



# **Your Reputation Precedes You**

**Friday, 7<sup>th</sup> October 9:30-10:00am**

- **Gunter Ollmann**

- VP of Research, Damballa Inc.
- Board of Advisors, IOActive Inc.



- **Brief Bio:**

- Been in IT industry for 2+ decades – Built and run international pentest teams, R&D groups and consulting practices around the world.
- Formerly Chief Security Strategist for IBM, Director of X-Force for ISS, Professional Services Director for NGS Software, Head of Attack Services EMEA, etc.
- Frequent writer, columnist and blogger with lots of whitepapers...
  - <http://blog.damballa.com> & <http://technicalinfodotnet.blogspot.com/>
  - Email: [gollmann@damballa.com](mailto:gollmann@damballa.com)      Twitter: @gollmann



# **(Brief) Background to Reputation**

The minimum stuff you need to know to understand the rest of the material

- **Reputation systems:**
  - Basically a summary of past actions
  - Past context to make decisions today
- **Static reputation**
  - Traditional list of known good/bad
  - Binary view (listed or not)
- **Dynamic reputation**
  - Sliding windows and aggregate scoring
  - “live” reputation scores



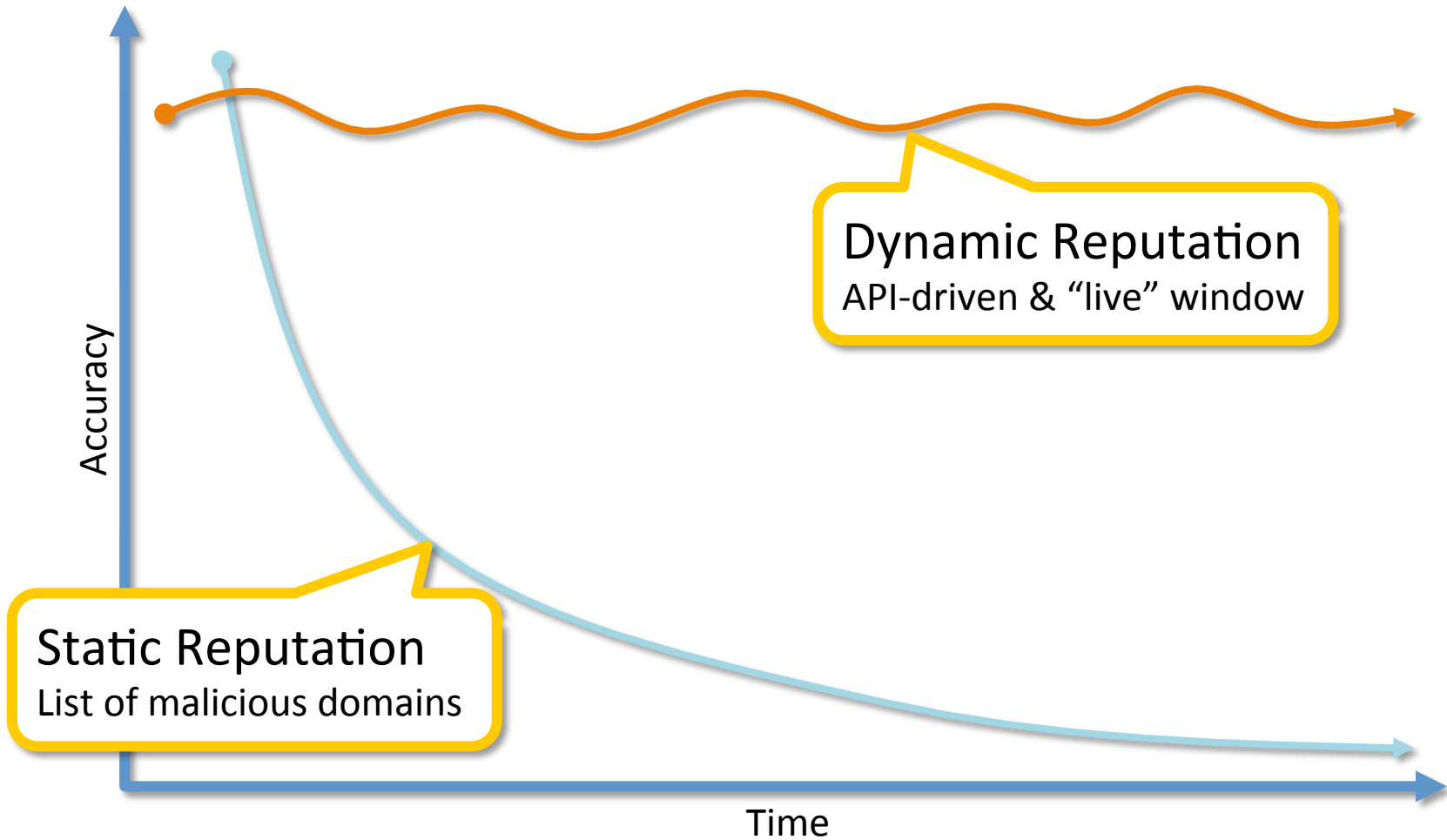
- **Most common form of “reputation” system**
  - Blacklists = stuff you don’t want
  - Whitelists = stuff you don’t want to interrupt
  - Static reputation
- **Used in all sorts of places:**
  - Firewall filtering
  - File inspection
  - Web filtering
  - Training sets for dynamic reputation



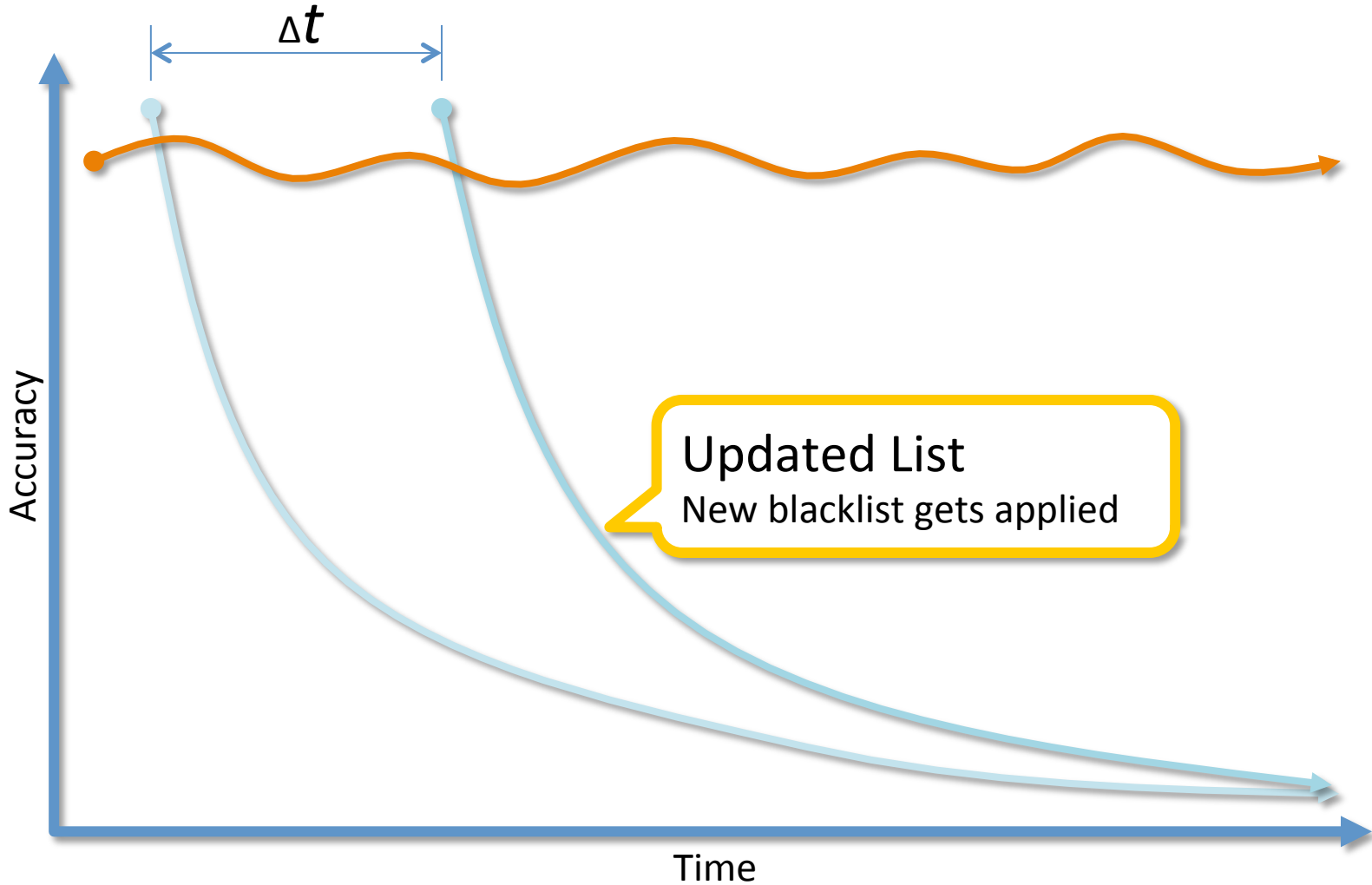
- **Frequency of monitoring**
- **Frequency of updates**
- **Passive or active monitoring**
- **Visibility and coverage**
  - Local spam in China?
- **IP assignment**
  - NAT & DHCP



