks across all sectors in 2023, with the total rising to 5,028 attacks—an 84% YoY increase (2,720).**



LockBit was the most prolific ransomware group of the year, claiming 1,049 victims—**over one fifth of all known ransomware attacks in 2023.** The group has gained notoriety for its sophisticated and ruthless strain of ransomware. Recent analysis of a possible LockBit 4.0 variant noted functionality that includes randomizing the victims' file naming to complicate restoration efforts, a self-delete mechanism that overwrites LockBit's own file contents with null bytes, and the ability to delete victims' shadow copies and backups to inhibit recovery. Coupled with their harsh negotiation practices, including the use of a triple extortion method, victims of LockBit are often left to grapple with difficult decisions.

The Most Active Ransomware Groups of 2023



On February 20, 2024, US authorities, in collaboration with the UK's National Crime Agency and additional international allies, announced the disruption of the LockBit ransomware group as part of a concerted initiative known as "Operation Cronos."

Despite the success of Operation Cronos, the LockBit ransomware collective has persisted. They quickly established a new Dark Web blog, alleging that law enforcement only managed to seize control of a segment of their operations. According to its new site, they have resumed their ransomware operations, though these assertions have not been confirmed as of this publishing. Even with LockBit's continued activities post-disruption, indications are suggesting that Operation Cronos has had a more significant impact on their operations than they are willing to admit.

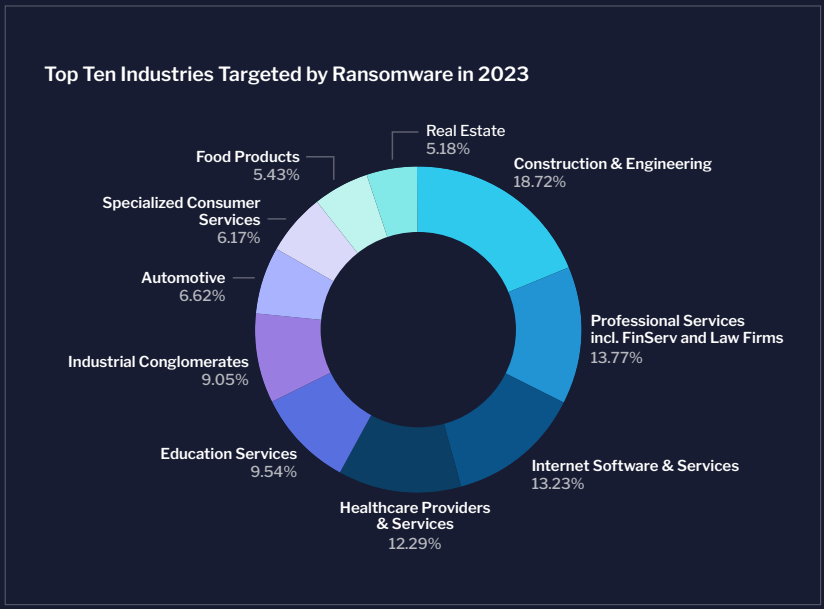
Seven Stages of a Ransomware Attack

	Time to Complete	MITRE ATT&CK ID	Flashpoint Solutions
1 Initial Access During this stage, threat actors employ a range of techniques to gain illegal access.	Continually at risk	**T1046** Network Service Discovery	✓ Account Takeover ✓ Shop Monitoring ✓ Auctions ✓ VulnDB
2 Lateral Movement Threat actors traverse through the network to find additional targets, or to gain control over multiple machines, servers, and devices.	4 - 48 hours	**S0552** AdFind **TA0004** Privilege Escalation **S0357** Impacket	✓ Intel Reports ✓ Technical IOCs ✓ VulnDB
3 Data Exfiltration Threat actors exfiltrate data by leveraging vulnerability exploits, stolen credentials, or abusing trusted applications or services.		**T1071** Application Layer Protocol: Command and Control **T1567** Exfiltration Over Web Service	
4 File Encryption Threat actors encrypt the victim's files and inflict significant damage on their systems.		**S1040** Rclone **T1071** Application Layer Protocol: Command and Control	✓ Malware IOCs
5 Data Extortion Threat actors establish communication with their victims and begin the process of extortion.	2 days - 3 weeks		✓ Threat Readiness and Response Services (TR2)
6 Ransomware Negotiations Organizations consult with legal counsel, law enforcement agencies, and experienced incident response professionals.			
7 Ongoing exposure Continuous risk and potential harm that persists even after the initial attack has been mitigated or resolved.	Continually at risk		✓ Ransomware Monitoring

Nevertheless, as of this publishing, LockBit remains the most prolific ransomware group in 2024, documenting 154 public victim announcements on their leak site within the first two months alone—almost triple the number of the second most active groups (8Base, BlackCat). There's a possibility that the group could recover. However, even if they don't, numerous other cybercriminal factions are poised to take their place, indicating that the fight against cybercrime is expected to persist indefinitely.

