FLASHPOINT

State of Cyber Threat Intelligence: Australia Edition

The following report focuses on the Australian cyber threat landscape, which rolls up into Flashpoint's global State of Cyber Threat Intelligence report.

Our data and intelligence

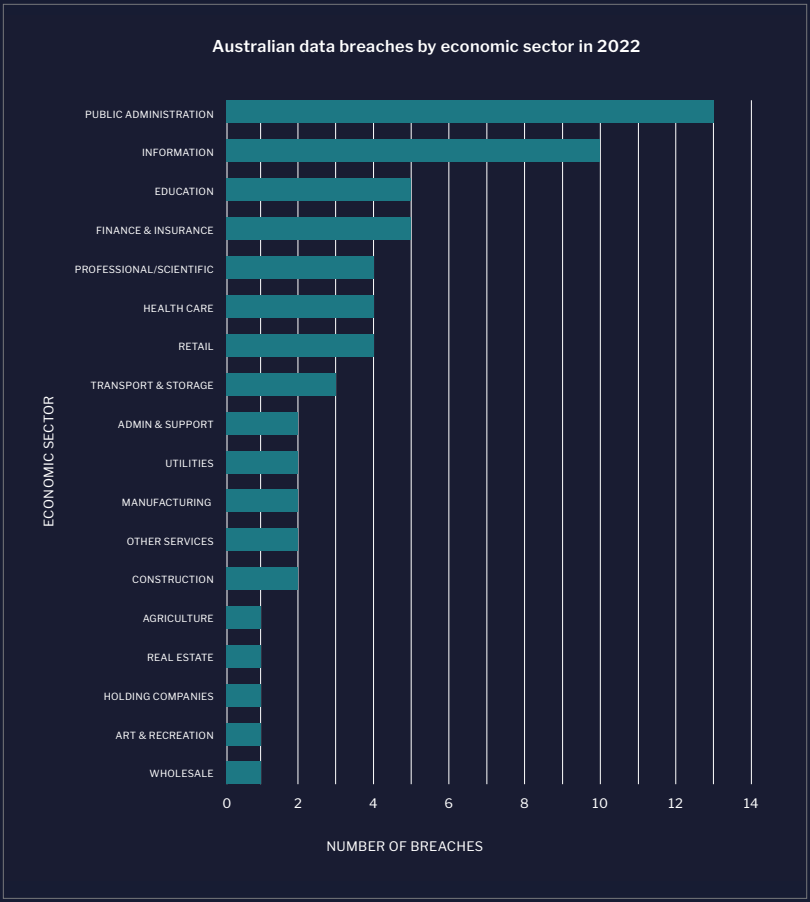
All the data and intelligence in this report is derived from Flashpoint's collections and intelligence team. Flashpoint's collections utilise a mix of technologies that include AI/ML, and NLP models that are internally trained to surface relevant information for each customer.

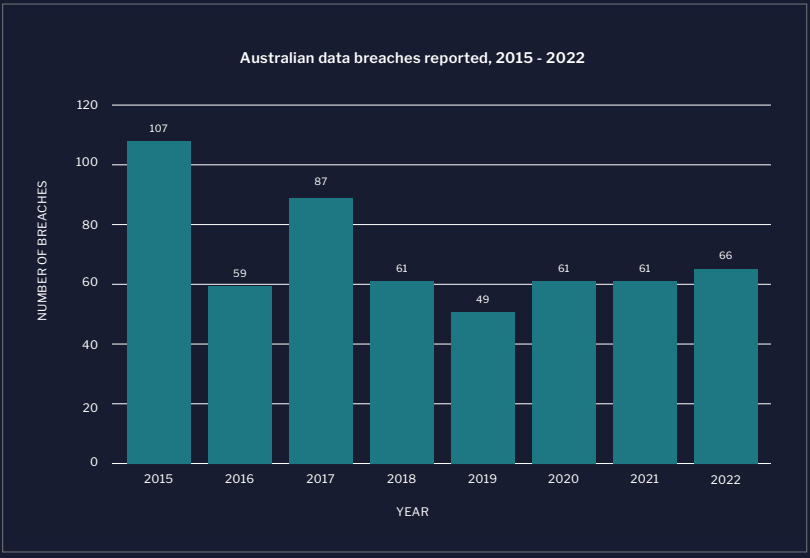
The Flashpoint intelligence team comprises over 100 experts who speak 35 languages and counting. Flashpoint uses highly efficient translation models for our datasets, which span more than 25 languages, providing a wider range of search results from foreign language sources within Flashpoint collections.

