baffin bay

by

Technical Threat Report

Q4 2023

Contents

About the research

The following report examines global attack traffic during Q4 in 2023, outlining findings and trends from multiple threat domains.

In this latest data collection we delve into malicious internet traffic over a 90-day period - October 1, 2023 through December 31, 2023. The purpose is to provide industry practitioners in cyber security with hands-on data for technical hygiene checks, threat reduction measures and research.

The findings are extracted from data collectors within Baffin Bay's Threat Protection (TP) platform and Global Sensory Network (GSN).

This report is released on a quarterly basis by Baffin Bay's Cyber Threat Intelligence (CTI) team. Visit our website to learn more about our products and services. Our Threat Insight service is available for anyone to consume here.

1. Threat protect

The following section presents insights from Baffin Bay's cloud based DDoS Protection service*.* The datasets are aggregations of Distributed Denial of Service (DDoS) attacks towards Baffin Bay's customer base.

1.1 Top attacking AS organizations

Top 10 AS organizations launching DDoS attacks.

n.	AS organization	Source IPs
1	Rostelecom	7211
2	JSC ER-Telecom Holding	5195
3	UNINET	3719
4	CAT TELECOM Public Company Ltd	2711
5	Chinanet	2664
6	TOT Public Company Limited	2607
7	Philippine Long Distance Tele. Comp.	2485
8	Data Communication Business Group	2093
9	CHINA UNICOM China169 Backbone	2043
10	EPM Telecomunicaciones S.A. E.S.P.	2014

Graph 1

1.2 Top source traffic countries

Top 10 source traffic countries[1] launching DDoS attacks.

[1] In this context, ''source traffic country'' refers to the geographical source of IP address. It does not assume that the country itself, individuals, or organizations based in that country were responsible for the malicious traffic. The traffic could be coming through a proxy server or compromised systems with IP addresses assigned in a particular country.

n.	Country	Source IPs
1	Russia	18039
2	Indonesia	8353
3	Ukraine	6061
4	Colombia	4639
5	Brazil	4539
6	United States	4480
7	Argentina	2751
8	Mexico	2641
9	Poland	2490
10	Thailand	2975

Graph 2

1.3 Top reflection ports

Top 10 reflection ports used in DDoS attacks.

n.	Port	Description
1	123	Network Time Protocol (NTP)
2	427	Service Location Protocol (SLP)
3	53	Domain Name System (DNS)
4	11211	Memcached
5	3702	Web Services (WS) Discovery
6	3283	Apple Remote Desktop 2.0 or later
7	19	Character Generator Protocol
8	1900	Simple Services Discovery Protocol (SSDP)
9	1194	OpenVPN

Graph 3

2. Global Sensory Network (GSN)

Baffin Bay gathers, aggregates and enriches data through our extensive Global Sensory Network (GSN) consisting of multiple data collectors dispersed across the internet. The sensors capture exploits, attack attempts, malicious uploads and OSINT[1], allowing for the discovery of unique threat intelligence.

2.1 Generic

General statistics on events captured by the GSN.

n	Metric	Hits
1	Total amount of events recorded	1.08 Bil
2	Port scanning events	643 Mil
3	Credential stuffing events	436 Mil
4	Malware upload events	1.19 Mil
5	Spam events	104 K
6	HTTP attack events	1.60 Mil

Graph 4

2.2 Top source traffic countries - Global

Top 10 source traffic countries[2] launching malicious traffic

[1] The exploits, attack attempts, malicious uploads and OSINT captured by Baffin Bay Networks' GSN account for unsolicited traffic, i.e. traffic that is not targeting any specific individual, entity or organization, but rather passes through the collectors that are being monitored.

[2] In this context, ''source traffic country'' refers to the geographical source of an IP address. It does not assume that the country itself, individuals, or organizations based in that country were responsible for the malicious traffic. The traffic could be coming through a proxy server or compromised systems with IP addresses assigned in a particular country.

n.	Country	Region	Hits	%
1	United States	NA	116.45 Mil	10.77
2	India	AS	106.70 Mil	9.87
3	Russia	EU	88.79 Mil	8.21
4	China	AS	84.06 Mil	7.78
5	Iran	AS	46.64 Mil	4.31
6	Vietnam	AS	41.75 Mil	3.86
7	Germany	EU	39.40 Mil	3.64
8	Egypt	AF	36.72 Mil	3.40
9	Ukraine	EU	30.34 Mil	2.81
10	Singapore	AS	29.98 Mil	2.77

Graph 5

2.3 Top attacking IPs

IP addresses most frequently captured by the GSN engaging in malicious activity. A global outlook followed by regional statistics.

