ThreatMon

The Global Cyber Security Intelligence Risk Report 2023

@threatmon

@MonThreat

Welcome

ThreatMon is a Cyber Threat Intelligence firm founded in 2022. ThreatMon automatically identifies all digital assets of an organization that are open to the outside world that can be attacked by cybercriminals and performs continuous vulnerability analysis.

TM EXTERNAL ATTACK SURFACE MANAGEMENT

External Attack Surface Management is a service context where ThreatMonIT consultants specify attack vectors in today's dynamic, distributed and shared environments. Continuously monitor for discovered risks and enable your organization to operationalize and inform risk management.

TM DIGITAL RISK PROTECTION

Digital Risk Protection is the service content that ThreatMonIT consultants provide services in the fields of "Social Media Risk", "Account Leakage", "Deep/Dark Web Finding", "Phishing Monitoring" and "Source Code Leakage" to companies through Dashboard data. You can strengthen every aspect of your company by being able to monitor and make inferences at any time.

TM THREAT INTELLIGENCE

Your company's data leaks, hacking situations, attack plans circulating about your company among attackers or attackers, etc. is knowing the attacks before they happen. Because you will be able to increase your precautions before the attacks start. Your company's data leaks, hacking situations, attack plans circulating about your company among attackers or attackers, etc. You should take a look at the intelligence solution of ThreatMonIT consultants so that you can learn about the situations.

TM SECURITY VALIDATION

Security Validation is a cybersecurity technique that allows companies to get an extensive report on what could happen if they suffer a cyber attack. Tests allow us to determine whether our organization's security is efficient and provide relevant data to the company in the event of a security breach. In this way, you can understand in detail the defense aspects of your organization against possible attacks and if it is you are inadequate, ThreatMonIT consultants will assist you in your efforts to increase your defense.

Table of Contents

Summary

The year 2022 was a busy year for cybersecurity and cyber threats. Numerous cyber attacks and data leaks occurred, threatening the security of companies and organizations. At the same time, the growing needs for online education and work have increased attacks by fraudsters and hackers on online workers and students. In addition, the proliferation of 5G networks and the increasing number of IoT devices have created more risks for cybersecurity. 2022 was a year that required more attention and care regarding cybersecurity and cyber threat.

In 2022, artificial intelligence technology developed rapidly and had significant implications for cybersecurity. AI could be used to detect, prevent and analyze cyberattacks. However, AI can also become a tool that can be used for cyberattacks. Furthermore, AI systems have inherent vulnerabilities that can be exploited by hackers. In conclusion, in 2022, AI technology had positive and negative impacts on cybersecurity.

ThreatMon analyzed cybersecurity activities in 2022 and commented on possible threats in 2023. In 2022, ThreatMon provided services in various fields by early detection of many cyber security incidents and minimizing their interventions to a minimum delay thanks to various modules it has developed.

The year 2022 was an important year for cybersecurity. Ransomware groups, APT groups and thieves targeted government sites, companies and individual users, resulting in leaked data, vulnerabilities and IOC data. The report analyzes in detail the rise of these threats and how to manage them. It provides recommendations on the necessary measures to detect, prevent and manage these threats. The report is a very important resource for experts and those interested in cyber security issues. It is also a resource for anyone who wants to be aware of cyber threats and security vulnerabilities and how to manage these threats.

ONE OF YEAR THREATMON

521.826
PORT

210.552
SSL

380.341
TECHNOLOGY

298.459
IP ADRESS

371.265
WEBSITE

1.320.231
CYBER THREAT INTELLIGENCE ALARMS

1.924.897
ATTACK SURFACE MANAGEMENT ALARMS

3.245.128
ALARM

5000+
NEWS

THREATMON

RANSOMWARE GROUPS ACCORDING TO ANNUAL DATA

threatmon.io

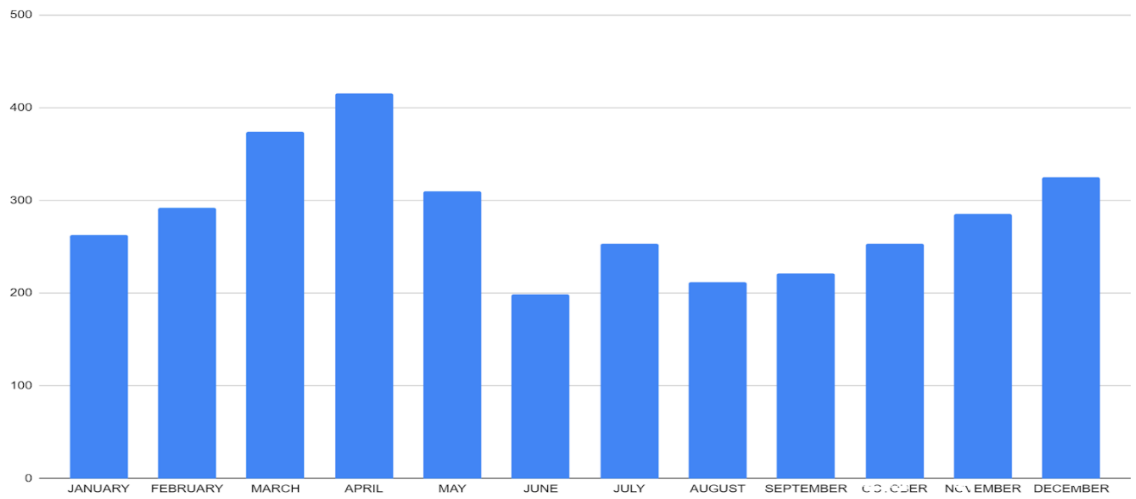
Ransomware in 2022

Ransomware cases have increased rapidly compared to previous years. While this increase was much more accelerated during the pandemic, the end of the pandemic did not slow down the situation and this increase continued in 2022.

ThreatMon has been analyzing ransomware activity in 2022 and has been reporting on this activity internally. Below is the data about the data collected by ThreatMon in 2022.

This area lists the monthly distribution of victims detected from Ransomware attacks in 2022 on a monthly basis.

Ransomware Groups in Annual Data

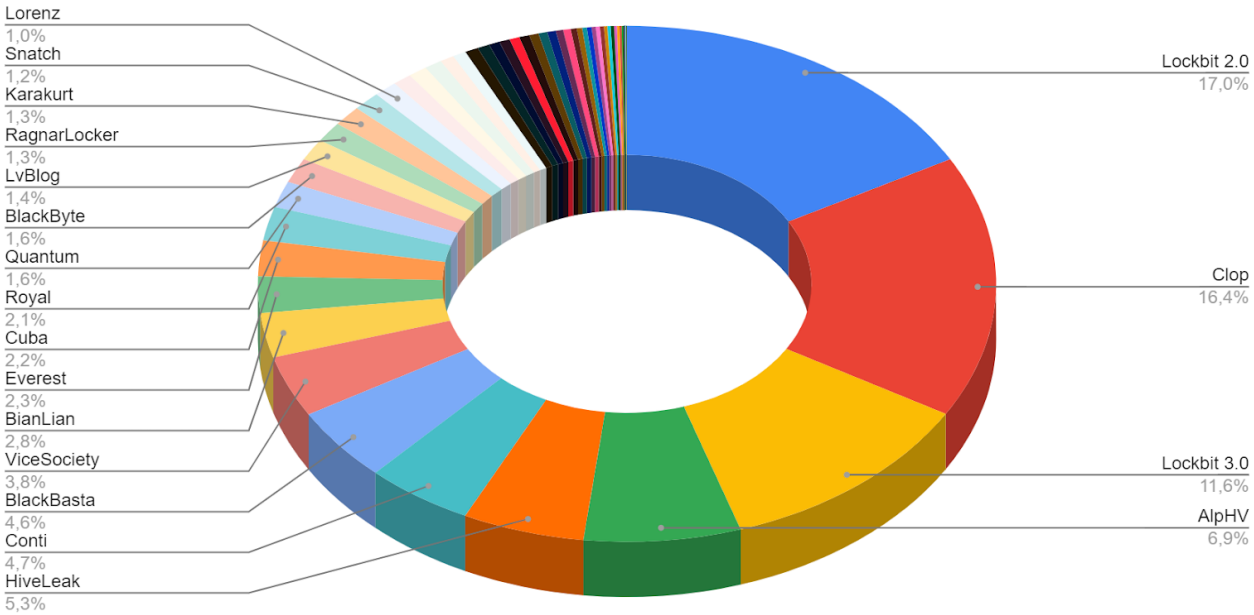


Monthly 2022:

- January: 283
- February: 292
- March: 354
- April: 415
- May: 310
- June: 199
- July: 253
- August: 212
- September: 221
- October: 253
- November: 285
- **December: 323**

On a monthly basis, there is a high difference in ransomware cases in some months compared to other months. These increases may be due to the change of activity within the Ransomware groups themselves or their orientation to different sectors.

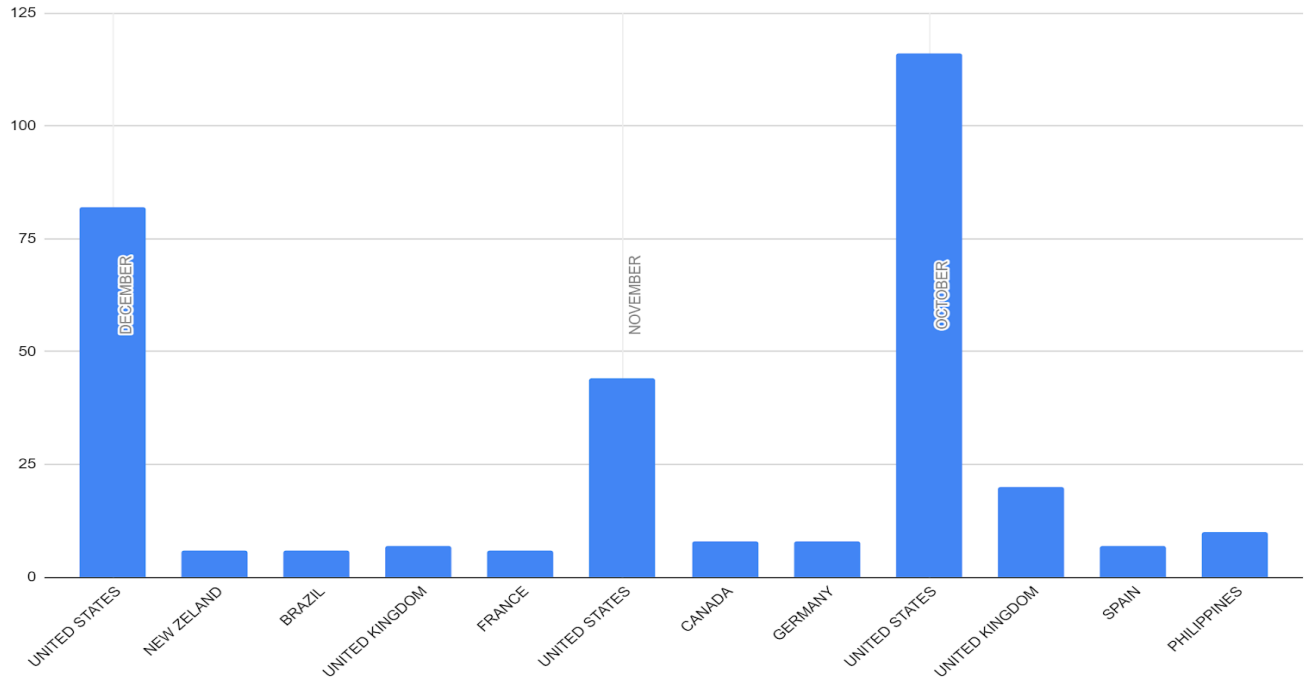
The activities of ransomware groups in 2022, by group, can be seen below.



