Building a Dynamic Reputation System for DNS

Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, and Nick Feamster

Georgia Institute of Technology
College of Computing
Atlanta, Georgia

August, 2010

Outline and Credits

- Problem Description and Motivation
- Preparation
  - Notation, Passive DNS trends and Anchor Classes
- Notos' Components
  - Network based profile modeling
  - Network and zone based profiles clustering
  - Reputation function
- Reputation Results
- Conclusions and Future Work

Special thanks to:

- Damballa
  - Passive DNS data, Malware and BL
- SIE@ISC
  - Passive DNS data
- Robert Edmonds
  - Many useful comments

Outline and Credits

- Problem Description and Motivation
- Preparation
  - Notation, Passive DNS trends and Anchor Classes
- Notos' Components
  - Network based profile modeling
  - Network and zone based profiles clustering
  - Reputation function
- Reputation Results
- Conclusions and Future Work

Special thanks to:

- Damballa
  - Passive DNS data, Malware and BL
- SIE@ISC
  - Passive DNS data
- Robert Edmonds
  - Many useful comments

Problem Description

- Malware families utilize large number of domains for discovering the "up-to-date" C&C address
- IP-based blocking technologies have well known limitation and are very hard to maintain
- DNSBL based technologies cannot keep up with the volume of new domain names used by botnet
  - Examples are Sinowal, Bobax and Conficker bots families which generate thousands on new C&C domains every day
- Detecting such type of **agile botnets** cannot be achieved by the current state of the art detection mechanisms

Problem Description

- Malware families utilize large number of domains for discovering the "up-to-date" C&C address
- IP-based blocking technologies have well known limitation and are very hard to maintain
- DNSBL based technologies cannot keep up with the volume of new domain names used by botnet
  - Examples are Sinowal, Bobax and Conficker bots families which generate thousands on new C&C domains every day
- Detecting such type of **agile botnets** cannot be achieved by the current state of the art detection mechanisms

Problem Description

- Malware families utilize large number of domains for discovering the "up-to-date" C&C address
- IP-based blocking technologies have well known limitation and are very hard to maintain
- DNSBL based technologies cannot keep up with the volume of new domain names used by botnet
  - Examples are Sinowal, Bobax and Conficker bots families which generate thousands on new C&C domains every day
- Detecting such type of **agile botnets** cannot be achieved by the current state of the art detection mechanisms

The Proposed Solution: Notos

- We designed Notos; a dynamic, comprehensive reputation system for DNS
- We constructed network and zone based statistical features that can capture the characteristics of domains
- These features enable Notos to learn the models of legitimate and malicious domains in order to compute reputation scores for new domains
- Notos can correctly classify new domains with a very low FP_{rate} (0.38) and high TP_{rate} (96.8), several days or even weeks before they appear on static blacklists

The Proposed Solution: Notos

- We designed Notos; a dynamic, comprehensive reputation system for DNS
- We constructed network and zone based statistical features that can capture the characteristics of domains
- These features enable Notos to learn the models of legitimate and malicious domains in order to compute reputation scores for new domains
- Notos can correctly classify new domains with a very low FP_{rate} (0.38) and high TP_{rate} (96.8), several days or even weeks before they appear on static blacklists

The Proposed Solution: Notos

- We designed Notos; a dynamic, comprehensive reputation system for DNS
- We constructed network and zone based statistical features that can capture the characteristics of domains
- These features enable Notos to learn the models of legitimate and malicious domains in order to compute reputation scores for new domains
- Notos can correctly classify new domains with a very low FP_{rate} (0.38) and high TP_{rate} (96.8), several days or even weeks before they appear on static blacklists

Some of the Previous Work ...

Passive DNS

- Florian Weimer with "Passive DNS replication"
- Zdrnja et al. "Passive monitoring of DNS anomalies"

IP Reputation and Blacklisting

- Shinha et al. "Shades of grey"
- Hao et al. with "Snare"
- Zhang et al. "Highly predictive blacklisting"
- Anderson et al. with "Spamscatter"
- Spamhaus: CIDR drop list, Team Cymru's Do-Not-Route

DNS Reputation and Blacklisting

- Holz ed al. on fast-flux service networks detection
- Felegyhazi's et al. "On the potential of proactive domain blacklisting"
- Surbl, SORBS, Zeus Tracker, etc

Some of the Previous Work ...

