Threat Intelligence Report Q3, 2022

by Cybersecurity Help

21.11.2022

Contents

Vulnerabilities in 2022

General statistics

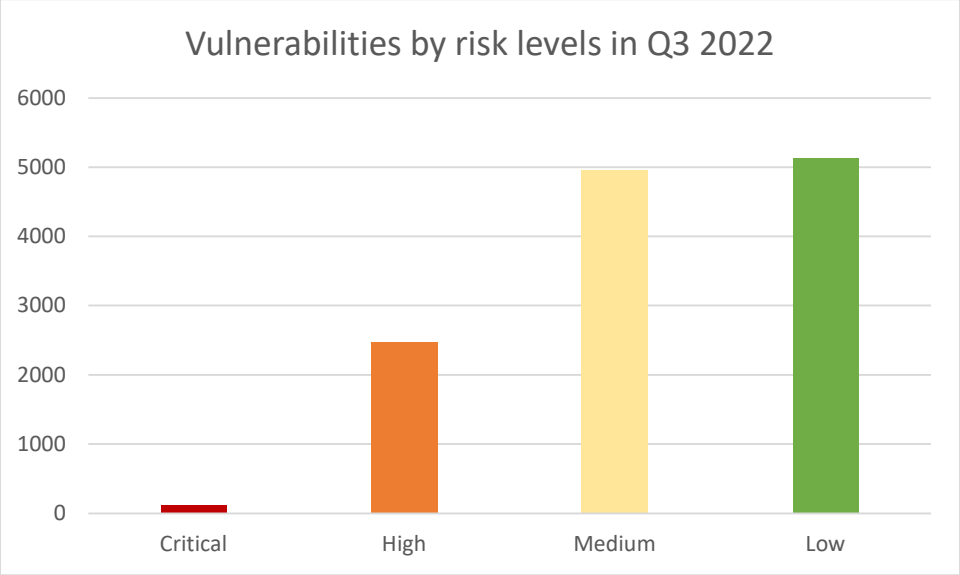
In 2022 Cybersecurity Help has issued 8030 security bulletins that contain description of 28 167 vulnerabilities. 1837 vulnerabilities have publicly available PoC-codes or fully working exploits integrated into various exploitation packs or penetration testing frameworks.

Statistics for 2022	**Q3**	Q2	Q1
Total bulletins	**3303**	2443	2284
Total vulnerabilities	**12692**	8106	7369
Vulnerabilities with exploits	**729**	577	531
Vendors	**73**	67	64
Applications	**5157**	2729	1451
Exploited in the wild	**57**	42	59

Table 1. Security bulletins and vulnerabilities released in Q1-Q3 2022

Risk levels

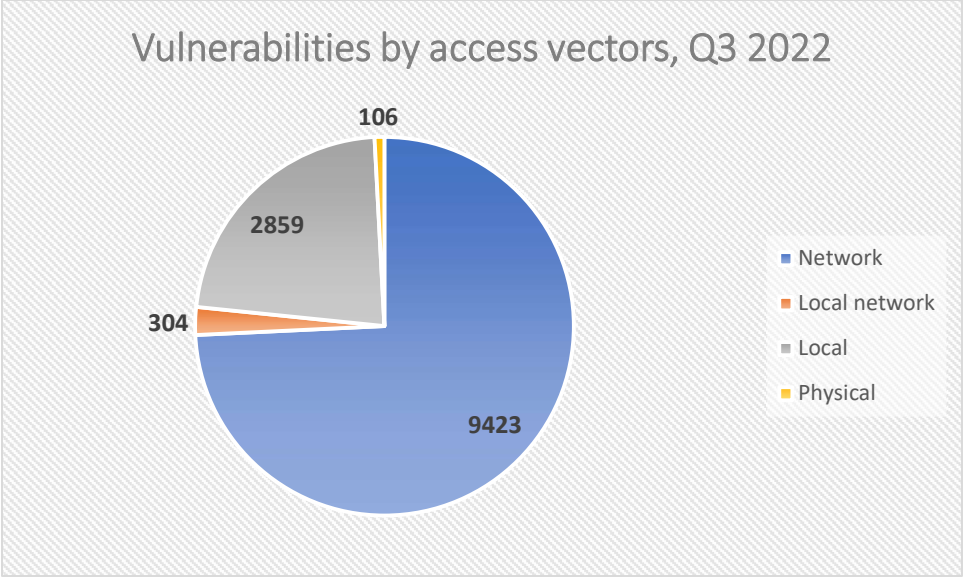
The majority of published vulnerabilities in Q3 were scored with low to medium security risk by our analysts. At the same time, about 2500 vulnerabilities were scored high to critical, meaning that most of these vulnerabilities can be exploited remotely and without authentication.



