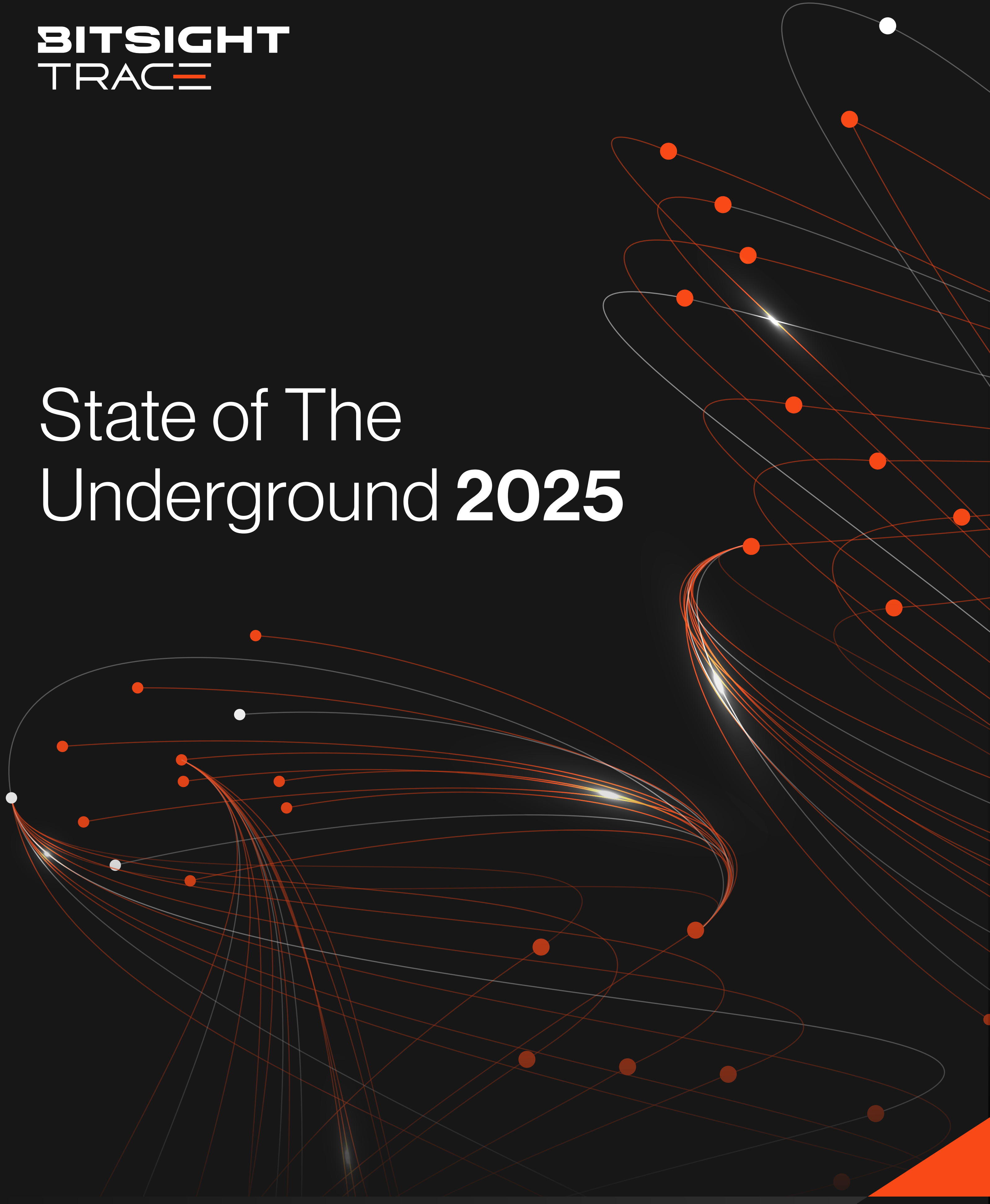
BITSIGHT TRACE

State of The Underground **2025**



Executive Summary

Ransomware attacks (as measured by unique victims listed on leak sites) rose by almost 25% in 2024, and the number of ransomware group leak sites rose by 53%. The rise in both attacks and groups indicates that this sophistication is diffusing to additional entities, possibly as group members spin off and establish their own ransomware gangs.

The number of data breaches shared on underground forums rose by 43%, with US organizations accounting for nearly 20% of victims. Professional, Scientific, and Technical Services were the most targeted sectors.

In 2024, logs from 7.7 million endpoints were listed on underground markets, an increase from 6.8 million in 2023. India was the leading origin of these logs (9.3% of total). While Raccoon stealer led in 2022 and 2023, it vanished in 2024, replaced by Lumma and Risepro.

We collected 2.9 billion unique sets of compromised credentials leaked in 2024, a significant increase from 2023's figure (2.2 billion). This rise is partially a result of advancement in Bitsight's credential collection capabilities and partially because of increased data breaches and the surge in stealer logs.

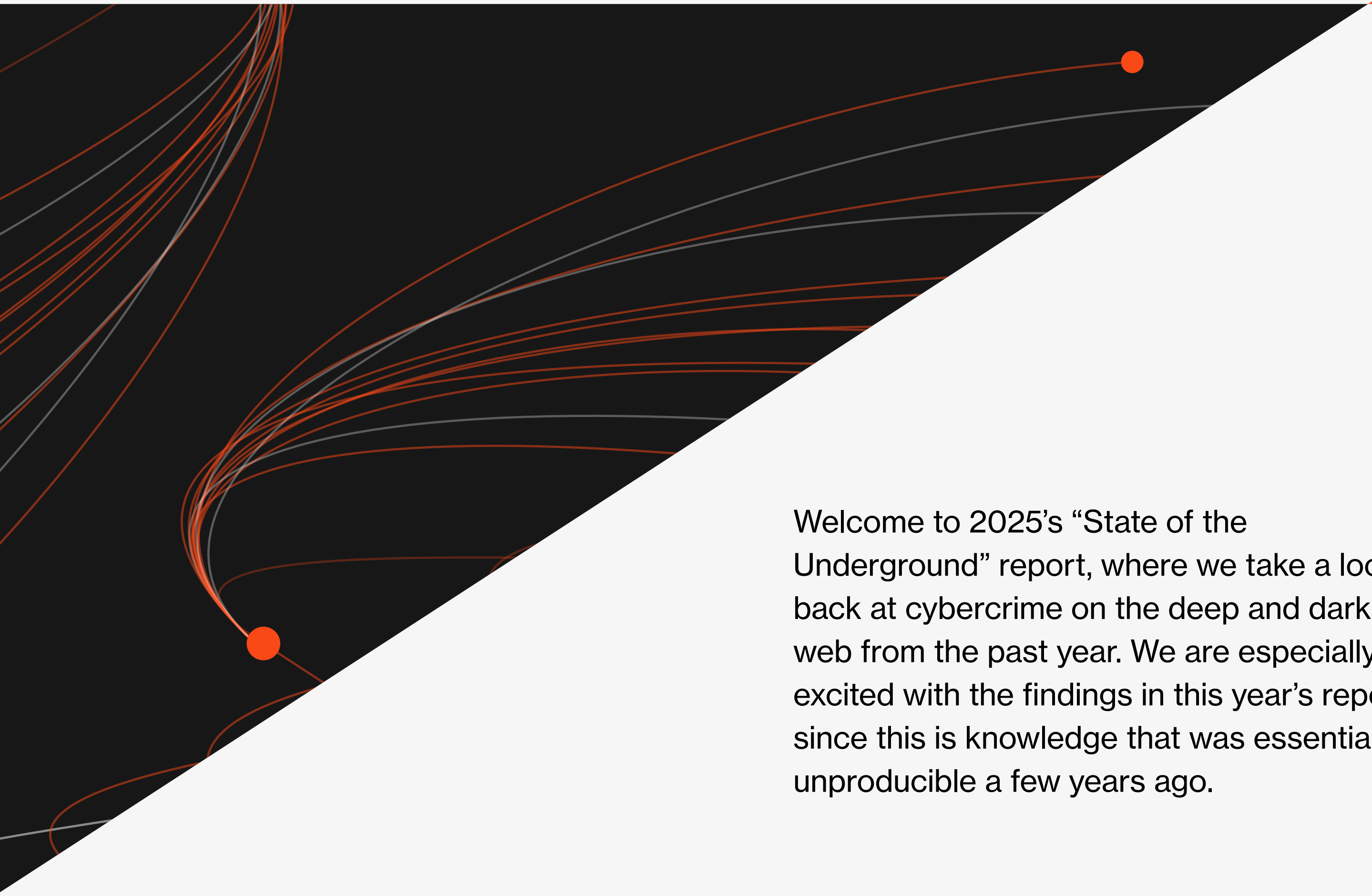
Reflecting geopolitical tensions surrounding the war in Gaza, #OpIsrael was the leading hacktivist hashtag in 2024.

