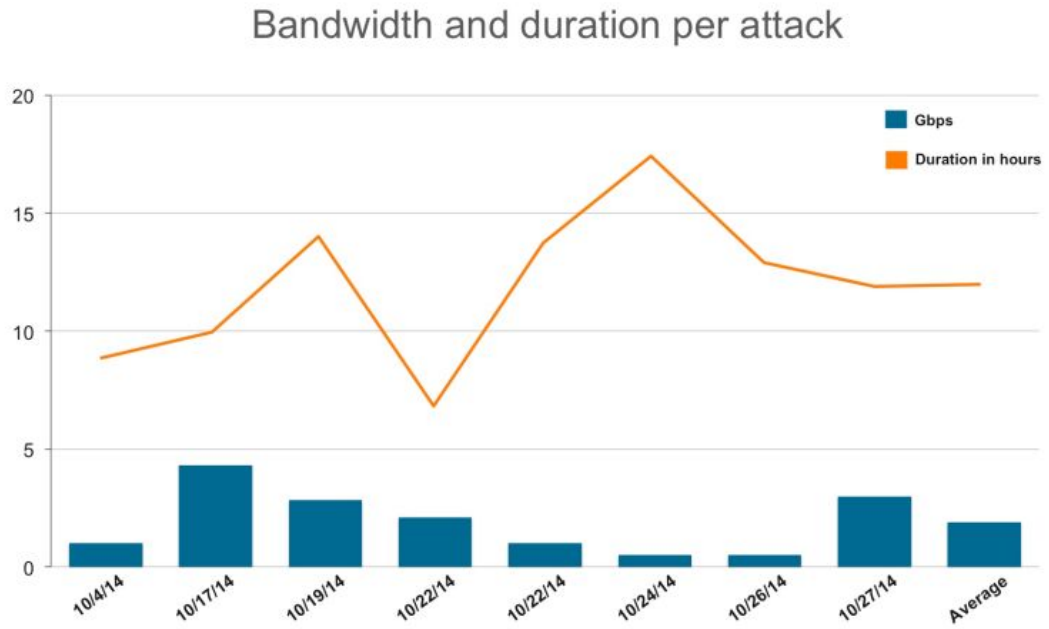
Security in Plain TXT

Observing the Use of DNS TXT Records in the Wild

Adam Portier, Villanova University
Henry Carter, Villanova University
Charles Lever, Georgia Institute of Technology

October 2014 DNS Amplification Attack



Akamai: Security bulletin: Crafted dns text attack.
https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/dns-txt-amplification-attacks-cybersecurity-threat-advisory.pdf (2014)

Why TXT Records?

- Very little research performed in this area
- Use cases varied and unconstrained
- Expected to find misuse

DNS TXT Records

```
google.com. 300 IN TXT "v=spf1 include:_spf.google.com ~all"

google.com. 300 IN TXT "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"

google.com. 300 IN TXT "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="

google.com. 300 IN TXT "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
```

Methodology

- Collected 1.4 B DNS TXT records collected over a 2 year period
- Developed a taxonomy to describe categories of record uses
- Performed analysis on records

