Cobaltstrike-Beacons analyzed

zero.bs/cobaltstrike-beacons-analyzed.html

from time to time, threathunters and OSINT-guys releasing information and analysis on Cobaltstrike-Beacons, how to find them, and lists as well.

we collect and analyze these information for no other reasons than to archive those information.

- 2021-05-07 - 464 IPs, analysis by threatview.io
- 2020-04-18 - 1275 IPs based on dorks by heige

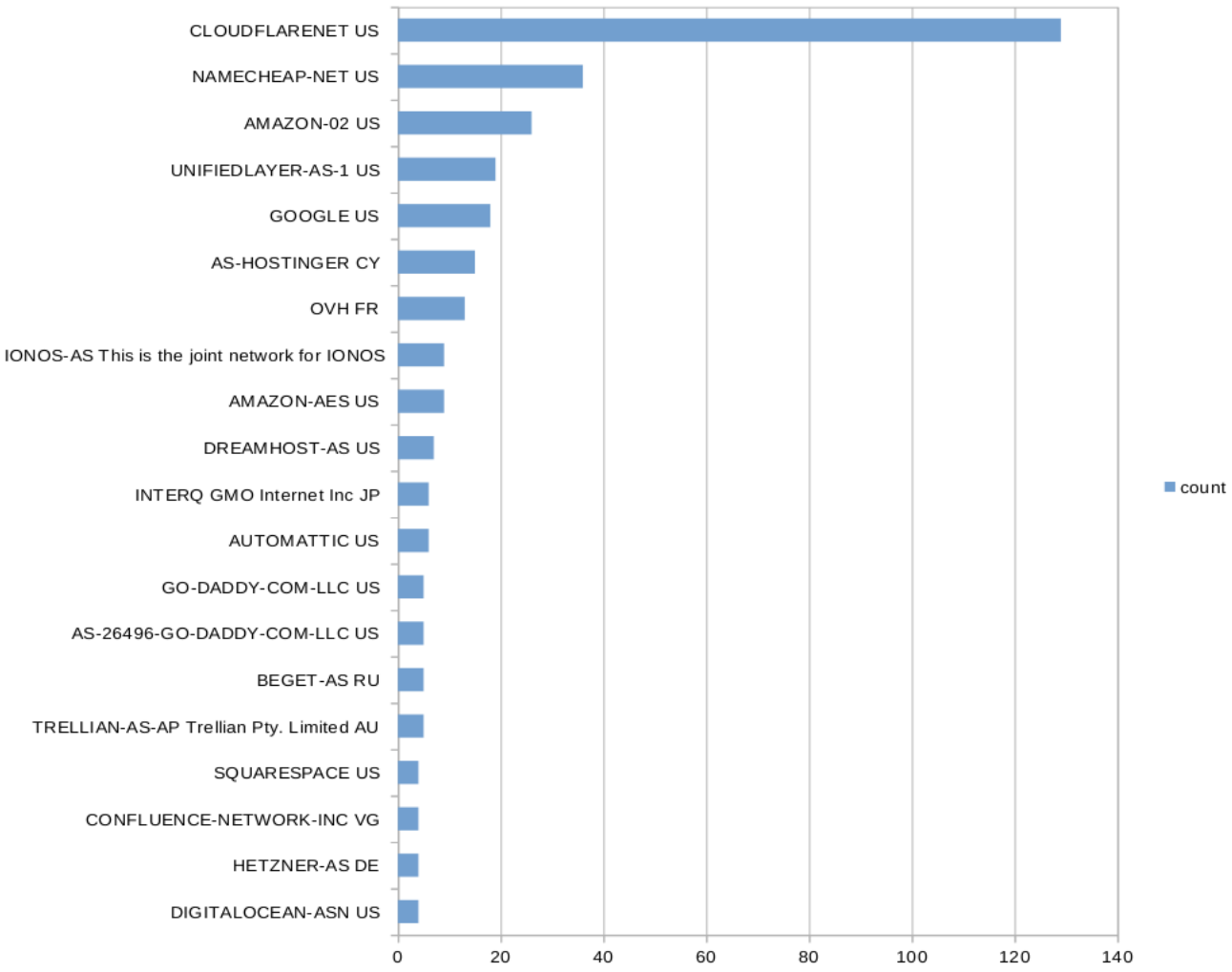
some nicies

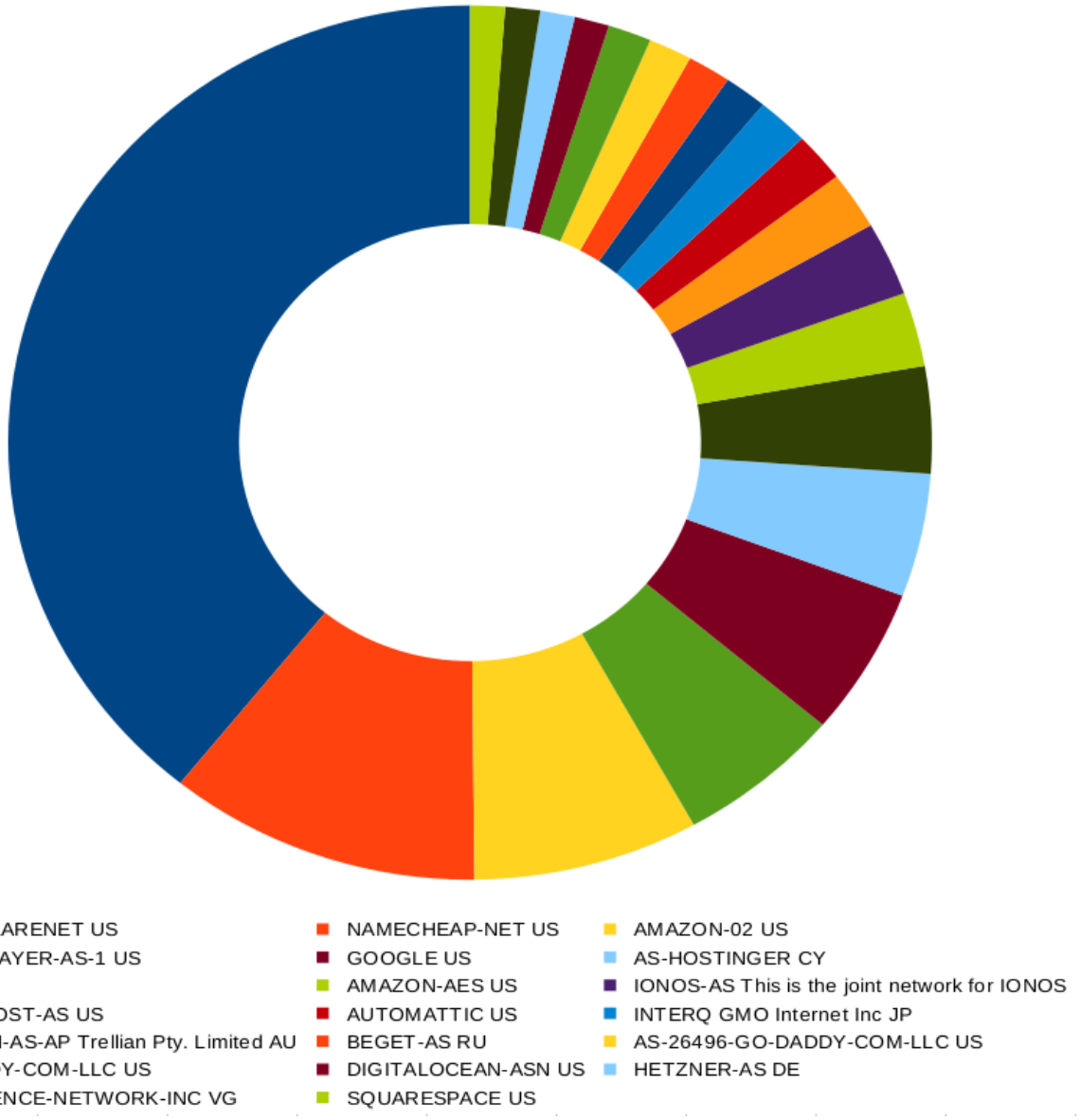
Threatview.io / twitter 2021-05-07

SRC: Twitter

below is summary for those 464 IPs mentioned, separated after AS, Countries and Networks where these IPs originate from.

The charts represent the distribution in % and count for the Top 20 AS


CLOUDFLARENET US
NAMECHEAP-NET US
AMAZON-02 US
UNIFIEDLAYER-AS-1 US
GOOGLE US
AS-HOSTINGER CY
OVH FR
IONOS-AS This is the joint network for IONOS
AMAZON-AES US
DREAMHOST-AS US
INTERQ GMO Internet Inc JP
AUTOMATTIC US
GO-DADDY-COM-LLC US
AS-26496-GO-DADDY-COM-LLC US
BEGET-AS RU
TRELLIAN-AS-AP Trellian Pty. Limited AU
SQUARESPACE US
CONFLUENCE-NETWORK-INC VG
HETZNER-AS DE
DIGITALOCEAN-ASN US
0
20
40
60
80
100
120
140
count


CLOUDFLARENET US
NAMECHEAP-NET US
AMAZON-02 US
UNIFIEDLAYER-AS-1 US
GOOGLE US
AS-HOSTINGER CY
OVH FR
AMAZON-AES US
IONOS-AS This is the joint network for IONOS
DREAMHOST-AS US
AUTOMATTIC US
INTERQ GMO Internet Inc JP
TRELLIAN-AS-AP Trellian Pty. Limited AU
BEGET-AS RU
AS-26496-GO-DADDY-COM-LLC US
GO-DADDY-COM-LLC US
