baffin bay

by

Technical Threat Report

Q1 2024

Contents

About the research

The following report examines global attack traffic during Q1 in 2024 outlining findings and trends from multiple threat domains.

In this latest data collection we delve into malicious internet traffic over a 90-day period - January 1, 2024 through March 31, 2024. 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 results are derived from 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	10348
2	JSC ER-Telecom Holding	7545
3	UNINET	5882
4	Data Communication Business Group	5121
5	Chinanet	4641
6	CAT TELECOM Public Company Ltd,CAT	3962
7	CHINA UNICOM China169 Backbone	3700
8	FPT Telecom Company	3685
9	VNPT Corp	3445
10	Viettel Group	3305

Table 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	44388
2	Indonesia	24136
3	United States	23583
4	Brazil	14536
5	Ukraine	14145
6	Colombia	10324
7	China	9937
8	Vietnam	7735
9	Mexico	7343

Table 2

1.3 Top reflection ports

Top 10 reflection ports used in DDoS attacks.

n.	Port	Description
1	1900	Simple Services Discovery Protocol (SSDP)
2	69	Trivial File Transfer Protocol (TFTP)
3	53	Domain Name System (DNS)
4	1194	OpenVPN
5	427	Service Location Protocol (SLP)
6	123	Network Time Protocol (NTP)
7	3702	Web Services (WS) Discovery
8	3283	Web Services (WS) Discovery
9	37810	DHCPDiscover

Table 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.

Metric	Hits
Total amount of events recorded	979 Mil
Port scanning events	553 Mil
Credential stuffing events	423 Mil
HTTP attack events	2.53 Mil
Malware upload events	825 K
Spam events	123 K

Table 4

2.2 Top source traffic countries - Global

Top 10 source traffic countries[2] generating malicious traffic

n.	Country	Region	Hits	%
1	United States	NA	126.91 Mil	12.97

[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.

2	China	AS	87.75 Mil	8.96
3	Poland	EU	84.47 Mil	8.63
4	Russia	EU	69.86 Mil	7.14
5	Germany	EU	59.31 Mil	6.06
6	India	AS	50.06 Mil	5.11
7	The Netherlands	EU	42.68 Mil	4.36
8	Estonia	EU	37.24 Mil	3.80
9	Singapore	AS	36.56 Mil	3.74
10	Vietnam	AS	30.43 Mil	3.11

Table 5

2.3 Top attacking IPs

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

2.3.1 Top 10 Global

n.	IP address	Country	Hits
1	185.73.125.23	Estonia	22 Mil
2	31.43.185.65	Ukraine	21 Mil
3	87.251.67.221	Poland	17 Mil
4	87.251.67.183	Poland	15 Mil
5	79.137.202.16	Germany	15 Mil
6	185.73.124.154	Estonia	13 Mil
7	80.66.88.148	Netherlands	12 Mil
8	87.251.67.225	Poland	9 Mil
9	80.66.88.145	Netherlands	8 Mil
10	87.251.67.169	Poland	8 Mil

Table 6

2.3.2 Top 5 - Europe

n.	IP address	Country	Hits
1	185.73.125.23	Estonia	22 Mil
2	31.43.185.65	Ukraine	21 Mil
3	87.251.67.221	Poland	17 Mil
4	87.251.67.183	Poland	15 Mil
5	79.137.202.16	Germany	15 Mil

Table 7

2.3.3 Top 5 - North America

n.	IP address	Country	Hits
1	66.94.123.164	United States	6 Mil
2	104.236.1.59	United States	3 Mil
3	109.199.104.207	United States	2.6 Mil
4	167.99.127.131	United States	2.5 Mil
5	45.55.66.199	United States	2.4 Mil

Table 8

2.3.4 Top 5 - South America

n.	IP address	Country	Hits
1	200.178.173.130	Brazil	660K
2	181.212.66.98	Chile	545K
3	186.224.22.90	Brazil	335K
4	201.216.239.205	Argentina	295K
5	186.167.80.164	Venezuela	280K

Table 9

2.3.5 Top 5 - Asia

n.	IP address	Country	Hits
1	80.66.83.68	Russia	1.6 Mil
2	103.106.177.21	India	1.5 Mil
3	115.84.224.194	Philippines	1.3 Mil
4	117.24.13.16	China	1.12 Mil
5	43.155.146.66	South Korea	1.11 Mil