As can be seen from the graph, some groups have changed their names or versions. Ransomware groups have to improve themselves in order not to be caught and easily detected. In these changes, they have changed their names or updated their version information.

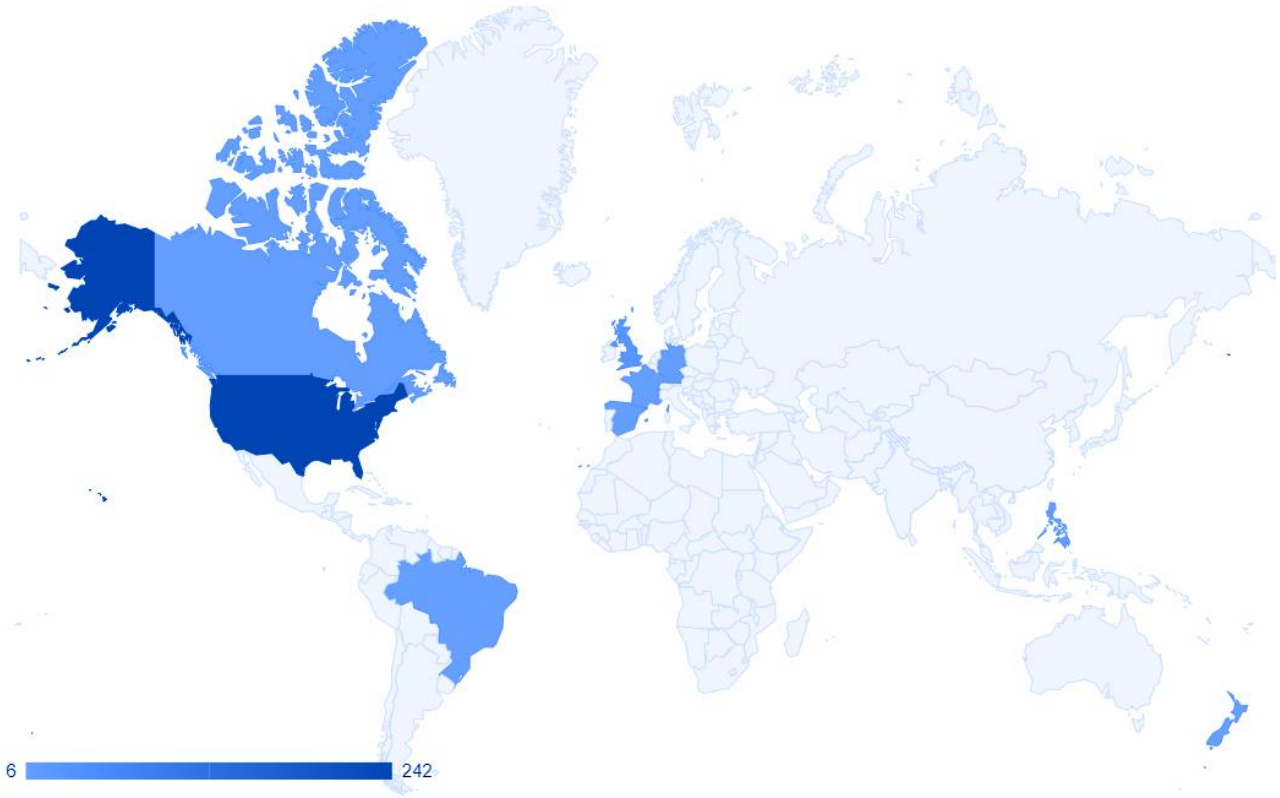
Ransomware Cases in the Last Quarter

ThreatMon analyzed the activity of ransomware groups in the last three months, as well as the data they collected on annual data. As a result of the analysis, the number of activities on an annual basis has been stable in recent months.
Graphs of the last three months' data;

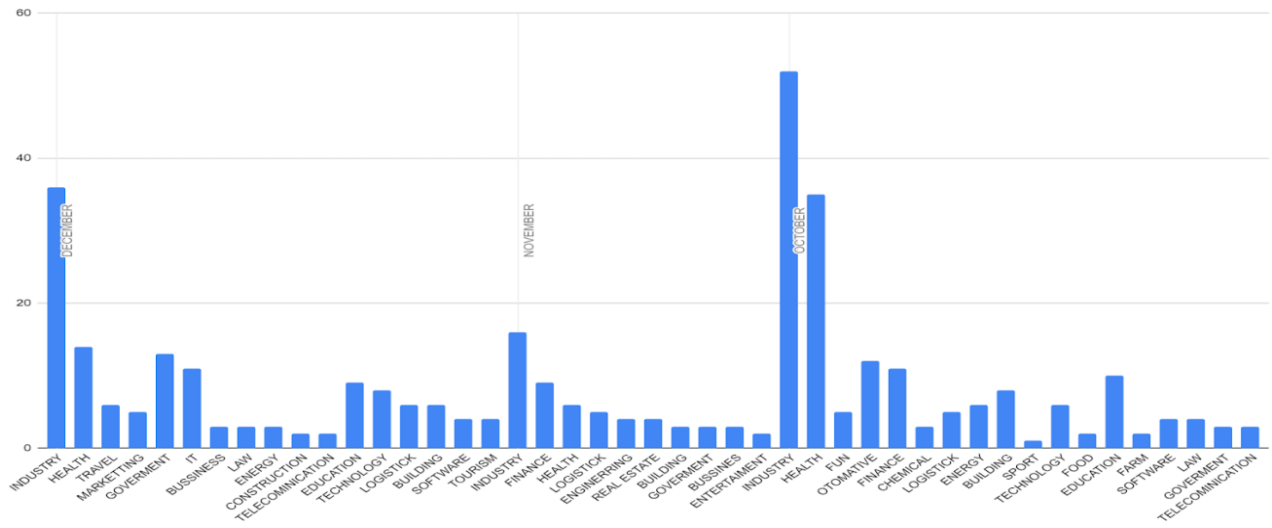


A country-by-country analysis of the activity of ransomware groups in the last three months is given in the image above.

The country with the highest number of victims in the last three months and for the whole year was the United States. The United States, which is a common point for many sectors, is also the country with the highest number of victims in the first month of 2023. ThreatMon predicts that this ransomware activity will continue in 2023.



ThreatMon, which analyzed the last three months of data by sector, found that the Industrial sector was the most targeted sector by Ransomware groups. When we focus these analyzes on the whole year, Industry was one of the most targeted sectors in 2022.



ThreatMon predicts that there will be a similar picture in 2023, and that the Industry sector will be one of the most attacked sectors.

Even if there is variability in other sectors, it is seen that the attack will increase in the Health and Tourism sectors in 2023.

