FLASHPOINT

State of Cyber Threat Intelligence: 2023

A deep dive into the perpetual cycles of cybercrime—and how to fight back

Table of Contents

Introduction

THREATS ARE CONVERGING, CYCLICAL

A growing body of evidence, outlined in this report, demonstrates just how extensively cyber threats are overlapping, intersecting, and relating. Furthermore, we examine why these threats—from the online spaces in which cybercriminals operate to the tactics, techniques, and procedures (TTPs) they use to execute their attacks—are cyclical and what that means from an intelligence and security perspective.

These two themes—convergence and the cyclical nature of cybercrime—are front and center in this report, Flashpoint's inaugural "State of Cyber Threat Intelligence." In the following pages, we examine the factors that feed these unending cycles, their evolving interconnectedness, the real impact they have on the effectiveness of cyberattacks, and the targets they affect.

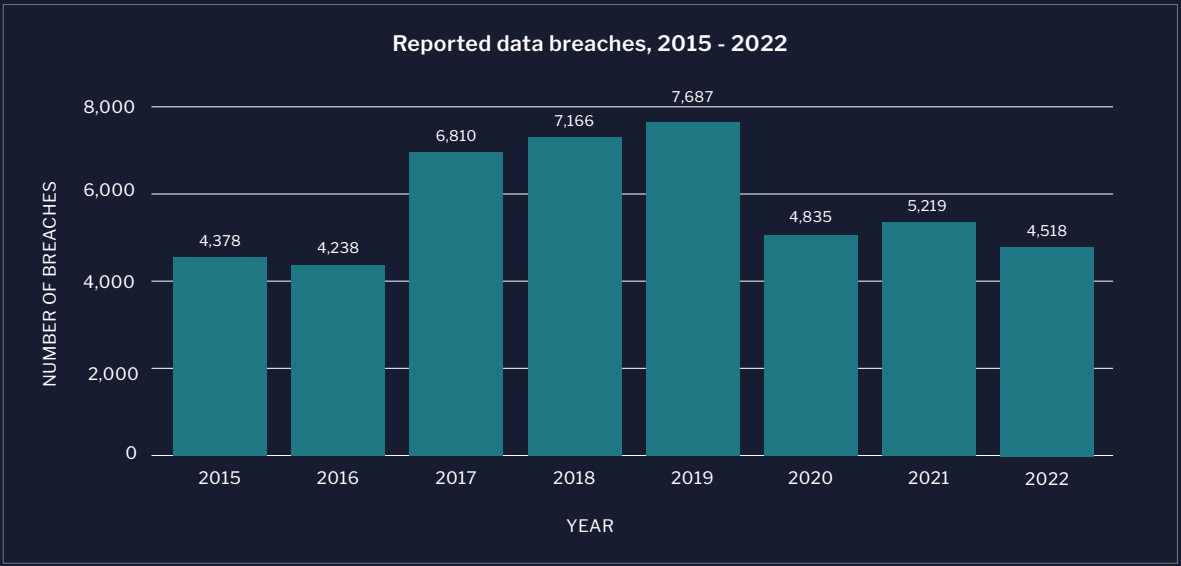
Consider the cycle of illicit communities, which is marked by the motions of takedowns (Raid Forums), resurrections (AlphaBay), and new venues (Libre) which may then be taken down. Call it a game of cat-and-mouse, of chicken-and-egg. To aim to understand where this cycle begins and ends, however, is to miss the point. Like other cycles in the threat landscape, the cycle of illicit markets should be viewed as a converged, self-serving mechanism whose continuity is fueled by competition, evolving technology, communication preferences, law enforcement partnerships, know-how and other intangibles, and much more. And, like most modern organizations, threat actors employ multiple teams or individuals, with varying motivations and targets, as well as various tools to streamline the tasks that contribute to their main goal—the compromise of a victim's systems.

Our research and experience has demonstrated time and again that security practitioners seeking to better understand and protect their enterprises should think—and act—accordingly. Organizations cannot afford to view, prepare for, mitigate, and prevent these threats in silos, as though one threat (and the cycle it exists in) is separate from another. Multiple disjointed feeds and solutions make identifying, prioritizing, and mitigating persistent and evolving threats difficult and costly. Since threat vectors are converging, CISOs should aim to unify and rally their security and intelligence teams behind a single source of truth that integrates workflows between their Cyber Threat Intelligence (CTI), Fraud, Vulnerability Management (VM), and IT Security teams, as well as other functions.

