DNSBL Quiz

Match the DNSBL level with its description:

E	White
C	Black
B	Grey
D	Yellow
A	NoBL

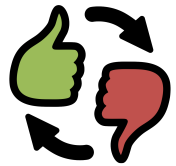
A. This IP address does not send spam, and should not be blacklisted. But it is not fully trustworthy.

B. This IP address is not directly involved in spamming but is associated with spam-like behaviors

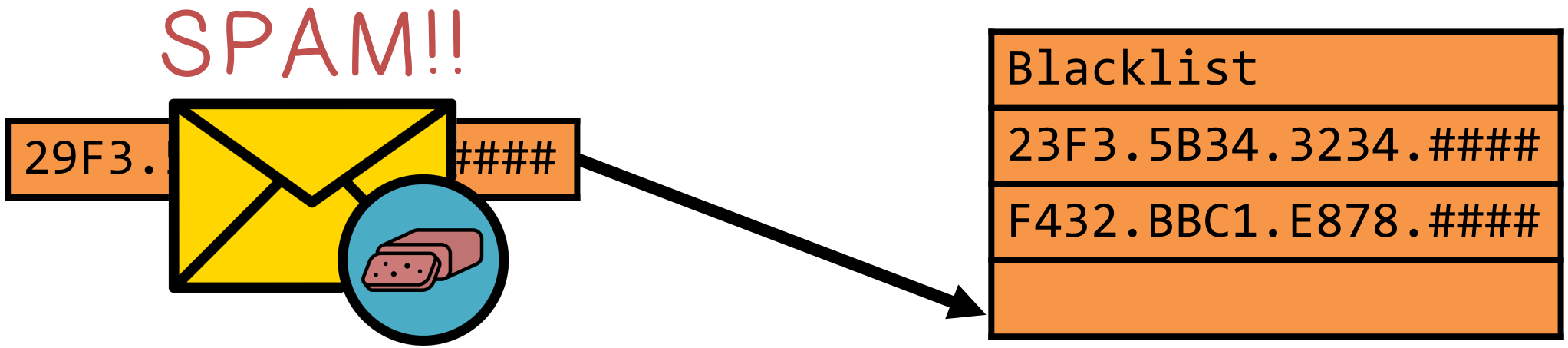
C. No trust in this IP address

D. This IP address is known to produce spam and non-spam email

E. Complete trust in this IP address



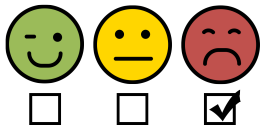
Motivation for Reputation



New IP addresses are trusted with the static blacklist model.

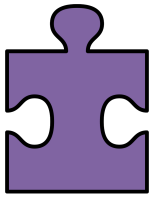
Static Blacklist Model: Innocent until proven guilty

Everyone is suspect until proven innocent.



New Blocklist Model Criteria

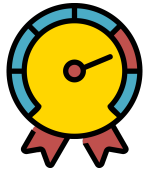
Motivation	• Static DNSBL increasingly ineffective • Need a dynamic, comprehensive reputation system outputs reputation scores for domains
Intuitions	• Legitimate uses of domains/sites are different from botnet uses, and the differences can be observed in DNS query traffic • Patterns/reputation of Requesters, Resolved IPs, Network providers
Approach	• Extract temporal and statistical features from DNS traffic, compute/learn models



DNS Quiz

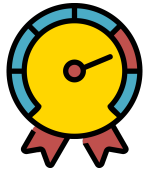
Match the malicious application with its DNS characteristic.

C	Botnets(B),	A. Anonymously registered domains
A	Spyware(S),	B. Disposable domains
B	Adware(A)	C. Short lived domains



NOTOS

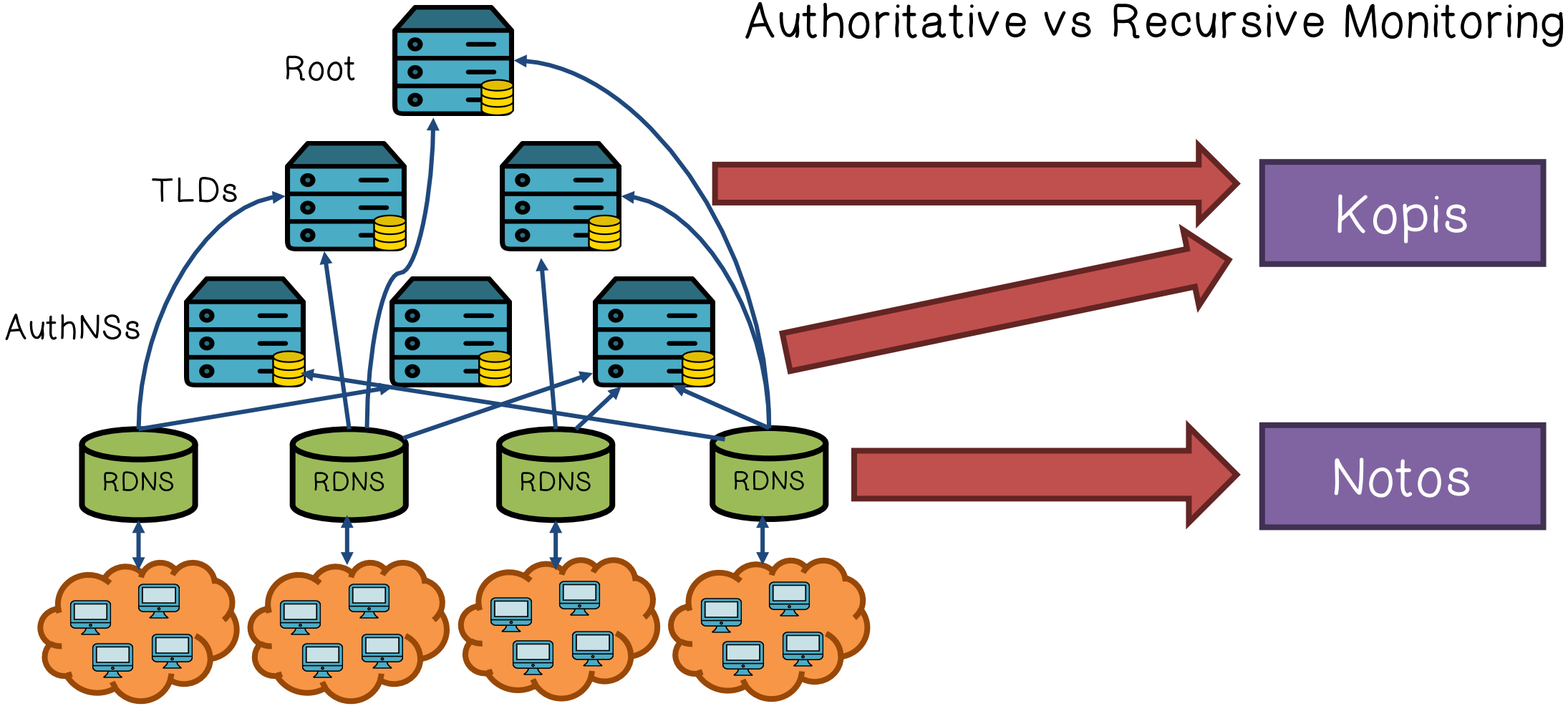
- Notos: a system that dynamically assigns reputation scores to domain names
- Network and zone based features capture the characteristics of resource provisioning, usages, and management of DNS domains
- Models of legitimate and malicious domains for computing reputation scores for new domains
- Accuracy: can correctly classify new domains with a very low FP% *(0.3846%)* and high TP% *(96.8%)*
- Predictability: able to detect and assign a low reputation score to fraudulent domain names, several days or even weeks before they appear on static blacklists

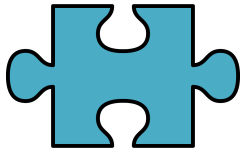


Kopis

- Passive monitoring in the upper levels of the DNS hierarchy; Internet-wide visibility
- Analyze streams of DNS queries and responses at AuthDNS or TLD servers, and extracts a set of statistical features and trains a model
- Accuracy: high TP% *(98.4%)* and low FP% *(0.3%)*
- Predictability: able to identify newly created and previously unclassified malicious domain names weeks before they were listed in any blacklist
- Detected a DDoS botnet rising in networks within China almost one month before it propagated within other countries

Kopis vs. Notos





Malicious Domain Names Quiz

List the types of characters a malicious domain name detection program should look for in a domain name.