# Static vs. Dynamic Reputation

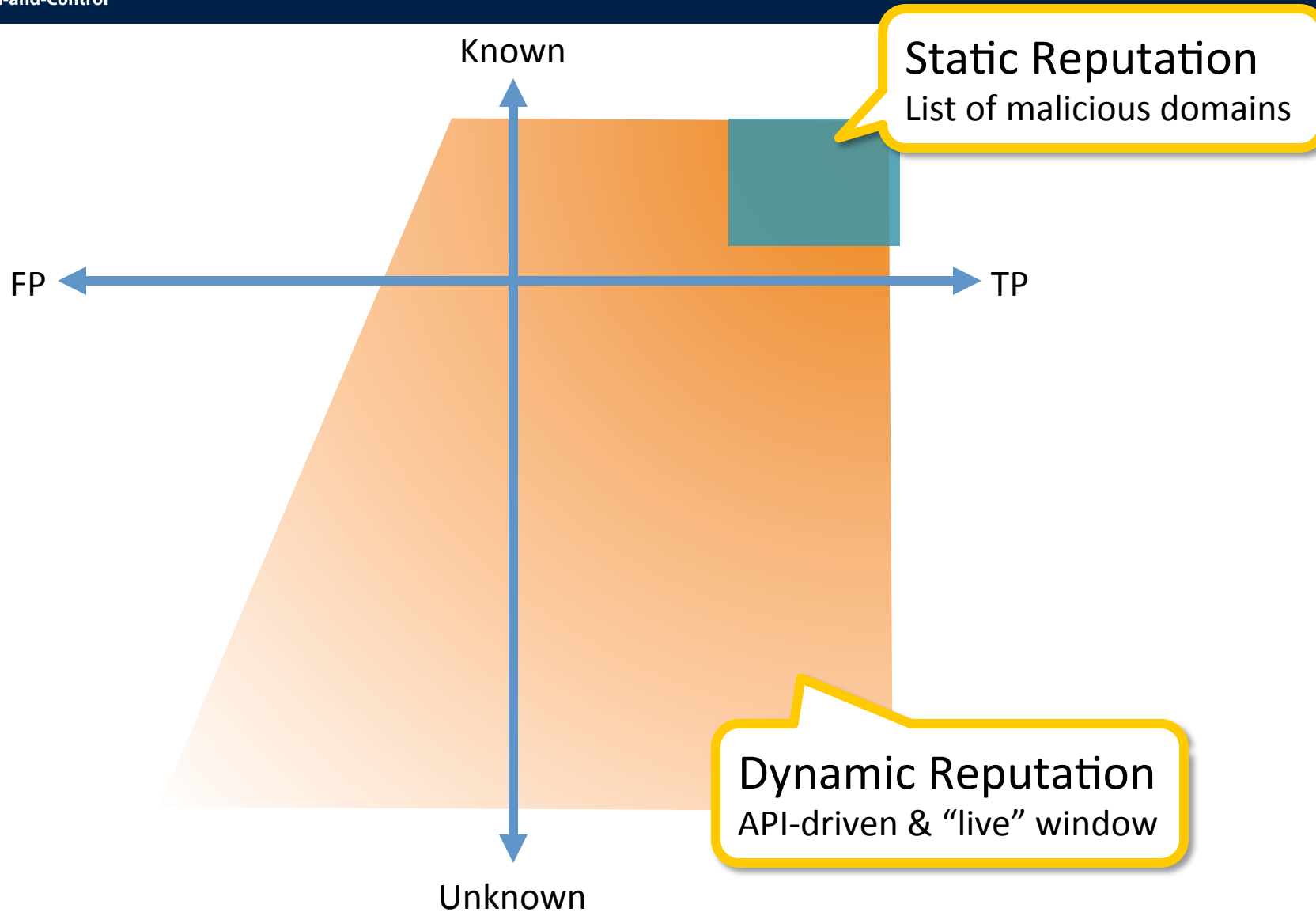


# Static vs. Dynamic Reputation

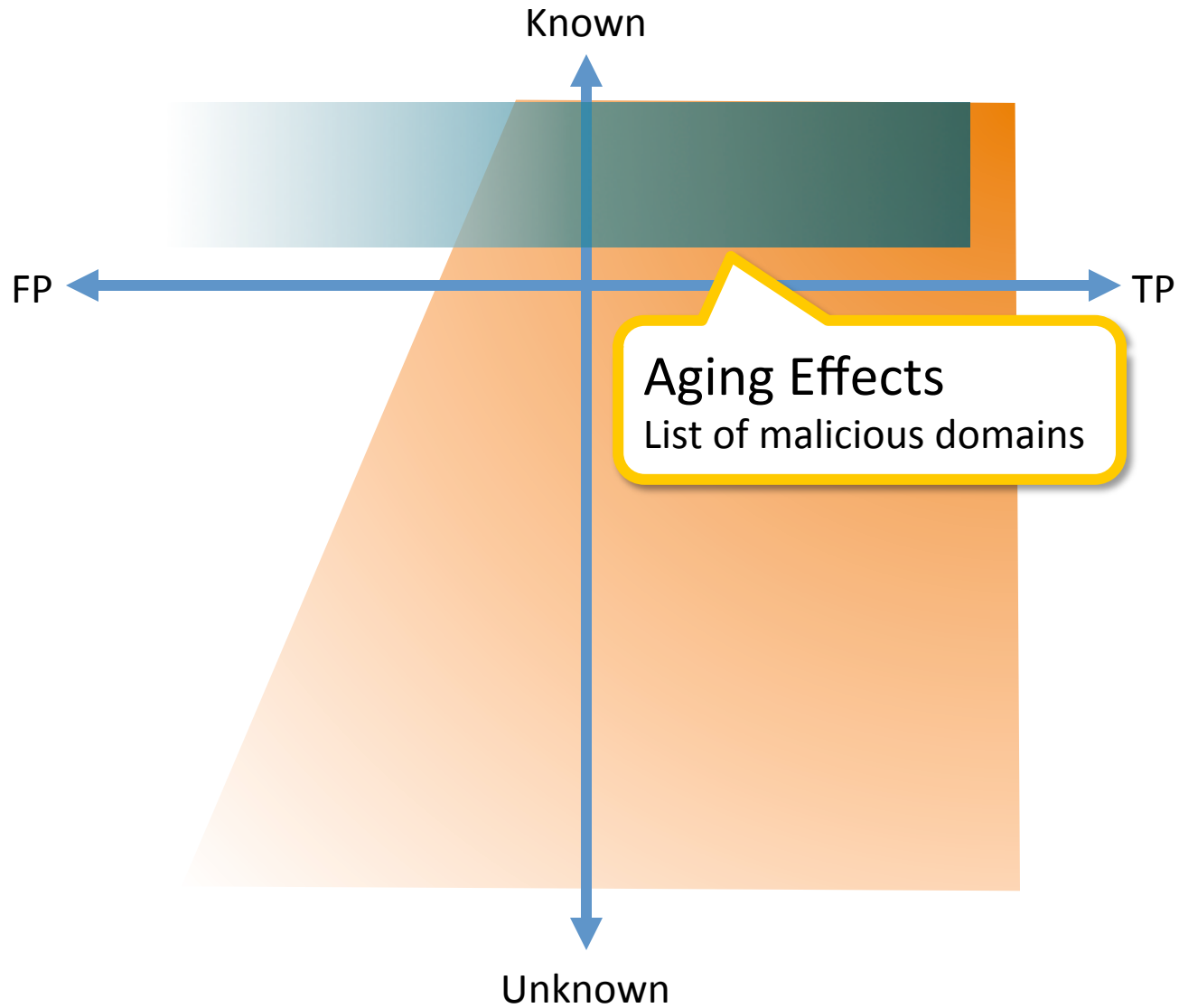