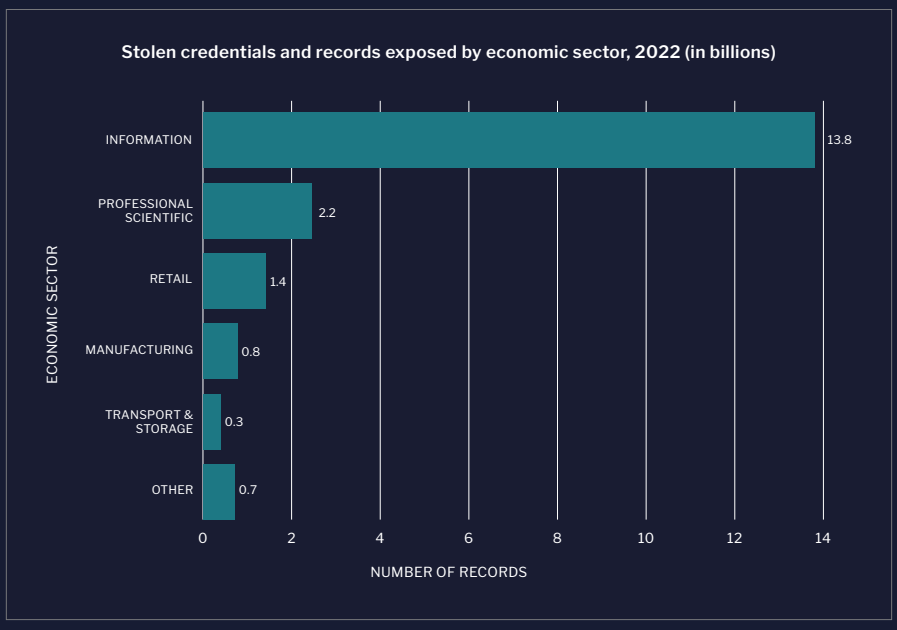
It is through this lens that we examine the trends, data, analysis, strategies, and insights that will impact the ways in which security and intelligence teams tackle challenges in 2023.

The impact of converged threats

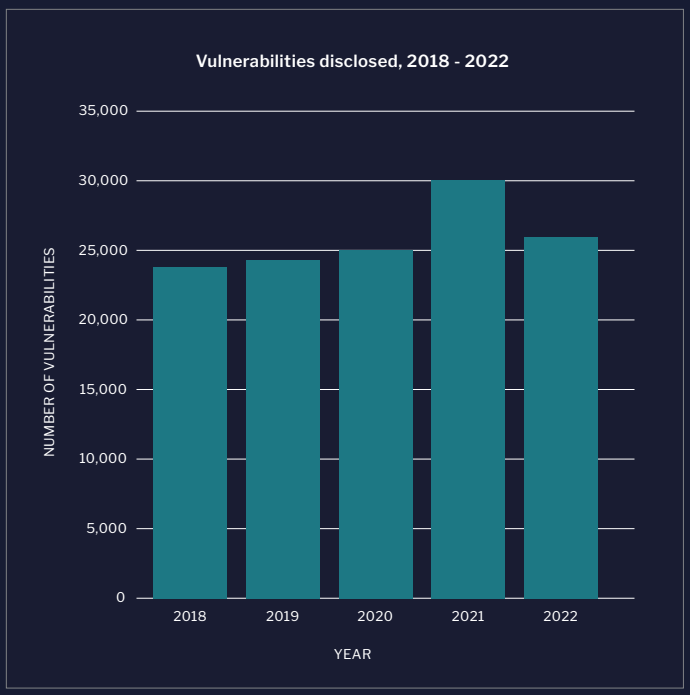
BY THE NUMBERS



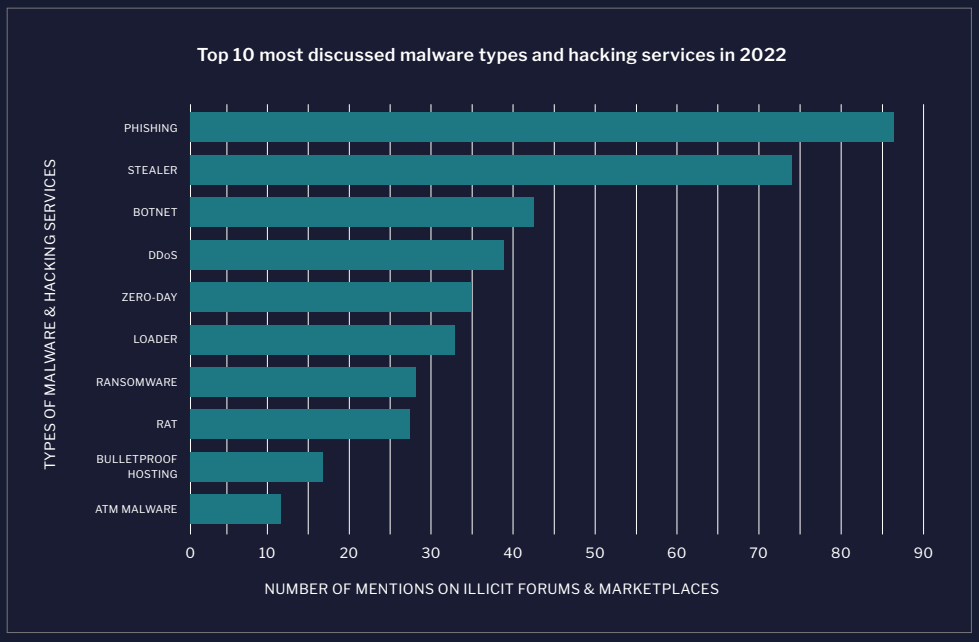
Last year, 4,518 data breaches were reported, according to Flashpoint's collections. Threat actors exposed or stole 22.62 billion credentials and personal records, ranging from account and financial information to emails and Social Security numbers.



61 percent (13.8 billion) of 2022's stolen credentials and personal records came from the information sector, which often processes or houses data for a wide array of industries and consumers—such as software publishers, telecommunications companies, data processing, and web hosting services.



Meanwhile, 26,900 vulnerabilities were reported in 2022, of which approximately 55 percent (14,871) are remotely exploitable. This brings the total number of known vulnerabilities to 306,000—with the Common Vulnerabilities and Exposures (CVE) and the National Vulnerability Database (NVD) failing to report 97,000.