DIGITALOCEAN-ASN US
HETZNER-AS DE
CONFLUENCE-NETWORK-INC VG
SQUARESPACE US

SUMMARY for cobaltstrike_beacons / CV

IPs   : 464
Networks : 271
ASNs   : 119
Countries : 29

Top 100 ASNs

ASN_NR	Count	ASNName
13335	129	CLOUDFLARENET, US
22612	36	NAMECHEAP-NET, US
16509	26	AMAZON-02, US
46606	19	UNIFIEDLAYER-AS-1, US
15169	18	GOOGLE, US
47583	15	AS-HOSTINGER, CY
16276	13	OVH, FR
14618	9	AMAZON-AES, US
8560	9	IONOS-AS This is the joint network for IONOS, Fasthosts, Arsys, 1&1 Mail and Media and 1&1 Telecom. Formerly known as 1&1 Internet SE., DE
26347	7	DREAMHOST-AS, US
2635	6	AUTOMATTIC, US
7506	6	INTERQ GMO Internet,Inc, JP
133618	5	TRELLIAN-AS-AP Trellian Pty. Limited, AU
198610	5	BEGET-AS, RU
26496	5	AS-26496-GO-DADDY-COM-LLC, US
398101	5	GO-DADDY-COM-LLC, US
14061	4	DIGITALOCEAN-ASN, US
24940	4	HETZNER-AS, DE
40034	4	CONFLUENCE-NETWORK-INC, VG
53831	4	SQUARESPACE, US
197695	3	AS-REG, RU
206834	3	TEAMINTERNET-CA-AS, DE
20738	3	GD-EMEA-DC-LD5, DE
27257	3	WEBAIR-INTERNET, US
45102	3	CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd., CN
47846	3	SEDO-AS, DE
51852	3	PLI-AS, PA
131965	2	XSERVER Xserver Inc., JP
13213	2	UK2NET-AS, GB
136800	2	XIAOZHIYUN1-AS-AP ICIDC NETWORK, US
19871	2	NETWORK-SOLUTIONS-HOSTING, US
203576	2	INTERNETBILISIM, TR
27647	2	WEEBLY, US
29873	2	BIZLAND-SD, US
32244	2	LIQUIDWEB, US
32748	2	STEADFAST, US
33070	2	RMH-14, US
34788	2	NMM-AS D - 02742 Friedersdorf Hauptstrasse 68, DE
36352	2	AS-COLOCROSSING, US
39729	2	REGISTER-AS, IT
40021	2	CONTABO, US
46636	2	NATCOWEB, US

