DNS Firewall with Response Policy Zone

Suman Kumar Saha
bdCERT
suman@bdcert.org
Amber IT Limited
suman@amberit.com.bd

DNS Response Policy Zone(RPZ) as Firewall

- RPZ allows a recursive server to control the behavior of responses to queries.
- Administrator to overlay custom information on top of the global DNS to provide alternate responses to queries.
- RPZ data is supplied as a DNS zone, and can be loaded from a file or retrieved over the network by AXFR/IXFR.
- It works like firewall on cloud.
- DNS RPZ will block DNS resolution, machines connecting to the C&C via IP address will not be blocked.

DNS Response Policy Zone(RPZ)

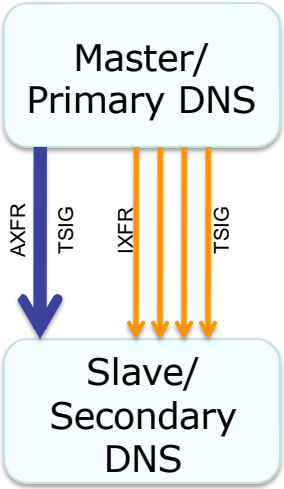
- Reputation data is packaged into Response Policy Zones (RPZs)
- RPZ's update frequently via IXFR/AXFR
- RPZ include both the filter criteria, and a response policy action
- BIND evaluates whether its response matches a filter in the RPZ and applies the policy specified
- RFC: https://tools.ietf.org/html/draft-ietf-dnsop-dns-rpz-00

Why We Need DNS RPZ?

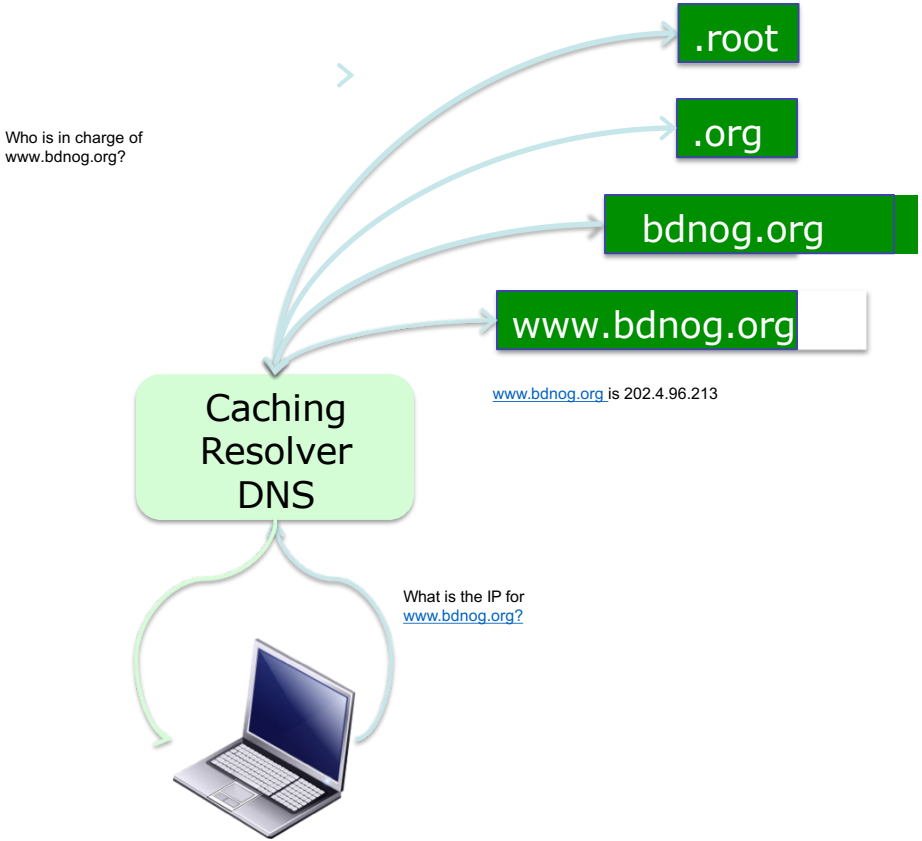
Ways of Content Filtering

- **Router ACLs**
- **Web proxy filter**
- **Content-aware firewall**
- **DNS RPZ**

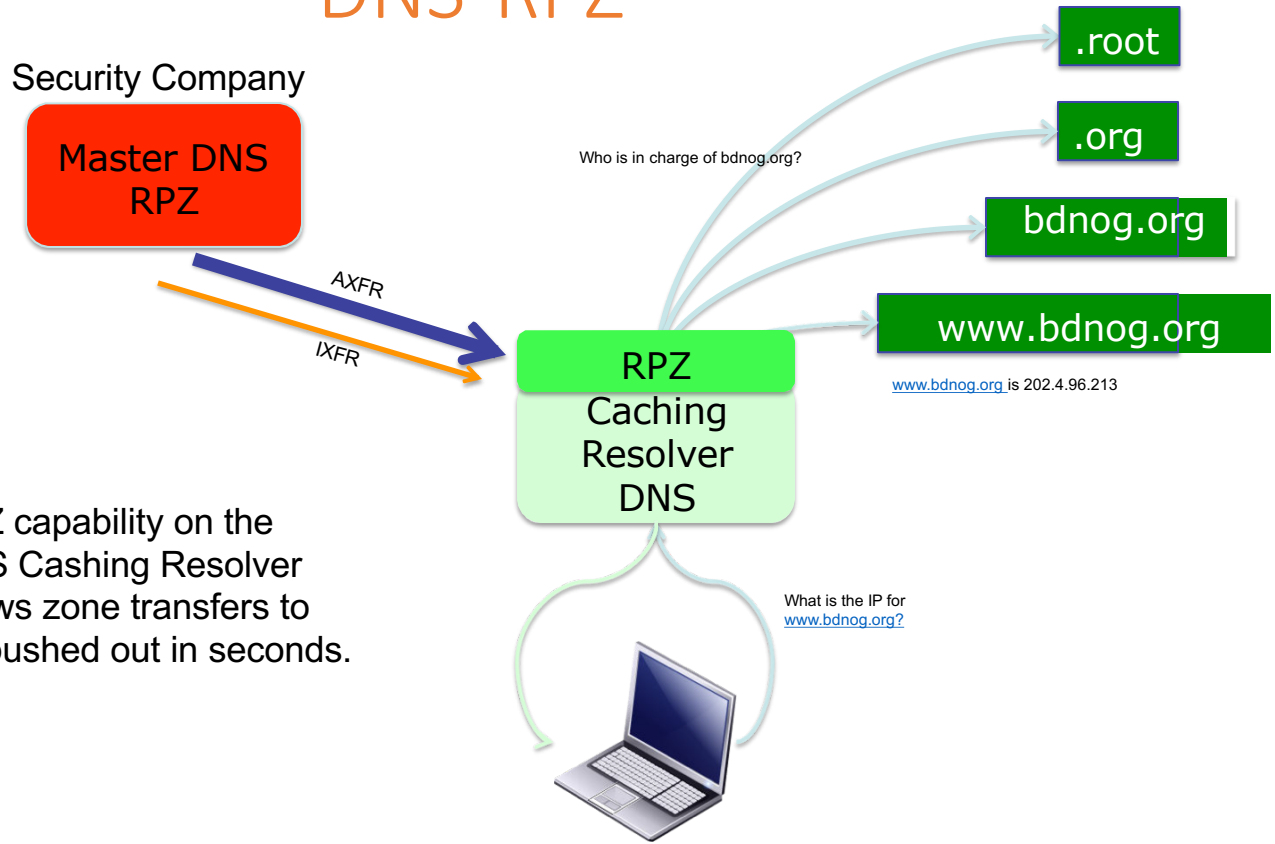
Core DNS Principles



AXFR - Full Zone Transfers
IXFR - Incremental Zone Transfers
TSIG - **Transaction SIGnature**
used to secure the AXFR/IXFR

