

DATA	TARGET	DESCRIZIONE	TIPO	OBBIETTIVO	CLASSE ATTACCO	POSIZIONE GEOGRAFICA	RECORD INTERESSATI
1/4/2023	Twitter	A threat actor released a data set consisting of 200 million Twitter profiles for approximately \$2.	API vulnerability	Information and communication	Cyber Crime	US	200,000,000.00
1/10/2023	Undisclosed marketing provider in Japan	The Japanese customers of two large insurance companies, Aflac and Zurich, have their personal information leaked after the breach of a third-party service provider. It is unclear if the breaches are related and the service provider is the same.	Vulnerability in a file transfer server	Finance and insurance	Cyber Crime	JP	2,100,000.00
1/19/2023	T-Mobile	T-Mobile discloses a new data breach after a threat actor stole the personal information of 37 million current postpaid and prepaid customer accounts through one of its Application Programming Interfaces (APIs).	API Vulnerability	Information and communication	Cyber Crime	US	37,000,000.00
1/24/2023	DuoLingo	Language learning platform DuoLingo says it is investigating a post on a hacking forum offering information on 2.6 million customer accounts for \$1,500.	Misconfiguration	Education	Cyber Crime	US	2,600,000.00
1/30/2023	CommuteAir	A U.S. No Fly list with over 1.5 million records of banned flyers and upwards of 250,000 'selectees' is shared publicly on a hacking forum.	Misconfiguration	Transportation and storage	Cyber Crime	US	1,750,000.00
2/1/2023	Heritage Provider Network	Multiple medical groups in the Heritage Provider Network in California suffer a ransomware attack, exposing sensitive patient information to cybercriminals.	Malware	Human health and social work	Cyber Crime	US	3,300,000.00
2/3/2023	PeopleConnect	PeopleConnect, the owners of the TruthFinder and Instant Checkmate background check services, confirm they suffered a data breach after hackers leaked a 2019 backup database containing the info of 20 millions of customers.	Inadvertent leak	Professional, scientific and technical	Cyber Crime	US	20,000,000.00
2/8/2023	Weee!	The Weee! Asian and Hispanic food delivery service suffers a data breach exposing the personal information of 1.1 million customers.	Unknown	Accommodation and food service	Cyber Crime	US	1,100,000.00
2/10/2023	AT&T	A threat actor named IntelBroker claims to have found a third-party vendor's unsecured cloud storage containing 37 million AT&T client records. The threat actor shares a sample of 5 million records.	Misconfiguration	Information and communication	Cyber Crime	US	37,000,000.00
2/10/2023	Verizon	IntelBroker leaks a database, allegedly from Verizon, for free, containing 7.5 million clients' records, only first names, device types (Apple or Android), and service plans. Verizon verified that the data leak was legitimate and originated from a vendor which creates videos to assist clients.	Unknown	Information and communication	Cyber Crime	US	7,500,000.00
2/13/2023	Community Health Systems	Community Health Systems estimates that 1 million patients have been impacted by the GoAnywhere breach.	CVE-2023-0669 Vulnerability	Human health and social work	Cyber Crime	US	1,100,000.00
2/16/2023	MySejahtera	The personal information of three millions of MySejahtera users is exposed after an account authorised for vaccine administration stole data from three million vaccine recipients.	Account Takeover	Human health and social work	Cyber Crime	MY	3,000,000.00
2/20/2023	RailYatri	RailYatri, a popular Indian train ticket booking platform, suffers a massive data breach that exposes the personal information of over 31 million (31,062,673) users/travellers.	Unknown	Transportation and storage	Cyber Crime	IN	31,000,000.00
3/1/2023	Unknown target(s)	Researchers from Cyble reveal that the carding marketplace known as BidenCash has leaked online a free database of 2,165,700 debit and credit cards in celebration of its first anniversary.	Unknown	Finance and insurance	Cyber Crime	>1	2,165,700.00
3/6/2023	Undisclosed marketing vendor	AT&T notifies roughly 9 million customers that some of their information was exposed after a marketing vendor was hacked in January.	Unknown	Administration and support service	Cyber Crime	US	9,000,000.00
3/8/2023	HDB Financial Services	A hacker using the alias Kernelware leaks 7.5 GB of customer data with over 72 million entries belonging to HDB Financial Services, a subsidiary of India's largest private bank, HDFC Bank.	Unknown	Finance and insurance	Cyber Crime	IN	72,000,000.00
3/10/2023	Zoll Medical	Medical technology developer Zoll Medical notifies roughly one million individuals that their personal information might have been compromised in a recent data breach.	Unknown	Professional, scientific and technical	Cyber Crime	US	1,004,443.00
