DNS Response Policy Zone (DNSRPZ)

BIND's New Security Feature: the "DNS Firewall"

Barry Raveendran Greene & Vernon Schryver

bgreene@isc.org

Version 1.1

Logistics

- This presentation can be downloaded from the Webinar recording and from ISC’s Knowledge Base: http://deepthought.isc.org
- ISC updates, presentations, and materials can be followed on:
  - Facebook - http://www.facebook.com/InternetSystemsConsortium
  - Twitter - ISCdotORG
  - Linkedin - http://www.linkedin.com/company/internet-systems-consortium
  - RSS via our Website

Our Goal – Take Back DNS

DNS works as well for the **bad guys** (criminals, spammers, spies) as for **respectable citizens.** The bad guys are taking better advantage of DNS's resiliency and distributed autonomy.

Something has got to be done!

ISC is acting:

- Act I – Massive Passive DNS Deployment
- Act II - DNSRPZ

Agenda

- The DNSRPZ Quick Talk
- Why do we need DNSRPZ?
- More Details
- DNSRPZ Providers

Gratitude

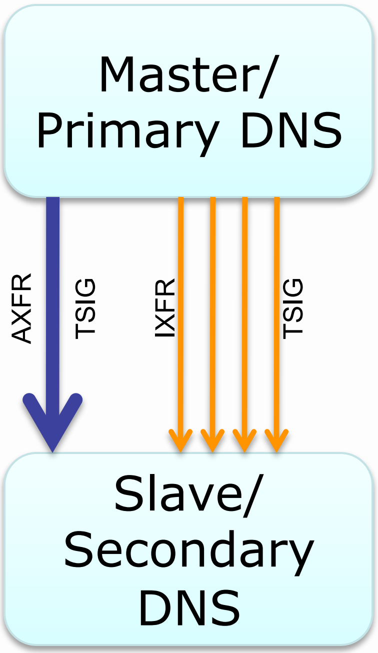
- Paul Vixie and Vernon Schryver for all the heavy lifting to make DNSRPZ happen.
- ISC's BIND Engineering Team – for integrating this new feature so quickly.
- Eric Ziegast - my partner in explaining DNSRPZ to people.
- For the new DNSRPZ Providers:
  - Simon Forster forster@spamteq.com
  - Arnie Bjorklund arnieb@securityzones.net
  - Rod Rasmussen rod.rasmussen@internetidentity.com
- Johanna Mansor who helped put this together so quickly.

DNSRPZ Quick Talk

DNS Response Policy Zone (DNS RPZ)

- DNS RPZ is *policy information* inside a specially constructed DNS zone.
- This enables DNS reputation data producers and consumers to cooperate in the application of such policy to real time DNS responses.
- DNS RPZ turns the *recursive DNS server* into a security hammer …
  - ➢ Provide the same capabilities of an anti-spam DNSBL (DNS Block List, ne RBL) and RHSBL (Right Hand Side Block List)….
  - ➢ … with greater degrees of scaling and speed.

Core DNS Principles



Master/ Primary DNS

AXFR

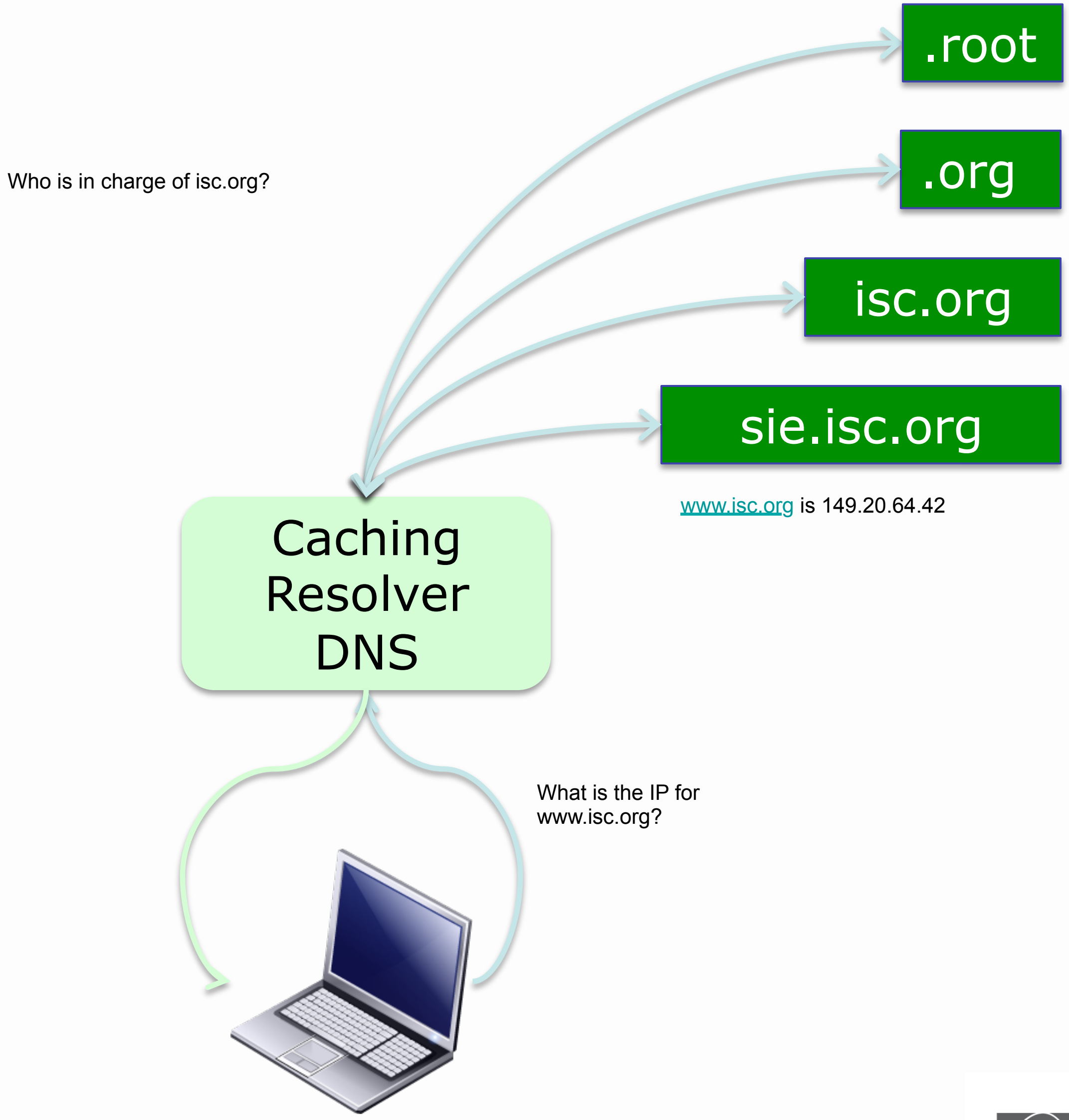
TSIG

IXFR

TSIG

Slave/ Secondary DNS

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



Who is in charge of isc.org?

.root

.org

isc.org

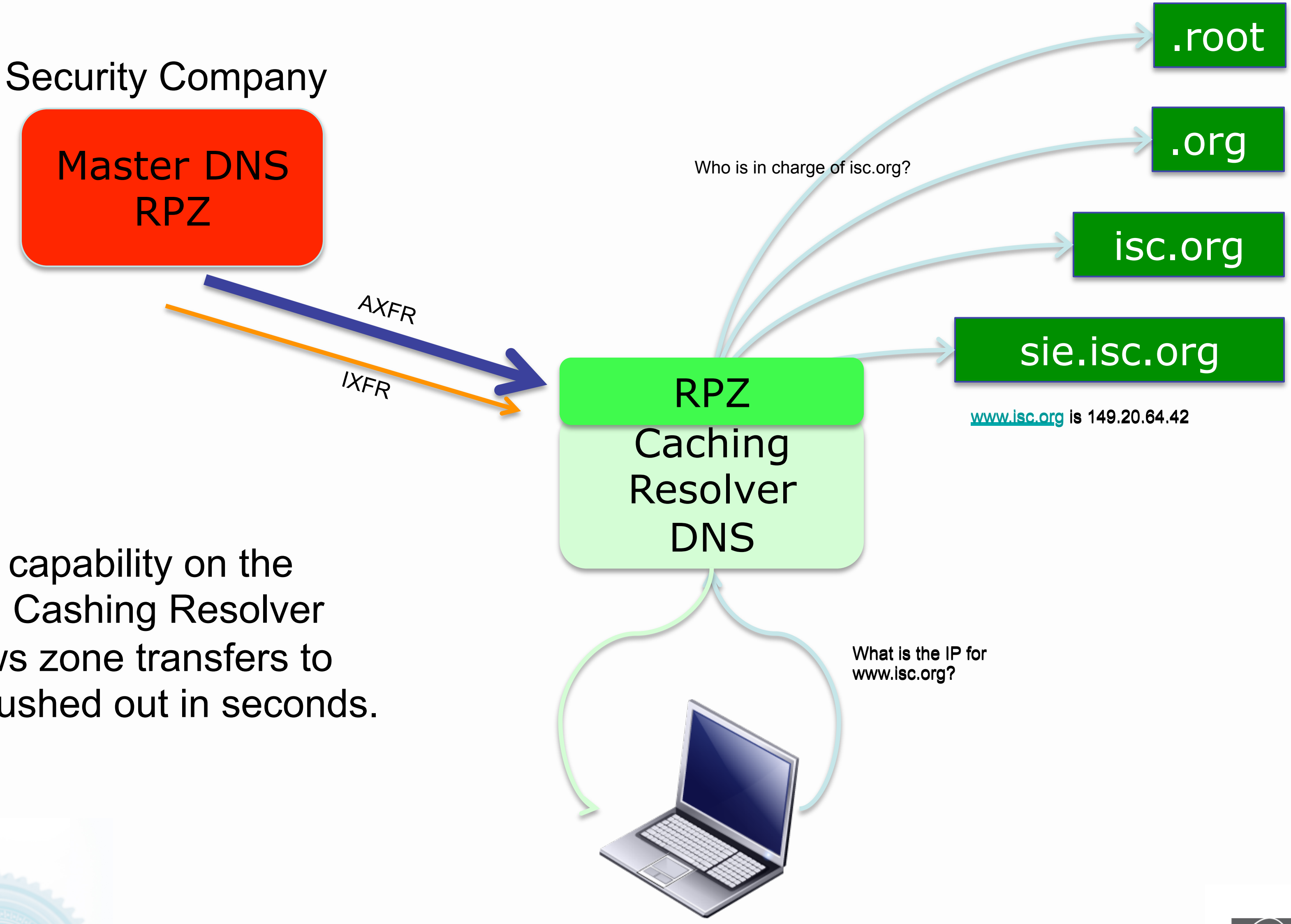
sie.isc.org

www.isc.org is 149.20.64.42

Caching Resolver DNS

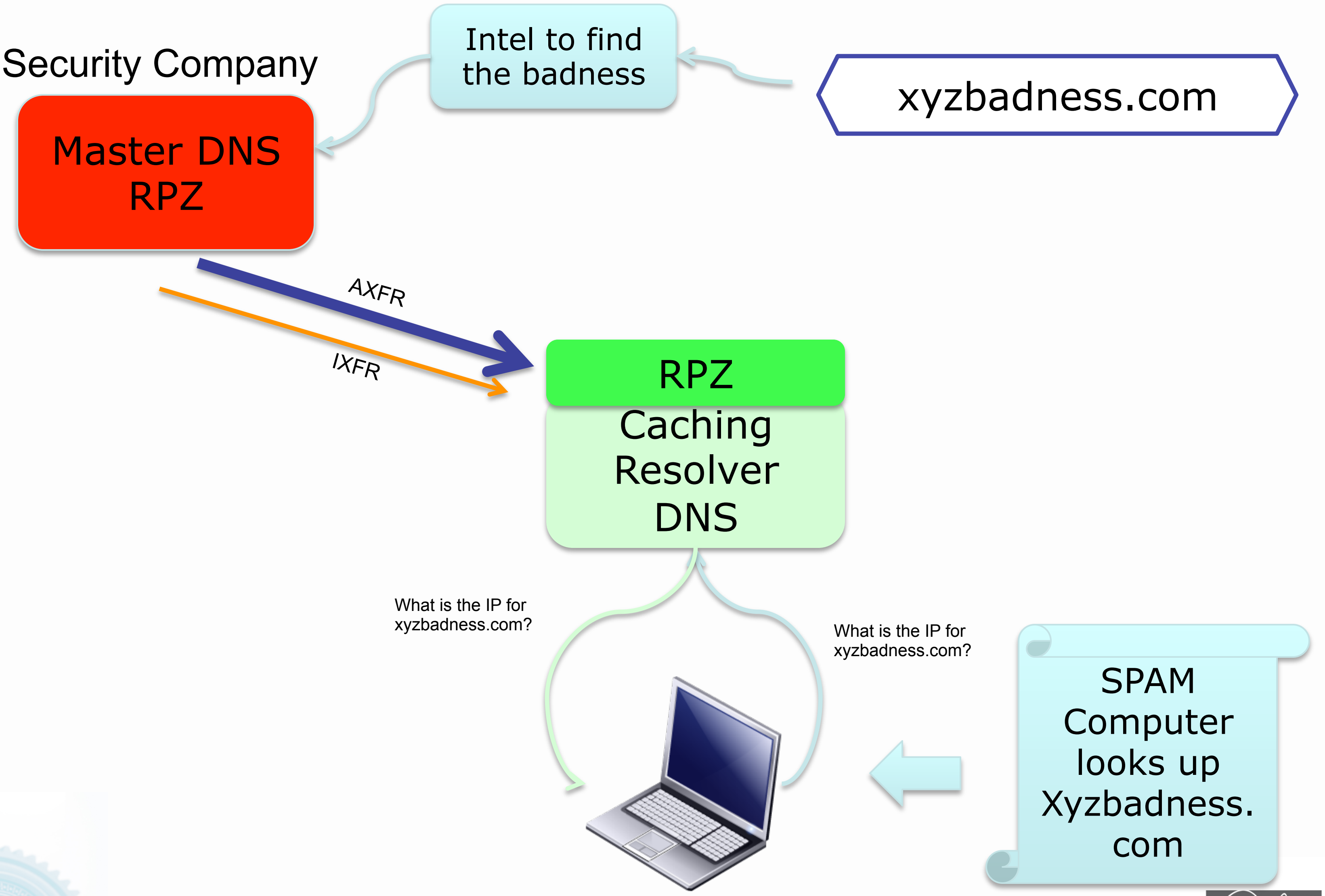
What is the IP for
www.isc.org?