Diag 1. Distribution of vulnerabilities by risk levels

Access vectors

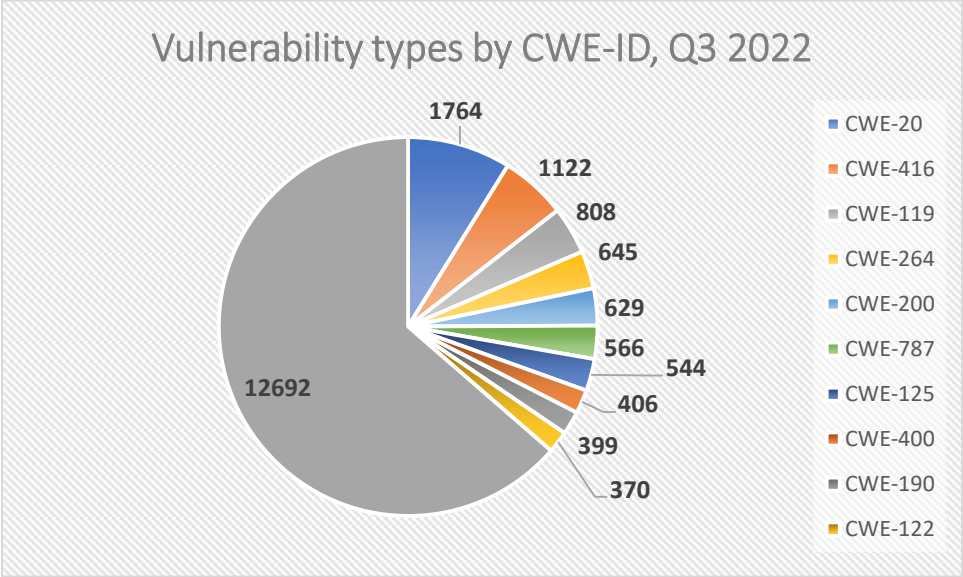
The majority (more than 75%) of published vulnerabilities can be exploited remotely, while 106 vulnerabilities required physical access to the system.



Diag 2. Distribution of vulnerabilities by access vectors

TOP-10 vulnerability types

The most common vulnerabilities in Q3 were caused by input validation and memory management errors (6 out of 10 most common vulnerability types are related to memory management).



Diag 3. Distribution of vulnerabilities by type

Zero-day vulnerabilities reported in Q3

In Q3 2022 we have observed 17 zero-day vulnerabilities that were exploited in the wild before the official vendor patch release.

#	Software	EUVDB-ID	CVE-ID	Security Bulletin
1	Google Chrome	#VU64910	CVE-2022-2294	SB2022070440
2	Windows	#VU65161	CVE-2022-22047	SB2022071220
3	Windows	#VU66229	CVE-2022-34713	SB2022080926
4	Google Chrome	#VU66565	CVE-2022-2856	SB2022081704
5	macOS	#VU66586	CVE-2022-32894	SB2022081718
6	macOS	#VU66587	CVE-2022-32893	SB2022081718
7	Crypto Application Server (CAS)	#VU66683	N/A	SB2022082211
8	Google Chrome	#VU66953	CVE-2022-3075	SB2022090301
9	Photo Station	#VU66993	CVE-2022-27593	SB2022090612
10	BackupBuddy	#VU67167	CVE-2022-31474	SB2022091201
11	macOS	#VU67192	CVE-2022-32917	SB2022091229
12	Apex One	#VU67207	CVE-2022-40139	SB2022091318
13	Windows	#VU67233	CVE-2022-37969	SB2022091342
14	WPGateway	#VU67294	CVE-2022-3180	SB2022091411
15	Sophos Firewall	#VU67624	CVE-2022-3236	SB2022092401
16	Microsoft Exchange Server	#VU67764	CVE-2022-41082	SB2022093001
17	Microsoft Exchange Server	#VU67770	CVE-2022-41040	SB2022093001

Table 2. Zero-day vulnerabilities in Q3 2022

From the list above only 4 vulnerabilities were exploited by financially motivated hackers. The rest were used in targeted attacks by various APT groups.