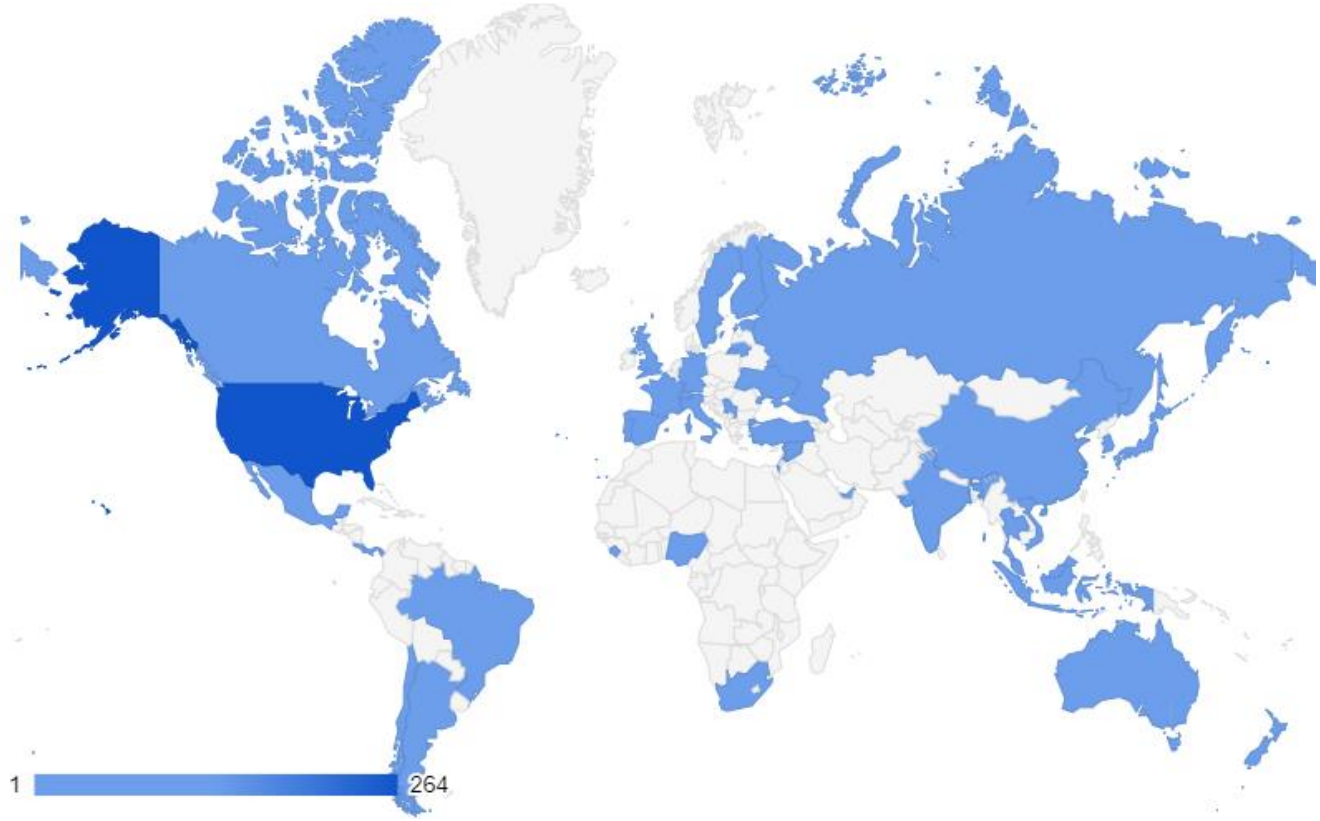
THREATMON

APT GROUPS ACCORDING TO ANNUAL DATA

threatmon.io

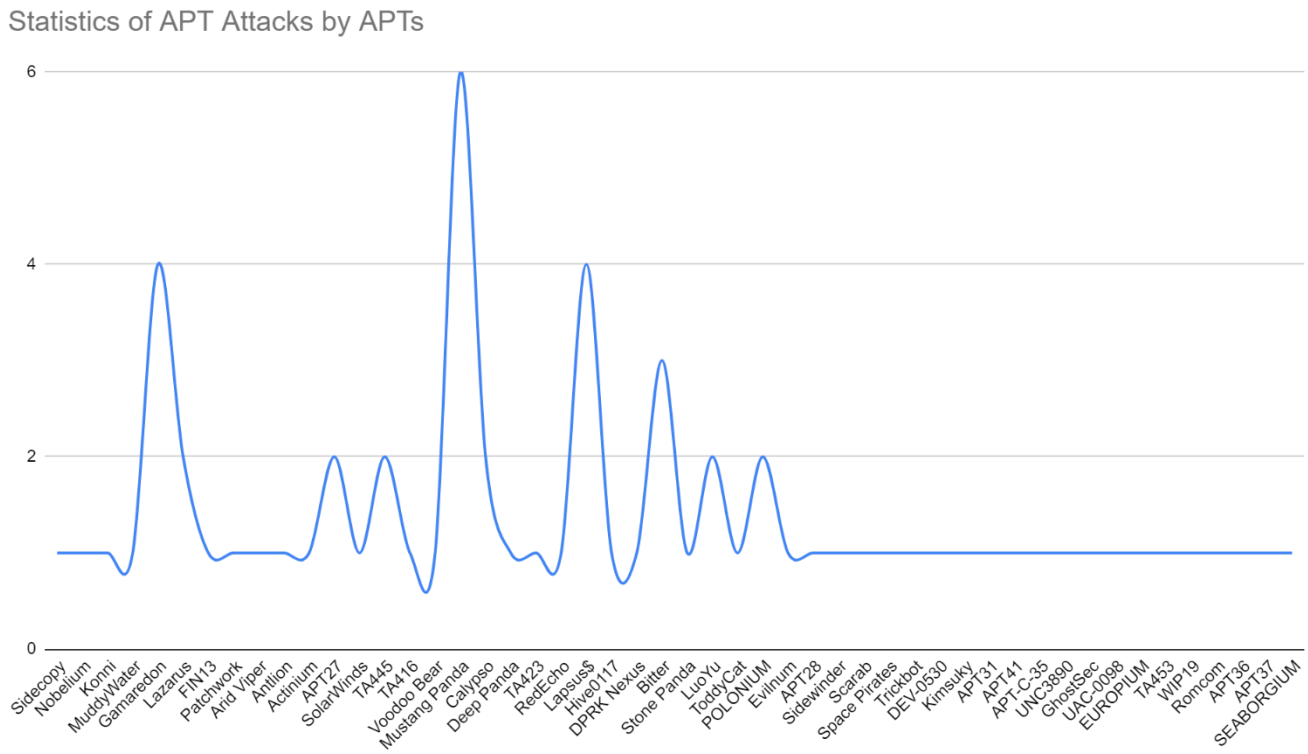
APT Groups According to Annual Data

When we look at the data we have, we see that China, Russia, and Ukraine are the countries that receive the most cyber-attacks. With Ukraine having 36.36%, Russia 27.27% and China 18.18% of total APT attacks. It is possible to say that this is because of the war between Russia and Ukraine.



Statistics of APT Attacks by APTs

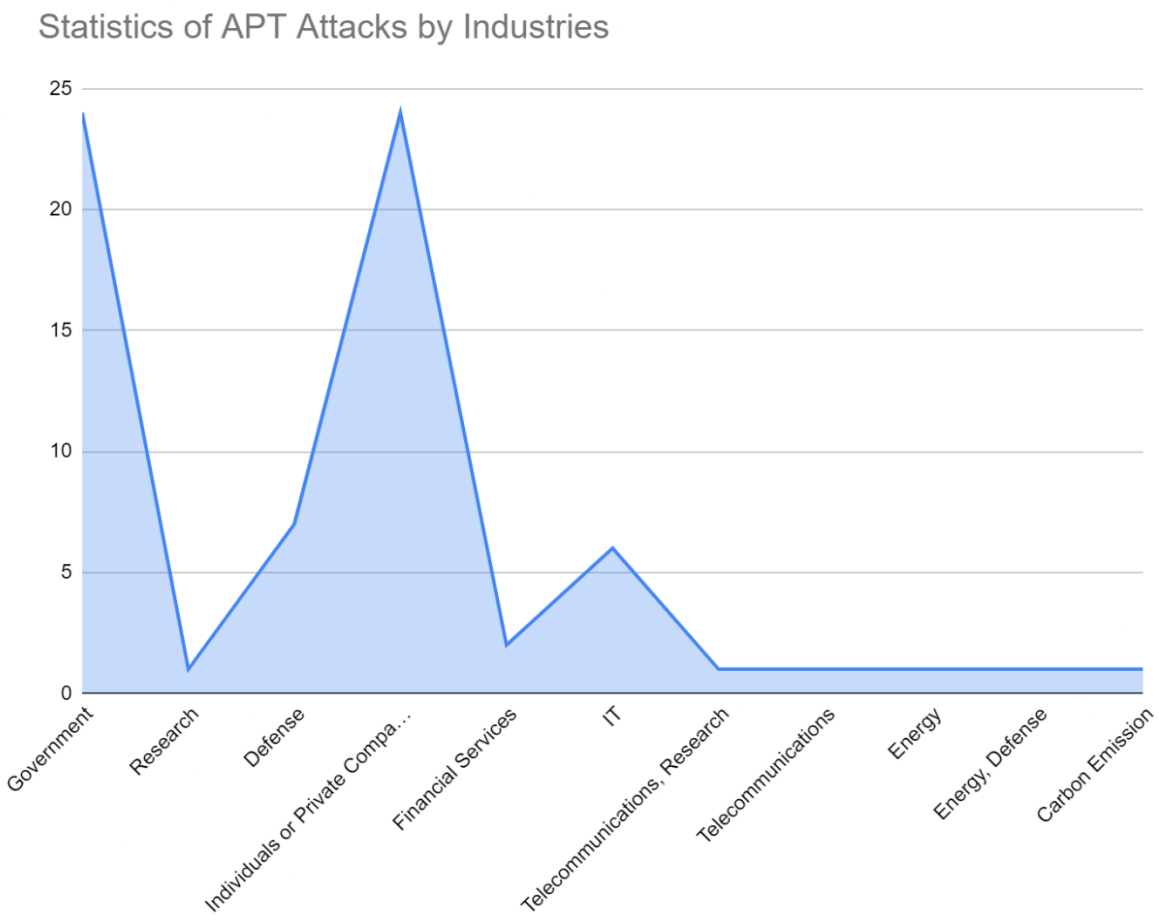
When we look at the data we have, we see that Mustang Panda, Gamaredon and Lapsus$ are the APT groups that are most active. Mustang Panda group took 9%, Gamaredon 6%, and Lapsus$ 6% of the top APT groups that attacked the most this year.



The Mustang Panda group continued its attacks in Asia Pacific countries and Europe using the Russia-Ukraine war. While the Gamaredon group continued its attacks on Ukraine, Lapsus attacked private IT companies.

Statistics of APT Attacks by Industries

The statistics indicate that the government sector, individuals or private companies, and the defense industry are the most targeted by APT attacks, with 35% each of attacks directed towards the government and individuals/private companies, and 10% towards the defense industry.



Given the ongoing conflict between Ukraine and Russia, it is possible that APT attacks may increase in the government and defense sectors, particularly if the conflict escalates or expands to cyber operations.