DNS RPZ



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

DNS RPZ in Action



Security Company

Master DNS RPZ

Intel to find the badness

xyzbadness.com

AXFR

IXFR

RPZ

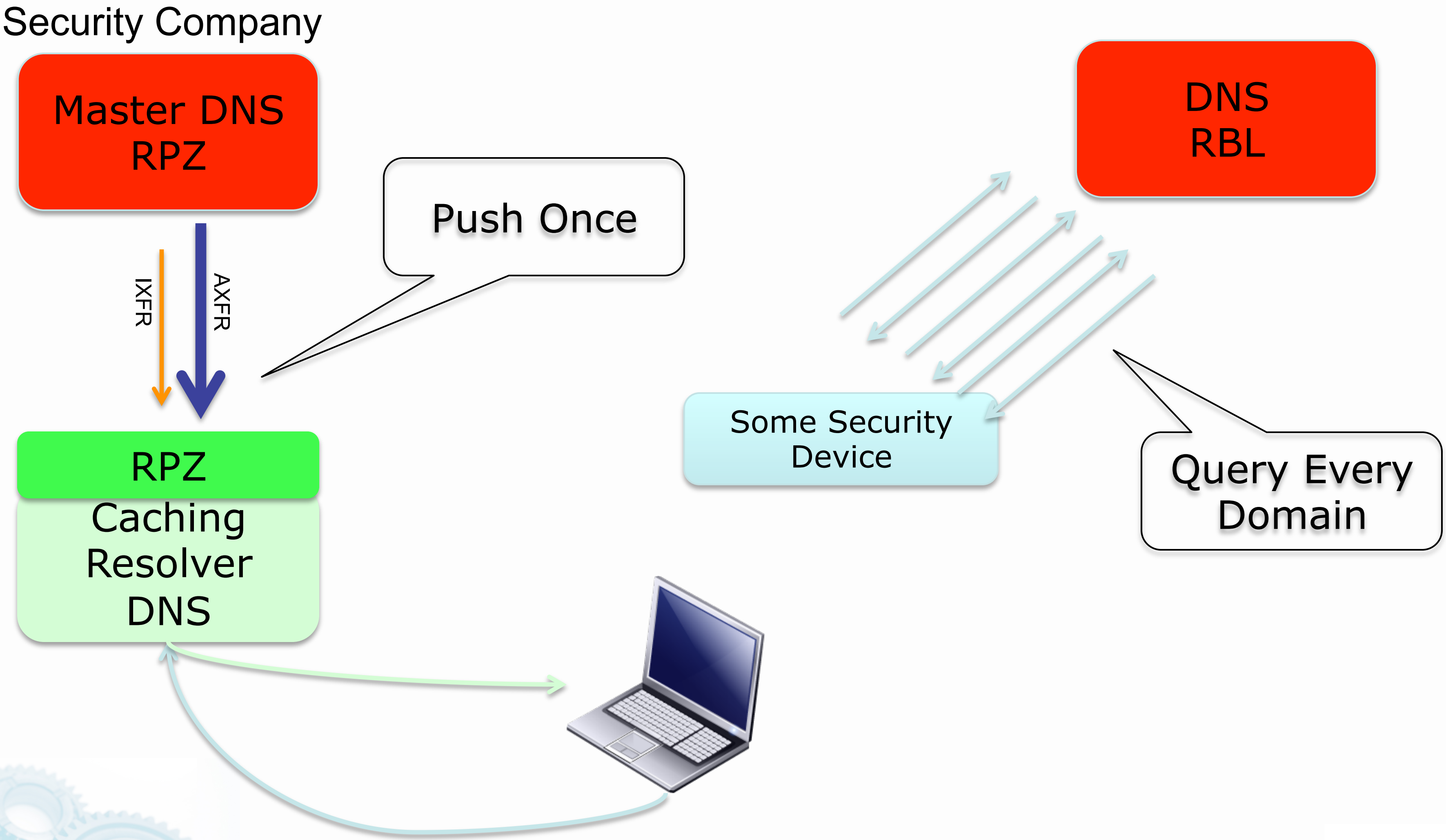
Caching Resolver DNS

What is the IP for xyzbadness.com?

What is the IP for xyzbadness.com?

SPAM Computer looks up Xyzbadness. com

How is DNSRPZ Different?



Security Company

Master DNS
RPZ

IXFR

AXFR

Push Once

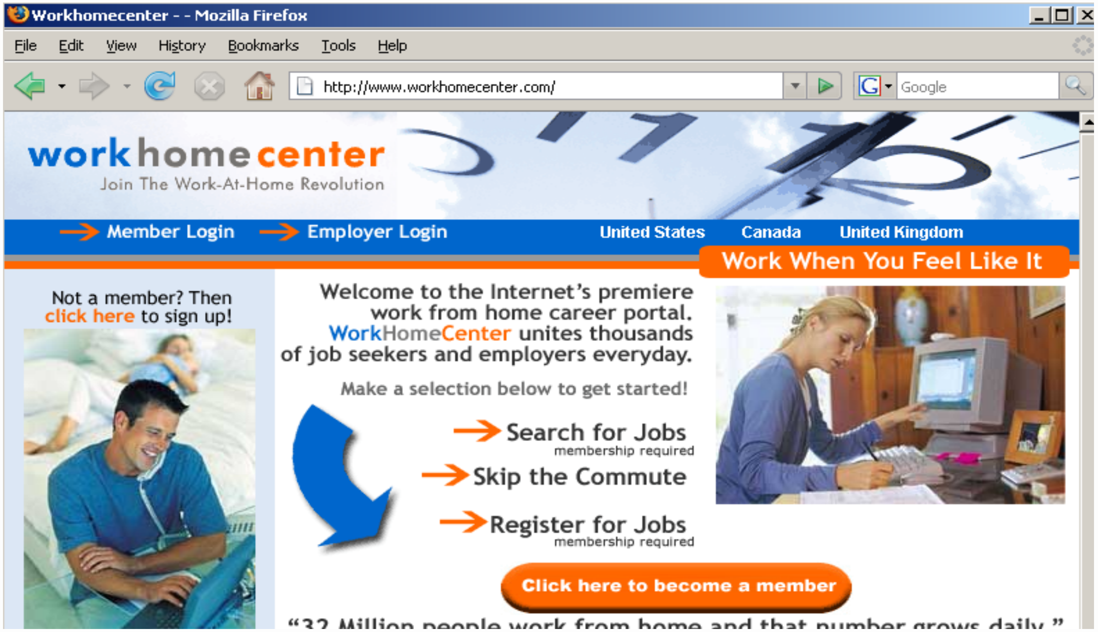
RPZ
Caching
Resolver
DNS

DNS
RBL

Some Security
Device

Query Every
Domain

Demo - before


Workhomecenter - - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.workhomecenter.com/
Google
work home center
Join The Work-At-Home Revolution
Member Login
Employer Login
United States
Canada
United Kingdom
Work When You Feel Like It
Search for Jobs
membership required
Skip the Commute
Register for Jobs
membership required
Click here to become a member

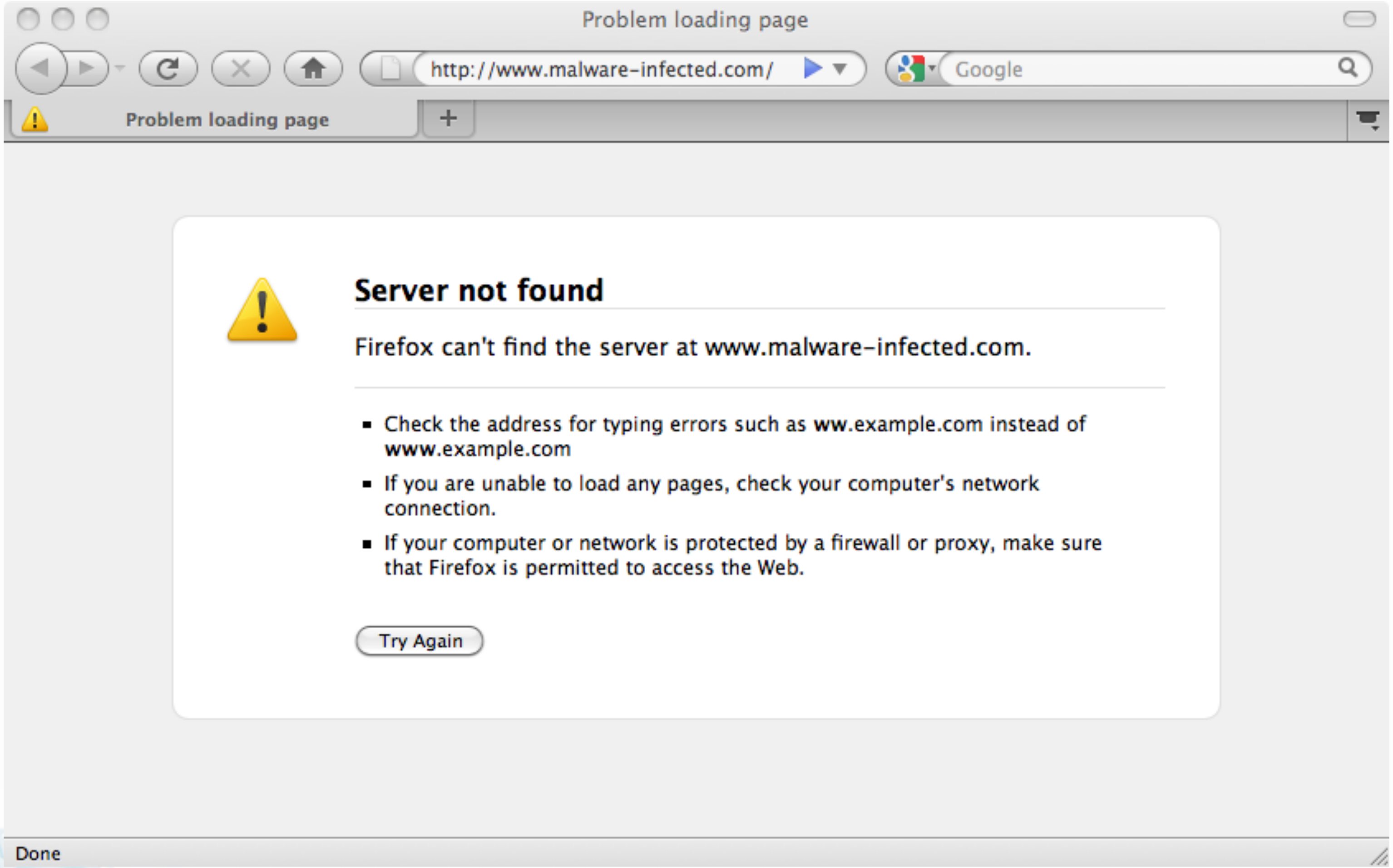
Not a member? Then click here to sign up!

Welcome to the Internet's premiere work from home career portal. WorkHomeCenter unites thousands of job seekers and employers everyday.

Make a selection below to get started!

"32 Million people work from home and that number grows daily."