On the top three criminal forums, 384 unique varieties of malware were sold in 2024. Stealers, followed by RATs, have been the most prevalent malware types for each of the past three years.

The most exposed devices to the most critical vulnerabilities were found in the US, and the most affected sectors were either Information (including telecommunications) and Professional, Scientific, and Technical Services (including security and software vendors).

In 2024, underground markets listed nearly 14.5 million compromised credit cards, a 20% increase from 2023. This rise is exclusively due to a surge in US cards; the number of cards from the rest of the world declined by 1.6 million, but listings of US cards increased by 4.5 million, accounting for 80.7% of all compromised card listings in 2024.

Introduction



Welcome to 2025's "State of the Underground" report, where we take a look back at cybercrime on the deep and dark web from the past year. We are especially excited with the findings in this year's report, since this is knowledge that was essentially unproducible a few years ago.

What changed?

Well, traditionally, threat intelligence is a field in which analysts suffer from information overload: too many signals, too much noise, and inadequate resources to process everything. Analysts simply need assistance with data labeling and classification at scale, which is a modest request of an LLM; it's a far cry from asking it to invent a new, lifesaving medicine.

Therefore, while an excessive amount of (digital) ink has been spilled hyping up how advances in genAI are going to benefit cyberattackers, we don't think that enough attention has been paid to the power of AI in the hands of cyber defenders, or, more specifically, cyber threat intelligence (CTI) practitioners.

We strongly believe that LLMs are capable of fundamentally changing the way we approach CTI.

43%

increase in breaches occurred from 2023 to 2024.

45%

of breaches in 2024 included a free download link.

The report in your hands is our proof: we used Bitsight IQ to process tens of thousands of deep and dark web posts, a project that previously would have only been possible with a brigade of analysts working around the clock.

Indeed, Bitsight IQ is integrated within many aspects of our threat intelligence offering, including smarter collection, automated curation of relevant intel items in Bitsight Pulse, generation of audience-tailored intel reports, and creation of item, actor, and entity summaries. It's there to assist at each stage of the intelligence cycle. The fact that analysts need to spend less time collecting, filtering, and labeling data means that they can spend more time analyzing. They can ask hard questions and discover the answers. They can produce insights that were previously considered unattainable. All of this is done with a singular goal in mind: to advise their organizations on how to be more secure.

While many readers might be satisfied with this polished report, we know that the most exacting analysts will want to delve into the raw data and slice and dice the numbers as they see fit. For them, we recommend checking out the Bitsight Pulse API, which includes access to a breadth of structured intelligence beyond what could fit in this report.

One final note

The data presented in this report reflects Bitsight's collected intelligence. Collecting from the underground is a game of cat and mouse; underground forums and markets can stealthily rise and suddenly vanish, and sites can implement mechanisms to make collection more difficult. Therefore, we are presenting what we observed, which probably varies to a certain degree from the exact numbers. While underground activity is constantly shifting, our collection provides a representative picture of the overall landscape.

Ransomware

We examined ransomware attacks in 2024 and compared them to the numbers of previous years. In order to do so, we extracted posts from ransomware dedicated leak sites (DLS) and then used genAI to extract victim, victim location, and victim sector. We then deduplicated instances of which the same ransomware group posted more than once about the same victim.

Ransomware attacks

Overall, ransomware groups posted about 5,021 unique attacks in 2024, an increase from 4,029 in 2023.

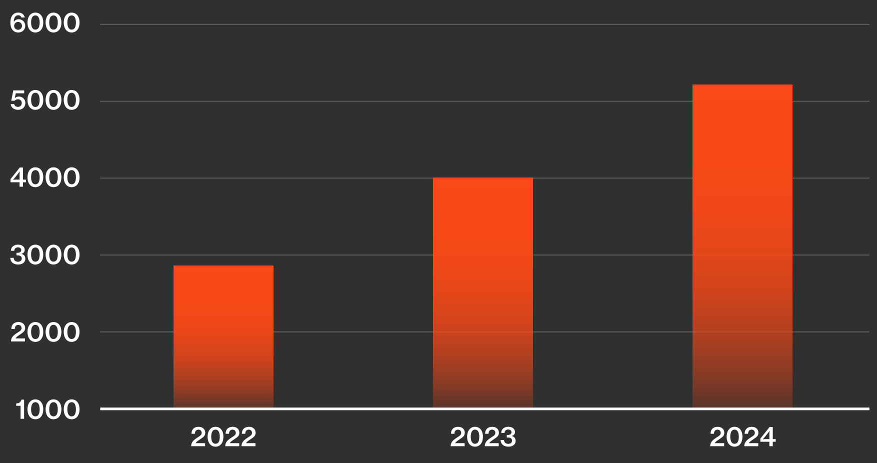


Figure 1. Number of ransomware attacks over the past three years.

Active ransomware groups

After declining from 2022 to 2023, the number of ransomware groups also rose; 89 leak sites were in operation, 31 more than in 2023.