# Static vs. Dynamic Reputation



# Static vs. Dynamic Reputation



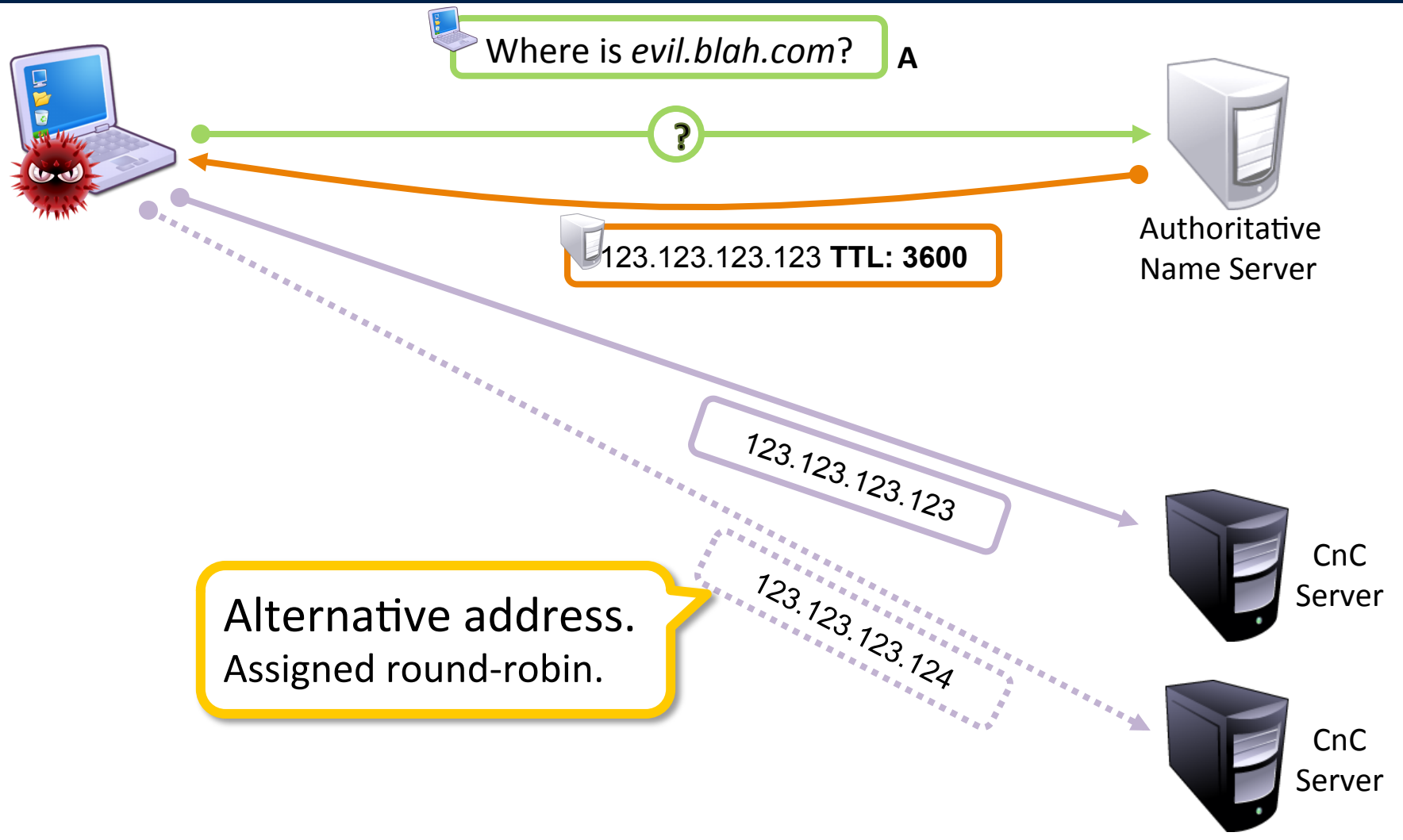
*The* **FLASH**

