MimeDefang: le dernier rempart

Fabrice Prigent

Université Toulouse Capitole

Jeudi 25 avril 2024

L'Université Toulouse Capitole

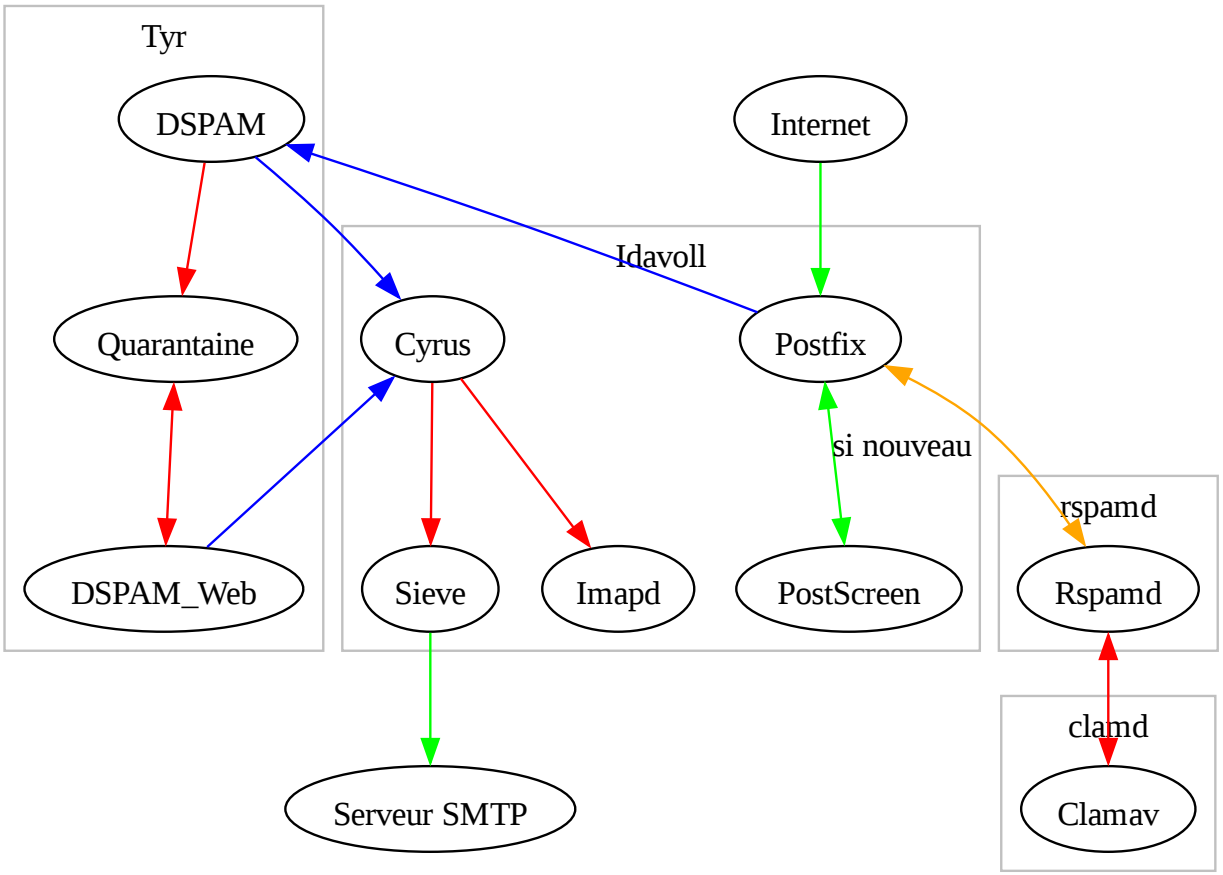
- Université en droit, économie et gestion, avec une petite UFR informatique,
- 21000 étudiants,
- 2100 personnels (dont 1000 vacataires),
- Très forte centralisation (2 entités semi-indépendantes),
- DSI de 30 informaticiens

Avec, comme tout le monde, des problèmes de phishing/spam/virus

Gestion technique de la problématique

- 2 antispams
  - Rspamd lié à un Clamav lui même lié avec
    - des signatures chez securiteinfo
    - un oletools pour analyser des macros
  - DSPAM (bayésien qui va utiliser les tags Rspamd)
- Le filtre postscreen, intégré dans postfix, qui bloque dès le début et fait du greylisting.
- Des fausses adresses (honeymail) sur nos sites web, permettant à RSPAMD de repérer certains expéditeurs assez vite.
- Du phishing pédagogique chaque 2 mois.
- Un filtrage d'URL et un DNS-RPZ

Le schéma


Tyr
DSPAM
Internet
Idavoll
Quarantaine
Cyrus
Postfix
si nouveau
rspamd
DSPAM_Web
Sieve
Imapd
PostScreen
Rspamd
clamd
Serveur SMTP
Clamav