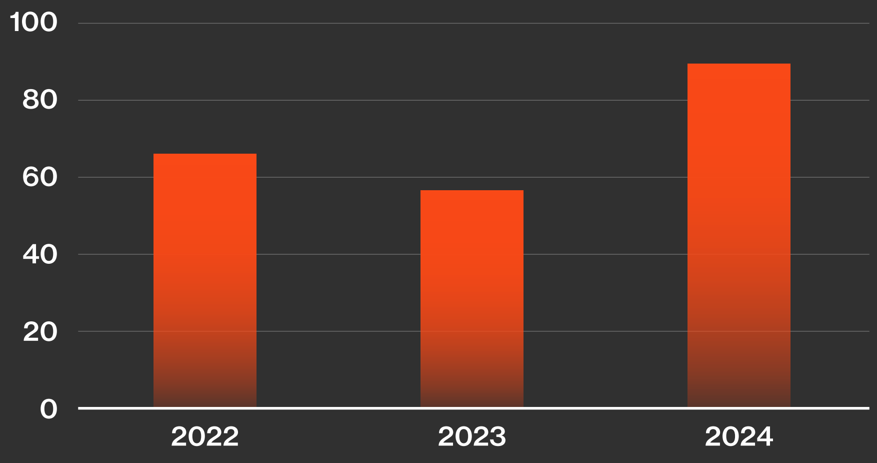


Figure 2. Number of active ransomware groups over the past three years.

RansomHub, a newcomer in 2024, led all ransomware groups with 534 attacks, or 10.6% of the total.

Interestingly, while the 10 largest groups of 2023 accounted for 77.7% of all attacks (3,131 in total), the 10 largest groups of 2024 accounted for 56.6% (2,843 total). This change in distribution can mostly be attributed to the fact that Lockbit's 1,027 attacks accounted for over a quarter of attacks in 2023, before it was taken down by an international law enforcement operation in 2024.

Most victims per ransomware group (2024)

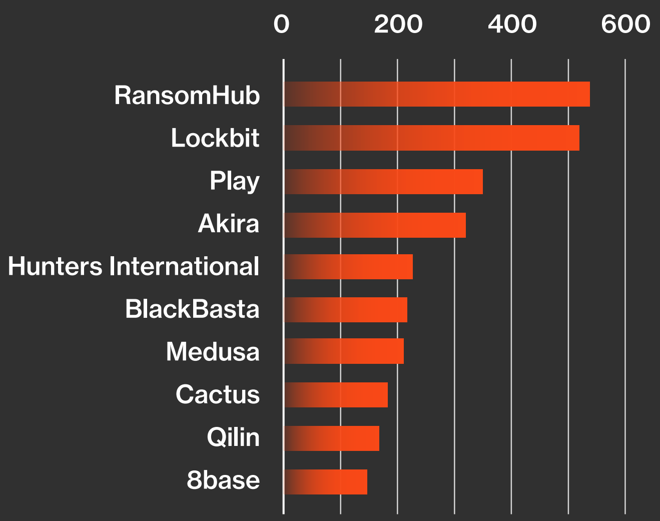


Figure 3: Number of victims per ransomware group.

The more even distribution of attacks is reflected in the fact that the average number of attacks per group declined from 76 to 58 from 2023 to 2024, but the median only ticked down slightly, from 22 to 19.

Indeed, the fact that the top 10 groups carried out fewer attacks even as the total number of attacks rose by about a quarter indicates a troubling trend: Big-game ransomware attacks are highly sophisticated and include many stages and competencies, including malware development, initial access, malware deployment, data exfiltration, encryption, DLS hosting, ransom negotiation, and money laundering. The rise in attacks indicates that this sophistication is diffusing to additional entities, possibly as group members spin off and establish their own ransomware gangs (such as Lynx, Fog, and Funksec). It also appears that the victims, while greater in number, tend to be smaller organizations that provide smaller payouts.

A Chainalysis report noted a 35% decrease in ransom payments in 2024, and it cited a researcher from Coveware, who noted that "the current ransomware ecosystem is infused with a lot of newcomers who tend to focus efforts on the small- to mid-size markets, which in turn are associated with more modest ransom demands."

This analysis matches our data. We can presume that the largest organizations possess the resources to prevent major ransomware attacks, while smaller ones do not. Similarly, law enforcement can only target so many groups, so they undoubtedly prioritize the larger ones, enabling relative impunity for the others. Thus, we assess that the environment is ripe for medium-sized groups to proliferate and to target medium-sized organizations.

Victim locations and sectors

We identified 4,081 attack locations, with the US accounting for 55.5% – up slightly from 52.9% in 2023. Canada followed distantly at 4.7%. Countries ranked 2–7 (Canada, UK, Germany, Italy, Brazil, France, and Australia) remained the same year over year, though in a different order.

Top ransomware victims per country (2024)

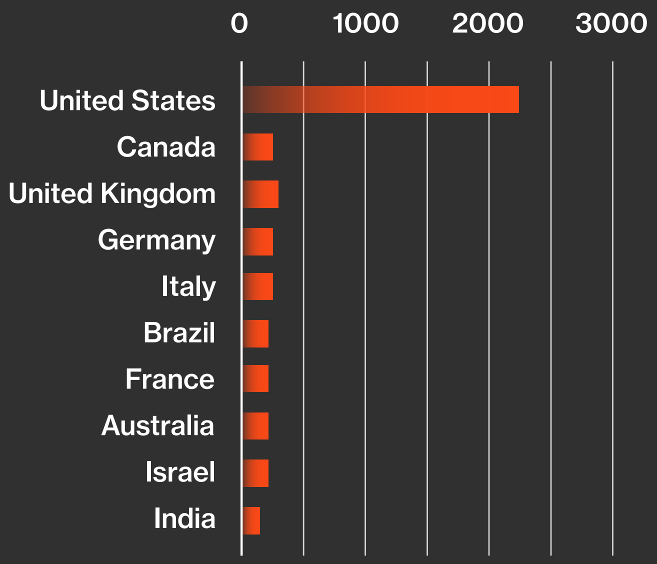


Figure 4: Number of ransomware victims identified per country.

The Manufacturing sector was the most targeted for the third year in a row, accounting for 22% of the 4,853 attacks for which we could attribute a sector. Considering that manufacturing is hardly the largest sector by number of businesses or by market cap, it would be interesting to investigate why it was the most targeted sector, but this is out of the scope of this report.