48287	2	RU-CENTER, RU
51167	2	CONTABO, DE
53667	2	PONYNET, US
55293	2	A2HOSTING, US
58061	2	SCALAXY-AS, NL
60781	2	LEASEWEB-NL-AMS-01 Netherlands, NL
6724	2	STRATO STRATO AG, DE
12824	1	HOMEPL-AS, PL
12876	1	Online SAS, FR
132839	1	POWERLINE-AS-AP POWER LINE DATACENTER, HK
137386	1	CW-AS-AP Child Wisdom Limited, HK
13768	1	COGECO-PEER1, CA
140068	1	INTERNETINC-AS-AP 360 Internet Inc, BD
14117	1	Telefonica del Sur S.A., CL
16347	1	RMI-FITECH, FR
17506	1	UCOM ARTERIA Networks Corporation, JP
18779	1	EGIHOSTING, US
19318	1	IS-AS-1, US
19324	1	DOSARREST, US
197902	1	HOSTNET, NL
198203	1	ASN-ROUTELABEL, NL
19867	1	VOODOO1, US
199753	1	UDMEDIA-AS, DE
199968	1	IWSNET, SE
200000	1	UKRAINE-AS, UA
20446	1	HIGHWINDS3, US
204915	1	AWEX, CY
207569	1	IHOR-SERVERS-EUROPE-CZ to AS51765 announce AS207569, SC
20847	1	PREVIDER-AS, NL
211871	1	ODEAWEB, TR
21740	1	TF-178, US
24446	1	NETREGISTRY-AS-AP NetRegistry Pty Ltd., AU
2519	1	VECTANT ARTERIA Networks Corporation, JP
263702	1	GRUPO ZGH SPA, CL
27357	1	RACKSPACE, US
27956	1	Cyber Cast International, S.A., PA
29169	1	GANDI-AS Domain name registrar - http://www.gandi.net, FR
29182	1	THEFIRST-AS, RU
29486	1	WEBHUSET-AS, DE
31034	1	ARUBA-ASN, IT
31400	1	ACCELERATED-IT, DE
32475	1	SINGLEHOP-LLC, US
32613	1	IWEB-AS, CA
327979	1	DIAMATRIX, ZA
33182	1	DIMENOC, US
33387	1	NOCIX, US
35278	1	SPRINTHOST, RU
35908	1	VPLSNET, US
36024	1	AS-TIERP-36024, US
36647	1	YAHOO-GQ1, US
37153	1	xneelo, ZA
3842	1	RAMNODE, US
38719	1	DREAMSCAPE-AS-AP Dreamscape Networks Limited, AU
394695	1	PUBLIC-DOMAIN-REGISTRY, US
398968	1	GROUP-IID-01, US

40509	1	FLY, US
42807	1	AEROTEK-AS, TR
42831	1	UKSERVERS-AS UK Dedicated Servers, Hosting and Co-Location, GB
43350	1	NFORCE, NL
46475	1	LIMESTONENETWORKS, US
48254	1	TWENTYI, GB
48635	1	PCEXTREME-, NL
48689	1	WEBGLOBE-SK-AS, SK
52030	1	SERVERPLAN-AS, IT
53057	1	RedeHost Internet Ltda., BR
5404	1	CONOVA-AS ASN conova communications GmbH, AT
54600	1	PEGTECHINC, US
55933	1	CLOUDIE-AS-AP Cloudie Limited, HK
57724	1	DDOS-GUARD, RU
57910	1	SCIP-AS Soluciones Corporativas IP (SCIP), ES
58955	1	BANGMODENTERPRISE-TH Bangmod Enterprise Co., Ltd., TH
59504	1	Hosting vpsville.ru, RU
62900	1	COLOMX-LLC, US
63949	1	LINODE-AP Linode, LLC, US
7684	1	SAKURA-A SAKURA Internet Inc., JP
8342	1	RTCOMM-AS, RU
9583	1	SIFY-AS-IN Sify Limited, IN

Top 100 Countries

Country	Count
US	312
DE	35
RU	15
FR	11
JP	11
GB	11
CA	11
NL	10
AU	7
SC	4
TR	4
PA	4
IT	4
ZA	3
VG	3
HK	2
CL	2
IN	2
LT	2
CY	2
PL	1
BD	1
UA	1
SK	1
BR	1
AT	1
CN	1
ES	1
TH	1

