CrowdSec

The Majority Report

Outnumbering Cybercriminals All Together

Q2 2023

Table of Contents

CrowdSec is a modern, collaborative cybersecurity company

About Us

CrowdSec is a modern, collaborative cybersecurity company committed to proactively safeguarding your digital assets.

With its open source software developed for the SOC and DevSecOps community and powered by a growing community of 65,000+ active users, CrowdSec is revolutionizing cybersecurity by capitalizing on collective intelligence to detect and mitigate emerging and targeted threats in real-time.

This collaborative approach empowers every user and provides an evolving defense against cyber threats.

What Is the Majority Report?

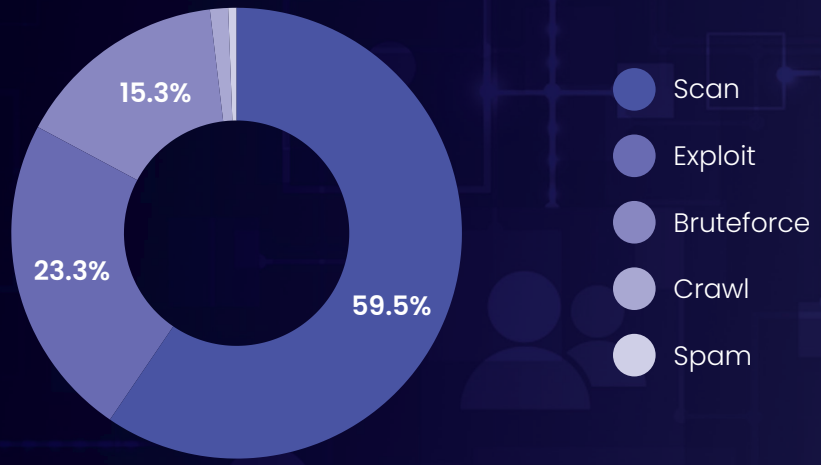
Inspired by the 2002 film, *Minority Report*, the CrowdSec team created the Majority Report to showcase the power of crowdsourced data in detecting malicious behavior and preventing imminent cyberattacks. In this report, you will find evidence of the effectiveness of the CrowdSec network in spotting and blocking malicious IPs before they get a chance to breach a system.

Overview of Cyber Threats Worldwide

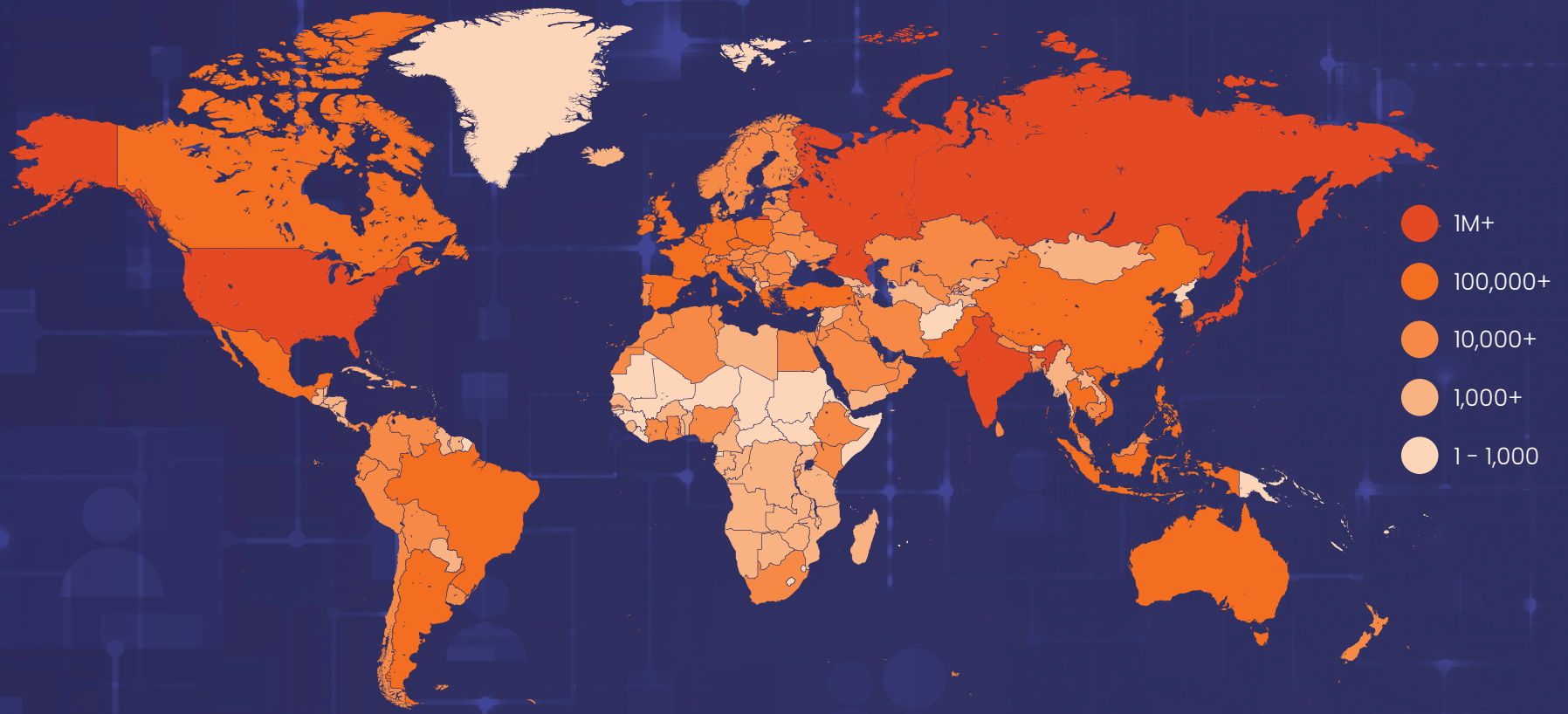
The map on the following page highlights the country of origin of the IP addresses reported as malicious during Q2 2023.