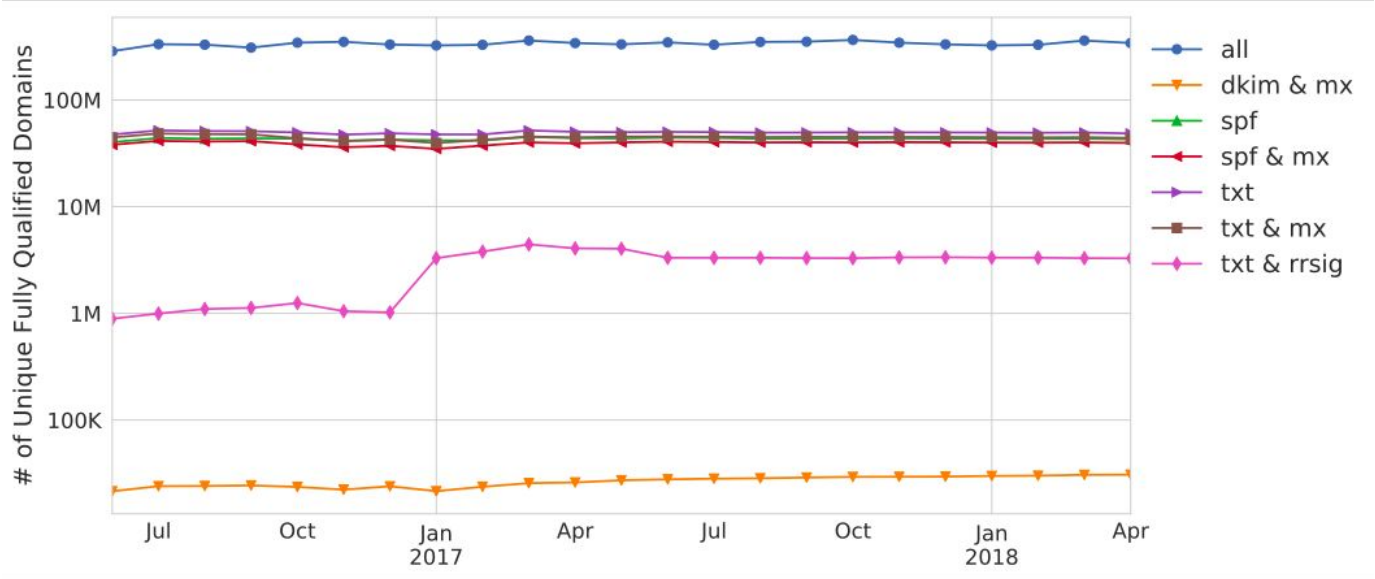
ActiveDNS Dataset June 2016 - May 2018

RR Type	RR Count
TXT	1,410,219,403
MX	1,784,771,811
RRSIG	338,693,718
Total	3,533,684,932

Taxonomy

Category	RR Count	Percent	Apps
Protocol Enhancement	1,080,278,464	76.60%	5
Domain Verification	220,168,210	15.61%	43
Resource Location	9,961	0.00%	4
Unknown	109,762,768	7.78%	
Total	1,410,219,403		52