THREATMON

GOVERNMENT DATA HACKED BY YEARLY DATA

threatmon.io

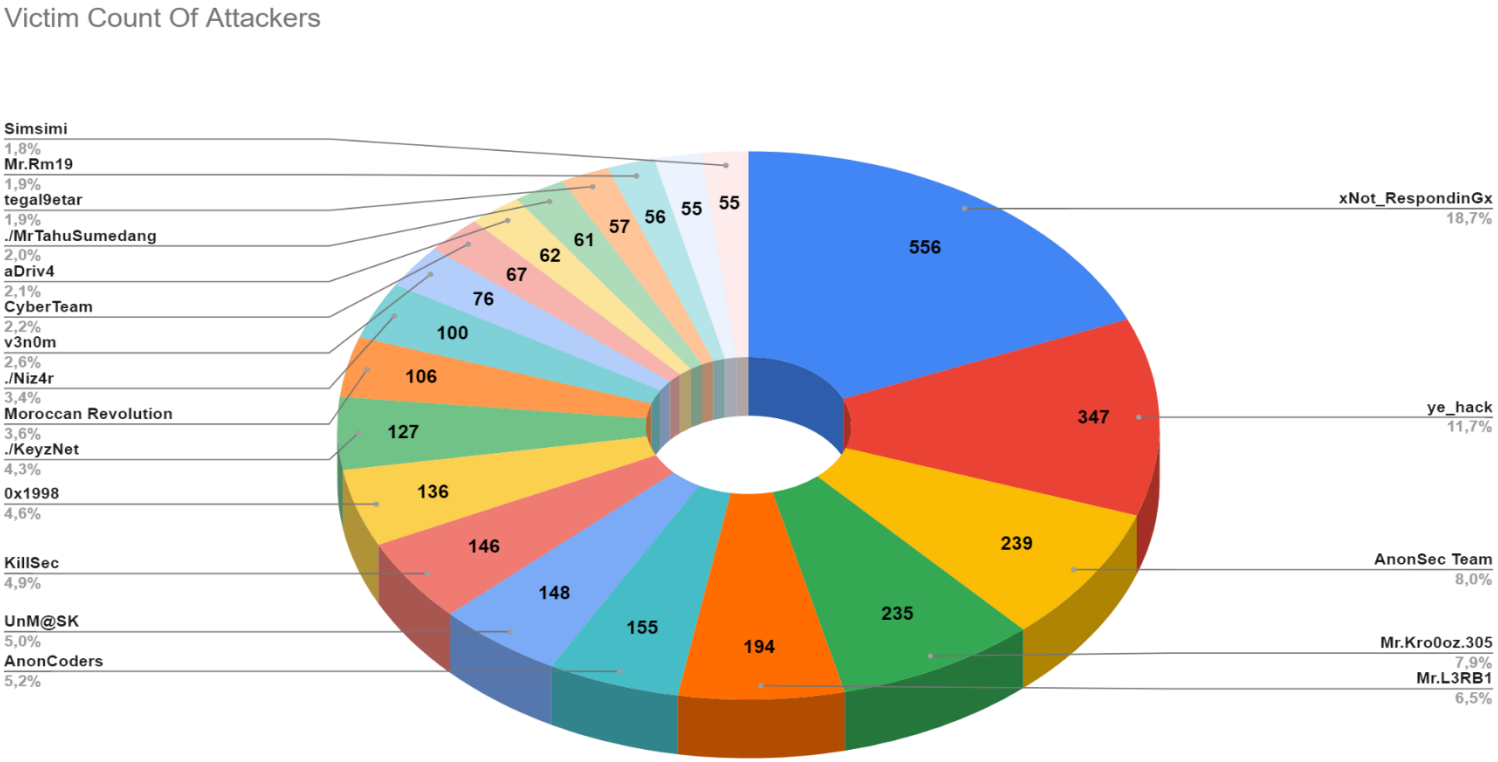
Government Data Hacked by Yearly Data

ThreatMon monitors government websites that are hacked annually. In 2022, the statistical data of hacking incidents on government websites is below.

Number of Top 20 Threat Actors And Victim Counts

The number of attacks that took place between 2022-2023 and targeted government websites is 4839. In the chart below, we shown the top 20 threat actors that are responsible for the attacks.

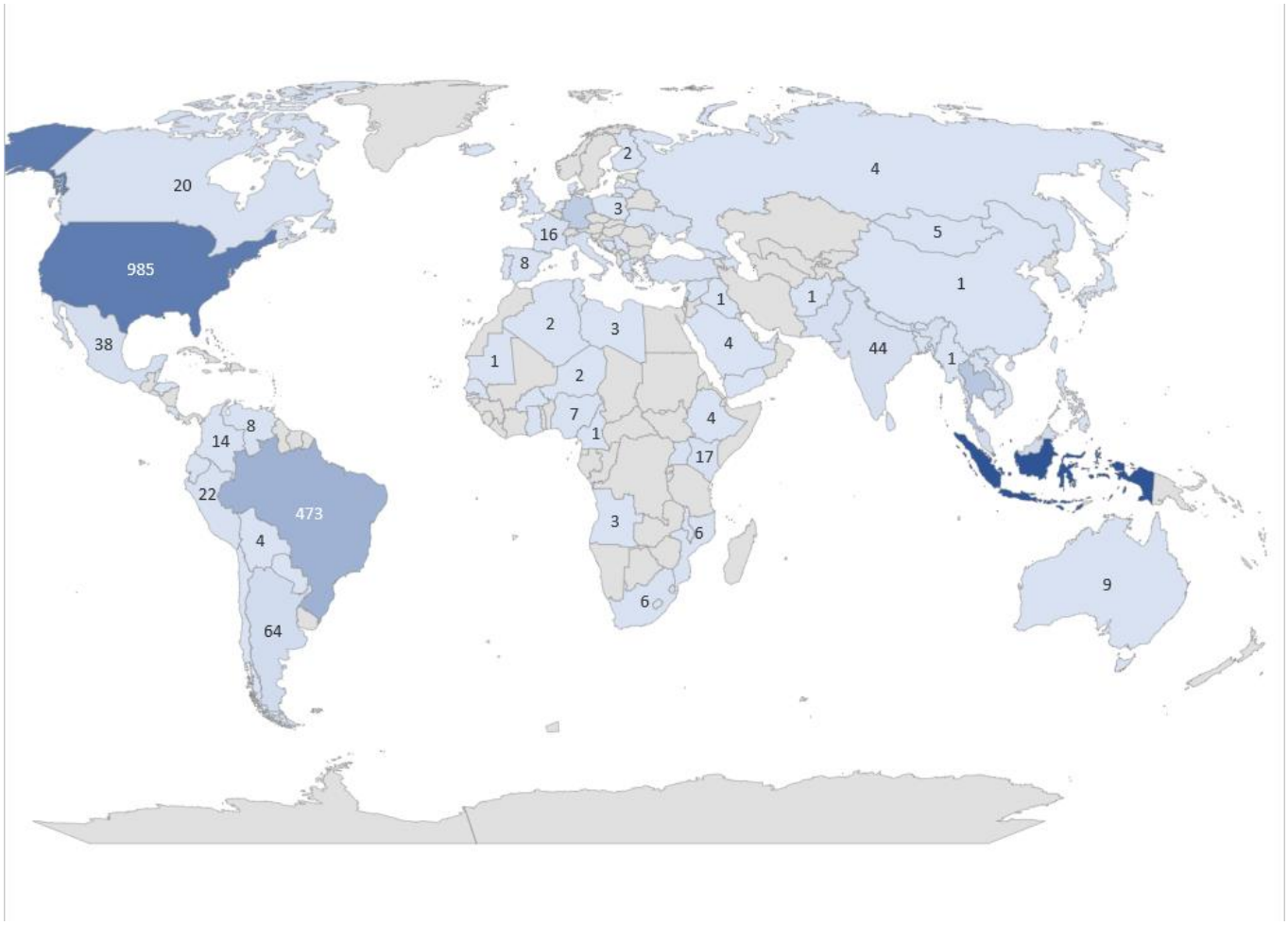
Threat actors are categorized into various types that differ according to the motivations of the threat actors. While the main motivation of many threat actor groups is to make money, there are also threat actors that target various countries based on their national values. The vast majority of the groups in the 2022 data analyzed by ThreatMon are nationalist threat actors. Therefore, they show a show of force against the institutions and organizations of countries that threaten or attack their national values.



Countries Targeted By Threat Actors

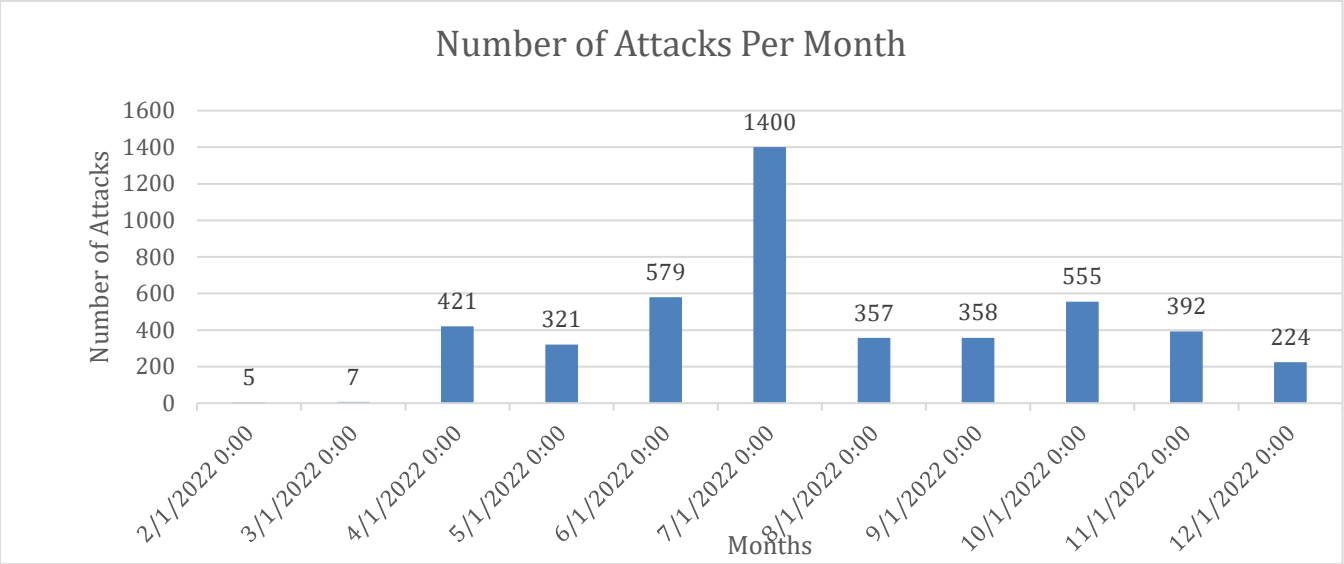
Based on the data ThreatMon has collected throughout 2022, Indonesia, United States of America and Singapore were the most targeted countries. It is very likely that political tension between the U.S. and China triggered the cyber attacks on the United States. In addition, just before and during the time the G20 Summit that was held in Indonesia, increased number of cyberattacks by different threat actors on Indonesia were observed.