Demo - after

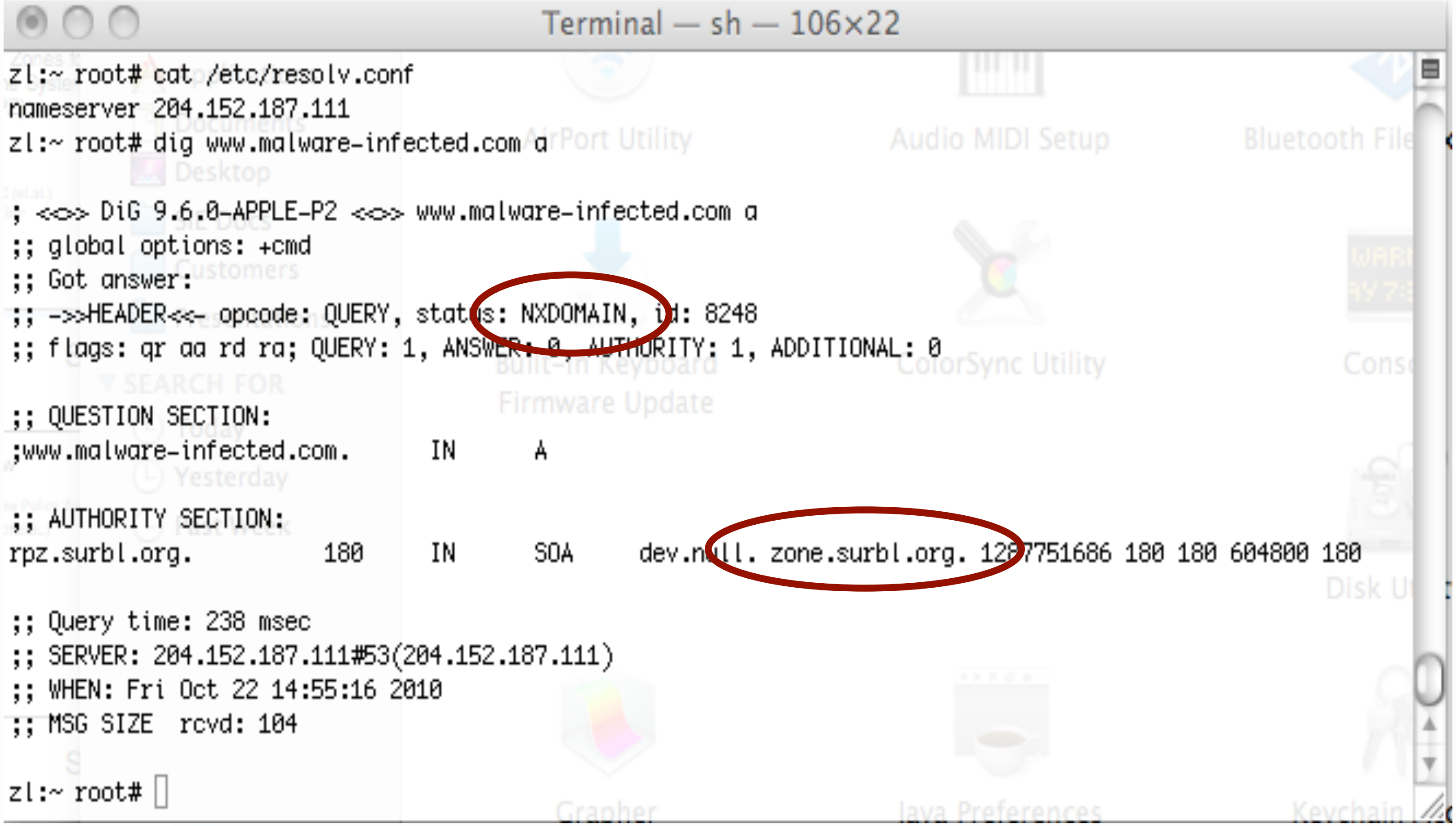


Server not found

Firefox can't find the server at www.malware-infected.com.

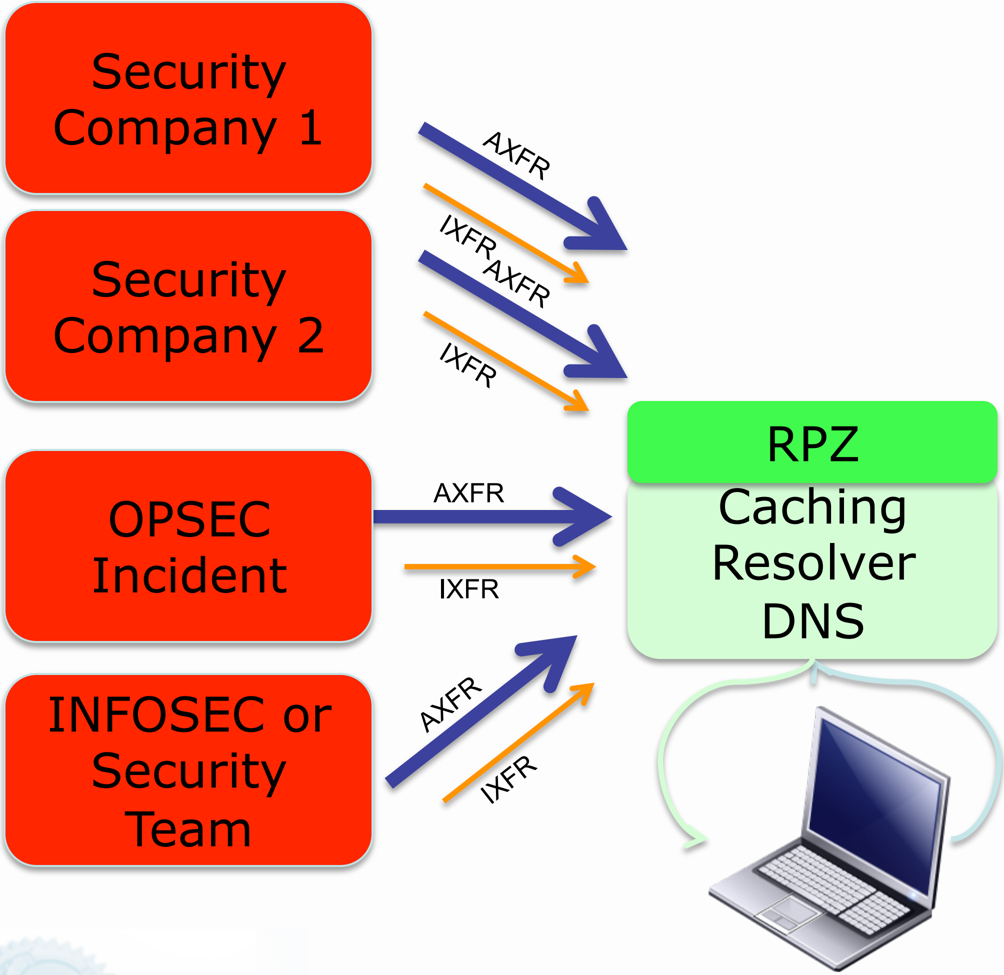
- Check the address for typing errors such as **ww**.example.com instead of **www**.example.com
- If you are unable to load any pages, check your computer's network connection.
- If your computer or network is protected by a firewall or proxy, make sure that Firefox is permitted to access the Web.

What it looks like



```
zl:~ root# cat /etc/resolv.conf
nameserver 204.152.187.111
zl:~ root# dig www.malware-infected.com a

; <<>> DiG 9.6.0-APPLE-P2 <<>> www.malware-infected.com a
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 8248
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;www.malware-infected.com.      IN      A

;; AUTHORITY SECTION:
rpz.surbl.org.          180     IN      SOA     dev.null. zone.surbl.org. 1287751686 180 180 604800 180

;; Query time: 238 msec
;; SERVER: 204.152.187.111#53(204.152.187.111)
;; WHEN: Fri Oct 22 14:55:16 2010
;; MSG SIZE  rcvd: 104

zl:~ root# 
```

How is DNSRPZ Different?



Security Company 1

Security Company 2

OPSEC Incident

INFOSEC or Security Team

RPZ

Caching Resolver DNS

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

IID

SURBL

THE SPAMHAUS PROJECT

Possible DNS RPZ Uses

- Block or redirect **malicious drop sites** (DNS used by URLs)
- Block ability of **C&C** to find its way back using DNS
- *Walled garden notification* for infected clients
- Services that use PTR lookups (IP reputation can map into here).

Possible Uses Examples

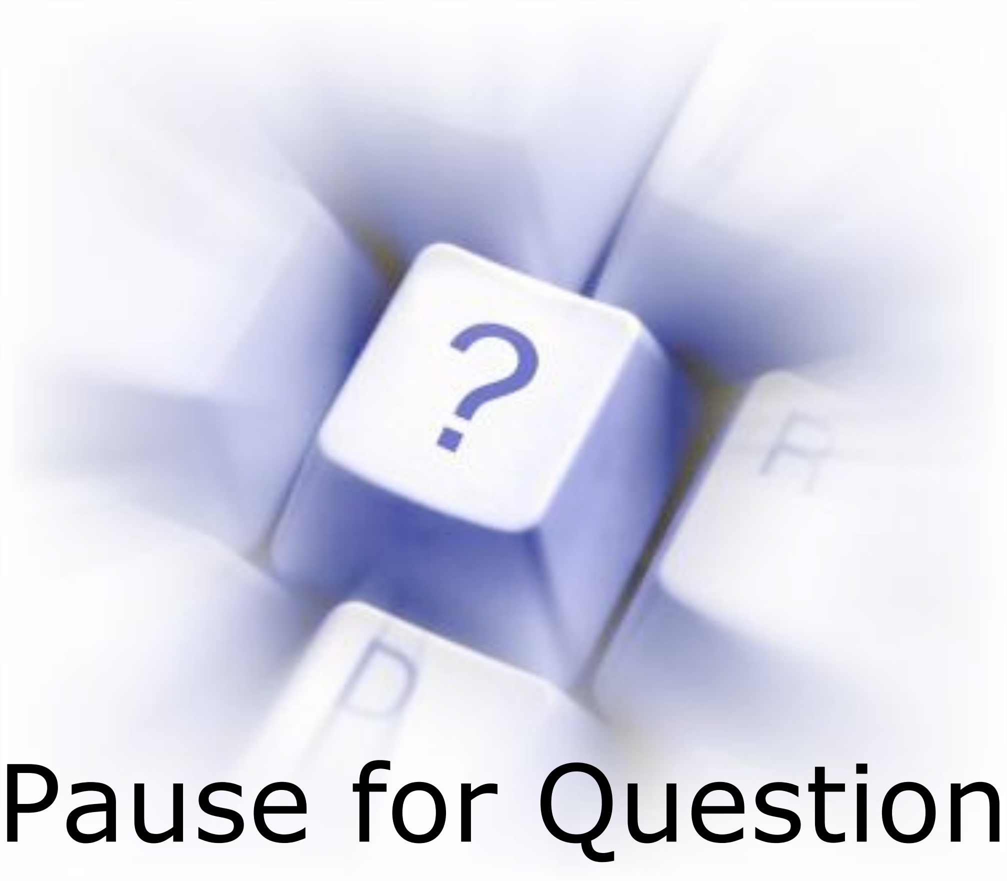
- Enterprise networks can us it to stop infections – and let NOC know something is wrong.
- Hosting Provider can use it to block infected customer host – and let NOC know something is wrong.
- Service Providers – can use it to protect customers AND notify customer AND let the help desk know customers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

DNSRPZ Getting the Word out

- There was a healthy amount of pre-announced to operational security community to build a ecosystem.
- With BIND 9.8.1, we have a solid version for operators and networks to migrate and try DNSRPZ.
- ISC's role is to now get the word out. The next wave of deployments would determine the utility of this security widget.

ISC's Role with DNS RPZ

- ISC has three roles with DNS RPZ as a new "hammer" in our security toolkit:
  - Code and Functionality in BIND & working with all DNS Recursive Resolver Software Vendors to insure everyone is adopting the same formats.
  - Work with all potential Black List Providers.
  - Work with Operators on DNS RPZ Deployment.
- ISC will NOT be providing any black list capacities. Our role is to help design, build, and deploy the "hammer" as a new tool in our security toolkit.



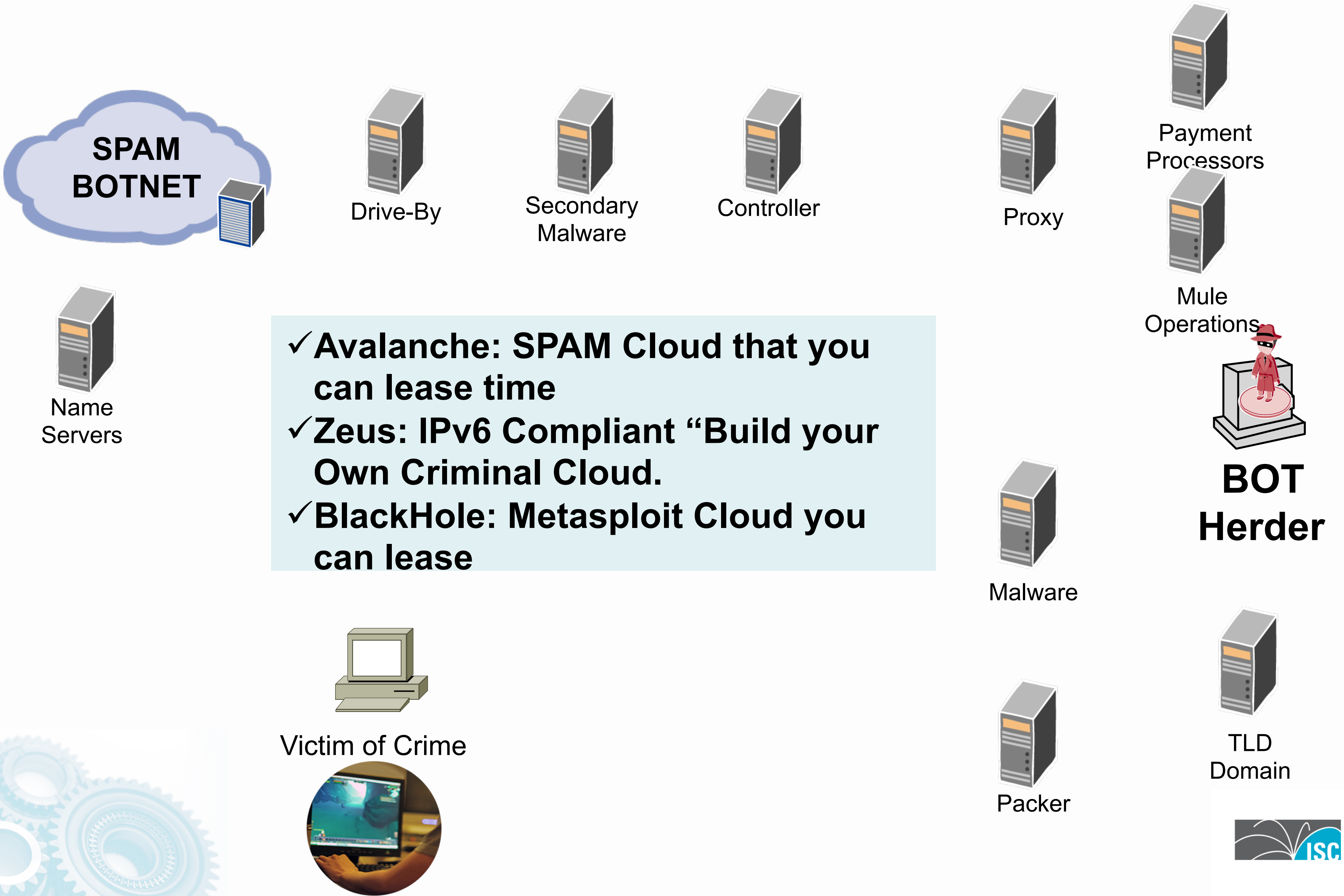
Pause for Questions

Links while you are thinking …

- Discussion List
  - https://lists.isc.org/mailman/listinfo/dnsrpz-interest
- Taking back the DNS, Paul Vixie, 29th July 2010
  - http://www.isc.org/community/blog/201007/taking-back-dns-0
- Google "taking back the dns"
- Draft Specification
  - ftp://ftp.isc.org/isc/dnsrpz/isc-tn-2010-1.txt
- BIND 9.8.1
  - ftp://ftp.isc.org/isc/bind9/9.8.1/