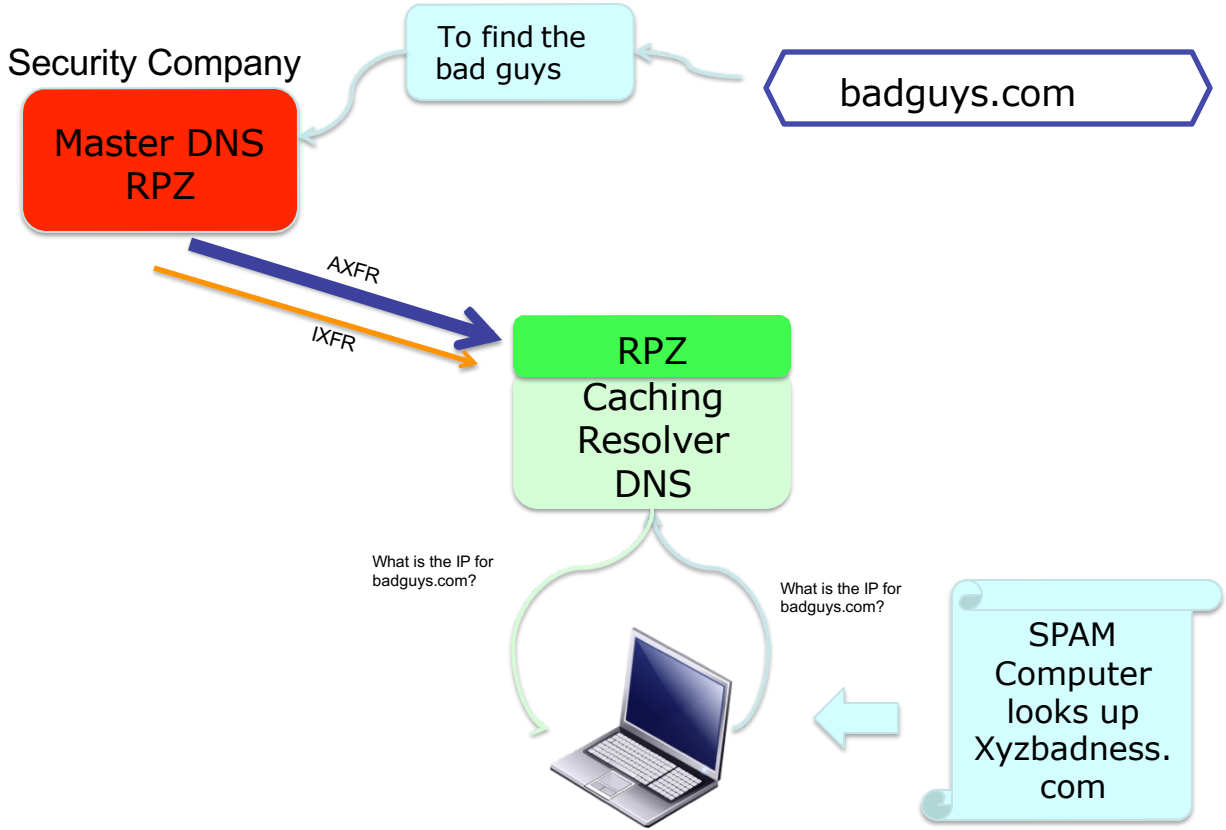


DNS RPZ

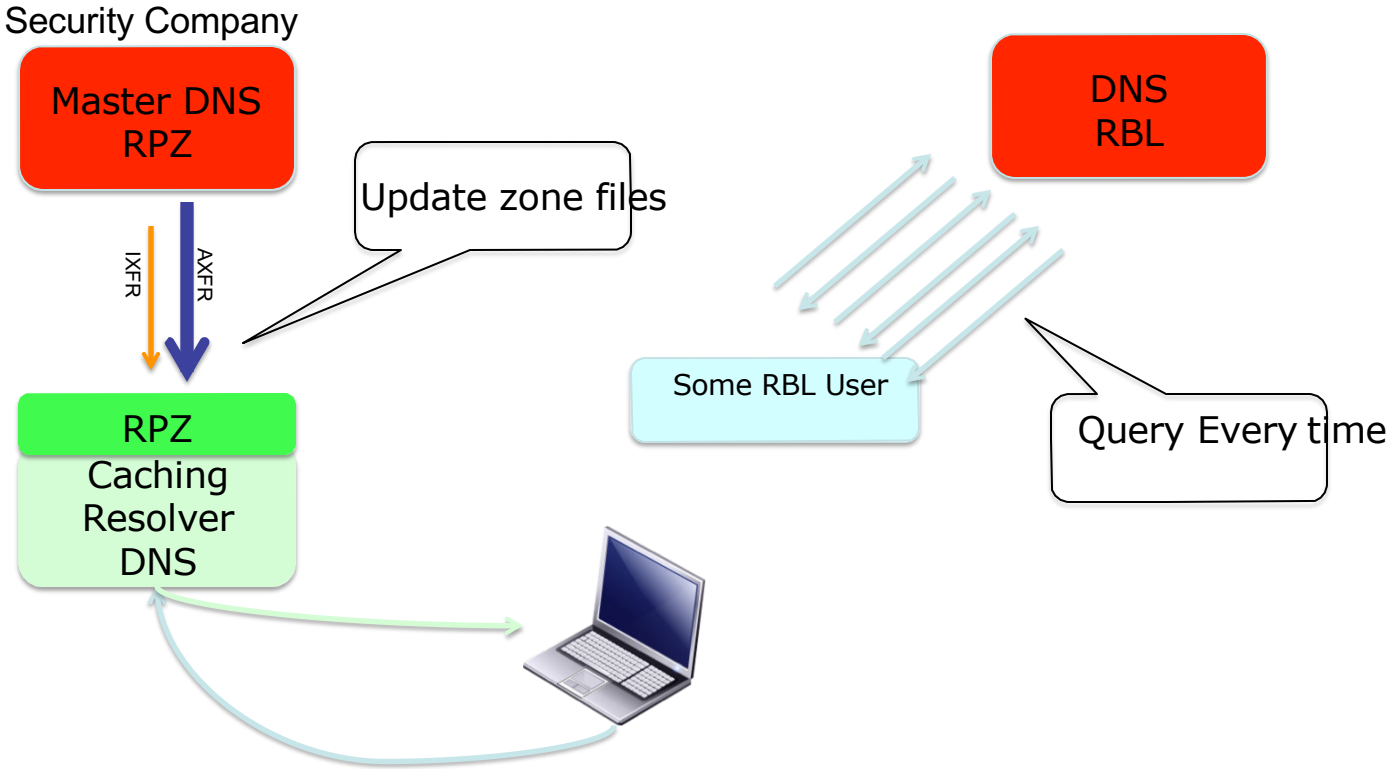


RPZ capability on the DNS Cashing Resolver allows zone transfers to be pushed out in seconds.

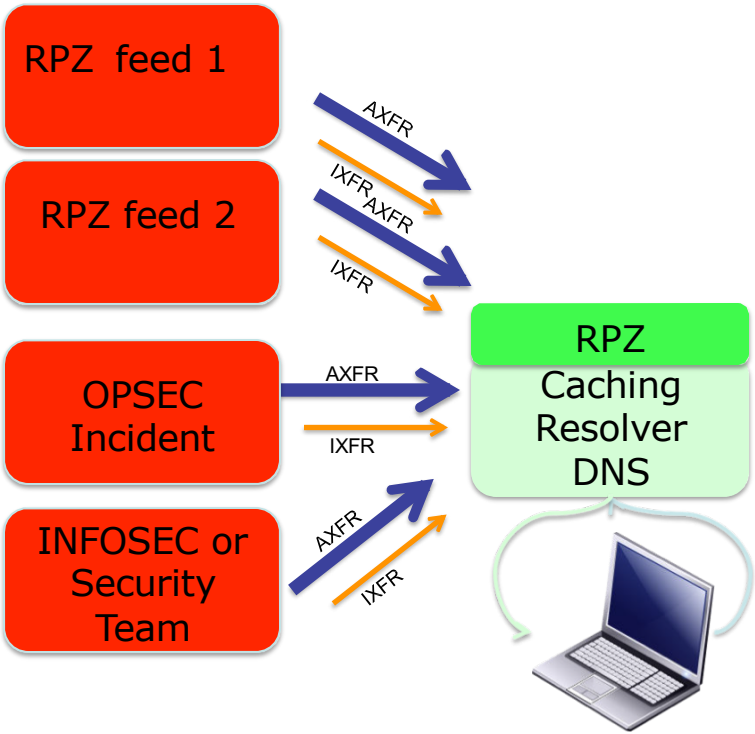
DNS RPZ in Action



How is DNSRPZ Different?



