

TRENDS FROM THE UNDERGROUND

H1 2023

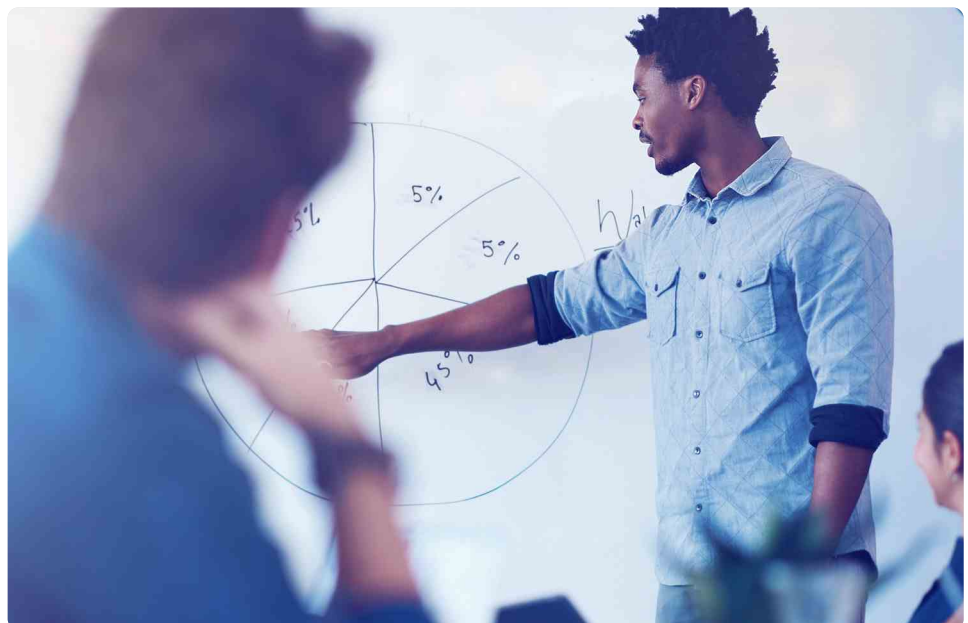




Introduction

As we head into the second half of 2023, its time to look back on the last six months and review what threat actors have been up to around the world. Unsurprisingly, we are witnessing further growth in ransomware attacks and vulnerability exposures, but we are also seeing a few notable changes in compromised credit card trends which were not as easy to predict.

Generative AI solutions continue to dominate the headlines as threat actors and cyber defenders alike rush to add AI capabilities to their arsenal to support their efforts in the never-ending cyber arms race. Earlier this year Cybersixgill launched IQ, our own generative AI solution that is proving to prop up efforts in the defenders' court. Simultaneously, over the past months, tens of thousands of ChatGPT login credentials have been offered for sale in underground forums, while threat actors have remained committed to their dedicated efforts to optimize the automation of malicious activity with AI.






The next 12 months are anticipated to be full of change. We expect to see cybersecurity vendors enhancing their technology and solutions at a much faster pace than ever before, while cybercriminals will undoubtedly increase their efforts to trade credentials on initial access broker markets (IABs) and deploy as-a-service solutions to bridge their own skills gaps.

The findings and data from our latest underground observations will hopefully inform your cybersecurity strategy for the remainder of the year, highlighting critical areas of focus and identifying key shifts in activity.

The key trends discussed in this report are:

A change in direction for credit card fraud	4
Ransomware attack trends including the ransomware groups dominating our headlines in 2023	6
Initial access broker market movements	11
Dark web forums vs. encrypted messaging apps	16
Vulnerability exposure trends including the top 10 vulnerabilities of 2023	21

 cybersixgill

Visit the Dark Lab Experience at Black Hat

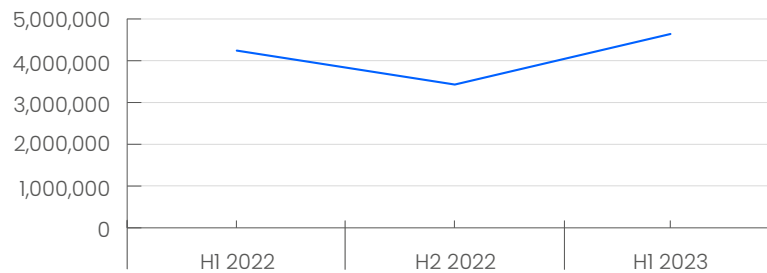
Join us at Business Meeting Room #485
5th-10th August



A change of direction for compromised credit cards

Over the past six months, the cyber threat landscape has experienced noteworthy shifts. One of the prominent developments is the end of the multiyear decrease in the number of compromised credit cards sold on the underground. From January to June 2023, the total number of compromised credit cards sold increased by 5.7% when compared with the previous 6 month period.

Number of global compromised credit cards collected



This upturn indicates a need for increased vigilance in protecting credit card information. Notably, the United States experienced a significant rise in compromised credit cards, surging from 1.9 million compromised cards sold in the second half of 2022 to a total of almost 3.1 million in the first half of 2023.