Top ransomware victims per sector (2024)

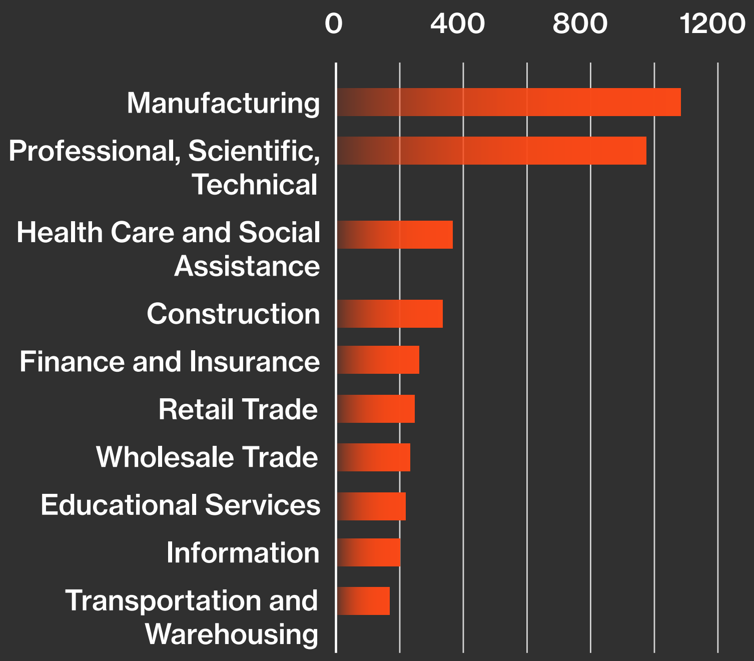


Figure 5: Top ransomware victims per sector.

Meanwhile, “Professional, Scientific, and Technical Services” came in second for the third consecutive year.

Therefore, while there has been a significant rise in the number of attacks, in the number of active groups, and apparently, in the size of the victims, the top victim locations and sectors have remained remarkably consistent. Perhaps this is because individuals that break off from existing ransomware gangs to start on their own still follow the battle-proven TTPs of their former groups.

43%

increase in breaches occurred from 2023 to 2024.

45%

of breaches in 2024 included a free download link.

55%

of breaches in 2024 were presumably offered for sale.

1 in 2

breaches in 2024 involved data that was shared openly.

Data breaches

On underground forums, threat actors share and sell data breaches. This includes data that was procured through web app attacks, malware, scraping, and social engineering. The type of breached data varies; it can include an organization's internal data, employee data, or customer data.

We define a data breach as data that comes from a single victim organization, thus excluding combos, fullz, and other collections and compilations frequently shared on the underground.

Producing reliable metrics about data breaches is tricky; anyone can share an alleged data breach on an underground forum. While this is partially mitigated by forum participants and admins calling out and banning actors that post fake data, we still need to be wary that not every claim of a breach is an actual breach.

Furthermore, many data breaches are re-shared, so we removed duplicates within this data set. Accordingly, while the data from 2023 and 2024 does not include duplicates, 2022's figure includes re-shared databases from years prior. (For what it's worth, 20–25% were duplicates in 2023–2024, so applying this to 2022's data, we assess that in 2022, there were more breaches than in 2023 but probably fewer than 2024.)

Data breaches shared on underground forums

All this said, there was a 43% increase in breaches from 2023 to 2024: 45% of 2024's breaches included a link to download the data, indicating that they were shared for free, while the other 55% were presumably for sale.

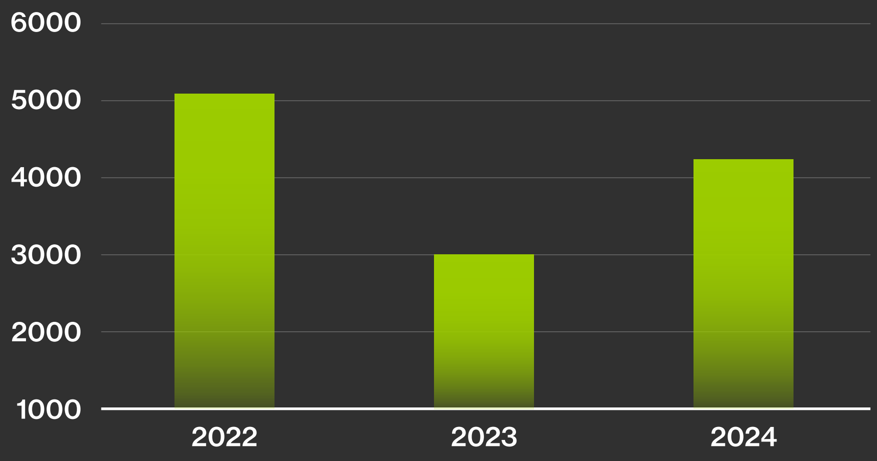


Figure 6. Number of data breaches shared on underground forums over the past three years.

Of the data breaches for which we could identify a victim location (n=2003), the US accounted for nearly 20%.

Top data breach victims per country (2024)

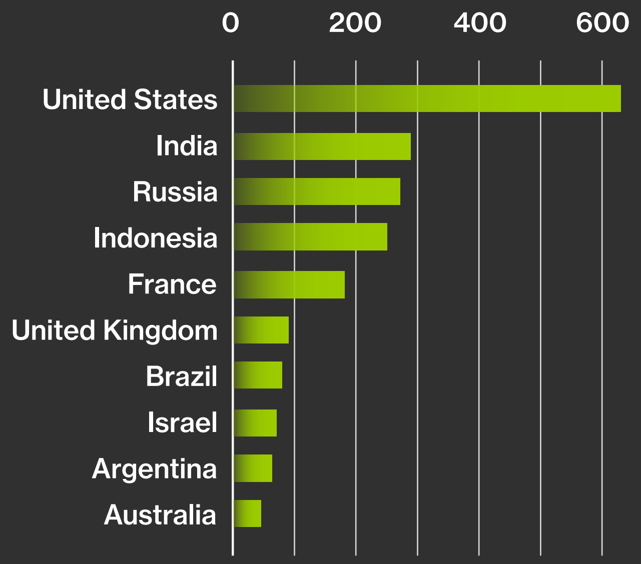


Figure 7. Number of data breach victims identified per country.

Top data breach victims per sector (2024)

Professional, Scientific, and Technical Services led other sectors, edging out Information and Retail Trade by a handful (n=3430). The order of sectors makes sense, as the leaders tend to have large quantities of user data hosted on internet-facing systems.

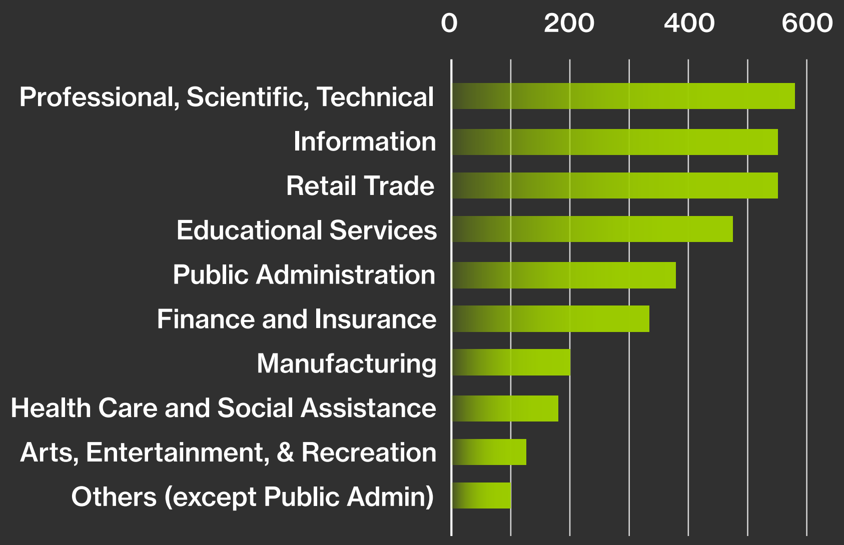


Figure 8. Top data breach victims per sector.