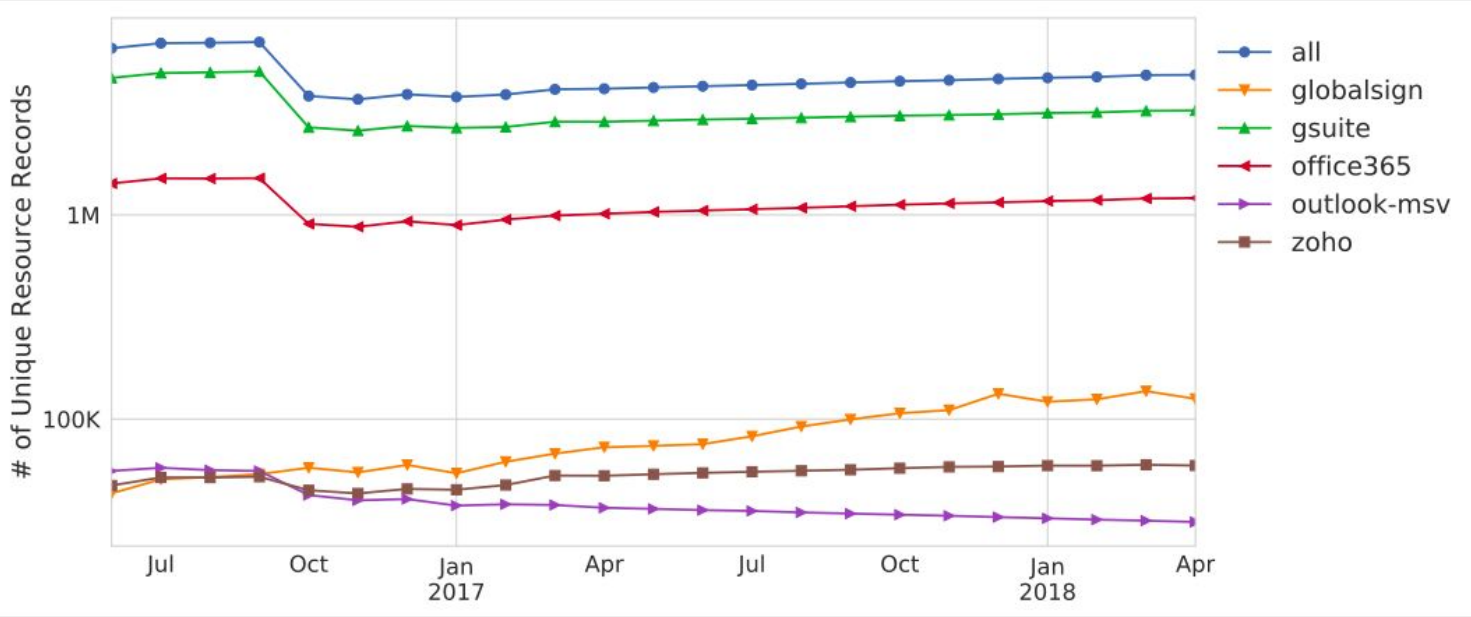
Protocol Enhancement Records



Protocol Enhancement Takeaways

- SPF Usage is Increasing
- The majority of domains are using some SaaS for email
- DMARC adoption is slow
- RRSIG coverage was very low (apx 6%)

Domain Verification Records



Domain Verification Takeaways

- Wide variety of SaaS applications requiring verification
- Public documentation poor
- Size and complexity of records vary widely

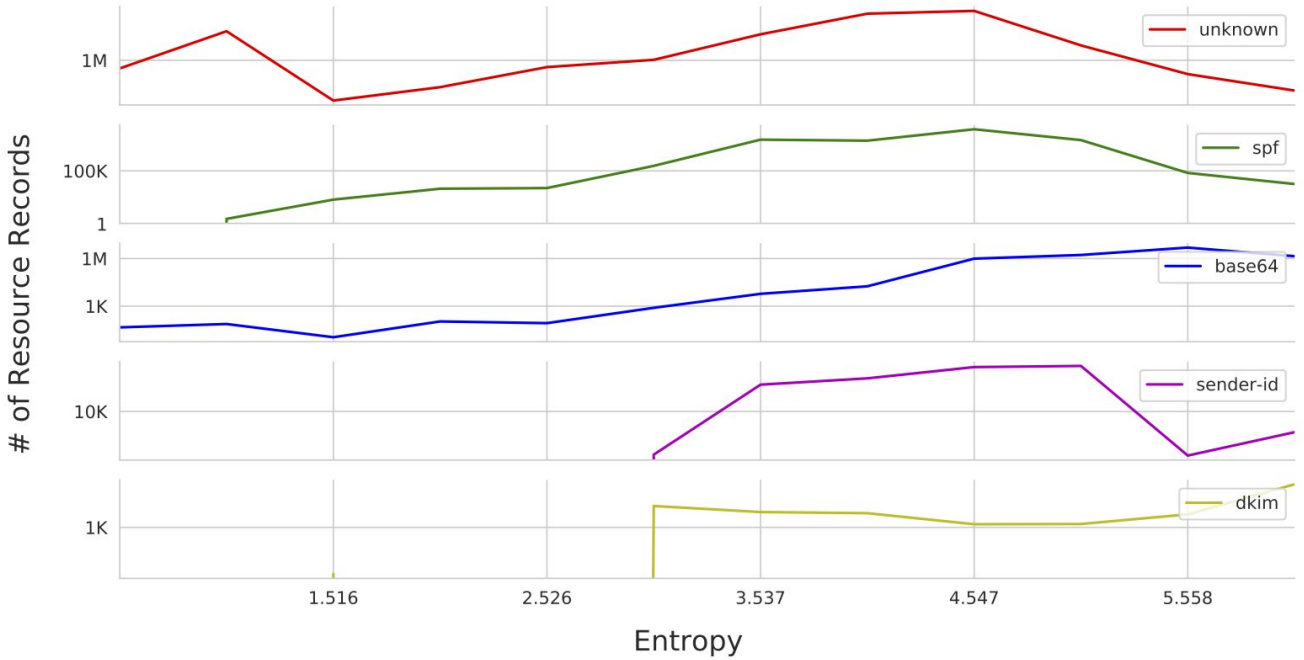
Resource Location Records

- Found 9,961 records from 4 applications
  - Ivanti Landesk
  - Symantec MDM
  - JBoss Fuse
  - Bittorrent