Note: The data shown on the map is unlikely to represent the nationality of the attacker but rather the localization of compromised assets used to perpetrate malevolent activities.

Most Common Threats



Overview of Cyber Threats Worldwide



Unique Attack Vectors Reported

146

Trends and Analysis

Most Common Threats

#1 Scan

The scan attack (also known as port scanning or network scanning) refers to an attacker systematically scanning the network for open ports, services, or vulnerabilities that they can exploit. Once a vulnerability is discovered, the attacker can launch the following attacks, such as gaining unauthorized access, launching a Distributed Denial-of-Service (DDoS) attack, or compromising the target's infrastructure. CrowdSec automatically bans an IP that has been identified as a scanner. The CrowdSec community blocklist also provides more than 20,000 IPs matching this category.

#2 Exploit

The exploit attack refers to an attacker trying to exploit known vulnerabilities in order to break through your system — one of the most dangerous attacks you can encounter. Similar to remediating the scanning attack, CrowdSec identifies malicious IPs attempting to exploit known vulnerabilities and blocks them.

#3 Brute force

This type of attack is often mistaken for the background noise of the internet. What happens, in reality, is that attackers are trying to exploit common weak passwords set by default. One of the main targets of this attack is SSH services, the most common remote administration service on Linux servers. CrowdSec covers a wide range of attack vectors to detect brute-force attacks on multiple services (WordPress, SSH, Telnet, FTP, Samba, common databases, etc.). The CrowdSec remediation components act at the firewall level to drop the packets on malicious connection attempts.

#4 Crawl

A crawler is an automatic process that jumps from link to link on your website. Search engines or security companies can do this for legitimate reasons, but it can also serve as the initial step for identifying vulnerabilities or extracting valuable information. Crawling could include activities like discovering competitor pricing details in the case of e-commerce websites. CrowdSec seamlessly reads the logs of your reverse proxy or web server in order to detect this behavior and take action to remediate it.

Trends and Analysis

What Is an Autonomous System?

An Autonomous System (AS) is an organization in charge of operating a collection of IP addresses. These addresses are organized in IP ranges and can be disposed of by the organization. **It is part of the organization's duty to identify compromised network assets and take action in case IP abuse is reported**. Autonomous systems are uniquely identified online using an Autonomous System Number (ASN).

How to Compare and Rank AS?

