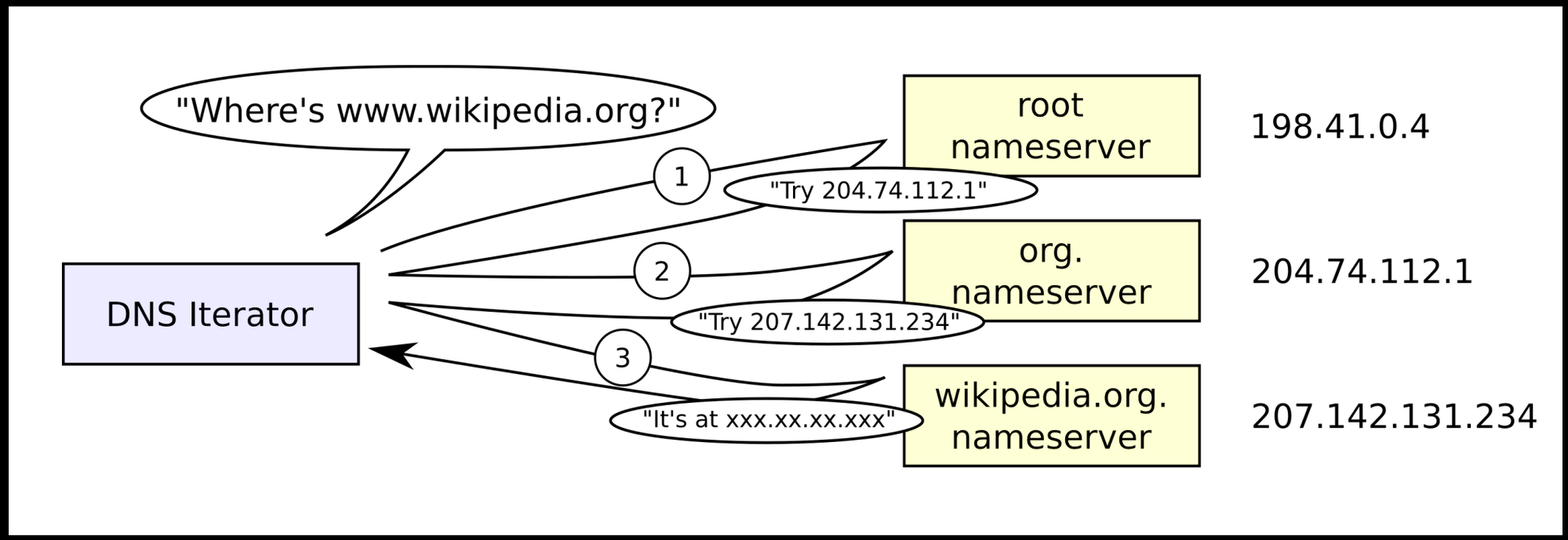
$0.02 DNS Firewall with MISP

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”

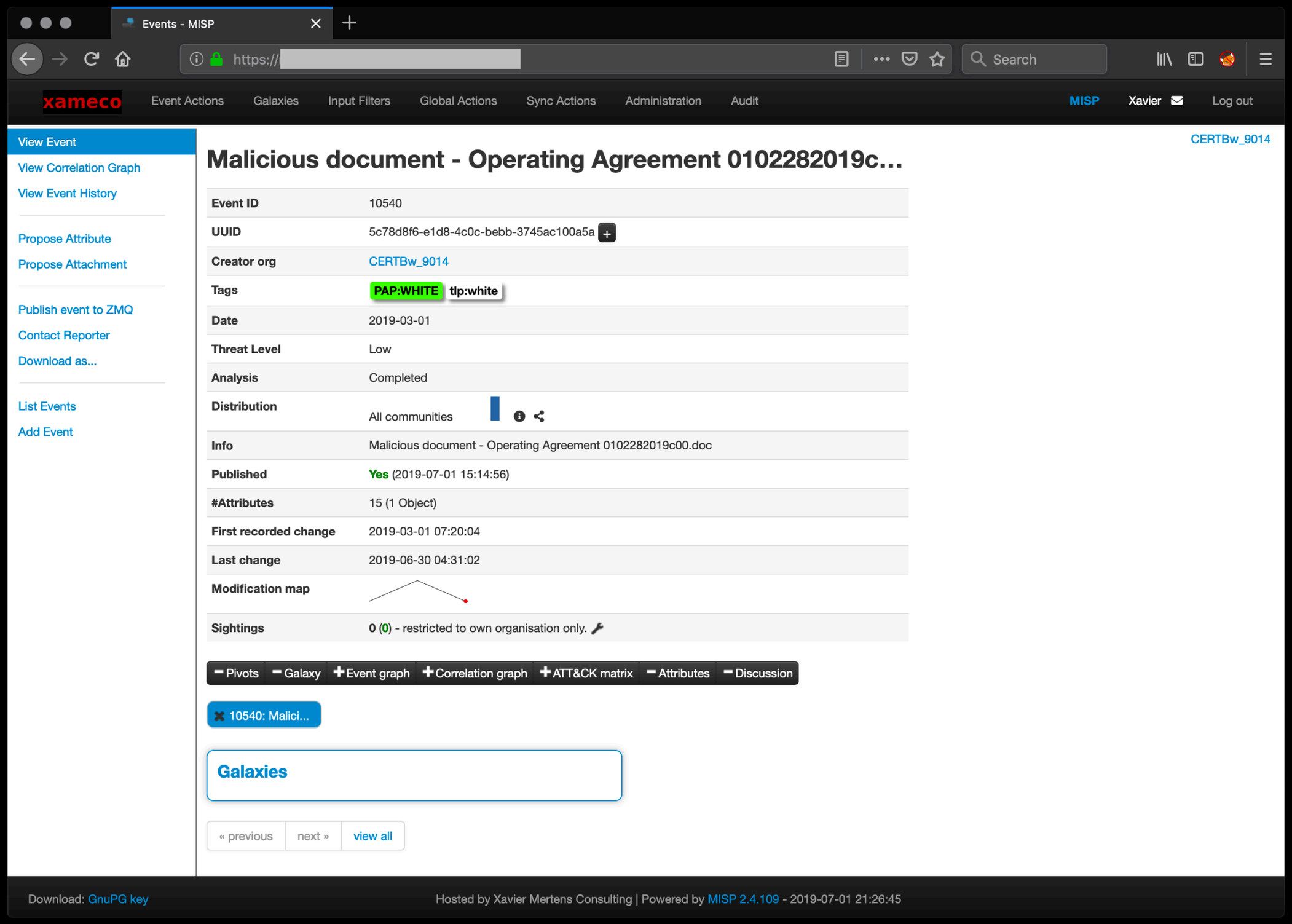
Domain Name Service Response Policy Zones (DNS RPZ) is a method that allows a nameserver administrator to overlay custom information on top of the global DNS to provide alternate responses to queries. It is currently implemented in the ISC BIND nameserver (9.8 or later). Another generic name for the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

(© Wikipedia)

“RPZ”

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

$malicious_domains_list?



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