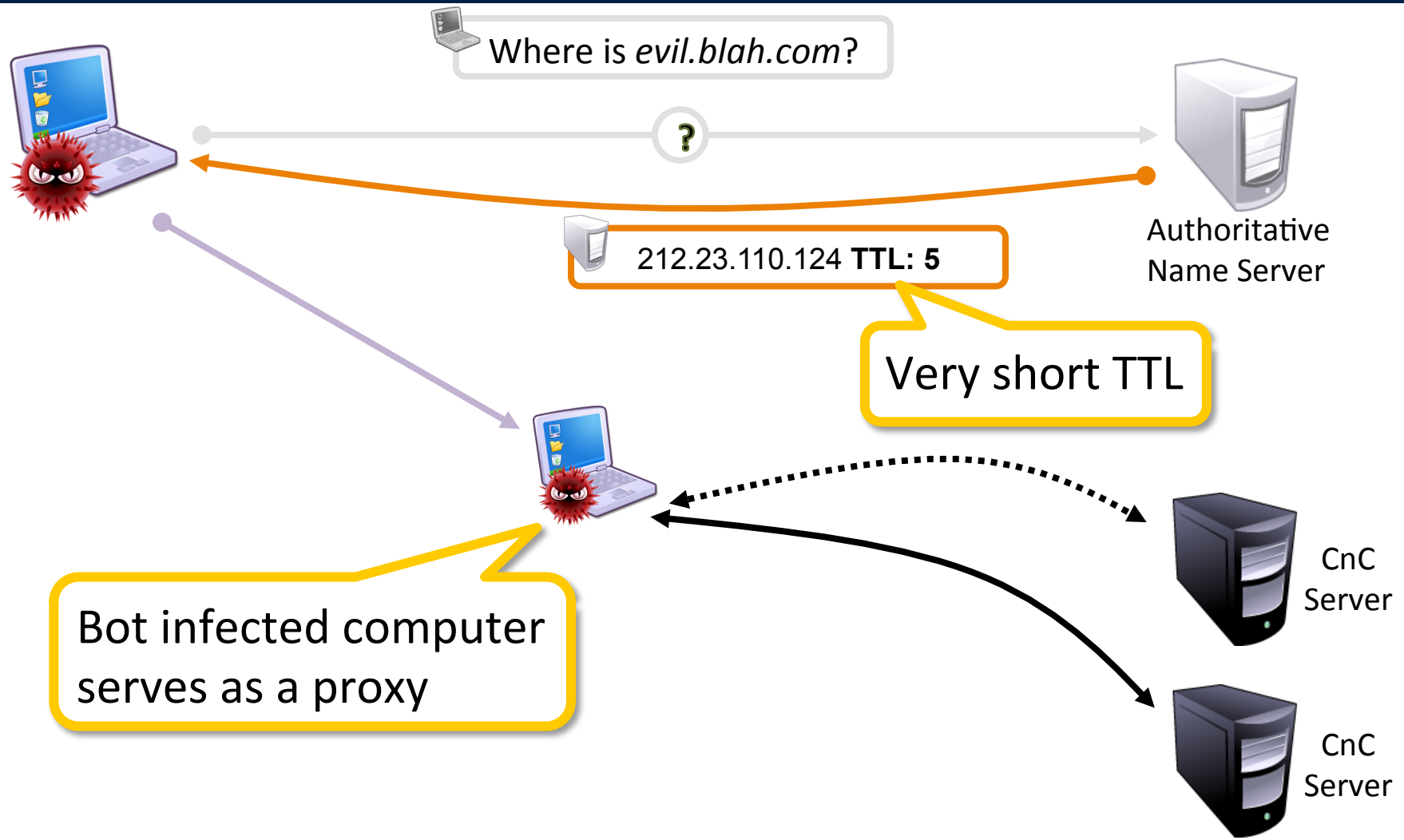


# The Agile Threat

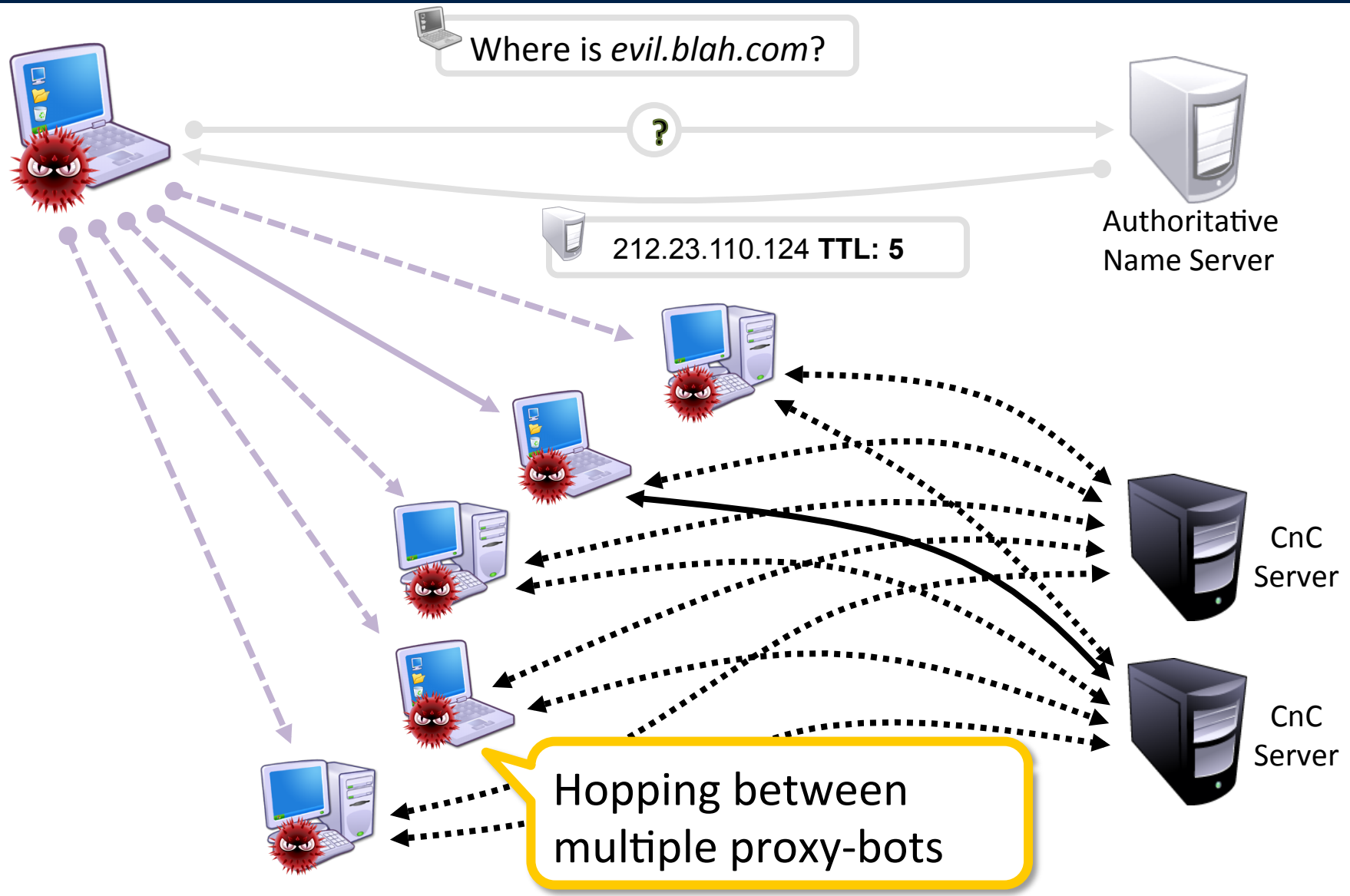
What the badguys do to make things hard for reputation systems