So far in 2024, the frequency and severity of ransomware attacks on organizations have increased, with 637 public ransomware attacks in the first two months, up from 518 in the same period of 2023. To mitigate this rising threat, it's crucial for organizations to develop and implement robust prevention and response strategies proactively. Delaying these discussions until after an attack occurs significantly hampers the ability to reduce its impact.

The construction and engineering sector emerged as the most targeted industry by ransomware in 2023, with 416 public incidents. The professional services, internet software and services, and healthcare sectors were also heavily targeted in 2023, highlighting the cross-industry impact of ransomware and the critical need for sector-specific defense strategies. In the first two months of 2024, the construction and engineering sector remained the most targeted with 57 public attacks so far. The manufacturing and healthcare sectors follow behind, each with 49 public attacks in the first two months of 2024. These critical infrastructure sectors share several commonalities that make them lucrative for ransomware groups:



1. They each contain rich amounts of senstive and confidential data that threat actors can hold ransom or exploit for financial gain.
2. Because of both the sensitivity of the data they possess (for sectors like healthcare), and the high costs of operation that make it expensive to halt during ransom negotiations (for sectors like manufacturing and construction and engineering), organizations in these sectors may have a higher willingness to pay the ransom.
3. These organizations often generate higher amounts of revenue, which means ransomers can yield a higher profit per victim compared to other industries.
4. They rely on operational technology that could contain vulnerabilities, providing a window for threat actors to gain access to victims' systems.

Geographically, the **United States** bore the brunt of ransomware attacks, with **2,386 incidents**, reflecting its status as a major target due to its economic significance and digital infrastructure.

Emerging Extortion Tactics...

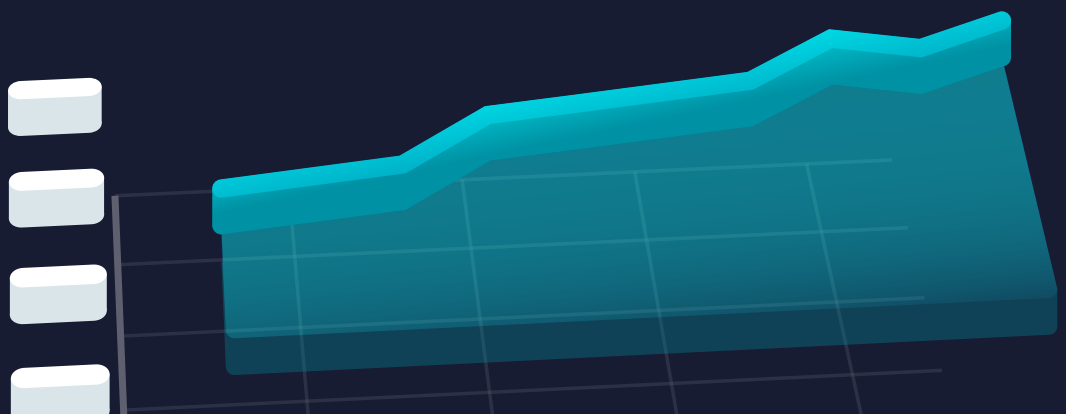
As ransomware groups become more sophisticated, threat actors are becoming increasingly hostile and brazen as well. They are adopting new tactics to add external pressures. This includes doxxing executives, threatening to release embarrassing or sensitive information, or notifying the victim's stakeholders that the company has been breached and is not willing to pay to protect compromised data—all to increase the likelihood of payment. The "extortion economy" represents a growing risk to organizations that parallels many ransomware threats.

To add further complexity, the lines between overt malicious actors and self-proclaimed ethical hackers are increasingly blurred. Consequently, organizations must actively engage in these environments to preemptively counter threats and adapt strategies from ransomware response playbooks to address these lesser-known extortion techniques.