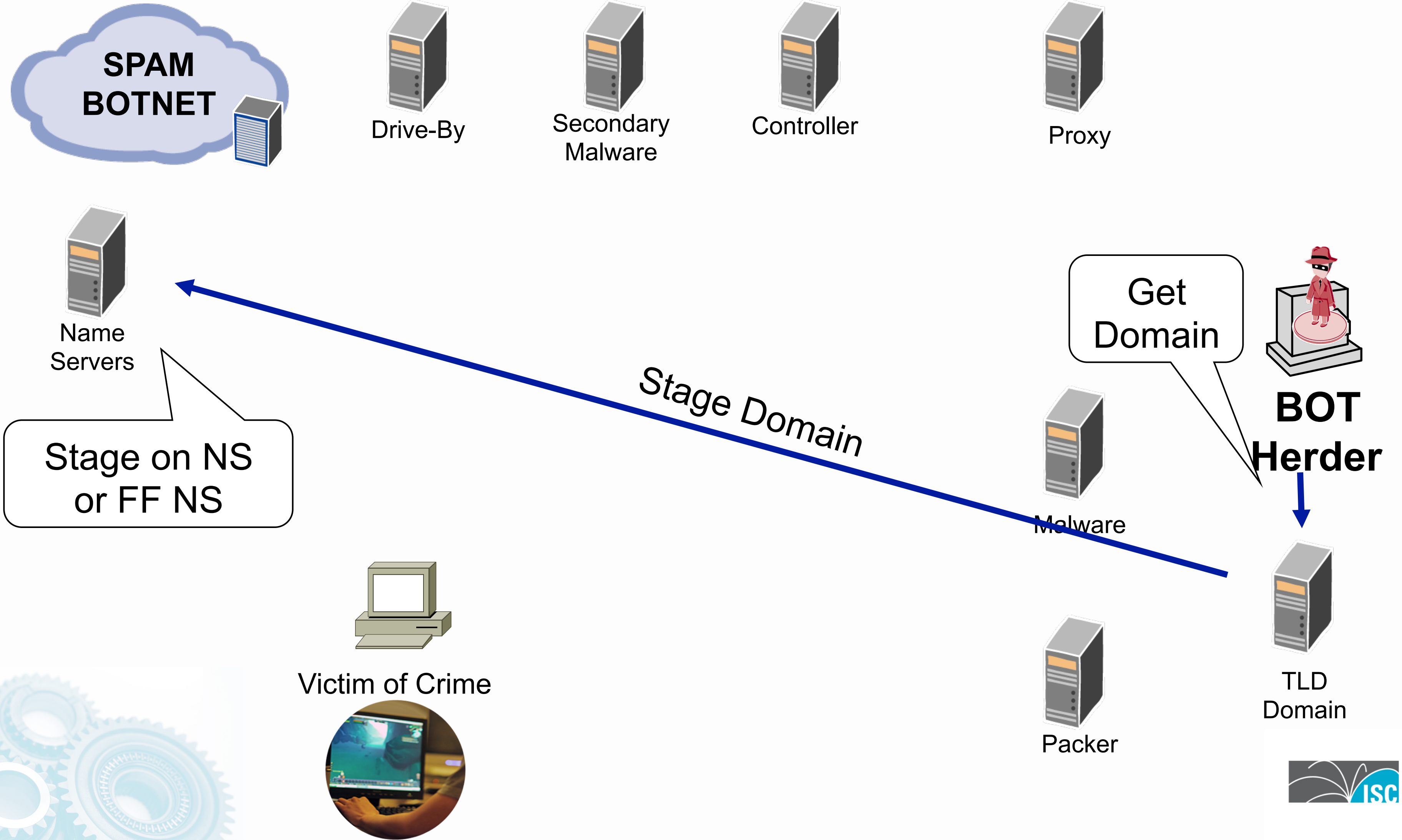
Why We Need DNSRPZ?

Components of the Criminal Cloud

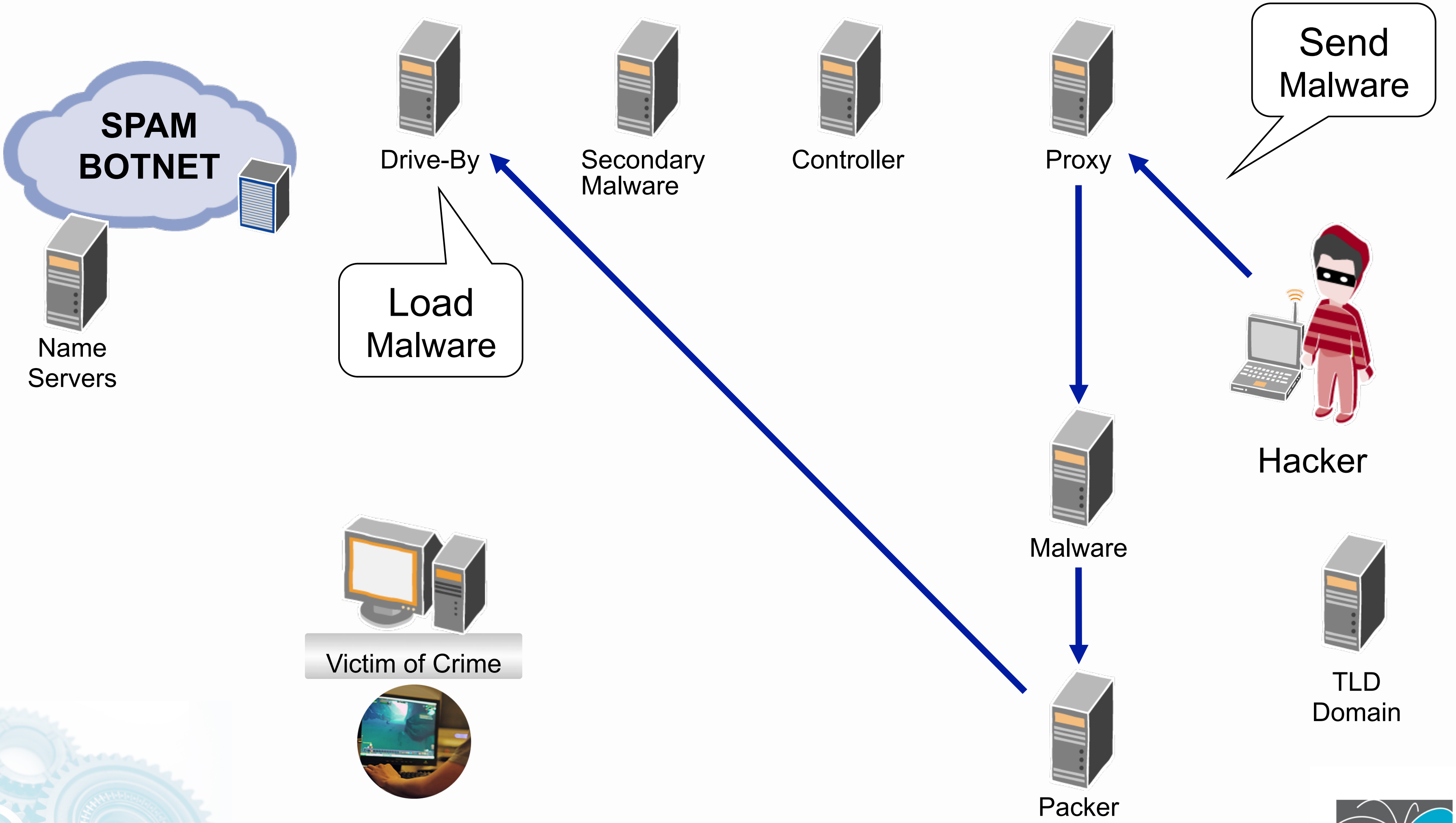


- ✓Avalanche: SPAM Cloud that you can lease time
- ✓Zeus: IPv6 Compliant "Build your Own Criminal Cloud.
- ✓BlackHole: Metasploit Cloud you can lease