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

Data breaches in Australia



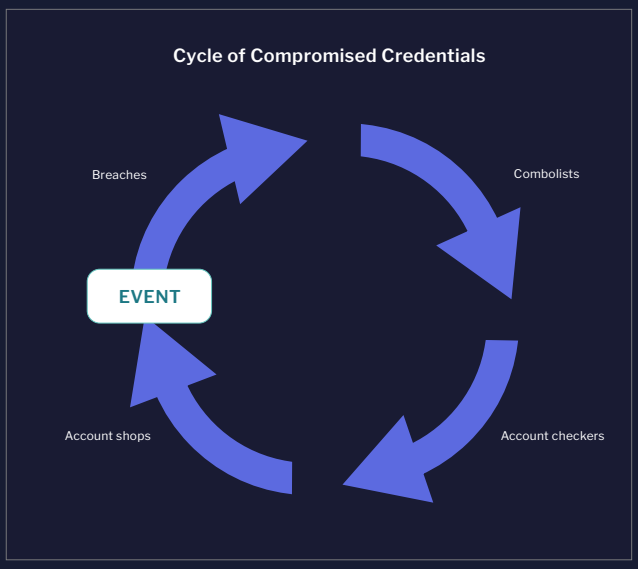


The Australia Cyber environment has changed dramatically since the COVID-19 pandemic, associated lockdowns, and a workforce required to undertake employment remotely, often without having the necessary information technology infrastructure or security in place. This has seen a number of vendors suffer large-scale data breaches including telecommunication providers, health insurance vendors, and Australian Government entities.

The 2022 calendar year has seen a marked increase in the total number of Australian breaches reported when compared to the previous 2020 and 2021 years respectively. In terms of types of data exposed, Flashpoint has seen threat actors primarily focusing on obtaining email addresses and account credentials—however, they will exfiltrate any kind of personally identifiable information—in order to either ransom it, or sell it within illicit markets.

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. Fraud and phishing campaigns also remain as one of the more commonly used methods employed by threat actors. However, more recent events have indicated that ransomware attacks are increasingly being used by APT groups. Such events have been highlighted through the large scale breaches suffered by Australia's second largest Telecommunications Company, Optus, as well as Private Health Insurance provider Medibank.

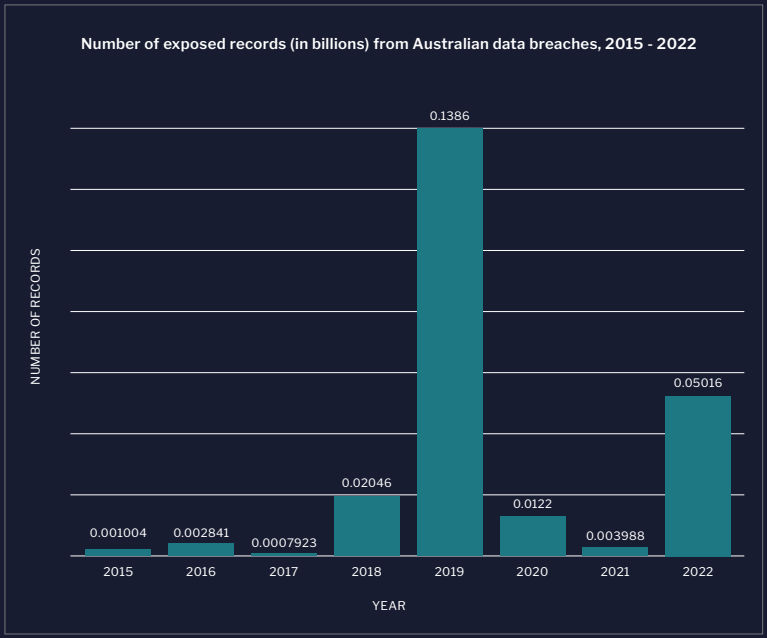


Source: Flashpoint

How are cybercriminals gaining access to organisations?