Threat actors take advantage of both vulnerabilities and stolen credentials. Exposed records are used to inform phishing campaigns, and stolen credentials are leveraged in credential stuffing, brute-forcing, and other cyberattacks.

Adversaries use vulnerabilities to power information-stealing malware. Or they weaponize specific vulnerabilities, hoping to exploit them before Vulnerability Management teams can patch them.

The proliferation of illegally obtained data gives threat actors ample opportunities to circumvent organizational security measures and controls—empowering ransomware groups like LockBit to hold data for ransom, or sell or expose it on illicit markets. Regardless of what they do with the data, ransomers publicly post victim identities on their own websites to showcase their illicit resumes. The efforts of threat actors—fed by human error, vulnerabilities, and the past victories of their malicious peers—perpetuates an endless cycle.

Our data and intelligence

All the data and intelligence in this report is derived from Flashpoint's collections and intelligence team. Flashpoint's collections utilize a mix of technologies that include AI/ML, and NLP models that are internally trained to surface relevant information for each customer.

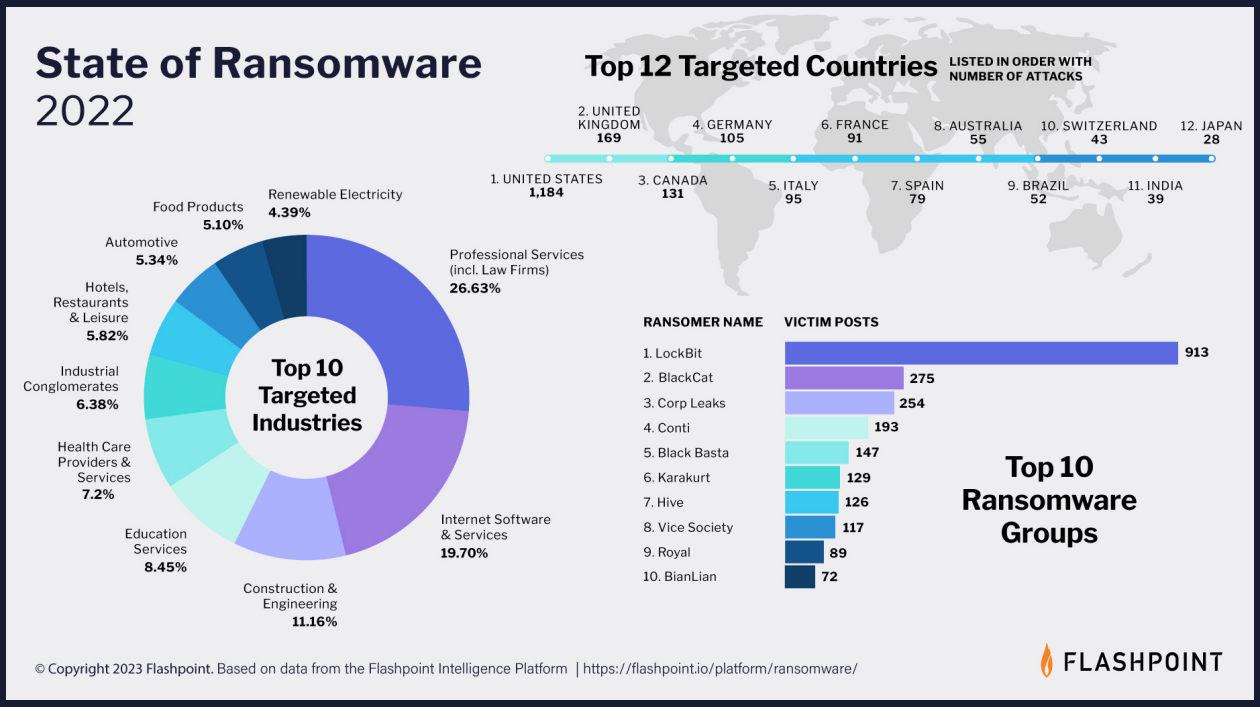
The Flashpoint intelligence team comprises over 100 experts who speak 35 languages and counting. Flashpoint uses highly efficient translation models for our datasets, which span more than 25 languages, providing a wider range of search results from foreign language sources within Flashpoint collections.

At the end of 2022, Flashpoint's data collections included the following:

- 575M illicit forum posts
- 3.6B chat services messages
- 350M media assets
- 306K vulnerabilities (97,000 of which are not available in NVD)
- 1.1M threat actor mentions of CVEs
- 200+ of the most prevalent malware families and associated IOCs
- 39B compromised credentials
- 85B unique email/password credentials
- 2B+ stolen credit cards

Ransomware as a microcosm

Regardless of industry or location, ransomware is a scourge. Last year, Flashpoint recorded 3,164 reported ransomware victims—a 7 percent increase from 2021. And looking into 2023, our collections indicate that the number of reported ransomware victims is on track to exceed 2022.