Top 100 Networks

NW	Count	NetworkName
104.21.32.0/20	13	CLOUDFLARENET, US
104.21.80.0/20	12	CLOUDFLARENET, US
172.67.128.0/20	12	CLOUDFLARENET, US
172.67.144.0/20	12	CLOUDFLARENET, US
162.255.119.0/24	11	NAMECHEAP-NET, US
104.21.64.0/20	10	CLOUDFLARENET, US
172.67.160.0/20	10	CLOUDFLARENET, US
172.67.192.0/20	10	CLOUDFLARENET, US
104.21.16.0/20	9	CLOUDFLARENET, US
172.67.176.0/20	9	CLOUDFLARENET, US
104.21.0.0/20	7	CLOUDFLARENET, US
104.21.48.0/20	7	CLOUDFLARENET, US
172.67.208.0/20	7	CLOUDFLARENET, US
192.0.78.0/24	6	AUTOMATTIC, US
104.17.192.0/20	5	CLOUDFLARENET, US
192.64.119.0/24	5	NAMECHEAP-NET, US
217.160.0.0/16	5	IONOS-AS This is the joint network for IONOS, Fasthosts, Arsys, 1&1 Mail and Media and 1&1 Telecom. Formerly known as 1&1 Internet SE., DE
13.225.208.0/21	4	AMAZON-02, US
54.230.102.0/23	4	AMAZON-02, US
162.214.0.0/15	4	UNIFIEDLAYER-AS-1, US
103.224.182.0/23	3	TRELLIAN-AS-AP Trellian Pty. Limited, AU
35.208.0.0/15	3	GOOGLE, US
18.216.0.0/14	3	AMAZON-02, US
87.236.16.0/24	3	BEGET-AS, RU
104.247.80.0/23	3	TEAMINTERNET-CA-AS, DE
69.163.216.0/21	3	DREAMHOST-AS, US
192.185.0.0/18	3	UNIFIEDLAYER-AS-1, US
151.106.96.0/20	3	AS-HOSTINGER, CY
81.17.16.0/20	3	PLI-AS, PA
74.208.0.0/16	3	IONOS-AS This is the joint network for IONOS, Fasthosts, Arsys, 1&1 Mail and Media and 1&1 Telecom. Formerly known as 1&1 Internet SE., DE
23.227.38.0/23	2	CLOUDFLARENET, US
66.235.200.0/24	2	CLOUDFLARENET, US
103.224.212.0/23	2	TRELLIAN-AS-AP Trellian Pty. Limited, AU
35.168.0.0/13	2	AMAZON-AES, US
147.135.0.0/17	2	OVH, FR
194.58.112.0/24	2	AS-REG, RU
94.136.40.0/24	2	GD-EMEA-DC-LD5, DE
192.64.117.0/24	2	NAMECHEAP-NET, US
198.187.29.0/24	2	NAMECHEAP-NET, US
198.187.31.0/24	2	NAMECHEAP-NET, US
173.236.128.0/17	2	DREAMHOST-AS, US
75.119.192.0/20	2	DREAMHOST-AS, US
199.34.228.0/22	2	WEEBLY, US
66.96.162.0/24	2	BIZLAND-SD, US
208.117.0.0/19	2	STEADFAST, US
81.88.48.0/20	2	REGISTER-AS, IT
173.201.176.0/20	2	GO-DADDY-COM-LLC, US
208.91.197.0/24	2	CONFLUENCE-NETWORK-INC, VG
162.144.0.0/16	2	UNIFIEDLAYER-AS-1, US

```
  162.241.0.0/16 |      2 | UNIFIEDLAYER-AS-1, US
192.185.192.0/19 |      2 | UNIFIEDLAYER-AS-1, US
 74.220.192.0/19 |      2 | UNIFIEDLAYER-AS-1, US
 185.201.10.0/23 |      2 | AS-HOSTINGER, CY
185.224.136.0/22 |      2 | AS-HOSTINGER, CY
 91.195.240.0/23 |      2 | SEDO-AS, DE
198.185.159.0/24 |      2 | SQUARESPACE, US
  198.49.23.0/24 |      2 | SQUARESPACE, US
   37.1.216.0/21 |      2 | SCALAXY-AS, NL
 81.169.144.0/22 |      2 | STRATO STRATO AG, DE
   118.27.0.0/17 |      2 | INTERQ GMO Internet,Inc, JP
 163.44.176.0/20 |      2 | INTERQ GMO Internet,Inc, JP
 46.242.128.0/17 |      1 | HOMEPL-AS, PL
   62.210.0.0/16 |      1 | Online SAS, FR
 202.233.66.0/23 |      1 | XSERVER Xserver Inc., JP
 219.94.200.0/24 |      1 | XSERVER Xserver Inc., JP
   46.23.64.0/21 |      1 | UK2NET-AS, GB
 83.170.124.0/24 |      1 | UK2NET-AS, GB
  103.75.44.0/22 |      1 | POWERLINE-AS-AP POWER LINE DATACENTER, HK
  104.21.96.0/20 |      1 | CLOUDFLARENET, US
 172.65.224.0/20 |      1 | CLOUDFLARENET, US
156.255.128.0/17 |      1 | XIAOZHIYUN1-AS-AP ICIDC NETWORK, US
 23.235.160.0/20 |      1 | XIAOZHIYUN1-AS-AP ICIDC NETWORK, US
 103.96.120.0/24 |      1 | CW-AS-AP Child Wisdom Limited, HK
 209.54.113.0/24 |      1 | COGECO-PEER1, CA
 103.148.14.0/24 |      1 | INTERNETINC-AS-AP 360 Internet Inc, BD
 128.199.64.0/18 |      1 | DIGITALOCEAN-ASN, US
 138.197.96.0/20 |      1 | DIGITALOCEAN-ASN, US
 178.62.192.0/18 |      1 | DIGITALOCEAN-ASN, US
  64.225.96.0/20 |      1 | DIGITALOCEAN-ASN, US
 190.121.64.0/18 |      1 | Telefonica del Sur S.A., CL
   100.24.0.0/13 |      1 | AMAZON-AES, US
  174.129.0.0/16 |      1 | AMAZON-AES, US
   34.192.0.0/12 |      1 | AMAZON-AES, US
     52.0.0.0/15 |      1 | AMAZON-AES, US
    52.44.0.0/15 |      1 | AMAZON-AES, US
   54.160.0.0/14 |      1 | AMAZON-AES, US
   54.172.0.0/15 |      1 | AMAZON-AES, US
 216.239.32.0/24 |      1 | GOOGLE, US
 216.239.34.0/24 |      1 | GOOGLE, US
 216.239.36.0/24 |      1 | GOOGLE, US
 216.239.38.0/24 |      1 | GOOGLE, US
  23.236.48.0/20 |      1 | GOOGLE, US
   34.100.0.0/14 |      1 | GOOGLE, US
   34.124.0.0/14 |      1 | GOOGLE, US
    34.80.0.0/14 |      1 | GOOGLE, US
    34.96.0.0/14 |      1 | GOOGLE, US
   35.186.0.0/16 |      1 | GOOGLE, US
   35.200.0.0/14 |      1 | GOOGLE, US
   35.204.0.0/15 |      1 | GOOGLE, US
  35.207.64.0/18 |      1 | GOOGLE, US
```

cobaltstrike-beacons-dork / heige @ 2020-04-10

SRC: blog

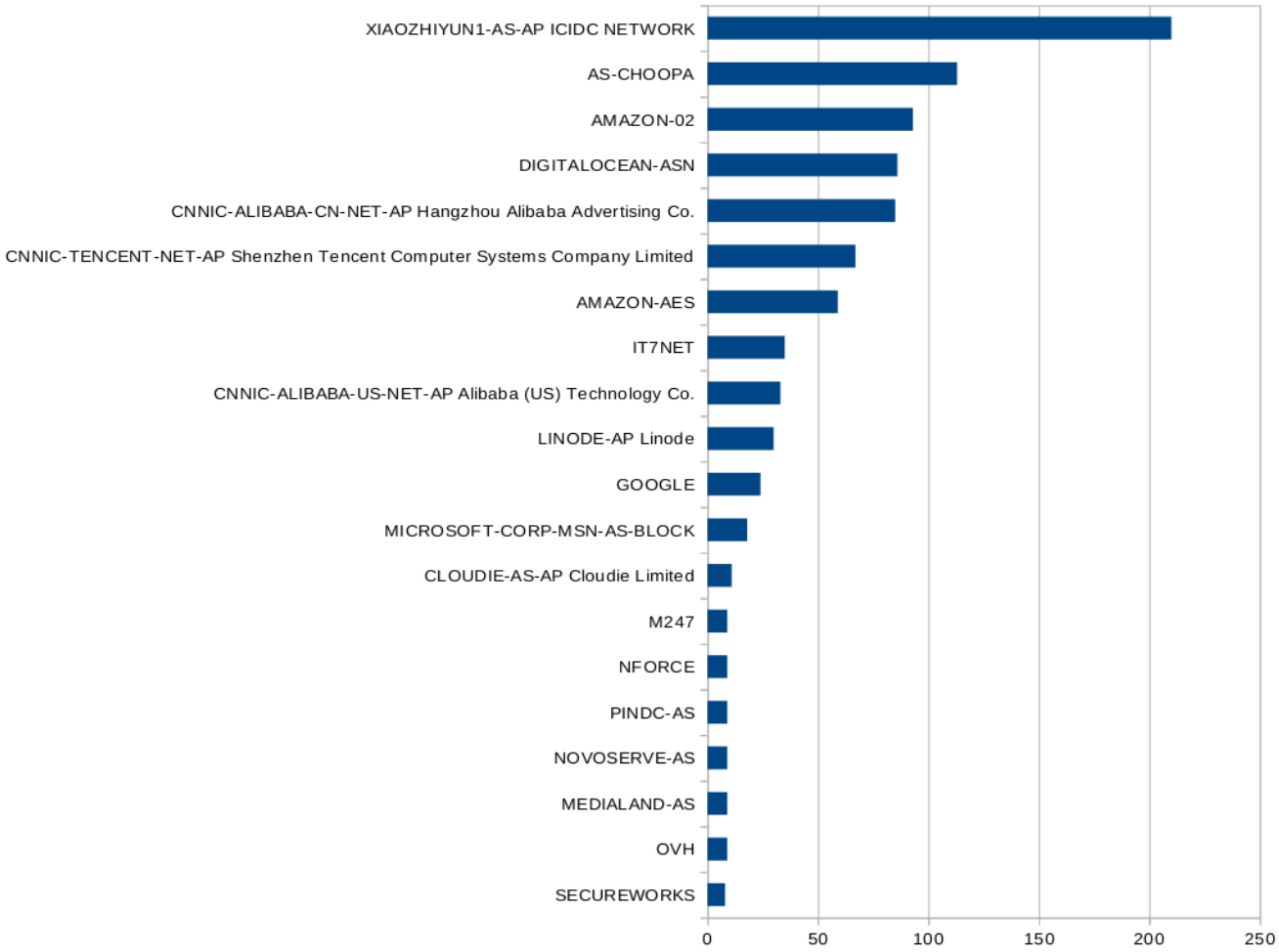
Identifying Cobalt Strike team servers in the wild by using ZoomEye(Part 2)