Conversely, the United Kingdom witnessed a substantial decrease, dropping from 559,991 in the latter half of 2022 to 152,000 in the first six months of 2023, indicating improved security measures or perhaps a change in focus by cybercriminals to target lower-hanging fruit.

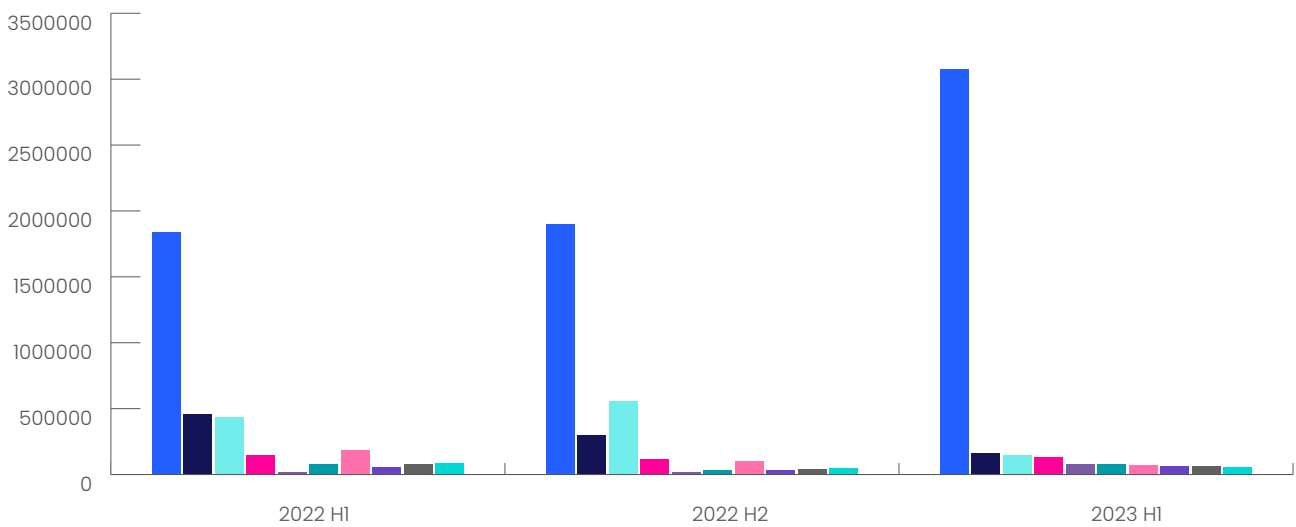
Another significant development is the emergence of Brazil as the second-highest



country in terms of compromised credit cards, with a total of 162,934 cards sold in the first half of 2023.

These shifts underscore the dynamic global nature of the underground credit card fraud market and the continuous need for adaptive security measures to combat evolving cybercriminal tactics.

Compromised Credit Cards Recorded By Country



Top 10

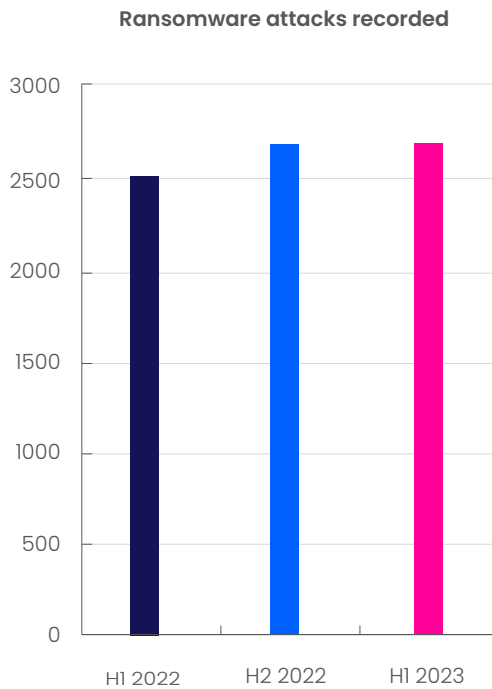
- USA
- UK
- Netherlands
- Mexico
- Australia
- Brazil
- Canada
- Spain
- Germany
- Italy



Ransomware attack trends

Between Jan-June 2023, Cybersixgill recorded 2,713 ransomware attacks, which is slightly higher than the 2,702 attacks recorded in the second half of 2022.

In terms of the top ransomware attacks and gangs, Lockbit maintains its position as the most prominent group with a total of 639 attacks, followed by Clop with 424 attacks, and Alphv with 251 attacks.





Ransomware attacks targeting companies in 2023

During the last 6 months, we have been witness to a number of ransomware attacks across multiple industries. The table below provides an example of some of the activity we have observed by month.