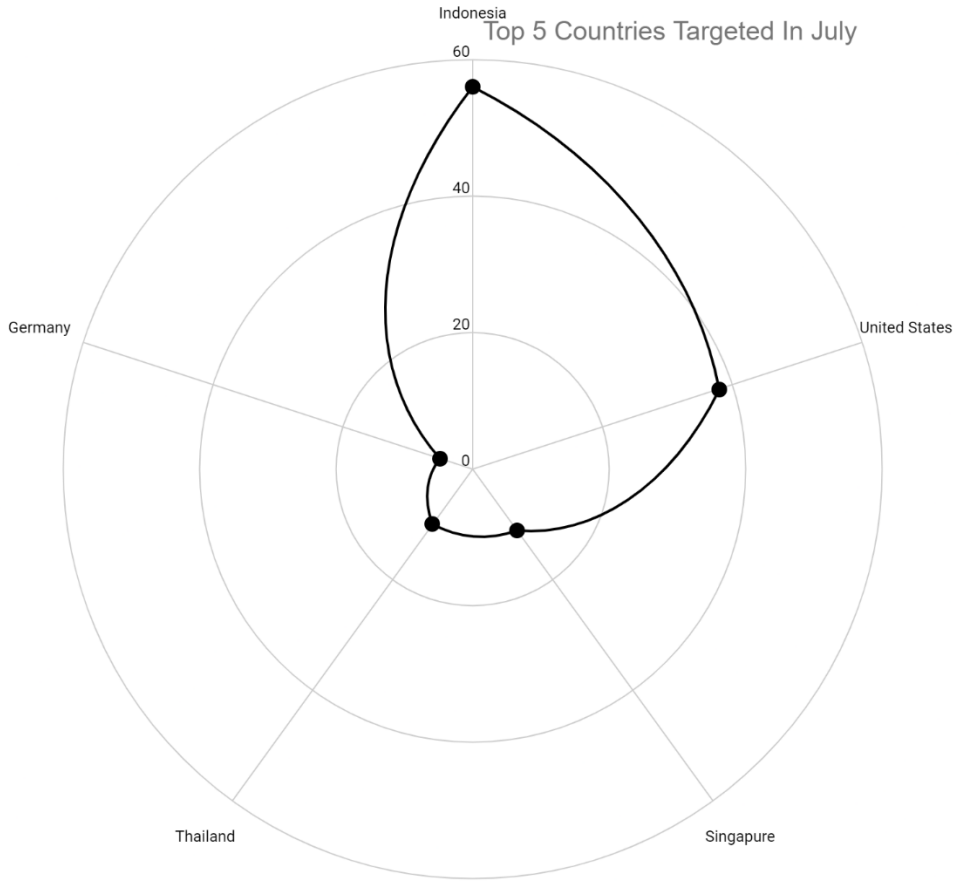
Global Cyber Attacks Per Country



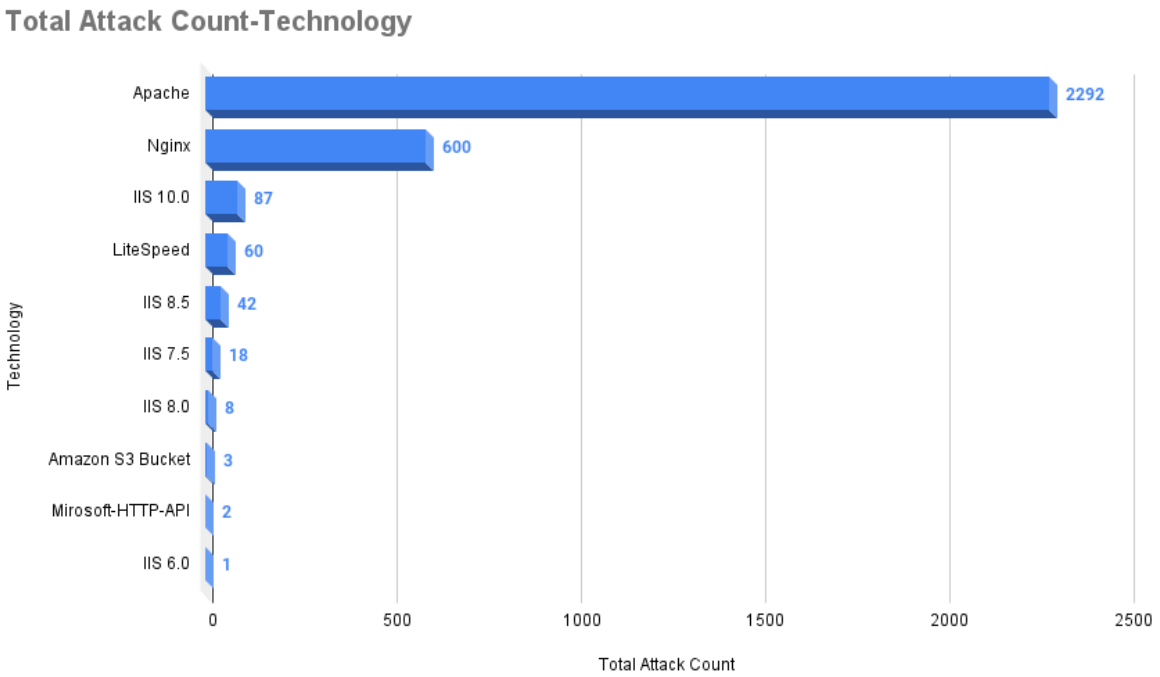
Number of Attacks Per Month

As shown on the graph below, most of the cyberattacks in 2022 occurred in July. If we look at the data gathered by Threatmon, 25th of July was the most active day and Mr.L3RB1 were the most active group and targeted espcalially the United States and Indonesia.





Attacks Most Vulnerable Technologies



When the attacks carried out in a one-year period are monitored, the most attacked technologies as a result of the vulnerabilities revealed were **Apache**, **Nginx** and **IIS 10.0** technologies, respectively.

THREATMON

VULNERABILITIES WITH DATA IN 2022

threatmon.io

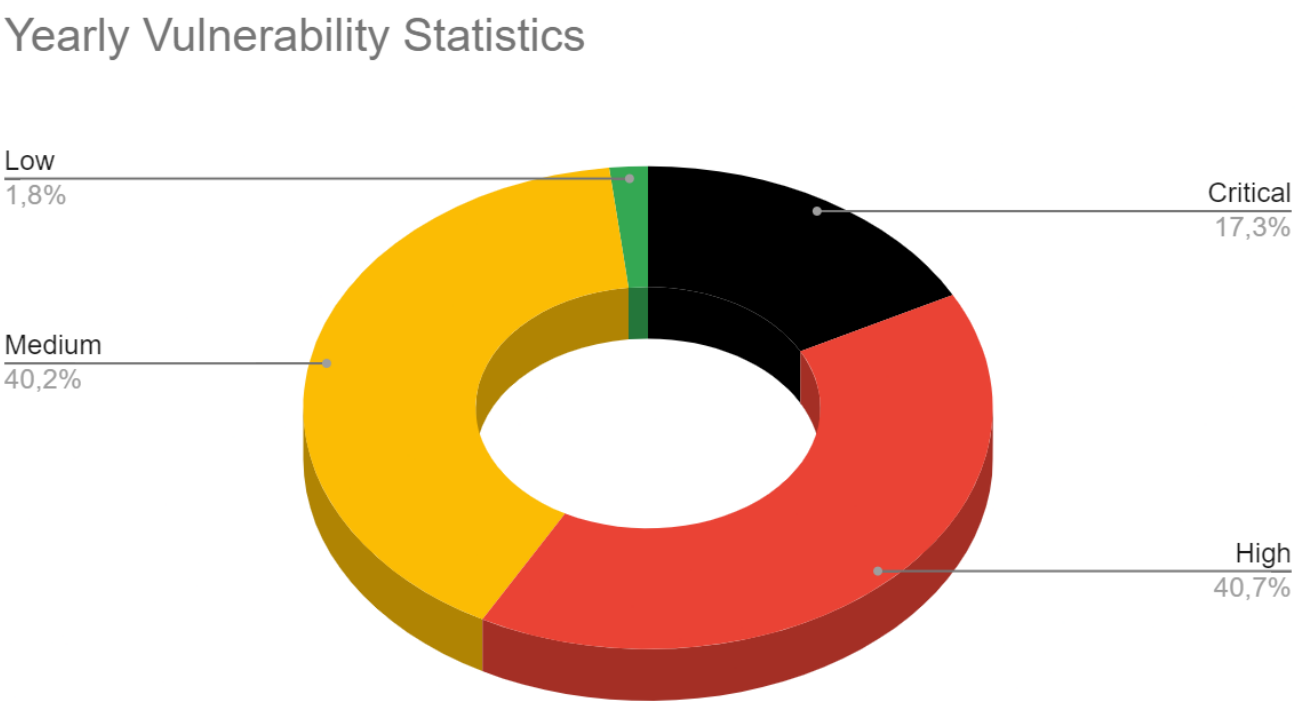
Vulnerabilities with Data in 2022

ThreatMon monitors vulnerabilities on a product basis. It analyzes the products used by its customers and warns its customers with an alert when a vulnerability occurs in these products.

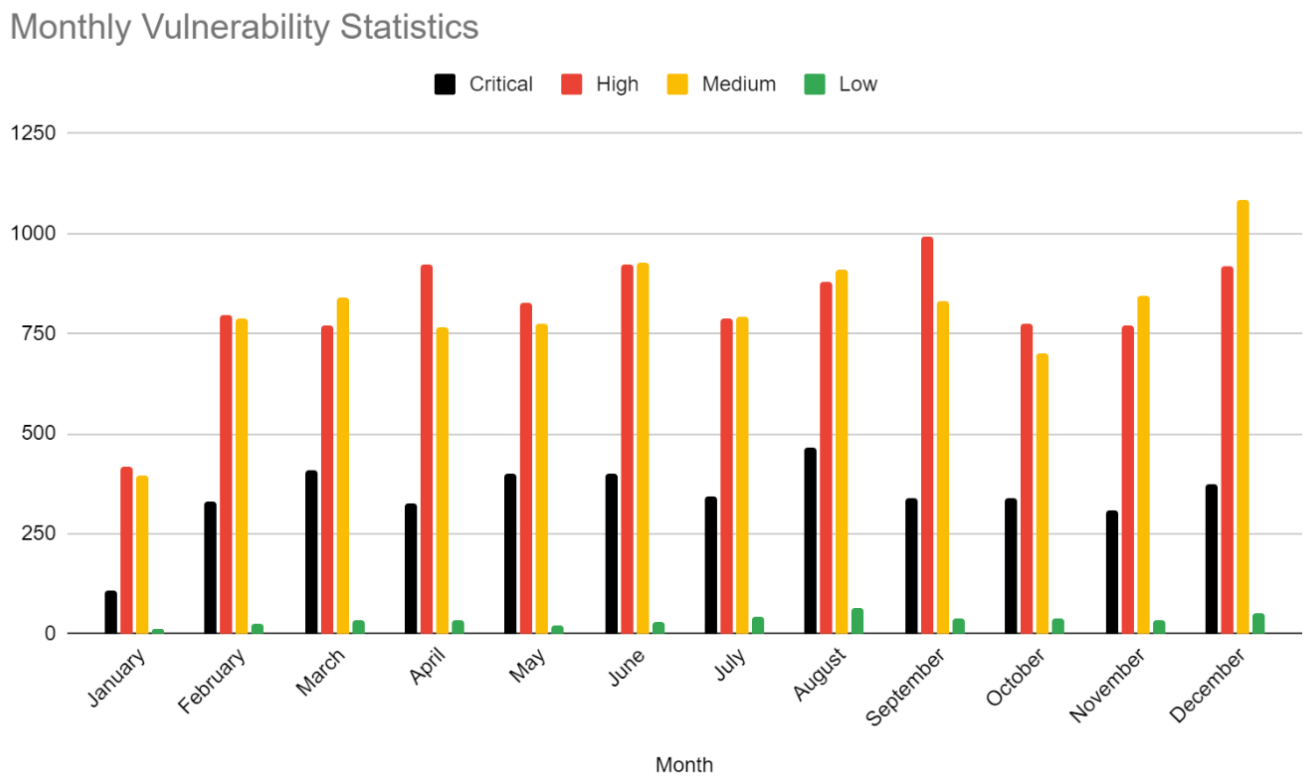
According to the security research conducted by ThreatMon for the year 2022, 24010 vulnerabilities were detected in 2022. Of the detected vulnerabilities, 4145 were at Critical, 9775 at High, 9659 at Medium, and 431 at Low.