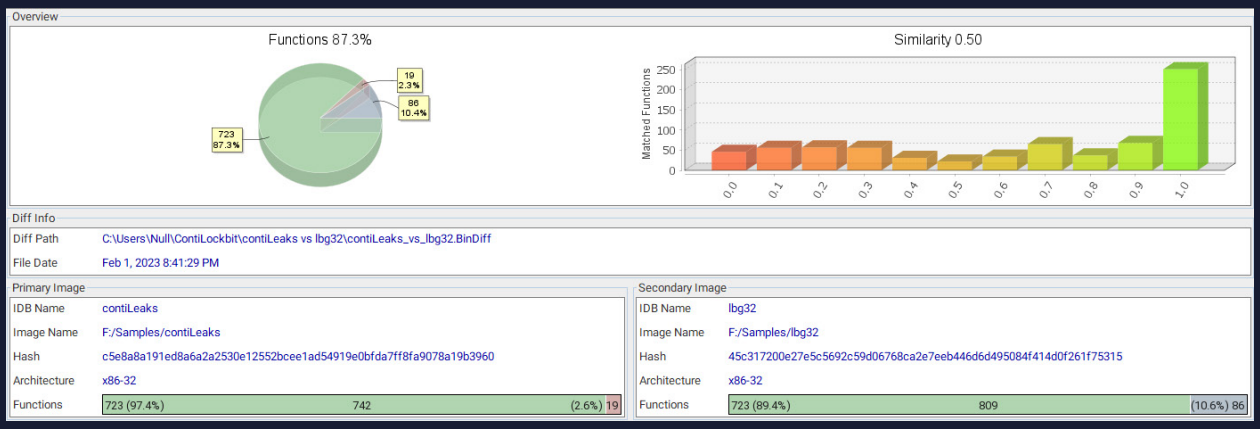


Albeit at the expense of impacted organizations, the activities of ransomware groups, such as Conti and LockBit, can give business leaders and their security teams a panoramic view into the overall state of Cyber Threat Intelligence (CTI), serving as a microcosm for the convergence of threat actors and, by extension, threat vectors.

Unlike most modern organizational security teams, threat actors do not operate in silos, and instead pool resources while learning from one another. Flashpoint is finding that adept threat actors and ransomware gangs increasingly share code, in addition to tactics, tools, and procedures—largely thanks to the proliferation of illicit markets. This can be witnessed with the ransomware group Conti: Despite its exit in May, Flashpoint has noted significant overlaps between indicators associated with Conti and with other groups such as Diavol, Karakurt, and Royal.

LockBit was the most prolific ransomware group in 2022, being responsible for nearly 29 percent of reported ransomware attacks.

Furthermore, Flashpoint analysts have observed code similarities between Conti and the prominent data extortion group LockBit. Earlier this year, Flashpoint discovered that a new LockBit ransomware variant, dubbed LockBit Green, shares large amounts of code with Conti ransomware.

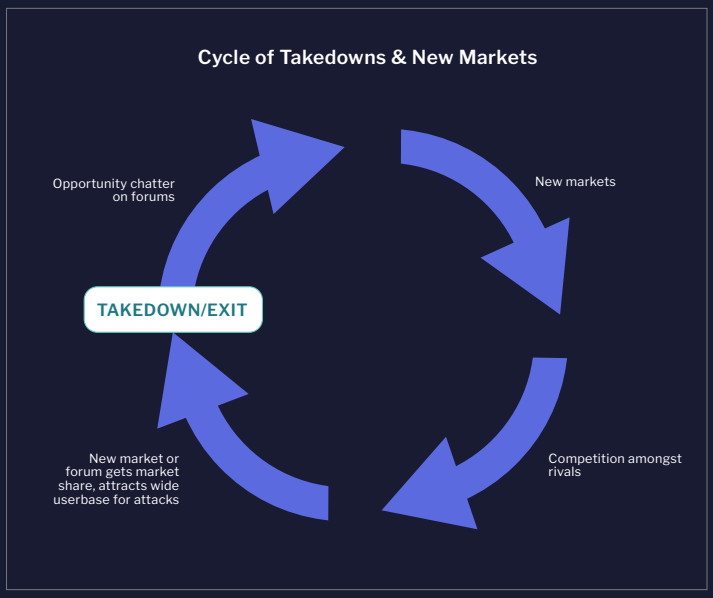


The binary difference results show an 87.3 percent code similarity between the LockBit Green and Conti samples. (Source: Flashpoint)

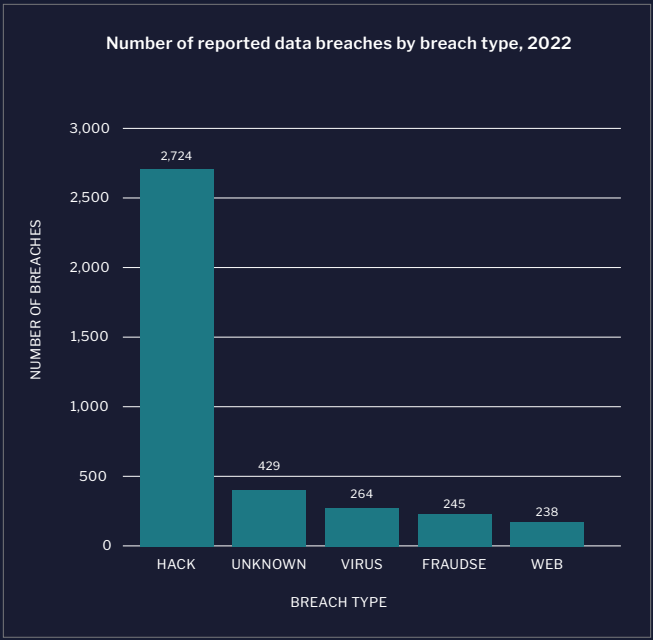
The resiliency of threat actors and illicit markets

While not all cyber threat actors are intent on cyber extortion, there is a perpetual cycle that facilitates cybersecurity events, which is supported by the resiliency and proliferation of illicit communities and markets. Understanding the factors that keep these cycles in place, and evolving, is vital to understanding not only how and where cybercriminals work, think, and act but also how to stay one step ahead of them.