Info	Victim	Description
<p>Month - January</p> <p>Gang - ALPHV</p>	<p>The Federal Institute of Pará (IFPA)</p> <p>Industry: Public Education</p> <p>Location: Brazil</p>	<p>In January 2023, IFPA (Instituto Federal Do Pará) experienced a ransomware attack, compromising and exfiltrating sensitive data belonging to both employees and students.</p> <p>The attackers threatened to publish and sell the data after the institute ignored their ransom demands. The ransom sum has not yet been disclosed and the IFPA have not yet released a statement regarding the attack.</p>
<p>Month - February</p> <p>Gang - LOCKBIT</p>	<p>La Segunda Seguros CLSG</p> <p>Industry: Insurance</p> <p>Location: Argentina</p>	<p>In February 2023, La Segunda Seguros CLSG, an insurance company based in Rosario, Argentina, fell victim to a ransomware attack. During the attack, the company's servers were blocked, and its data stolen.</p> <p>The compromised data included insurance information, personal customer data (including passports, legal documents and medical records) and details about insured properties. The attackers threatened to publish over 100,000 files to the public if the company refused to pay the ransom, demanding a payment of \$6,000,000 to decrypt the network and delete the stolen data.</p> <p>The compromised data was leaked on February 28th, causing significant disruption to La Segunda Seguros CLSG's operations and exposing 52GB of sensitive company data.</p>



Info	Victim	Description
<p>Month - March Gang - EVEREST</p>	<p>XEFI Industry: IT Services Location: France</p>	<p>In March 2023, the French IT services company XEFI was hit by a ransomware attack by the Everest group. The company's files were encrypted and the ransomware gang demanded a payment of €1 million to recover the files, which included customer records, employee data, and financial information. Everest threatened to publicly expose the stolen data if the ransom demands were not met.</p> <p>XEFI refused to pay the ransom, resulting in the publication of the stolen data on the dark web. Eventually, XEFI was able to restore its systems from backups, but the attack caused significant damage to the company's reputation and finances. The company was forced to pay for credit monitoring for its customers, and it also incurred the cost of investigating the attack and the implementation of new security measures.</p>
<p>Month - April Gang - LOCKBIT</p>	<p>TF-AMD Microelectronics (Penang) Sdn. Bhd. Industry: Computing Location: Malaysia</p>	<p>On April 5, 2023, LockBit gained unauthorized access to the company's systems and stole a significant amount of confidential data and intellectual property, including postal censuses, financial documents, contracts with customers, technical documentation of developments from major companies like AMD and Nokia, software solutions for chips, and drawings of the chips themselves.</p> <p>The stolen data also included information about processors used in the development of space carriers. The ransomware gang threatened to publish part of the stolen data to the public if a ransom was not paid, and sell the rest on the underground black market. The ransomware gang offered the victim organization options to resolve the attack, including extending the timer for 24 hours for a payment of \$2,000, destroying all information for a payment of \$14,793,870, or downloading the data at any moment for the same payment of \$14,793,870.</p> <p>On June 4th, LockBit announced on their dark web dedicated leak site that all files had been published.</p>



Info	Victim	Description
<p>Month - May</p> <p>Gang - CLOP</p>	<p>Several organizations across multiple industries - including:</p> <p>Zellis BBC Aer Lingus Boots British Airways Harvard Pilgrim Health Care Curry County, Oregon (government) City of Atlanta, Georgia (government) Norwegian University of Science and Technology (education) NTT Ltd. (information technology) Universal Health Services (healthcare) Swissquote Bank (finance) Norsk Hydro (energy) JBS (food processing) Kaseya (software)</p>	<p>On May 27, 2023, the Clop ransomware gang began actively exploiting a zero-day vulnerability in Progress Software's MOVEit Transfer technology - used by many organizations to exchange sensitive data and large files - to gain access to victim networks. Once inside, the ransomware encrypted the victim's files and demanded ransom payment of between \$1 million and \$5 million to recover the stolen data.</p> <p>On June 5, 2023, a representative of the Clop gang confirmed their role in the series of attacks. In subsequent weeks, the gang began listing some of the affected organizations on the group's dark web dedicated leak site, which steadily climbed to 137 companies by June 29th.</p> <p>Clop has published data stolen from some of its victims. In a few cases, the data has been published on the dark web, while in other cases it has been published on social media. The data that has been published includes sensitive information such as customer records, employee data, and financial information. The attack remains ongoing as of July 10th, 2023.</p>
<p>Month - June</p> <p>Gang - ALPHV</p>	<p>Barts Health NHS Trust</p> <p>Industry: Healthcare</p> <p>Location: UK</p>	<p>On June 30th, 2023, the Alphv ransomware gang announced that it had compromised over 70TB of data from UK-based healthcare organization Barts Health NHS Trust.</p> <p>The gang published a selection of files purportedly stolen from Barts Health, including copies of employees' driving licenses and passports, in addition to internal emails and correspondence marked confidential. In broken English, the hackers claimed on their dark web page that the haul of data from Barts Health amounted to the "most bigger leak from health care system in UK."</p> <p>Alphv gave given the victim 3 days to comply with their ransom demands.</p>