1. Number of characters
2. Number of hyphens
3. Number of digits

Notation and Terminology

RR	Resource Record	www.example.com 192.0.32.10
2LD, 3LD	2nd and 3rd level domain	2LD = example.com 3LD = www.example.com
RHIPs	Related Historic IPs	All "routable" IPs historically mapped with the domain name in the RR or any domain name under the 2LD and 3LD
RHDNs	Related Historic Domains	All fully qualified domain names (FQDN) that historically have been linked with the IP in the RR, its corresponding CIDR and AS
ADNT	Authoritative domain name tuple	The requester (or RDNS), the domain name and the RDATA

Data Used in Research

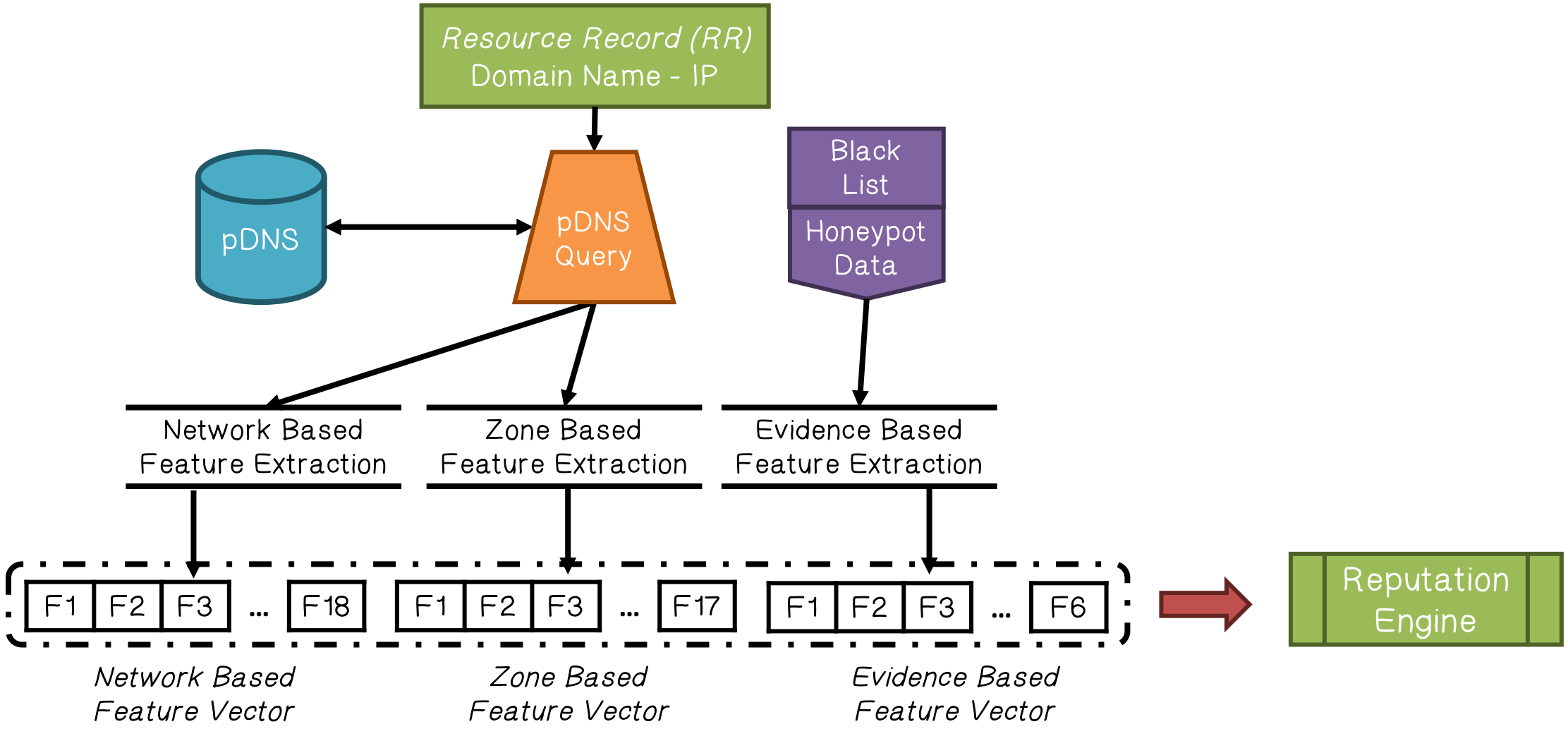
Passive DNS *(pDNS)* data collection is the harvesting of successful DNS resolutions that can be observed in a given network

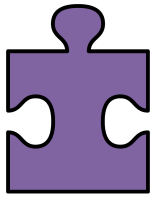
Passive DNS database contains traffic from several ISP sensors and data repositories

- Observed that different classes of zones demonstrate different passive DNS behaviors

Obtained authoritative DNS traffic from 2 large authoritative DNS servers (AuthNS) and the Canadian TLD

Statistical Features of Notos





DNS Database Quiz

The information extracted from the pDNS database can be grouped into three categories. Match the category to its definition.

C Network-based features(N),

B Zone-based features(Z),

A Evidence-based features (E)

A. The number of distinct malware samples that connected to any of the IPs.

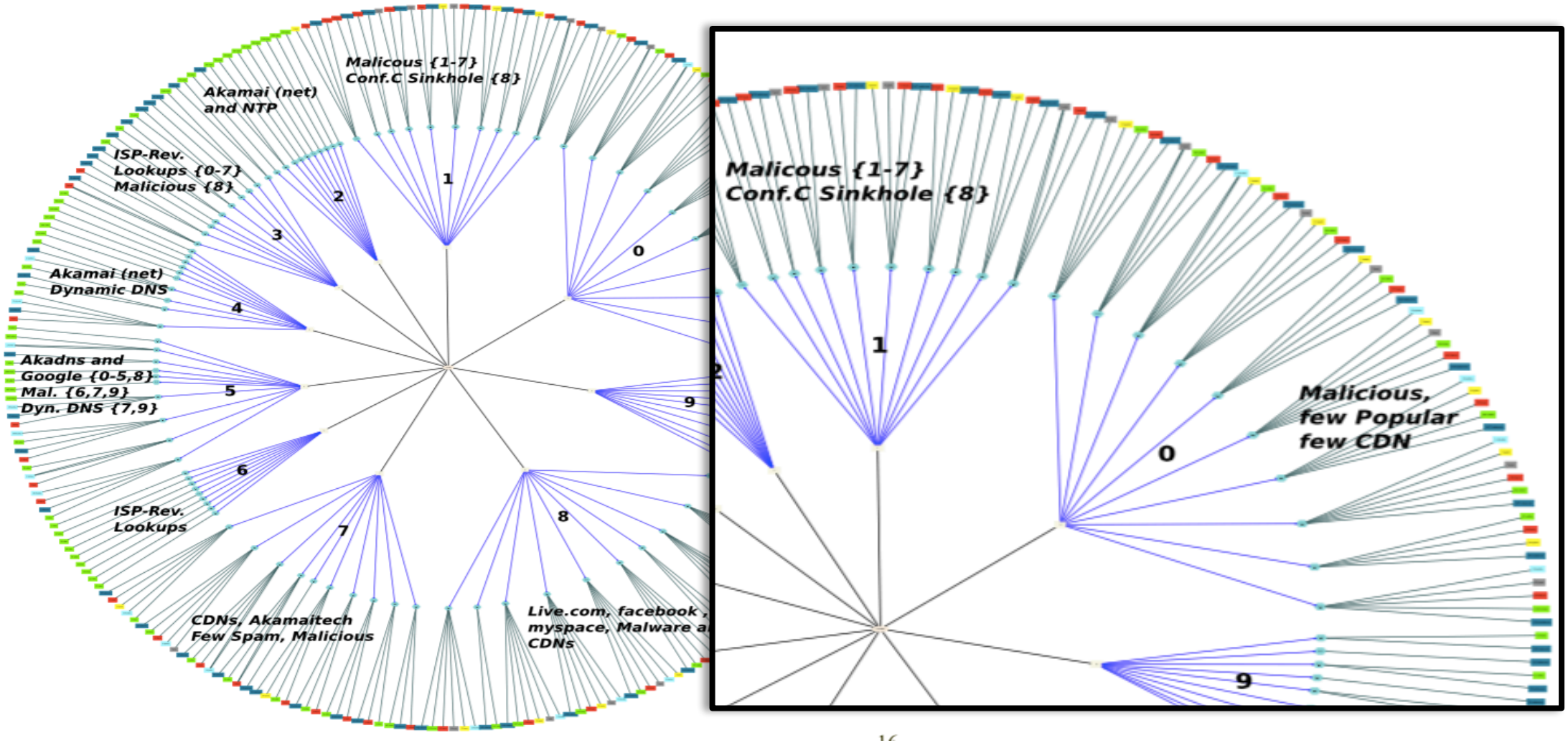
B. The average length of domain names, the occurrence frequency of different characters, etc.

C. Quantities such as the total number of IPs historically associated with the diversity of their geographical locations, the number of distinct autonomous systems, etc.

Notos Statistical Features

Network-Based Features:	• Extracted from the set RHIPs • E.g., the total number of IPs historically associated with a domain, the diversity of their geographical location, the number of distinct autonomous systems (ASs) in which they reside, etc.
Zone-Based Features:	• Extracted from the set RHDNs. • E.g., the average length of domain names in RHDNs, the number of distinct TLDs, the occurrence frequency of different characters, etc
Evidence-Based Features:	• E.g., the number of distinct malware samples that contacted the domain, and the same for any of the resolved IPs, etc.