Stage Domain Name

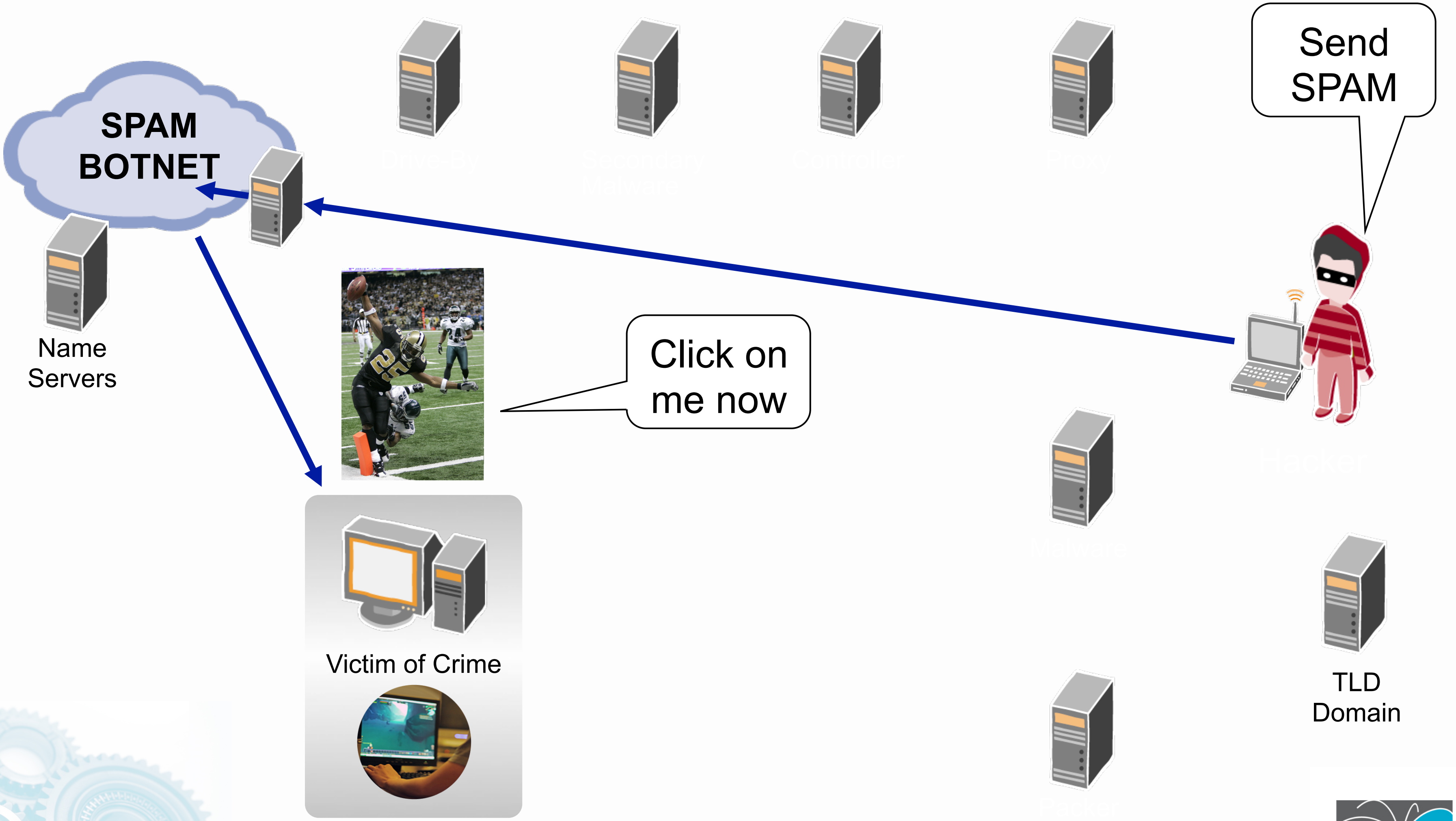


Prepare Drive-By

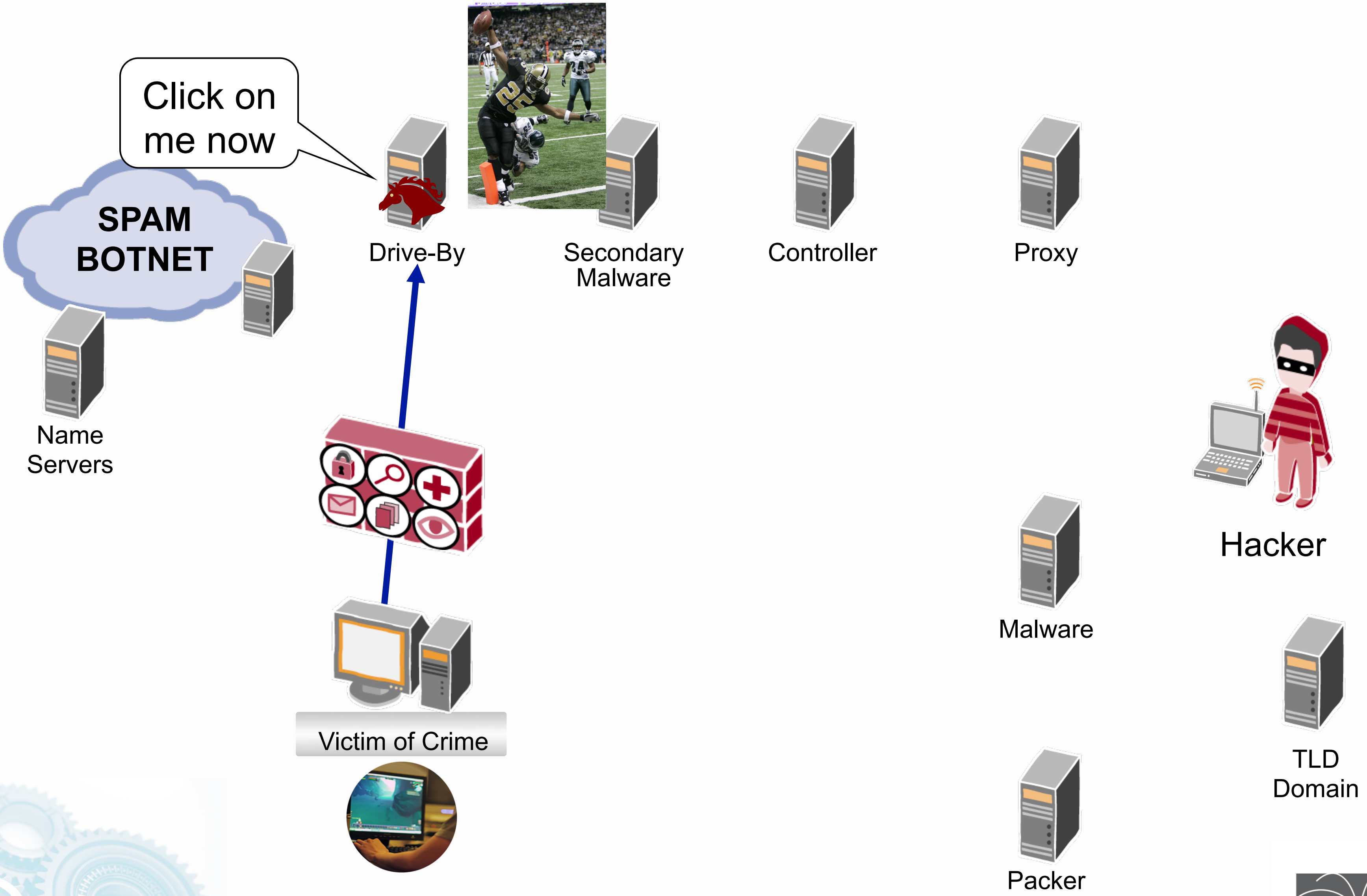


Social Engineered SPAM to Get People to Click

(Spear Phishing)