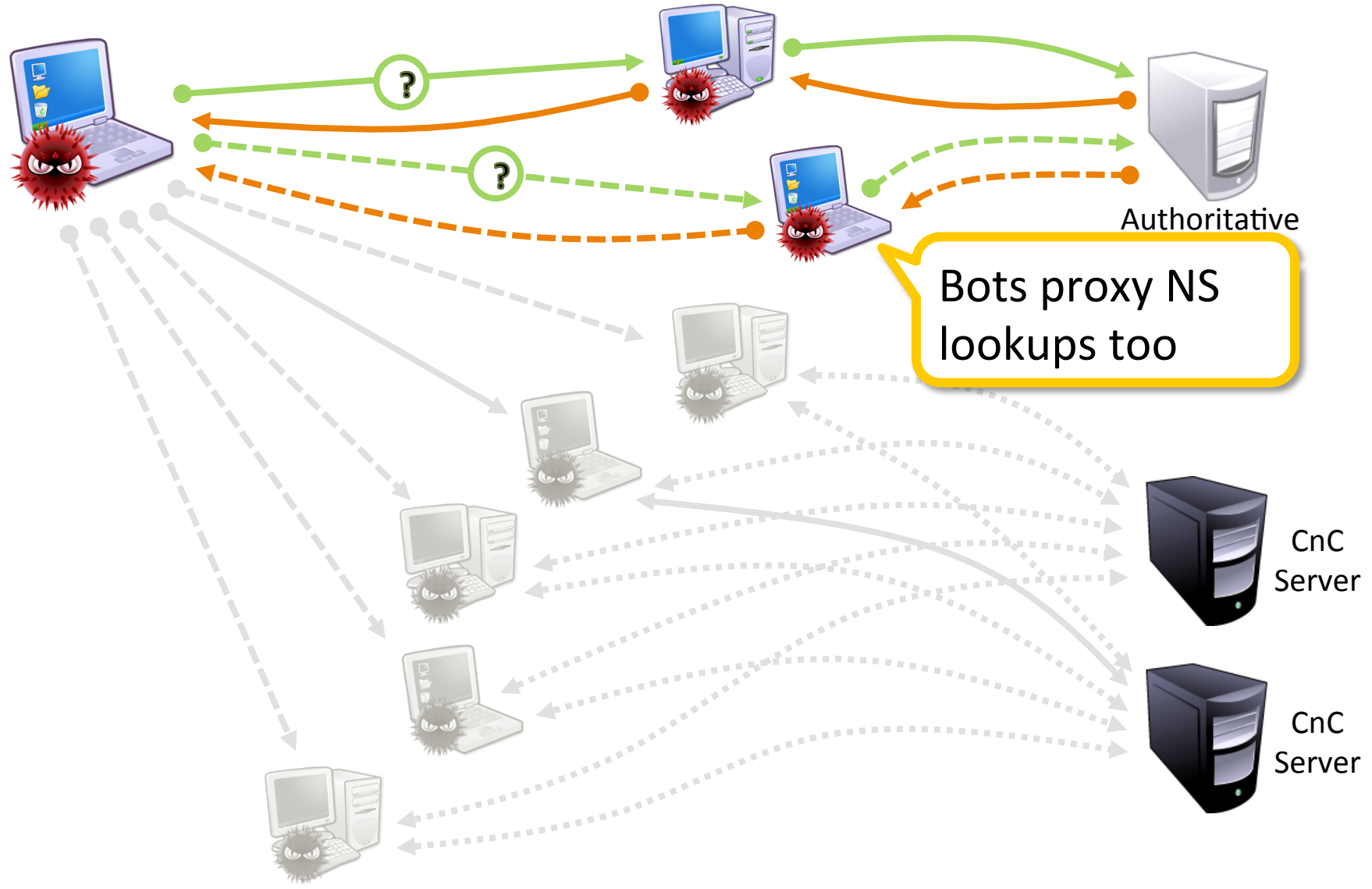
# Where's the CnC





Bot infected computer serves as a proxy





- **Mass registrations**
  - Pattern to domains
  - Mix of characters/numbers
  - Sometimes dictionary words
- **May be free DDNS too**

```
freakyfriday23a.3322.cn  
freakyfriday24d.3322.cn  
freakyfriday23a.ddns.com  
freakyfriday24d.ddns.com  
freakyfriday23a.dyn-dns.com
```

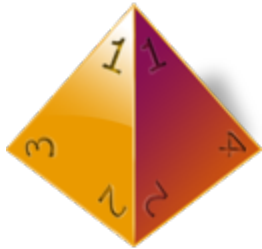
```
command.blah20110923a.com  
command.blah20110923b.com  
command.blah20110924a.com  
command.blah20110924b.com  
command.blah20110924e.com
```

```
cnc.a0a01603e2ff.blah.com  
cnc.a0a01603e3ff.blah.com  
cnc.a0a01603e4ff.blah.com  
cnc.a0b21603e2ff.blah.com  
cnc.a0b2160307ff.blah.com
```

```
freakyfriday23a.blah.com  
freakyfriday24d.blah.com  
freakyfriday33t.blah.com  
freakyfriday25m.blah.com  
freakyfriday28k.blah.com
```



- **Domain Generation Algorithm (DGA)**
  - Mathematical algorithm – date/time based
  - Generate 10's thousands, try a few hundred
  - Customize “seeds” in some malware DIY kits
  - May use DDNS or “personalized” 3LD services



## Bobax Variant

q6obbbx.r00t.la  
5w61675.themafia.info  
qr1agp1.servepics.com  
081a4jh.serveftp.com  
eet88nd.shell.la  
cwlhuwl.sexypenguins.com  
9t9iw4u.serveblog.net  
cz46ht0.lamer.la  
41stwa1.sexypenguins.com  
tsz1twx.sytes.net

## Murofet

osudhnmqjsrsip.info  
osudhnmqjsrsip.com  
wumlmmrsyw Kempx.net  
wumlmmrsyw Kempx.biz  
wnxfsoevnomago.info  
wnxfsoevnomago.com  
kmsxphusznhrb.org  
kmsxphusznhrb.com  
diuuvkgvszqproh.biz  
diuuvkgvszqproh.org

## Sinowal

rdixtxezwt.com  
vmithskvme.com  
ocefyfhqmf.com  
vifqgbccxg.com  
slwamznmcq.com  
knbriyfnsq.com  
oqabpwrxxa.com  
wwtnekmjij.com  
sxtxlixtnt.com  
lbqghhpudt.com

## Unknown

mdecub-ydyg.ru  
mgefa-bugin.com  
mkoza-diyyk.com  
mmoby-dotir.com  
mpodod-axoz.ru  
msofy-debef.com  
mvahif-ufum.ru

mzakef-ihos.ru  
mfenaf-anyg.ru  
mjepuf-erin.ru  
mleraf-yvot.ru  
mpetyf-uxeb.ru  
mryvof-ibuh.ru  
mvyzyf-ofop.ru

- **Technique to spread traffic over array of IP's**
  - Often associated with spam delivery
  - Multiple blocks of IP's used
- **Multiple domains related to IP's**
  - Further obfuscation of attack traffic
  - Fake domain whois data



- **Mass hacks of popular/legit servers**
  - Web servers are most common
  - Target servers that have been around for a while
  - “Mass hacks” of virtual host servers

Legend:  
H - Homepage defacement  
M - Mass defacement (click to view all defacements of this IP)  
R - Redefacement (click to view all defacements of this site)  
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	★	Domain	OS	View
2011/09/16	JCA	H		R	★	www.sudan.gov.sd	Linux	mirror
2011/09/16	sm3		M			www.samamentalhealth.ir/fa/	Linux	mirror
2011/09/16	lorans		M			vanegasinmobiliaria.com	Linux	mirror
2011/09/16	sm3	H	M			cnf.sttu.ac.ir/ias22/fa/	Linux	mirror
2011/09/16	00X					muangthaitoday.com	Linux	mirror
2011/09/16	1923Turk	H	M			webdesign.happygalaxy.org/tmp/...	Linux	mirror
2011/09/16	SmartGhost	H	M			jeeransport.com	Linux	mirror
2011/09/16	HEXB00T3R	H				www.suplesklep.pl	Linux	mirror
2011/09/16	Elsaba			M		arabic.bayynat.org.lb/index.html	Linux	mirror
2011/09/16	sm3			M		www.gostareshfarsi.ir/fa/	Win 2003	mirror
2011/09/16	Barbaros-DZ	H			★	...		mirror