Mais la réalité nous rattrape: ils s'adaptent

- Mais ça passe.. parce que les escrocs s'adaptent en
  - privilégiant les urls aux fichiers
  - évitant les domaines trop jeunes
  - utilisant domaines généralistes (forms.google.com, ipfs.io, googleapis.com, etc.)
  - utilisant des raccourcisseurs d'URLs (parfois imbriqués)
  - créant par IA des textes corrects
  - produisant des texte très courts (pour éviter les IA des antispams)

Mais la réalité nous rattrape: les compromissions

- Mais ça passe parce que les comptes compromis sont légion
  - 3 comptes UT Capitole compromis par des infostealer
  - 15 campagnes provenant de la communauté Education/Recherche
  - les clients des massmailer (sendgrid et consorts) se font piratés
- Ce qui fait que
  - Les IP d'origine ont une bonne réputation (par exemple en provenance de la communauté)
  - Les contenus des en-têtes sont connus, voire carrément "locaux", ex. Office365, Partage, etc.

Que faire de plus ?

- Bloquer les URLs dangereuses.
  - Tout en sachant que cela sera imparfait (bloquer surveymonkey.net, sendgrid.net ?)
- Laisser l'utilisateur juger
  - Car il est souvent le seul à pouvoir le faire.
  - Mais il faut l'aider à réfléchir.
  - En lui donnant les éléments nécessaires.

Concept: neutralisation d'URL

- L'idée a été de neutraliser les URLs potentiellement nocives
- en les remplaçant par un lien que nous contrôlons.
- grâce à /etc/postfix/body_checks.regexp

```
/^(.*)(https?:..|https?=3A..)([A-Za-z0-9_\.\-]+
(?:\.|=2E))?(linktr\.ee|liurl\.cn|
ct=2Esendgrid=2Enet|REGEXP_DE_10Ko)(.*)$/ REPLACE
${1}https://dsi.ut-capitole.fr/t.php?
i=${3}${4}${5}
```

Concept: neutralisation d'URL

L'URL

```
https://firebasestorage.googleapis.com/v0/b/huzbrcmesitr88.appspot.com/o/index.html?alt=media&amp;token=347d6f17-7ff1-43ac-9de2-75834fbaee19
```

devient donc

```
https://dsi.ut-capitole.fr/t.php?i=firebastorage.googleapis.com/v0/b/huzbrcmesitr88.appspot.com/o/index.html?alt=media&amp;token=347d6f17-7ff1-43ac-9de2-75834fbaee19
```

Ecran d'avertissement

body_checks: les limites

Plusieurs limites arrivent rapidement

- La regexp est maintenable.. par un psychopathe,
- Les urls ne sont pas traitées si elles sont coupées (RFC822 découpe à 78 caractères)
- Le remplacement a lieu avant les antispams
  - qui voient des signatures DKIM potentiellement cassées
  - qui ne peuvent analyser les domaines en lien (résoudre les raccourcisseurs, évaluer les urls, etc.).
  - qui finissent par considérer que le site de validation est "nocif"

UNIVERSITÉ TOULOUSE CAPITOLE

Mimedefang

- MimeDefang (https://mimedefang.org) est un outil antispam en perl
- Très ancien (août 2000)
- Moins efficace que nos antispams déjà présents (même s'il intègre SpamAssasin)
- Mais il embarque toute la mécanique de désassemblage, interprétation, reconstruction des mails

Les modifications de mimedefang-filter

- Alléger le script (Spamassassin, unzip, caractères dangereux, etc.)
- Ajouter des procédures pour repérer les URLs nocives (à partir des fonctions anonymize_text_uri)
- Faire la version "texte" et "html"
- Eviter de réécrire les urls des images
- Remplacer par une url avec un hash
- Prendre des catégories spécialisées (shortener, filehosting, site de formulaire, hébergement P2P, etc.) pour faire des filtres à jour.

Les modifications de /etc/postfix/main.cf

```
# Pour exclure les clients internes
smtpd_milter_maps = cidr:/etc/postfix/smtpd_milter_map
# Le Mimedefang après le rspamd
smtpd_milters = inet:rspamd.ut-capitole.fr:11332, inet:127.0.0.1:11400
```

Les modifications

En simplifiant:

```
if($text =~ /$regexp/oi) {
  while ($text =~ m{(https?:?=?3?A?//[^\s<>"'\)\\]+)}gi) {
    my $url = $1;
    if (($url =~ /$regexp/oi) && ($url !~ /$regexp_ignore/oi)){
      md_graphdefang_log("html_sanitize dangerous ".$url);
      my $md5=md5_hex($url.$secret_md5);
      my $now=time();
      $dbh->do("REPLACE INTO md5_url (md5,url,last) values ('$md5','$url',NOW())");
      $remplacement="https://ds1.utcapitole.fr/t.php?md5=$md5";
      $text =~ s/\Q$url\E/$remplacement/gi;
    }
  }
}
```