1. **Data Encryption:** The most well-known tactic of using malware to lock or encode a victim's data, demanding payment for its decryption and release.
2. **Data Extortion:** Threats have evolved from just ransom demands to broader threats of public data exposure.
3. **Unethical Vulnerability Disclosures:** While many ethical hackers aim to responsibly disclose vulnerabilities, some blur the lines by tying their discoveries to monetary demands.
4. **Underground Economies' Influence:** Beyond merely trading stolen data, Dark Web marketplaces increase the value of this data, treating it as a secondary market commodity to gain access to victims' systems.
5. **Access Brokers:** The sale of unauthorized system access is on the rise, often serving as the precursor to multifaceted cyber attacks.
6. **Distributed Denial-of-Service (DDoS) Attacks:** Attackers overwhelm a target's online services, causing them to be unavailable. They then demand a ransom to stop the attack.
7. **Physical Threats Related to Cyber Activities:** Extortionists sometimes combine cyber threats with physical threats, suggesting harm might come to a victim or their loved ones unless demands related to cyber activities are met.

...And How to Fight Back

1. **Implement Robust Encryption and Backup Procedures:** To counter data encryption tactics, organizations should ensure that all sensitive data is encrypted and regularly backed up to secure, off-site locations. This minimizes the impact of ransomware attacks by allowing organizations to restore encrypted data without paying a ransom.
2. **Advanced Threat Detection and Response:** Employ advanced threat detection systems that utilize machine learning and AI to identify unusual data access or transfer patterns, indicative of data extortion attempts. Establish a swift incident response plan to contain and mitigate threats before they escalate.
3. **Vulnerability Management Program:** Develop a comprehensive vulnerability management program that includes regular security assessments, penetration testing, and the prompt patching of software vulnerabilities. This reduces the risk of unethical vulnerability disclosures and ensures that potential security gaps are addressed before they can be exploited.
4. **Monitor and Analyze Dark Web Activities:** Engage in continuous monitoring of Dark Web forums and marketplaces to understand the latest trends in underground economies. Utilize this intelligence to strengthen your security posture against emerging threats and to be aware of any mention of your organization's data on these platforms.
5. **Zero Trust Architecture:** Adopt a zero-trust security model that verifies every user and device trying to access your network, regardless of their location. This approach minimizes the risk posed by access brokers by ensuring that access is strictly controlled and monitored.
6. **Protect Against DDoS Attacks.** Implement DDoS protection solutions that can detect and mitigate large-scale DDoS attacks. These services can help maintain the availability of online services during an attack, reducing the attackers' leverage for ransom demands.
7. **Employee Education and Physical Security Measures:** Educate employees about the risks of cyber threats and the importance of physical security. This includes training on recognizing phishing attempts, securing personal and company devices, and reporting any suspicious activities. Enhance physical security measures to protect against threats that merge cyber and physical elements.



Commentary

By Andrew Borene
Executive Director of Global Security

Beyond Bytes and Bullets: Shaping the Future of Allied Threat Intelligence

> Strategies for integrating OSINT capabilities with cyber, physical, and geopolitical intelligence to proactively fight global security threats.

The need for a holistic, integrated approach to intelligence and security has never been more acute. The challenges ahead are not only defending against attacks and increasing resilience; they lie in understanding and shaping the future of intelligence in a world where the digital and physical realms are inexorably linked.

The importance of high-fidelity, high-reliability data in this context cannot be overstated, as it forms the very backbone of an intelligence enterprise that enables various decision makers to distill actionable insights from vast streams of information. Governments must make informed decisions to safeguard national interests and those of their allies. Private enterprises and corporate boards need insights to protect themselves from a growing field of e-crime actors and state-backed threats. Universities and research institutions must protect intellectual property. Global media entities need means to help validate trusted information and to debunk false narratives that may be amplified with deepakes and generative AI.

Navigating this new era demands not just vigilance but innovation, as we chart a course through the intertwined fog of digital and physical conflicts to safeguard our collective future.