2.3.1 Top 10 Global

n.	IP address	Country	Hits
1	31.43.185.65	Ukraine	16.49 Mil
2	79.137.202.16	Germany	14.29 Mil
3	185.73.125.23	Estonia	5.86 Mil
4	193.37.69.79	Russia	5.84 Mil
5	79.124.58.138	Bulgaria	4.15 Mil
6	14.194.49.6	India	2.721 Mil
7	79.124.49.58	Bulgaria	2.72 Mil
8	78.128.114.90	Bulgaria	2.68 Mil
9	79.124.59.130	Bulgaria	2.45 Mil
10	78.128.114.2	Bulgaria	2.11 Mil

Graph 6

2.3.2 Top 5 - Europe

n.	IP address	Country	Hits
1	31.43.185.65	Ukraine	16.49 Mil
2	79.137.202.16	Germany	14.29 Mil
3	185.73.125.23	Estonia	5.86 Mil
4	193.37.69.79	Russia	5.84 Mil
5	79.124.58.138	Bulgaria	4.15 Mil

Graph 7

2.3.3 Top 5 - North America

n.	IP address	Country	Hits
1	104.236.1.59	United States	2.47 Mil
2	198.199.71.131	United States	2.11 Mil
3	167.99.127.131	United States	2.05 Mil
4	161.35.109.85	United States	2.03 Mil
5	198.211.104.222	United States	2.01 Mil

Graph 8

2.3.4 Top 5 - South America

n.	IP address	Country	Hits
1	200.75.2.138	Chile	629K
2	177.92.5.242	Brazil	495K
3	45.161.176.1	Brazil	481K
4	200.178.173.130	Brazil	474K
5	191.180.132.11	Brazil	467K

Graph 9

2.3.5 Top 5 - Asia

n.	IP address	Country	Hits
1	14.194.49.6	India	2.72 Mil
2	115.84.224.194	Philippines	1.86 Mil
3	112.122.100.235	China	1.44 Mil
4	118.216.255.73	South Korea	1.25 Mil
5	182.70.117.153	India	1.22 Mil

Graph 10

2.3.6 Top 5 - Africa

n.	IP address	Country	Hits
1	41.33.169.196	Egypt	790K
2	196.219.125.58	Egypt	788K
3	41.130.229.69	Egypt	705K
4	41.129.52.246	Egypt	646K
5	196.221.206.143	Egypt	636K

Graph 11

2.3.7 Top 5 - Oceania

n.	IP address	Country	Hits
1	154.26.154.160	Australia	188K
2	170.64.188.173	Australia	177K
3	170.64.158.52	Australia	117K
4	170.64.158.217	Australia	102K
5	170.64.167.61	Australia	90K

Graph 11

2.4 Top attacking AS organizations

Top 10 AS organizations launching attacks globally

n.	ASN	AS Org	Hits	%
1	14061	DIGITALOCEAN-ASN	93 Mil	8.66
2	132203	Tencent Building, Kejizhongyi	36 Mil	3.39
3	208091	Xhost Internet Solutions Lp	32 Mil	2.99
4	45090	Shenzhen Tencent Computer Syst	25 Mil	2.39
5	58224	Iran Telecommunication Company	24 Mil	2.25
6	4134	Chinanet	22 Mil	2.12
7	50360	Tamatiya EOOD	21 Mil	1.97
8	8452	TE-AS	21 Mil	1.95
9	12389	Rostelecom	20 Mil	1.92
10	9829	National Internet Backbone	18 Mil	1.68

Graph 12

2.5 Port scanning

2.5.1 Top port scanning sources

Top 10 IP-addresses engaging in port scanning activity.

n	Hits	IP	ASN
1	8.24 Mil	31.43.185.65	211736
2	2.91 Mil	185.73.125.23	208091
3	2.84 Mil	193.37.69.79	208091
4	2.73 Mil	14.194.49.6	45820
5	2.47 Mil	104.236.1.59	14061
6	2.12 Mil	198.199.71.131	14061
7	2.07 Mil	79.124.58.138	50360

8	2.05 Mil	167.99.127.131	14061
9	2.03 Mil	161.35.109.85	14061
10	2.01 Mil	198.211.104.222	14061

Graph 13

2.5.2 Top targeted ports

Top 10 ports targeted by scanning activity.

n.	Port	Attack type	Hits	%
1	22	credentialStuffing	26.11 Mil	24.2
2	3389	credentialStuffing	68.87 Mil	6.37
3	2222	credentialStuffing	54.52 Mil	5.04
4	5900	credentialStuffing	37.97 Mil	3.5
5	2223	credentialStuffing	6.84 Mil	0.63
6	3306	credentialStuffing	4.13 Mil	0.38
7	445	malwareUploads	1.18 Mil	0.11
8	21	credentialStuffing	1.0 Mil	0.09
9	8080	httpAttacks	612K	0.05
10	5432	credentialStuffing	576K	0.05