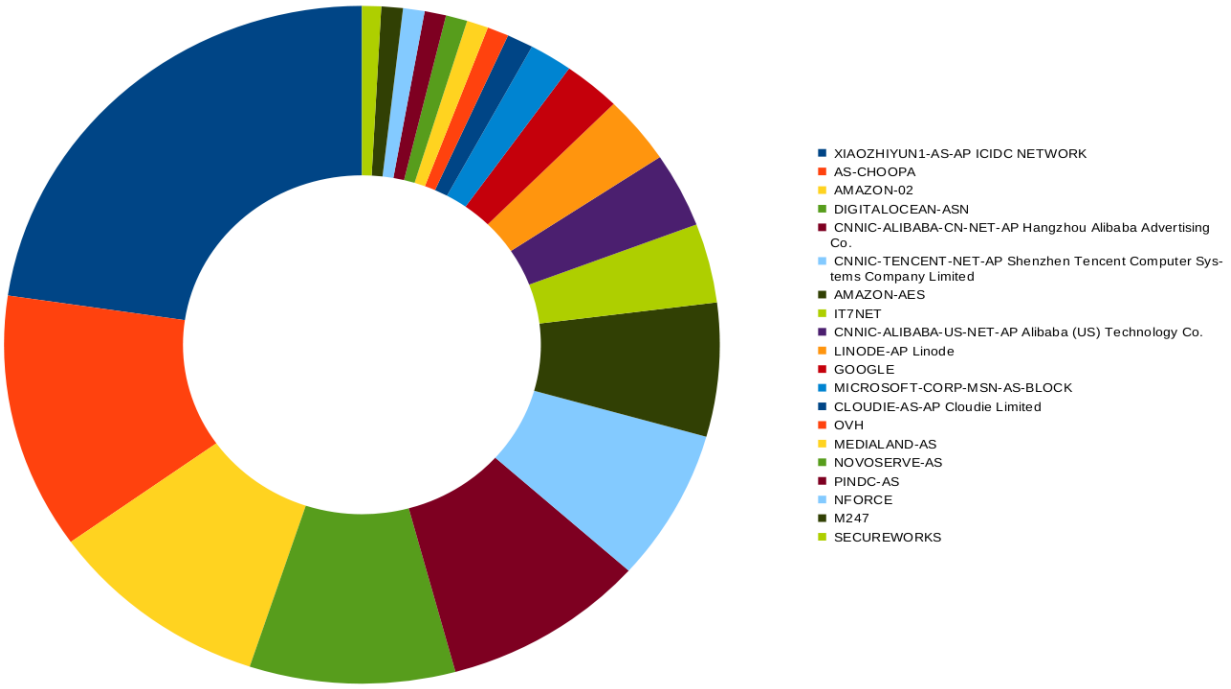
heige Apr 10, 2020 · 3 min read

by Heige of KnownSec 404 Team 04/10/2020

below is summary for 1200 IPs found with a dork mentioned in the blog by @heige separated after AS, Countries and Networks where these IPs originate from.

The charts represent the distribution in % and count for the Top 20 AS




XIAOZHIYUN1-AS-AP ICIDC NETWORK
AS-CHOOPA
AMAZON-02
DIGITALOCEAN-ASN
CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.
CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited
AMAZON-AES
IT7NET
CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co.
LINODE-AP Linode
GOOGLE
MICROSOFT-CORP-MSN-AS-BLOCK
CLOUDIE-AS-AP Cloudie Limited
OVH
MEDIALAND-AS
NOVOSERVE-AS
PINDC-AS
NFORCE
M247
SECUREWORKS