Converging Threats Across Conflicts and Competitive Domains

Ongoing war between Russia and Ukraine, the Israel-Hamas War in Gaza, expanding proxy violence in the Middle East, rising tensions in the Taiwan Strait, and new forms of large scale data theft and extortion all underscore a near-term future fraught with increasingly complex geopolitical and cyber challenges. This emerging landscape demands a profound reevaluation of how nations, non-state actors, and intelligence communities navigate the intelligence needed for warfare, peacekeeping, and protecting prosperity in our interconnected world.

> **This emerging landscape demands a profound reevaluation of how nations, non-state actors, and intelligence communities navigate the intelligence needed for warfare, peacekeeping, and protecting prosperity in our interconnected world.**

Through lenses of what is generally termed Great Power Competition by allies, and Hybrid Warfare or Unrestricted Warfare by adversaries, our understanding of global security is in a pivotal phase of transformation. This digital transformation and the entanglement of commercial, government, and nonstate actors across an observed fragmentation of the cyber domain calls security professionals toward a unified intelligence framework to seamlessly integrate cyber and physical threat intelligence in real time and at scale.

Developing Professionally-Sourced Intelligence (Pro-SINT) within OSINT

As we confront these multifaceted threats, we may need to embrace a subtle distinction between Open-Source Intelligence (OSINT) and a subset that I call Professionally-Sourced Intelligence (Pro-SINT). What I unofficially refer to as "Pro-SINT" is distinct from a growing set of crowdsourced, hobbyist, and other unfiltered OSINT efforts using publicly-available information. Pro-SINT leverages more proprietary and commercially-available information and is marked by professional standards, oversight, privacy compliance, ability to collaborate with law enforcement entities, and most importantly a deep commitment to a set of international ethics that aligns with those of allied governments, regulated industries, and a scientific standard for verification and auditability.

The type of Professional OSINTer I've described, may reside in a government, a company, an NGO, or a university, but they all share a focus on deep-web data, Dark Web exploration, cyber-physical convergence, and sophisticated analysis, enriching traditional human observational intelligence methods and analytical judgment with the technologies required to provide nuanced insights at scale among the complex interplay of cyber and physical threats in real time.

Professional OSINT is not only about enhancing defensive measures or reducing mean times to resolution of vulnerabilities, but about preemptively understanding and countering the strategic moves of adversaries, frequently seen in the chatter of encrypted communications preceding abrupt attacks or indicating persistent intrusion. Moreover, the integration of well-trained and auditable artificial intelligence and machine learning technologies into intelligence operations for commercially-available information offers unprecedented capabilities in detecting deepfakes and other sophisticated cyber threats, further enhancing our ability to anticipate and mitigate potential escalations in both cyber and kinetic domains, bolstering security postures for individual organizations, governments, and alliances.

A professional ethos is also essential to navigate the complexities introduced by decentralized platforms and Dark Web tools, which, while enabling resilience against censorship and protection from hostile surveillance in many parts of the world, also can pose challenges in distinguishing credible intelligence from misinformation in open societies.

