CrowdSec

The MAJORITY REPORT

Outnumbering cybercriminals all together

#1 - Q4 2021

About us

CrowdSec is a french company, created in 2020, developing a **free**, **open-source** & **collaborative** cybersecurity software.

The CrowdSec solution operates as a new generation **IPS/IDS** software that prevents your exposed machines from intrusions and offers a way of mitigating against malicious IPs.

CrowdSec is building a **massive CTI**, where users reports and share informations about threats on the Internet to outnumber attackers.

TABLE OF CONTENTS

Overview of the world's cyber threats 01

CrowdSec Network Strength 02

Trends & Expert analysis 03
Attack Types
IP Malevolence duration

Methodology & Data sources 04

Overview of the world's cyber threats

Changes (⇧) are calculated from the last quarter

	Top ten Countries	Bad IP
1.	United States	196.9K
2.	China	157.7K
3.	Germany	141K
4.	Taiwan	80.4K
5.	Ukraine	69.4K
6.	Vietnam	38.3K
7.	India	32.9K
8.	France	32.2K
9.	Russia	30.8K
10.	Brazil	30.5K

Malicious IPs reported
1.1M

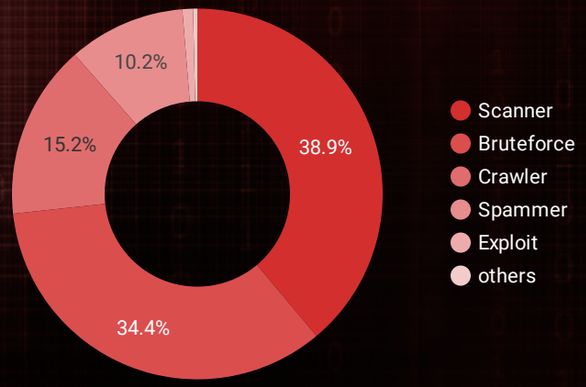
For this quarter
748.5K
No data

Total threats reported
28.8M

For this quarter
24.7M
No data

New IPs reported by day
12,947
No data

Threats reported by day
364,350
No data



Top threats reported by the Community

detail of known scenarios

Malevolent duration

	Top ten AS	Bad IP	days
1.	Deutsche Telekom AG	36,765	6
2.	Chinanet	34,684	10
3.	AMAZON-02	29,115	3
4.	DIGITALOCEAN-ASN	17,378	23
5.	Vodafone GmbH	15,657	11
6.	CHINA UNICOM China169 B...	15,129	11
7.	Kyivstar PJSC	12,660	7
8.	Data Communication Busin...	12,293	10
9.	AMAZON-AES	9,236	7
10.	Telefonica Germany	6,414	1