How is DNSRPZ Different?

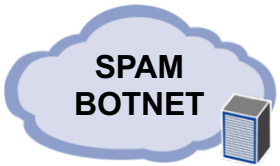


- DNSRPZ allows for multiple providers – building a richer list of "bad domains"
- Allows for industry incident feeds.
- Allows for local incident management feeds.

What DNS Firewall Can block Using RPZ

- **Phishing :** When a user clicks on a link in an email, for example from a fake banking site, you can intercept the lookup of that site.
- **Malware:** When a user attempts to navigate to a domain name known to host malware, you can redirect them to a site of your own with instructions on scanning their computer.
- **Ransomware:** Ransomware, is a type of malware in which someone takes over assets on your network and blocks access to them until you pay a ransom. This is a rapidly growing threat.
- **Botnet Command and Control sites :**When devices inside your network attempt to contact suspected botnet command central, drop the queries, and log them for analysis and followup.
- **Identify Infected Machines:** By analyzing the query logs, you can track down the machines in your network that are attempting to contact these abuse sites, and clean up any infections or botnet code.

Components of the Criminal Cloud




Drive-By


Secondary Malware


Controller


Proxy


Payment Processors


Mule Operations


Name Servers

- Avalanche: SPAM Cloud that you can lease time
- Zeus: Build your Own Criminal Cloud.
- BlackHole: Metasploit Cloud you can lease