Table 10

2.3.6 Top 5 - Africa

n.	IP address	Country	Hits
1	41.33.131.108	Egypt	419K
2	197.255.224.193	Comoros	397K
3	41.59.197.83	Tanzania	290K
4	196.189.185.241	Ethiopia	284K
5	196.221.206.143	Egypt	250K

Table 11

2.3.7 Top 5 - Oceania

n.	IP address	Country	Hits
1	91.108.240.199	Australia	89K
2	170.64.133.120	Australia	88K
3	170.64.131.178	Australia	87K
4	170.64.143.152	Australia	66K
5	170.64.135.76	Australia	64K

Table 12

2.4 Top attacking AS organizations

Top 10 AS organizations engaging in malicious activity.

n.	ASN	AS Org	Hits
1	208091	Xhost Internet Solutions Lp	143.18 Mil
2	14061	DIGITALOCEAN-ASN	77.48 Mil
3	132203	Tencent Building, Kejizhongyi	45.82 Mil
4	210644	Aeza International Ltd	33.57 Mil
5	45090	Shenzhen Tencent Computer Syst	22.60 Mil
6	211736	FOP Dmytro Nedilskyi	21.46 Mil
7	37963	Hangzhou Alibaba Advertising C	17.20 Mil
8	4134	Chinanet	16.43 Mil
9	16509	AMAZON-02	16.22 Mil
10	50360	Tamatiya EOOD	14.98 Mil

Table 13

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	11.35 Mil	185.73.125.23	208091
2	10.83 Mil	31.43.185.65	211736
3	8.67 Mil	87.251.67.221	208091
4	8.16 Mil	87.251.67.183	208091
5	6.73 Mil	185.73.124.154	208091
6	6.43 Mil	80.66.88.148	208091
7	4.49 Mil	87.251.67.225	208091
8	4.33 Mil	80.66.88.145	208091

9	4.33 Mil	87.251.67.169	208091
10	3.93 Mil	87.251.67.216	208091

Table 14

2.5.2 Top targeted ports

Top 10 ports targeted by scanning activity.

n.	Port	Attack type	Hits	%
1	22	credentialStuffing	201186307	20.6
2	5900	credentialStuffing	105875061	10.8
3	3389	credentialStuffing	68564949	7.00
4	2222	credentialStuffing	36898838	3.77
5	3306	credentialStuffing	4158921	0.425
6	2223	credentialStuffing	3276194	0.335
7	8080	httpAttacks	1040590	0.106
8	21	credentialStuffing	864992	0.0884
9	445	malwareUploads	824852	0.0843
10	443	httpAttacks	816143	0.0834

Table 15

2.6 Credential stuffing

2.6.1 Top credential stuffing sources

Top 10 IP addresses conducting credential stuffing.

n.	Hits	IP address	ASN	%
1	16 Mil	79.137.202.16	210644	3.78
2	11 Mil	185.73.125.23	208091	2.69
3	10 Mil	31.43.185.65	211736	2.52

4	8.6 Mil	87.251.67.221	208091	2.04
5	8 Mil	89.208.103.89	210644	1.91
6	8 Mil	87.251.67.183	208091	1.91
7	6.8 Mil	79.137.198.250	210644	1.60
8	6.7 Mil	185.73.124.154	208091	1.58
9	6.4 Mil	80.66.88.148	208091	1.52
10	4.5 Mil	87.251.67.225	208091	1.07

Table 16

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	345gs5662d34	4 Mil
2	3245gs5662d34	3.8 Mil
3	123456	3.2 Mil
4	123	1 Mil
5	admin	690K
6	password	375K
7	root	296K
8	12345678	285K
9	1234	268K
10	12345	215K

Table 17

2.8 Top spam sources

Top 10 IP addresses involved in spamming.

n.	IP	AS Org.	ASN
1	194.55.186.248	VertexLink Inc.	50236
2	156.96.151.53	VDI-NETWORK	46664
3	194.48.251.106	IP-Projects GmbH & Co. KG	48314
4	105.112.197.30	Celtel Nigeria Limited t.a ZAIN	36873
5	194.55.186.172	VertexLink Inc.	50236
6	105.112.200.18	Celtel Nigeria Limited t.a ZAIN	36873
7	193.222.96.28	Constant MOULIN	203168
8	87.120.84.98	Relcom HOST LLC	211256
9	194.48.251.190	Constant MOULIN	203168
10	194.48.251.100	IP-Projects GmbH & Co. KG	48314

Table 18

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.