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 exposed and stolen credentials reached over 50 million last year, a 99 percent increase compared to 2021.



Following global trends, the Information Media and Telecommunications division was responsible for the bulk of records lost, losing 72 percent (36 million) of Australia's 50 million total. Vendors in this division include web-hosting companies, data processing services, and programming design—services that are often employed in every division. 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.

Poor cybersecurity practices, in addition to the constant targeting of APT groups from China and Russia—such as REvil—resulted in the massive increase in Australian records exposed, as well as for the majority of

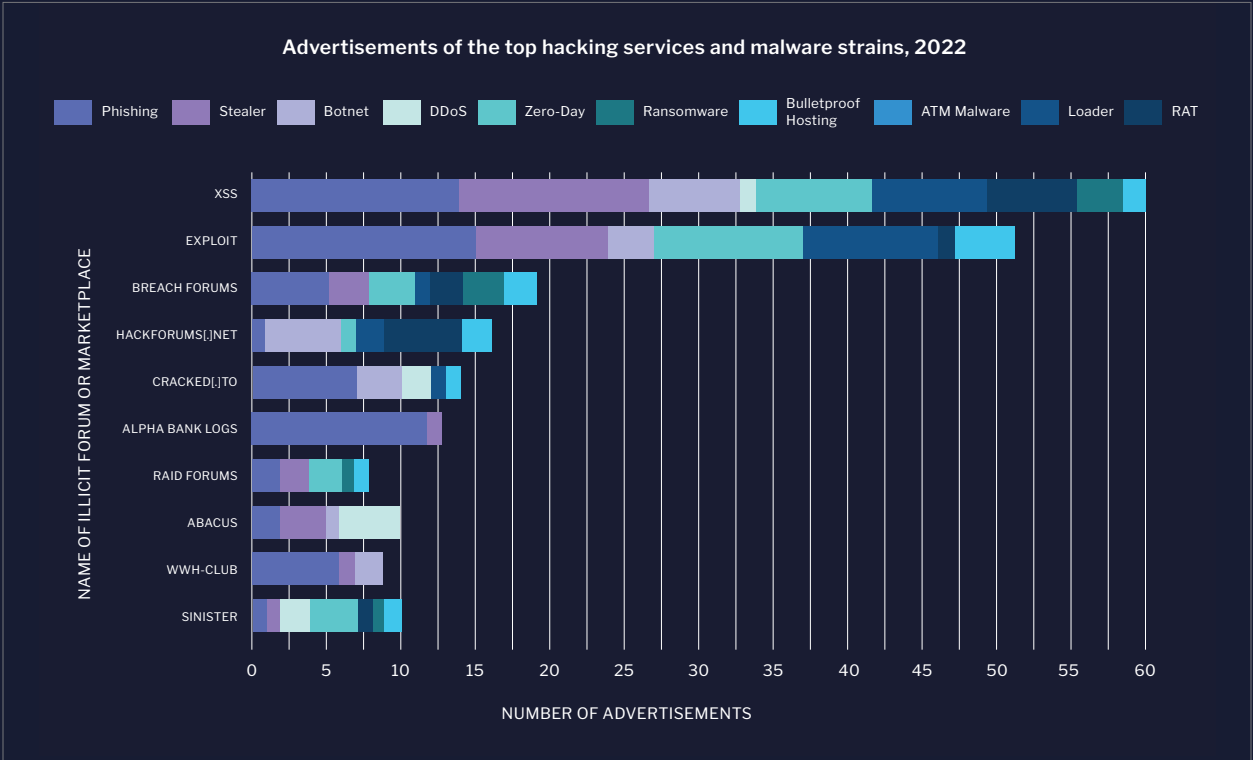
experienced breaches. The Australian Public Sector industry was responsible for nearly 20 percent of the country's data breach total. The Australian government sector, its cyber security vendors, and the Information Media and Telecommunications division practiced a lax security culture—which was exacerbated by COVID's rapid shift to remote work. Existing infrastructure could not support such a sudden and dynamic change.