BOT Herder

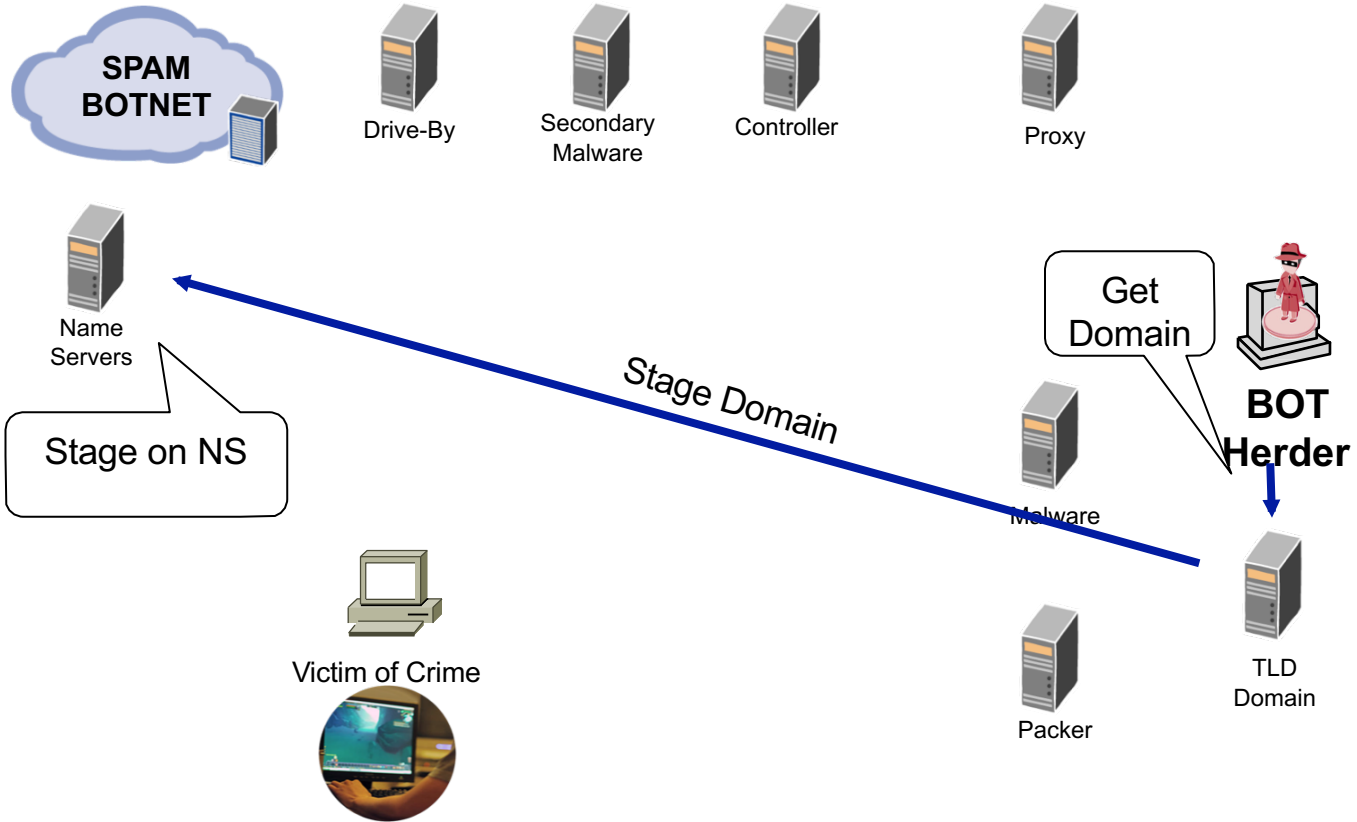

Malware


Victim of Crime

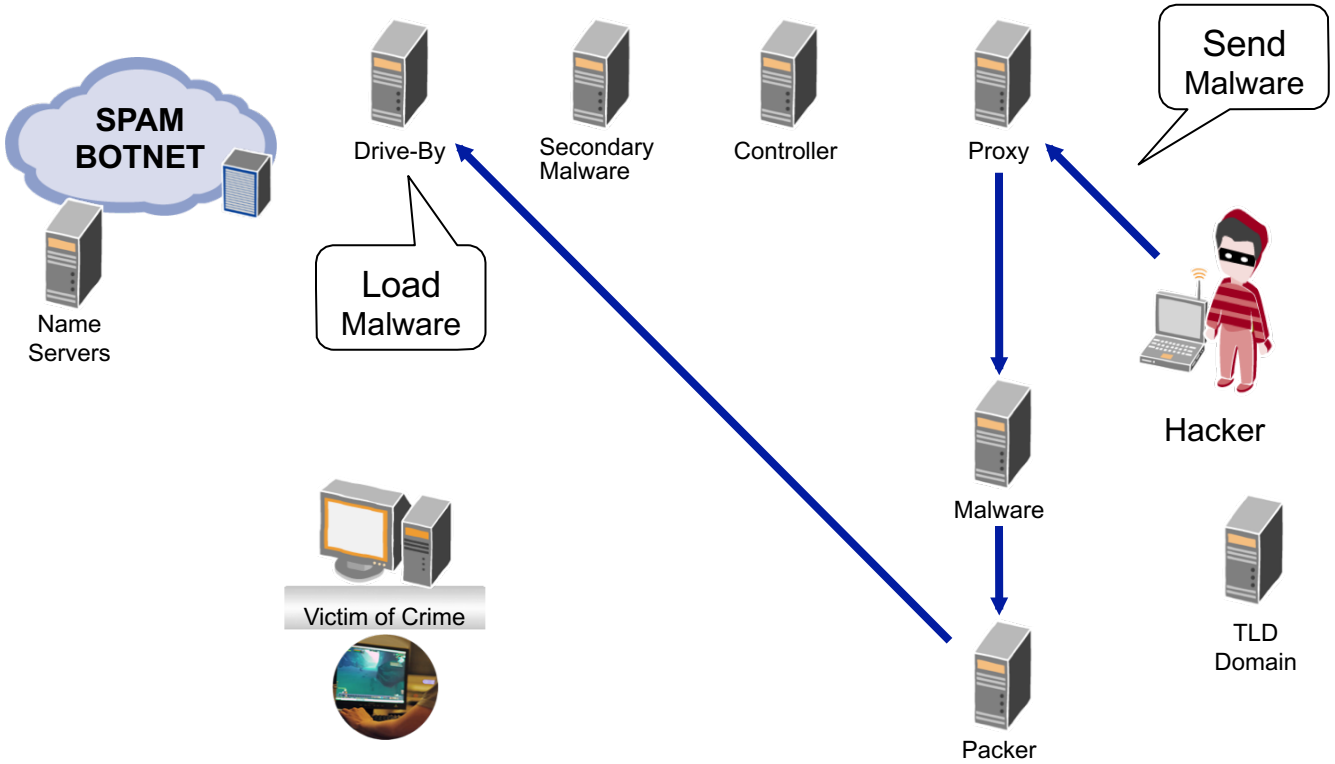

Packer


TLD Domain

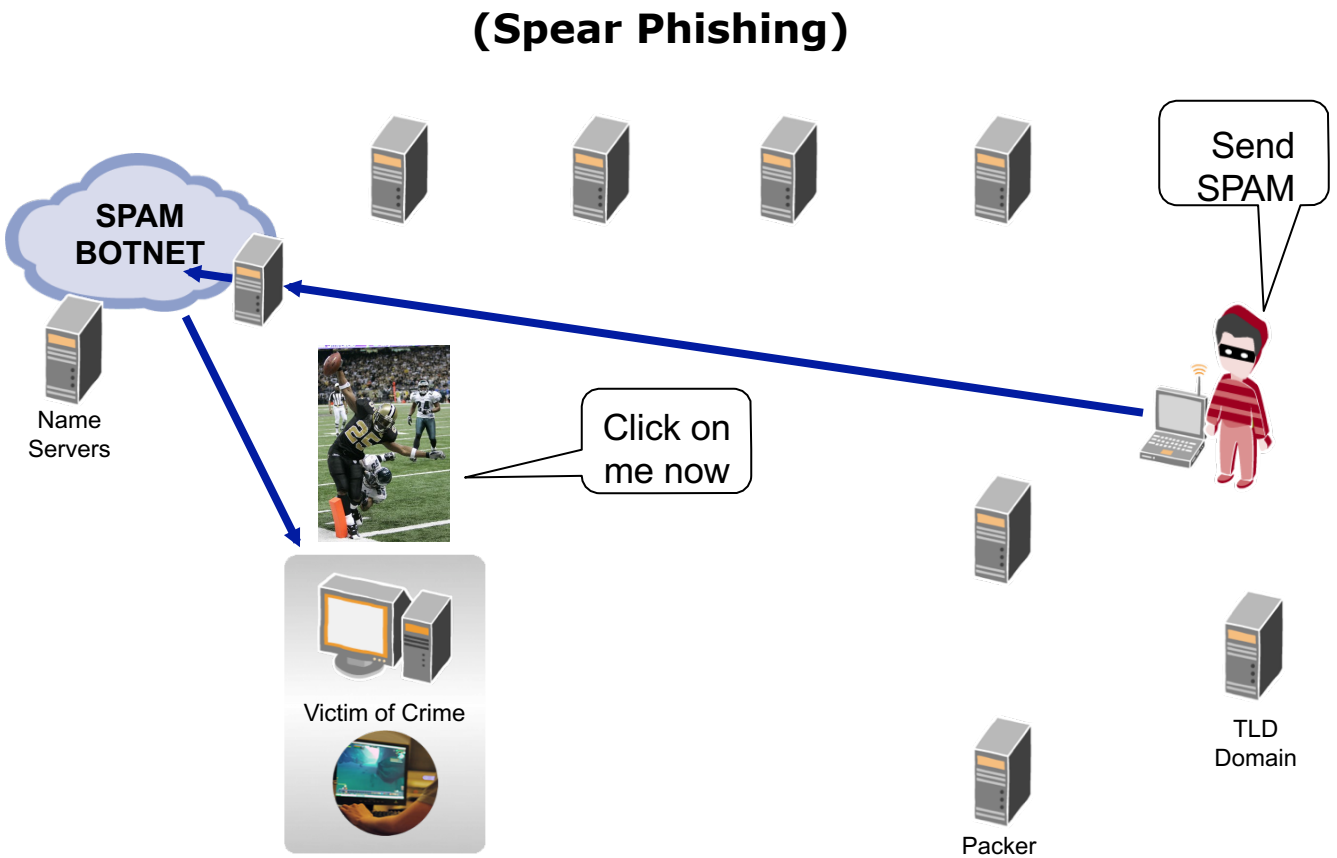