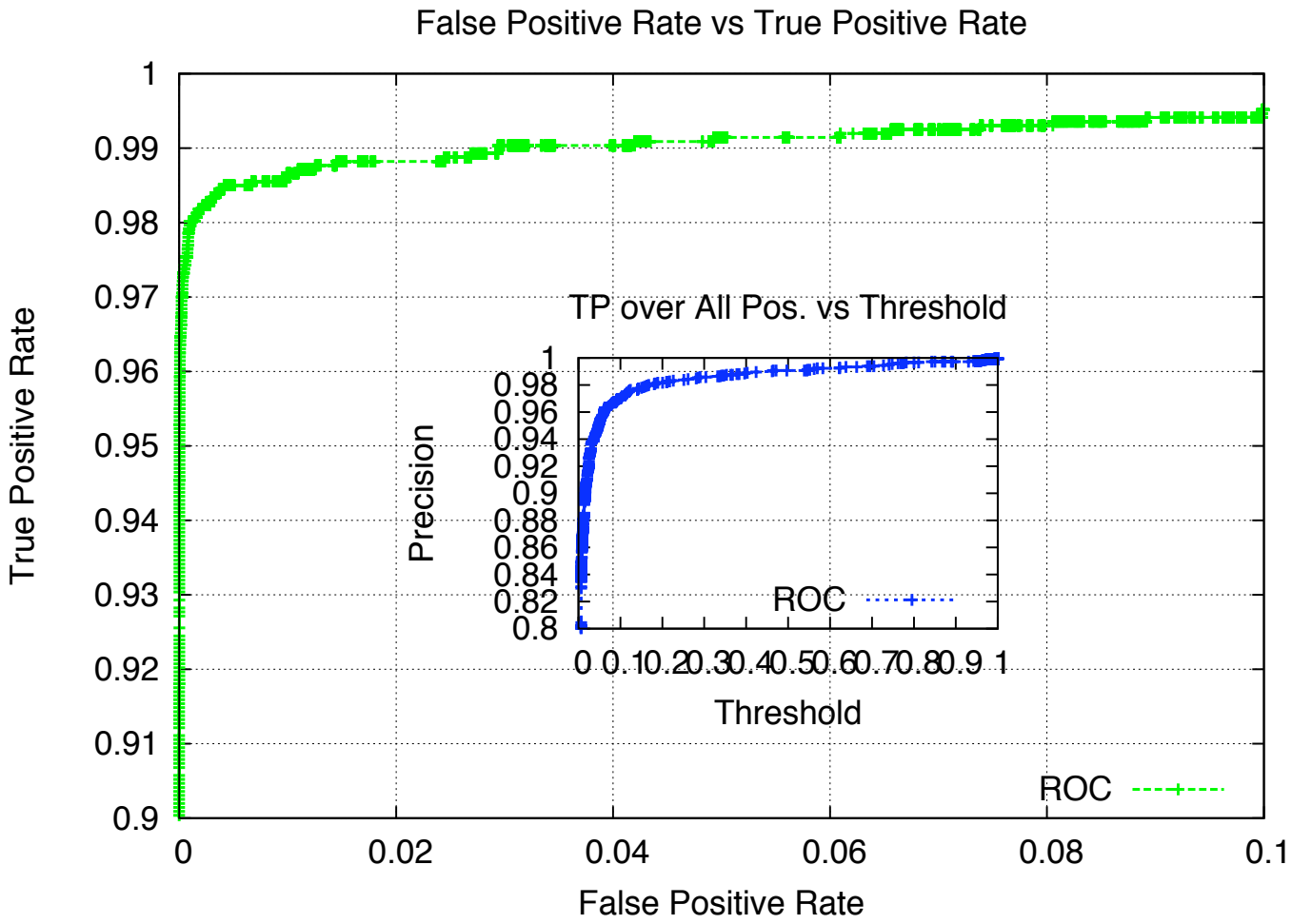
Clusters of DNS Domains



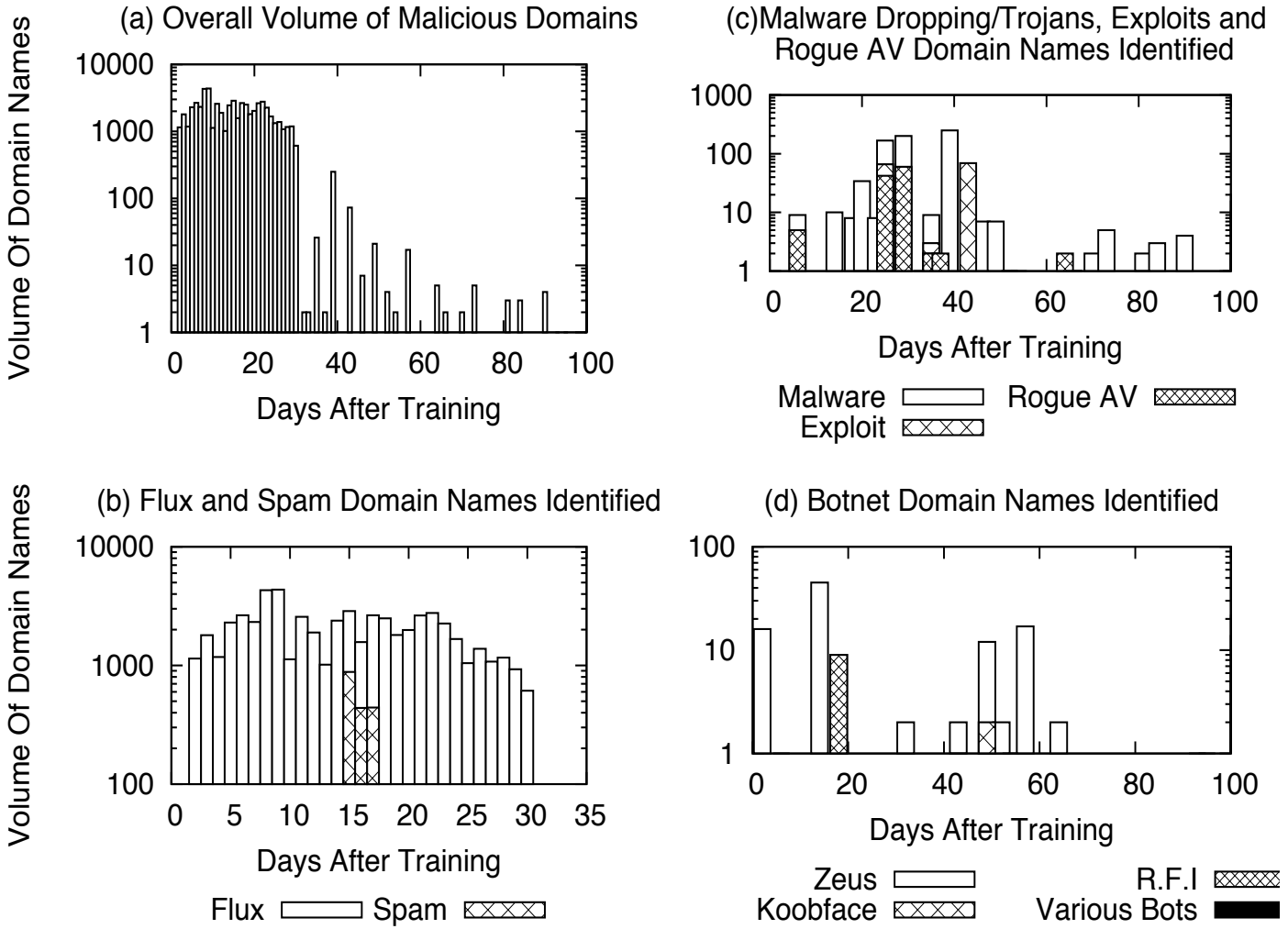
Notos Reputation Function

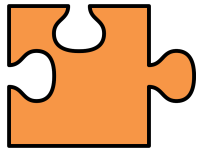
Given domains known to be legitimate and malicious:

- Gather Notos features for each domain
- Malicious domain label: 1
- Legitimate domain label: 0
- Learn a function that given the Notos feature vector for a domain, outputs a label (0 or 1)
- Reputation score is the "confidence" of the label (or, the probability that the domain is malicious)