Initial access broker market movements

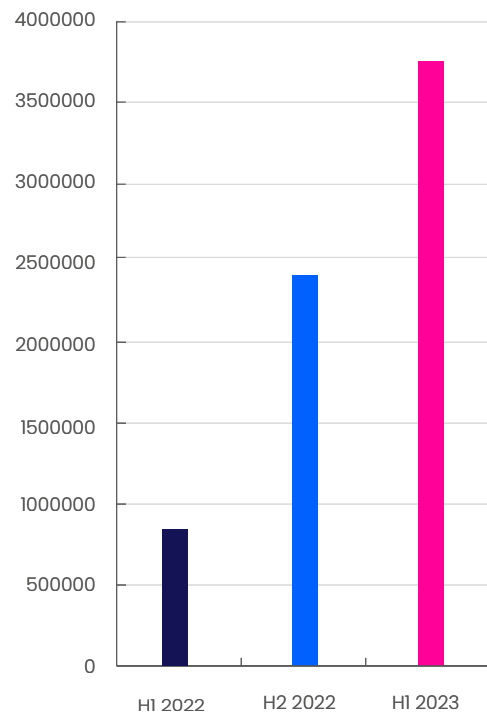
Initial access broker markets (IABs) play a pivotal role in the cybercriminal underground ecosystem by providing a platform for the sale of compromised access to target networks. These markets enable threat actors to bypass the arduous and time-consuming process of establishing an initial foothold within a network.

Cybercriminals can purchase pre-established access points, such as compromised endpoints, corporate logins, web shells, CPanel, or remote protocols like RDP and FTP, to expedite their attacks.

In recent years, initial access broker markets have experienced exponential growth due to the surging demand for outsourced access. This underground economy has become increasingly lucrative, leading to the creation of two distinct market categories: initial access broker markets and wholesale access markets (WAMs). IABs offer access to enterprise networks for hundreds to thousands of dollars, while WAMs sell access to singular compromised endpoints for around \$10 apiece.

Observing trends from previous years, it is evident that the market for compromised access credentials has been expanding rapidly. In 2021, over 4.5 million access vectors were sold, highlighting the rising demand for outsourced initial access within the cybercriminal community. This trend continued into 2022, with approximately 10.3 million initial access vectors sold on a single market alone.

Number of credentials for sale on a single IAB market





Analyzing the data from the first six months of 2023, Cybersixgill has once again observed a significant surge in the availability of compromised endpoints for sale across the cybercriminal underground, with a total of 3,736,387 compromised endpoints advertised for sale between January and June. This represents a substantial increase of 59.7% compared to the second half of 2022. This increase has been potentially fueled by the escalating demand for outsourced entry points into corporate networks.

Furthermore, the data indicates a concerning trend of increasing accessibility and affordability of compromised access credentials. As the number of brokers and listings continues to rise, the prices for these credentials decrease, enabling a broader range of threat actors to engage in cyberattacks. This accessibility, coupled with the advancement of AI models like ChatGPT that lower technical barriers of entry for pre-ransomware activities and the establishment of initial access vectors, presents a substantial challenge for organizations defending their environments.





Our threat intelligence collection is 100% automated, meaning we are able to collect more threat data from the clear, deep and dark web than our competitors. We index over 10 million new intelligence items - including messages from dark web forums and Telegram daily.

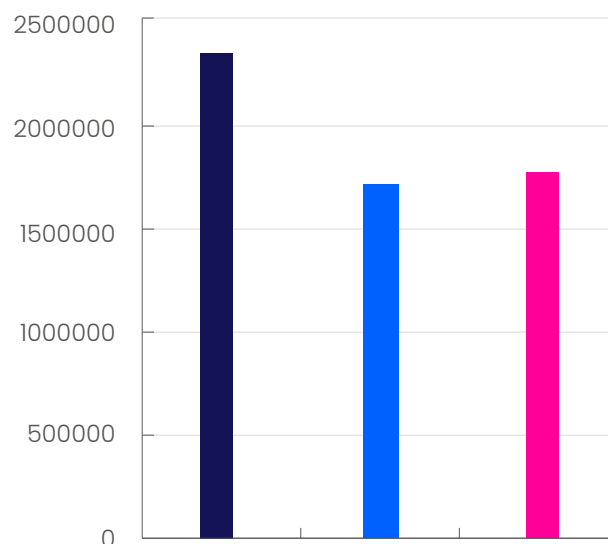
Dark web forums vs. encrypted messaging apps

The underground cybercriminal landscape has witnessed a notable shift in recent years, with threat actors increasingly utilizing encrypted messaging platforms alongside traditional dark web forums. These encrypted messaging platforms, such as Telegram and Discord, have emerged as important hubs for cybercriminal activities, enabling collaboration, communication, and the exchange of illicit goods and services.