Malware

We examined malware and hacking tools for sale on the top three criminal forums. 384 unique varieties of malware were sold in 2024, an increase from 349 in 2023. Stealers, followed by RATs (remote access trojans), have been the most prevalent malware types for each of the past three years.

Most popular malware types on top crime forums (2024)

The vast majority of malware varieties target Windows, followed by a few dozen targeting Android. The others target a variety of platforms, ranging from Telegram to Chrome to Netflix.

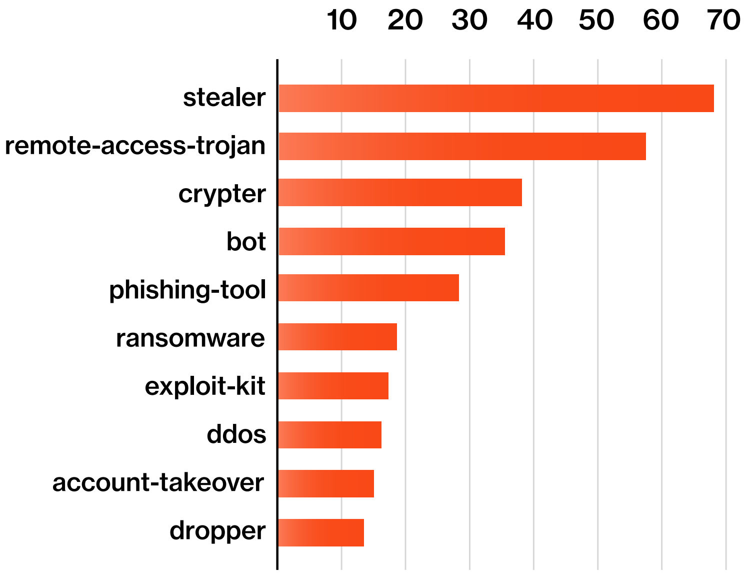
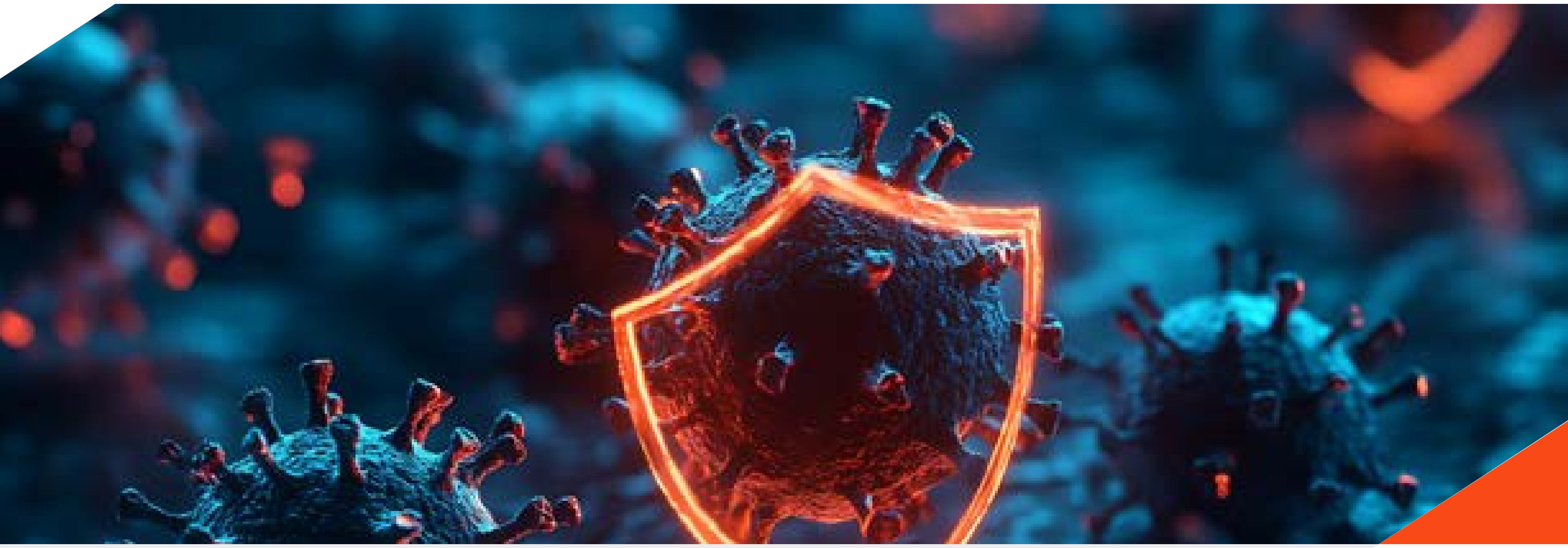


Figure 9. Most popular malware types as seen on crime forums.

Note that "for sale" means malware explicitly being sold (as opposed to shared for free), and this set includes unique malware (though it considers different versions to be different malware). Furthermore, keep in mind that slight variations in name also result in unique designations.



Hacktivism

Hacktivism (i.e. ideologically motivated cyberattacks) largely follows geopolitical developments. Considering that the two largest conflicts over the past few years are the wars in Ukraine and Gaza, it makes sense that these attracted the most hacktivist attention. #OpIran was also a major hashtag, as hacktivists joined in-person demonstrations in Iran that followed the detention and death of Mahsa Amini.

In our collected data, #OpIran led in 2022 and 2023 and was replaced by #OpIsrael in 2024.

Leading hacktivist op hashtags (Telegram and Twitter)

2022	2023	2024
OpIran	OpIran	OpIsrael
OpRussia	OpIceISIS	OpRussia
OpIceISIS	OpIsrael	OpLove
OpKremlin	OpRussia	OpIndia
OpUkraine	OpIndia	OpChildSafety
OpIsrael	OpJapan	OpUSA
OpLove	OpColombia	OpIran
OpBelarus	OpFukushima	OpGaza
OpNowar	OpGOP	Op404
OpLeakageJp	OpLove	OpGOP

Op descriptions

Op404: Op404 is most commonly used by Russian-aligned hacktivists seeking to deny service to Ukrainian websites. The 404 references the HTML “page not found” error.

OpBelarus: OpBelarus targets the Belarusian government and state-affiliated institutions. The operation protests perceived authoritarian governance and seeks to expose corruption and political repression in the region.

OpChildSafety: OpChildSafety targets entities perceived to be neglecting child protection measures both online and offline. The operation seeks to expose and disrupt platforms that compromise child safety, advocating for stronger regulatory practices.