3/14/2023	Independent Living Systems (ILS)	Independent Living Systems (ILS), a Miami-based healthcare administration and managed care solutions provider, discloses a data breach that exposed the personal information of 4,226,508 individuals.	Unknown	Human health and social work	Cyber Crime	US	4,226,508.00
3/23/2023	ID Tech	Attackers steal the personal data of about one million of users from kids' tech coding camp ID Tech.	Unknown	Education	Cyber Crime	US	1,000,000.00
3/27/2023	Multiple organizations in India	Indian police arrests six members of an alleged criminal gang that sold the personal data of 168 million Indian citizens, including defense personnel and government employees.	Unknown	Multiple Industries	Cyber Crime	IN	168,000,000.00
3/27/2023	Latitude Financial Services	Australian financial services company Latitude Financial Services reveals that personal information of approximately 14 million individuals might have been compromised in a data breach.	Unknown	Finance and insurance	Cyber Crime	AU	14,000,000.00
3/30/2023	TMX Finance	TMX Finance and its subsidiaries TitleMax, TitleBucks, and InstaLoan have collectively disclosed a data breach that exposed the personal data of 4,822,580 customers.	Unknown	Finance and insurance	Cyber Crime	CA	4,822,580.00
3/31/2023	Blauw	Blauw, a dutch marketing firm suffers a data breach affecting 1.5 million individuals.	Unknown	Professional, scientific and technical	Cyber Crime	NL	1,500,000.00
4/1/2023	Unnamed Thai Government Agency	A hacker named "9Near" claims to have stolen the personal data of 55 million Thai citizens from an unnamed Government agency.	Unknown	Public admin and defence, social security	Hacktivism	TH	55,000,000.00
4/13/2023	NationsBenefits Holding	NationsBenefits Holding files a notice of data breach after learning that the company and its customers were affected by the third-party data breach at Fortra.	CVE-2023-0669 Fortra GoAnywhere MFT Vulnerability	Finance and insurance	Cyber Crime	US	3,000,000.00
4/20/2023	American Bar Association (ABA)	The American Bar Association (ABA) discloses a data breach after hackers compromised its network and gained access to older credentials for 1,466,000 members.	Unknown	Professional, scientific and technical	Cyber Crime	US	1,466,000.00
4/23/2023	Terravision	The Airport transfers service Terravision suffers a data breach, exposing over 2M records of customer data including names, phone numbers, email addresses, salted password hashes and in some cases, date of birth and country of origin.	Unknown	Transportation and storage	Cyber Crime	IT	2,000,000.00
4/25/2023	Unknown organization in China	Unknown threat actors post a massive data set on a Russian forum, allegedly offering the opportunity to buy sensitive details of over 630 million users from China.	Unknown	Unknown	Cyber Crime	CN	640,000,000.00
4/26/2023	Individuals in Eastern Europe	The Cyber Police of Ukraine arrests a man for selling the personal data of more than 300 million individuals stolen via closed groups and channels in Telegram. Stolen information includes Ukrainian and European passport, taxpayer and driver's license numbers, as well as bank account data and birth certificates	Account Takeover	Individual	Cyber Crime	>1	360,000,000.00

4/28/2023	NextGen Healthcare	NextGen Healthcare, a U.S.-based provider of electronic health record software, admits that hackers breached its systems and stole the personal data of 1.05 million patients.	Account Takeover	Professional, scientific and technical	Cyber Crime	US	1,005,000.00
5/11/2023	Brightly	Software maker Brightly confirms that hackers stole close to three million SchoolDude user accounts in an April data breach.	Malware	Professional, scientific and technical	Cyber Crime	US	3,000,000.00
5/12/2023	PharMerica	PharMerica, one of the largest pharmacy service providers in the United States has confirmed that hackers accessed the personal data of almost six million patients.	Malware	Wholesale and retail	Cyber Crime	US	5,800,000.00
5/19/2023	Luxtotta	Luxtotta confirms that one of its partners suffered a data breach in 2021 that exposed the personal information of 70 million customers after a database was posted for free on hacking forums.	Unknown	Manufacturing	Cyber Crime	IT	70,000,000.00
5/22/2023	Apria Healthcare	Apria Healthcare notifies over 1.8 million patients and employees that their personal, financial and health data was accessed during a systems hack.	Unknown	Human health and social work	Cyber Crime	US	1,800,000.00