Flashpoint analysts observed security incidents throughout 2022 where government workers and contractors had used personal emails on government systems to subscribe to services that were completely unrelated to their workloads—one of the many cardinal sins of cybersecurity.

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 organisation 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 prioritising 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 AUD$3,000 to AUD$6,000, with advanced ones demanding prices above AUD$15,000. Factors such as the range of products affected or the ease of use can also impact the selling price.

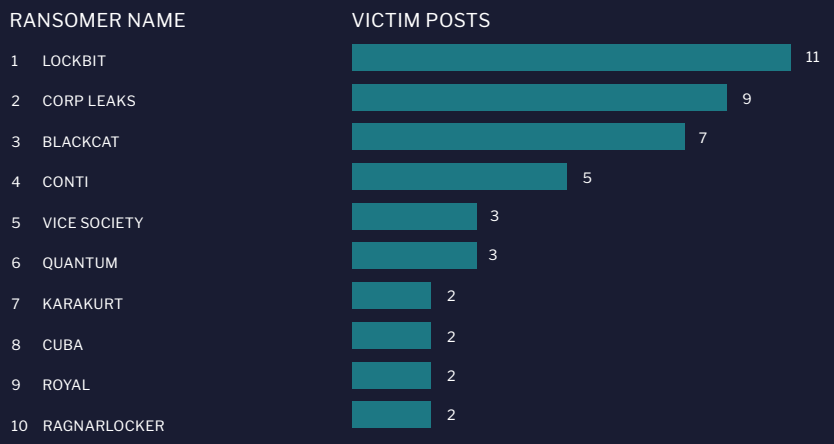
The following vulnerabilities are fully weaponised and were offered for sale on illicit markets. They are notable because they affect well-known products and third-party libraries.

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

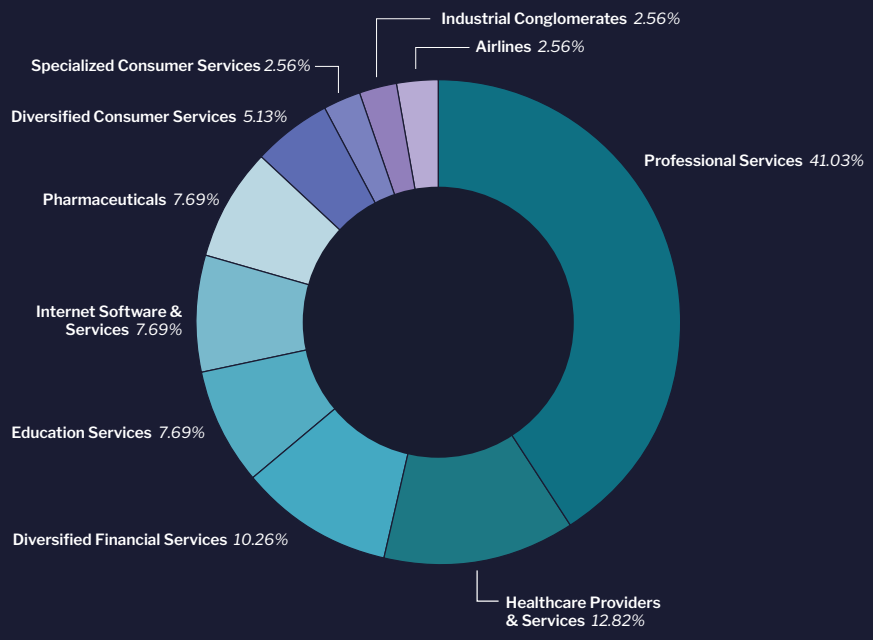
Based on analysis from the Flashpoint Intelligence Platform

The use of all these tactics have contributed to a prolific year of cyberattacks—particularly ransomware. Last year, Flashpoint recorded 56 ransomware attacks attributed to Australian organisations, and looking into 2023, our collections indicate that the number of reported ransomware attacks is on track to exceed 2022.