CrowdSec

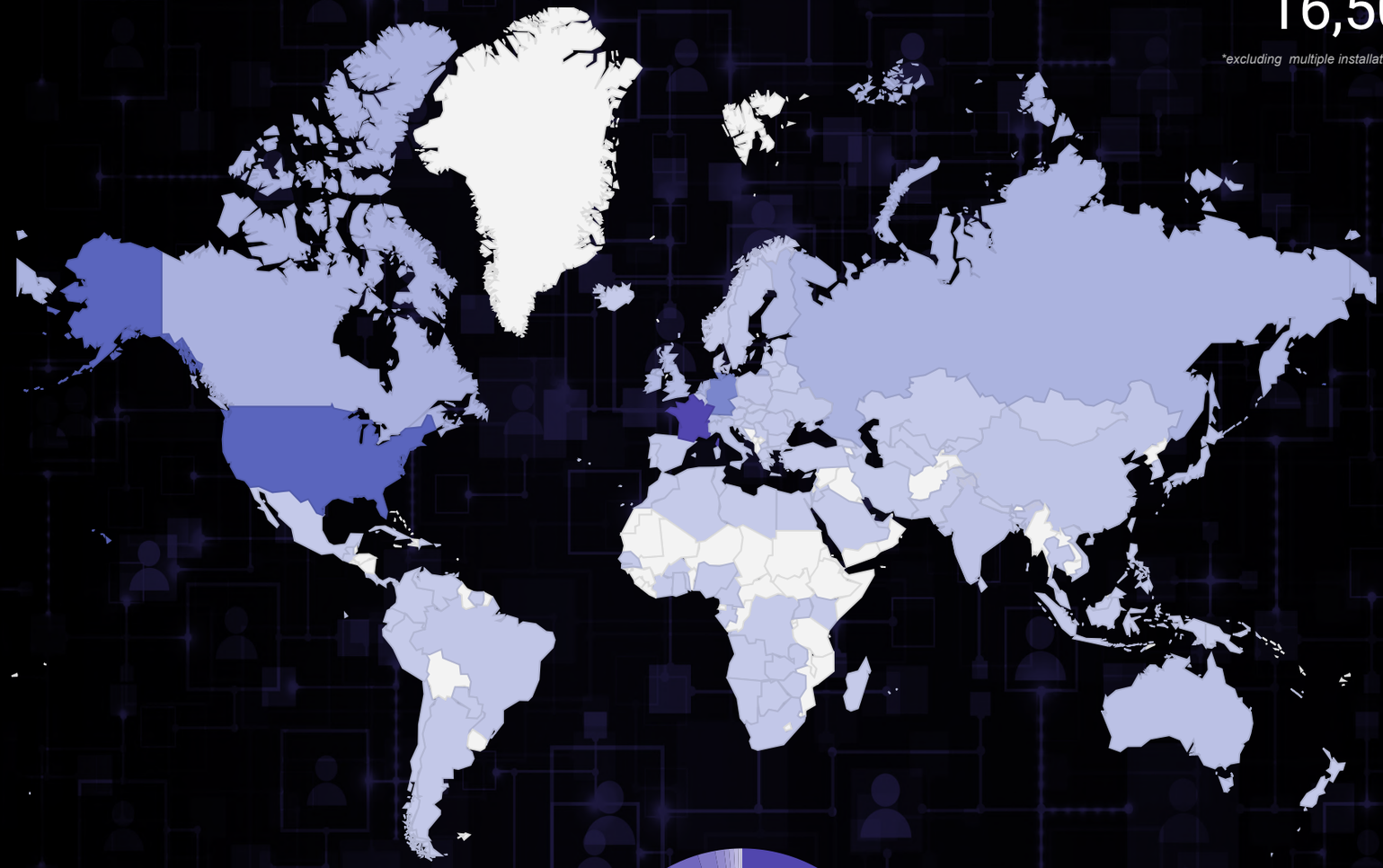
CrowdSec Network Strength

Changes (⬆) are calculated from the last quarter

Unique Installations*
16,506
*excluding multiple installations in containers

in

Countries
224
No data



	Top ten Countries	Installs
1.	France	4,954
2.	United States	2,885
3.	Germany	1,778
4.	Canada	645
5.	Netherlands	607
6.	Russia	603
7.	Finland	456
8.	Ireland	450
9.	United Kingdom	417
10.	Japan	251

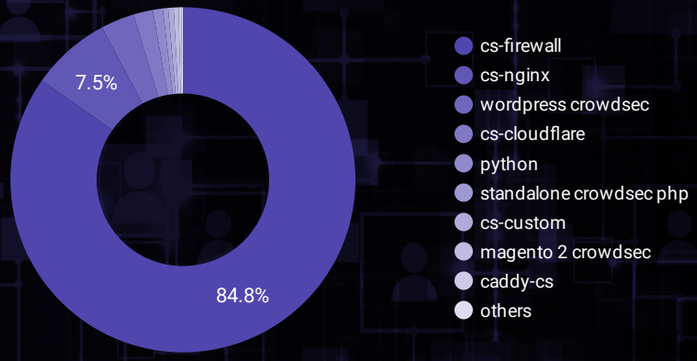
Deployed Bouncers (I.P.S.)

15,072
No data

IPS : Internet Protection System

Average bad IP reported / user
214

Average threats reported / user
2,431



Top 10 Bouncers (*I.P.S.*) used by the Community

[Documentation on bouncers]

Trends & Expert analysis - Most Common Threats

Focus on threats detected by the community (page #3)

Brute-force Attacks

This type of attack can be seen as the background noise of the Internet: attackers try to exploit common weak passwords set by default. One of the main targets is ssh services, the most common remote administration service on Linux servers.

Hence it is not surprising that most of the reported IPs by CrowdSec are flagged for brute-force attacks. We have a wide range of *scenarios* to detect it (*WordPress, SSH, Telnet, FTP, Samba, ...)* and also various *bouncers* which will act at the firewall level to drop the packets on malicious connection attempts.