Actively exploited vulnerabilities

Below is the list of vulnerabilities that were reported or addressed by vendors and are known to be exploited in the wild.

EUVDB-ID	CVE-ID	Public exploit	Impact	Software
#VU64910	CVE-2022-2294	N	RCE	Google Chrome
#VU61756	CVE-2022-22965	Y	RCE	Pivotal Spring Framework
#VU65161	CVE-2022-22047	N	EoP	Windows
#VU58816	CVE-2021-44228	Y	RCE	Apache Log4j
#VU61754	CVE-2022-22963	Y	RCE	Spring Cloud Function
#VU60982	CVE-2022-22947	Y	RCE	Spring Cloud Gateway
#VU11918	CVE-2018-1273	Y	RCE	Pivotal Spring Data Commons
#VU65653	CVE-2014-0114	Y	RCE	Apache Commons BeanUtils
#VU65739	CVE-2022-26138	Y	RCE	Questions for Confluence
#VU65762	CVE-2022-36408	N	RCE	PrestaShop
#VU25502	CVE-2020-1938	Y	RCE	Apache Tomcat

#VU18110	CVE-2019-0211	Y	EoP	Apache HTTP Server
#VU56678	CVE-2021-40438	Y	RCE	Apache HTTP Server
#VU66156	CVE-2022-27924	N	RCE	Zimbra Collaboration
#VU66165	CVE-2022-37042	Y	RCE	Zimbra Collaboration
#VU66173	CVE-2022-27925	Y	RCE	Zimbra Collaboration
#VU66229	CVE-2022-34713	Y	RCE	Windows
#VU66399	CVE-2022-0028	N	RCE	Palo Alto PAN-OS
#VU54103	CVE-2021-30762	N	RCE	Apple iOS
#VU54102	CVE-2021-30761	N	RCE	Apple iOS
#VU52816	CVE-2021-30666	N	RCE	Apple iOS
#VU23175	CVE-2019-8720	N	RCE	WebKitGTK+
#VU61032	CVE-2022-26485	N	RCE	Mozilla Firefox
#VU61033	CVE-2022-26486	N	RCE	Mozilla Firefox
#VU57063	CVE-2021-41773	Y	RCE	Apache HTTP Server
#VU57127	CVE-2021-42013	Y	RCE	Apache HTTP Server
#VU54006	CVE-2021-30551	Y	RCE	Google Chrome
#VU61629	CVE-2022-1096	Y	RCE	Google Chrome
#VU60007	CVE-2021-4034	Y	EoP	polkit
#VU66565	CVE-2022-2856	N	RCE	Google Chrome
#VU66586	CVE-2022-32894	N	EoP	macOS
#VU66587	CVE-2022-32893	N	RCE	macOS
#VU52652	CVE-2021-30661	N	RCE	macOS
#VU66683	N/A	N	RCE	Crypto Application Server (CAS)
#VU66798	CVE-2022-36804	Y	RCE	Bitbucket Server
#VU60520	CVE-2022-22620	Y	RCE	Apple iOS
#VU56504	CVE-2021-38647	Y	RCE	Azure Open Management Infrastructure
#VU56067	CVE-2021-30860	Y	RCE	Apple iOS
#VU66953	CVE-2022-3075	N	RCE	Google Chrome
#VU66993	CVE-2022-27593	Y	RCE	Photo Station
#VU57320	CVE-2021-39226	Y	RCE	Grafana
#VU67167	CVE-2022-31474	Y	RCE	BackupBuddy
#VU67192	CVE-2022-32917	N	EoP	macOS
#VU67206	CVE-2016-4437	Y	RCE	Apache Shiro
#VU67207	CVE-2022-40139	N	RCE	Apex One
#VU67233	CVE-2022-37969	N	EoP	Windows
#VU67294	CVE-2022-3180	N	RCE	WPGateway
#VU50040	CVE-2021-3156	Y	EoP	Sudo
#VU47741	CVE-2020-15999	Y	RCE	FreeType
#VU48668	CVE-2020-28949	Y	RCE	Archive_Tar
#VU49907	CVE-2020-36193	Y	RCE	Archive_Tar
#VU48815	CVE-2020-17530	Y	RCE	Apache Struts