In 2022, 24040 security vulnerabilities emerged in products belonging to 4627 different vendors. The vendor with the highest number of security vulnerabilities in its products was Google with 1569 security vulnerabilities.
The most popular vulnerabilities in the products were Cross Site Scripting, Out-of-Bounds Write and SQL Injection, respectively.

In 2022, 24010 vulnerabilities were detected. Of the vulnerabilities detected, 4145 were Critical, 9775 High, 9659 Medium, and 431 Low.



In 2022, 936 in January, 1942 in February, 2059 in March, 2049 in April, 2023 in May, 2280 in June, 1969 in July, 2321 in August, 2198 in September, 1850 in October, 1957 in November, 2426 in December security vulnerability has been detected. Thus, a total of 24010 security vulnerabilities emerged in 2022. December was the month with the most security vulnerabilities in 2022.



The most common CWEs in 2022; Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'), Out-of-bounds Write and Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection').

The most common **CWEs in January** were **Cross-site Scripting**, **Out-of-bounds Write**, **Improper Input Validation**;

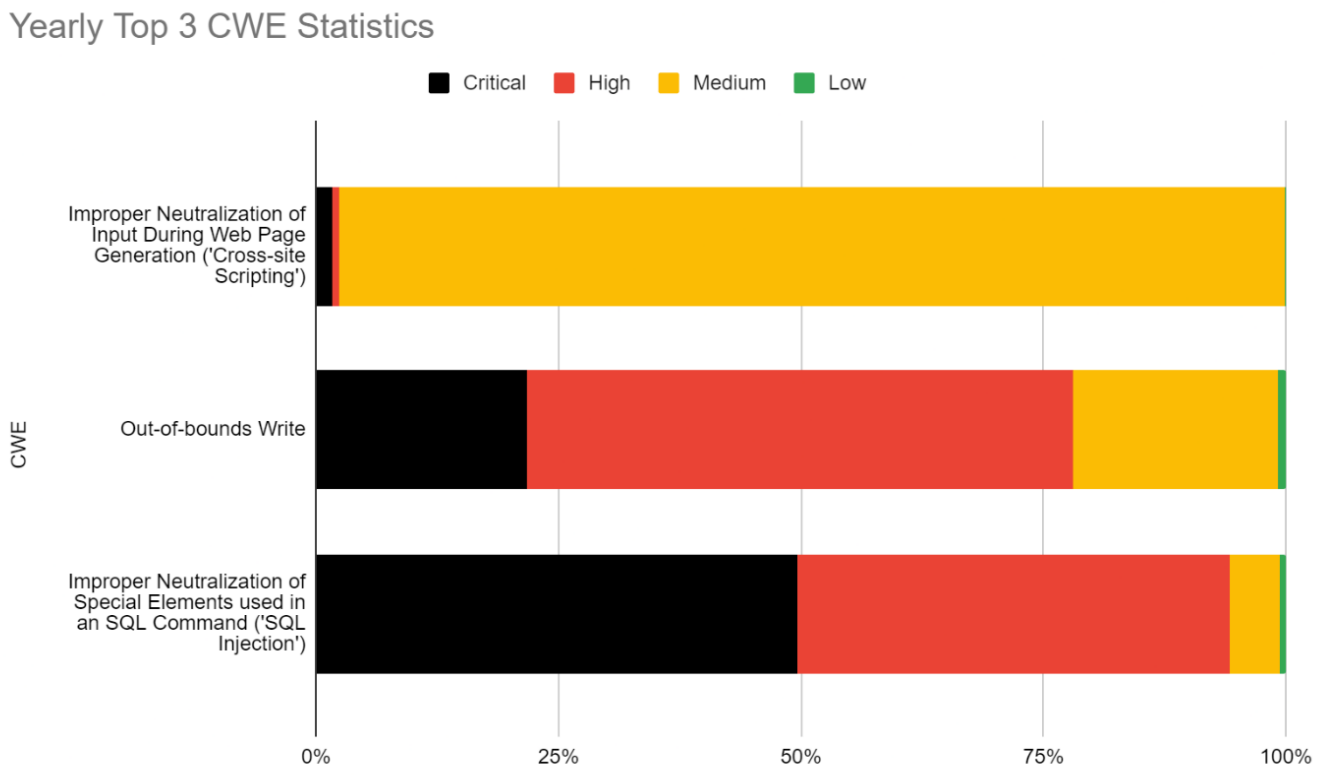
The most common **CWEs in February** were **Cross-site Scripting**, **Out-of-bounds Write**, **Out-of-bounds Read**, while the most common **CWEs in the remaining months** were **Cross-site Scripting**, **Out-of-bounds Write** and **SQL Injection**.

In addition, the month with the greatest diversity of vulnerabilities was recorded as December.

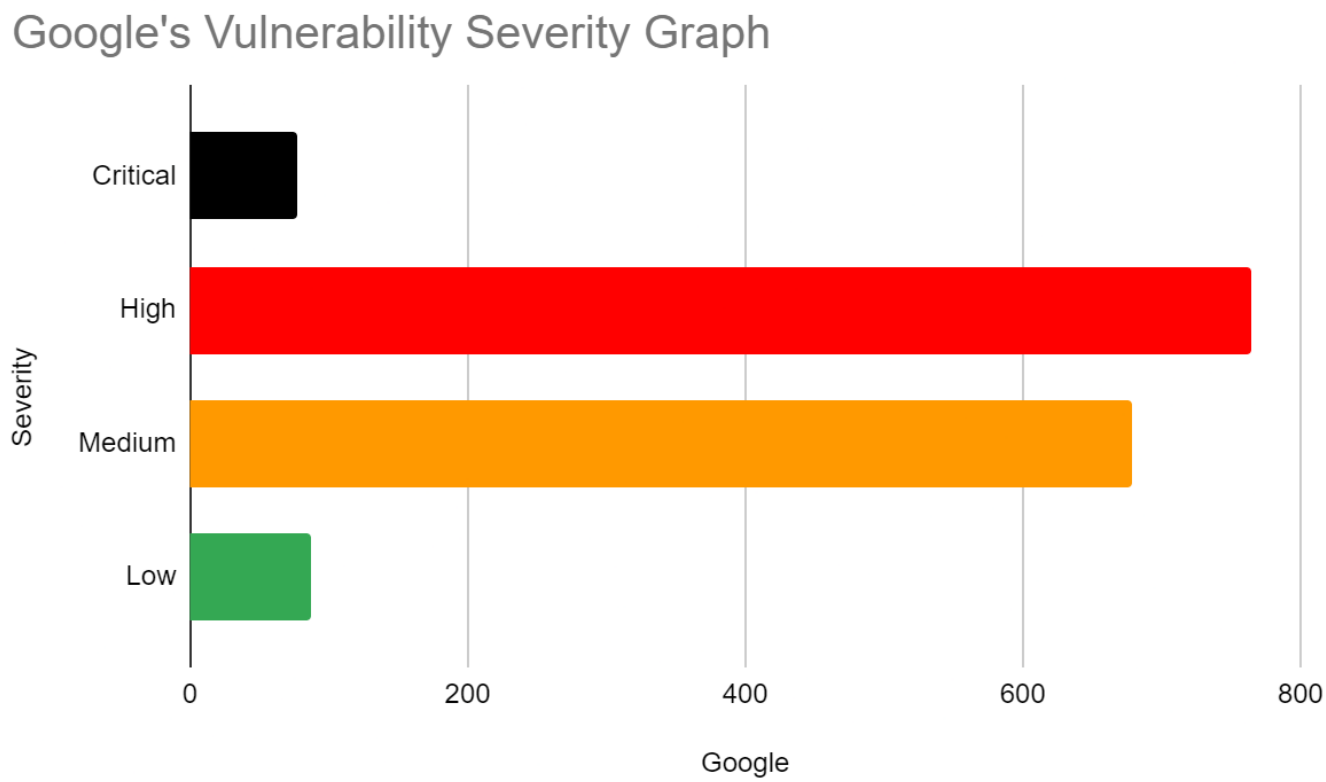
This year, Cross Site Scripting vulnerabilities ranked 1st with 52 Critical, 27 High, 3192 Medium, 4 Low vulnerabilities and a total of 3275 vulnerabilities.

Out of Bounds Write vulnerabilities ranked 2nd with 445 Critical, 1148 High, 433 Medium, 15 Low vulnerabilities and a total of 2031 security vulnerabilities.

SQL Injection vulnerabilities ranked 3rd with 766 Critical, 688 High, 79 Medium, 9 Low vulnerabilities and a total of 1532 security vulnerabilities.



In 2022, security vulnerabilities were detected in 4627 different vendors. The month with the highest vendor diversity was recorded as December. Among the vendors with vulnerable products in 2022, Google ranked first with 78 Critical, 764 High, 679 Medium, 67 Low and 1569 vulnerabilities in total.