Passive DNS

- Florian Weimer with “Passive DNS replication”
- Zdrnja et al. “Passive monitoring of DNS anomalies”

IP Reputation and Blacklisting

- Shinha et al. “Shades of grey”
- Hao et al. with “Snare”
- Zhang et al. “Highly predictive blacklisting”
- Anderson et al. with “Spamscatter”
- Spamhaus: CIDR drop list, Team Cymru's Do-Not-Route

DNS Reputation and Blacklisting

- Holz ed al. on fast-flux service networks detection
- Felegyhazi's et al. “On the potential of proactive domain blacklisting”
- Surbl, SORBS, Zeus Tracker, etc

Some of the Previous Work ...

Passive DNS

- Florian Weimer with "Passive DNS replication"
- Zdrnja et al. "Passive monitoring of DNS anomalies"

IP Reputation and Blacklisting

- Shinha et al. "Shades of grey"
- Hao et al. with "Snare"
- Zhang et al. "Highly predictive blacklisting"
- Anderson et al. with "Spamscatter"
- Spamhaus: CIDR drop list, Team Cymru's Do-Not-Route

DNS Reputation and Blacklisting

- Holz ed al. on fast-flux service networks detection
- Felegyhazi's et al. "On the potential of proactive domain blacklisting"
- Surbl, SORBS, Zeus Tracker, etc.

Notation and Terminology

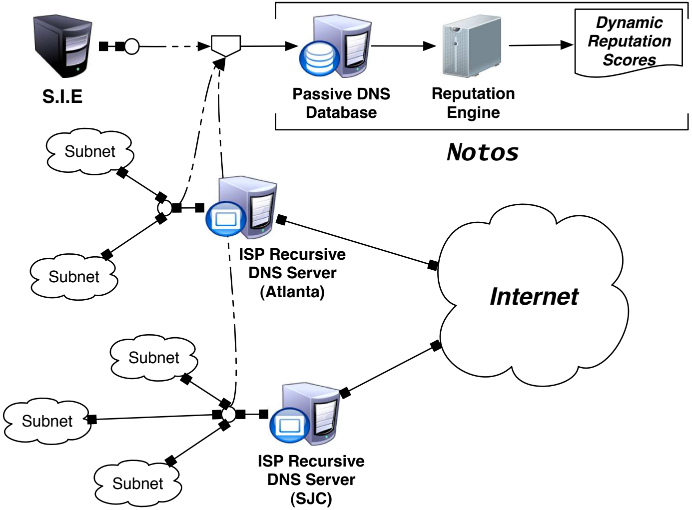
- What is a Resource Record (RR)?
  - `www.example.com 192.0.32.10`
- What is a 2^{nd} level domain (2LD) and 3^{rd} level domain (3LD)?
  - For the domain name `www.example.com`: 2LD is `example.com` and 3LD is `www.example.com`.
- What we define as Related Historic IPs (RHIPs)?
  - All "routable" IPs that historically have been mapped with the domain name in the RR, or any domain name under the 2LD and 3LD
- What we define as Related Historic Domains (RHDNs)?
  - All fully qualified domain names (FQDN) that historically have been linked with the IP in the RR, its corresponding CIDR and AS

Notation and Terminology

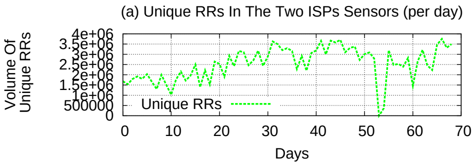
- What is a Resource Record (RR)?
  - `www.example.com 192.0.32.10`
- What is a 2nd level domain (2LD) and 3rd level domain (3LD)?
  - For the domain name `www.example.com`: 2LD is `example.com` and 3LD is `www.example.com`.
- What we define as Related Historic IPs (RHIPs)?
  - All "routable" IPs that historically have been mapped with the domain name in the RR, or any domain name under the 2LD and 3LD
- What we define as Related Historic Domains (RHDNs)?
  - All fully qualified domain names (FQDN) that historically have been linked with the IP in the RR, its corresponding CIDR and AS