Challenges in Decentralized Communications and the Dark Web

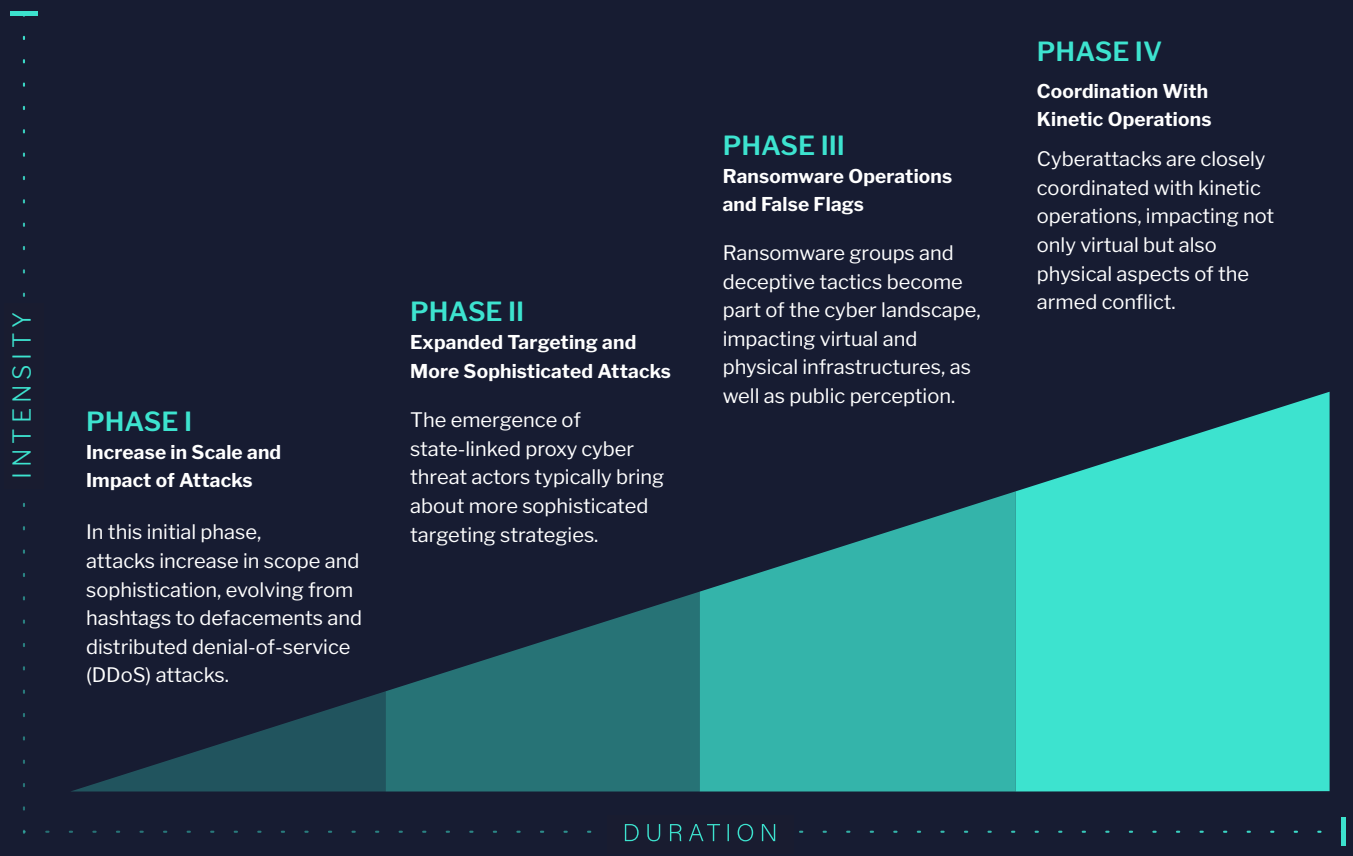
A unique aspect of a hybrid digital evolution has been the role of decentralized communication platforms and the expanding use of Dark Web communications by both threat actors and friendly users with legitimate needs for protection and undetected attribution.

These platforms have transcended their initial purposes to become digital command centers and sanctuaries for many unfiltered narratives. Their observed impact in facilitating real-time, unedited information flows during the conflicts in Ukraine and Gaza has been profound, underscoring the blurring lines between cyber, information, and kinetic warfare and highlighting the strategic significance of data in modern warfare.

Cross-platform, encrypted messaging, and Dark Web service platforms have also proved useful sources for key insights into the strategic, operational, and tactical context of challenges including proxy violence in the Middle East, tensions in the Taiwan Strait, hostile espionage activities against allies, in addition to the evolving tactics, techniques, and procedures (TTPs) used by cyber criminals for extortion or fraud.

Cyber Escalation in Modern Conflict: Exploring Four Possible Phases of the Digital Battlefield

In the midst of the Israel-Hamas War, a digital battlefield emerged, echoing patterns seen in previous conflicts like the Russia-Ukraine War.



Strengthening collaboration among allies becomes crucial as we collectively counteract the threats posed by adversaries and protect shared economic interests and democratic values in cyberspace. However, achieving such unity in intelligence and security efforts presents its own set of challenges. Divergent political interests, varying levels of technological sophistication, and concerns over sovereignty and privacy can hinder the formation of a cohesive global threat picture for allies across public sector and private sector pillars. Recognizing these differences and ensuring an ability to appropriately tailor data collection and use for each individual client is paramount as we strive for a collaborative, multidisciplinary approach to professional security intelligence.

Toward a Unified Approach to Global Security Intelligence

The interwoven nature of ongoing wars, global conflicts, and the critical role of digital platforms in these dynamics underscore the imperative for comprehensive and forward-looking intelligence collaboration strategies. These strategies must not only address the immediate challenges posed by the current geopolitical and cyber threats but also anticipate the evolving nature of warfare, espionage, and transnational criminal enterprise.