Stage Domain Name



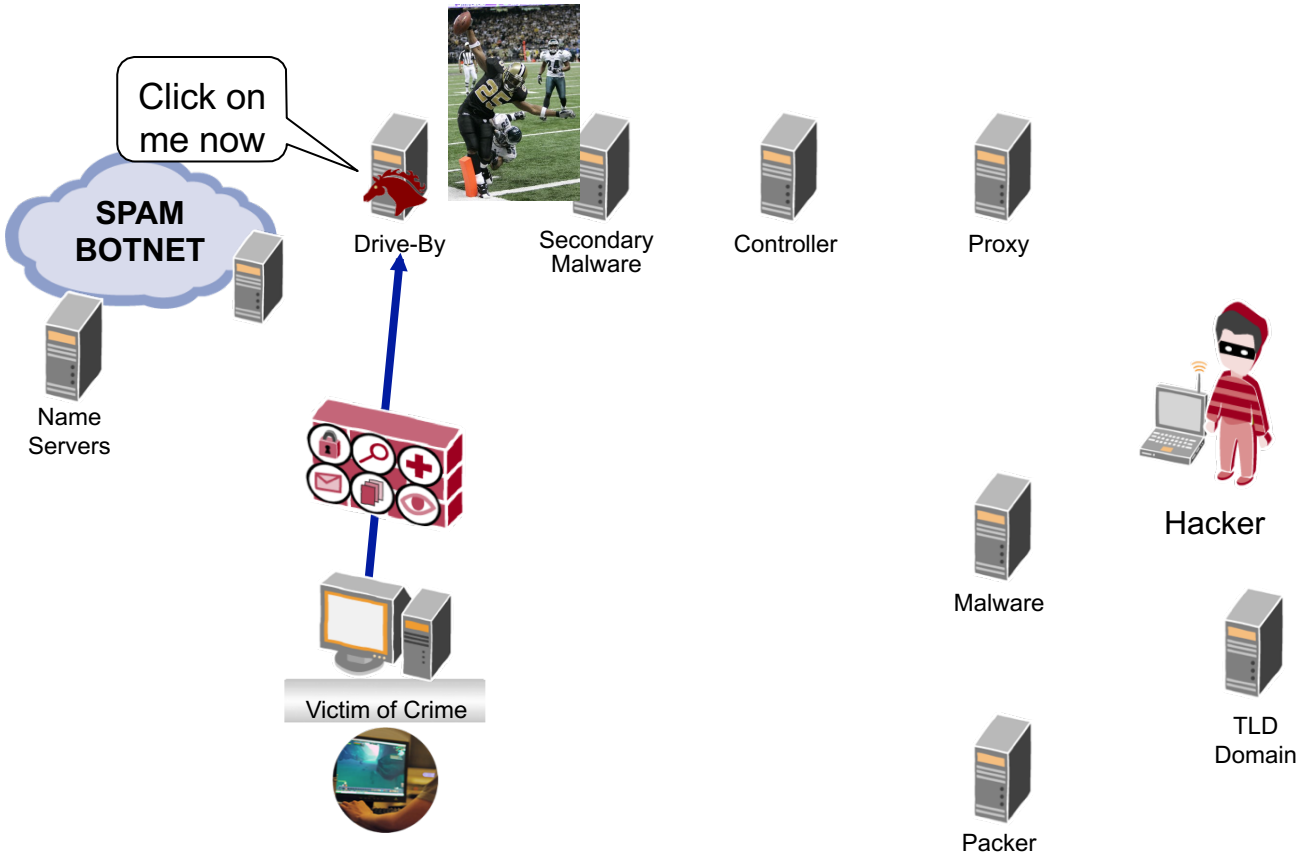
Prepare Drive-By



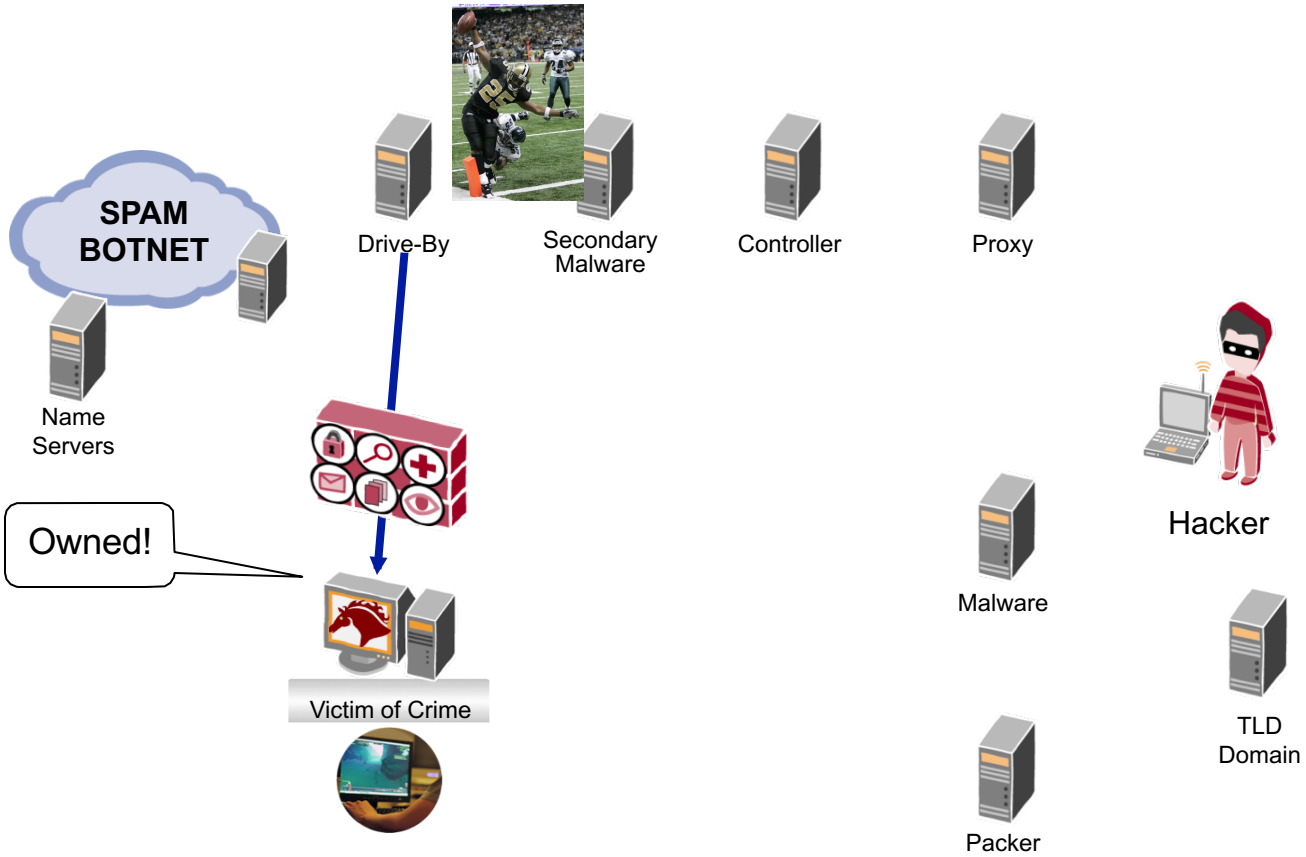
Social Engineered SPAM to Get People to Click