OpColombia: OpColombia targets Colombian state institutions or corporate entities, likely in response to perceived governmental corruption or social injustices. The operation seeks to expose systemic issues through digital activism.

OpFukushima and OpLeakageJp: These ops protest alleged TEPCO and Japanese government mismanagement following the Fukushima nuclear incident. It targeted these entities to demand transparency and accountability in handling radioactive leaks.

OpGaza and OpIsrael: These ops target entities involved in the Gaza conflict, particularly those associated with Israeli military and governmental actions.

OpGOP: OpGOP targets the United States Republican Party and its affiliated institutions in protest of policies and actions of Republican officials.

OpIceISIS: OpIceISIS targets the online infrastructure of extremist groups such as ISIS. Its goal is to disrupt propaganda channels and undermine the digital presence of terrorism.

OpIndia: OpIndia targets institutions associated with the Indian government in protest against its actions and perceived Hindu nationalism.

OpIran: OpIran targets Iranian government digital infrastructure in protest against censorship and state surveillance. It aims to expose state repression and promote free speech. #OpIran became specifically notable in protesting the detention and death of Mahsa Amini.

OpJapan: OpJapan targets Japanese governmental or corporate entities in response to political or social issues.

OpKremlin and OpRussia: These hashtags are used by Ukrainian hacktivists targeting Russian websites and institutions. They are also used by hacktivists targeting Russian state institutions, attempting to expose perceived political corruption and authoritarian practices.

OpLove and OpNowar: Hashtags advocating for peace, sometimes by targeting military and governmental entities involved in warfare.

OpUkraine: This hashtag is employed by both pro and anti Ukrainian hacktivists, in support of or in opposition to one of the belligerent parties.

OpUSA: OpUSA targets United States governmental and corporate systems, focusing on exposing actions perceived as unethical or oppressive.

Endpoint logs

Logs are underground slang for username, passwords, and occasionally cookies extracted from a victim endpoint with stealer malware. Threat actors can purchase these logs for around $10 and use them to access confidential accounts and data and even to deploy further attacks, such as ransomware.

In 2024, logs from 7.7 million endpoints were listed on underground markets, an increase from 6.8 million in 2023. It is especially notable that the surge of logs for sale on markets coincides with Telegram's growing popularity as a venue for sharing and selling logs.

Endpoint logs for sale on underground markets

Logs, especially those including cookies, can be useful at evading MFA, suggesting that a rising supply may reflect growing demand.

It is especially notable that the surge of logs for sale on markets coincides with Telegram's growing popularity as a venue for sharing and selling logs.

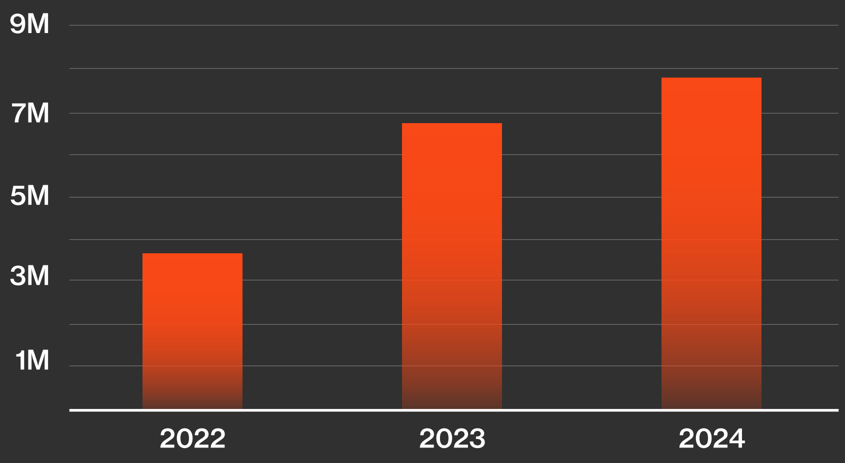


Figure 10. Number of endpoint logs listed for sale on underground markets.

Of the logs that list a country, 9.3% are from endpoints in India, followed by Brazil (7.8%).

It is notable and worthy of further investigation to understand why these countries are the most compromised. (Keep in mind that stealer malware is generally sprayed in a non-targeted fashion such as via malspam, as opposed to the more judicious targeting employed in ransomware attacks and data breaches.)

Most logs per country

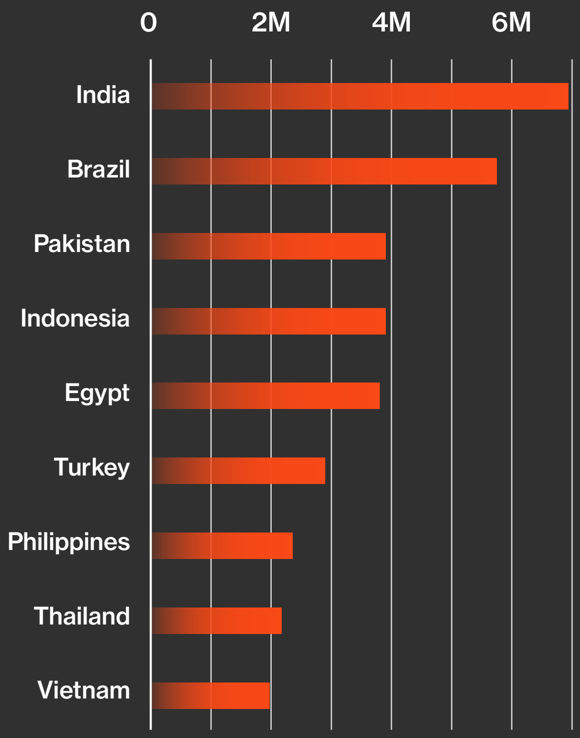


Figure 11. Most logs per country.

Top stealers for endpoint compromise

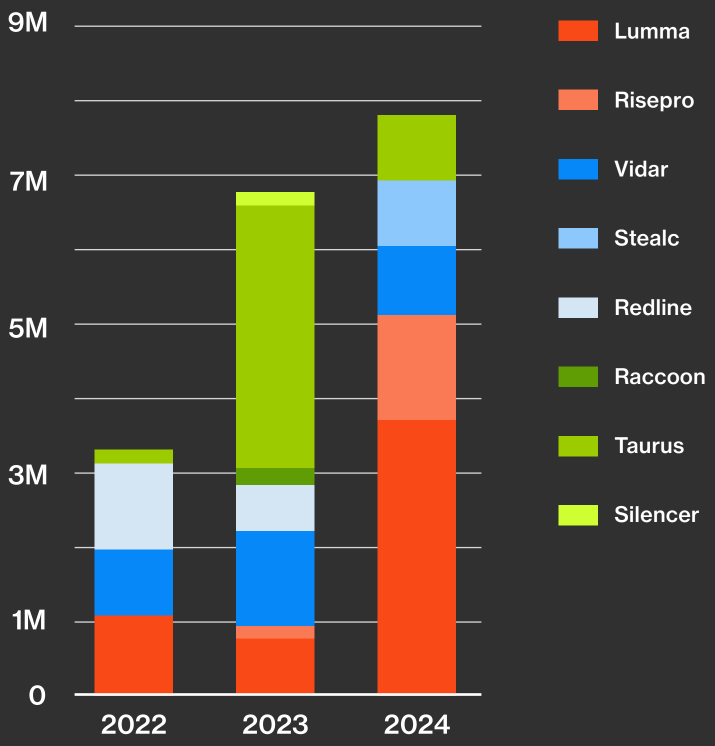


Figure 12. Top stealers seen for compromising endpoints.