Here is a list of CVEs for the most critical vulnerabilities among the security vulnerabilities found on Google this year:

CVE-2021-39675	CVE-2022-20120	CVE-2022-20361	CVE-2022-35938
CVE-2022-0097	CVE-2022-20229	CVE-2022-2587	CVE-2022-36852
CVE-2022-23587	CVE-2022-1312	CVE-2022-20400	CVE-2022-20386
CVE-2021-39635	CVE-2022-20222	CVE-2022-20402	CVE-2022-20385
CVE-2021-39658	CVE-2022-2010	CVE-2022-20365	CVE-2022-35937
CVE-2022-0290	CVE-2022-20216	CVE-2022-20122	CVE-2022-20389
CVE-2021-39616	CVE-2022-0973	CVE-2021-39815	CVE-2022-20388
CVE-2022-23425	CVE-2022-1799	CVE-2022-20381	CVE-2022-35939
CVE-2021-39723	CVE-2022-1309	CVE-2022-20237	CVE-2022-20390
CVE-2021-39737	CVE-2022-33719	CVE-2022-20239	CVE-2021-0942
CVE-2021-39708	CVE-2022-20403	CVE-2022-20387	CVE-2022-3075
CVE-2022-25818	CVE-2022-20405	CVE-2022-20391	CVE-2022-41880
CVE-2021-39710	CVE-2022-20378	CVE-2022-36856	CVE-2022-39887
CVE-2022-3890	CVE-2022-41900	CVE-2022-4135	CVE-2022-41910
CVE-2022-20473	CVE-2022-41902	CVE-2022-42529	CVE-2022-20472

THREATMON

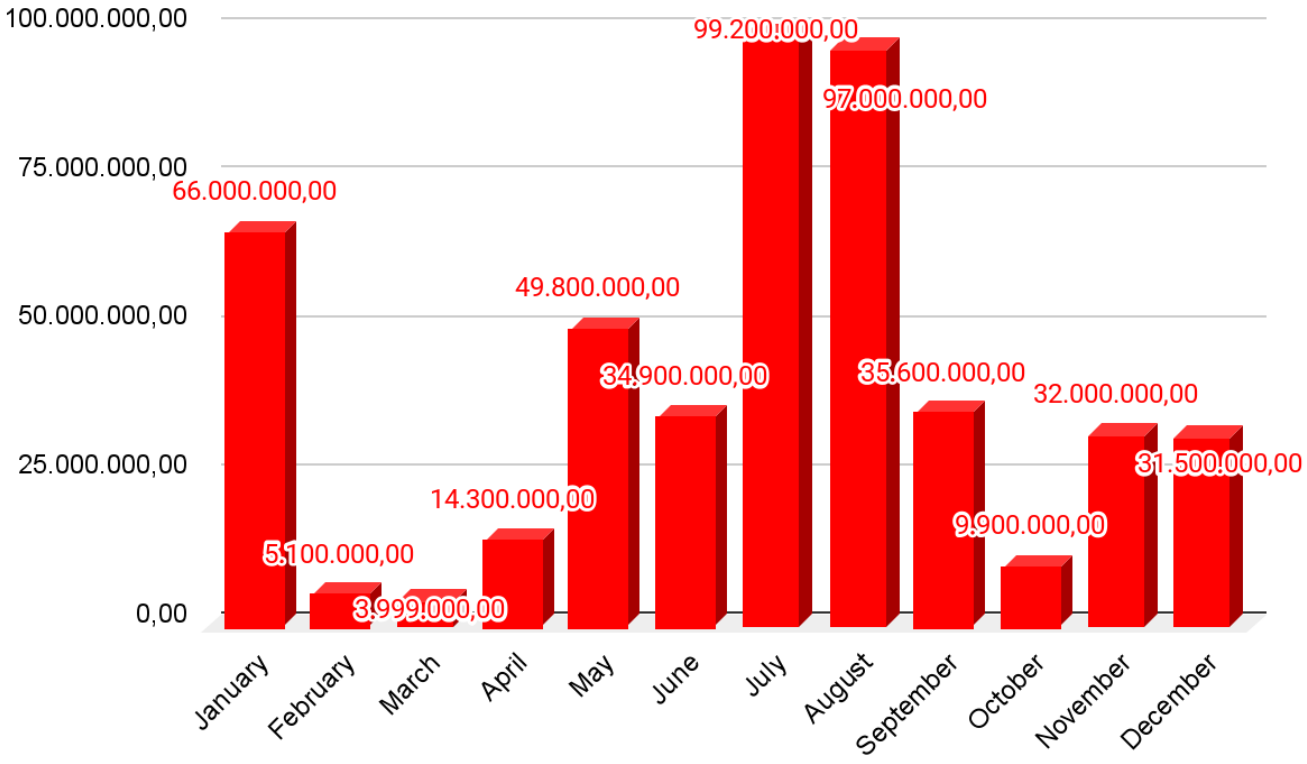
CYBER ATTACKS AND DATA BREACHES IN 2022

threatmon.io

Cyber Attacks and Data Breaches in 2022

ThreatMon monitors data breaches and cyber attacks. It announces these attacks and news to its customers in the fastest way possible. ThreatMon identified and analyzed cyberattacks and data leaks in 2022.

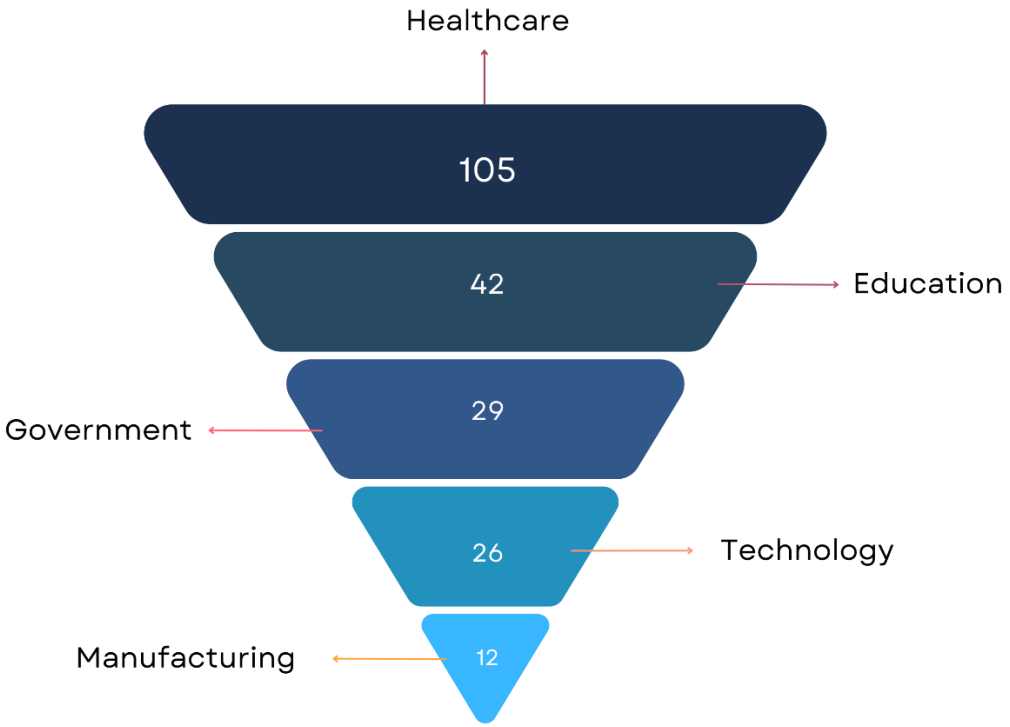
- The most breached month was July with **99.2 million records**.
- The least breached month was October with **9.9 million records**.
- The average number of records breached per month is **48.18 million records**.
- The total number of records breached over the course of the year was **578.2 million records**.



Statistics of Breaches by Industries

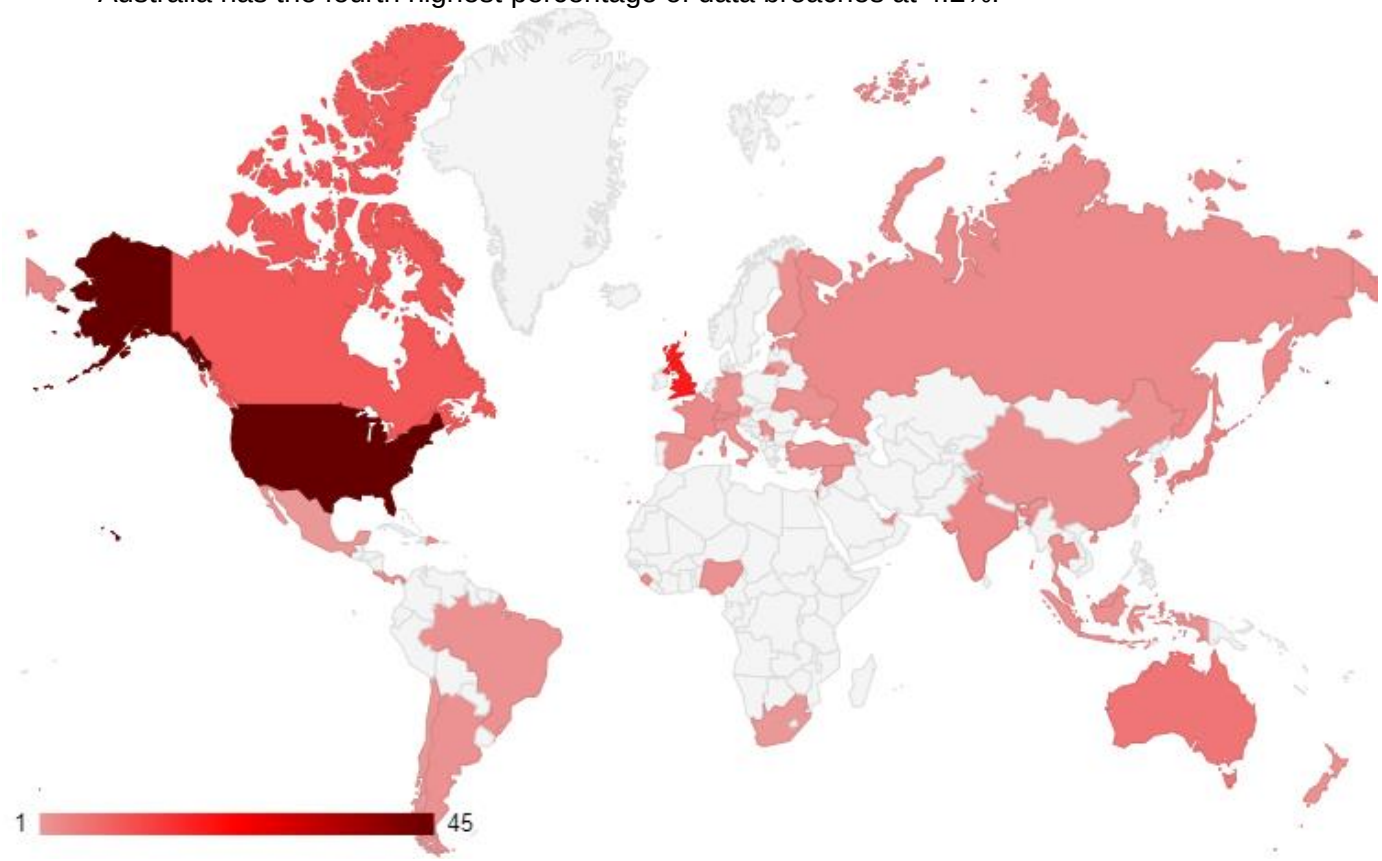
- The most breached sector is healthcare with 25.3% of total breaches.
- The next highest sector is the Government with 7.7% of total breaches .
- Education sector is also higher at 10% of total breaches.
- Other sectors with a significant percentage of breaches include finance with 2.1% , insurance with 3.4% and technology with 6.2% .