Notos Reputation Function





Dynamic Detection Quiz

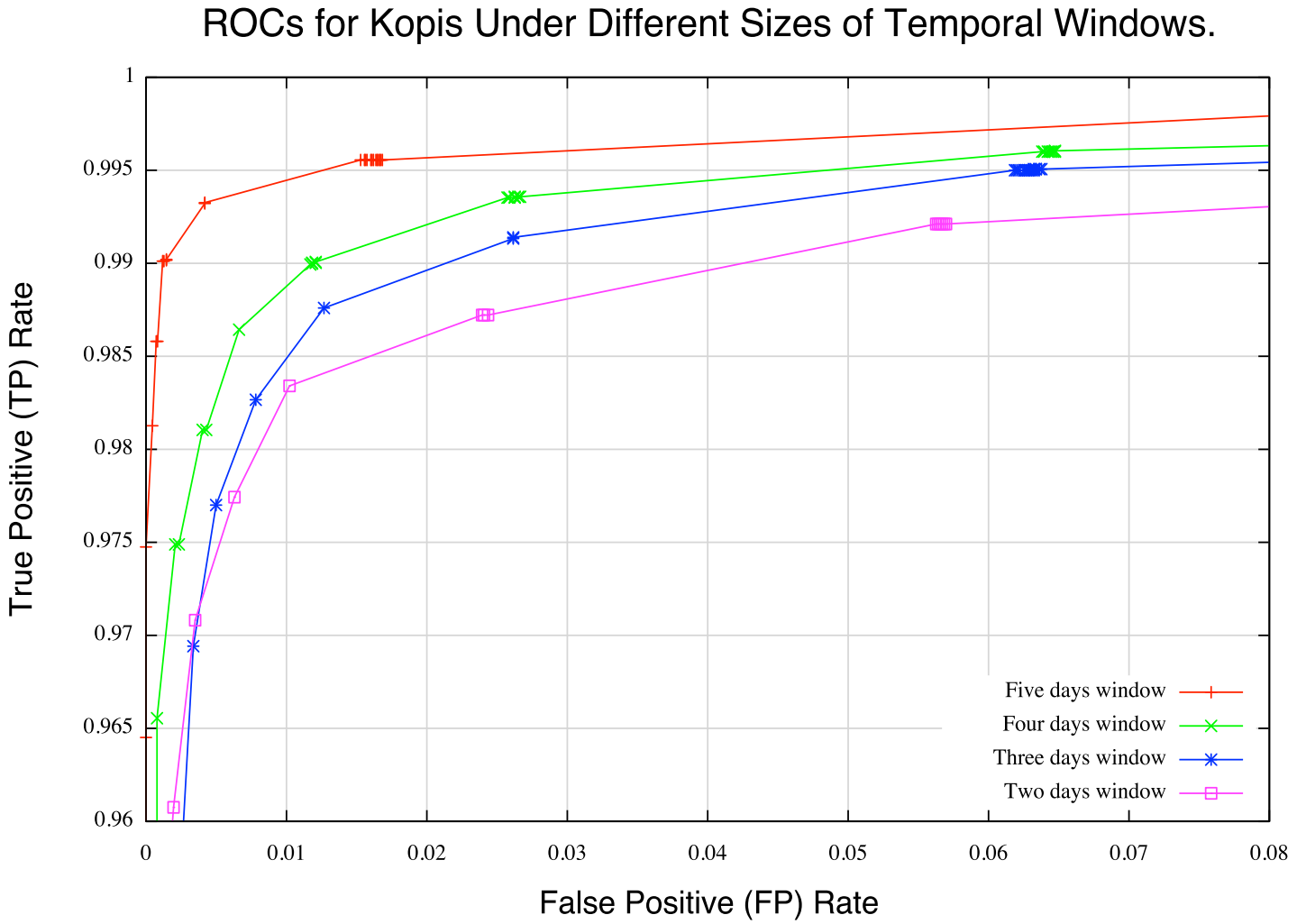
Check all the true statements that pertain to A dynamic malware-related domain detection system. A dynamic malware-related domain detection system should:

- [x] Have global visibility into DNS request and response messages
- [ ] Not be able to detect malware domains before the infection reaches a local network
- [x] Not require data from other networks
- [x] Be able to detect malware-related domains even if there is no reputation data.

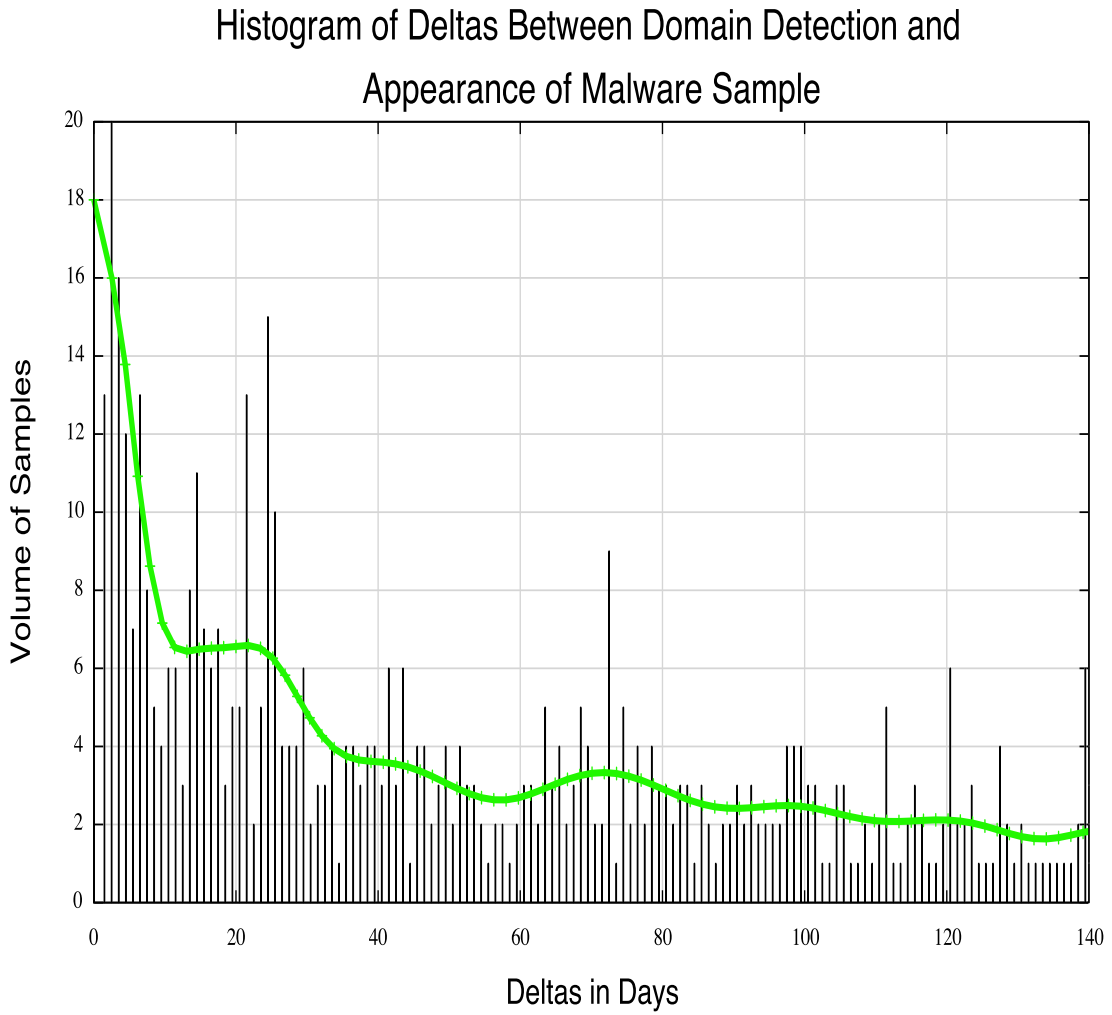
Kopis Statistical Features

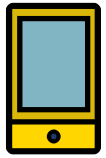
Requester Diversity (RD)	• Characterize if the machines (e.g., RDNS servers) that query a given domain name are localized or are globally distributed (based on BGP prefixes, AS numbers, country codes, etc.)
Requester Profile (RP)	• Distinguish between requesters located in ISP/small business and home networks • Assign a higher weight to RDNS servers that serve a large client population because a larger network would have a larger number of infected machines.
Resolved-IPs Reputation (IPR)	• Whether, and to what extent, the IP address space pointed to by a given domain has been historically linked with known malicious activities, or known legitimate services