Let's examine the cycle of illicit markets, for instance. In 2022 alone, Flashpoint observed 190 significant new illicit markets emerge. Meanwhile, there were several notable takedowns of long-running forums and markets—SSNDOB, Raid Forums, and Hydra among them—while new markets quickly emerged to take their place, including Raid's successor Breach Forums and Hydra's successor Kraken.



Source: Flashpoint



Unauthorized access to systems and services accounted for 60 percent of all reported data breaches.

We have observed this cycle of Dark Web markets before, from Silk Road to Silk Road II to Silk Road Reloaded; there are always competitors, copycats, and scammers looking to capitalize on displaced Dark Web users. Enterprising administrators have used name recognition and familiar web design to capture Dark Web customers. Some of these markets are scams meant to entrap uninformed and eager users. Others, such as Empire Market, have short-lived success followed by an exit. And when all hope is lost, a market like AlphaBay returns with its former administrator.

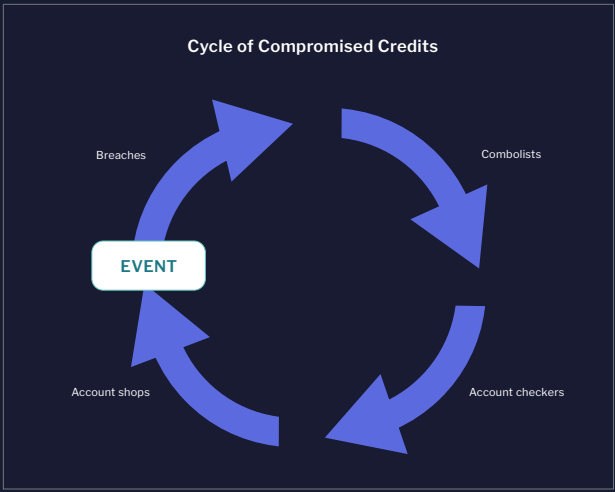
So what fuels this cycle?

For one, there has been a marked movement toward decentralized open-source communication channels—meaning encrypted and unencrypted messaging platforms where illicit activity is based around individual channels to organize, share information, and establish trust between threat actors. Decentralized open-source channels like Telegram, which have become an increasingly popular medium for cyber and physical threat actors, have eroded long-standing barriers to entry to the Deep and Dark Web.

While there is chaos at the genesis of a takedown or market exit, platforms like Telegram act as a rallying point for affected communities. Once threat actors realize that a forum or market is no more, they identify the void created in the market, quickly create an alternative, and then advertise it using Telegram or other forums and communication channels. The lack of oversight and censorship of open-source channels, as well as their widespread use, has made it easier for newcomers to find illicit communities, and for veterans to learn new tricks or expand their sphere of influence. As a result, illicit communities and markets are thriving.

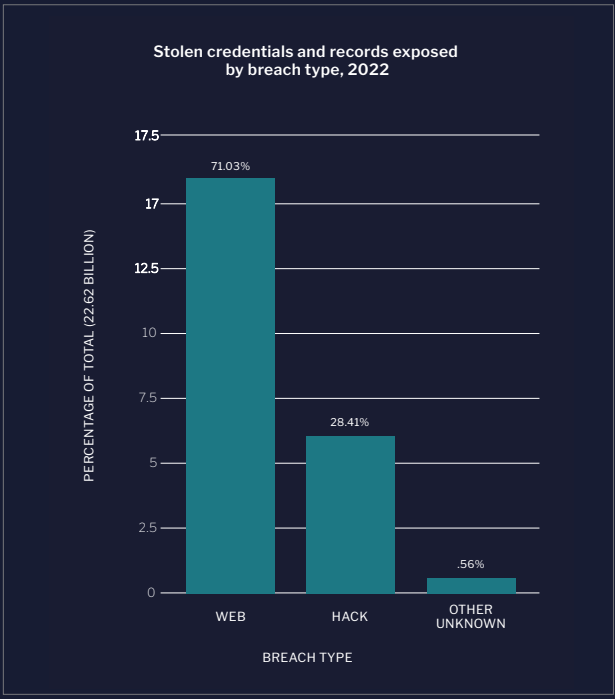
Flashpoint saw this cycle with the creation of Breach Forums, which was formed as a refuge for former Raid Forums users. Our analysts observed that from March 2022 to November 2022, the site's membership expanded from 1,500 users to over 192,000. Similarly, Hydra's takedown last April led to the creation of several markets. Competition—another key aspect in the cycle of takedowns—led to the creation of RuTor, Mega, Nova, OMG!, and Solaris, with each of them vying for Hydra's previous market share.

How illicit markets are fed



Source: Flashpoint

Misconfigurations only accounted for 5 percent of all reported breaches, but they were responsible for leaking more than 71 percent of all personal records.



Illicit markets directly impact data breaches and cyberattacks. Fraudsters, initial access brokers, ransomware groups, and Advanced Persistent Threat (APT) groups alike turn to these markets, shops, and forums to trade in stolen credentials and personal records, which are leveraged in a variety of illicit activities—from DDoS attacks to ransomware.

Here's how cyber threat actors get their supply of stolen data.