Drive-By Violation



Click on me now

SPAM BOTNET

Name Servers

Drive-By

Secondary Malware

Controller

Proxy

Hacker

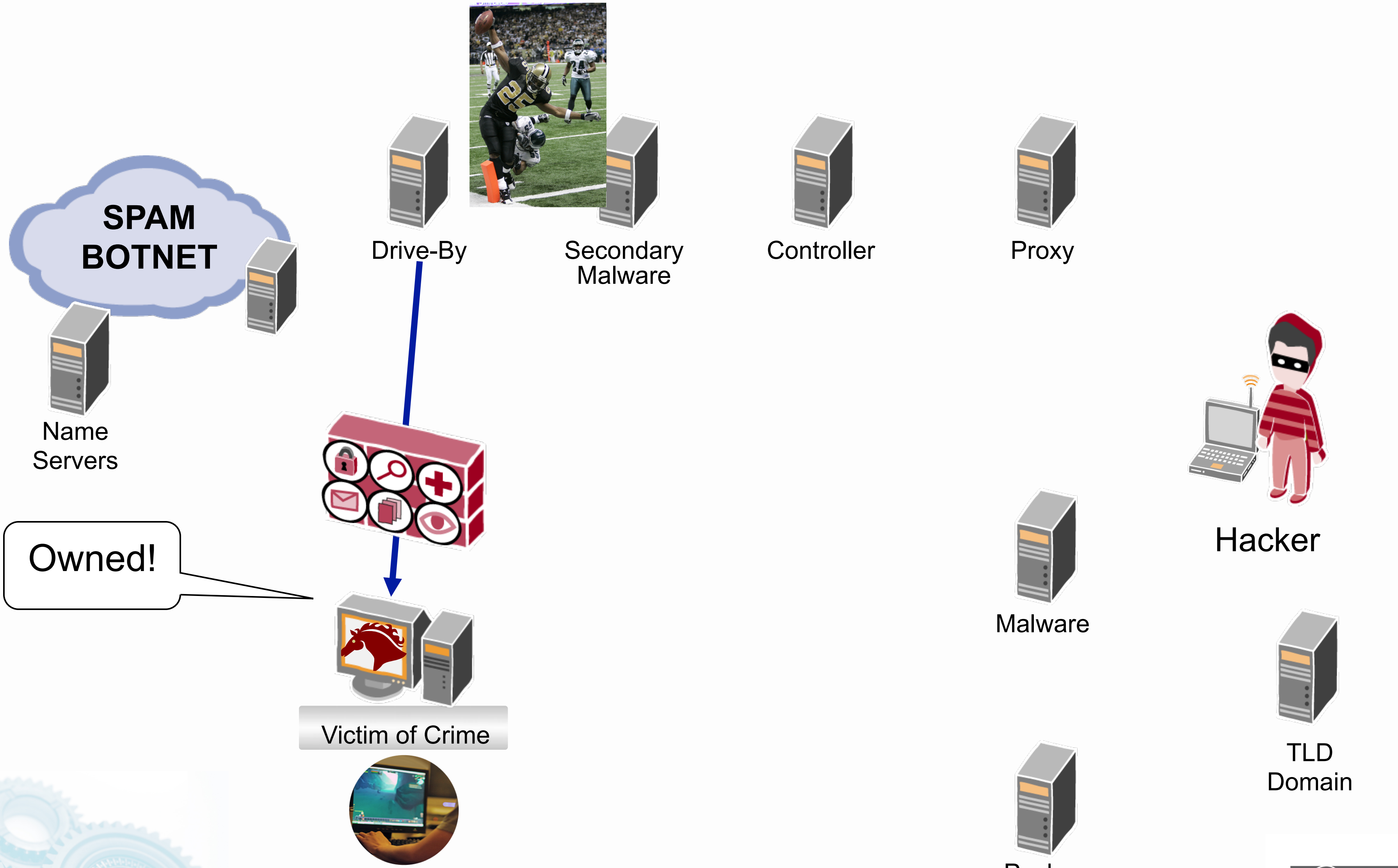
Malware

TLD Domain

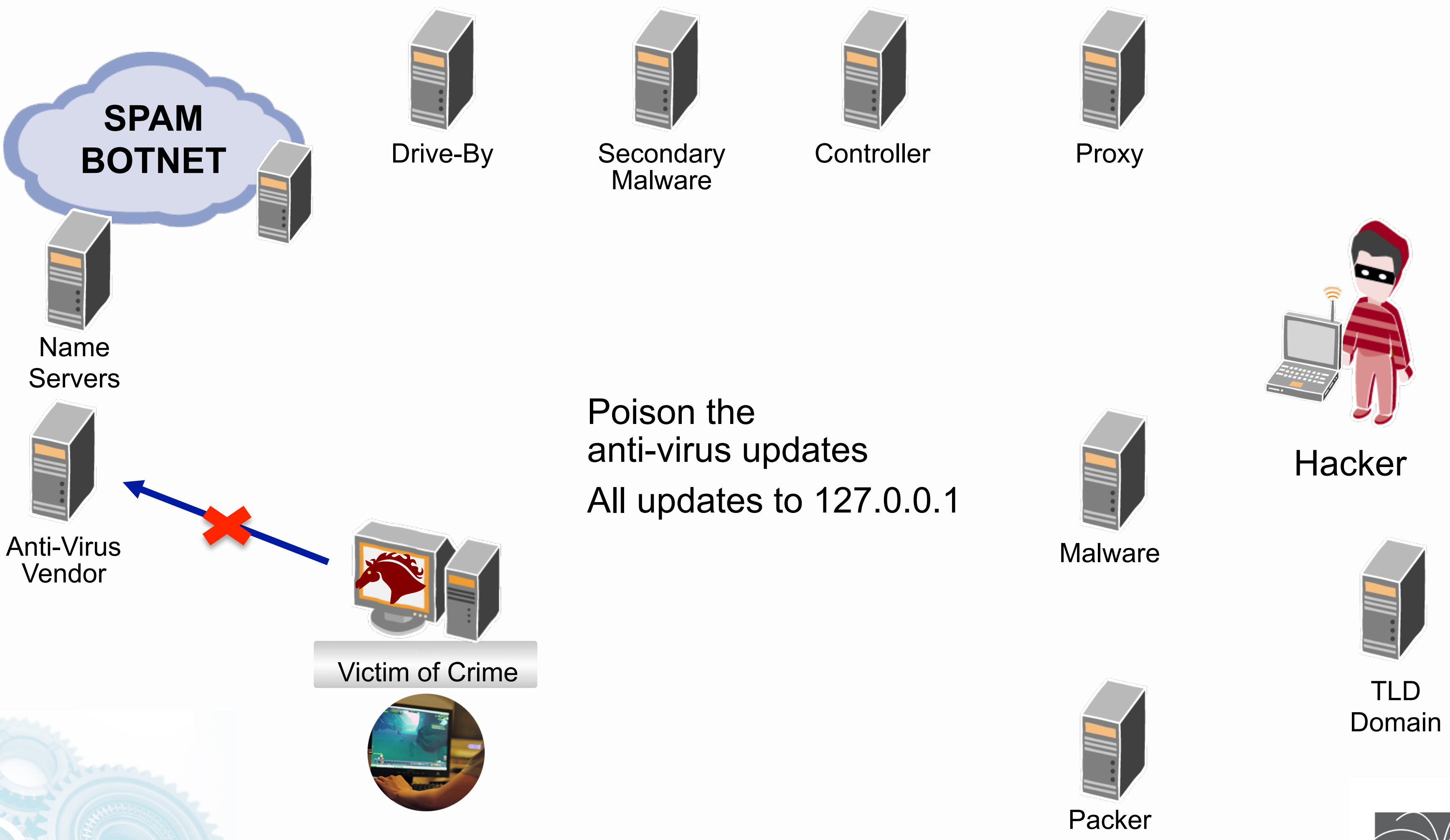
Packer

Victim of Crime

Drive-By Violation



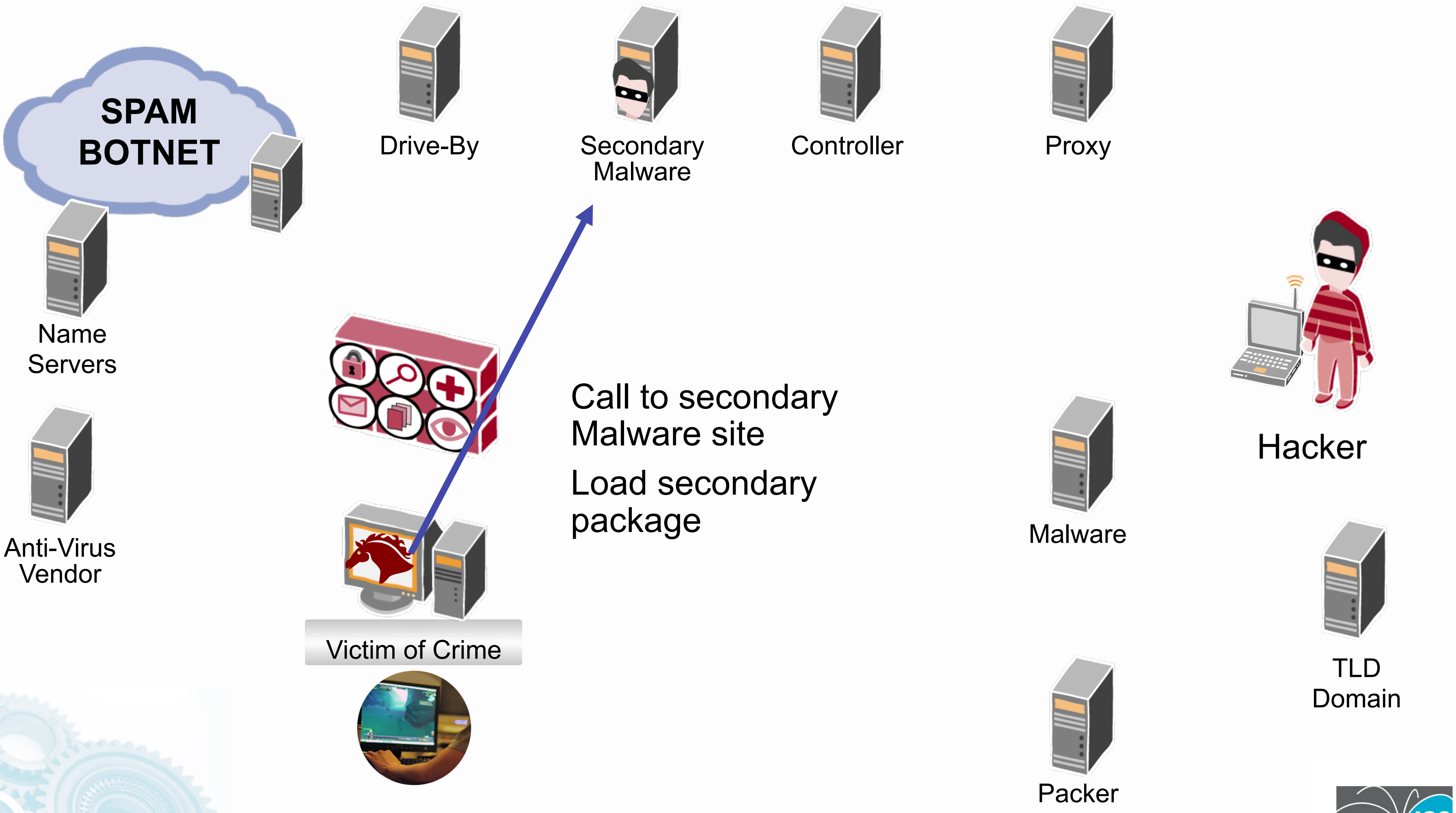
Poison Anti-Virus Updates



Poison the
anti-virus updates

All updates to 127.0.0.1

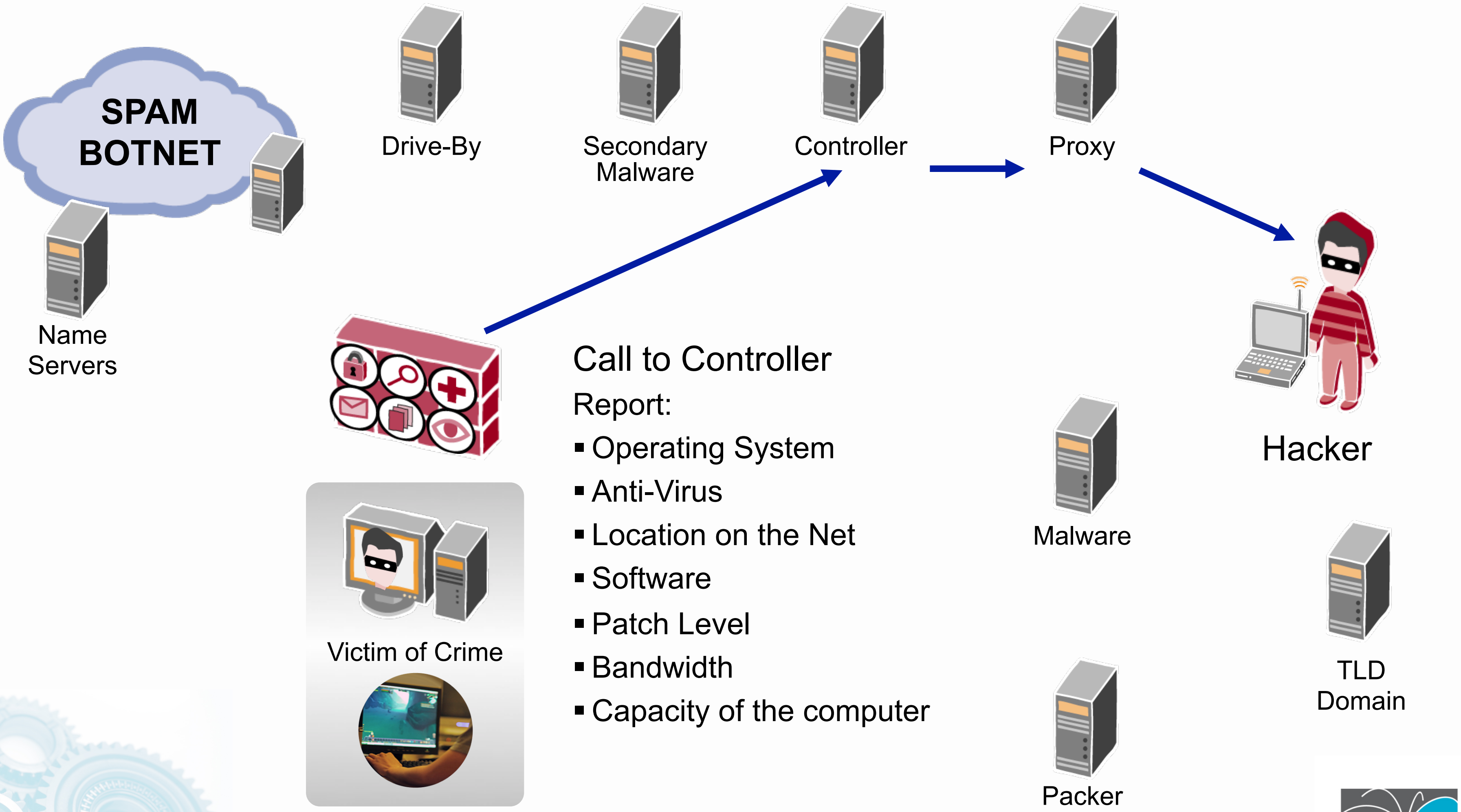
Prepare Violated Computer



Call to secondary Malware site

Load secondary package

Call Home

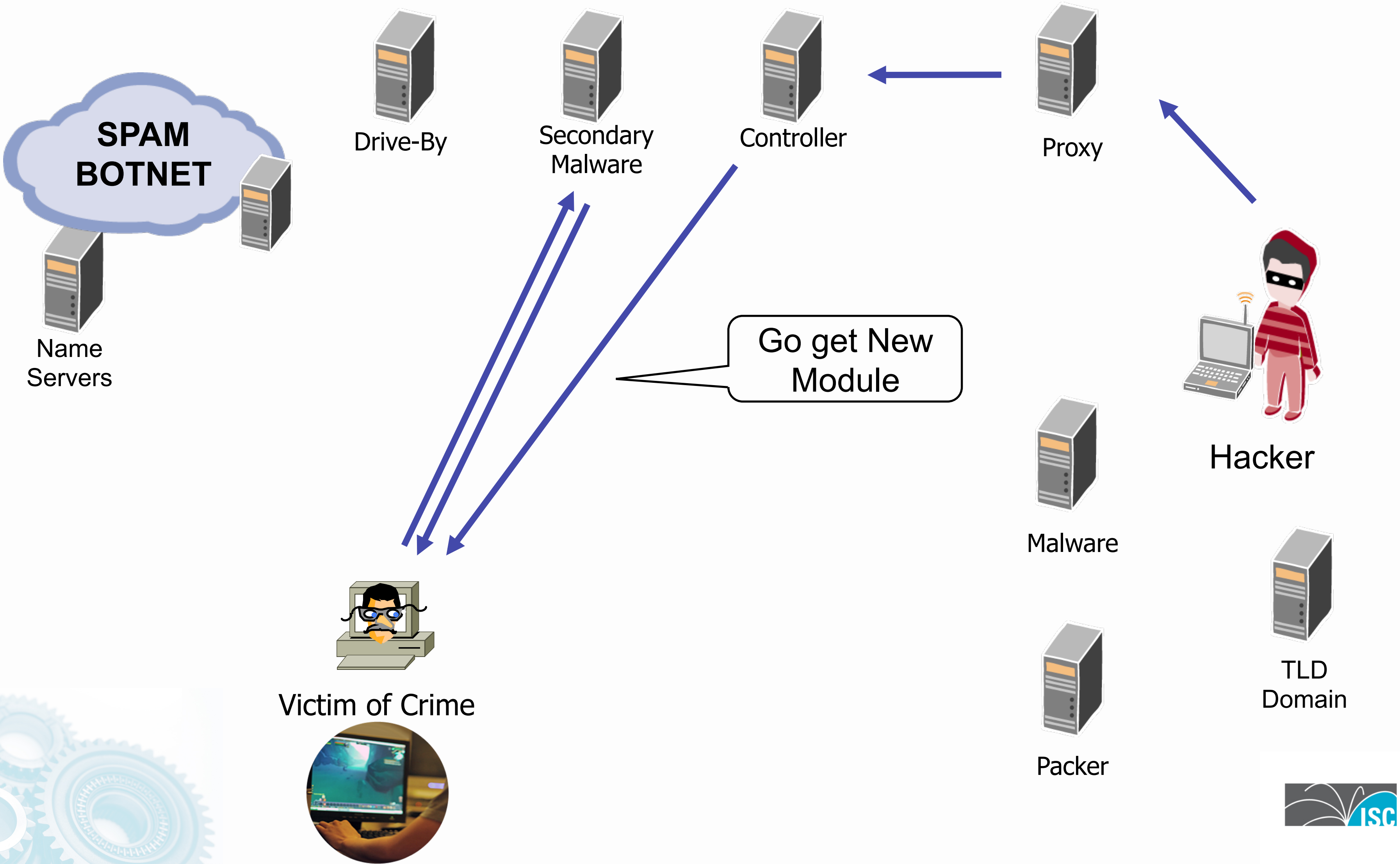


Call to Controller

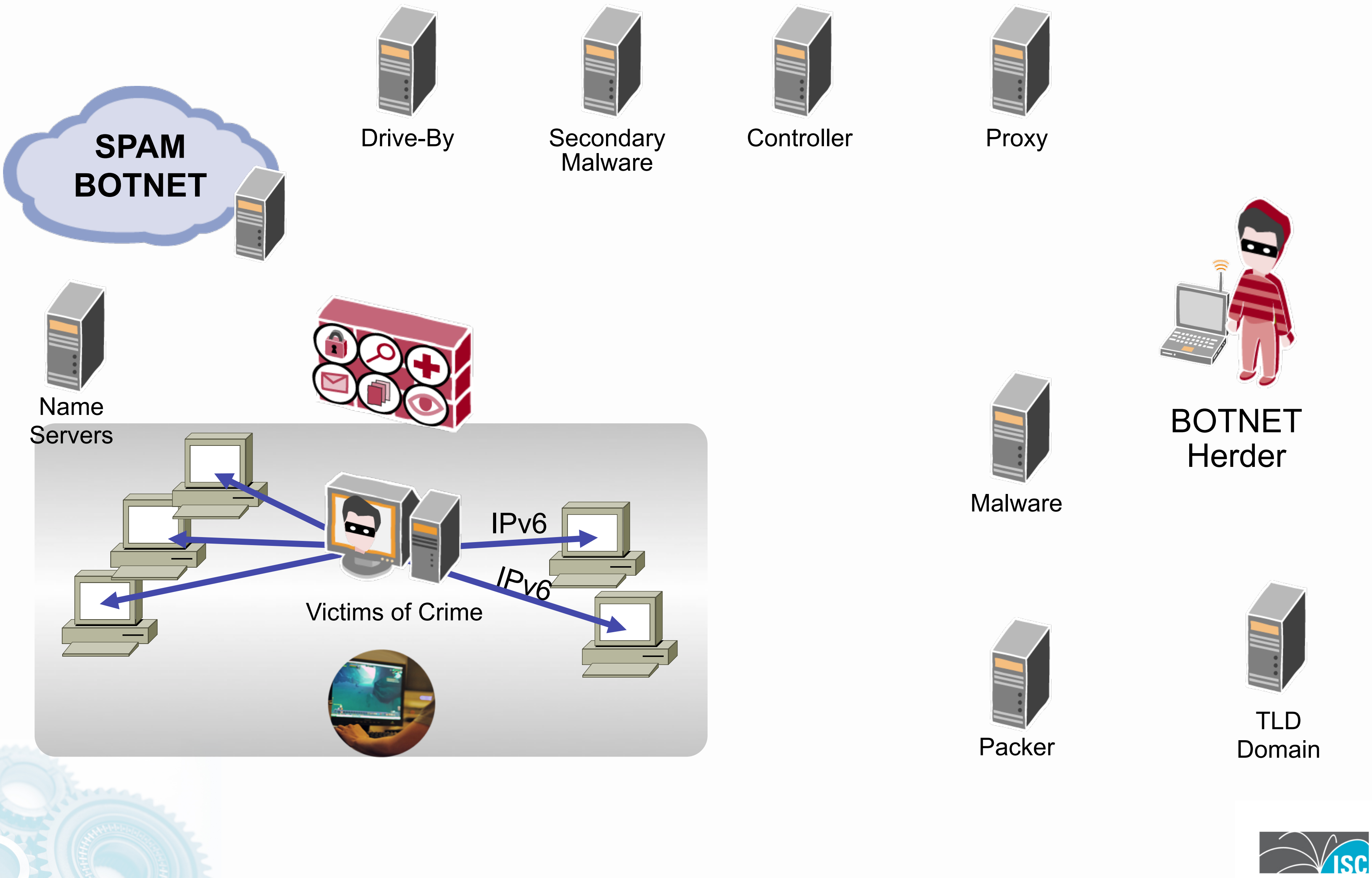
Report:

- Operating System
- Anti-Virus
- Location on the Net
- Software
- Patch Level
- Bandwidth
- Capacity of the computer