Mimedefang: le remplacement

L'URL

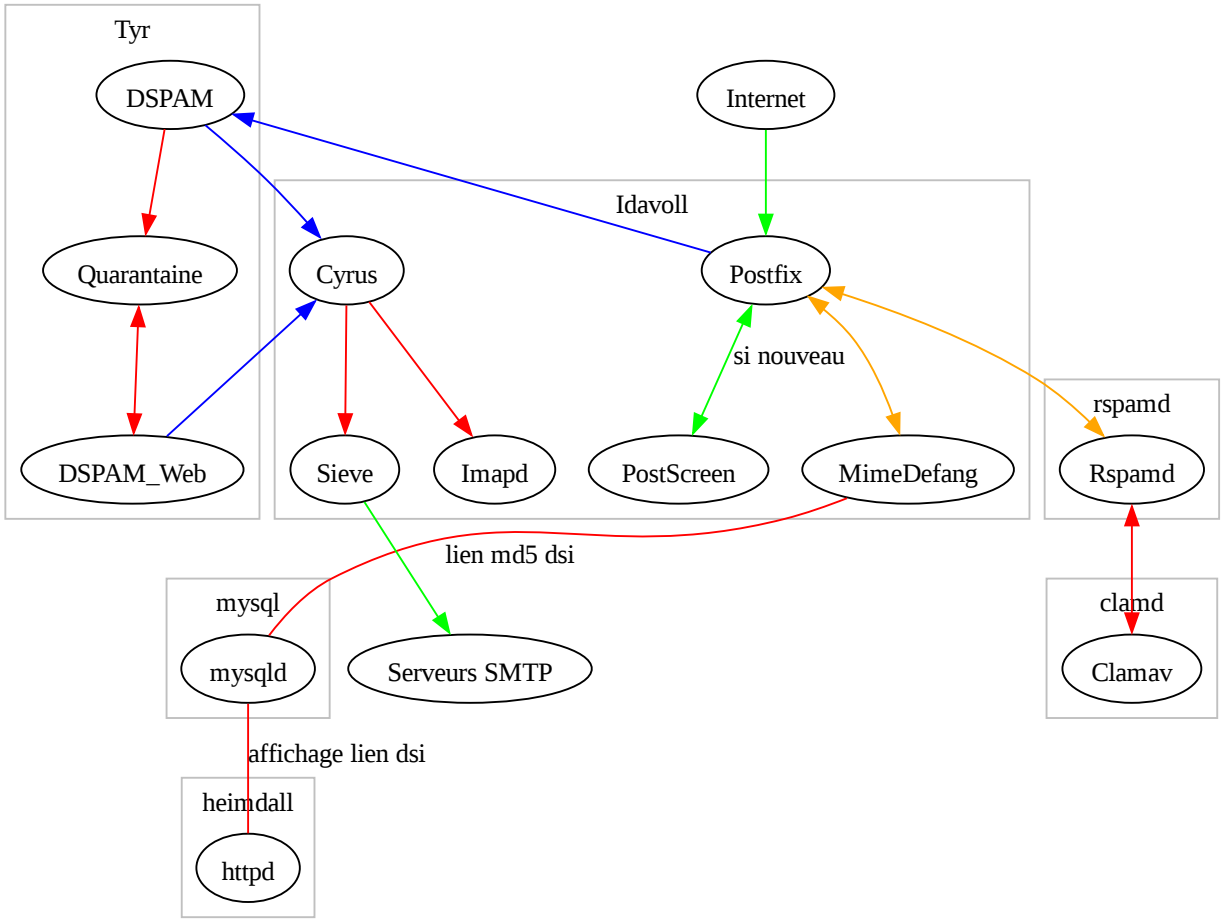
```
https://firebasestorage.googleapis.com/v0/b/huzbrcmesitr88.appspot.com/o/index.html?alt=media&amp;token=347d6f17-7ff1-43ac-9de2-75834fbaee19
```

devient donc

https://dsi.ut-capitole.fr/t.php?md5=309b17cd9b3618fca60ecee67331a113

Ecran d'avertissement

Le schéma


Tyr
DSPAM
Internet
Idavoll
Quarantaine
Cyrus
Postfix
si nouveau
rspamd
DSPAM_Web
Sieve
Imapd
PostScreen
MimeDefang
Rspamd
lien md5 dsi
mysql
clamd
mysqld
Serveurs SMTP
Clamav
affichage lien dsi
heimdall
httpd

Les précautions et les risques

- Conversion des . en "=2E"
- Compiler de manière optimale les regexp
- Les URLs sont parfois très longues (celles de sendgrid.net font parfois 2 Ko !)
- Déplacer le mimedefang après TOUS les autres antispams.
- Il faut parfois expliquer qu'il est normal que l'url ait été remplacée dans le mail, par une url "locale".

Statistiques

En un mois

- 549 domaines gérés
- 4283 "tests" dont 924 par des serveurs (cloudflare)
- 751 urls uniques concernées
- A vue de nez, 50%-70% des phishing qui contournent toute la chaine sont neutralisés par MimeDefang.

Questions

Des questions ?