The insights gained by professional OSINTers are indispensable in this endeavor, enabling responses that are as dynamic and multifaceted as the threats faced by our clients.

In navigating this complex landscape, a collaborative, multidisciplinary approach to security becomes paramount. By fostering unity among commercial enterprises, governmental agencies, and international partners, we can develop robust, adaptable security strategies that transcend traditional paradigms. This unified approach, leveraging the latest technological advancements and prioritizing ethical, legal, and political frameworks, is our best defense against the insidious threats that seek to undermine our institutions, economies, and democracies.

Embracing the interconnected world as it is, not as we wish it to be, is a key first step. It requires understanding the criticality of machine speed and scale in the digital domain, while always remembering that humans are more important than hardware. Developing high-fidelity data sourcing and high-trust professional networks will help us protect the foundations of our global society alongside our allies and in defense of our collective security. Our shared prosperity demands it.

Security and intelligence professionals all face a new hybrid era. The global threat landscape is transforming and scaling—fortunately, so are we.

Case Study

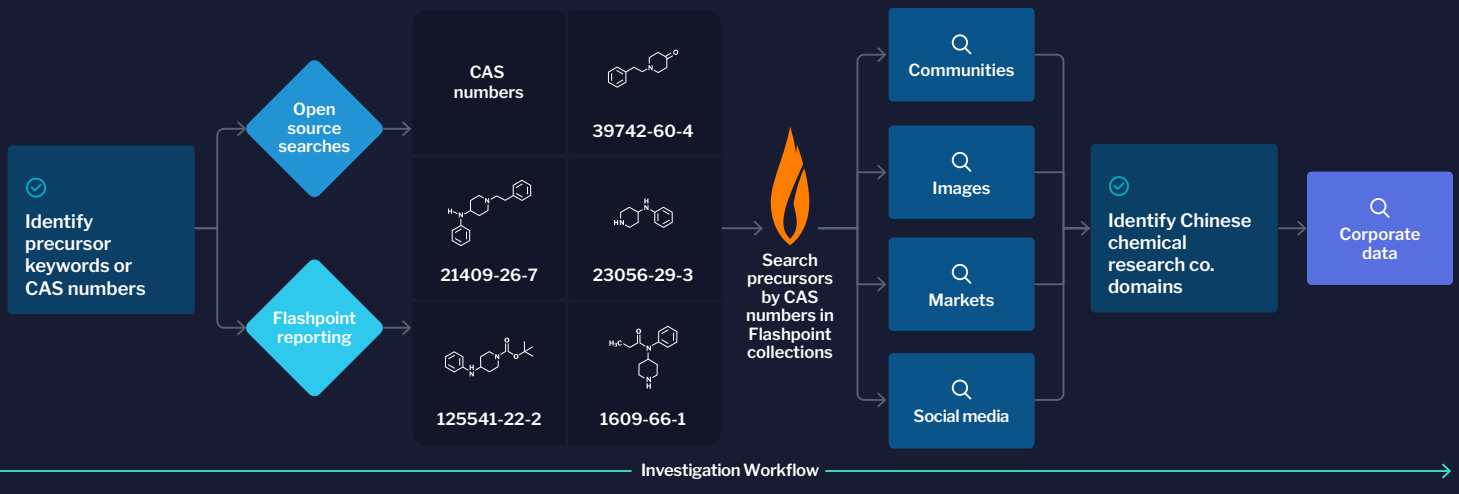
Leveraging Threat Intelligence in Public Safety Missions: Investigating Sales of Fentanyl Precursors

In the complex global security challenge posed by the trafficking of synthetic opioids like fentanyl, the importance of open-source intelligence (OSINT) in public safety missions cannot be overstated. Flashpoint National Security Solutions (FNSS) stands at the forefront of addressing these challenges by providing tailored intelligence that empowers government and public sector entities to conduct effective investigations.

This case study explores how Flashpoint's advanced OSINT capabilities have empowered government and public sector agencies to unravel the sophisticated networks behind the sales of fentanyl precursors (chemicals used to manufacture the synthetic opioid) on digital platforms. By dissecting the digital footprint of the fentanyl precursor trade, Flashpoint provides the critical tools and intelligence needed for public safety and national security teams to anticipate, mitigate, and disrupt these illicit activities effectively.

