Bad ASes

silentpush.com/blog/bad-ases

September 15, 2021

Sep 15

Written By Martijn Grooten

An autonomous system (AS) is a collection of IP subnets that is managed by a single administrative entity. Think of an ISP or a hosting provider, but also a large corporation or a university, many of which manage one or more autonomous systems. Each AS is assigned a unique number, called an ASN; in practice the terms AS and ASN are often used interchangeably.

ASNs play a crucial role in routing and thus in making the Internet work. But because each of them is managed by a single entity, it also makes sense to assign a reputation to them, based on the amount of malicious activity hosted on the AS.

Silent Push assigns a reputation to each ASN, that takes into account both the number of active IP addresses within the AS and the number of these that are currently being used for malicious activities.

The reputation of an ASN reflects the current state rather than a historical reputation, so that ASNs that shut down malicious activity will see their reputation drop immediately. Historic reputation data is available through the API.

The following are the ASNs with the worst reputation — each of them has the maximum reputation score of 100 — ranked by the number of IP addresses currently listed:

ASN	AS NAME	Country	Reputation	Number of listed IPs
263089	V de M Vargas	Brazil	100	66
265080	AD TELECOM	Brazil	100	23
267124	Paulino Perreira Dos Santos ME	Brazil	100	15
211341	SCOPESKY-FTTX	Iraq	100	13
209160	MITI2000	Bulgaria	100	11
200391	KREZ999AS	Bulgaria	100	9
207812	DM_AUTO	Bulgaria	100	9
210228	WHG-NETWORK	UK	100	6
209588	AS57043	Panama	100	6
264847	ENRED S.DE.R.L	Honduras	100	3

However, all of ASNs are all quite small, with each containing 2048 or fewer IP addresses. They host a relatively large amount of malicious activity, but in absolute terms, their contribution to ‘bad things on the Internet’ is pretty small.

So let’s look at those ASN with contain at least 100,000 IP addresses (active or not):

ASN	AS NAME	Country	Reputation	Number of listed IPs
24086	VIETTEL-AS-VN Viettel Corporation	Vietnam	86	257
17622	CNCGROUP-GZ China Unicom Guangzhou network	China	63	155
132203	TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue	China	61	950
14061	DIGITALOCEAN-ASN	United States	55	2256
37963	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd	China	54	1812
4134	CHINANET-BACKBONE No.31,Jin-rong Street	China	51	816
38365	BAIDU Beijing Baidu Netcom Science and Technology Co., Ltd.	China	51	148
21859	ZEN-ECN	United States	50	179
14987	RETHEMHOSTING	United States	49	16
396982	GOOGLE-PRIVATE-CLOUD	United States	48	106

Now a number of well-known companies appear in the list, including Tencent, Digital Ocean, Alibaba and Google.

Each of these cloud providers make it easy for someone to quickly and more or less anonymously set up a virtual server. That has many advantages for researchers and developers but also attracts those hosting malicious infrastructure, such as malware authors or those providing services to them.

We would certainly not recommend blocking something just because it is hosted at any of these providers. But something unknown hosted there definitely deserves some extra scrutiny.

Takedown reputation

In fairness, it is unreasonable to expect a hosting provider or other network to be able to proactively block all malicious activity on its network. After all, it's not like a malicious actor is open about their intentions when renting a server or purchasing a domain.

This is why at Silent Push, we also assign a 'takedown reputation' to each ASN, that assigns a score from 0 to 100 that measures how well (or how badly, for 0 is the best score) an ASN takes down malicious activity hosted on its network.

If we add the takedown reputations to the previous table, we note they are all low, but in some cases not 0, leaving some room for improvement for these ASNs when it comes to their due diligence in keeping the Internet free of malware and scams.

ASN	AS NAME	Country	Reputation	Takedown reputation	Number of listed IPs
24086	VIETTEL-AS-VN Viettel Corporation	Vietnam	86	0	257
17622	CNCGROUP-GZ China Unicom Guangzhou network	China	63	0	155
132203	TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue	China	61	1	950
14061	DIGITALOCEAN-ASN	United States	55	0	2256
37963	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd	China	54	0	1812
4134	CHINANET-BACKBONE No.31,Jin-rong Street	China	51	0	816
38365	BAIDU Beijing Baidu Netcom Science and Technology Co., Ltd.	China	51	1	148
21859	ZEN-ECN	United States	50	1	179
14987	RETHEMHOSTING	United States	49	0	16
396982	GOOGLE-PRIVATE-CLOUD	United States	48	1	106

Finally, we can look at the ASNs with the worst takedown reputation. These are all pretty small, containing 4096 IP addresses or fewer, and have a takedown reputation higher than 90:

ASN	AS NAME	Country	Takedown reputation
204915	AWEX	Cyprus	99
27647	WEEBLY	United States	98
132647	IDNIC-PANDI-AS-ID Pengelola Nama Domain Internet Indonesia	Indonesia	97
60503	FNXTEC	Brazil	96
51381	ELITETEAM-PEERING-AZ1	Seychelles	95
48693	NTSERVICE-AS	Ukraine	94
213268	CLOUDWEBSERVICES	the Netherlands	93
26337	OIS1	United States	92
47846	SEDO-AS	Germany	91
48090	PPTECHNOLOGY	United Kingdom	90

Conclusion

Simply ranking ASNs or hosting providers by the number of IP addresses that are hosting or have hosted malicious content ignores both their actual size and their responsiveness when it comes to takedown requests. By including both, Silent Push provides you with a clearer picture of what ASNs to consider somewhat suspicious, which combined with other context can help during an investigation.

Martijn Grooten