Between 2019 and 2020, there was a substantial 730% increase in the number of items collected by Cybersixgill from encrypted messaging platforms. Although the growth rate slowed to 338% from 2020 to 2021, the data from 2022 still reflects a significant 23% increase, with a staggering 1,967,643,024 items collected from messaging platforms during that year.

In contrast, dark web forums experienced a decline in activity during the same period. The total number of forum posts and replies decreased by 13% between 2021 and 2022. However, it's important to note that while the number of active participants in the top forums slightly decreased by 4%, in the first half of 2023 the participants became more active, leading to an increase of 2.9% in posts on these forums.

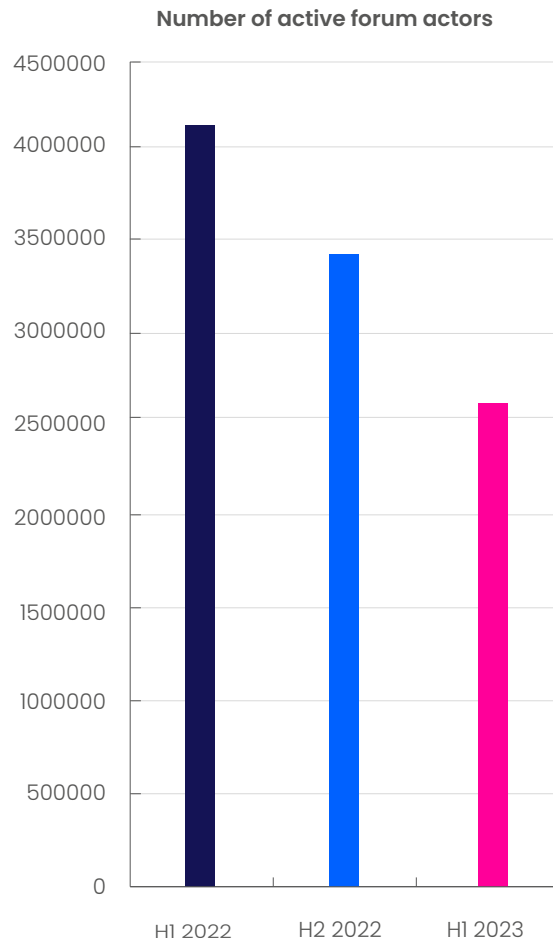
Number of Forum Posts Collected From The Dark Web





Active threat actors on dark web forums

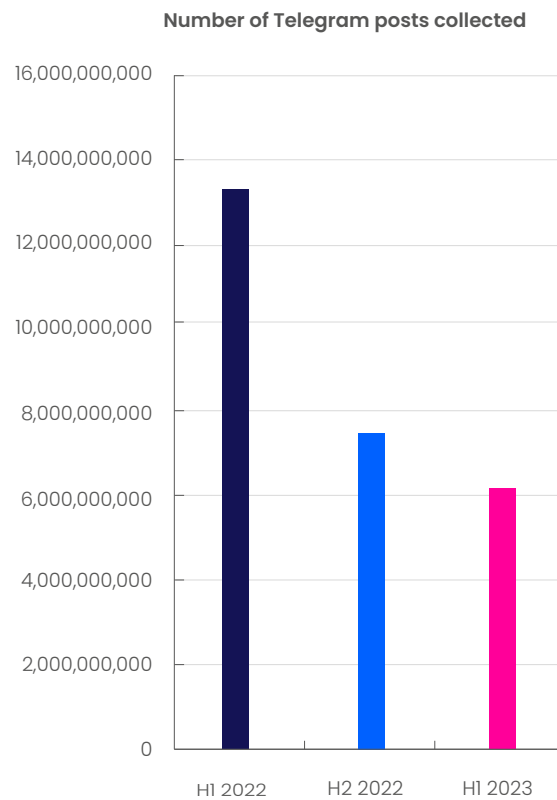
Analyzing the data from the first half of 2023, Cybersixgill observed a decline in the total number of active forum actors in the largest 10 forums. This can be attributed to several forums closing down, such as Raidforums and Breached (with the latter resurfacing in early June). However, there was a slight rebound in the number of forum posts, increasing by 3% compared to the second half of 2022.





Telegram posts

There was a decrease in the number of Telegram posts in the first half of 2023 compared to the second half of 2022. However, the most significant decrease occurred within 2022 itself, primarily due to the internal cleaning of spam-inundated Telegram groups, as well as restrictive measures implemented by the Chinese regime to prevent users from bypassing the 'Great Firewall.'



These trends underscore the evolving dynamics of cybercriminal activities. While dark web forums remain the central sphere of operations for experienced threat actors with advanced technical expertise, the accessibility, automated functionalities, and ease of use offered by messaging platforms have attracted a growing number of novice threat actors looking to break into the cybercrime industry. Setting up a channel on platforms like Telegram is quick and straightforward, lowering the entry barrier for these newcomers.