In 2024, there were major changes regarding which stealer malware was used to compromise those endpoints.

Raccoon led in 2022 and 2023, despite the fact that in 2022 law enforcement arrested one of its operators and dismantled its infrastructure. It reemerged in 2023 with a new version, however, the underground forum account managed by its operators went silent without warning in December 2023.

With Raccoon no longer actively for sale, its usage in producing endpoint logs essentially disappeared in 2024. Several stealers filled the resulting void, predominantly Lumma and Risepro.

Credentials

A unique credential set includes a previously unseen combination of email, username, password, and URL domain.

Compromised credentials

While this rise can largely be explained by advancement in Bitsight's credential collection capabilities, we assess that the precise number of credentials shared on the underground has also risen, fueled by increased data breaches and the spike in stealer logs.

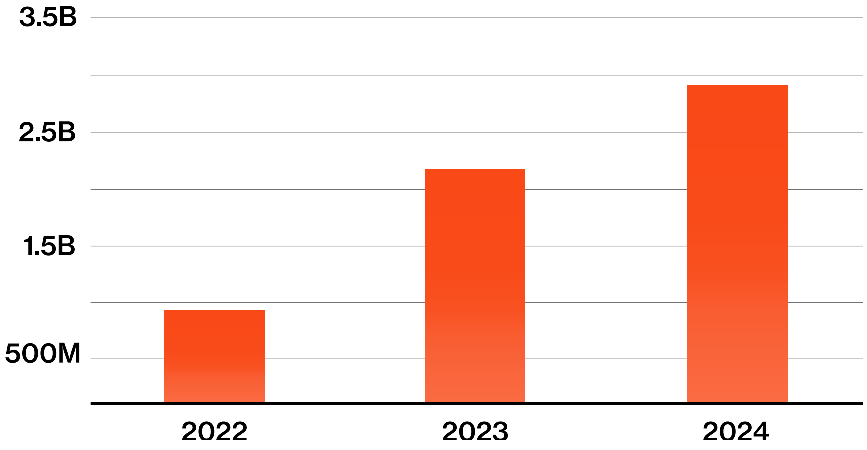


Figure 13. Number of leaked compromised credentials collected over the past three years.

Credit cards

In 2024, 14,468,620 compromised credit cards were listed for sale on underground markets. Notably, the number of cards rose nearly 20% over 2023's total (12,064,697), following an increase from 2022's total. The rise over the past three years has slightly reversed the precipitous decline that began after 2019, when the number of cards peaked at over 140 million.

Compromised credit cards

Remarkably, the number of US credit cards rose by over 4.5 million to 12,658,491, accounting for 80.7% of all compromised cards, vastly increasing from its share of 63.8% in 2023.

Indeed, the number of cards from the rest of the world declined by 1.6 million, so the rise of US cards was responsible for the uptick. If we separate US versus global numbers, we can see that the rise of compromised cards over the past three years appears to be solely an American problem.

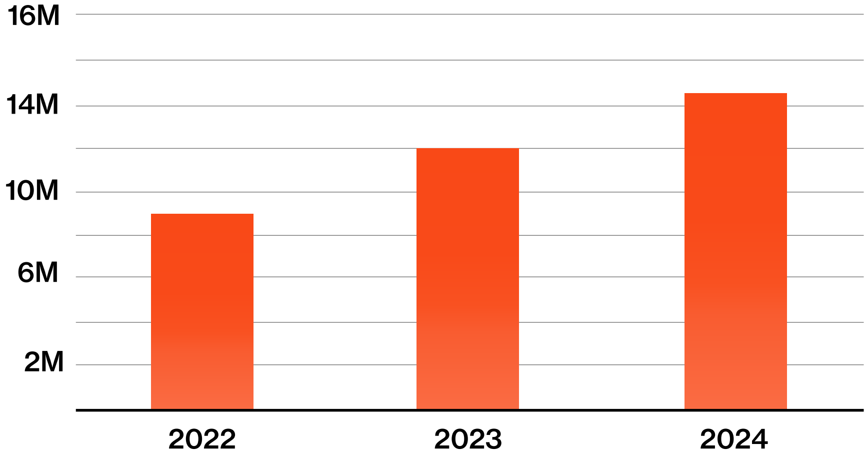


Figure 14. Number of compromised credit cards listed for sale on underground markets over the past three years.

Most logs per country

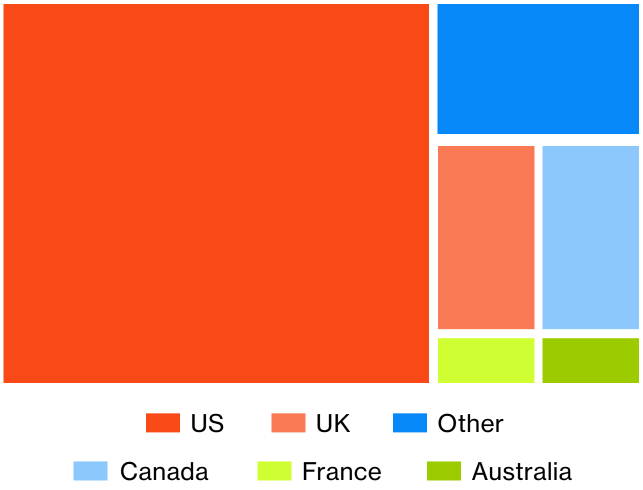


Figure 15. Compromised credit card share by country.

Top stealers for endpoint compromise

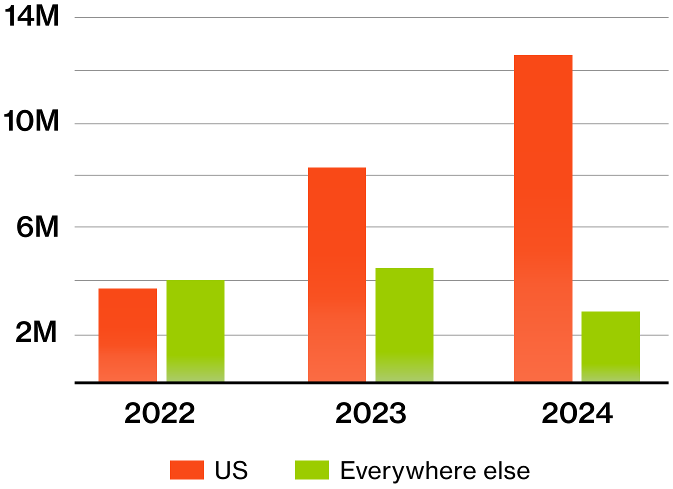


Figure 16. Number of compromised credit cards from the US versus global.