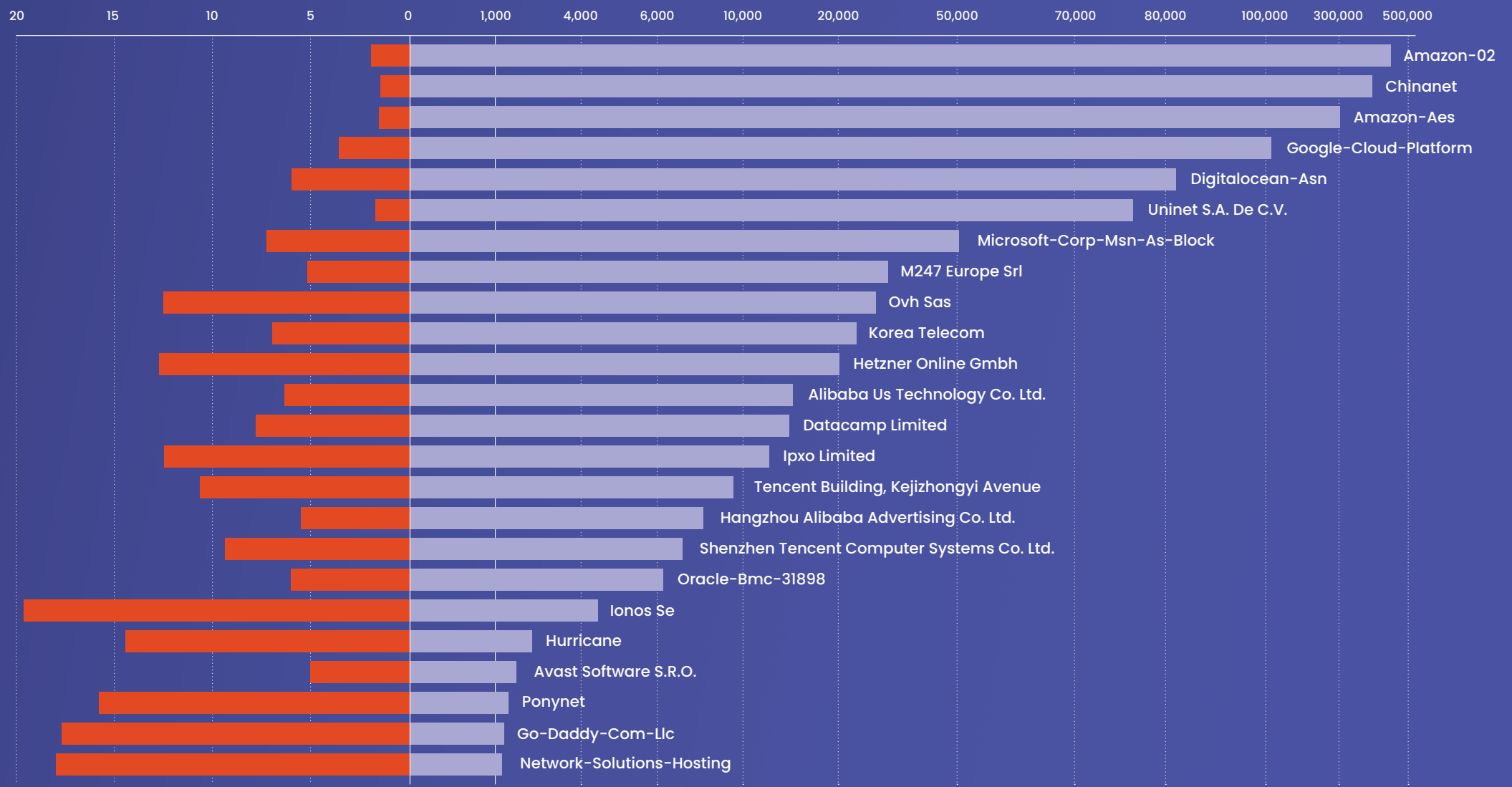
Number of IPs reported: Measures the number of compromised assets inside the AS. While looking simply at the number of compromised assets seems like a reasonable approach, there are more accurate methods of evaluating AS. Not all operators are equal in size. Inevitably, users report a greater number of IPs affiliated with big operators. However, smaller operators own fewer IPs — therefore receiving fewer reports — but may be hosting riskier services than others.

Number of CrowdSec reports: Measures the reporting power of the community. The more an attack hits the machines, the higher the metric.

Malevolent Duration (MD): This metric refers to the number of days for which the community reports an IP. The average MD of all the IPs in the same AS indicates the operator's due diligence in identifying and dealing with compromised assets.

The following diagram compares the most reported Autonomous Systems based on the number of reported IPs versus Malevolent Duration (in days).