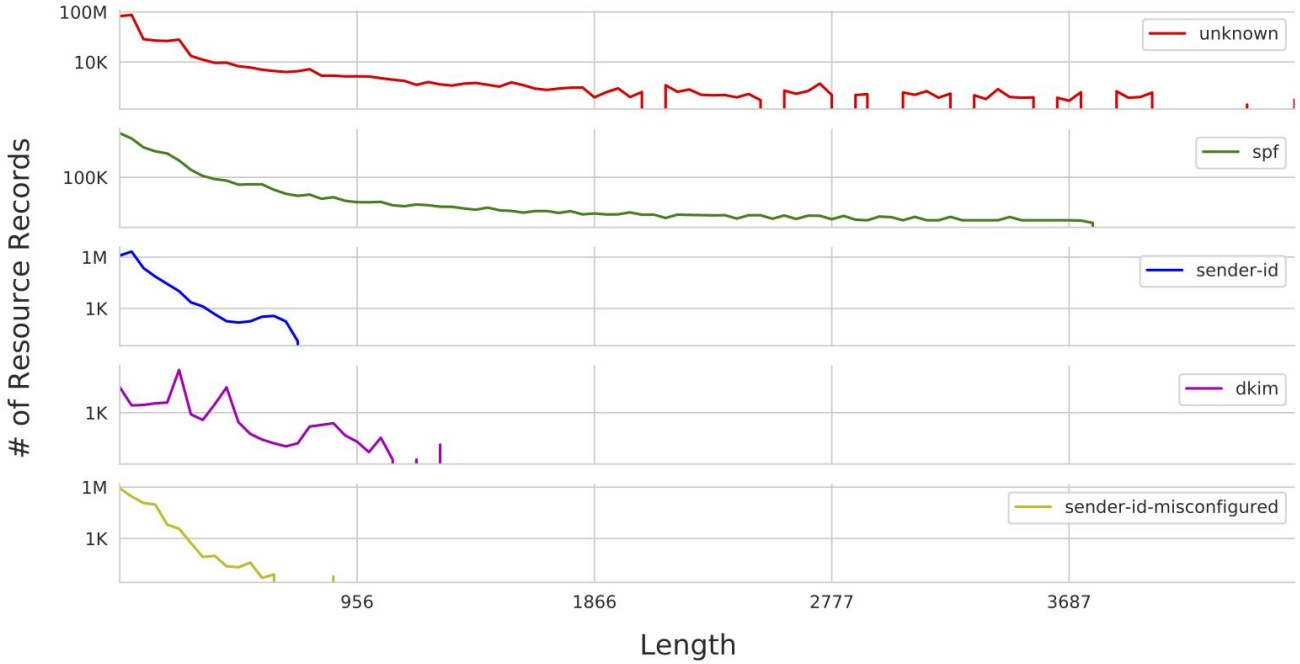
Long Tail

- 8% of the records were initially categorized as “unknown”
- Diminishing returns on patterns
- Wanted to identify if records were structured or random
- Explore if records could be used in amplification attacks