Kopis Detection Performance



Predictability





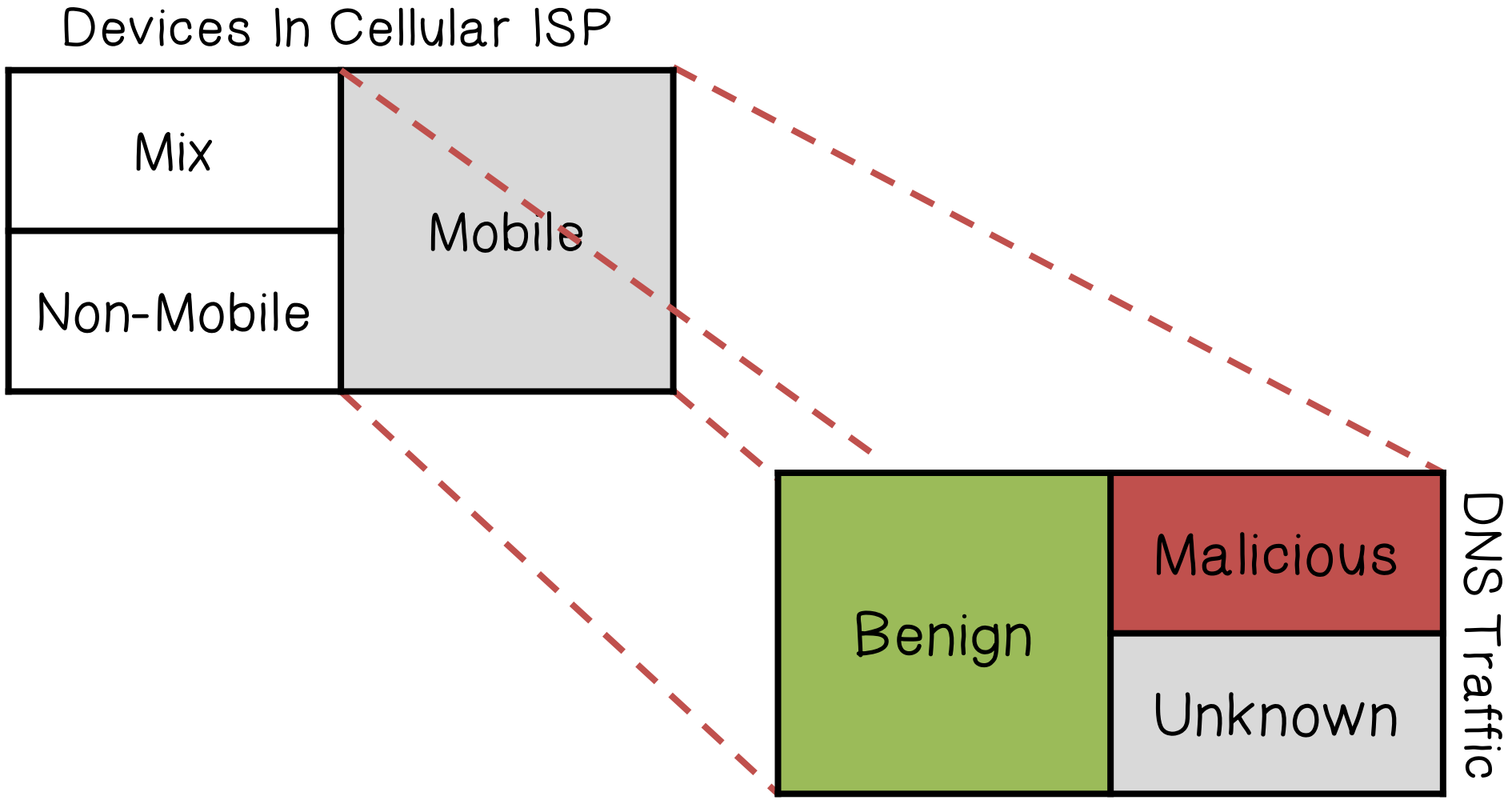
Study of Mobile Malware Prevalence

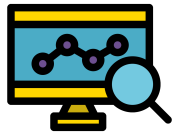
Motivation	• Much work on mobile malware has been on analysis of (malicious) mobile apps • But, how prevalence are infections on mobile devices?
Intuitions	• The (malicious) mobile web is a part of the (malicious) web • Mobile malware uses similar infrastructure (C&C) techniques as non-mobile/Internet malware
Approach	• Obtain DNS traffic in cellular network and identify domains looked up by mobile apps • Analyze information related to the Internet hosts pointed by these domains.

Key Data and Findings

- Three months of data from a major US cellular provider and a major US non-cellular ISP
- Known mobile malware samples remain rare in US: only 6,585 out of 380,537,128 devices, or 0.002%
- iOS vs. Android and other devices: equally likely to connect to suspicious domains

Methodology





Reputation Analysis

Use Notos to analyze the hosting infrastructures of the mobile domains

Obtain the host IPs pointed to by the mobile domains, for each IP, extract statistical features of:

- Related historic non-cellular domains
- Related historic mobile domains
- Malware association
- URLs for phishing and drive-by download
- Blacklisting incidents

Tainted Hosts and Platforms

Device platform	% Total Requests by mobile device	% Population requesting tainted hosts	% Total tainted host requests
iOS	31.6%	8.8%	33.2%
All others (Android, etc.)	68.4%	8.2%	66.8%

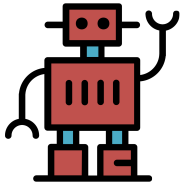
Mobile Malware Prevalence

Malware Family	# Associated Domains	# Devices
DroidDreamLight	3	44
DroidKungFu	1	6
FakeDoc	1	2145
Fatakr	1	151
GGTrackers	3	1
NotCompatible	3	762
Planton	4	286
Malware **β**	1	1
WalkInWat	1	95
Gone60	1	1

Botnet Takedown

With regards to botnets, select all the true statements:

- [ ] One of the more successful methods to taking down a botnet requires investigators to find and target each bot in the net
- [x] A proven method to stop botnets requires isolating the C&C domain from the botnet
- [ ] With regards to takedowns, P2P-based networks are much easier than C&C networks



Botnet Takedowns

Takedowns are: *ad-hoc*, *of arguable success*, are performed *without oversight*

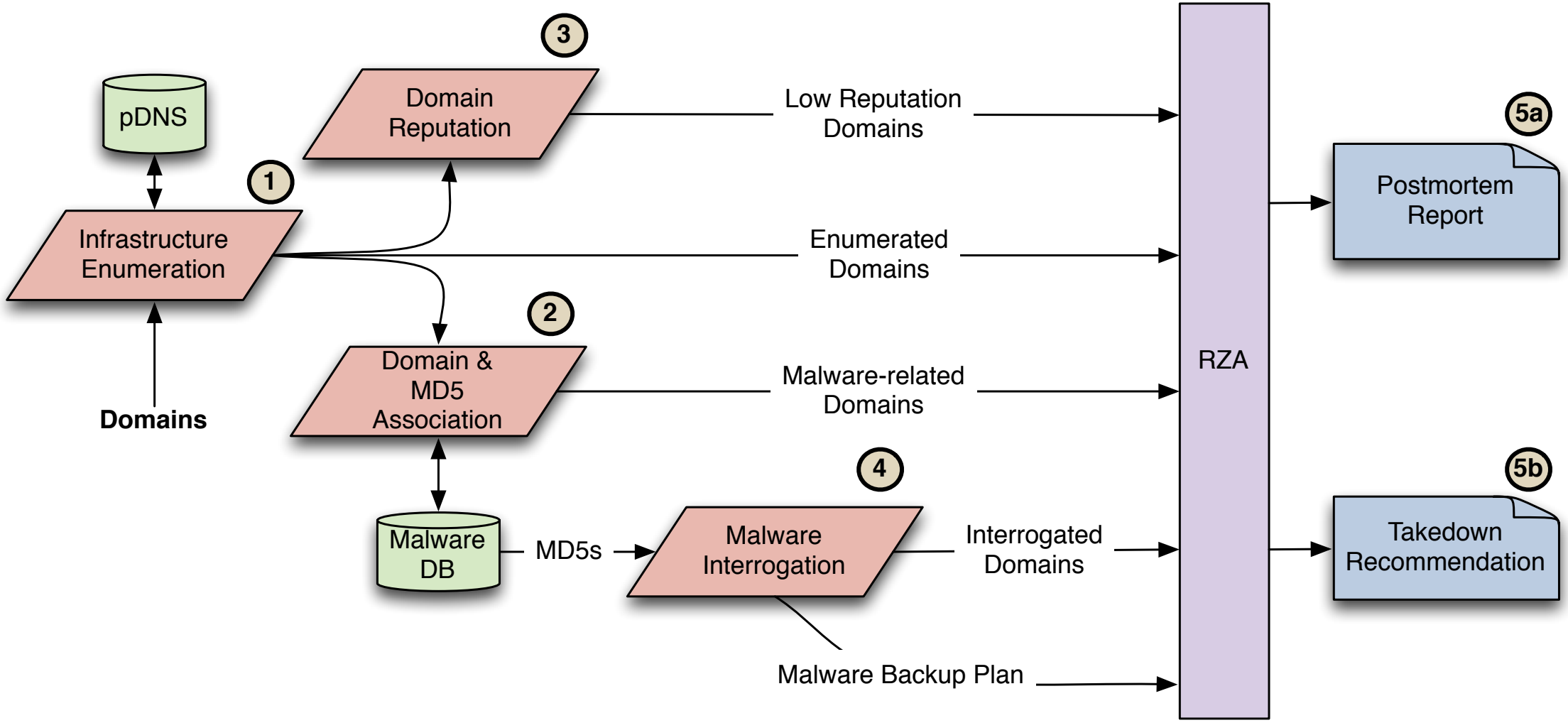
System goal: add rhyme/reason to takedowns

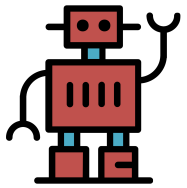
- *evaluate* previous takedown attempts, and
- *recommend* and *inform* on/for future takedowns