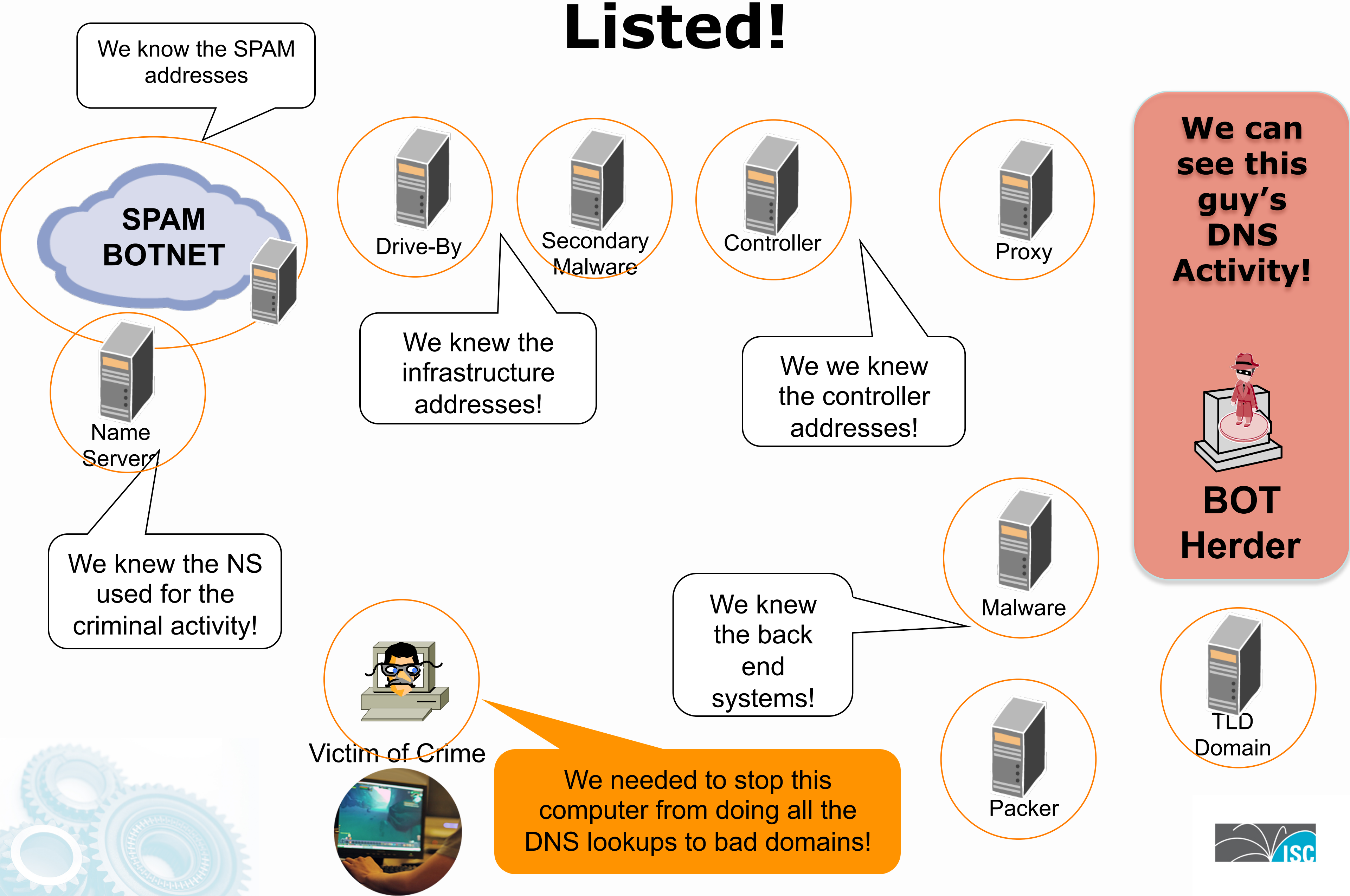
Load Custom Malware



Start Worming, Scanning, & Spreading



The Domain names were Black Listed!



We know the SPAM addresses

We knew the infrastructure addresses!

We we knew the controller addresses!

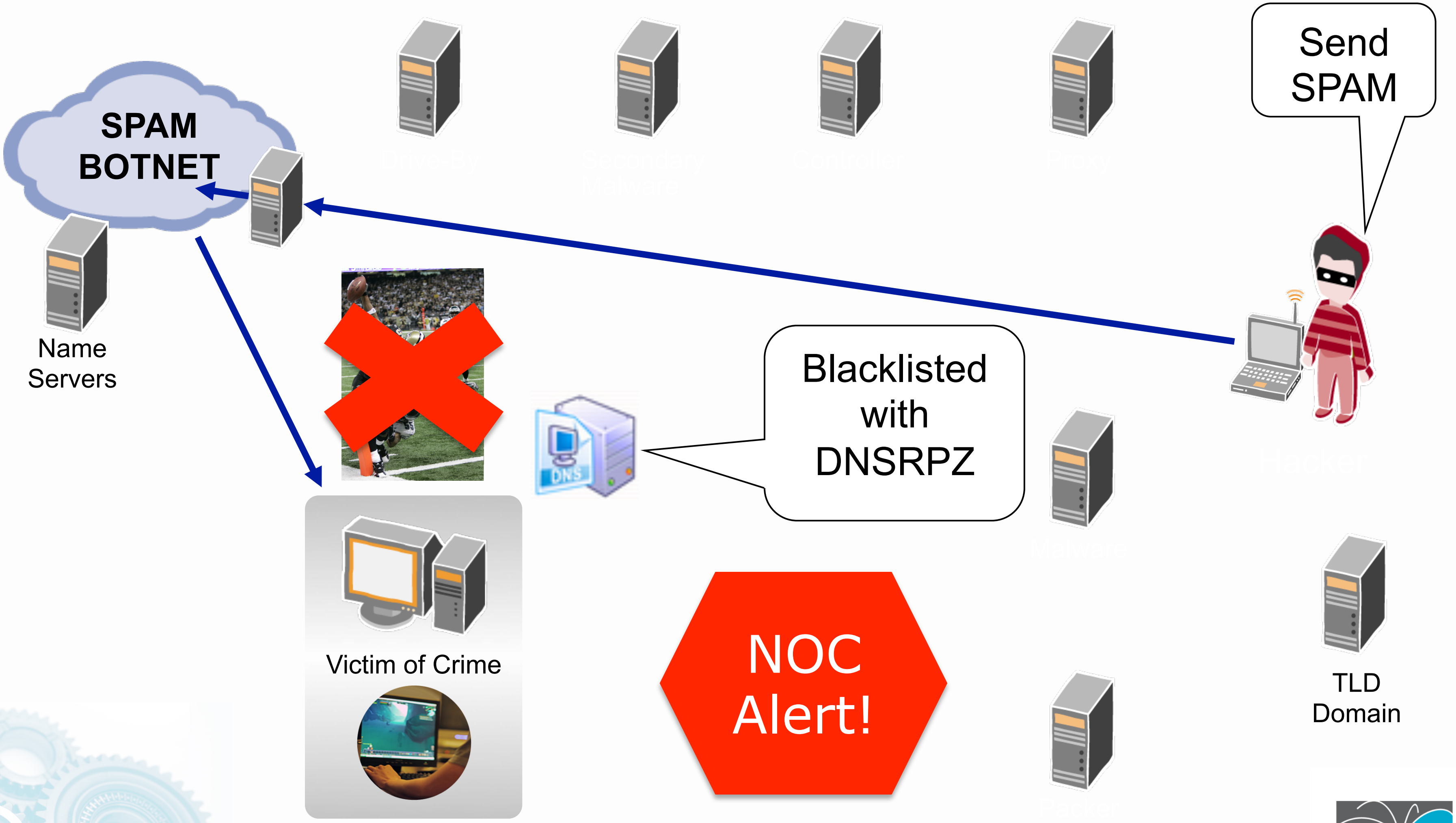
We knew the NS used for the criminal activity!

We knew the back end systems!

We can see this guy's DNS Activity!

We needed to stop this computer from doing all the DNS lookups to bad domains!

DNS RPZ would have stopped this attack!



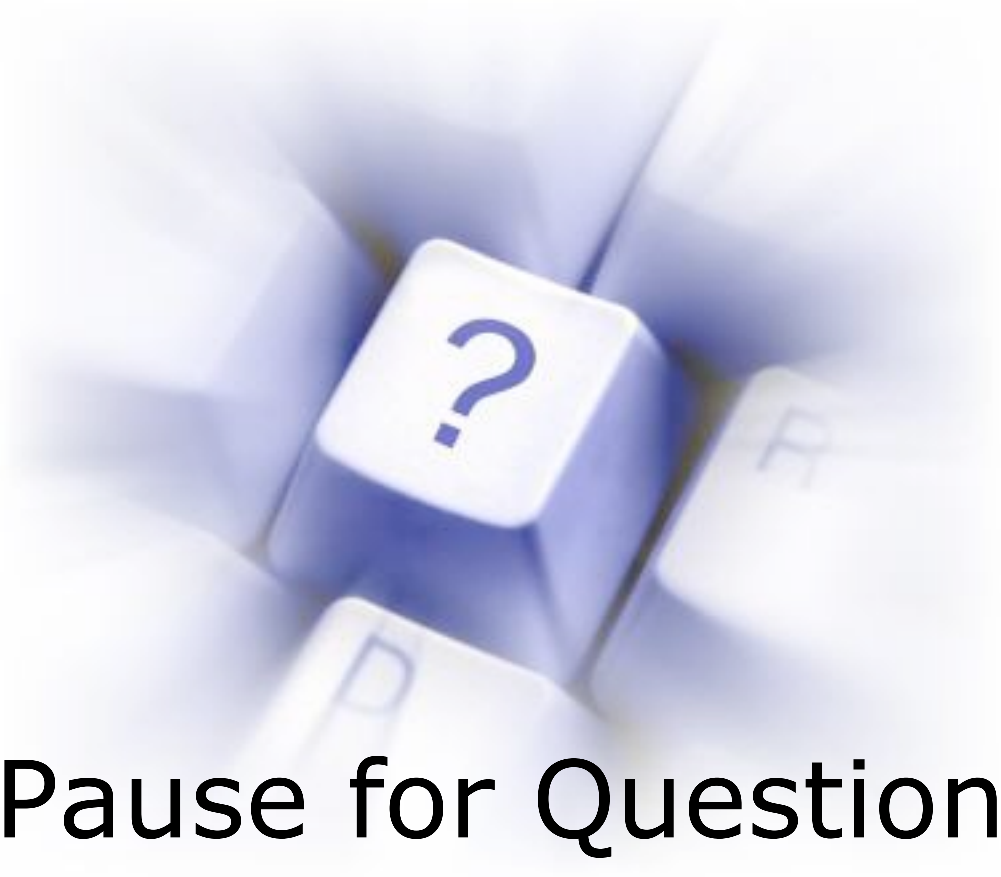
Send SPAM

Blacklisted with DNSRPZ

NOC Alert!

We need to look "out of the Box"

- Put things in context – this illustrate was real.
  - The computer was up to date with all the patches.
  - The anti-virus was up to date.
  - The users getting hit with MEBROOT/Torpig were all using Firefox and Noscipt
  - Some of the users were security people.
  - The network was locked down with firewalls, IDPs, and all the other BCP recommended.
  - The zero day hit was orchestrated from the criminals known domains!



Pause for Questions

During the Questions …..

- How do you get support for DNSRPZ?
- Today, that is with BIND:
  - ➢ Public Benefit support through the community:

    https://lists.isc.org/mailman/listinfo/dnsrpz-interest
  - ➢ Public Benefit support through the ISC Knowledge Base:

    http://deepthought.isc.org
  - ➢ **BIND Software Support Package**
    - Yes! ISC does Internet Critical Software Support Services.
    - http://www.isc.org/getbindsupport for a BIND upgrade package

DNSRPZ More Details

Original Problem Statement

- DNS is a decentralized system offering complete distributed autonomy. The relationships between operators and content owners are both tenuous and resilient.
- The split **registry**/**registrar**/**registrant** model insulates all parties from responsibility, so the global DNS lacks accountability. Complaints are ineffective, even with provable crime/losses.
- This resiliency and unaccountability benefits the bad actors committing cyber-crime.

Historical Context

- DNS is not unique in its unaccountability. Most Internet systems (mail, blogs, I-M) are similar.
- In e-mail it's extremely common to subscribe to an DNSBL (realtime blackhole list) in order to reject messages from known-bad sources.
- Features similar to DNSBL exist for DNS in proprietary products (Nominum) and services (OpenDNS).
- RPZ (ISC Response Policy Zone) is an open standard for DNSBL-like features in the DNS.

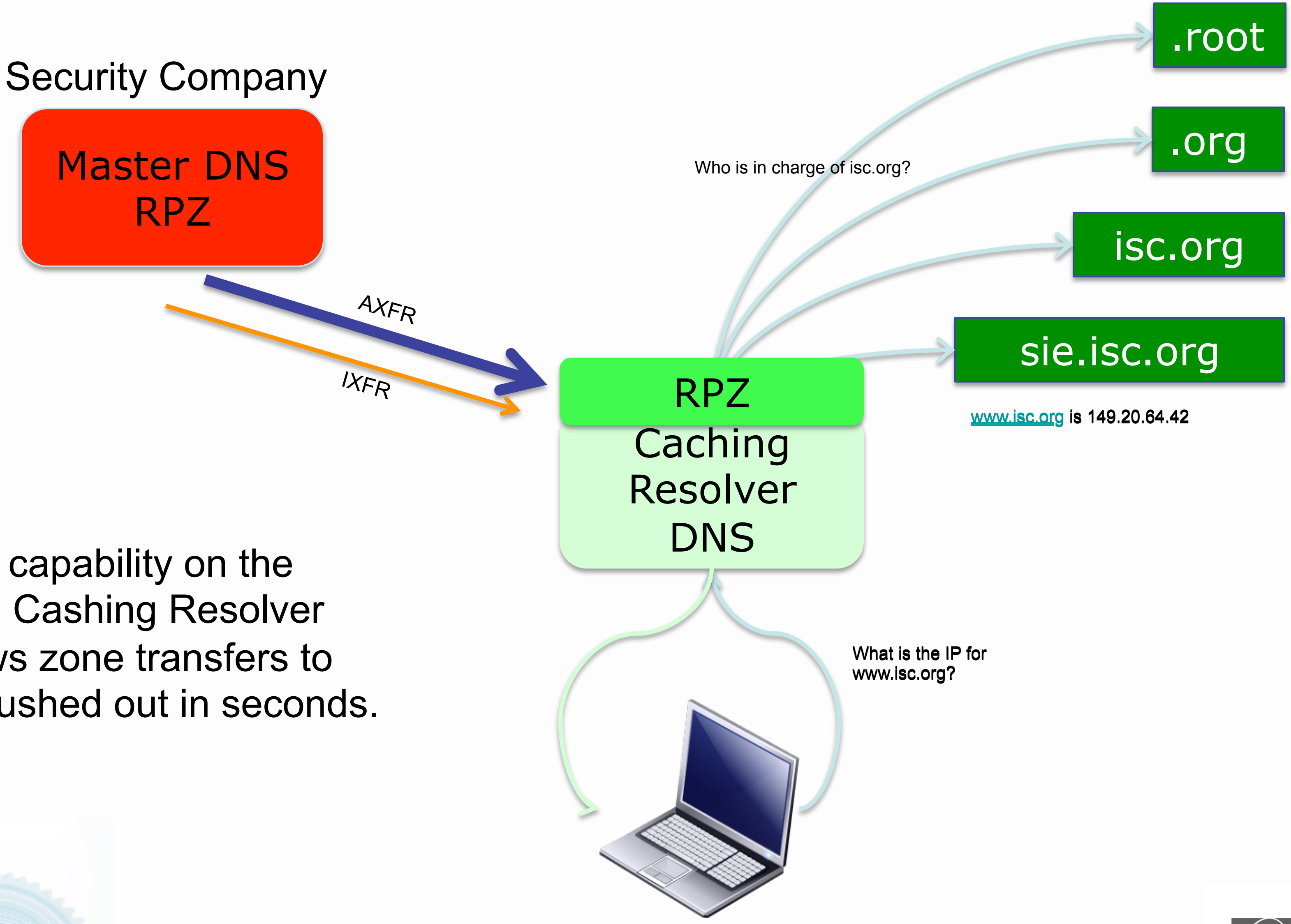
DNS IND (&T)