The Challenge

The trafficking of synthetic opioids has reached alarming levels, with threat actors employing increasingly sophisticated methods to evade detection. In particular, the sale of fentanyl precursors—often advertised openly yet obscured through scientific nomenclature and digital platforms—poses significant hurdles for law enforcement and public safety agencies. To effectively understand, counteract, and dismantle these illicit networks, adopting an innovative investigative strategy—integrating both proprietary technology and open-source intelligence—is crucial, as illustrated in the accompanying chart.



The Solution

In response to the growing threat, Flashpoint analysts embarked on an investigation targeting the sale of fentanyl precursors, particularly those originating from Chinese chemical manufacturing companies. Utilizing a multi-faceted approach, the team leveraged:

- The Flashpoint intelligence platform for insights into synthetic opioid trafficking trends on the Deep and Dark Web (DDW) and social media
- Optical character recognition (OCR) to sift through digital images for hidden clues
- Open-source intelligence for additional context on trafficked substances
- Advanced data mining techniques to sift through vast datasets, including social media chatter, market advertisements, and digital communications
- Echosec, a component of Flashpoint's Physical Security Intelligence suite, to expand the investigation into a broader array of social media platforms
- Corporate data sources to investigate the ownership and operational structures of companies involved in the precursor trade

The Results

The investigation unveiled a complex web of Chinese chemical companies involved in the manufacture and distribution of fentanyl precursors. Despite China's regulatory efforts, these entities have found ways to cater to the US market, often using mislabeling tactics and intermediaries to skirt US laws. Flashpoint's analysis revealed:

- Indictments against several companies and individuals for their role in the fentanyl precursor trade
- Advertisement strategies employed by these companies on various digital platforms, including social media and dedicated websites
- The use of advanced money-laundering techniques and encrypted communication platforms like WeChat to facilitate operations

Closing Thoughts

Taken together, the data and analysis in the Flashpoint 2024 Global Threat Intelligence Report depict a landscape of threats that continue to grow in volume and complexity, from ransomware attacks and data breaches to vulnerability exploitation and geopolitical conflict. Three themes rise above as takeaways to navigate this challenging environment:

Anticipate and adapt to the convergence of cyber, physical, and geopolitical threats.

As attacks increasingly target where geopolitical and commercial interests intersect—then take hybrid forms—organizations must not get caught in their traditional silos of functions and geographies. New levels of collaboration are required both within and outside of organizations, from the sharing of data and analysis to defining the protocols to act decisively on it.

Raise the bar on the actionability of data.

It is impractical for security teams to grow at the same rate as the attacks that we've reported on in this report. More data isn't the solution to staying a step ahead; it's about the quality, actionability, and tailoring of data to an organization's specific needs.

Harness the power of technology and artificial intelligence (AI) in service of human intelligence, not in place of it.

AI is already delivering powerful capabilities to help organizations distill overwhelming amounts of information about potential threats. Amid the hype, however, some have lost sight of the central role of human intelligence in marshaling this power. The adversaries documented in this report will be less effective when matched with the combination of human expertise and technology on the other side.

By offering these threat data sets, insights and recommendations, this report has aimed to illuminate a path forward, empowering readers not only to confront the challenges of today but also to anticipate the risks of tomorrow.

Flashpoint Solutions and Services

Intelligence Platform

Flashpoint Ignite

Flashpoint Ignite 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.

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 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)

Boost your situational awareness with Flashpoint Physical Security Intelligence (PSI), which provides real-time, geo-enriched data and expert intelligence insights. In an era of expanding digital communications, PSI helps security and intelligence teams cut through the noise by offering access to a wide range of global open sources, including social media, messaging apps, defense forums, and underground networks. This enables the effective identification and analysis of significant events, geopolitical dynamics, and executive threats, transforming overwhelming volumes of data into actionable intelligence.

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.

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.

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.

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.

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.

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.

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.

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.

About Flashpoint

Flashpoint is the pioneering leader in threat data and intelligence. We empower commercial enterprises and government agencies 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.

FLASHPOINT

The Best Data for the Best Intelligence

Join the conversation:
LinkedIn | X | Threat Intel Blog

See Flashpoint Ignite in action:
https://flashpoint.io/demo/

Copyright © 2024 Flashpoint. All rights reserved.