High-level idea: push our knowledge of infrastructure towards completeness

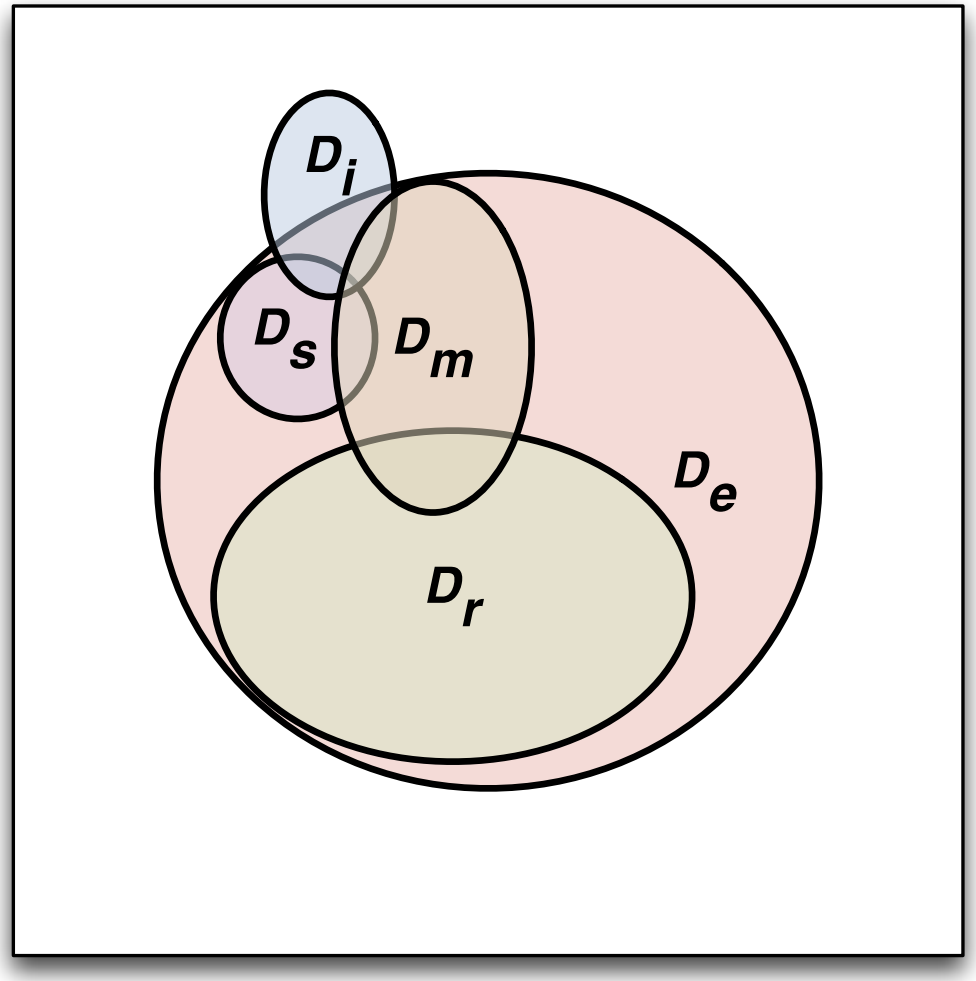
- *Network-side:* passive DNS
- *Malware-side:* malware backup infrastructure

Botnet Takedowns: RZA Overview





Botnet Takedowns: RZA Overview



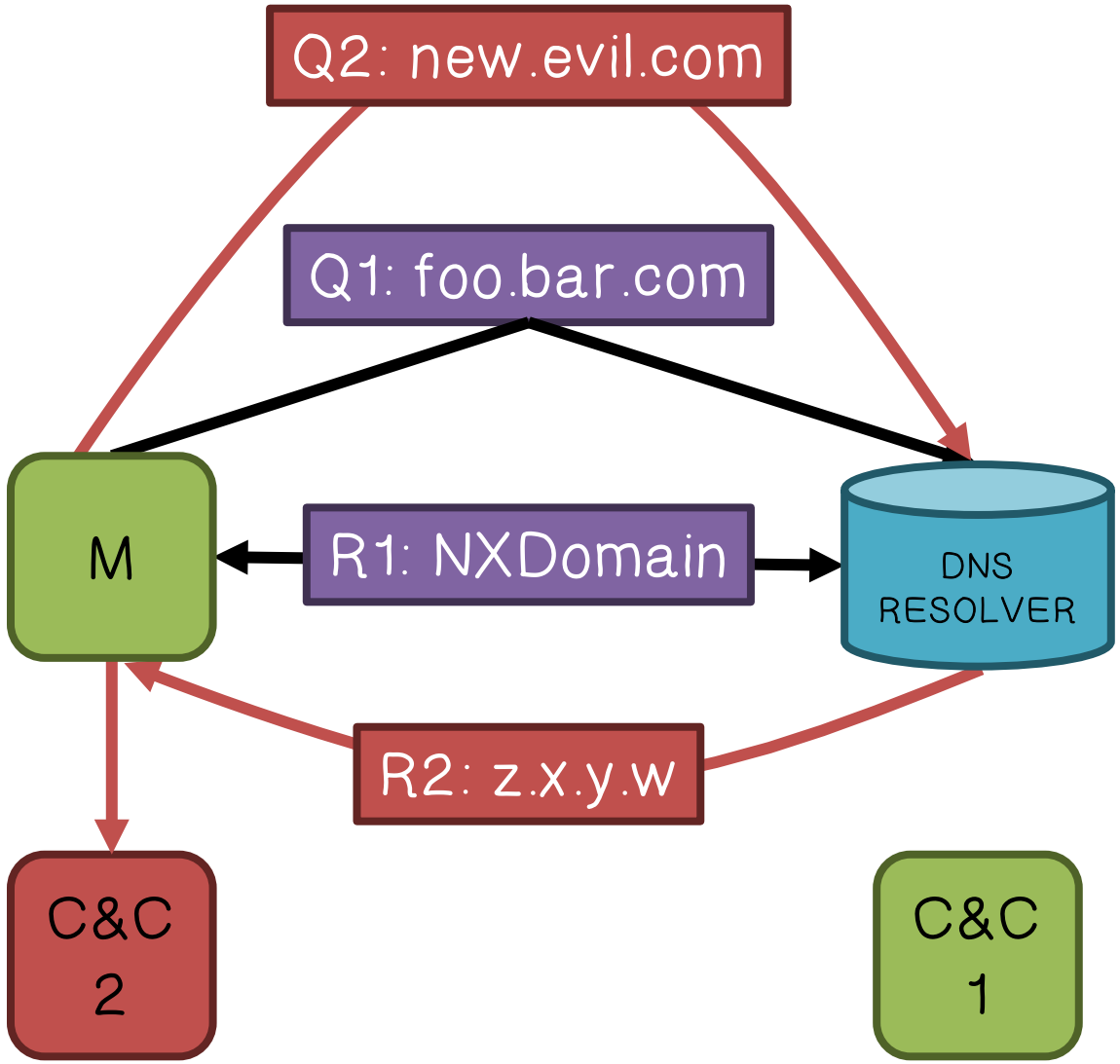
D_s: seed domains

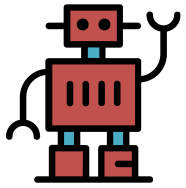
D_e: enumerated domains

D_r: low reputation domains

D_m: malware-related domains

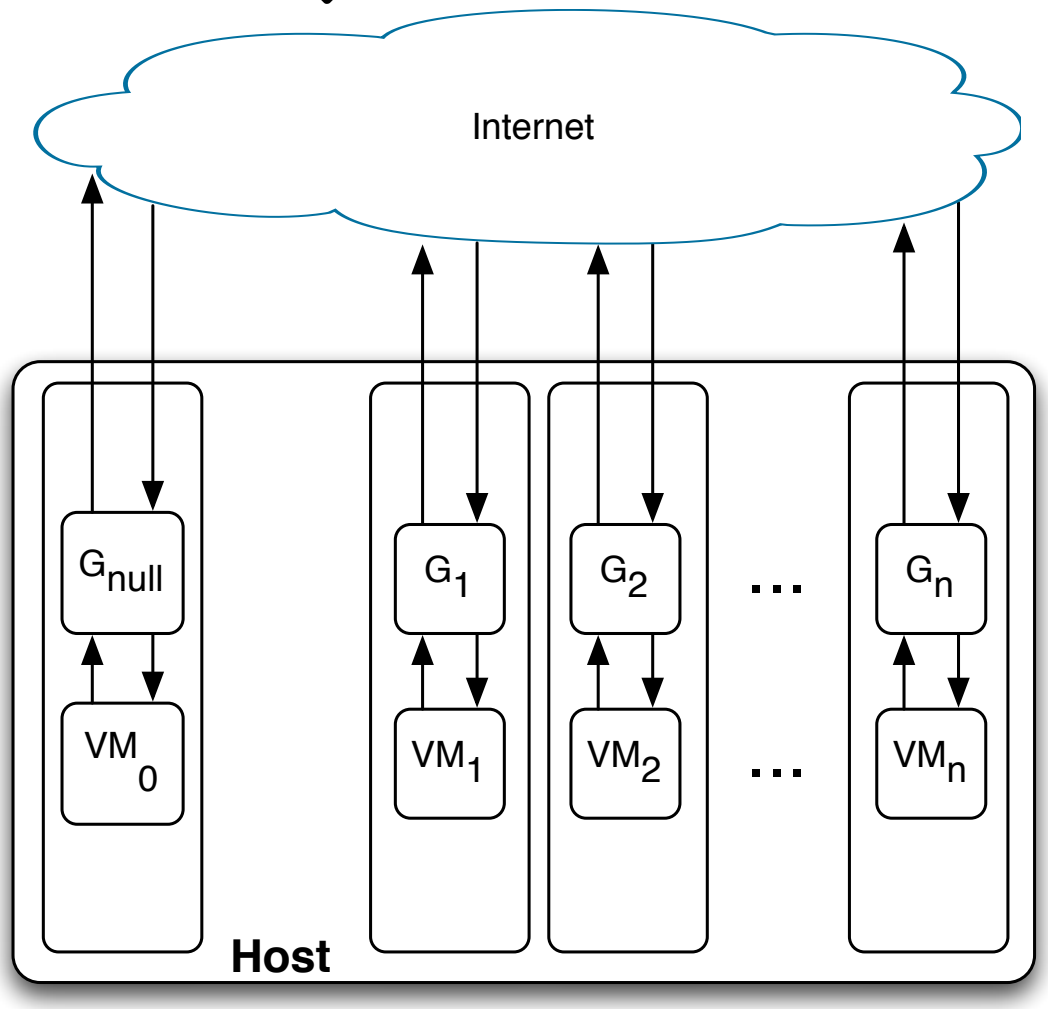
D_i: malware interrogation domains





Botnet Takedowns: RZA Overview

RZA Malware Interrogation



- *Game* malware to present primary infrastructure failure
- DNS/TCP packet manipulation (NXDomain/TCP RST)
- *Automatically* determine backup behaviors