Average Malevolent Duration (In Days) of Most Reported AS



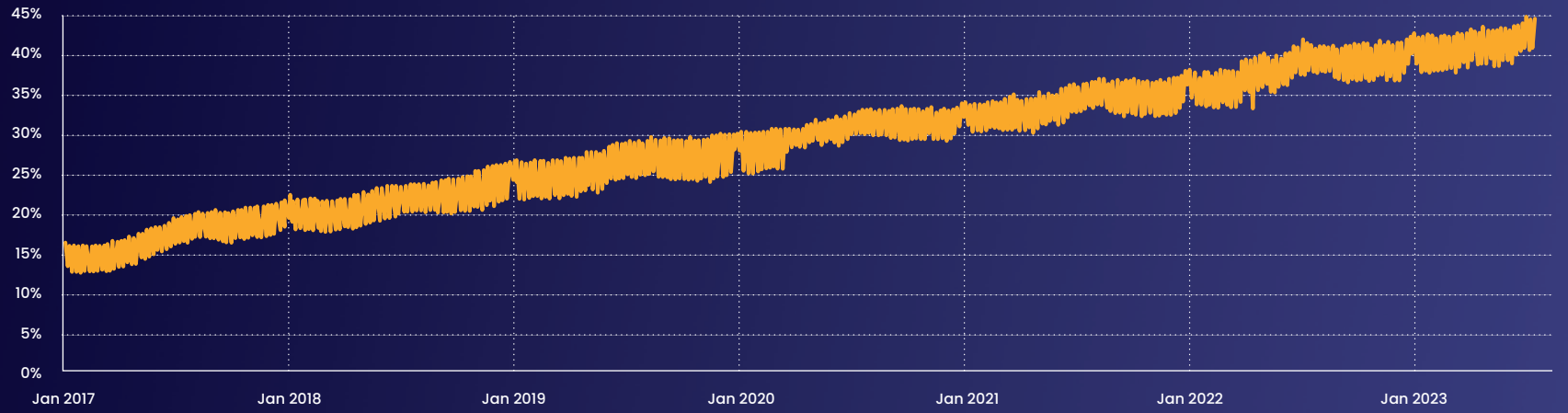
Trends and Analysis

The Rise of IPv6 in Cybercriminal Activities

IPv6 (Internet Protocol version 6) is the most recent version of the IP and was developed as the successor to IPv4 to address the limitations and exhaustion issues of IPv4 addresses. IPv6 provides an expanded addressing scheme compared to IPv4, allowing for a significantly larger number of unique IP addresses. While IPv4 uses 32-bit addresses and supports approximately 4.3 billion unique addresses, IPv6 uses 128-bit addresses, resulting in an enormous address space that can support approximately 3.4 × 10^38 unique addresses.

Although IPv6 was originally introduced in December 1998 as a Draft Standard for the IETF, it was in July 2017 that it was ultimately ratified as an Internet Standard. According to Google Statistics, the adoption of IPv6 between July 2017 and July 2023 shows a 120% increase, while in July 2023, 43% of all users accessed Google over IPv6.

Users Accessing Google Over IPv6



Note: What Google refers to as users include both human users and machines — i.e., bots.