1 AUTOMATED SCANNING FOR MISCONFIGURATIONS

Threat actors have quick access to tools that allow them to search the internet for misconfigured databases and services. And although these types of web-based breaches are easily preventable, the number of records lost from misconfigurations skyrocketed by 93 percent in the latter half of 2022—climbing from 1.46 billion to 16 billion.

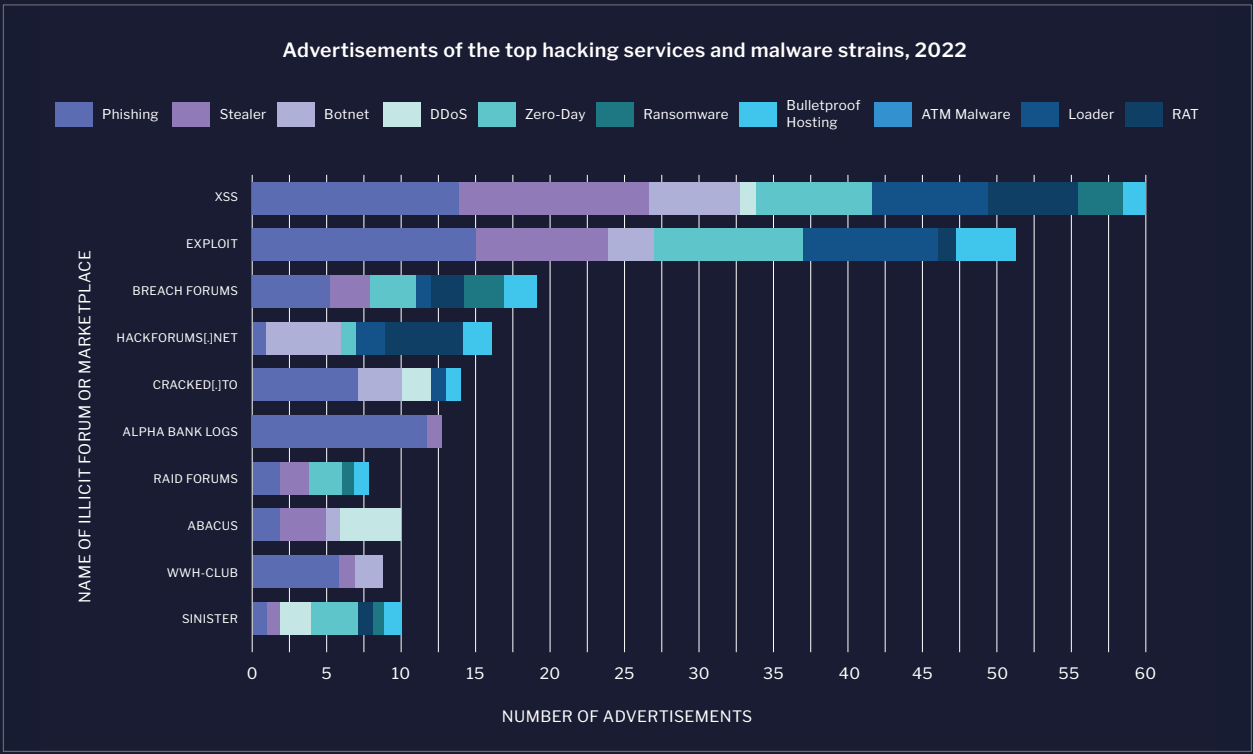
The information economic sector and the professional, scientific, and technical sector were responsible for the bulk of records lost, losing 13.8 billion and 2.2 billion, respectively. Vendors in these sectors include web-hosting companies, data processing services, accounting, and payroll firms—services that are often employed in every industry.

This data shows that once organizations employ vendors to perform these services on their behalf, those same vendors leave sensitive customer and employee data out in the open. As such, it is critical for business leaders to have an active Vendor Risk Management Program, or to ensure that their digital supply chain is implementing effective security controls.

2 STEALERS AND PHISHING

Flashpoint has observed new information-stealing malware ("stealers") such as AcridRain and TyphonStealer enter the market, in addition to long-running strains like Raccoon, RedLine, and Vidar remaining popular. Stealers have been a prolific tool in 2022, responsible for supplying log shops with massive amounts of compromised credentials. The use of stealers has been tied to several high-profile breaches—particularly by the data extortion gang LAPSUS$. In March 2022, Microsoft cited the group's use of credentials and session data that were harvested from stealer malware, which Flashpoint then linked to the use of RedLine.

Stealers, as well as other types of malware, have become much more readily accessible. The popularity of open-source communication methods has made it easy for threat actors of all skill levels to find illicit markets advertising crimeware. The majority of these services were advertised and discussed on XSS, Exploit, and Breach Forums. The popularity, use, and growing sophistication of stealers will continue into 2023.



Alongside stealers, phishing continues to be immensely popular among threat actors, with Flashpoint analysts observing a peak in the number of unique phishing pages created in 2022. Phishing will likely continue to dominate as the primary attack vector. Flashpoint observed phishing kits advertised for compromising cryptocurrency wallets, as well as cloud services used to distribute malicious files to facilitate phishing attacks.

Throughout 2022, threat actors developed new tools to intercept credentials and session data to carry out phishing campaigns and to undermine existing security controls. In 2022, Flashpoint analysts witnessed the launch of EvilProxy, a phishing-as-a-service platform that serves as a person-in-the-middle (PITM). It enables threat actors to capture credential and session data—including multi factor authentication (MFA) tokens—in between phishing pages and legitimate sign-in portals.