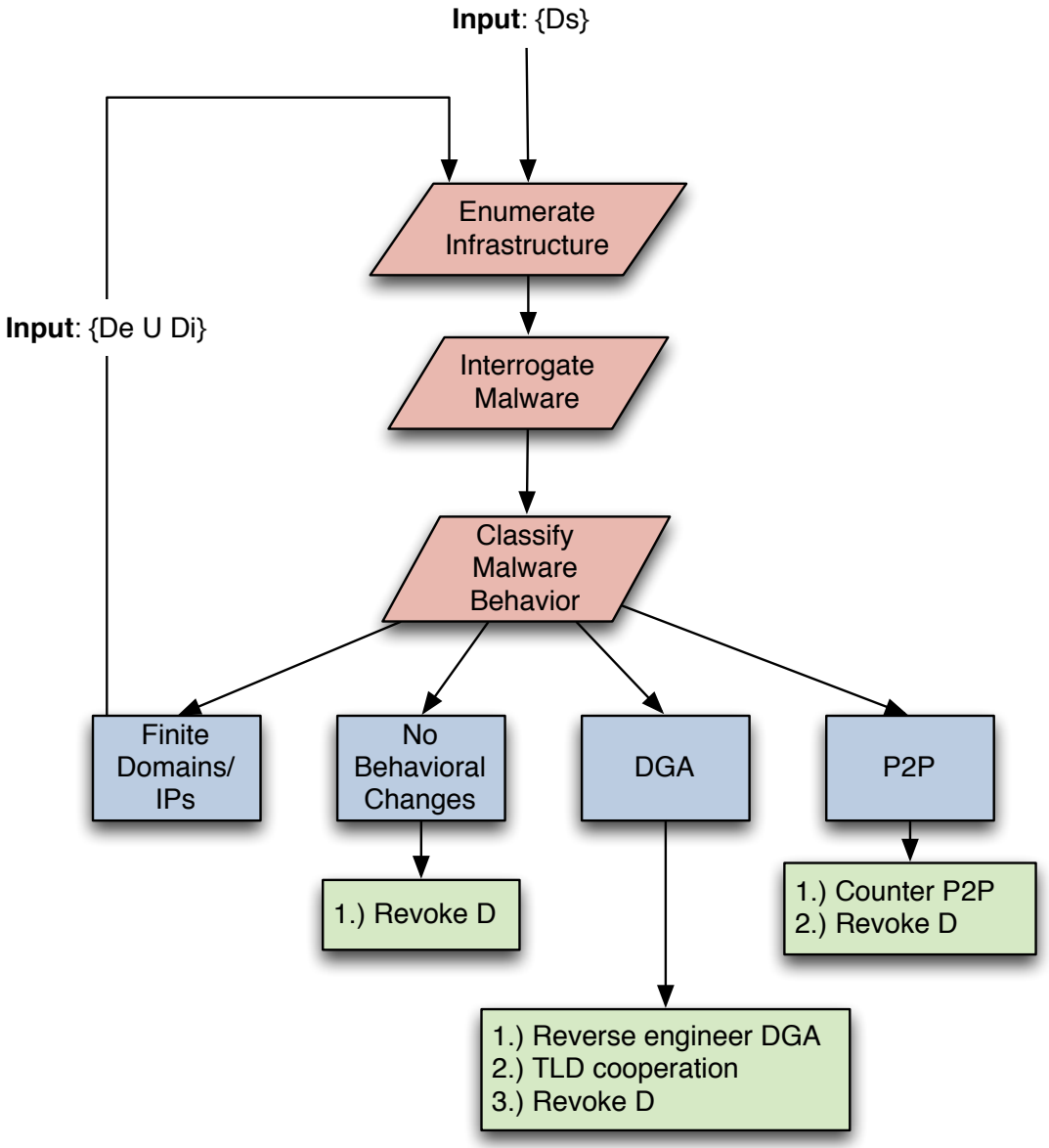
RZA Malware Interrogation

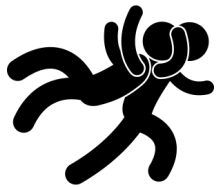
If malware is presented with unavailable infrastructure:

- Retries hardcoded IPs/domains,
- Tries to reach a *finite* set of IPs/domains, or
- Tries to reach an *increasing number* of IPs/domains (DGA/P2P)

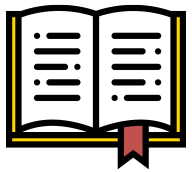
Manipulate fundamental protocol packets to convince malware its primary network asset is unavailable