Dumps vs. CVV

The number of cards identified as dumps (i.e. those with magnetic strip data that were compromised at a physical point-of-sale) dropped to 6,253,969 in 2024 from 8,129,006 in 2023. Their average listing price rose from $10.5 to $12.80.

Meanwhile, the number of cards identified as CVV (i.e. those that include the 3 digit number, compromised in an e-commerce transaction) rose by nearly 130% to 7,774,042 in 2024 from 3,400,237 in 2023. Their average listing price was $11.45, up from $9.59 in 2023.

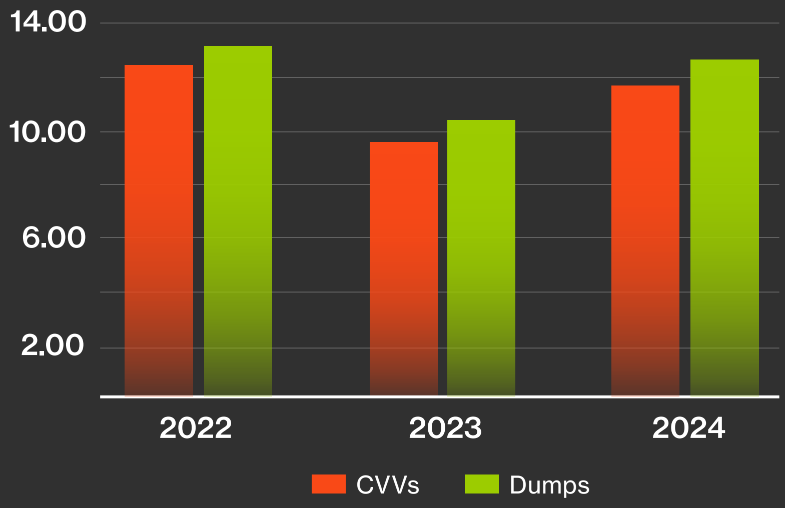


Figure 17. Number of endpoint logs listed for sale on underground markets.

+130%

increase in CVV-compromised cards, rising to 7.77M in 2024 from 3.4M in 2023; average price grew to $11.45 (up from $9.59).

57%

of listed US cards were CVVs, compared to just 15% globally—highlighting lower PoS compromise but widespread e-commerce fraud in the US.

The breakdown between CVVs and dumps was not uniform. In the US, CVVs comprised 57% of listed cards, while globally, CVVs accounted for only 15%. This ratio in the US could indicate that on one hand, PoS compromise is relatively lower due to the high penetration of EMV chips; however, e-commerce compromise is a very prevalent problem.

Vulnerabilities and exploits

The following CVEs received the highest DVE scores in 2024. Across the board, the most exposed devices were found in the US (with the exception of CVE-2024-37085 in China), and the most affected sectors were either Information (including telecommunications) and Professional, Scientific, and Technical Services (including security and software vendors).

CVE	PUBLICATION DATE	HIGHEST DVE SCORE	VENDOR	PRODUCT	MOST AFFECTED COUNTRY	MOST AFFECTED SECTOR
CVE-2024-21762	2/9/2024	10	Fortinet	FortiProxy	US	Information
CVE-2024-4577	6/9/2024	10	PHP	PHP	US	Professional, Scientific, and Technical Services
CVE-2024-23897	1/24/2024	10	Jenkins	Jenkins	US	Professional, Scientific, and Technical Services
CVE-2024-3400	4/12/2024	10	Palo Alto Networks	PAN-OS	US	Professional, Scientific, and Technical Services
CVE-2024-21887	1/12/2024	10	Ivanti	Connect Secure	US	Information
CVE-2024-1709	2/21/2024	9	ConnectWise	ScreenConnect	US	Information
CVE-2024-37085	6/25/2024	9	VMware	ESXi	CN	Information

Bitsight's DVE scoring engine predicts the likelihood of vulnerability exploitation by threat actors over the next 90 days, providing an accurate and real-time assessment of the immediate risks of each vulnerability based on threat actors' intent. This empowers customers to confidently rank their vulnerabilities and prioritize patching decisions in order of urgency and in light of real-time threat intelligence, allowing them to determine if a CVE is one of the 6% that demands immediate attention, or another distraction amid the noise of the 94%.

The DVE score is not dependent on NVD's scoring and rapidly updates to reflect the changing events in the cybercriminal underground. Scoring is robust, validated and transparent, backing each score with an audit trail detailing the rationale for the score and allowing customers to conduct independent investigations to gain deeper insight into the vulnerability's evolution.

Conclusion

Considering that big game ransomware remains the highest-impact cyberattack, any significant changes in the ransomware landscape are worth reiterating. The nearly 25% increase in the number of active gangs indicates that more actors possess the sophistication needed to carry out a successful attack. What was once the domain of the world's most advanced cybercriminals is becoming worryingly widespread.

If we were forced to make a prediction, we think that it's reasonable for these trends to continue. The knowledge of how to carry out an attack is spreading faster than law enforcement can shut down attack groups.

Furthermore, while ransomware groups may have targeted large organizations in the past in order to maximize payouts, these enterprises are better protected. Smaller organizations will continue to be increasingly appealing targets, because attackers know that many don't adequately invest in security.

We also recommend keeping a close eye on the geopolitical arena. As the post-Cold War order continues to go through an upheaval, the complicated relationships between the US, Russia, China, and Europe might alter the playing field for financially- and ideologically-motivated attackers. The world is becoming increasingly unpredictable. We are not going to be bold enough to tell you what we think will happen, but we do believe that fear, uncertainty, and doubt are a fertile breeding ground for cyberwarfare, cybercrime, and hacktivism.

Despite everything happening, however, best practices for defenders remain remarkably consistent. Employing defense-in-depth, multifactor authentication, backups, data segmentation, employee awareness, and using robust identity management, to name a few, can go a long way in preventing major attacks.

And remember, defensive capabilities are also improving, so it is possible for defenders to stay ahead in this arms race. Stay alert, use this report's insights, delve deeper into the report's data via the Pulse API, and produce the golden recommendations that your organization needs to stay safe. Thanks for reading, and let us know how we can help!

sales@bitsight.com

BOSTON (HQ)
RALEIGH
NEW YORK
LISBON
SINGAPORE

Bitsight is the global leader in cyber risk intelligence, helping teams make informed decisions with the industry's most extensive external data and analytics. With 3,400 customers and 65,000 organizations active on its platform, Bitsight delivers real-time visibility into cyber risk and threat exposure—enabling teams to quickly identify vulnerabilities, detect threats, prioritize actions, and mitigate risk across their extended attack surface.

BITSIGHT