Graph 14

2.6 Credential stuffing

2.6.1 Top credential stuffing sources

Top 10 IP addresses conducting credential stuffing.

n.	Hits	IP address	ASN	%
1	14.38 Mil	79.137.202.16	210644	3.30
2	8.25 Mil	31.43.185.65	211736	1.90
3	3.05 Mil	193.37.69.79	208091	0.70

4	2.96 Mil	185.73.125.23	208091	0.68
5	2.08 Mil	195.3.221.32	201814	0.48
6	2.07 Mil	79.124.58.138	50360	0.48
7	2.02 Mil	185.16.39.70	201814	0.47
8	2.02 Mil	195.230.23.162	58294	0.47
9	1.97 Mil	77.105.146.123	210644	0.45
10	1.93 Mil	164.132.200.137	16276	0.44

Graph 15

2.6.2 Top values of passwords used in credential stuffing

Top 10 passwords used in attempts to access unrelated systems.

n.	Password	Hits
1	3245gs5662d34	5.76 Mil
2	345gs5662d34	5.76 Mil
3	123456	4.43 Mil
4	admin	1.34 Mil
5	123	1.21 Mil
6	password	945K
7	1234	607K
8	12345	533K
9	12345678	463K
10	root	360K

Graph 16

2.7 Malware

2.7.1 Most active generic malware

Top 10 most frequent generic malware hashes captured by the GSN.

n.	Hash (SHA-MD5)	Hits
1	d64dc93e51af87e033063032191fe291	55K
2	685bc2af410d86a742b59b96d116a7d9	14K
3	57a71607bb704159d230dda1e0ff0147	9K
4	70ccd9220cebb56eaa38b9f1bd1a1cd8	7,5K
5	beb68e9c7ef18f421df8230c032fe02a	7K
6	7107326e81d955aff29f49487aa3da23	6K
7	0d9d766f1738b6986c0ea69a0e905fc4	4,5K
8	feaa2ebb565f21f7214289788222ca39	4,4K
9	ca71f8a79f8ed255bf03679504813c6a	3K

Graph 17

2.7.2 Most active IoT malware

Top 10 most frequent IoT malware hashes captured by the GSN.

n.	Hash (SHA-256)	Hits
1	4293c1d8574dc87c58360d6bac3daa182f64f7785c9d41da5e0741d2b1817fc7	1,487
2	b5cf68c7cb5bb2d21d60bf6654926f61566d95bfd7c9f9e182d032f1da5b4605	578
3	64cd497a29a6801daa66b3ca23b63a1355b0b84fdf5a23a12810b88685b22f63	281
4	f6c97b1e2ed02578ca1066c8235ba4f991e645f89012406c639dbccc6582eec8	229
5	ca35f2e3b3f297c371f0a58398cb43e24c1d1419f08baff9b9223b9032ccf4c1	139

6	65bd6390cd25d2afdd26e2afd6a572b371af8bae42b43bb9f34609bd1ea6b105	138
7	2e4506802aedea2e6d53910dfb296323be6620ac08c4b799a879eace5923a7b6	114
8	667e0db9b74bb51b05798777399f2aa4f4ecf31b9c1825bad57c99026a2eff09	91
9	31b184c9ba6420e9d37d619e584d134c36d401f09ccf2284a09bbaf8810b2137	89
10	c7a9d41be328955649c824fabbd5bf98307af65bcb0d3aceb6eb2f3aec95520b	86

Graph 18

2.8 Top spam sources

Top 10 IP addresses involved in spamming.

n.	Hits	IP	AS Org.	ASN
1	59K	156.96.151.53	VDI-NETWORK	46664
2	13K	37.139.129.19	Delis LLC	211252
3	5K	45.66.230.97	Delis LLC	211252
4	2K	45.12.253.177	Delis LLC	211252
5	997	194.33.191.17	Constant MOULIN	203168
6	888	87.120.84.116	Relcom Host LLC	211256
7	885	91.92.248.79	LIMENET	394711
8	427	141.98.6.15	Delis LLC	211252
9	423	147.78.103.38	Net4India Ltd	17447
10	357	23.172.112.118	VDI-NETWORK	46664

Graph 19

baffin bay

by

DISCLAIMER

This report is solely distributed for informative purposes. The data presented can be subject to errors, changes and variations without notice. Baffin Bay by Mastercard takes no liability with respect to the findings and their implications.