- DNS and TCP
- Easy to add additional protocols





RZA Takedown



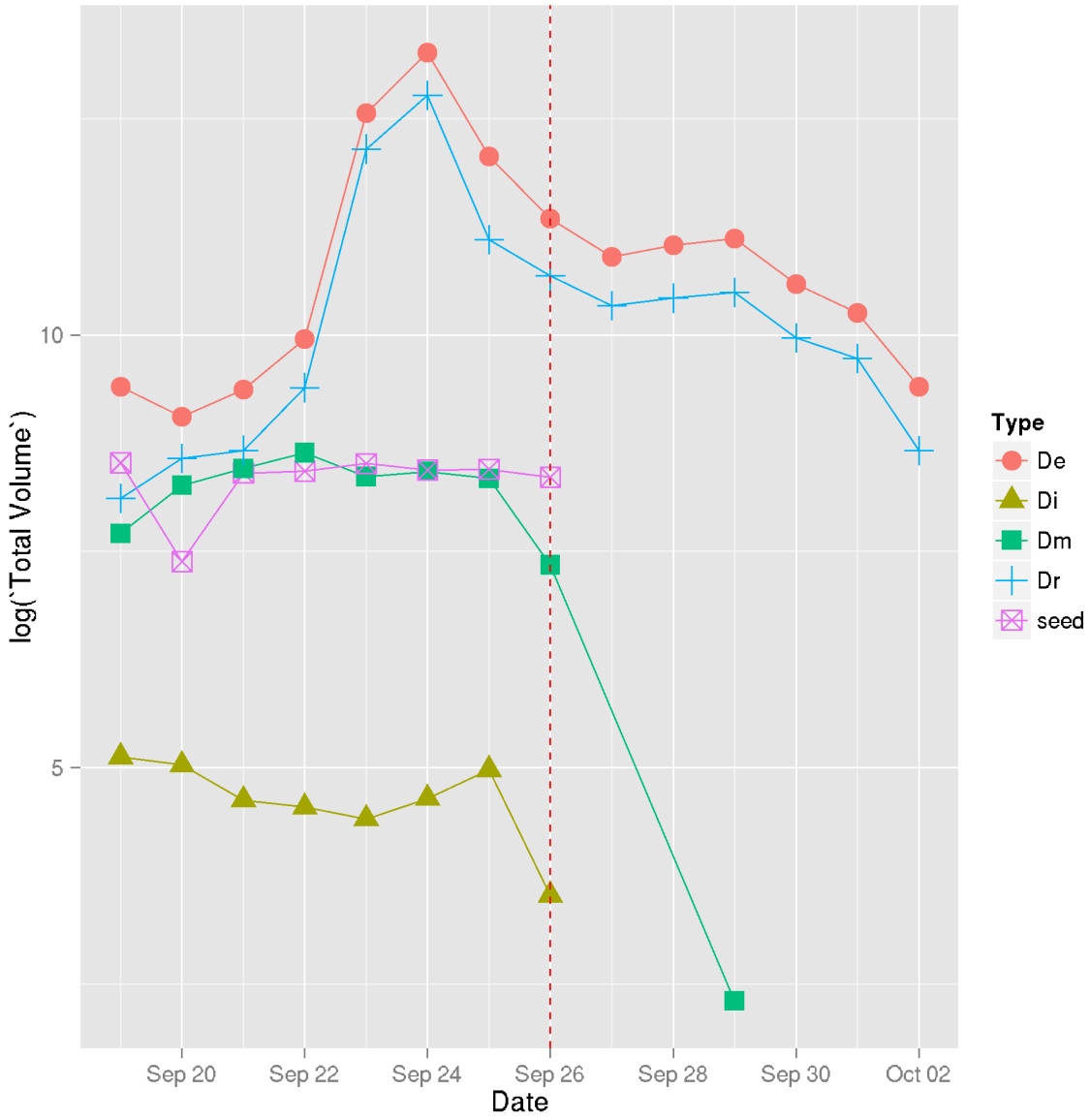
RZA Studies

Postmortem study: analysis of *Kelihos*, *ZeuS*, and *3322.org/Nitol* takedowns

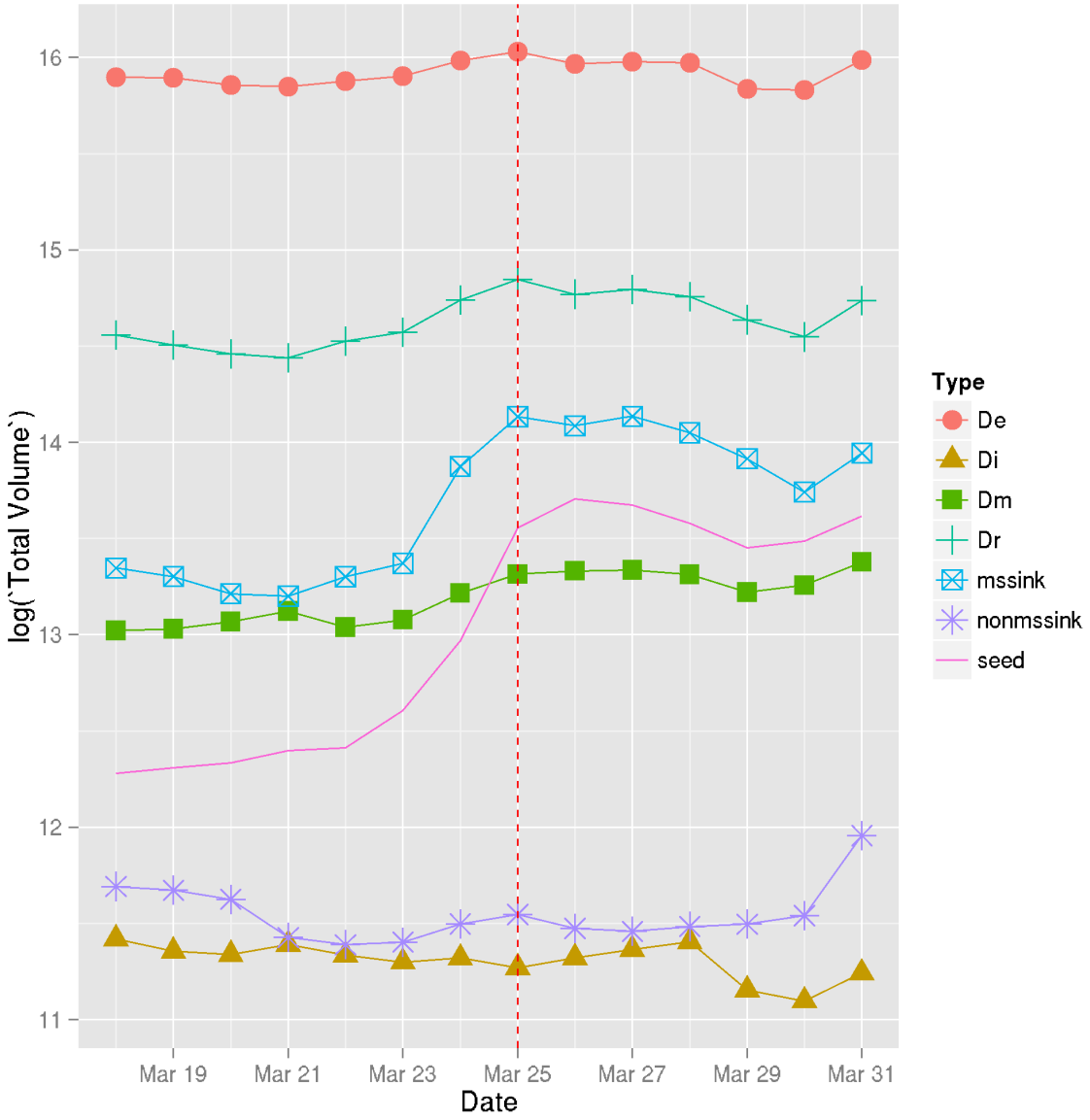
- Use lookup volume to show activity to infrastructure

Takedown study: analysis of 45 active botnet C&Cs

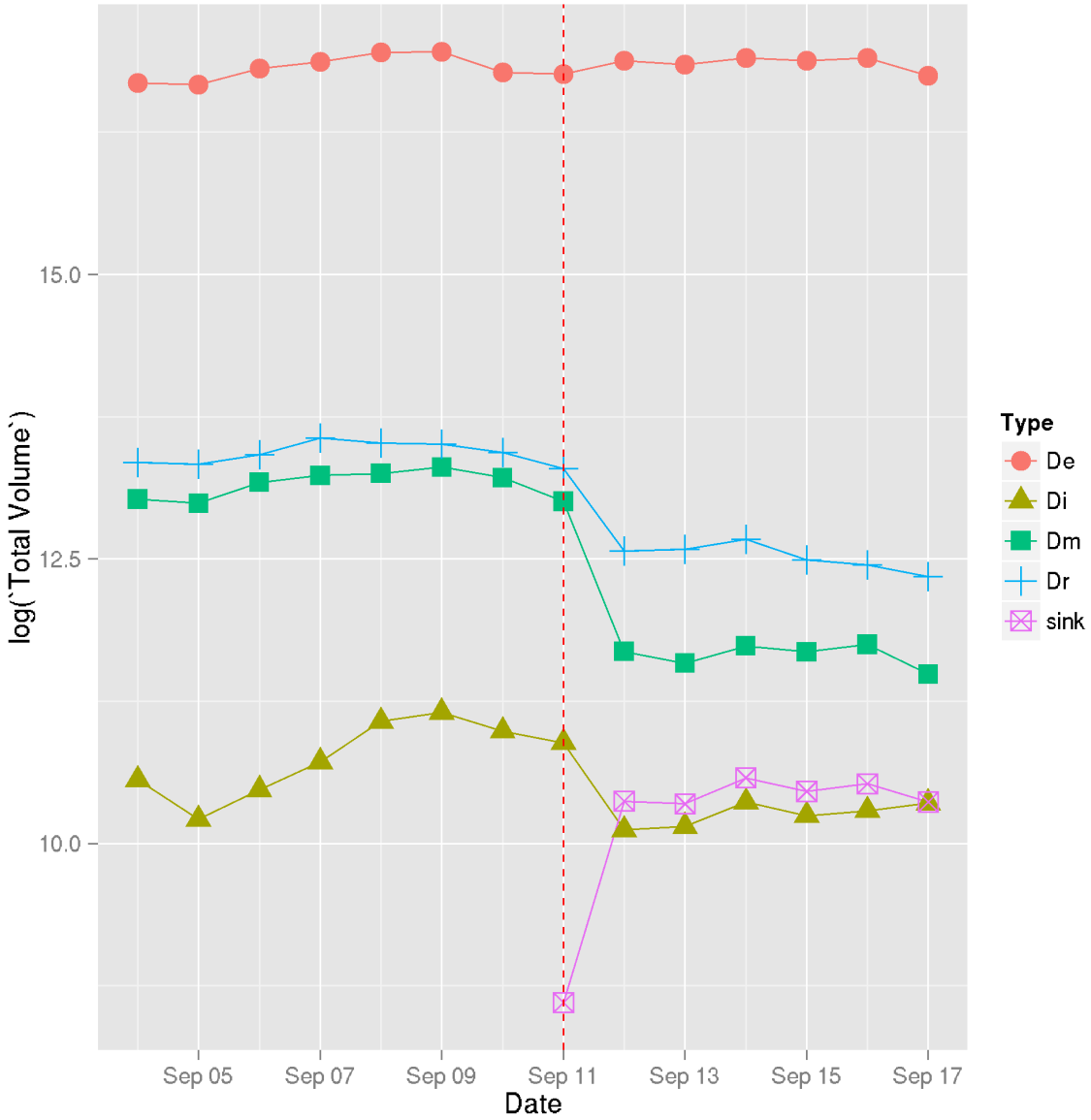
- Can we take them down?

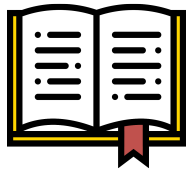


RZA Studies: Postmortem Kelihos



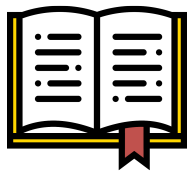
RZA Studies: Postmortem Zues





RZA Studies: Postmortem

3322.org/Nitol



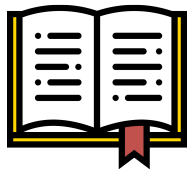
RZA Takedown Study

Of the 45 botnets:

- 2 had DGA-based backup mechanism
- 1 had P2P-based backup mechanism
- 42 susceptible to DNS-only takedown

Current drawbacks to takedown

- Ad-hoc
- Little oversight
- Arguable success
- All point to need for central authority



RZA Takedown Study

ICANN's UDRP/URS as example frameworks

- Criteria for takedown
- More eyes = more successes
- Test with new TLDs (much like w/ URS)