5/24/2023	Harvard Pilgrim Health Care (HPHC)	Harvard Pilgrim Health Care (HPHC) discloses that a ransomware attack to its parent company Point32Health in April 2023 impacted 2,550,922 people, with the threat actors also stealing their sensitive data from compromised systems.	Malware	Human health and social work	Cyber Crime	US	2,550,922.00
5/24/2023	NCB Management Services	NCB Management Services starts sending breach notification letters to affected users about a data breach that exposed nearly 1.1 million people. The company has hinted at paying a ransom to attackers.	Malware	Finance and insurance	Cyber Crime	US	1,100,000.00
5/26/2023	Managed Care of North America (MCNA)	A LockBit ransomware attack on Managed Care of North America (MCNA), a major dental insurance provider, compromises the personal information of nearly nine million people across the United States, according to documents filed with state regulators.	Malware	Human health and social work	Cyber Crime	US	9,000,000.00
5/30/2023	Enzo Biochem	A ransomware attack on Enzo Biochem resulted in the compromise of test information and personal data of nearly 2.5 million people, according to regulatory filings.	Malware	Professional, scientific and technical	Cyber Crime	US	2,500,000.00
6/9/2023	e-Devlet	A website called sorgupaneli.org is offering to provide Turkish 85 million citizens' private data allegedly stolen from the e-Devlet government services website, even claiming to be able to offer President Recep Tayyip Erdogan's personal information.	Unknown	Public admin and defence, social security	Cyber Crime	TR	85
6/9/2023	NHS	1.1 million records belonging to NHS are compromised in the University of Manchester cyberattack (rumored as ransomware) where threat actors likely stole data from the University's network.	Malware	Human health and social work	Cyber Crime	GB	1,100,000.00
6/12/2023	Zacks Investment Research	Zacks Investment Research (Zacks) reportedly suffers an older, previously undisclosed data breach impacting 8.8 million customers, with the database now shared on a hacking forum.	Unknown	Professional, scientific and technical	Cyber Crime	US	8,800,000.00
6/15/2023	Louisiana Office of Motor Vehicles	Louisiana Office of Motor Vehicles warns that six millions of driver's licenses were exposed in a data breach after the Clop ransomware gang hacked their MOVEit Transfer security file transfer systems to steal stored data.	CVE-2023-34362 Vulnerability	Public admin and defence, social security	Cyber Crime	US	6,000,000.00
6/15/2023	Oregon Office of Motor Vehicles	Oregon Office of Motor Vehicles warns that six millions of driver's licenses were exposed in a data breach after the Clop ransomware gang hacked their MOVEit Transfer security file transfer systems to steal stored data.	CVE-2023-34362 Vulnerability	Public admin and defence, social security	Cyber Crime	US	3,500,000.00
6/23/2023	PBI Research Services (PBI)	PBI Research Services (PBI) suffers a data breach with three clients (Genworth Financial, Wilton Reassurance, and CalPERS - California Public Employees' Retirement System) disclosing that the data for 4.75 million people was stolen in the recent MOVEit Transfer data-theft attacks.	CVE-2023-34362 Vulnerability	Administration and support service	Cyber Crime	US	4,750,000.00
6/23/2023	Undisclosed airport	The database of an undisclosed Italian airport with 7.8 million records is on sale in the dark web.	Unknown	Transportation and storage	Cyber Crime	IT	7,800,000.00
7/5/2023	Unknown organizations in Indonesia	The personal information of nearly 35 million Indonesian passport holders is up for sale on the dark web for \$10,000 by notorious hacker Bjorka.	Unknown	Unknown	Hacktivism	ID	35,000,000.00
7/11/2023	HCA Healthcare	HCA Healthcare discloses a data breach impacting an estimated 11 million patients who received care at one of its hospitals and clinics after a threat actor leaked samples of the stolen data on a hacking forum.	Unknown	Human health and social work	Cyber Crime	US	11,000,000.00
7/14/2023	Teachers Insurance and Annuity Association of America (TIAA)	Teachers Insurance and Annuity Association of America (TIAA) files a notice of data breach after discovering to have been hit by the MOVEit CVE-2023-34362 vulnerability.	CVE-2023-34362 Vulnerability	Finance and insurance	Cyber Crime	US	2,600,000.00
7/19/2023	Tampa General Hospital	Tampa General Hospital discloses that the sensitive data of 1.2 million was stolen in a failed ransomware attack.	Malware	Human health and social work	Cyber Crime	US	1,200,000.00
7/23/2023	Egyptian Ministry of Health and Population	An 'established' threat actor claims to be in possession of two million data records stolen from the Egyptian Ministry of Health and Population.	Unknown	Public admin and defence, social security	Cyber Crime	EG	2,000,000.00