- IETF DNSIND working group (mid 1990's):
  - (I)ncremental zone transfer – RFC 1995
  - (N)otification of zone changes – RFC 1996
  - (D)ynamic update of zone content – RFC 2136
  - (T)ransaction signatures (TSIG) – RFC 2845
- Pre-IND DNS zone changes had long latency, heavy bandwidth, and low trust – so, high cost
- Post-IND DNS zone changes are immediate, with small deltas and good forward secrecy

RPZ History

- RPZ 1.0 released as patches to BIND9 in 2010:
- Rule-based system, triggered on query name/ type
- Rule-forced outcomes:
  - Return a fake alias (CNAME), for walled gardens
  - Return a fake NXDOMAIN, to blackout the name
  - Return a fake answer of the type being queried
  - Protect the name against subsequent policy triggers
- Subscription model: recursive name servers would become stealth servers for one or more RPZs.
- Rules/outcomes encoded as RPZ zone content.

DNS RPZ



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

RPZ Content Examples (1)

- If rpz.net is a response policy zone and example.com is a name to be blacked out:

  example.com.rpz.net CNAME .

- If all subdomains of example.com are to be aliased to a local walled garden:

  *.example.com.rpz.net CNAME wg.isc.org

- If www.example.com/A should be redirected:

  www.example.com A 198.168.6.66

RPZ Content Examples (2)

- If www.partner.com is to be protected from any policy action by any subsequent RPZ:

  www.partner.com.rpz.net CNAME www.partner.com

- If www.example.com is to appear to be empty:

  www.example.com.rpz.net CNAME *.

- If a A RRs in 192.168.1.0/24 are to be replaced with a local walled garden address:

  24.0.1.168.192.rpz-ip.rpz.net A 192.168.6.66

RPZ Content Examples (3)

- If AAAA RR's in 2001:500:2f::/48 ought to cause fake NXDOMAIN responses, except 2001:500:2f::f which is to be returned as normal:

```
128.f.zz.2f.500.2001.rpz-ip.rpz.net CNAME *.
48.zz.2f.500.2001.rpz-ip.rpz.net CNAME .
```

- Note: “zz” in this context means “::”.

Lessons Learned From RPZ 1.0

- Sometimes the trigger has to be answer-based
  - E.g., if the A or AAAA RR is within a CIDR block
  - E.g., if the NS name or address is poisoned
- Sometimes the subscriber wants to import the triggers but locally specify the policy outcome
  - E.g., import a list of bad names, but decide locally whether to blackout or alias those names
- We have implemented some of these features in RPZ Format 2, released in BIND 9.8.0.

RPZ Data as DNS Control

- DNS data maps *<owner,type>* → *record-set*
- RPZ data overloads *<owner,type>* as a *trigger* and *record-set* as an *action*
- A hybrid recursive/authoritative name server which subscribes to one or more RPZs can answer untruthfully according to RPZ policy
- RPZ data plane is promoted into the recursive DNS control plane according to name server configuration

RPZ Format 1 (in 2010)

- Triggers:
  - Q-name (all types)
  - Q-name, Q-type

- Actions:
  - Exemption
  - Force NXDOMAIN
  - Force empty answer
  - Force CNAME answer
  - Force specific answer

RPZ Format 2 (in 2011)

- New Triggers:
  - Answer in netblock
  - Name server name
  - Name server address in netblock

- New Actions:
  - None

Subscriber Configuration in BIND9

```
options {
   // other stuff
   response-policy {
        zone "dns-policy1.vix.com";
        zone "dns-policy2.vix.com" policy given;
        zone "dns-policy3.vix.com" policy NO-OP;
        zone "dns-policy4.vix.com" policy NXDOMAIN;
        zone "dns-policy5.vix.com" policy NODATA;
        zone "dns-policy6.vix.com" policy CNAME walled-garden.isp.net;
      };
   };
zone “dns-policy1.vix.com” {
     type slave;
     masters { 192.168.1.123; };
     // note: TSIG would probably be used in a production environment
};
     // and similar for the other rpz zones
```

Producer/Consumer Model in RPZ

- Producers can use RFC 2136 “UPDATE” to maintain their zone, or just periodically regenerate it and use “ixfr-from-differences” to tell BIND to compute deltas.
- Producers will use IXFR for efficient zone delta transmission, and TSIG for protection of RPZ data and authenticity of producer/consumer endpoints.
- Result: low cost, low bandwidth, low latency, and strong data protection.

Possible Good

- Specialization of labor: security experts can produce robust and targeted patterns for use by customer DNS recursive name servers.
- Competition: many security experts, many name server implementers (not just BIND!), and a global market of potential customers.
- Effect on crime: a domain or IP address used only for evil will not remain usable even if its registrant, registrar, registry, or ISP never suspends or terminates it.

Possible Harm

- Governments could use RPZ to enforce laws about censorship, since it is an open standard.
- Some RPZ data sources will inevitably be politically, racially, or religiously motivated (“all Christian web sites” or “all Muslim web sites”).
- As with all reputation systems, the systemic effect on DNS will be to make it less reliable and harder to diagnose or characterize.
- We hope these effects will be more pronounced on bad actors than on the rest of us.

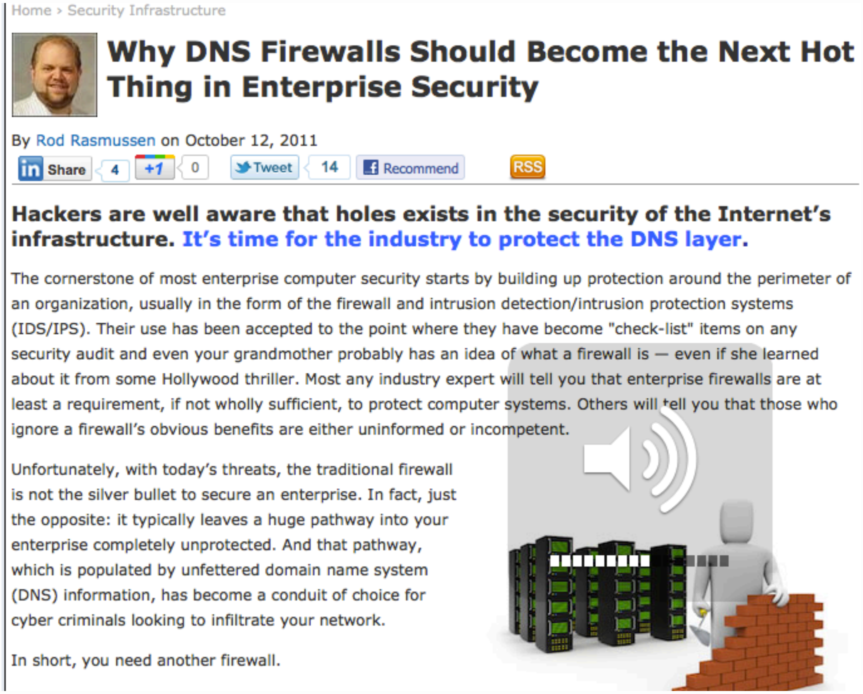
Pause for Questions

During the Questions …..

- Download & save for later reading the Protect IP Paper:
- *Security and Other Technical Concerns Raised by the DNS Filtering Requirements in the Protect IP Bill*.
    - http://infojustice.org/archives/3469

- Security Week Article:

  http://www.securityweek.com/



Home › Security Infrastructure

Why DNS Firewalls Should Become the Next Hot Thing in Enterprise Security

By Rod Rasmussen on October 12, 2011

Hackers are well aware that holes exists in the security of the Internet's infrastructure. It's time for the industry to protect the DNS layer.

The cornerstone of most enterprise computer security starts by building up protection around the perimeter of an organization, usually in the form of the firewall and intrusion detection/intrusion protection systems (IDS/IPS). Their use has been accepted to the point where they have become "check-list" items on any security audit and even your grandmother probably has an idea of what a firewall is — even if she learned about it from some Hollywood thriller. Most any industry expert will tell you that enterprise firewalls are at least a requirement, if not wholly sufficient, to protect computer systems. Others will tell you that those who ignore a firewall's obvious benefits are either uninformed or incompetent.

Unfortunately, with today's threats, the traditional firewall is not the silver bullet to secure an enterprise. In fact, just the opposite: it typically leaves a huge pathway into your enterprise completely unprotected. And that pathway, which is populated by unfettered domain name system (DNS) information, has become a conduit of choice for cyber criminals looking to infiltrate your network.

In short, you need another firewall.

DNSRPZ Providers

Spamhaus' DBL as RPZ

- Domains seen in spam or under control of spammers
- Includes malware domains
- Published at rpz.spamhaus.org
- Email rpz-data@spamhaus.org for access
- More info at
  http://www.spamhaus.org/news.lasso?article=669

ActiveTrust® Resolver RPZ

- Focused on enterprise threats
  - Malware distribution and communications
  - Phishing, including spear-phishing
  - Data exfiltration
- Constantly updated with fresh information
  - Market-leading detection of phishing and malware sites
  - Criminal infrastructure analysis using passive DNS
  - Malware reverse-engineering including DGAs
  - Detection and analysis of anomalous DNS requests
- Updated every 15 minutes
- Optional TrapTrace™ redirection and analysis service to determine who, what, when for blocked connections
  - Detailed info on threats on your network from IID Threat Intel Team
- More info at internetidentity.com

DNS RPZ & SURBL

- What is SURBL RPZ?

  ➢SURBL RPZ is a version of SURBL's high-quality anti-spam, anti-phishing and anti malware data in the form of a DNS Response Policy Zone (DNS RPZ). DNS RPZs are used to deny or modify the resolution of low-reputation domains, in other words, to deny DNS services for known-bad domains. SURBL is the world's first provider of RPZ data.

- Why use SURBL RPZ?

  ➢SURBL RPZ data are typically used to protect users from visiting objectionable or dangerous spam, phishing or malware web sites. Doing so can prevent identity theft, phishing attacks, malware infection, loss of revenue due to visiting objectionable spam sites, and more. This is made possible by SURBL's highly-regarded, multi-sourced, real-time intelligence about such domains.

- How to use SURBL RPZ

  ➢SURBL RPZ is available via DNS zone transfer using recent versions of BIND 9. Local SURBL RPZ queries are answered by your local BIND recursive nameserver where they can be used to deny resolution (NXDOMAIN is the default behavior) or to send traffic to a local walled garden for example, instead of allowing the successful resolution known-bad domains. Other RPZsupported behaviors are available by modifying the response values as needed in your operational environment. SURBL RPZ data are available by private incremental zone transfer.

➢Please contact us using the Data Feed Request form on our web site www.surbl.org
in order to arrange access, or call Arnie Bjorklund 302-231-1201, arnieb@securityzones.net

Questions?

dnsrpz@isc.org

Don’t get Caught Off Guard with Old BIND!

- Get Professional Support to help you upgrade BIND!
  - ➢ http://www.isc.org/getbindsupport
- Special Offer Software Support & Consulting Deal!
  - ➢ Take advantage of this special deal that combines 6 months of Basic Support & 8 hours of Expert Consulting to get your organization started with BIND support, have enough support time to get your systems upgraded, and convince management to budget for critical DNS infrastructure support.
- Webinar Special Discount!
  - ➢ ISC will E-mail all participants after the webinar. If you did not get or cannot wait, E-mail to sales@isc.org

ISC In a Nutshell

Forum

- BIND
- BIND 10 Working Group
- DHCP
- AFTR/PCP
- SIE
- Open Source Routing

RPKI (Securing BGP) and more to come … first reference, standards based code.

Professional Services

- Consulting
- Training
- Software Support Services
- Custom Software Development
- F-root Corporate Node
- DNS SNS-Com
- Full version The Domain Survey

Public Benefit Services

- DNS “F-ROOT”
- DNS Secondary Server Resiliency (SNS) PB
- Hosted@ - hosting a range of open source code)
- Free Domain Survey Report
- ISC assistance at IETF, ICANN, ARIN, ISOC RIPE WG, UKNOF, etc

Empowerment

- Standards drivers – with first implementation of standards based code.
- Policy Meetings – Empowering Spheres of Influence
- Operational Security – Pioneering new approaches to safe guard the Internet (OPSEC-Trust).
- Operations Meeting Empowerment (APRICOT, AFNOG, NANOG, etc)
- Research (DNS OARC)

New from ISC

Open Source Routing Forum

+
+
=
SIE@ISC
Security
Trust
Information

ISC

Technology Leadership for the Common Good

Internet Systems Consortium