The DVE score forms part of our DVE Intelligence solution that correlates asset exposure and impact severity data with unique real-time vulnerability exploit intelligence from the deep and dark web. The DVE score indicates the likelihood of a vulnerability being exploited and is updated in real-time as events unfold on the cybercriminal underground.

Vulnerability exposures

The exploitation of software vulnerabilities and exposures continues to be a significant avenue for cybercriminals to gain initial access to target systems. The data from the first half of 2023 highlights several vulnerabilities that have attracted attention and are deemed high-risk, with three having reached a perfect DVE score of 10/10.

The amplification of the threat posed by vulnerability exposures in recent years is directly linked to the acceleration of global digitization efforts in the wake of the COVID-19 pandemic. As individuals, businesses, and governments embrace digital technologies and remote work practices to streamline operations, enhance connectivity, and improve services, the attack surface expands accordingly. Digital transformation, while providing numerous benefits, has also created a fertile ground for malicious threat actors.

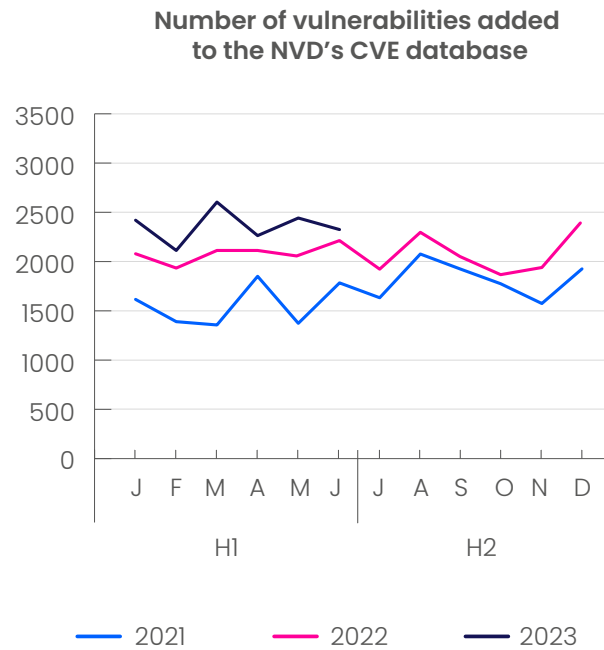
Every device or system that is connected to the organizational network presents cybercriminals with a potential entry point for attack.

Moreover, the interconnected nature of modern systems further amplifies the potential impact of vulnerability exploitation. With the proliferation of connected devices and the integration of various technologies, the consequences of a single vulnerability in a widely used product or platform can be far-reaching. This interconnectedness creates a domino effect, where the exploitation of one vulnerability can propagate through networks and compromise the security of multiple entities. Such vulnerabilities have the potential to affect countless users and organizations, leading to data breaches, financial losses, and disruptions to critical services down the supply chain.



The persistent rise of identified vulnerabilities

The increasing number of vulnerabilities discovered month-over-month in recent years - as recorded in the NVD CVE database - serves as irrefutable evidence of the growing risk of exposure faced by organizations in the digital era. Year-over-year, there is a clear and consistent rise in the number of discovered vulnerabilities.



In the first half of 2023, the NVD recorded 14,227 new vulnerabilities - marking an increase of 11% from H2 2022 to H1 2023, and bringing the total number of discovered vulnerability exposures to 219,164¹. These figures demonstrate a consistent gradual upward trend, and serve as a direct illustration of the growing magnitude of the challenge organizations face in mitigating the risk of vulnerability exposures.

¹Data correct as of 5th July 2023



By assessing vulnerabilities based on their risk - considering factors such as affected organizational systems, potential impact, available compensating controls, likelihood of exploitation, and urgency - organizations can focus their efforts on addressing the most critical exposures. Cybersixgill's DVE Intelligence automates this process, instantly prioritizing the vulnerabilities that pose the greatest risk, using real-time threat intelligence from the cybercriminal underground.

Zero day vulnerabilities

This challenge is further compounded by 'zero day' vulnerabilities that are not yet known to software developers or the broader cybersecurity community. They are highly valuable to cybercriminals because they can exploit them before developers have a chance to generate and distribute patches or mitigation measures. By their very nature, zero-day vulnerabilities do not have a CVE ID assigned to them, making them particularly challenging to track and address.

Zero-day vulnerabilities can have severe consequences. Malicious actors actively search for these vulnerabilities to gain unauthorized access, steal sensitive information, launch ransomware attacks, or disrupt critical services. The clandestine nature of zero-day vulnerabilities allows attackers to maintain an element of surprise, making them difficult to defend against. Without proactive threat intelligence from the epicenter of cybercrime, organizations are helpless to defend against zero-day vulnerability exploitation, left with little to no time to implement effective countermeasures.

It is no longer possible, feasible or necessary to patch every vulnerability exposure discovered within the organizational attack surface due to resource constraints, cost considerations, disruption to business operations, and the quantity discovered. According to Gartner, an estimated 6% of vulnerability exposures are actually weaponized and exploited by cybercriminals in attack. Given these factors, it is critical that organizations shift from indiscriminate patching processes to risk-based vulnerability prioritization.