2022 also saw the use of "browser-in-the-browser" attacks to spoof single sign-on services, as well as campaigns in which threat actors imitate Remote Desktop Protocol services such as ConnectWise.

3 VULNERABILITIES AND EXPLOITS

As Flashpoint monitors various illicit markets and channels, we often see threat actors discussing vulnerabilities—flaws in computer software or hardware that allow an attacker to cross privilege boundaries. If an organization is using a vulnerable device or software, hackers can "exploit" its flaws—leveraging it to gain control of that asset or compromise other systems in the network by using other vulnerabilities to move laterally. Ultimately, they can destroy or exfiltrate sensitive data, implement ransomware, or lurk within to plan future attacks.

In 2022, Flashpoint observed 766 instances in which threat actors referred to a vulnerability by its Common Vulnerabilities and Exposures (CVE) ID.

Vulnerability exploits often underpin stealer malware and crimeware. However, obtaining exploit code can be a highly technical and time-consuming process. As such, threat actors are constantly canvassing promising vulnerabilities on illicit forums and markets.

The most mentioned CVE IDs from 2022, according to Flashpoint's collections, are as follows:

Month	Most Mentioned CVE
January 2022	CVE-2021-44228
February 2022	CVE-2021-40444
March 2022	CVE-2022-0847
April 2022	CVE-2022-26809
May 2022	CVE-2022-1388
June 2022	CVE-2022-30190
July 2022	CVE-2022-30190
August 2022	CVE-2022-20699
September 2022	CVE-2022-26134
October 2022	CVE-2022-40684
November 2022	CVE-2022-40684
December 2022	CVE-2022-40684

Based on analysis from the Flashpoint Intelligence Platform

All of the following vulnerabilities have been addressed by their respective vendors. If any of these issues potentially impacts your environment, Flashpoint strongly recommends prioritizing the patching of these vulnerabilities—since they have seen the most active discussions and could result in remote code execution (RCE).

Flashpoint additionally tracked specific illicit market discussions that involved the trade, purchase, sale, or general procurement of exploit code. Vulnerability exploits can demand prices typically ranging from US$2,000 to US$4,000, with advanced ones demanding prices above US$10,000. Factors such as the range of products affected or the ease of use can also impact the selling price.

The following vulnerabilities are fully weaponized and were offered for sale on illicit markets. They are notable because they affect well-known products and third-party libraries.

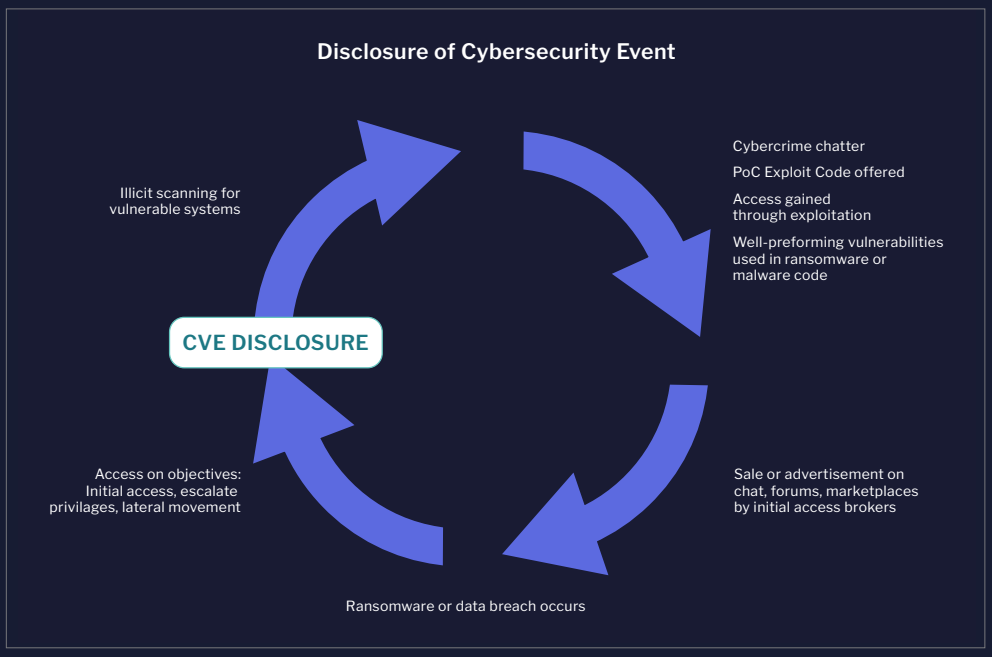
CVE ID	Exploitation Consequences
CVE-2021-35587	Remote code execution
CVE-2021-39144	Remote code execution
CVE-2022-21497	Information disclosure
CVE-2022-22960	Privilege escalation
CVE-2022-24112	Remote code execution
CVE-2022-24706	Remote code execution
CVE-2022-31675	Authentication bypass
CVE-2022-36804	Remote code execution
CVE-2022-40684	Authentication bypass
CVE-2022-41045	Privilege escalation

Based on analysis from the Flashpoint Intelligence Platform

Best practices:

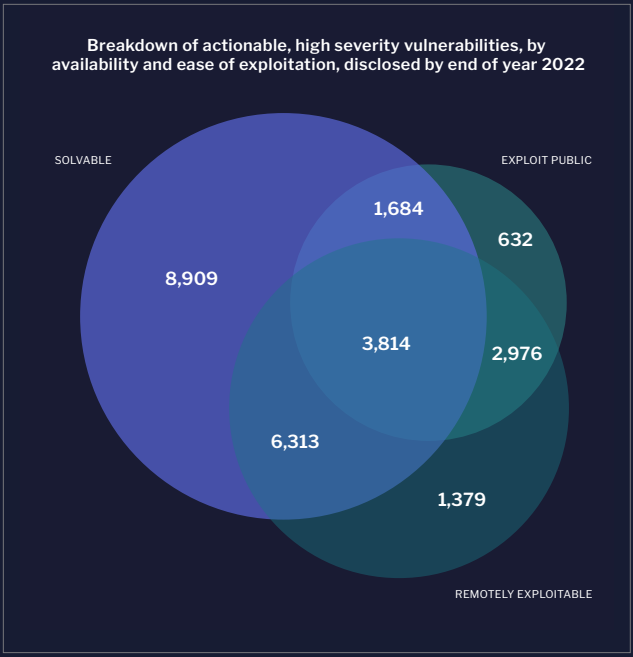
HOW TO FIGHT BACK

To stop threat cycles from perpetuating, organizations should aim to understand how attacks are perpetrated, which includes a detailed understanding of how each phase of an attack sequence is coordinated (and can be mitigated). However, in order to do this effectively, security teams require access to a single source of truth—a place where they can see and understand their risk profile across multiple use cases, from fraud to ransomware. As cyber threats overlap and intertwine, it is critical that each security team has equal visibility into the cyber threat landscape, which will facilitate communication and integrate workflows.



Source: Flashpoint

The functions and processes of each team play a critical role in preventing and responding to cybersecurity events. Even though data breaches can result from misconfigurations and some ransomware attacks can be attributed to a malicious link, behind these events is often an exploited vulnerability. Therefore, integrating CTI and Vulnerability Management workflows can reap major benefits for organizations—helping to guide patching in an environment ripe with volatility.

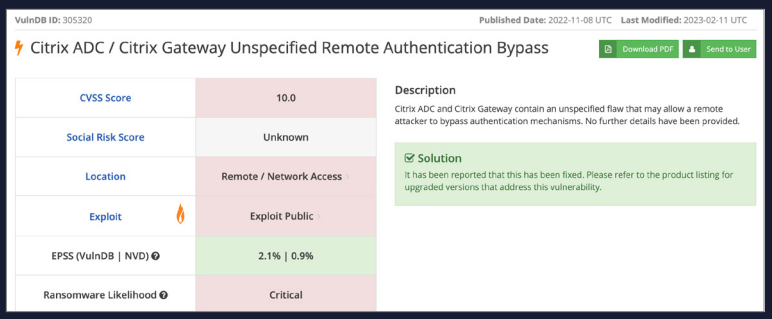


Based on analysis from Flashpoint's VulnDB

Threat actor monitoring and illicit chatter can be a valuable tool for Vulnerability Management teams, providing them a clear path for identifying risk. Last year, Flashpoint collected 26,900 disclosed vulnerabilities—too many for one organization to patch in a timely manner. However, by focusing on issues that are actively being discussed by illicit communities and then shifting attention to actionable, high-severity vulnerabilities—those that are remotely exploitable with a known exploit—that have a documented solution, those teams can potentially reduce their immediate workload by nearly 85 percent since these issues pose the most risk and are fixable.

According to Flashpoint's collections, there are over 306,000 known vulnerabilities—97,000 of which cannot be found in CVE and NVD.

CTI teams can also reap similar benefits from VM processes—especially in regards to ransomware. Well-versed threat actors and APTs actively exploit vulnerabilities found in end-user software, third-party libraries, and dependencies to conduct ransomware campaigns. VulnDB's Ransomware Prediction Model gives VM teams the ability to use predictive analysis to assess the likelihood that any known or newly disclosed vulnerability will be used in future ransomware operations. Using this information, security teams can prioritize remediating these issues, better protecting their organization as a whole.



Organizations cannot afford to have their security teams operating in a vacuum. As threat actors unite and learn from one another, their tactics, tools, and procedures become more effective and potent. In order to not be swept away by 2023's rising wave of cybercrime, business leaders need to break the perpetual cycle, do away with the multiple disjointed feeds and solutions, and work toward achieving a single source of truth that is powered by consolidated intelligence.

Consolidate intelligence with Flashpoint

Threat vectors are converging at breakneck speeds, and the multiple disjointed feeds and solutions makes addressing risk increasingly difficult. Therefore, organizations need consolidated intelligence that unites and supports all of their security and intelligence teams. Sign up for a free trial for a single source of truth that supports Cyber Threat Intelligence, Vulnerability Management, DevSecOps, Fraud, and other functions.

FREE TRIAL

ABOUT FLASHPOINT

Trusted by governments, commercial enterprises, and educational institutions worldwide, Flashpoint helps organizations protect their most critical assets, infrastructure, and stakeholders from security risks such as cyber threats, ransomware, fraud, physical threats, and more. Leading security practitioners—including physical and corporate security, cyber threat intelligence (CTI), vulnerability management, and vendor risk management teams—rely on the Flashpoint Intelligence Platform, comprising open-source (OSINT) and closed intelligence, to proactively identify and mitigate risk and stay ahead of the evolving threat landscape. Learn more at www.flashpoint.io