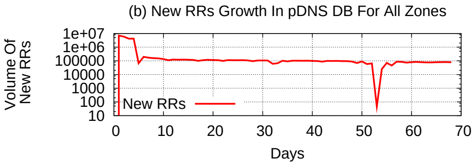
Notation and Terminology

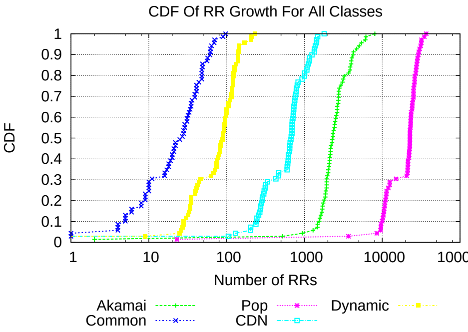
- What is a Resource Record (RR)?
  - `www.example.com 192.0.32.10`
- What is a 2^{nd} level domain (2LD) and 3^{rd} level domain (3LD)?
  - For the domain name `www.example.com`: 2LD is `example.com` and 3LD is `www.example.com`.
- What we define as Related Historic IPs (RHIPs)?
  - All "routable" IPs that historically have been mapped with the domain name in the RR, or any domain name under the 2LD and 3LD
- What we define as Related Historic Domains (RHDNs)?
  - All fully qualified domain names (FQDN) that historically have been linked with the IP in the RR, its corresponding CIDR and AS


S.I.E
Passive DNS Database
Reputation Engine
Dynamic Reputation Scores
Notos
Subnet
Subnet
ISP Recursive DNS Server (Atlanta)
Internet
Subnet
Subnet
Subnet
ISP Recursive DNS Server (SJC)

Passive DNS growth

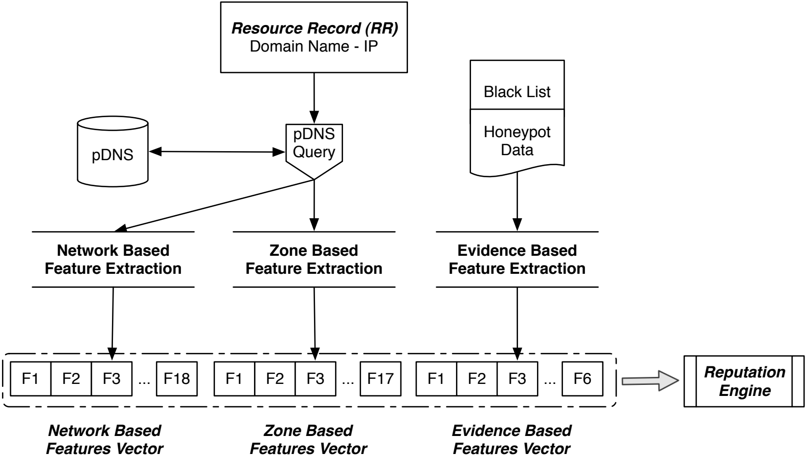






Anchor Classes in pDNS: Akamai, CDN, $Common_{Alexa_{10}}$**,** $Popular_{Alexa_{100}}$ **and Dynamic DNS**

Three Main Feature Vectors for Notos



Network, Zone and Evidence Vectors

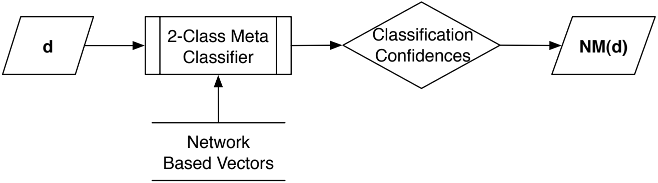
- Vectors for Clustering and Classification
  - **Network Based vector (18)**
    - M/M/STD of frequencies from the set of different networks properties in the list of RHIPs
  - **Zone Based vector (17)**
    - M/M/STD of frequencies from observation based on the zone structure of the domains in the list of RHDNs
- **Evidence vector** (used in the reputation function)
  - Various BLs (3 - IP/CIDR/AS) using public and private IP and DNS BLs
  - Malware Analysis (3 - IP/CIDR/AS) using domain names extracted from malware analysis

Network, Zone and Evidence Vectors

- Vectors for Clustering and Classification
  - **Network Based vector (18)**
    - M/M/STD of frequencies from the set of different networks properties in the list of RHIPs
  - **Zone Based vector (17)**
    - M/M/STD of frequencies from observation based on the zone structure of the domains in the list of RHDNs
- **Evidence vector** (used in the reputation function)
  - Various BLs (3 - IP/CIDR/AS) using public and private IP and DNS BLs
  - Malware Analysis (3 - IP/CIDR/AS) using domain names extracted from malware analysis

Network Profile Modeling

We train a Meta-Classifier based on the 5 anchor-classes.