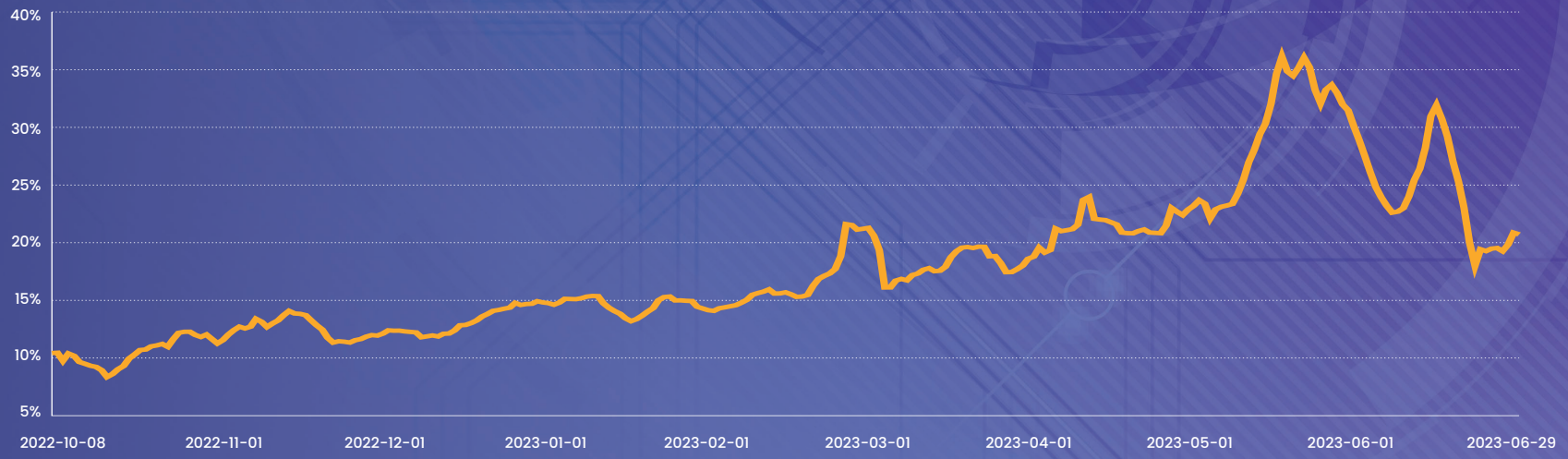
Trends and Analysis

With such high adoption, it was inevitable that IPv6 eventually started registering on cybersecurity radars. For October 2022–June 2023, the CrowdSec network detected increased new threats linked to IPv6 addresses.

In October 2022, IPv6 represented 10% of the total number of reported IPs. By the end of June 2023, this percentage doubled, with IPv6 now representing 20% of all reported IPs, and CrowdSec identifies an upward trend.

It is also important to note that the rate of IPv6 addresses reported went up to 35% between May and June 2023, which coincides with a period of increased scanning attacks, according to the data collected by the CrowdSec network.

Percentage of IPv6 Addresses Reported as Malicious



Trends and Analysis

The Role of VPNs and Proxies in Cybercriminal Activities

VPN's rise to popularity over the past few years sounded the alarm for many organizations. The joint action by Europol and 10 other countries in January 2022 to take down VPNLab.net — a VPN provider whose services were being used in support of serious criminal acts — seemed to reinforce the concern that VPNs are a convenient tool for cybercriminals.

However, contrary to popular belief, data collected by the CrowdSec network indicates that only **5% of reported IPs are flagged as VPN or proxy users**.

Top Autonomous Systems Hosting the IPs Which Are Flagged as VPNs or Proxies

AS Number	AS Name	Country	Number of IPs Flagged
55286	SERVER-MANIA	CA	1417
14061	DIGITALOCEAN-ASN	US	1155
35048	Biterika Group LLC	RU	792
212238	Datacamp Limited	UK	779
58065	Packet Exchange Limited	UK	771
174	COGENT-174	DE	726
24940	Hetzner Online GmbH	DE	720
9009	M247 Europe SRL	RO	683
36352	AS-COLOCROSSING	US	678
55081	24SHELLS	US	626

Note: CrowdSec has an expiration delay of a maximum of 7 days on the community blocklist, making sure that previously compromised IPs that the legitimate owner has restored do not continue to be blocked. **Disclaimer:** The nature of the services that the operator hosts and their potential attractiveness for an attacker are not taken into account in this analysis.

Trends and Analysis

Proactive Security Posture

In most cases, a malevolent actor will likely use legitimate assets to compromise other systems. Hosters and cloud providers play a huge role in this as they are the ones renting the machines — that will potentially get compromised — and owning the public IPs they are associated with.

When one of the IPs they lend to a user becomes malevolent, they can act quickly to block outgoing or incoming traffic, stopping the infected machine from performing further attacks. However, if hosters, cloud providers, or the legitimate owners of the assets do not act swiftly and responsibly to mitigate reported IPs, the attacks will continue.

The most proactive hosters even take a step further by analyzing the behavior of the machines and identifying suspicious behavior. For example, if a corporate website suddenly starts scanning the internet address space or sending millions of emails per day, it has most likely been infected, and the malware is trying to spread.

The Importance of the Malevolent Duration Metric

The ability to quickly deal with infected machines within your network reported by third parties, as well as proactively identifying infected machines based on behavioral patterns, significantly impacts how long a machine stays infected — as presented earlier in the diagram Average Malevolent Duration (In Days) of Most Reported AS.

Hosters and cloud providers that exhibit low MD provide businesses with a greater security incentive to adopt their products. Low MD translates to a lower risk for a business to inherit a machine that has been flagged as malevolent. By extension, this also minimizes the risk of a legitimate business asset being preemptively blocked by partners, prospects, or potential customers.

