

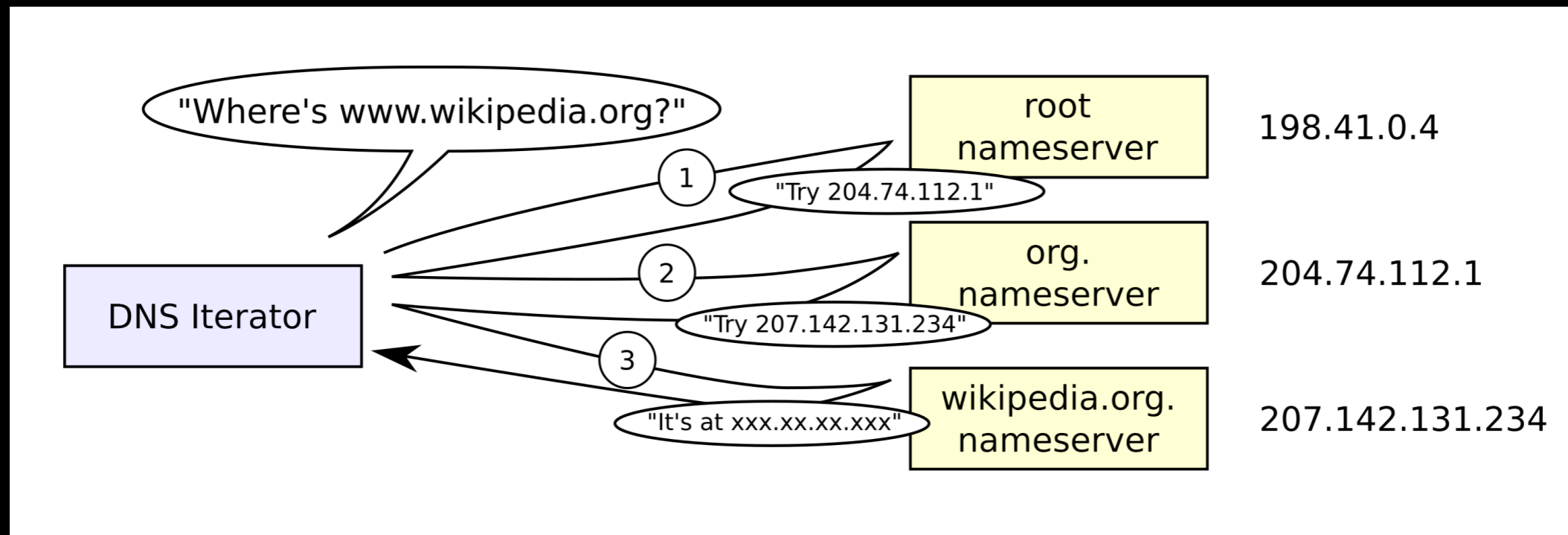
# \$0.02 DNS Firewall with MISP

PTS19 - @xme

# \$ whoami

<https://www.google.com/?q=Xavier+Mertens>

# No DNS == No Life



# Use your own resolver

- Restrict access to only local resolver only
- Log all queries
- DNS is a gold mine

# “RPZ”

Domain Name Service Response Policy Zones (DNS RPZ) is a method that allows a nameserver administrator to overlay custom information on top of the global DNS to provide alternate responses to queries. It is currently implemented in the ISC BIND nameserver (9.8 or later). Another generic name for the DNS RPZ functionality is "DNS firewall"

(© Wikipedia)

# “RPZ”

```
if $resolved_domain in $malicious_domains_list:  
    return $fake_address
```

# \$malicious\_domains\_list?

The screenshot shows the MISP (Malware Information Sharing Platform) interface. The browser address bar shows a URL starting with 'https://'. The navigation menu includes 'xameco', 'Event Actions', 'Galaxies', 'Input Filters', 'Global Actions', 'Sync Actions', 'Administration', and 'Audit'. The user is logged in as 'Xavier' and can 'Log out'. The event title is 'Malicious document - Operating Agreement 0102282019c...'. The event ID is 10540, and the UUID is 5c78d8f6-e1d8-4c0c-bebb-3745ac100a5a. The creator is CERTBw\_9014. The event is tagged with 'PAP:WHITE' and 'tlp:white'. The date is 2019-03-01, and the threat level is Low. The analysis is completed. The distribution is set to 'All communities'. The info field contains 'Malicious document - Operating Agreement 0102282019c00.doc'. The event was published on 2019-07-01 at 15:14:56. It has 15 attributes. The first recorded change was on 2019-03-01 at 07:20:04, and the last change was on 2019-06-30 at 04:31:02. There are 0 sightings, restricted to the own organization only. The interface includes a sidebar with options like 'View Event', 'View Correlation Graph', and 'Propose Attribute'. At the bottom, there are navigation buttons for 'Galaxies', 'previous', 'next', and 'view all'. The footer indicates the system is powered by MISP 2.4.109 on 2019-07-01 at 21:26:45.

Event ID	10540
UUID	5c78d8f6-e1d8-4c0c-bebb-3745ac100a5a
Creator org	CERTBw_9014
Tags	PAP:WHITE tlp:white
Date	2019-03-01
Threat Level	Low
Analysis	Completed
Distribution	All communities
Info	Malicious document - Operating Agreement 0102282019c00.doc
Published	Yes (2019-07-01 15:14:56)
#Attributes	15 (1 Object)
First recorded change	2019-03-01 07:20:04
Last change	2019-06-30 04:31:02
Modification map	
Sightings	0 (0) - restricted to own organisation only.

Navigation: - Pivots - Galaxy + Event graph + Correlation graph + ATT&CK matrix - Attributes - Discussion

Galaxies

« previous next » view all

Download: [GnuPG key](#) Hosted by Xavier Mertens Consulting | Powered by MISP 2.4.109 - 2019-07-01 21:26:45

# Step 1 - Extract data

```
# cat -n /usr/local/bin/misp-rpz-export.sh
1  #!/bin/bash
2  RPZFILE=/etc/bind/misp.rpz
3  curl \
4  -s \
5  -o $RPZFILE.new \
6  -d '{"returnFormat":"rpz","last":"30d","to_ids":1}' \
7  -H "Authorization: <redacted>" \
8  -H "Accept: application/json" \
9  -H "Content-type: application/json" \
10 -X POST https://<redacted>/attributes/restSearch \
11 && ( for i in {9..0}
12     do
13         mv $RPZFILE.$i $RPZFILE.$((i+1)) 2>/dev/null
14     done
15     mv $RPZFILE $RPZFILE.0 2>/dev/null
16     mv $RPZFILE.new $RPZFILE
17 ) \
18 && /usr/sbin/rndc reload
```



# Step 2 - Bind config

```
zone "misp.rpz" {
    type master;
    file "/etc/bind/misp.rpz";
}

options {
    response-policy {
        zone "misp.rpz" policy cname \
            malicious-domain-detected.<redacted>;
    };
};
```

# Step 2 - Bind config

```
logging {  
    channel rpz_log {  
        file "/mnt/named/rpz.log" versions 4 size 100m;  
        severity info;  
        print-category yes;  
        print-severity yes;  
        print-time yes;  
    };  
    category rpz { rpz_log; };  
}
```

# Test!

```
# host financialtimesguru.com
financialtimesguru.com is an alias for malicious-domain-detected.<redacted>.
malicious-domain-detected.<redacted>is an alias for malicious-domain-
detected.<redacted>.
malicious-domain-detected.<redacted> has address 127.0.0.1
```

# Thank You!

<https://isc.sans.edu/forums/diary/DNS+Firewalling+with+MISP/24556>