Vulnerabilities Scanner - HTTP Server

The user-agent is the signature of an http client located in the request. It is used by the server to identify the type of client or machine sending the request. Numerous tools used to exploit vulnerabilities on servers have a common user-agent which can be detected with the *http-bad-user-agent scenario*. Yet this measure is not perfect as the user-agent can easily be forged.

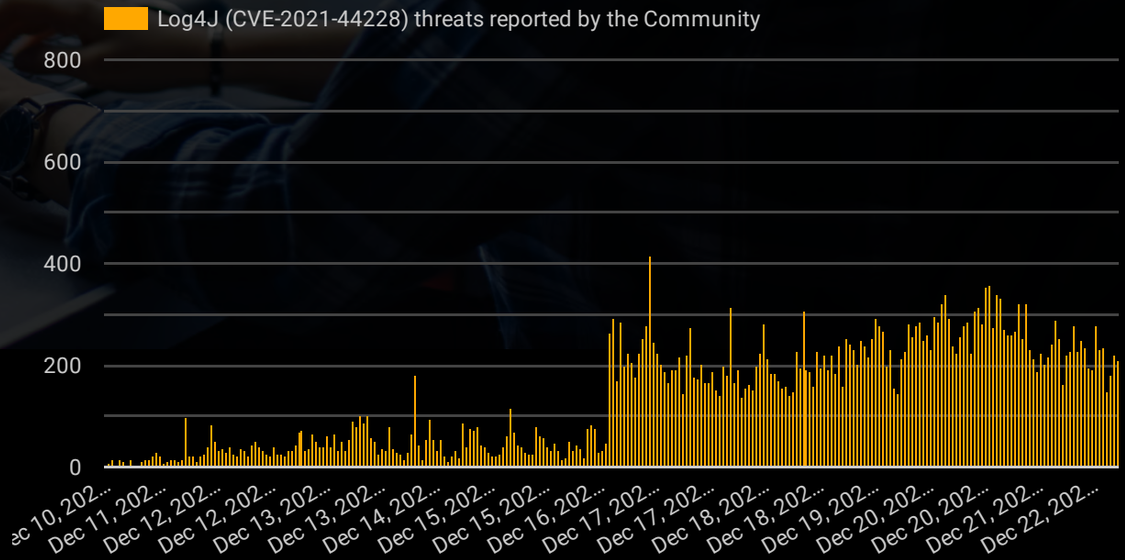
Other scenarios such as *http-probing* et *http-sensitive-files* can also help you to protect your HTTP server. It is meant to detect web scanners that try to exploit vulnerabilities by accessing files known for containing weakness or information leak. This behavior can be spotted in the servers logs, as they perform lots of requests trying to access files which do not exist. It is worth noting that crowdsec does not replace a WAF (Web Application Firewall) and will never be.

Emerging Threats - Log4j CVE

Thanks to CrowdSec and its active community, you can be protected even against the most recent threats.

As an example, the recent **CVE-2021-44228** (*aka Log4Shell*) allows remote code execution in the JAVA Log4J library. It was published on Dec 10, and a CrowdSec Scenario was created on the same day at 3 PM allowing users to detect and stop these new threats.

In the following hours, we have noticed a growing number of reports from the community (see chart) and we release a near real time tracker to monitor the origin of the attack



How does CrowdSec remediates ?

Installation (*2 min*)

Tutorial

Most Common Use-Cases

Protect Your WordPress

article

Defend against L7 DDOS

article

Trends & Expert analysis - IP Malevolence duration *(in days)*

Focus on threats detected by the community (page #3)

