

# TIDE

## THREAT IDENTIFICATION USING ACTIVE DNS MEASUREMENTS

ANNA SPEROTTO  
a.sperotto@utwente.nl

OLIVIER VAN DER TOORN  
o.i.vandertoorn@student.utwente.nl

ROLAND VAN RIJSWIJK-  
DEIJ

### MOTIVATION

The **DNS** contains a wealth of information about the **security, stability and health of the Internet**. Most **research** that leverages the DNS for detection of **malicious activities** does so by using **passive measurements**. The **limitation** of this approach, however, is that it is effective **only once an attack is ongoing**. We, on the other hand, **advocate** the use of **active DNS measurements** for **pro-active** (i.e., before the actual attack) identification of **domains set up for malicious use**.

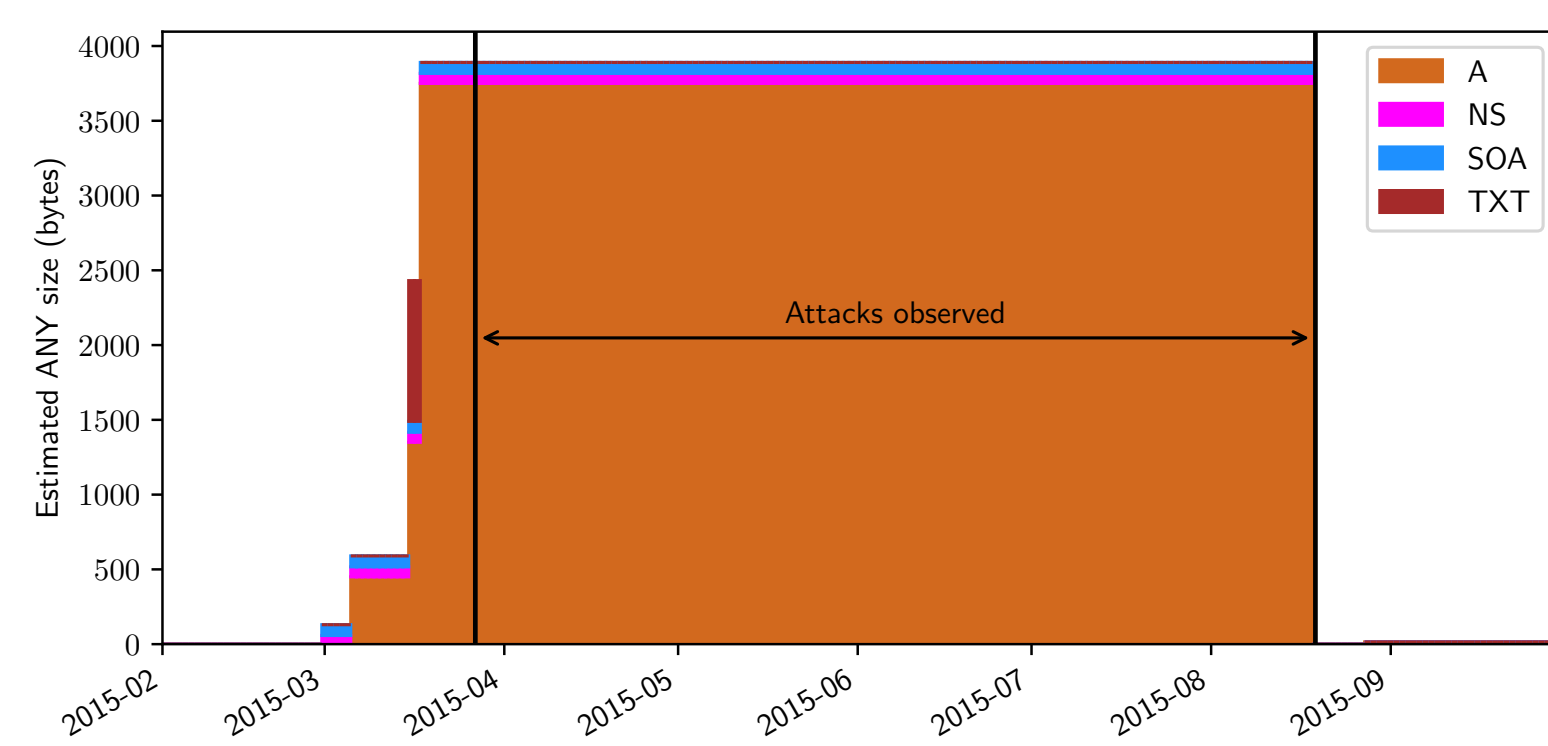


### OPENINTEL

**OpenINTEL** is a **unique active DNS measurement platform** that **collects daily active measurements** of all second-level domains in **60% of the global DNS name space**, including the largest TLDs .com, .net and .org, and many country-specific TLDs, such as .nl, .se and .ru.