SUMMARY for cobaltstrike_beacons / dork by heige 2020-04-18

IPs : 1275
Networks : 728
ASNs : 190
Countries : 39

Top 100 ASNs

ASN_NR	Count	ASNName
136800	210	XIAOZHIYUN1-AS-AP ICIDC NETWORK, US
20473	113	AS-CHOOPA, US
16509	93	AMAZON-02, US
14061	86	DIGITALOCEAN-ASN, US
37963	85	CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising Co.,Ltd., CN
45090	67	CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems Company Limited, CN
14618	59	AMAZON-AES, US
25820	35	IT7NET, CA
45102	33	CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co., Ltd., CN
63949	30	LINODE-AP Linode, LLC, US
15169	24	GOOGLE, US
8075	18	MICROSOFT-CORP-MSN-AS-BLOCK, US
55933	11	CLOUDIE-AS-AP Cloudie Limited, HK
16276	9	OVH, FR
206728	9	MEDIALAND-AS, RU
24875	9	NOVOSERVE-AS, NL
34665	9	PINDC-AS, RU
43350	9	NFORCE, NL
9009	9	M247, GB
22992	8	SECUREWORKS, US
57043	7	HOSTKEY-AS, NL
59253	7	LEASEWEB-APAC-SIN-11 Leaseweb Asia Pacific pte. ltd., SG
200019	6	ALEXHOST, MD
30823	6	COMBAHTON combahton GmbH, DE
133115	5	HKKFGL-AS-AP HK Kwaifong Group Limited, HK
137443	5	ANCHGLOBAL-AS-AP Anchnet Asia Limited, HK
202448	5	MVPS https://www.mvps.net, CY
206804	5	ESTNOC-AS, EE
20860	5	IOMART-AS, GB
210138	5	FLOWSPEC-AS, UA
38365	5	BAIDU Beijing Baidu Netcom Science and Technology Co., Ltd., CN
45753	5	NETSEC-HK NETSEC, HK
49877	5	RMINJINERING, RU
63473	5	HOSTHATCH, US
852	5	TELUS Communications, CA
132203	4	TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue, CN
134548	4	DXTL-HK DXTL Tseung Kwan O Service, HK
35913	4	DEDIPATH-LLC, US
36352	4	AS-COLOCROSSING, US
394380	4	LEASEWEB-USA-DAL-10, US
396362	4	LEASEWEB-USA-NYC-11, US

```
 40065 |      4 | CNSERVERS, US
 44812 |      4 | IPSERVER-RU-NET Fiord, RU
 48282 |      4 | VDSINA-AS, RU
 49505 |      4 | SELECTEL, RU
 54290 |      4 | HOSTWINDS, US
 64050 |      4 | BCPL-SG BGPNET Global ASN, SG
  8100 |      4 | ASN-QUADRANET-GLOBAL, US
  8987 |      4 | AMAZON EXPANSION, IE
 11042 |      3 | NTHL, US
135373 |      3 | EFLYPRO-AS-AP EFLY NETWORK LIMITED, HK
136933 |      3 | GIGABITBANK-AS-AP Gigabitbank Global, HK
139330 |      3 | SANRENDATALIMITED-AS-AP SANREN DATA LIMITED, HK
139640 |      3 | HKNEWCLOUD-AS-AP HK NEW CLOUD TECHNOLOGY LIMITED, HK
211895 |      3 | SERVERIUS-USERS-AS, NL
 31400 |      3 | ACCELERATED-IT, DE
 31863 |      3 | DACEN-2, US
395954 |      3 | LEASEWEB-USA-LAX-11, US
 40676 |      3 | AS40676, US
 44094 |      3 | WEBHOST1-AS, RU
 45996 |      3 | GNJ-AS-KR DAOU TECHNOLOGY, KR
 51852 |      3 | PLI-AS, PA
 55720 |      3 | GIGABIT-MY Gigabit Hosting Sdn Bhd, MY
 58329 |      3 | RACKPLACE, DE
 59371 |      3 | DNC-AS Dimension Network & Communication Limited, HK
 60117 |      3 | HS, AE
 60781 |      3 | LEASEWEB-NL-AMS-01 Netherlands, NL
 61272 |      3 | IST-AS, LT
  6134 |      3 | XNNET, US
132422 |      2 | TELECOM-HK Hong Kong Telecom Global Data Centre, HK
132839 |      2 | POWERLINE-AS-AP POWER LINE DATACENTER, HK
135377 |      2 | UCLOUD-HK-AS-AP UCLOUD INFORMATION TECHNOLOGY (HK) LIMITED, HK
136907 |      2 | HWCLOUDS-AS-AP HUAWEI CLOUDS, HK
137431 |      2 | RPCL-AS-AP ZORRO RITZ PUBLIC COMPANY LIMITED, MM
 16125 |      2 | CHERRYSERVERS1-AS, LT
   174 |      2 | COGENT-174, US
 20278 |      2 | NEXEON, US
 21100 |      2 | ITLDC-NL, UA
  2119 |      2 | TELENOR-NEXTEL Telenor Norge AS, NO
 22612 |      2 | NAMECHEAP-NET, US
 23470 |      2 | RELIABLESITE, US
 25369 |      2 | BANDWIDTH-AS, GB
 29802 |      2 | HVC-AS, US
 30633 |      2 | LEASEWEB-USA-WDC, US
 30860 |      2 | YURTEH-AS, UA
 35916 |      2 | MULTA-ASN1, US
 38283 |      2 | CHINANET-SCIDC-AS-AP CHINANET SiChuan Telecom Internet Data
Center, CN
398019 |      2 | DYNU, US
  4134 |      2 | CHINANET-BACKBONE No.31,Jin-rong Street, CN
 42237 |      2 | ICME, IM
 43513 |      2 | NANO-AS, LV
 44477 |      2 | WELLWEB, NL
 49981 |      2 | WORLDSTREAM, NL
 52173 |      2 | MAKONIX, LV
 55990 |      2 | HWCSNET Huawei Cloud Service data center, CN
```

```
    57367 |      2 | ECO-ATMAN-PL ECO-ATMAN-, PL
    62904 |      2 | EONIX-COMMUNICATIONS-ASBLOCK-62904, US
    63612 |      2 | XIAONIAOYUN Shenzhen Qianhai bird cloud computing Co. Ltd., CN
    63646 |      2 | XJKJ Beijing Xiaoju Science and Technology Co., Ltd., CN
       NA |      2 | NA
    12083 |      1 | WOW-INTERNET, US
    12876 |      1 | Online SAS, FR
   132347 |      1 | MIKIPRO-AS-AP MikiPro Ltd, NZ
   133199 |      1 | SONDERCLOUDLIMITED-AS-AP SonderCloud Limited, HK
   133774 |      1 | CHINATELECOM-FUJIAN-FUZHOU-IDC1 Fuzhou, CN
   133779 |      1 | HDIL-AS-AP Huayun Data International Limited, HK
   134176 |      1 | RAIBOW-AS-AP Rainbow network limited, HK
   134520 |      1 | GIGSGIGSCLOUD-AS-AP GigsGigs Network Services, HK
   134542 |      1 | UNICOM-GUIAN China Unicom IP network, CN
   134762 |      1 | CHINANET-LIAONING-DALIAN-MAN CHINANET Liaoning province Dalian
MAN network, CN
   134835 |      1 | SNL-HK Starry Network Limited, HK
   136038 |      1 | HDTIDCCLOUD-AS-AP HDTIDC LIMITED, HK
   136190 |      1 | CHINATELECOM-ZHEJIANG-JINHUA-IDC JINHUA, ZHEJIANG Province,
P.R.China., CN
   136958 |      1 | UNICOM-GUANGZHOU-IDC China Unicom Guangdong IP network, CN