Top ten ransomware groups targeting Australian organisations, 2022

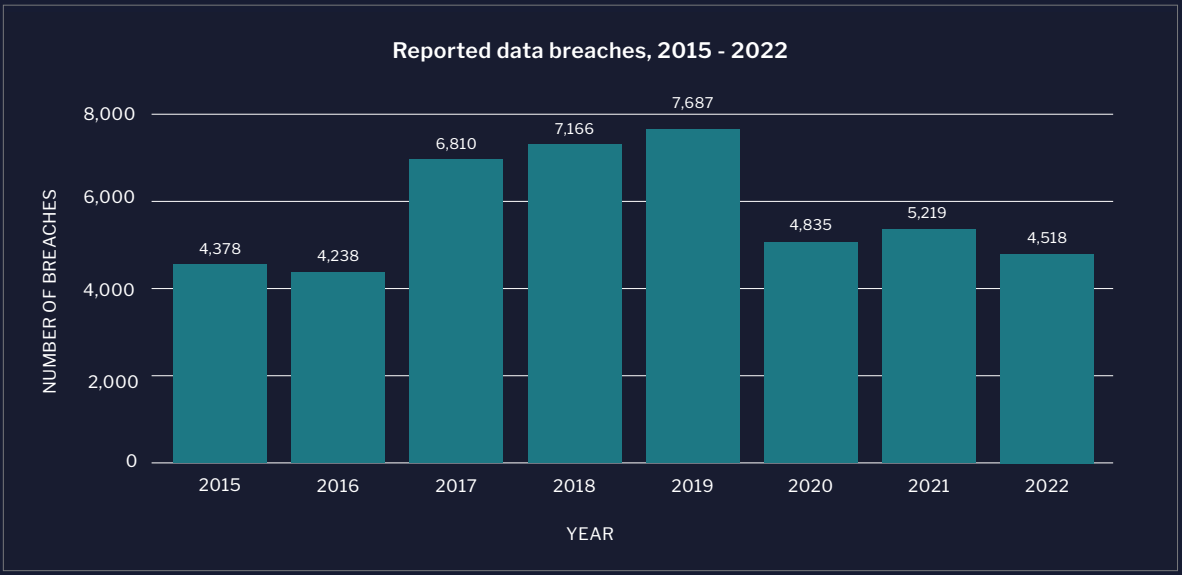


Australian industries most affected by ransomware attacks, 2022

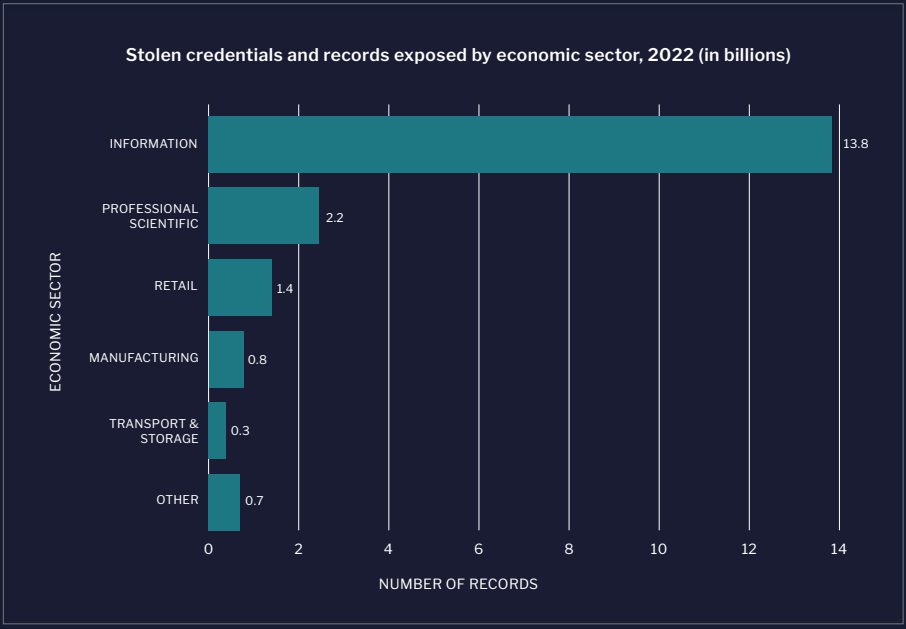


(A global look) The impact of converged threats

BY THE NUMBERS

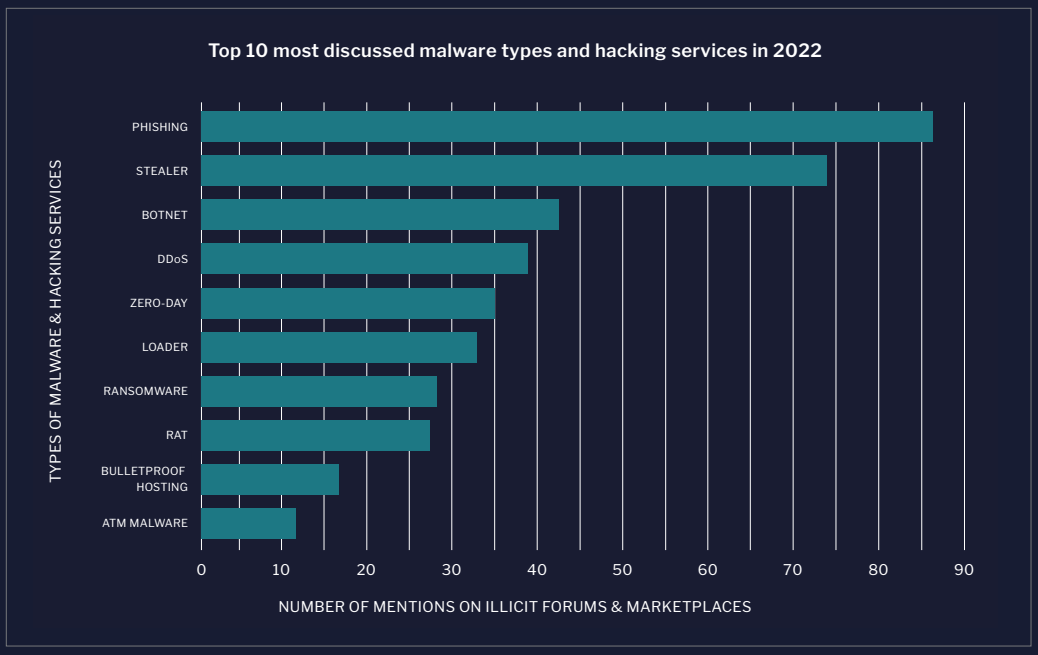


Last year, 4,518 data breaches were reported, according to Flashpoint's collections. Threat actors exposed or stole 22.62 billion credentials and personal records, ranging from account and financial information to emails and other personally identifiable information (PII).



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 weaponise 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 organisational 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.

Consolidate intelligence with Flashpoint

Threat vectors are converging at breakneck speeds, and the multiple disjointed feeds and solutions makes addressing risk increasingly difficult. Organizations need consolidated intelligence that unites and supports all of their security and intelligence teams. Read our global State of Cyber Threat Intelligence report to learn how a single source of truth can empower and support Cyber Threat Intelligence, Vulnerability Management, DevSecOps, Fraud, and other teams.

READ NOW

ABOUT FLASHPOINT

Trusted by governments, commercial enterprises, and educational institutions worldwide, Flashpoint helps organisations 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**