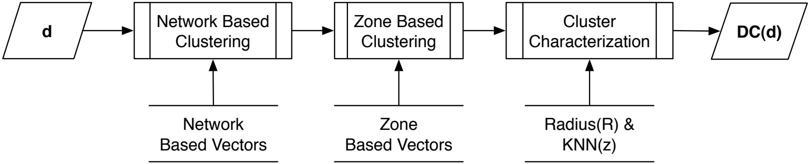


The network feature vector of a domain name *d* will be translated into the network modeling output (**NM(d)**) — the feature vector composed from the confidence scores for each different anchor-class.

The two clustering steps

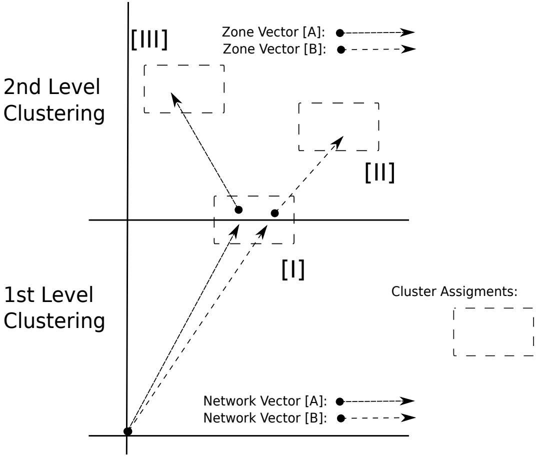
- 1^{st} **Level Clustering (using Network Feature Vectors):** Goal is to identify similarities in zones based upon their network profiles
- 2^{nd} **Level Clustering (using Zone Feature Vectors):** Goal is to further group domain names (within each 1^{st} level cluster) based upon their zone properties

Domain Clustering Flow



In this step we are able to **characterize** unknown domains within clusters based upon already labeled domains in close proximity. The **DC(d)** will assemble a 5 feature vector **characterizing the position of *d* in the 2^{nd} level sub-cluster**

Quick Note on the 2^{nd} Clustering Step



2^{nd} Level Clustering Split Due to Zone Properties

[A]: ns6.b0e.ru 218.75.144.6

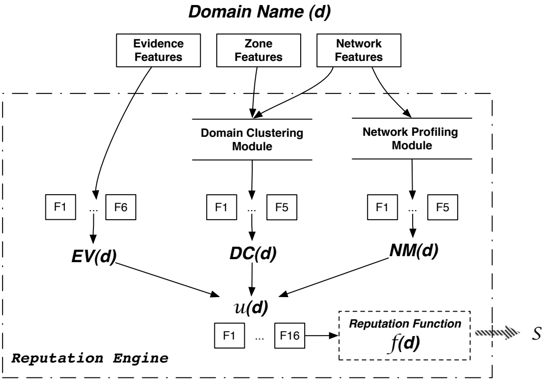
```
...
 188.240.164.122.dalfihom.cn  218.75.144.6
 0743f9.tvafifid.cn           218.75.144.6
 ns5.bg8.ru                   218.75.144.6
 097.groxedor.cn              218.75.144.6
 adelaide.zegsukip.cn         218.75.144.6
 07d2c.fpibucob.cn            218.75.144.6
 0c9.xyowijam.cn              218.75.144.6
 ns6.b0e.ru                   218.75.144.6
 0678fc.yxbocws.cn            218.75.144.6
 ns1.loverspillscalm.com      218.75.144.6
 09071.tjqsjfz.cn             218.75.144.6
 0de1f.wqutoyih.cn            218.75.144.6
 katnzvv.cn                   218.75.144.6
...
```

[B]: e752.p.akamaiedge.net 72.247.179.52

```
...
 e882.p.akamaiedge.net  72.247.179.182
 e707.g.akamaiedge.net  72.247.179.7
 e867.g.akamaiedge.net  72.247.179.167
 e747.p.akamaiedge.net  72.247.179.47
 e732.g.akamaiedge.net  72.247.179.32
 e932.g.akamaiedge.net  72.247.179.232
 e752.p.akamaiedge.net  72.247.179.52
 e729.g.akamaiedge.net  72.247.179.29
 e918.p.akamaiedge.net  72.247.179.218
 e831.p.akamaiedge.net  72.247.179.131
 e731.p.akamaiedge.net  72.247.179.31
...
```

Reputation Function

Each domain d will be transformed into 3 vectors $NM(d)$, $DC(d)$ and $EV(d)$ (or evidence vector) that is the final reputation vector $v(d)$.