7/26/2023	Maximus	U.S. government contractor Maximus confirms that the Clop Ransomware gang, exploiting the vulnerability in MOVEit Transfer accessed the protected health information of as many as 11 million individuals.	CVE-2023-34362 Vulnerability	Professional, scientific and technical	Cyber Crime	US	11,000,000.00
8/2/2023	Performance Health Technology (PH Tech)	Performance Health Technology (PH Tech), a company that provides data management services to U.S. healthcare insurers, confirms in a notice that it was impacted by the MOVEit mass-hacks	CVE-2023-34362 Vulnerability	Professional, scientific and technical	Cyber Crime	US	1,700,000.00
8/8/2023	Missouri's Department of Social Services	Missouri's Department of Social Services warns that protected Medicaid healthcare information was exposed in a data breach after IBM suffered a MOVEit data theft attack.	CVE-2023-34362 Vulnerability	Public admin and defence, social security	Cyber Crime	US	6,000,000.00
8/10/2023	Alberta Dental Service Corporation (ADSC)	Canadian dental benefits administrator Alberta Dental Service Corporation (ADSC) starts informing roughly 1.47 million individuals that their personal information was compromised in a 8base ransomware attack.	Malware	Administration and support service	Cyber Crime	CA	1,470,000.00
8/11/2023	Colorado Department of Health Care Policy & Financing (HCPF)	The Colorado Department of Health Care Policy & Financing (HCPF) alerts more than four million individuals of a data breach that impacted their personal and health information, after IBM suffered a MOVEit data theft attack.	CVE-2023-34362 Vulnerability	Public admin and defence, social security	Cyber Crime	US	4,000,000.00
8/11/2023	India Ministry of Food Processing Industries	A threat actor dubbed Fredens of Security takes credit for exposing 4.5GB, purportedly containing 3 million records linked to India's Ministry of Food Processing.	Unknown	Public admin and defence, social security	Hacktivism	IN	3,000,000.00
8/11/2023	India Ministry of Health & Family Welfare	A threat actor dubbed Fredens of Security takes credit for exposing 4.5GB, purportedly containing 3 million records linked to India's Ministry of Health & Family Welfare	Unknown	Public admin and defence, social security	Hacktivism	IN	1,000,000.00
8/11/2023	Shemaroo Entertainment	A user on a hacker forum is allegedly selling data attributed to Shemaroo Entertainment. The attacker claims that this compromised dataset contains 16.4 million user entries, exposing sensitive details such as email addresses, passwords, phone numbers, and additional personal information.	Unknown	Arts entertainment, recreation	Cyber Crime	IN	16,400,000.00
8/21/2023	Unknown organization in the healthcare sector	A database with 14GB of files with facial photos and 5.1 million records with El Salvadorans personal information is listed for sale on a popular hacking forum.	Unknown	Human health and social work	Cyber Crime	SV	5,100,000.00
8/22/2023	Pôle Emploi	Pôle Emploi, France's governmental unemployment registration and financial aid agency, informs of a data breach that exposed data belonging to 10 million individuals.	CVE-2023-34362 Vulnerability	Public admin and defence, social security	Cyber Crime	FR	10,000,000.00

8/22/2023	University of Minnesota	The University of Minnesota confirms that it is investigating a data breach after hackers claimed to have obtained over seven million Social Security numbers from the school's computer network.	Unknown	Education	Cyber Crime	US	7,000,000.00
8/25/2023	PurFoods	PurFoods the parent company of Mom's Meals, a meal delivery service for people with chronic health conditions, confirms a data breach affecting more than 1.2 million individuals.	Unknown	Accommodation and food service	Cyber Crime	US	1,200,000.00
8/29/2023	Topgolf Callaway	Topgolf Callaway (Callaway) reveals to have suffered a data breach at the start of August, which exposed the sensitive personal and account data of more than a million customers.	Unknown	Manufacturing	Cyber Crime	US	1,114,954.00
9/3/2023	Freecycle.org	Freecycle.org, a platform that allows users to recycle their belongings, prompts 7 millions of users to reset their passwords after their credentials were compromised in a data breach.	Unknown	Human health and social work	Cyber Crime	GB US	7,000,000.00
9/8/2023	Dymocks	Dymocks Booksellers warns customers their personal information was exposed in a data breach after the company's database was shared on hacking forums.	Unknown	Wholesale and retail	Cyber Crime	AU	836,000.00