#VU67624	CVE-2022-3236	N	RCE	Sophos Firewall
#VU61935	CVE-2022-22960	Y	EoP	VMware Workspace ONE Access
#VU58845	CVE-2021-4102	N	RCE	Google Chrome
#VU67764	CVE-2022-41082	Y	RCE	Microsoft Exchange Server
#VU67770	CVE-2022-41040	Y	RCE	Microsoft Exchange Server

Table 3. List of vulnerabilities exploited in the wild in Q3 2022

Overview of APT activity in Q3 2022

During Q3 2022 we were observing malicious activity caried out by 29 threat actors primarily from China, Iran, North Korea and the terrorist regime of Russia.

Threat actors

Threat Actor	Country	July	August	September
Andriel	North Korea	US healthcare		
DEV-0530	North Korea	SMBs worldwide		
APT37	North Korea	Czech Republic, Poland		
Kimsuky	North Korea	South Korea, EU, US		
Lazarus APT	North Korea		fintech industry worldwide	Worldwide
Gamaredon	Russia	Ukraine	Ukraine	Ukraine
UAC-0056	Russia	Ukraine		
APT28	Russia	Ukraine	Ukraine	Ukraine
Sandworm	Russia	Ukraine	Ukraine	Ukraine
APT29	Russia	Worldwide	NATO countries	
TA446	Russia		NATO countries	
N/A	Iran	Albania		Albania
MuddyWater	Iran	Israel		
APT35	Iran		Worldwide	
TA453	Iran			Worldwide
Nemesis Kitten	Iran			Worldwide
N/A	China	Russia		
APT27	China	Belgium		
APT30	China	Belgium		
APT31	China	Belgium		
N/A	China		N/A	
N/A	China		Internal activity	
LuckyCat	China			Tibet
N/A	China			Worldwide

Bronze President	China			EU, Middle East, South America
Stone Panda	China			Worldwide
APT36	Pakistan		Afghanistan, India, Pakistan, UAE, Saudi Arabia	
Metador	N/A			Telcos in Middle East, Africa
Bitter APT	N/A		New Zealand, India, Pakistan, UK	

Table 4. Overall threat actors' activity during Q3, 2022

Incidents

Below is the list of notable campaigns caried out by the sate-sponsored threat actors between July and September 2022 with a monthly breakdown for greater convenience.

July

July saw continued malicious cyber activity conducted by state-backed threat actors targeting individuals and organizations across the world for various purposes, including cyber-espionage and data theft. While tactics, techniques, and procedures (TTPs) of most APT groups have not significantly evolved over the time, some changes have been observed.

In particular, North Korean hackers (namely, the Andriel hacker group) known for orchestrating campaigns for financial gain has switched to ransomware. In one instance, they have deployed the Maui ransomware against healthcare and public health sector organizations in the United States.

Also, a North Korean hacker group, tracked as DEV-0530, has been observed attacking small businesses in various countries with a ransomware strain called H0lyGh0st.

In another campaign (STIFF#BIZON) the North Korea-linked APT37 group (aka Ricochet Chollima) targeted high-value organizations in the Czech Republic, Poland, and other countries with the Konni remote access trojan capable of executing arbitrary code on the target systems and stealing data.

Another North Korean threat actor, Kimsuky (aka Black Banshee, Thallium, SharpTongue, and Velvet Chollima), has been using a browser extension to steal content from victims' webmail accounts. Active since at least 2012, Kimsuky is known for the targeting of entities in South Korea, Europe and the United States.

Besides espionage, North Korean state-backed actors have a history of conducting financially-motivated attacks, including targeting blockchain companies and leveraging cryptocurrency thefts by making use of rogue wallet apps and exploiting crypto asset bridges.

In July, the US State Department announced it raised a reward to $10 million for information about North Korean state-backed threat actors.