   137951 |      1 | CLAYERLIMITED-AS-AP Clayer Limited, HK
   138152 |      1 | YISUCLOUDLTD-HK YISU CLOUD LTD, HK
   139293 |      1 | UFO-AS-AP UFO Network Limited, HK
   142032 |      1 | HFTCL-AS-AP High Family Technology Co., Limited, HK
    17444 |      1 | NWT-AS-AP AS number for New World Telephone Ltd., HK
    19148 |      1 | LEASEWEB-USA-PHX-11, US
   198203 |      1 | ASN-ROUTELABEL, NL
   198610 |      1 | BEGET-AS, RU
   200651 |      1 | FLOKINET, SC
    20141 |      1 | QTS-SUW1-ATL1, US
   202425 |      1 | INT-NETWORK, SC
    20326 |      1 | TERASWITCH, US
    20454 |      1 | SSASN2, US
   204601 |      1 | ON-LINE-DATA Server location - Netherlands, Dronten, NL
   207345 |      1 | OMITLTD, GB
   207566 |      1 | HOSTWAY-AS, RU
    23724 |      1 | CHINANET-IDC-BJ-AP IDC, China Telecommunications Corporation, CN
    23858 |      1 | XTOM-AS-AU xTom, AU
    24000 |      1 | LIHGL-AS-AP 24.hk global BGP, HK
    27715 |      1 | Locaweb Servicos de Internet S/A, BR
    29182 |      1 | THEFIRST-AS, RU
    30083 |      1 | AS-30083-GO-DADDY-COM-LLC, US
    30491 |      1 | CROWEHORWATH, US
    32097 |      1 | WII, US
   328608 |      1 | Africa-on-Cloud-AS, ZA
    34224 |      1 | NETERRA-AS, BG
    34888 |      1 | SIMPLECARRER2, US
     3549 |      1 | LVLT-3549, US
    36351 |      1 | SOFTLAYER, US
    36436 |      1 | INFOBUNKER, US
    38186 |      1 | FTG-AS-AP Forewin Telecom Group Limited, ISP at, HK
    38197 |      1 | SUNHK-DATA-AS-AP Sun Network (Hong Kong) Limited - HongKong
Backbone, HK
    39378 |      1 | SERVINGA, DE
```

```
   394991 |      1 | ASN-SWC, US
   395839 |      1 | HOSTKEY-USA, US
   396190 |      1 | LEASEWEB-USA-SEA-10, US
   398110 |      1 | GO-DADDY-COM-LLC, US
    42159 |      1 | DELTAHOST-AS, UA
    42675 |      1 | OBEHOSTING Obehosting AB, SE
    42708 |      1 | PORTLANE www.portlane.com, SE
    45538 |      1 | ODS-AS-VN Online data services, VN
    47583 |      1 | AS-HOSTINGER, CY
    48024 |      1 | NEROCLOUD, GB
     4808 |      1 | CHINA169-BJ China Unicom Beijing Province Network, CN
    48108 |      1 | VIRTUALDC, LV
     4816 |      1 | CHINANET-IDC-GD China Telecom (Group), CN
    48347 |      1 | MTW-AS, RU
     4837 |      1 | CHINA169-BACKBONE CHINA UNICOM China169 Backbone, CN
    49367 |      1 | ASSEFLOW Amsterdam Internet Exchange (AMS-IX), IT
    50340 |      1 | SELECTEL-MSK, RU
    50867 |      1 | HOSTKEY-RU-AS, NL
    51395 |      1 | AS-SOFTPLUS, CH
    53755 |      1 | IOFLOOD, US
    55960 |      1 | BJ-GUANGHUAN-AP Beijing Guanghuan Xinwang Digital, CN
    56067 |      1 | METRABYTE-TH 453 Ladplacout Jorakhaebua, TH
     5650 |      1 | FRONTIER-FRTR, US
    56694 |      1 | DHUB, RU
    57509 |      1 | LL-INVESTMENT-LTD, BG
    57918 |      1 | ACOD-AS, RU
    58061 |      1 | SCALAXY-AS, NL
    58466 |      1 | CT-GUANGZHOU-IDC CHINANET Guangdong province network, CN
    58593 |      1 | BLUECLOUD Shanghai Blue Cloud Technology Co.,Ltd, CN
    59711 |      1 | HZ-EU-AS, BG
    59729 |      1 | ITL-BG, UA
    60567 |      1 | DATACLUB-SE, BZ
    61046 |      1 | HZ-UK-AS, BG
    62370 |      1 | SNEL, NL
    62468 |      1 | VPSQUAN, US
    63252 |      1 | NEXTFORT, US
    64022 |      1 | KAMATERAINC-AS-AP Kamatera, Inc., HK
     6878 |      1 | AS6878, DE
     8315 |      1 | SENTIA, NL
     8560 |      1 | IONOS-AS This is the joint network for IONOS, Fasthosts, Arsys,
1&1 Mail and Media and 1&1 Telecom. Formerly known as 1&1 Internet SE., DE
     8920 |      1 | VTC-AS Russia, Vladivostok, RU
     9123 |      1 | TIMEWEB-AS, RU
     9919 |      1 | NCIC-TW New Century InfoComm Tech Co., Ltd., TW

Top 100 Countries
Country |  Count
--------+-----------
     US |    540
     SC |    226
     CN |    191
     RU |     53
     CA |     47
     NL |     35
     HK |     33
```

```
     SG |     25
     DE |     21
     GB |     16
     UA |     10
     FR |      9
     MD |      7
     RO |      7
     LT |      5
     CY |      5
     BG |      4
     PA |      4
     LV |      4
     PL |      3
     SE |      3
     KR |      3
     AE |      3
     MO |      2
     ZA |      2
     MM |      2
     IM |      2
     BZ |      2
     NZ |      1
     EE |      1
     NO |      1
     BR |      1
     VN |      1
     IT |      1
     CH |      1
     MY |      1
     TH |      1
     TW |      1
        |      1

Top 100 Networks
NW                |  Count | NetworkName
------------------+--------+-----------------------------------
 156.255.128.0/17 |    204 | XIAOZHIYUN1-AS-AP ICIDC NETWORK, US
    47.100.0.0/15 |     12 | CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising
Co.,Ltd., CN
     47.56.0.0/16 |     12 | CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co.,
Ltd., CN
    34.192.0.0/12 |     10 | AMAZON-AES, US
    34.224.0.0/12 |      7 | AMAZON-AES, US
       3.8.0.0/14 |      7 | AMAZON-02, US
  167.179.64.0/18 |      7 | AS-CHOOPA, US
  185.147.12.0/22 |      7 | NOVOSERVE-AS, NL
   31.44.184.0/24 |      7 | PINDC-AS, RU
     39.96.0.0/14 |      7 | CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising
Co.,Ltd., CN
  23.106.120.0/21 |      7 | LEASEWEB-APAC-SIN-11 Leaseweb Asia Pacific pte. ltd., SG
    34.240.0.0/13 |      6 | AMAZON-02, US
   45.141.86.0/24 |      6 | MEDIALAND-AS, RU
   23.226.56.0/21 |      5 | XIAOZHIYUN1-AS-AP ICIDC NETWORK, US
    18.208.0.0/13 |      5 | AMAZON-AES, US
     3.224.0.0/12 |      5 | AMAZON-AES, US
```

```
     3.132.0.0/14 |      5 | AMAZON-02, US
  176.121.14.0/24 |      5 | FLOWSPEC-AS, UA
    47.102.0.0/15 |      5 | CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising
Co.,Ltd., CN
    47.107.0.0/16 |      5 | CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising
Co.,Ltd., CN
    47.240.0.0/17 |      5 | CNNIC-ALIBABA-US-NET-AP Alibaba (US) Technology Co.,
Ltd., CN
 112.121.172.0/24 |      5 | NETSEC-HK NETSEC, HK
 185.153.196.0/22 |      5 | RMINJINERING, RU
   31.220.42.0/24 |      5 | HOSTHATCH, US
     13.64.0.0/11 |      5 | MICROSOFT-CORP-MSN-AS-BLOCK, US
   207.219.0.0/16 |      5 | TELUS Communications, CA
  206.189.32.0/20 |      4 | DIGITALOCEAN-ASN, US
     52.90.0.0/15 |      4 | AMAZON-AES, US
    18.130.0.0/16 |      4 | AMAZON-02, US
     3.120.0.0/14 |      4 | AMAZON-02, US
    34.208.0.0/12 |      4 | AMAZON-02, US
    35.176.0.0/15 |      4 | AMAZON-02, US
  149.28.192.0/19 |      4 | AS-CHOOPA, US
    45.77.32.0/20 |      4 | AS-CHOOPA, US
  78.129.128.0/17 |      4 | IOMART-AS, GB
  206.55.100.0/23 |      4 | SECUREWORKS, US
  206.55.102.0/23 |      4 | SECUREWORKS, US
    120.78.0.0/16 |      4 | CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising
Co.,Ltd., CN
     47.94.0.0/15 |      4 | CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising
Co.,Ltd., CN
  172.241.24.0/21 |      4 | LEASEWEB-USA-DAL-10, US
  46.166.128.0/21 |      4 | NFORCE, NL
 209.217.224.0/19 |      3 | NTHL, US
 103.143.159.0/24 |      3 | GIGABITBANK-AS-AP Gigabitbank Global, HK
 103.249.106.0/24 |      3 | SANRENDATALIMITED-AS-AP SANREN DATA LIMITED, HK
     3.208.0.0/12 |      3 | AMAZON-AES, US
      3.80.0.0/12 |      3 | AMAZON-AES, US
    34.64.0.0/14 |      3 | GOOGLE, US
    34.68.0.0/14 |      3 | GOOGLE, US
    34.92.0.0/14 |      3 | GOOGLE, US
    18.163.0.0/16 |      3 | AMAZON-02, US
      3.14.0.0/15 |      3 | AMAZON-02, US
    34.248.0.0/13 |      3 | AMAZON-02, US
    140.82.0.0/20 |      3 | AS-CHOOPA, US
  149.248.48.0/20 |      3 | AS-CHOOPA, US
    66.42.96.0/20 |      3 | AS-CHOOPA, US
   194.26.29.0/24 |      3 | MEDIALAND-AS, RU
 185.162.235.0/24 |      3 | SERVERIUS-USERS-AS, NL
  45.147.228.0/22 |      3 | COMBAHTON combahton GmbH, DE
    123.56.0.0/16 |      3 | CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising
Co.,Ltd., CN
    39.104.0.0/15 |      3 | CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising
Co.,Ltd., CN
    39.106.0.0/15 |      3 | CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising
Co.,Ltd., CN
    47.105.0.0/16 |      3 | CNNIC-ALIBABA-CN-NET-AP Hangzhou Alibaba Advertising
Co.,Ltd., CN
```

```
 109.201.128.0/19 |      3 | NFORCE, NL
 192.144.128.0/18 |      3 | CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems
Company Limited, CN
   49.232.32.0/20 |      3 | CNNIC-TENCENT-NET-AP Shenzhen Tencent Computer Systems
Company Limited, CN
  195.54.166.0/23 |      3 | SELECTEL, RU
  185.70.185.0/24 |      3 | HOSTKEY-AS, NL
  103.85.255.0/24 |      3 | DNC-AS Dimension Network & Communication Limited, HK
   2600:3c00::/32 |      3 | LINODE-AP Linode, LLC, US
    51.140.0.0/14 |      3 | MICROSOFT-CORP-MSN-AS-BLOCK, US
  163.53.245.0/24 |      2 | TELECOM-HK Hong Kong Telecom Global Data Centre, HK
  157.119.73.0/24 |      2 | EFLYPRO-AS-AP EFLY NETWORK LIMITED, HK
  154.209.64.0/19 |      2 | HKNEWCLOUD-AS-AP HK NEW CLOUD TECHNOLOGY LIMITED, HK
 104.248.112.0/20 |      2 | DIGITALOCEAN-ASN, US
 134.209.176.0/20 |      2 | DIGITALOCEAN-ASN, US
  138.68.240.0/20 |      2 | DIGITALOCEAN-ASN, US
 162.243.160.0/20 |      2 | DIGITALOCEAN-ASN, US
 167.172.128.0/20 |      2 | DIGITALOCEAN-ASN, US
 167.172.192.0/20 |      2 | DIGITALOCEAN-ASN, US
   167.71.64.0/20 |      2 | DIGITALOCEAN-ASN, US
 192.241.128.0/19 |      2 | DIGITALOCEAN-ASN, US
    100.24.0.0/13 |      2 | AMAZON-AES, US
    18.204.0.0/14 |      2 | AMAZON-AES, US
     52.20.0.0/14 |      2 | AMAZON-AES, US
    54.144.0.0/14 |      2 | AMAZON-AES, US
    54.174.0.0/15 |      2 | AMAZON-AES, US
    54.208.0.0/15 |      2 | AMAZON-AES, US
    35.200.0.0/14 |      2 | GOOGLE, US
    35.240.0.0/14 |      2 | GOOGLE, US
  46.166.168.0/21 |      2 | CHERRYSERVERS1-AS, LT
    18.176.0.0/15 |      2 | AMAZON-02, US
      3.20.0.0/14 |      2 | AMAZON-02, US
    35.156.0.0/14 |      2 | AMAZON-02, US
    35.178.0.0/15 |      2 | AMAZON-02, US
     52.58.0.0/15 |      2 | AMAZON-02, US
       38.0.0.0/8 |      2 | COGENT-174, US
   176.123.0.0/21 |      2 | ALEXHOST, MD
   45.67.229.0/24 |      2 | ALEXHOST, MD
  91.208.184.0/24 |      2 | ALEXHOST, MD
  45.153.184.0/24 |      2 | MVPS https://www.mvps.net, CY
```

Fragen? Kontakt: info@zero.bs
Filed: Mon 10 May 2021 (2021-05-10T00:00:00+02:00) | Analysis | Tags: cobaltstrike cti