- **It takes time to build/distribute blacklists**
  - Badguys just have to be faster than the list
- **“Registering” faster**
  - Automated domain registration
  - Free dynamic DNS
  - DNS wildcarding



- **Badguys maintain their own blacklists**
  - Firewall drop-list scripts (pastebin)
  - X-morphic delivery engine updates

```
.631. iptables -A INPUT -s 82.94.216.224/27 -j DROP #Spamhaus Logistics Corp.
.632. iptables -A INPUT -s 216.83.36.32/29 -j DROP #DroneBL
.633. iptables -A INPUT -s 174.121.168.208/29 -j DROP #The Honeynet Project
.634. iptables -A INPUT -s 174.123.14.64/28 -j DROP #WebsiteWelcome,hostexploit.com,etc...
.635. iptables -A INPUT -s 94.23.35.159 -j DROP #NoVirusThanks.org
.636. iptables -A INPUT -s 69.163.228.127 -j DROP #stopthehacker.com
.637.
.638. iptables -A INPUT -s 194.85.155.0/24 -p tcp -m multiport --dports 80,443,8080 -j DROP
#Scientific Research Center of Informatics of MFA of RF
.639. iptables -A INPUT -s 67.79.193.240/28 -p tcp -m multiport --dports 80,443,8080 -j DROP
#TIPPINGPOINT-TECH
.640. iptables -A INPUT -s 111.87.96.0/24 -p tcp -m multiport --dports 80,443,8080 -j DROP
#Security Operation Center KDDI Corporation
.641. iptables -A INPUT -s 77.124.145.20 -p tcp -m multiport --dports 80,443,8080 -j DROP
#HEAD BOT
.642. iptables -A INPUT -s 87.68.70.180 -p tcp -m multiport --dports 80,443,8080 -j DROP
#HEAD BOT
.643. iptables -A INPUT -s 87.70.86.117 -p tcp -m multiport --dports 80,443,8080 -j DROP
#HEAD BOT
```



# The Dynamic Network

Even without the badguys, network dynamics are a problem

- **It's tough enough without the bad guys!**
  - Internet is dynamic
- **Changes “to the core”**
  - Transition from IPv4 to IPv6
  - Cloud computing
  - Anycast routing

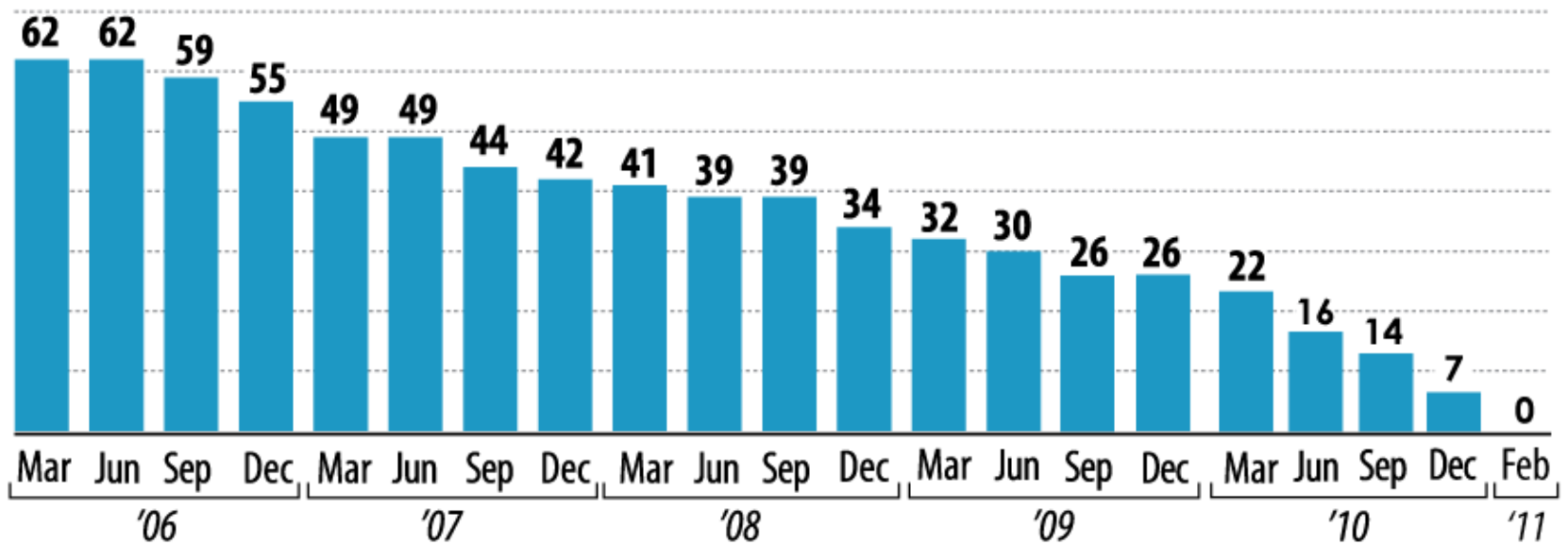




- **IPv6 address space is HUGE!**
  - $2^{128} = 340,282,366,920,938,463,374,607,431,768,211,456$
- **Plenty of places to run & hide**
  - Subnets allocated to residential “larger than IPv4”
  - Scanning & probing “empty space” infeasible
- **No marked “history”**
  - No basis for blacklists
  - Too small for many dynamic reputation approaches



- Available IPv4 Space in /8s



- The IANA pool of IPv4 address space depleted on February 3, 2011. This slide shows the steady depletion of that pool over time.



Home

FAQ

New Offer

## Create Bid

### Price Index

AFRINIC - *n/a*

APNIC - *max. bid: 4.00 USD*

*min. offer: N/A*

ARIN - *max. bid: 3.00 USD*

*min. offer: N/A*

LACNIC - *n/a*

RIPE - *max. bid: 3.00 USD*

*min. offer: N/A*

Global - *max. bid: 3.00 USD*

*min. offer: N/A*

## Welcome !

We are providing an open market for IPv4 addresses. [Learn more](#)

Don't have an account yet?

Signup

Email address /  
NIC handle:


You can bid for a block of IPv4 addresses. Specify the region in which you will use the addresses, and the minimum and maximum block size you request in CIDR bits (e.g. 22 as minimum if you want at least 1024 addresses). There are four maximum prices that you are willing to pay for the block:

- Sale: Price per IP address, in US\$, for sale from your region
- Lease: Price for renting the address block for a period of one year. [More details on leasing](#)
- Global sale: Price for buying the block to a service provider in a different region. [More details on global transfer of addresses](#)
- Global lease: Price for leasing the address block to a different region.

All of the prices are optional; you must specify at least one. If you don't propose a price, the address block is not offered for the respective kind of transaction.

All bids can be withdrawn at any time before they are being matched; please read the [policies](#) for more information.

Minimum block:  CIDR bits, e.g. 24

Maximum block:  CIDR bits, e.g. 22

APNIC ▼

USD per address

USD per address per year

USD per address

USD per address per year

bids

### Trading Policies

Offers and bids can be submitted and withdrawn at any point, until they are matched. If there is a match, buyer and seller are given 14 business days to confirm the deal. After that time and positive confirmation, contract details are exchanged. tradeipv4.com deducts 1% of the purchase price as commission. The commission is billed 14 days after deal confirmation.

For leases, the minimum contract period is one year; the negotiated rent is good for one year. After that time, the partners are free to extend the lease, or adjust the contract on mutual agreement; no new commission will be required.