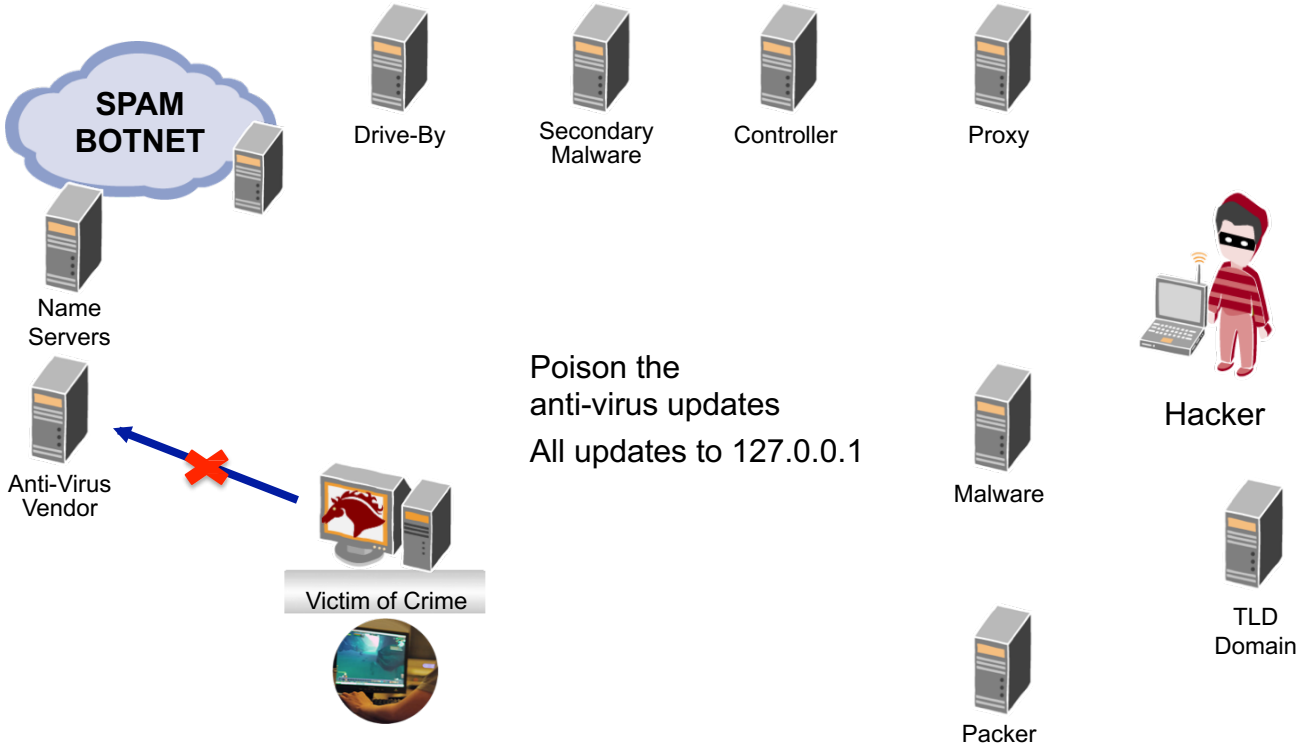
Drive-By Violation



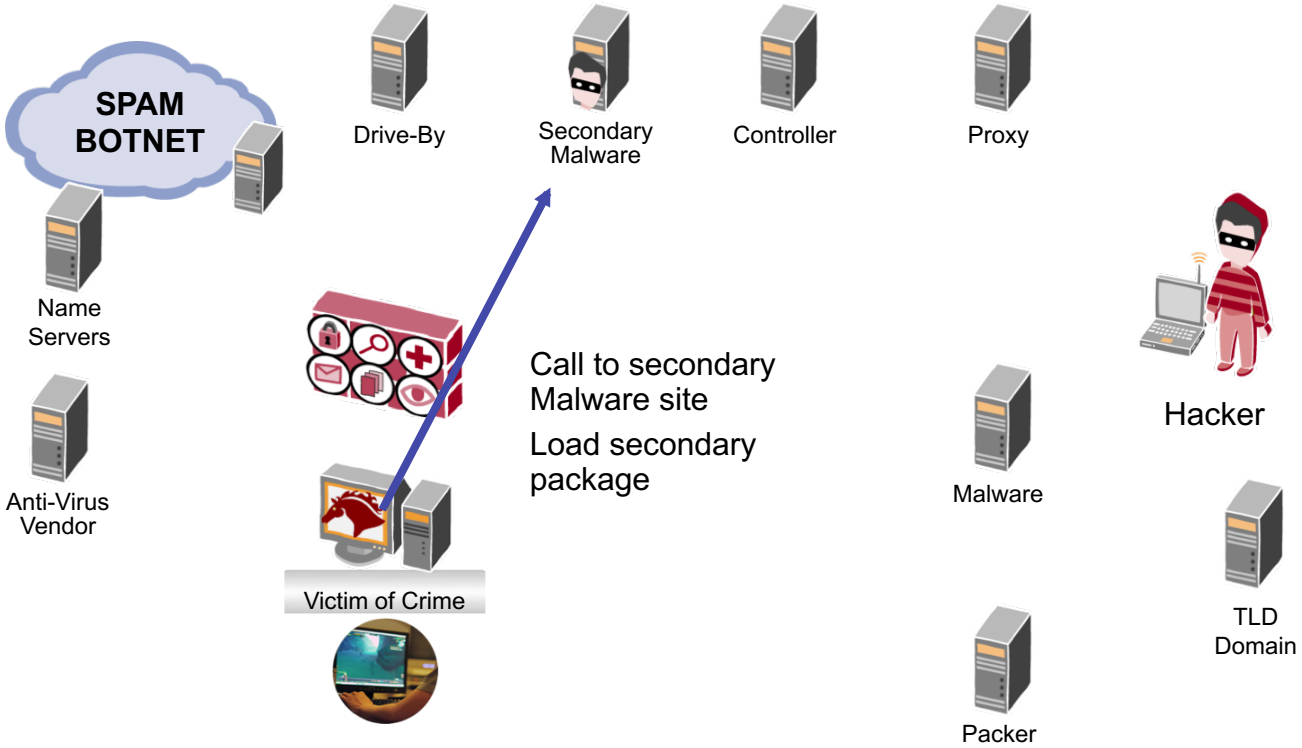
Drive-By Violation



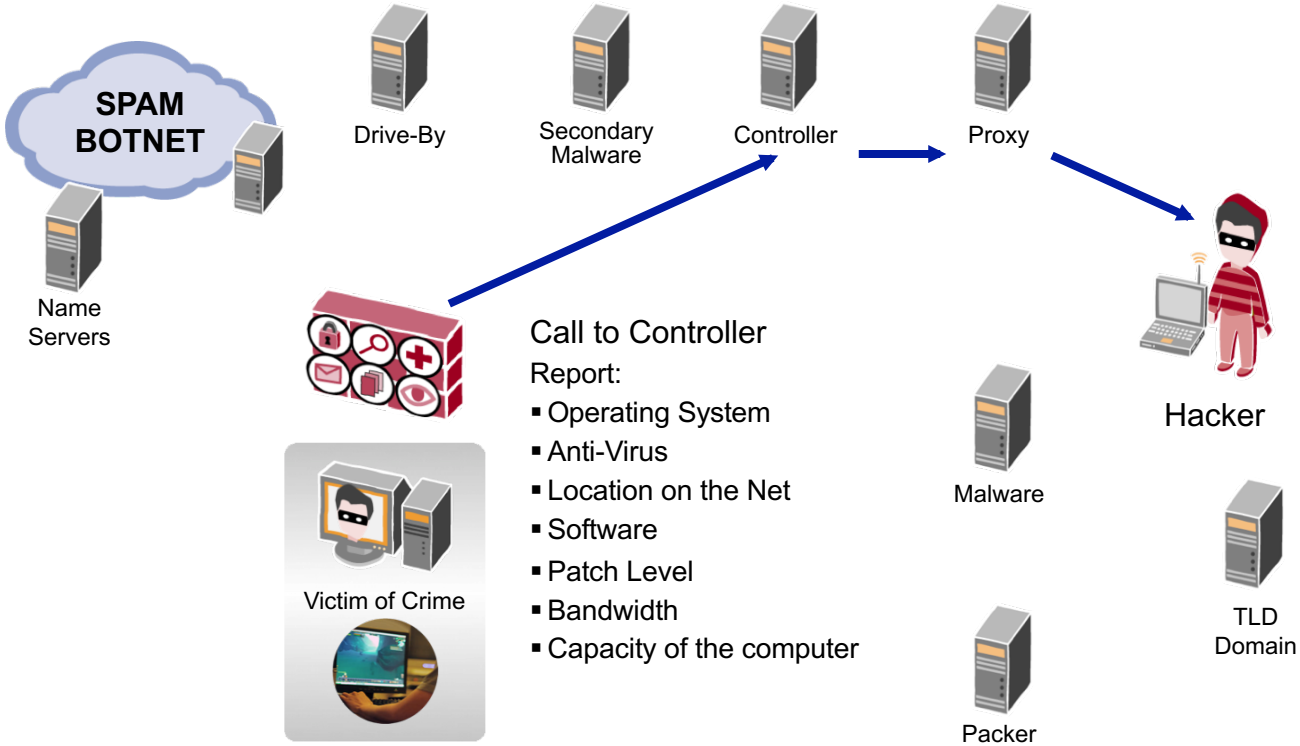
Poison Anti-Virus Updates



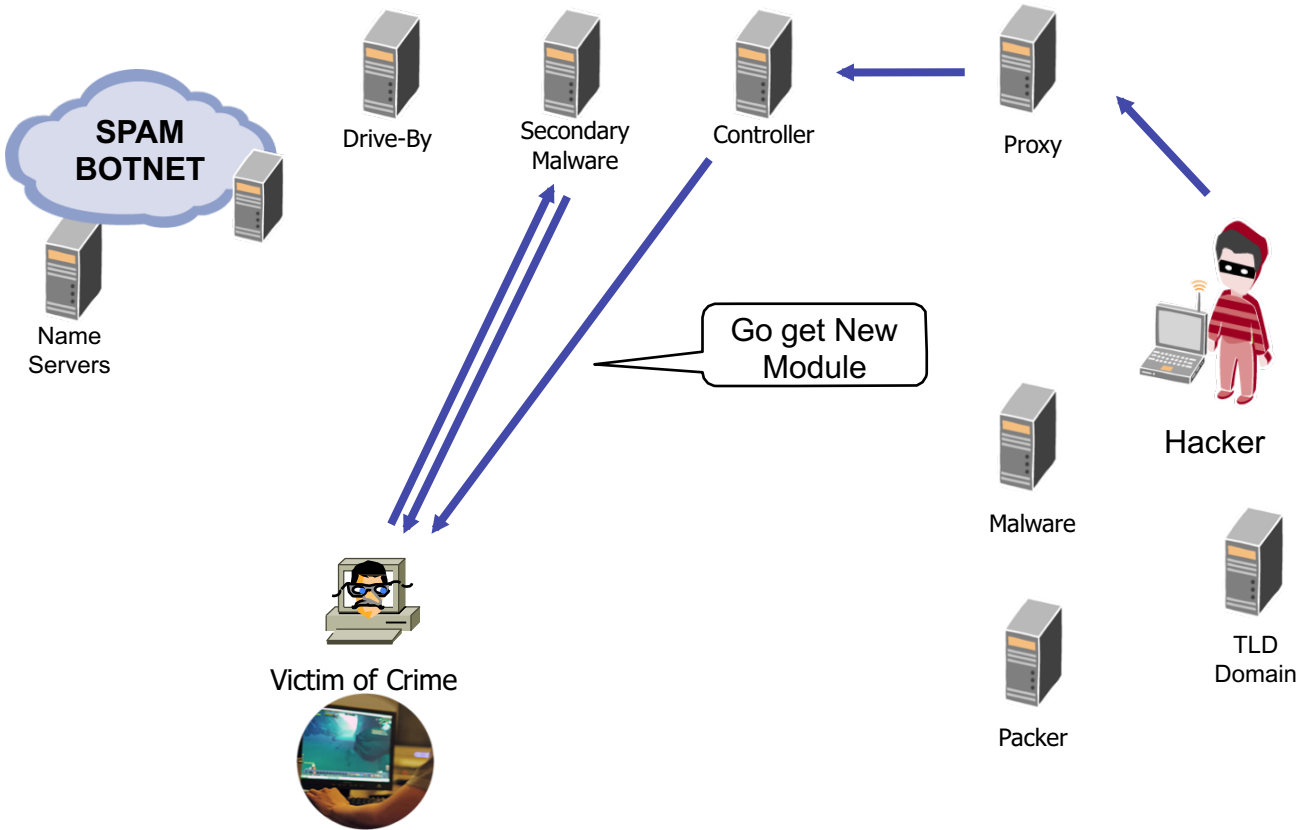
Prepare Violated Computer



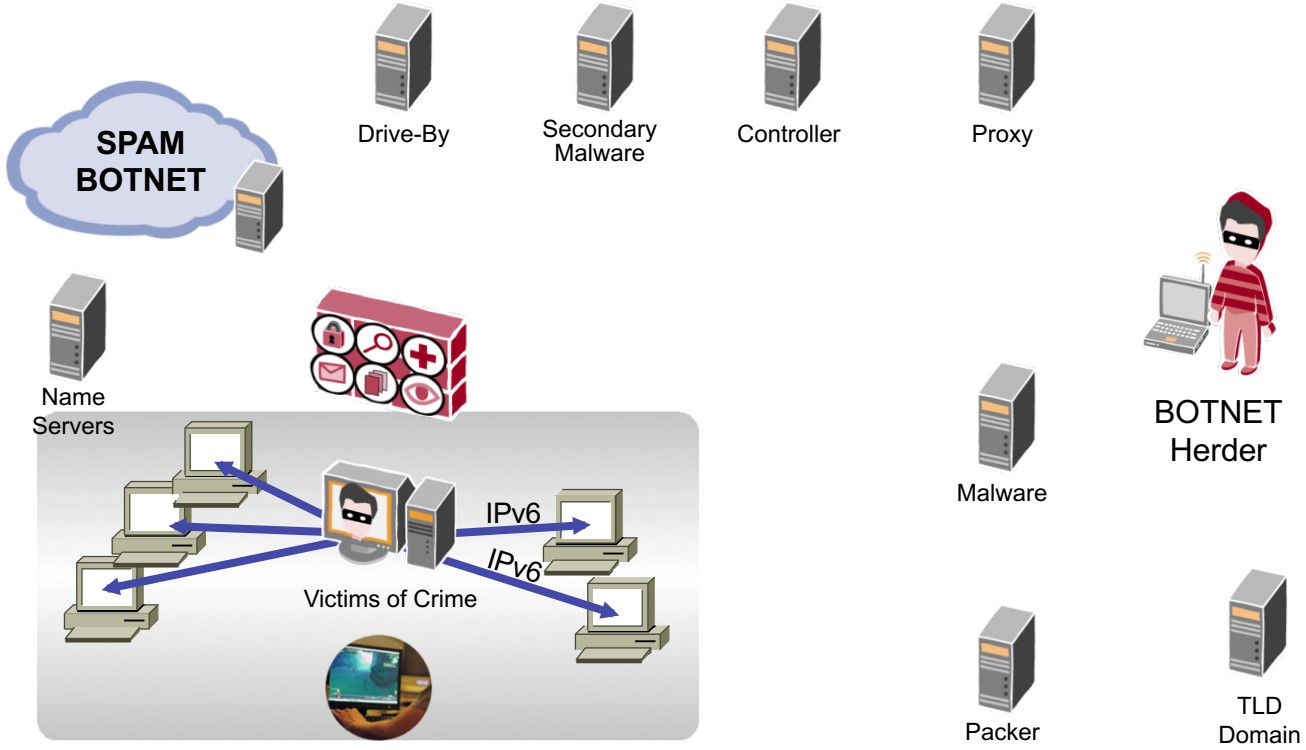
Call Home


SPAM
BOTNET
Name
Servers
Drive-By
Secondary
Malware
Controller
Proxy
Hacker
Victim of Crime
Call to Controller
Report:
▪ Operating System
▪ Anti-Virus
▪ Location on the Net
▪ Software
▪ Patch Level
▪ Bandwidth
▪ Capacity of the computer
Malware
Packer
TLD
Domain