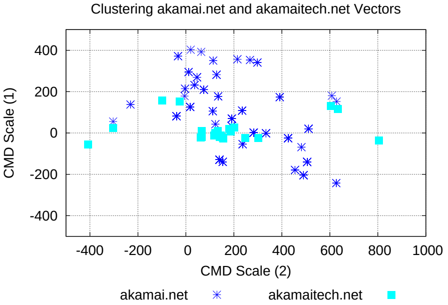


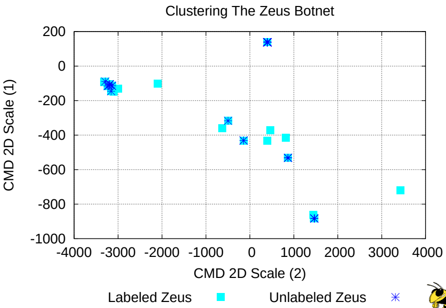
Training and Evaluating Notos

- We used the top 500 (and 10K and 100K) Alexa domains as our White-list
- We consult various public BLs
  - `malwaredomainlist.com`
  - Surbl, Zeus Tracker, SBL
- Damballa for Botnet and flux domains BLs
- We build a 15 days passive DNS database up 08/01
- We map IPs to the corresponding CIDRS/ASN/CC/etc. using the Team's CYMRU IP-to-ASN service
- We computed 250K vectors based on the 250K new RRs observed in the 08/01
- We evaluate the results based on the same BL sources
- We keep crawling the lists until ... today

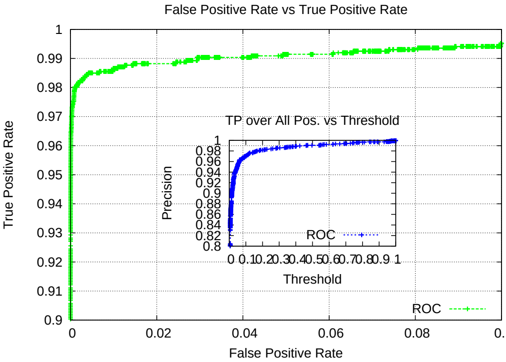
Akamaitech (unknown) VS Akamai (in knowledge base) domains

Clustering known with unknown domain names from Zeus botnet



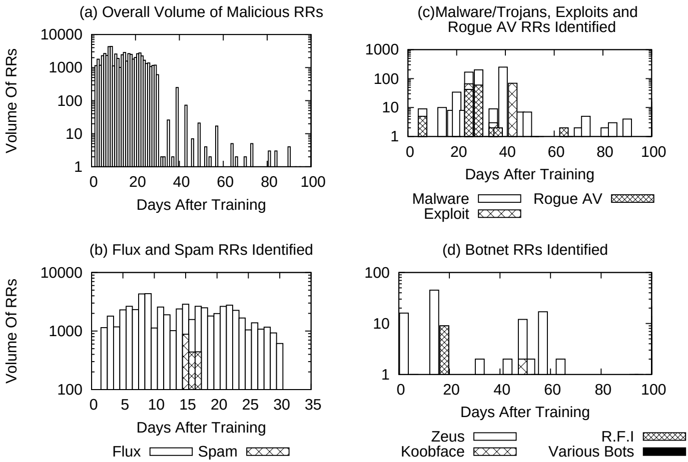


Results from the reputation function



- Results for 10-fold cross-validation, and detection threshold at 0.5, using different Alexa based White-lists:
  - (Top 500) FP_{rate} = 0.38 and TP_{rate} = 96.8 (ROC)
  - (Top 10K) FP_{rate} = 0.4 and TP_{rate} = 93.6
  - (Top 100K) FP_{rate} = 0.6 and TP_{rate} = 80.6

Early domain detections using Notos



Conclusions and Future Work

- Conclusions:
  - Clustering can give us the ability to dynamically associate known with unknown domains
  - Meta-Classification can provide us with very accurate confidences scores that help us dynamically expand our knowledge for the anchor-classes
  - Reputation function gives us very low FP_{rate} and high TP_{rate} making Notos an early warning system for DNS
- Future Work:
  - Targeted detection
  - Combine Notos with Spam detection systems for improving accuracy as a primary coarse filter

Conclusions and Future Work

- Conclusions:
  - Clustering can give us the ability to dynamically associate known with unknown domains
  - Meta-Classification can provide us with very accurate confidences scores that help us dynamically expand our knowledge for the anchor-classes
  - Reputation function gives us very low FP_{rate} and high TP_{rate} making Notos an early warning system for DNS
- Future Work:
  - Targeted detection
  - Combine Notos with Spam detection systems for improving accuracy as a primary coarse filter