On each trading day, the exchange rate is set to arrange for the maximum trading volume. Address blocks can be split into at most four subblocks to create a deal, within the limits of the minimum block sizes according to the regional transfer policies.


- **Matching buyers & sellers**

The screenshot shows the AddressX website. On the left, there is a graphic of several IP address cards with values like 190.22.1.0/24, 148.178.0.0/16, and 56.0.0.0/8. To the right, there is a login section with the text "Please enter your credentials to enter the site:" and two input fields for "Email" and "Password", followed by a "Login" button. Below the login section is a contact form with the text "please **Contact Us** for more information about Address and to request access". The contact form includes fields for "Email Address \*", "Phone", and "Message".

The screenshot shows the Depository Internet Registry website. At the top right, there is a "Sign in" section with "Username:" and "Password:" labels and input fields. Below this is a navigation menu with links for "Home", "Services", "Management", "Contact", and "Whois Search". The main heading is "DEPOSITORY Internet Registry". Below the heading, there is a paragraph of text: "Depository provides post-allocation Internet Registry services to entities (Commercial, Government, Education or Military) that hold Internet Protocol version 4 (IPv4) number resources that were granted to them, without a contract, by an authorized allocation authority." and another paragraph: "The company's services are fee based and do not require membership."

- **Commercial cloud providers being abused**
  - Convenient hosting for criminals
  - Easy to tear-down and restart elsewhere in cloud
  - Multiple (dynamic) egress IP's
  - Co-located with legitimate businesses
- **Reputation systems stalled**
  - Dynamic IP's = can't blacklist (all or nothing)
  - "history" element hard to nail down





Don't push  
this button

# Dynamic Reputation

Applying reputation to dynamic networks and threats

- **Dynamic reputation for dynamic threats**
  - “live” reputation scoring
  - Dynamic window of threat observations
- **Transition from “have to have seen it before”**
  - *Predictive scoring* based upon history, context, and known Internet structure (good/bad/gray)
- **Dynamic reputations:**
  - For IP
  - For Domains
  - For “DNS”

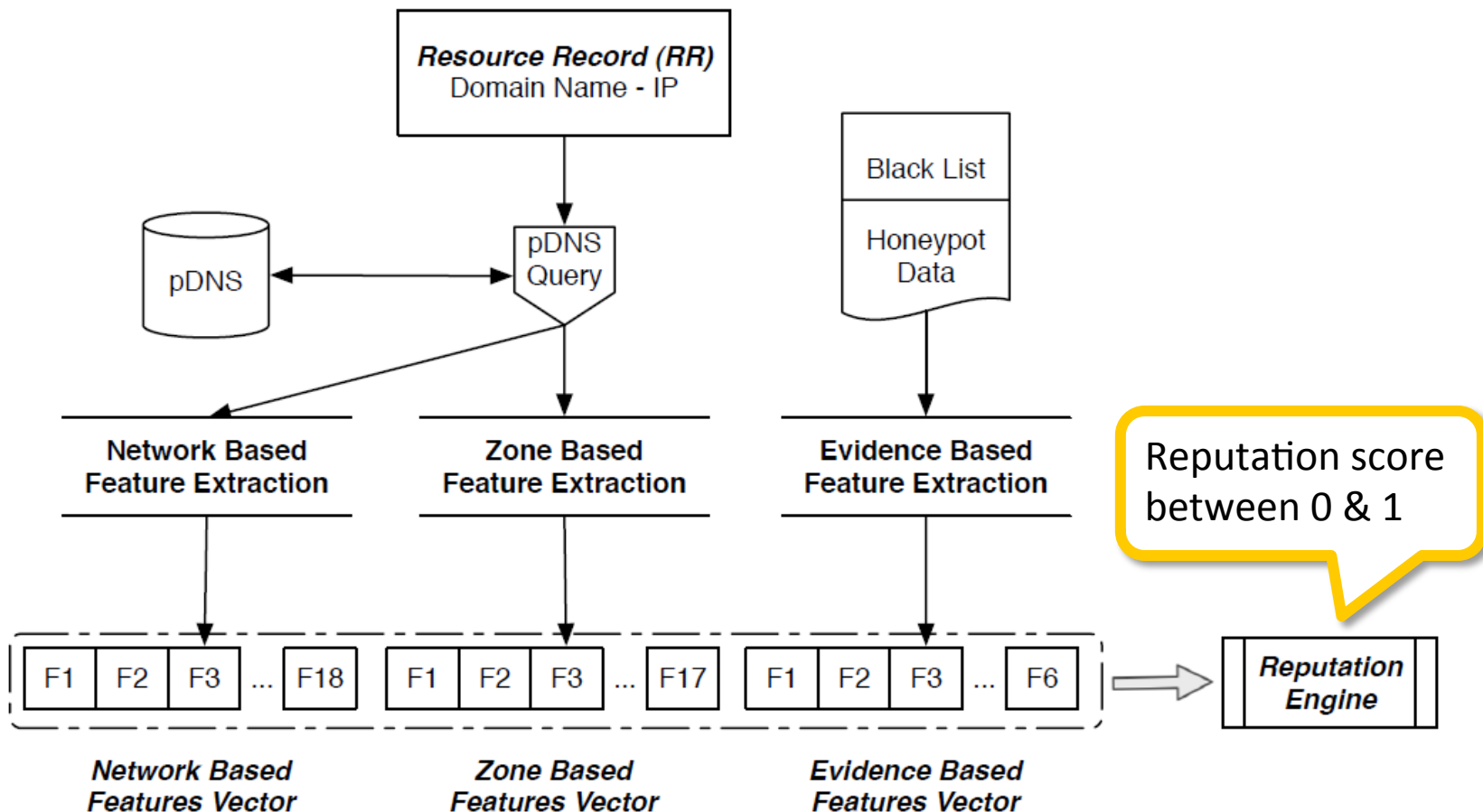
IP or Domain, by themselves, is of limited value in a threat context

- **Newest approaches: comprehensive reputation for DNS**
  - Notos
  - Exposure
- **Notos**
  - Outputs reputation scores for domains.
  - Use network and zone based features
  - Threat-oriented learning system
- **High fidelity classification and scoring**
  - very low FP% (0.3846%) and high TP% (96.8%).
  - Spot fraudulent domain names weeks before appearance on blacklists