The Healthcare sector experienced the highest number of cyberattacks among all sectors, accounting for 25.3% of total breaches. The next highest sector is the government, with 7.7% of total breaches. The education sector also had a high number of breaches, with 10% of total breaches. Other sectors that experienced a significant number of breaches include finance (2.1%), insurance (3.4%), and technology (6.2%). This highlights the need for increased security measures in these sectors to protect against cyberattacks. Additionally, it is important to note that in general, these sectors are highly sensitive and confidential, which makes them more vulnerable to cyber criminals.



Statistics of Breaches and Cyber Attacks by Countries

- The United States has the highest percentage of data breaches at 32%.
- The United Kingdom has the second highest percentage of data breaches at 13.5%.
- Canada has the third highest percentage of data breaches at 7.1%.
- Australia has the fourth highest percentage of data breaches at 4.2%.



THREATMON

IOC DATA COLLECTED IN 2022

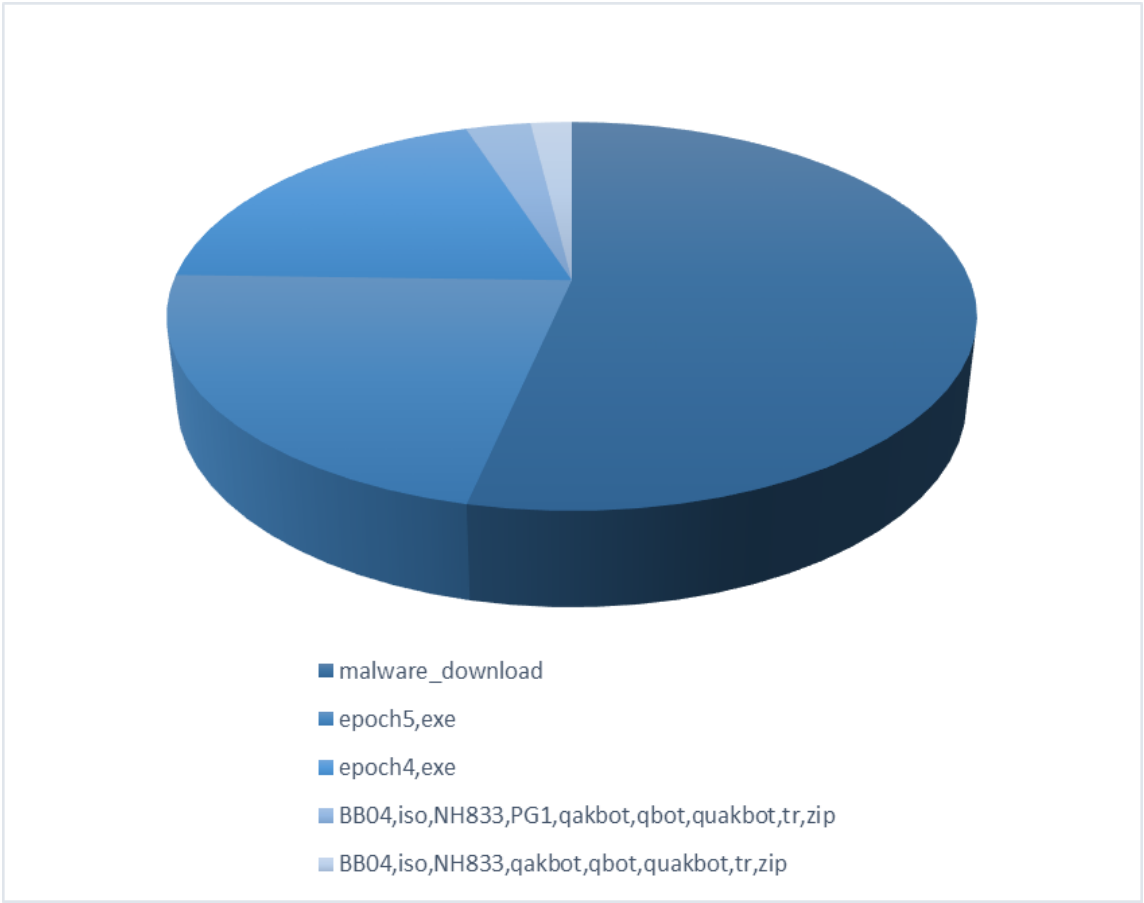
threatmon.io

IOC Data Collected in 2022

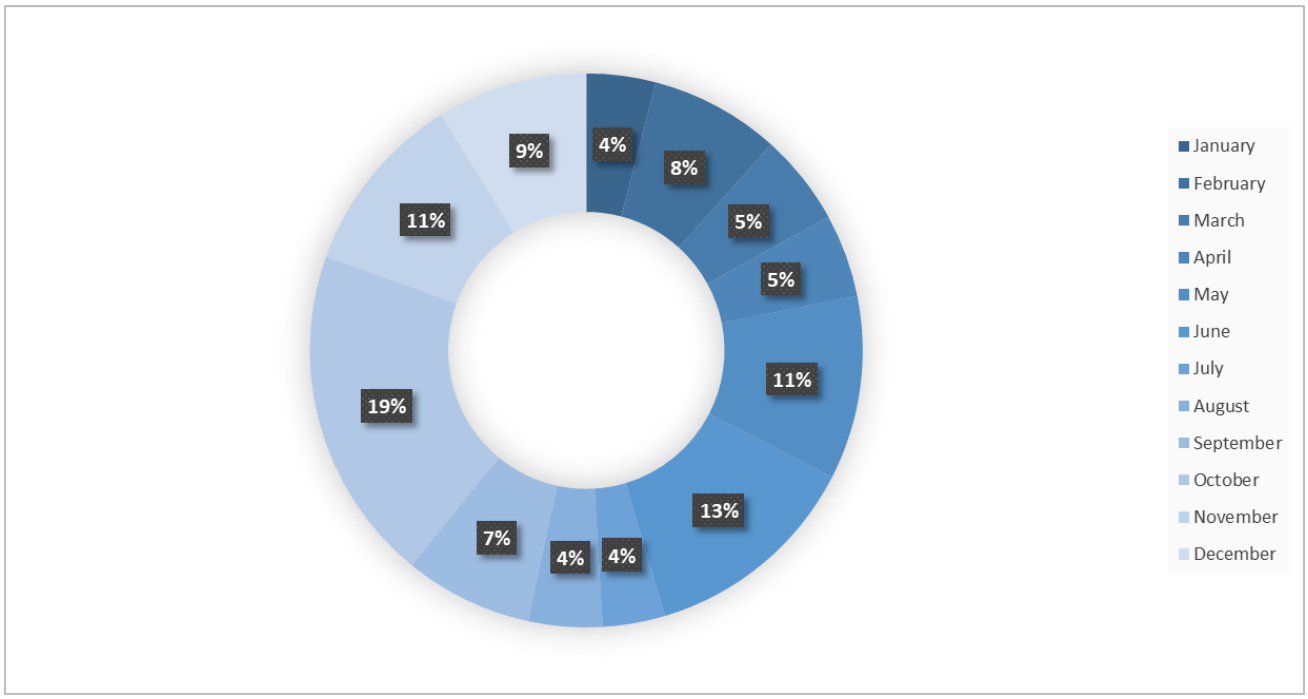
ThreatMon stores IOC information extracted from multiple sources and by its own analysts in its IOC Feed. It provides data flow to its customers with IOC information.

IOC tags are an important element of incident response and threat hunting, they are used to identify specific pieces of information that may indicate malicious activity on a system or network. They can be shared among security researchers and organizations to improve the ability to detect and respond to new or emerging threats. Furthermore, they can be used to create custom signatures or rules for intrusion detection systems, firewalls, and other security tools, helping to identify and isolate malicious activity.

Most Tagget IOC Data



A monthly schematized version of the IOC information collected by ThreatMon is given in the image below. The IOC information obtained from many different sources and obtained as a result of the analysis of malware by their own analysts has been classified according to the months.



THREATMON

THREATMON'S VIEWS ON 2023

threatmon.io

ThreatMon's Views on 2023

In 2022, ransomware attacks increased rapidly. These attacks infiltrated the data and systems of companies and governments and caused severe damage as a result of the encryption of this data. In 2023, the number and effectiveness of ransomware attacks are expected to increase. This is because hackers are using artificial intelligence and other advanced technologies, making these attacks even easier and more effective. In addition, the failure of companies and governments to take the necessary measures for cyber security will also lead to an increase in attacks. In 2023, companies and governments should improve and update their cyber security measures to protect themselves against ransomware attacks.

APT groups continued to be active in 2022. These groups worked to infiltrate important data and systems of governments and companies. In 2023, the activity and number of APT groups are expected to increase. Hackers will use artificial intelligence and other advanced technologies to further strengthen APT attacks and work to reach more targets. In addition, in 2022, state-sponsored APT groups in the cyber world joined the war between Russia and Ukraine on land. If the conflict continues, it is predicted that Russian and pro-Ukrainian APT groups will increase their power and carry out higher-scale attacks. Therefore, in 2023, governments and companies will need stronger protection systems against APT attacks. In addition, cybersecurity professionals and employees must be vigilant and alert to APT attacks and be able to identify and manage these threats.

Hacker groups continued to be active in 2022. These groups preferred to hack websites for economic, political or social purposes. In 2022, hacker attacks against state institutions caused damages such as data leaks and disruption of system capacities. In 2023, the activity and number of hacker groups is expected to increase. Using artificial intelligence and other advanced technologies, these groups will further strengthen their attacks and work with the aim of reaching more targets. Therefore, government organizations will need stronger protection systems against hacker attacks in 2023. In addition, cybersecurity professionals and employees must be vigilant and alert to hacker attacks and be able to identify and manage these threats.

Data leaks remained a frequent problem in 2022. Hackers targeted the databases of government agencies, large corporations and other organizations with personal data, leaking or marketing the data. In 2023, the frequency and quantity of data leaks are expected to increase. Data leaks can range from the disclosure of individual personal data to the leak of state secrets or critical information. Therefore, organizations should use up-to-date technologies, configurations and training programs to protect the security of their data and prevent leaks in 2023. In addition, these organizations should be regularly audited and updated for the security of their data.

IOC (Indicator of Compromise) data is data that identifies certain signs or characteristics of cyber attacks. In 2022, emerging IOC data can be used as an important resource for cyber security and can help identify, monitor and prevent cyber attacks. In 2023, new IOC data is expected to emerge and existing data is expected to be updated due to the update of cyber attacks. Therefore, organizations should use the IOC data and other cybersecurity resources provided by their cybersecurity teams and keep them continuously updated to identify, monitor and prevent cyber-attacks.

45305 Catalina cs St 150, Sterling VA 20166