Since the beginning of Russia's invasion of Ukraine on February 24, many Russian state-sponsored cyber actors (Gamaredon, UAC-0056 and others) remained focused on Ukraine and related issues, while Russian APT activity outside of Ukraine largely remained the same. In July alone, multiple malicious campaigns were observed targeting government entities and businesses in Ukraine. In some cases Russian threat actors, specifically APT28 and Sandworm, were seen exploiting the Follina RCE vulnerability (CVE-2022-30190), first disclosed in late May, while in others threat actors capitalized on the ongoing conflict to distribute Android malware (Turla APT), Cobalt Strike malware (UAC-0056), or Formbook, Snake Keylogger and Agent Tesla infostealers.

In an unrelated case, a well-known Russian-backed hacker group, tracked as APT29, Cloaked Ursa, Nobelium or Cozy Bear, was observed using trusted online storage services, including DropBox and Google Drive to deliver malware to businesses and government agencies to steal data and spread malware. This technique makes the group's attacks extremely challenging to detect.

July also saw an increase in Russian targeting by suspected Chinese threat actors. In particular, a campaign linked to China was discovered that was aimed at Russia-linked organizations targeting them with malware designed to collect intelligence on government activities.

China's recent intelligence objectives against Russia can be observed in multiple campaigns following the invasion of Ukraine, such as Scarab, Mustang Panda, and Space Pirates.

The government of Belgium reported that three China-linked state-backed threat actors (APT27, APT30, and APT31) attacked its public service and defense forces. The attack was thwarted.

August

In August, multiple state-backed threat actors were observed using novel attack techniques in their campaigns. For example, a threat actor known as Mercury or MuddyWater believed to be affiliated with Iran's Ministry of Intelligence and Security (MOIS) exploited the Log4Shell vulnerability (CVE-2021-44228) in attacks targeting vulnerable SysAid Server instances belonging to organizations in Israel.

Another Iran-linked cyber actor, tracked as APT35 and Charming Kitten, developed a novel tool, dubbed "Hyperscrape", designed to steal data from Gmail, Yahoo!, and Microsoft Outlook accounts.

China-linked hackers were observed using a new post-exploitation attack framework, similar to the Cobalt Strike and Sliver frameworks. Named "Manjusaka", the tool uses implants written in the cross-platform Rust programming language, while its binaries are written in the equally versatile GoLang, and can be deployed as an alternative to the widely abused Cobalt Strike framework.

Yet another campaign attributed to Chinese threat actors used a trojanized cross-platform instant messenger application focused on the Chinese market known as "MiMi" to deliver versions of the HyperBro and rshell backdoors to infected users in order to steal data from Linux and macOS systems.

State-backed hacker groups affiliated with the Russian government have been particularly prolific, orchestrating various malicious campaigns targeting organizations all over the world. These include a phishing operation that targeted individuals and organizations in NATO countries (SEABORGIUM, also

known as ColdRiver and TA446), and cyber-espionage campaign (APT29) focused on targeting organizations responsible for influencing and crafting the foreign policy of NATO countries. The latter campaign used newer tactics that involved the abuse of various Microsoft 365 features in order to evade detection. APT29 (aka NOBELIUM, Cozy Bear) was also observed leveraging a new post-compromise malware called MagicWeb that allowed the threat actors to exfiltrate the configuration database of compromised Active Directory Federation Services (ADFS) servers.

As for the North Korean hackers, the most notable campaign observed in August was a social engineering operation conducted by the Lazarus APT, which targeted experts in the fintech industry and involved fake Coinbase job offers laced with malware.

Meta, the owner of Facebook and Instagram, disrupted two separate cyber-espionage campaigns orchestrated by the Bitter APT and APT36 state-sponsored hacker groups.

In the Bitter APT (believed to be operating out of South Asia) campaign the attackers attempted to trick victims into downloading an iOS chat app via Apple's legitimate TestFlight service. The operation targeted users in New Zealand, India, Pakistan and the United Kingdom.