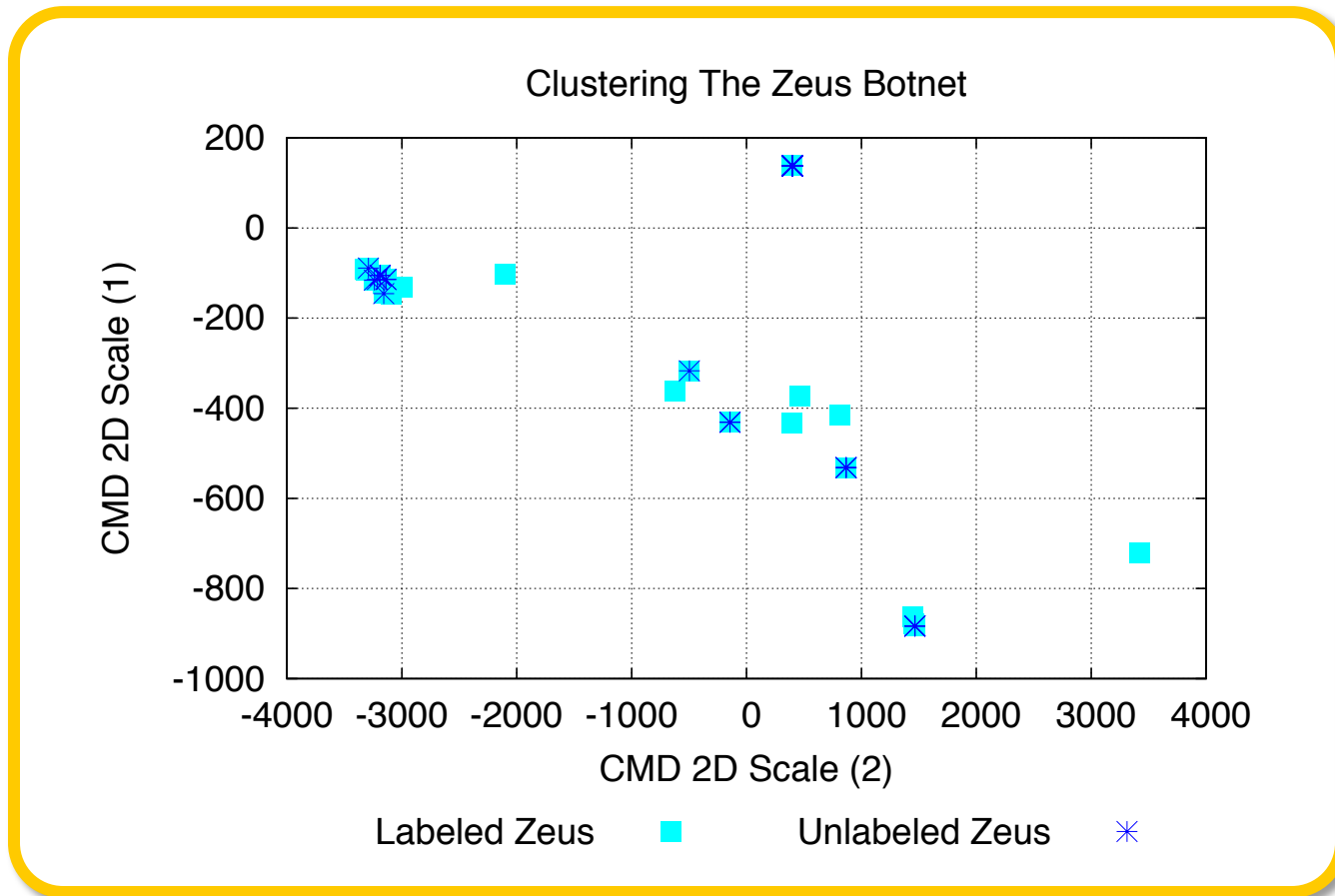


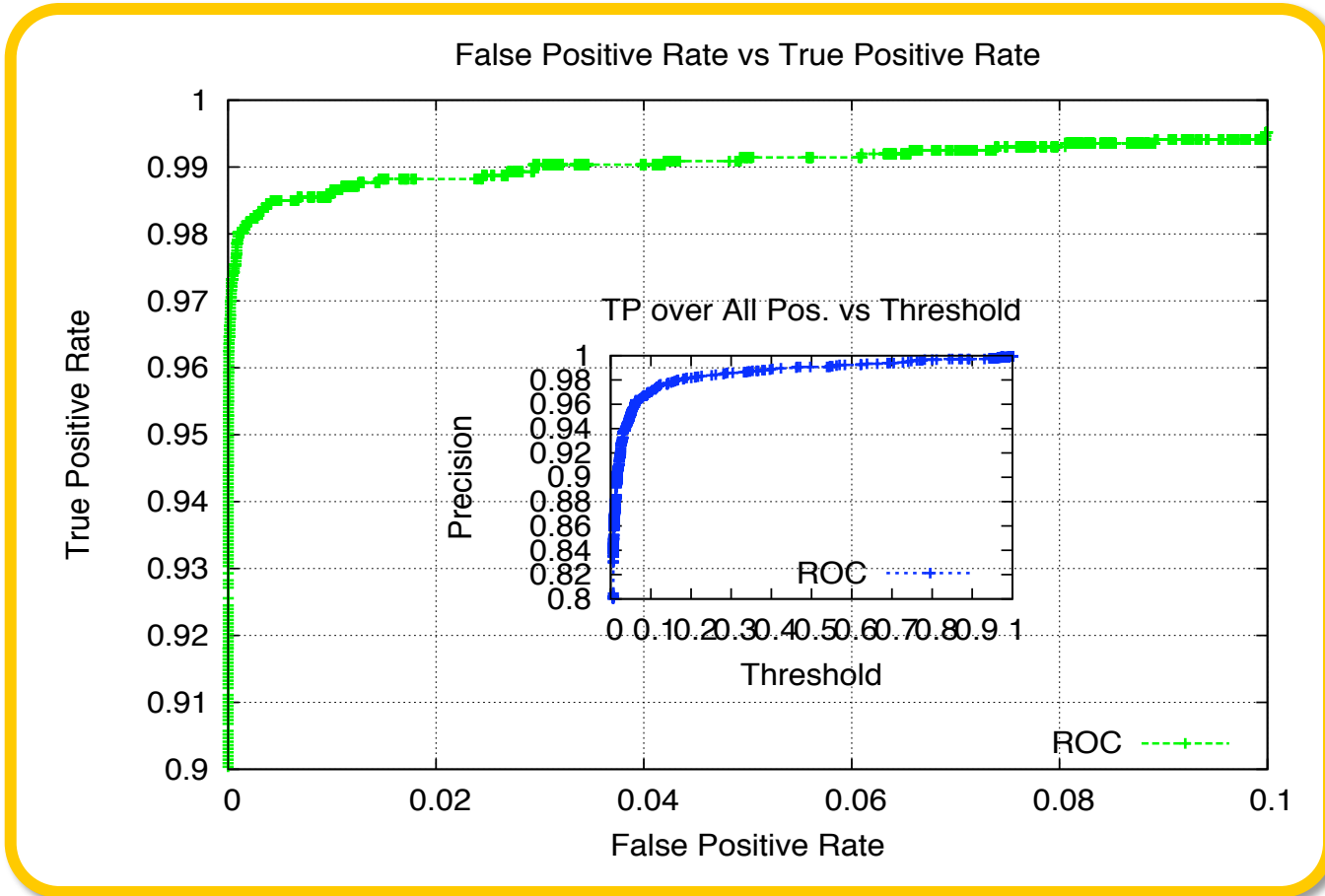
# Notos Features Overview



These 3 vectors are: *Network Based Feature Vector [18]*, *Zone Based Feature Vector [17]* and the *Evidence Based Feature Vector [6]*

- Labeled and unlabeled RRs clustering results from Zeus related domain names





FP%=0.3849% and TP%=96.8%.



# Conclusions

Light at the end of the tunnel

- **Adrenaline injection for blacklists**
  - Adding time element – depreciate “dated” views
  - Reduces “false positives”
- **Transition from static to dynamic reputation**
  - Requires real-time feeds and updates
  - API vs list approach
- **Movement away from domain/IP**
  - “holistic maps” of the Internet & threats
  - Dynamic reputation for DNS



- **Past reputation approaches have been binary**
  - On the list = bad
  - Not on the list = Ok/unknown/don't care
- **Reputation scores**
  - Scoring of malicious intent
  - “Forecasting” criminal usage
  - Threat category determination





**Thank You!**

Any questions?

**Gunter Ollmann**  
VP Research, Damballa  
[gunter@damballa.com](mailto:gunter@damballa.com)