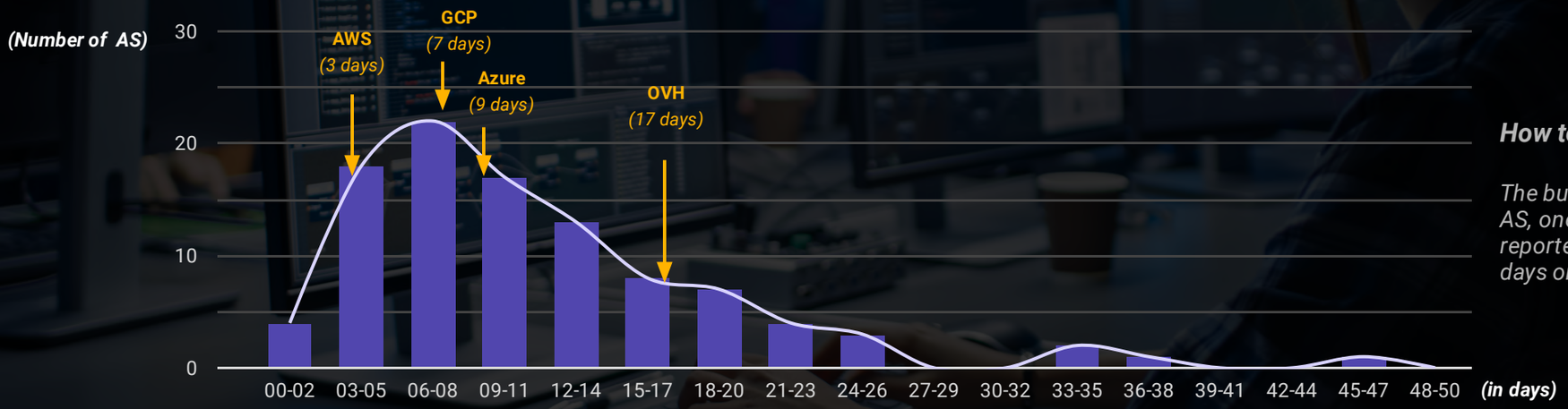
What is an Autonomous System (*AS*)?

An AS is an official organization being granted a number 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 assets within their network and to take actions in case of abuse reported to them.

How to compare and rank AS?

Number of IPs reported: While looking simply at the number of compromised assets might be an angle, it wouldn't be necessarily fair. In fact, not all operators are equal in size, and some are hosting more "risky" services (*hello outdated PHP CMS*) than others.

Malevolent Duration (*MD*): The number of days an IP is reported by the community. The **average MD** of all the IPs in the same AS gives an indicator of the operator's due diligence when it comes to identifying and dealing with compromised assets. The distribution of the average MD is shown below, with arrows pointing to the position of the most reported AS for the main cloud providers.



How to read the chart?

The bucket 3-5 days contains 18 AS, one belongs to AWS and the reported IPs stay malicious for 4 days on average.

Distribution of the average Malevolent Duration (in days) for the top 100 AS in terms of threats reported.

Furthermore & 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, but it might be an interesting angle to add in the future.

We are well aware that in most cases a malevolent machine at a given time was a legitimate asset a few days/weeks ago that was compromised. Once the legitimate owner is made aware of it, they will take the necessary steps and the machine will become "clean" again. This is why we are very careful to have a "short" expiration delay (*7 days*) for each IP on our community blocklist.

Data Sources & Methodology used

CrowdSec is a **free**, **open-source** & **collaborative** new-generation I.D.S./I.P.S. (*Intrusion Detection/Prevention System*)

It comes up with **Scenarios,** to detect a wide range of malicious behavior and **Bouncers** to take action upon the alerts raised.

CrowdSec is also building a **massive CTI** (*Cyber Threat Intelligence*), where users can share their alerts about threats with the community and benefit from the network effect in return.

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

Diversity: Reporters must be located in many different AS.

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

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

Expiration: Malicious IPs are redistributed for **7 days** and are then expired if no longer reported.

Check the FAQ for more details

Data presented here are threats reported by the CrowdSec software since 2020.

Alerts are different from usual user data, it only contains the type of the attack, the time, and the source (*IP*).

Users can choose not to disclose their alerts, but in turn, won't benefit from the **community blocklist**.

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

Metadata enrichment comes from MaxMind GeoIP.

Install the **CS software** on your servers

Design custom **scenarios** (*IDS*) or **bouncers** (*I.P.S.*) and share them with the community

Share logs and intelligence about attacks in our dedicated **Console**.

CrowdSec

CrowdSec

crowdsec.net

Stay informed to protect yourself against cyber threats.

Want to make Internet a safer place?

The Majority report uses the wisdom of the crowd to identify emerging trends, menaces and nefarious actors and we would love to have you. Become a contributor to next quarter report, by providing us with signals for improving the Majority Report.

Check out the CrowdSec GitHub page:
https://github.com/crowdsecurity

Interactive and up-to-date version of this report:
Please contact us: info@crowdsec.net