The second cyber-espionage campaign conducted by APT36, which is believed to be a Pakistani state-backed threat actor, involved a modified version of the XploitSPY Android malware called LazaSpy, and trojanized versions of WhatsApp, WeChat and YouTube delivering the Mobzsar or CapraSpy malware. The campaign targeted people in Afghanistan, India, Pakistan, UAE, and Saudi Arabia, including military personnel, government officials, employees of human rights and other non-profit organizations and students.

September

In September 2022, Iranian threat actors launched a second wave of cyberattacks against the Albanian government, similar to a July 15 ransomware attack that temporarily shut down numerous Albanian government digital services and websites. An investigation into the July intrusion showed that the attacks were carried by four hacker groups acting on behalf of Iran.

Following the attack Albania cut diplomatic ties with Tehran, and the US imposed new sanctions on Iran's Ministry of Intelligence and Security (MOIS) and its Minister of Intelligence, Esmaeil Khatib, for engaging in cyber-enabled activities against the US and its allies. The US authorities also charged three Iranian nationals for a global computer hacking campaign that allegedly targeted hundreds of victims for extortion.

Other notable Iranian cyber activity includes TA453's phishing campaign that targeted individuals specializing in Middle Eastern affairs, nuclear security, and genome research, and ransomware attacks carried out by DEV-0270 (aka Nemesis Kitten), a sub-group of Iranian actor PHOSPHORUS.

The North Korean state-backed hacker group Lazarus has been linked to several malicious campaigns that recently have come to light. One of the campaigns involved trojanized legitimate open-source software (such as PuTTY, KiTTY, TightVNC, Sumatra PDF Reader, and muPDF/Subliminal Recording) that was used to backdoor organizations in various industry sectors, including technology, defense, and

media entertainment. Lazarus was also seen installing a Windows rootkit that abuses a Dell hardware driver, as well as targeting energy providers around the globe, deploying a new remote access trojan dubbed ”MagicRAT,” and luring Apple’s macOS users with job opportunities in crypto industry.

Russian nation-state actors have continued their targeting of Ukraine with cyber-espionage campaigns. In one case a threat cluster linked to Russian APT known as Sandworm targeted entities in Ukraine with the Colibri Loader dropper and Warzone RAT posing as telecommunication providers. In another instance the Russia-linked Gamaredon group (aka Actinium, Armageddon, Primitive Bear, Shuckworm, and Trident Ursa) targeted employees of Ukrainian government, defense, and law enforcement agencies with custom-made information-stealing malware.

The well-known Russian threat actor APT28, also tracked as Fancy Bear and TSAR Team, was observed leveraging a new code execution method that makes use of mouse movement in decoy Microsoft PowerPoint documents to deploy malware.

China-linked state-backed threat actors have a long history of using zero-day exploits in their attacks. In one of the recent campaigns a China-aligned threat actor, tracked as TA413 or LuckyCat, weaponized the recently disclosed zero-day vulnerabilities in Sophos Firewall (CVE-2022-1040) and Microsoft Office (CVE-2022-30190) to deploy a previously undocumented backdoor dubbed ”Lowzero” as part of a cyber-espionage campaign aimed at Tibetan targets.

A China-linked threat group is believed to be behind the attacks exploiting

two unpatched zero-day vulnerabilities collectively dubbed “ProxyNotShell” in Microsoft Exchange servers to deploy Chinese Chopper web shells on compromised servers for persistence and data theft.

In another campaign a China-based threat actor known as Bronze President targeted government officials in Europe, the Middle East, and South America with the PlugX modular malware. Chinese cyber-espionage group Witchetty (aka LookingFrog) believed to be part of the Chinese APT Cicada (APT10, Stone Panda), updated its attack arsenal with new malware, including the Stegmap backdoor, which relies on steganography to extract a payload from a bitmap image and has an extensive array of features.

More recently, suspected Chinese hackers have been observed hijacking installer for widely used Comm100 software to distribute malware in a supply chain attack.

A previously unknown advanced threat actor dubbed ‘Metador’ has been linked to a series of intrusions at telecommunications firms, internet service providers, universities, and other entities across the Middle East and Africa. Metador is highly skilled and primarily focused on cyber-espionage. The new group has shown the ability to evade security tools, and the complexity of the malware and its active development suggests that the threat actor is well-resourced.

Q3 2022 data breach roundup

Below is the list of major data leaks that were exposed between July and September in 2022.