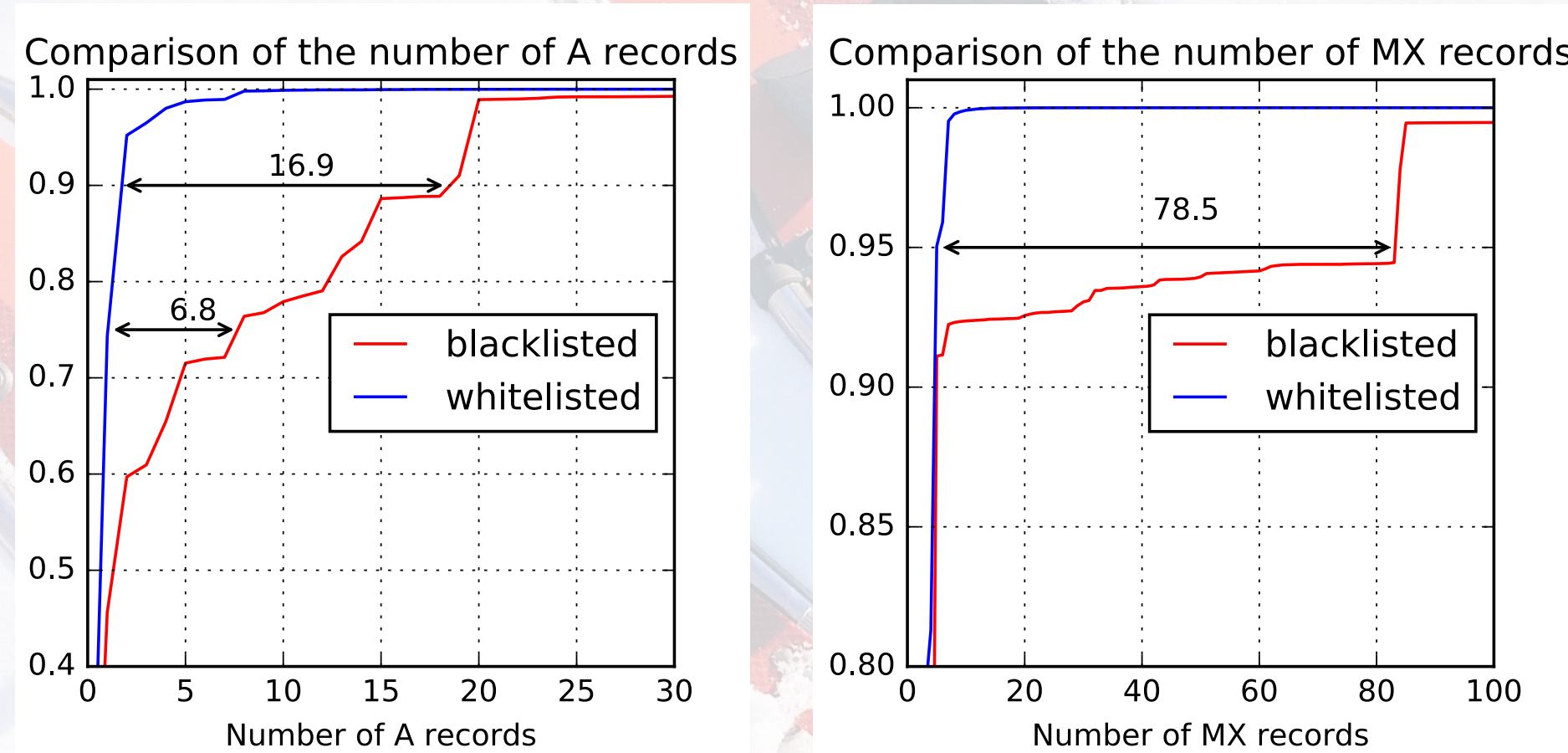
Data **collection started** in **2015**, providing us with a wealth of **longitudinal data** to **validate** our **approach**.

### DENIAL OF SERVICE ATTACKS



An effective way for achieving DNS amplification DDoS attacks is to use a domain under the control of the attacker himself. We observe such attack domains in the making **before they are used in attacks**.

### SNOWSHOE SPAM



In snowshoe spam, attackers distribute the load of spam among a large set of sources, to evade detection based on reputation (e.g. blacklists). Snowshoe spam is therefore **notoriously difficult to detect**.

### CEO FRAUD

TLD	#Domains sharing a specific Office 365 token													
	August						September							
	26	27	28	29	30	31	1	2	3	4	5	6	7	
.com	36	36	77	77	199	259	306	334	334	352	352	394	404	
.net	-	2	2	2	17	17	20	38	43	43	44	54	54	
.org	-	15	15	15	18	18	23	23	26	26	28	28	28	
Total	36	53	94	94	234	294	349	395	403	421	424	476	486	

This example shows a case of CEO fraud against the Dutch higher education sector. Domains used to send target phishing mails shared a common token stored in DNS. Using OpenINTEL data, we **uncovered 61% more domains** than found in an initial sweep by the security community.

### APPROACH

We are currently working on ways to **efficiently detect snowshoe spam** using data from the OpenINTEL platform, and have developed a **prototype** that we are running in an **operational environment**.

Using **machine learning** techniques, we **detect** snowshoe spam domains in the **long tail** of the OpenINTEL dataset. We generate an **RBL** based on the output of this process and feed this against a **live e-mail detection** system that processes approximately **ten million e-mails per day**.

### PRELIMINARY RESULTS