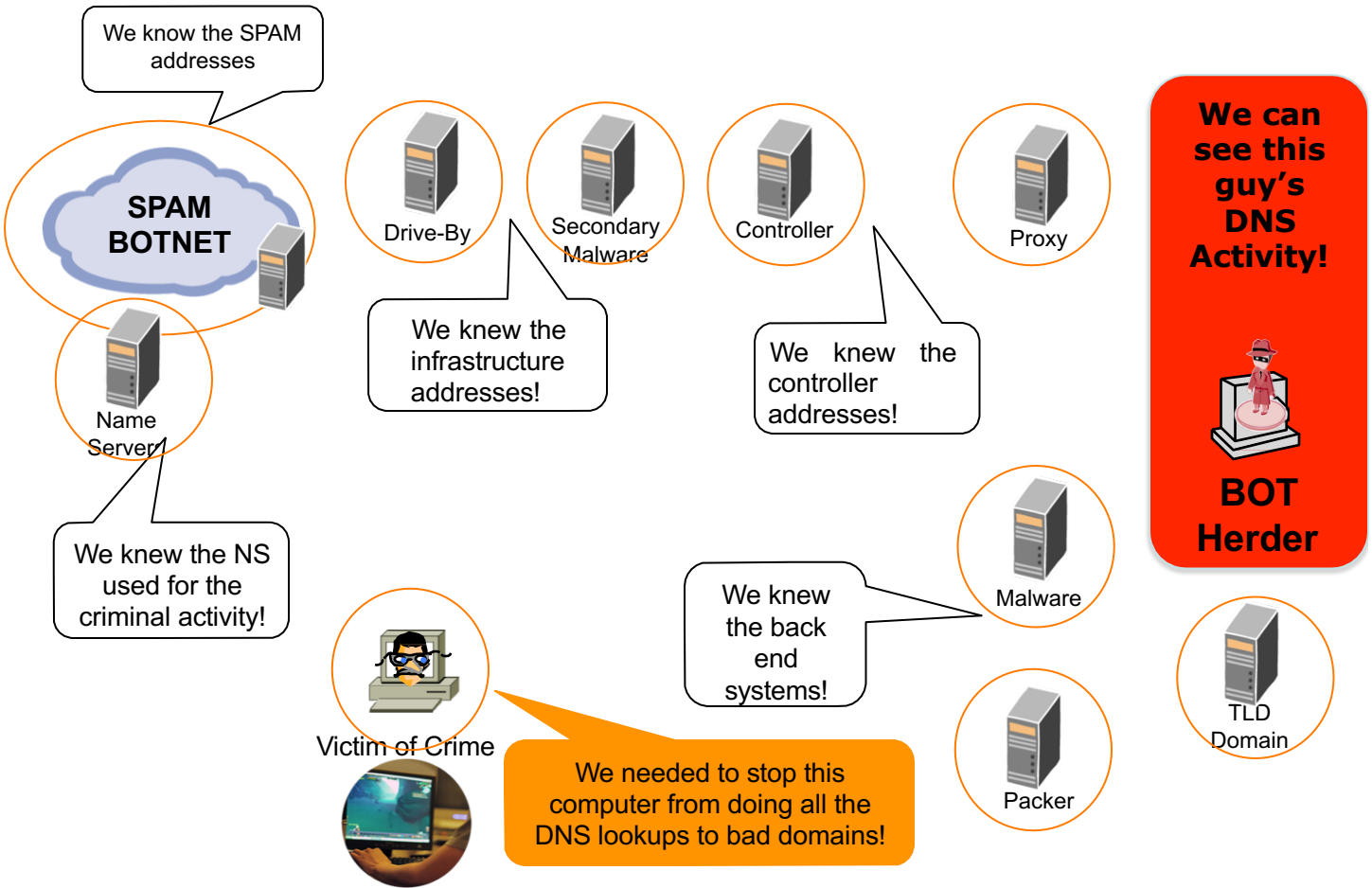
Load Custom Malware



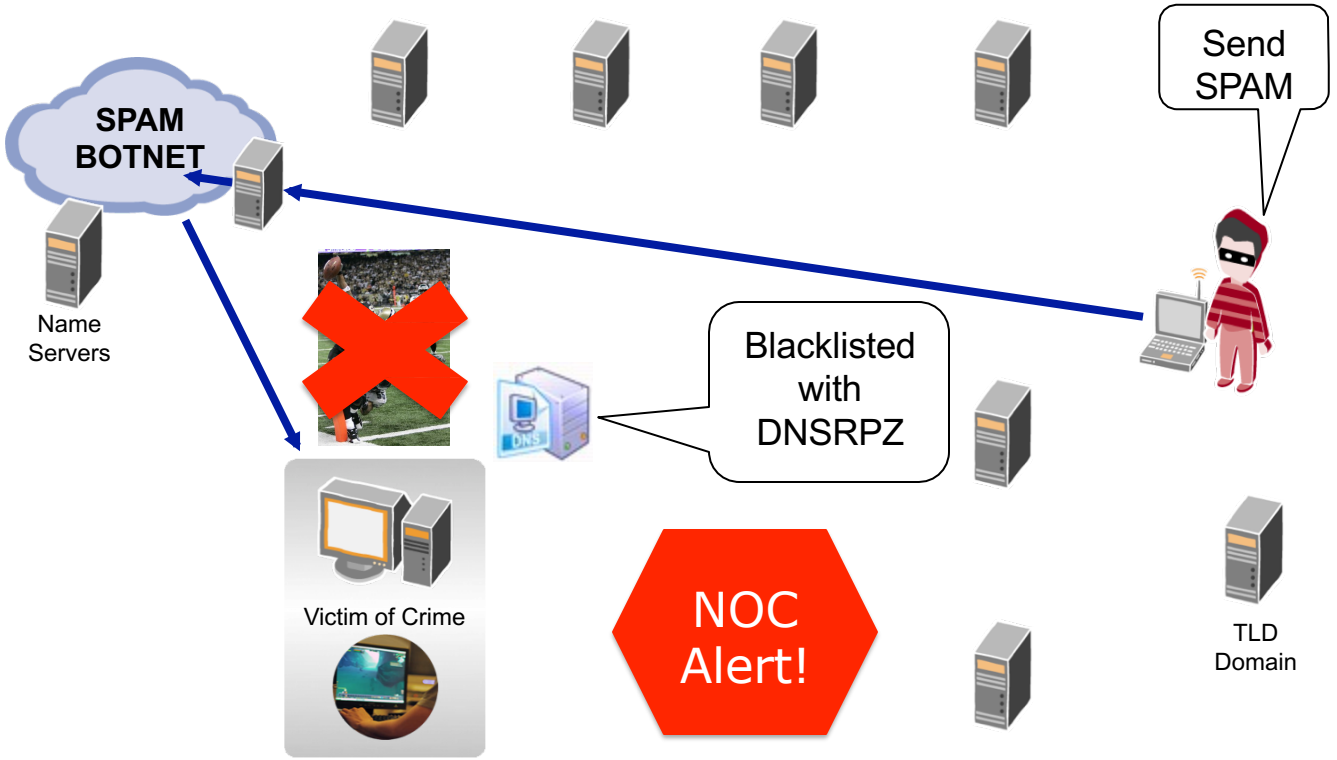
Start Worming, Scanning, & Spreading



The Domain names were Black **Listed!**



DNS RPZ would have stopped this attack!



Possible Uses Examples

- Enterprise networks can us it to stop infections – and let NOC know something is wrong.
- Hosting Provider can use it to block infected customer host – and let NOC know something is wrong.
- Service Providers – can use it to protect customers AND notify customer AND let the help desk know customers might be infected.

RPZ supported DNS Applications

RPZ is native in several of the industry's leading DNS platforms, including:

- BIND V9.9 (or greater)
- Power DNS

Numerous appliance vendors have enabled RPZ as well, including:

- Infoblox
- Efficient IP
- BlueCat

RPZ Rule

Let’s say we want to rewrite any DNS queries for a specific hostname, but allow lookups to the domain and other hosts in that domain:
host.filter.com IN CNAME .

This result in an NXDOMAIN (Non existence) response for a query for “host.filter.com”

Response Policy Triggers

The rules in a Response Policy Zone consist of triggers or filters that identify what responses to modify, and policy actions to apply to these responses. Each rule can use one of five policy triggers and specify one of eight policy actions.

- by the query name. [QNAME]
- by an address which would be present in a truthful response. [RPZ-IP]
- by the name or address of an authoritative name server responsible for publishing the original response. [RPZ-NSDNAME and RPZ-NSIP]
- by the IP address of the DNS client [RPZ-CLIENT-IP]

Response Policy Actions

- to synthesize a “domain does not exist” response. [NXDOMAIN]
- to synthesize a “name exists but there are no records of the requested type” response. [NODATA]
- to redirect the user via a CNAME to a walled garden [CNAME example.org
- to replace the response with specified data. [Local Data]
- to require the client to re-submit the query via TCP [CNAME rpz-tcp-only]
- to exempt the response from further policy processing. [DISABLED, CNAME rpz-passthru]
- to drop the query, without any response to the client [CNAME rpz-drop]

RPZ Logging

Since we're running RPZ, we definitely want to log any RPZ rewrites. To do that, we need to set up two things under the "logging" header.

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

CONFIGURE A SLAVE RPZ ZONE

```
zone "drop.rpz.spamhaus.org" {
        type slave;
        file "dbx.drop.rpz.spamhaus.org";
        masters {
        X.X.X.X;
        X.X.X.X; };
        allow-transfer { none; };
        allow-query { localhost; }; };
```

Configuring Response Policy Zones

Bind currently has a 32 zone limit.
RPZ zones are specified in the response-policy section:

```
response-policy {
zone "rpz-local";
zone "tor-exit-nodes.local";
zone "bogon.rpz.spamhaus.org";
zone "botnetcc.rpz.spamhaus.org";
zone "malware.rpz.spamhaus.org";
zone "malware-adware.rpz.spamhaus.org";
zone "malware-aggressive.rpz.spamhaus.org";
zone "bad-nameservers.rpz.spamhaus.org";
zone "drop.rpz.spamhaus.org";
};
```

Before Implementation

- At first implement on logging mode for at least for a week
- Use TSIG to transfer the RPZ zone
- Restricted RPZ recursive server to use from all
- Restricted users from using other name servers

RPZ Feed Providers

- Spamhaus/Deteque/SecurityZone
- Farsight security
- SURBL
- SWITCH
- Threat Stop

Implementation Case Study in an ISP in BD

- Using RPZ feed from SecurityZone with Bind (http://www.securityzones.net/images/downloads/BIND_RPZ_Installation_Guide.pdf)
- Redirected all DNS recursive request to RPZ name server
- Provided service for 390 devices using recursive DNS
- Name server hits 23000000 in a month.
- Domain blocked 55435
- Number of infected device detected 32
- Simple and easy approach to implement

Thanks!

Any questions?