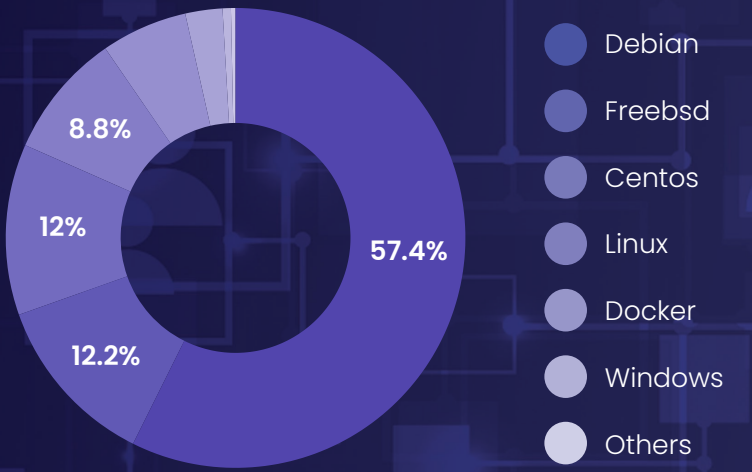
The Global CrowdSec Network

The map on the following page shows the countries where CrowdSec Security Engines are installed. Having a wide diversity is a key factor in covering a large number of attack vectors and discovering emerging threats in real-time.

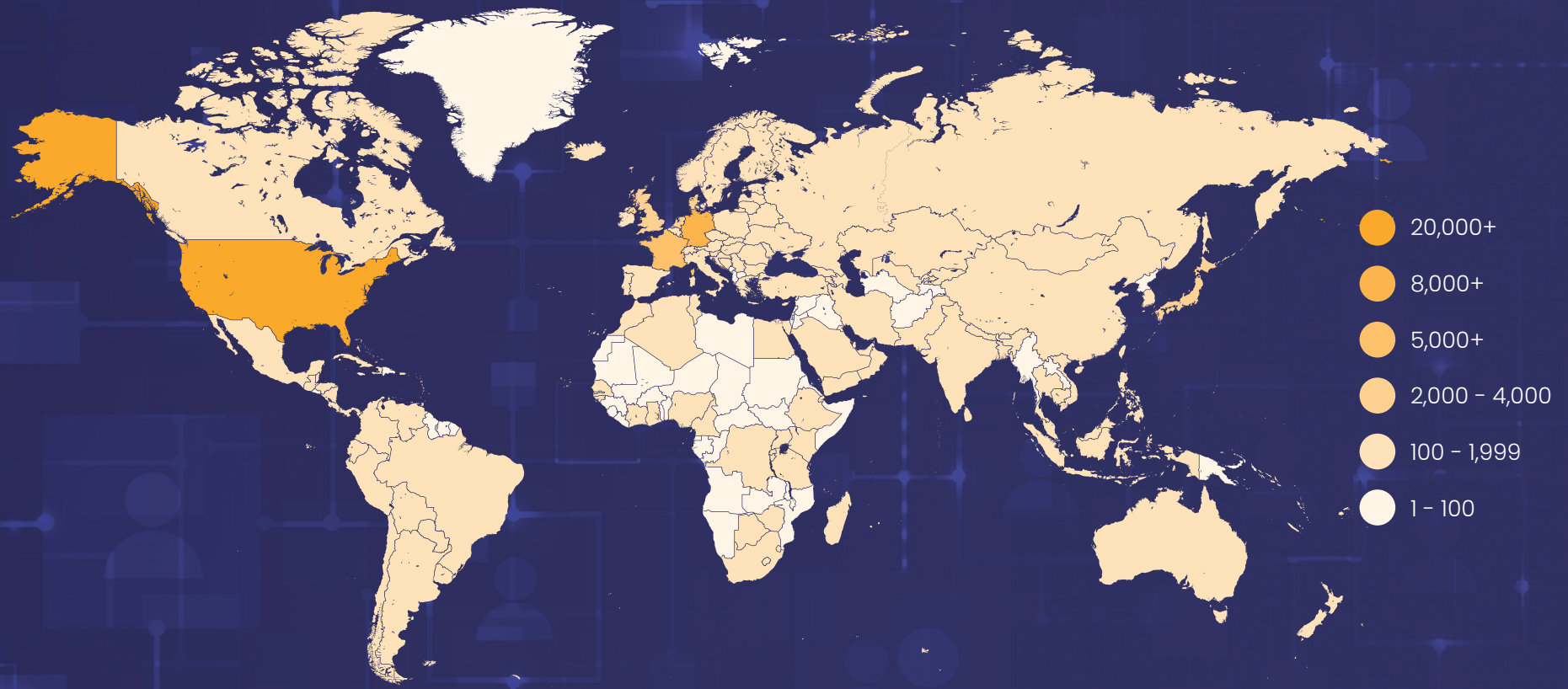
Top AS Hosting CrowdSec Security Engines