The top 10 highest ranking vulnerabilities, H1 2023

	HIGHEST DVE SCORE	CVSS 3.1	DESCRIPTION
CVE-2023-28252	10	7.8	<p>CVE-2023-28252 is a Windows Common Log File System Driver Elevation of Privilege Vulnerability.</p> <p>This CVE is known to be related to several advanced persistent threats (APTs) including Lunar Spider, APT37, AridViper, Tick, and YoroTrooper. It has a proof-of-concept (POC) exploit available and is trending on Twitter and GitHub. The highest DVE score recorded for this CVE was 10/10.</p>
CVE-2023-27350	10	9.8	<p>CVE-2023-27350 is a vulnerability that allows remote attackers to bypass authentication on affected installations of PaperCut NG 22.0.5 (Build 63914). This vulnerability does not require authentication to exploit.</p> <p>The flaw exists within the SetupCompleted class and is a result of improper access control. An attacker can leverage this vulnerability to bypass authentication and execute arbitrary code in the context of SYSTEM. The CVE currently has a high DVE score of 10.0, indicating a high chance of exploitation. It is also known to be related to APTs such as Charming Kitten, BlackCat, Skeleton Spider, The Mask, and BianLian.</p>
CVE-2023-23397	10	9.8	<p>CVE-2023-23397 is a Microsoft Outlook elevation of privilege vulnerability. It is known to be related to several APTs, including RECESS SPIDER, APT37, APT29, UNC2452, and Sofacy.</p> <p>This CVE has a proof-of-concept exploit and is trending in the cyber underground as well as on GitHub. It is also known to be related to a ransomware attack and has been exploited in the wild. The highest DVE score recorded for this CVE was 10/10 on 2023-03-16, however this has now reduced to 3.03.</p>



	HIGHEST DVE SCORE	CVSS 3.1	DESCRIPTION
CVE-2023-21716	9.94	9.8	<p>CVE-2023-21716 is a Microsoft Word remote code execution vulnerability. It is known to be related to several APTs including LEAD, Medusa, BianLian, Cutting Kitten, and Cobalt.</p> <p>This CVE has a proof-of-concept exploit and is associated with a ransomware attack and has been exploited in the wild. The highest DVE score recorded for this CVE is 9.99, on 2023-03-16, however this has now reduced to 2.24.</p>
CVE-2023-21554	9.94	9.8	<p>CVE-2023-21554 is a Microsoft message queuing remote code execution vulnerability. It is known to be related to several APTs, including Lazarus Group, APT37, RECESS SPIDER, AridViper, and Tick.</p> <p>This CVE has a proof-of-concept exploit and is associated with a ransomware attack. It has been observed being actively exploited in the wild and is considered a serious threat. The current DVE score for CVE-2023-21554 is 9.68, which is relatively high, indicating a high likelihood of exploitation.</p>
CVE-2023-23397	9.93	9.8	<p>CVE-2023-27997 is a heap-based buffer overflow vulnerability that affects FortiOS versions 7.2.4 and below, 7.0.11 and below, 6.4.12 and below, and 6.0.16 and below, as well as FortiProxy versions 7.2.3 and below, 7.0.9 and below, 2.0.12 and below, and all versions of 1.2 and 1.1. This vulnerability allows a remote attacker to execute arbitrary code or commands by sending crafted requests to the SSL-VPN.</p> <p>This CVE is known to be related to several APTs including MuddyWater, COSMIC WOLF, Skeleton Spider, Everest, and Team Jorge. It has a proof-of-concept exploit available and has been trending on Twitter, in the cyber underground, and on GitHub. The current DVE score for this CVE is 9.66, which is relatively high, indicating a high likelihood of exploitation.</p>



	HIGHEST DVE SCORE	CVSS 3.1	DESCRIPTION
CVE-2023-21674	9.91	9.8	<p>CVE-2023-21674 is a Windows advanced local procedure call (ALPC) elevation of privilege vulnerability. It is known to be related to several APTs, including Aquatic Panda, Nemesis Kitten, PROMETHIUM, and LEAD. This CVE is associated with a ransomware attack that has been exploited in the wild and is linked to at least one APT.</p> <p>The highest recorded DVE score for this vulnerability was 9.91, however this has now reduced to 1.54, suggesting the likelihood of this CVE being exploited is relatively low.</p>
CVE-2023-25717	9.9	9.8	<p>CVE-2023-25717 is a vulnerability that allows for remote code execution in Ruckus Wireless Admin through version 10.4. It can be exploited via an unauthenticated HTTP GET request. This vulnerability has a proof of concept exploit and is known to be related to a ransomware attack. It has been observed being exploited in the wild and is associated with several advanced persistent Threats such as COBALT JUNO, BITWISE SPIDER, Stone Panda, and Aquatic Panda.</p> <p>The current DVE score for the CVE is 9.75, which is relatively high. This suggests a high likelihood of this CVE being exploited in attack. The highest recorded DVE score for this vulnerability was 9.9.</p>
CVE-2023-24055	9.9	5.5	<p>CVE-2023-24055 is a vulnerability that affects KeePass versions up to 2.53. In a default installation, an attacker with write access to the XML configuration file can obtain cleartext passwords by adding an export trigger. It is known to be related to several APTs such as LEAD, Cobalt, PLATINUM, Royal, and APT32.</p> <p>However, the vendor's position is that the password database is not intended to be secure against an attacker who has that level of access to the local PC.</p> <p>The CVE currently has a relatively low DVE score of 0.34, indicating a lower chance of exploitation. The highest DVE score reported for this CVE was 9.9.</p>