Marriott

The Marriott International hotel chain, a company that was affected by a number of major security incidents in recent years, suffered yet another data breach that exposed employee and customer information. Hackers behind the breach claimed to have stolen 20GB of data, including confidential business documents and customer payment information, from the BWI Airport Marriott in Baltimore, Maryland. According to the attackers, they used social engineering to trick an employee at a Marriott hotel in Maryland into giving them access to their computer. However, a Marriott spokesperson said that the threat actors did not gain access to Marriott's core network.

The culprits attempted to extort the hotel chain before going public with the breach, but no money was paid.

Mangatoon

Information belonging to 23 million users of online comic book provider Mangatoon was exposed after a hacker stole it from an unsecured Elasticsearch database. The breach exposed names, email addresses, genders, social media account identities, auth tokens from social logins and salted MD5 password hashes.

The biggest data leak in China's history to date

Hackers stole data of more than 1 billion Chinese citizens from a Shanghai police database and tried to extort the department for about $200,000 in what appears to be one of the most expansive data breaches recorded to date. The trove of data contained names, phone numbers, government ID numbers, and police reports for the period from 1995 to 2019.

An investigation into the incident showed that the database itself was secure, but that a management dashboard was publicly accessible from the open internet, allowing anyone to access it without a password.

Neopets

Virtual pet website Neopets was hit by a data breach that resulted in the theft of source code and a database containing the personal information (usernames, real names, birthdays, zip codes, email addresses, etc.) of over 69 million members. The breach came to light after the stolen database had been put up for sale on the dark web. An investigation revealed that the hackers had access to Neopet's network for 18 months.

Twitter

A security vulnerability in Twitter's code led to the exposure of over 5.4 million Twitter users. Reports of the breach emerged after a database containing account details of millions of Twitter users was spotted on a hacker forum. The database included information about various accounts, including celebrities, companies, and random users.

Plex

Plex, one of the largest media streaming apps, reported a data breach that exposed customers' usernames, email addresses, and encrypted passwords. It appears that the attacker had managed to access a small portion of Plex database. The company did not reveal the number of compromised accounts, but recommended users to change their passwords.

LastPass

Password management software firm LastPass suffered a security incident that led to the theft of source code and proprietary technical information.

The attackers gained access to portions of the LastPass development environment through a single compromised developer account. The company said that the threat actor's activity was limited to a four-day period in August 2022 and that they found no evidence that the incident involved any access to customer data or encrypted password vaults.

Twilio

Digital communication platform Twilio suffered a data breach after some of the company's employees have fallen victim to a phishing campaign which tricked them into providing their login credentials. The attackers then used the stolen credentials to gain access to Twilio's internal systems and certain customer data. According to Twilio, only "a limited number" of customer accounts were affected in the incident.

Rockstar Games

Confidential information belonging to video game publisher Rockstar Games leaked online after a hacker gained access to the company's network. The leaked data included the early development footage from the next installment in its blockbuster "Grand Theft Auto" franchise.

The hack, described as "one of the biggest leaks in video game history," came to light after a user going online as "teapotuberhacker" posted the trove of data containing nearly 90 videos showing various game features on GTAForums. Rockstar confirmed the legitimacy of the videos.

Optus

Australian telecoms company Optus, the second largest wireless services provider in Australia, was hit by a massive data breach affecting the personal information of both former and current customers. The attackers were able to gain access to user data such as names, dates of birth, email and home addresses, phone numbers, and personal identification document numbers. The breach is said to have impacted all of Optus' 9.8 million customers, equivalent to around 40% of Australia's population. The company stressed that payment details and account passwords were not compromised.

Soon after the attack was publicly disclosed a user published data samples on an online forum and demanded a ransom of $1 million in cryptocurrency from Optus, but later withdrew their ransom demand and apologized. The Australian authorities blamed Optus for the hack and announced plans to adopt more strict privacy rules.

About Cybersecurity Help

Cybersecurity Help s.r.o. is a global vulnerability intelligence provider. The company was founded in 2015 in Czech Republic.

Follow us in social media:

Twitter: https://twitter.com/Cybershelp Facebook: https://www.facebook.com/cybershelp/

LinkedIn: https://www.linkedin.com/company/cyber-security-help