	Top 10 AS	Country	% Sec Engines
1.	OVH SAS	FR	4.7
2.	UNIFIEDLAYER-AS-1	US	4.6
3.	Hetzner Online G...	DE	3.7
4.	SAKURA Internet I...	JP	2.8
5.	NETWORK-SOLUT...	US	2.6
6.	GOOGLE-CLOUD...	US	2.3
7.	A2HOSTING	US	1.8
8.	DIGITALOCEAN-A...	US	1.6
9.	IONOS SE	DE	1.6
10	Previder B.V.	NL	1.4

Platforms Used by the Community



The Global CrowdSec Network



Active Installations
65,000+

Signals Shared Daily
14.5M

Malicious IPs Reported in Q2
12.2M

Data Sources & Methodology

CrowdSec offers a powerful and innovative approach to threat detection and prevention by leveraging the collective intelligence of 65,000+ active users all over the world, who share data and insights to help identify new threats and improve automated security response.

It comes with behavioral detection scenarios (attack vectors) to detect and identify a wide range of threats, as well as Remediation Components to take action upon the alerts raised. And, of course, it is free and open source.

Data presented in this report are threats reported by the CrowdSec software network during Q2 2023. Alerts are different from usual user data as they only contain the type of attack, the timestamp, and the source (IP). Users can choose not to disclose their alerts. In this case, users will not benefit from the community blocklist.

This report does not include alerts coming from modified scenarios at this time.

Metadata enrichment comes from MaxMind GeoIP.

Trust Score: Reporters are scored based on their lifetime in the CrowdSec network and their performance compared to our higher-ranked members and our honeypot network.

Diversity: Reporters must be located in many different AS.

Profiling: External tools help to determine the likelihood of a machine being compromised based on its description: open ports, exposed services, known vulnerabilities, etc.

Range Reputation: IP Ranges reported for the first time are reviewed by a human before being added to the community blocklist.

Expiration: Malicious IPs are shared for 7 days in the community blocklist and are then expired if no longer reported.

Install the CrowdSec Security Engine in your infrastructure, where it can access your exposed server logs.

Design custom behavioral detection scenarios or Remediation Components and share them with the community on the CrowdSec Hub.

Share logs and intelligence about attacks in our dedicated Console.

Glossary

IoC — Indicator of Compromise refers to information or evidence that can be used to detect a security incident or a potential breach. In this report, aggressive IPs constitute IoC.

SOC — Security Operations Center is the team within an organization that is responsible for monitoring, detecting, analyzing, and responding to cybersecurity incidents and threats.

CTI — Cyber Threat Intelligence provides insights into potential or existing threats helping organizations understand the threat landscape, identify emerging risks, and enhance their security posture.

SE — CrowdSec Security Engine is a lightweight software that identifies malicious behavior and shares the related IP across the CrowdSec Network, instantly protecting all users from the identified threat.

Remediation Component — CrowdSec Remediation Components are software components that propagate decisions to the enforcement points of the security infrastructure such as firewalls or web servers.

Poisoning — A malicious attempt to feed a crowdsourced database with incorrect inputs.

Attack Vectors (Scenarios) — Showcase attack behaviors (brute force, exploit, scan, etc.).

CrowdSec

Embrace the power of collective intelligence and protect your systems.

Want to make the internet a safer place?

The Majority Report uses the wisdom of the crowd to identify emerging trends, threats, and malicious behavior.

Contribute to the next version of the Majority Report, by becoming a member of the CrowdSec network and sharing signals on aggressive IPs and malicious behavior.

Try the CrowdSec Security Engine today!

Download Majority Report

github.com/crowdsecurity

@Crowd_Security

CrowdSec

@crowdsec6295

crowdsec.net

academy.crowdsec.net