	HIGHEST DVE SCORE	CVSS 3.1	DESCRIPTION
CVE-2023-23752	9.89	5.3	<p>CVE-2023-23752 is a vulnerability discovered in Joomla! versions 4.0.0 through 4.2.7. It is categorized as an improper access check issue, which allows unauthorized access to webservice endpoints.</p> <p>This vulnerability has a proof of concept exploit and is known to be related to a ransomware attack. It has been observed being exploited in the wild and is associated with several APTs such as COBALT JUNO, BITWISE SPIDER, Stone Panda, and Aquatic Panda.</p> <p>The CVE currently has a low DVE score of 0.2, indicating a low chance of exploitation. The highest DVE score reported for this CVE was 9.89.</p>



Honorable mention

While not included in the top 10 highest scored CVEs for the first half of 2023, CVE-2023-34362 – also known as the MOVEit vulnerability – has attracted significant attention due to the activities of the Clop group. Associated with multiple APTs, the presence of proof-of-concept exploits and Metasploit modules underscores the seriousness of this vulnerability.

	HIGHEST DVE SCORE	CVSS 3.1	DESCRIPTION
CVE-2023-34362 MoveIT	9.79	9.8	<p>CVE-2023-34362 is a SQL injection vulnerability found in the MOVEit Transfer web application. It affects versions of MOVEit Transfer before 2021.0.6, 2021.1.4, 2022.0.4, 2022.1.5, and 2023.0.1. This vulnerability allows an unauthenticated attacker to gain access to the MOVEit Transfer’s database. Depending on the database engine being used, the attacker may be able to infer information about the database structure and contents and execute SQL statements to alter or delete database elements.</p> <p>The exploitation of CVE-2023-34362 has been observed in the wild in May and June 2023, with an estimated 150 organizations affected via the Clop ransomware group alone. Clop have been actively targeting organizations worldwide and have a history of leveraging vulnerabilities to gain unauthorized access to systems and deploy their ransomware</p> <p>This CVE is also related to several APTs including QUILTED TIGER, Team Jorge, BlackCat, Skeleton Spider, and FSB 16th & 18th Centers. These APTs are known for their sophisticated and targeted cyber attacks.</p> <p>There is a proof-of-concept exploit available for CVE-2023-34362, as well as a Metasploit module. This indicates that the vulnerability has gained attention in the cyber underground and is actively being discussed and potentially weaponized. This CVE remains high-risk, being discussed and potentially weaponized. This CVE remains high-risk.</p>



Summary

The increase in activity identified within this report highlights the importance of embracing proactive cybersecurity programs and processes that automate security activities. This requires real-time insight into the threats, tactics, tools and procedures emerging from the cybercriminal underground - insight that not all threat intelligence vendors, or tools purported to be embedded with threat intelligence are able to provide.

The critical importance of context-rich threat intelligence, particularly from the deep and dark web cannot be overemphasized. These hidden corners of the internet are the epicenter of cybercriminal discourse and activity, including the sale and trade of stolen credit card information, the transaction of ransomware infrastructure and technology, and the flourishing initial access broker markets. By actively monitoring and analyzing these underground platforms, organizations can gain early indicators of potential attacks before they can materialize.

About Cybersixgill

Cybersixgill continuously collects and exposes the earliest possible indications of risk, moments after they surface on the clear, deep and dark web. Our proprietary algorithms extract data from a wide range of sources, including content from limited-access deep and dark web forums, underground markets, invite-only messaging groups, code repositories, paste sites and clear web platforms, as well as an unparalleled archive of indexed, searchable historical data from as early as the 1990s. This data is processed, correlated and enriched with machine learning techniques to create profiles and patterns of malicious threat actors and their peer networks, and deliver critical insight into the nature, source and context of each threat.

Our extensive body of threat intelligence data can be consumed through various solution offerings and integrations, each addressing critical customer pain points and use cases. These solutions are scalable, searchable and seamlessly integrated into existing security stacks, quickly arming enterprises, government and MSSPs alike with accurate, relevant and actionable insights to proactively block threats before they materialize into attacks.

Learn more at www.cybersixgill.com

Follow us



cybersixgill