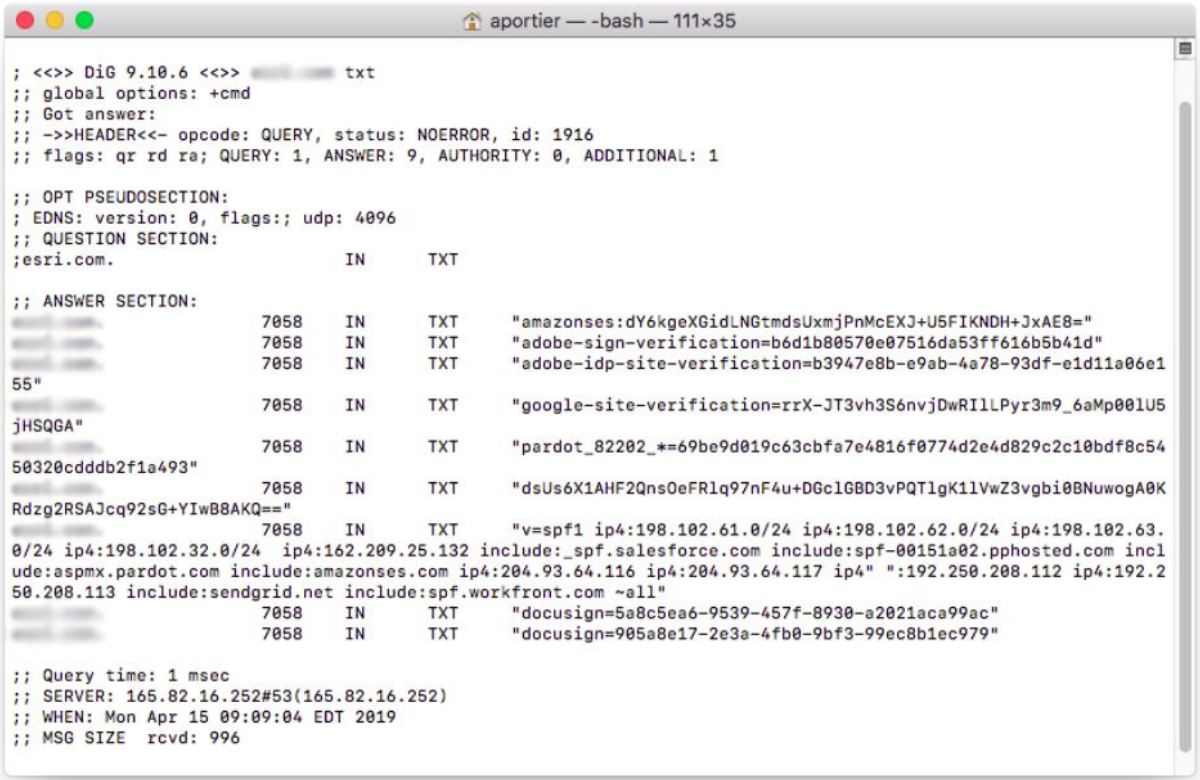
Analysis of Long Tail - Entropy



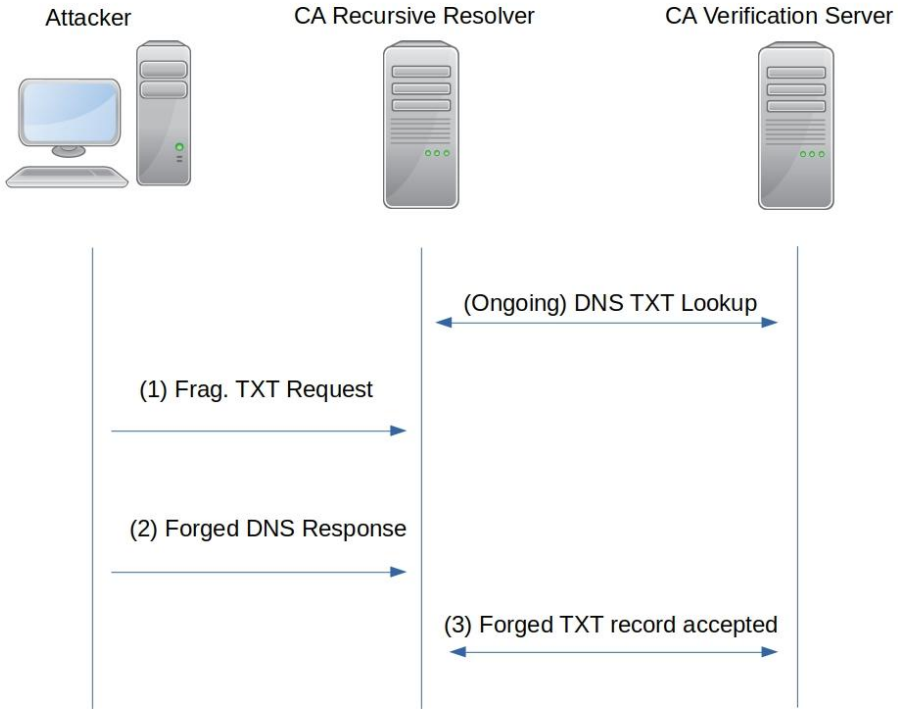
Analysis of Long Tail - Length



Information Leakage



Service Hijacking



Amplification Attacks

“What is .tel?

The .tel is the only top level domain (TLD) that offers a free and optional hosting service that allows individuals and businesses alike to store and manage all their contact information and media directly in the DNS without the need to build, host or manage a website. A typical top-level domain stores IP addresses in the DNS and returns them when queried. If you do not wish to use the free Telhosting service, that is fine as you can use your .tel for any purpose of your choosing e.g. hosting your own website.”

Summary

- 52 Distinct Applications
- 3 Categories of Use
- All use cases have potential abuses
- Documentation around when records checked very poor
- Records should be obfuscated
  - Unguessable subdomains
  - Remove service specific identifiers
- Records should be signed with DNSSEC

Questions?

Adam Portier aporti01@villanova.edu
aportier@haverford.edu