

# Inside Upas Kit (1.0.1.1) aka Rombrast C&C - Botnet Control Panel

Archived: 2026-04-05 19:15:08 UTC

2012-08-16 - Panel

## Upas

In middle of june a new botnet was advertised on underground forum as Upas Kit. (see end of this post for advert). Bot is recognized by Microsoft in Win32/Rombrast family

Upas

**Login**

UserName  
admin

Password  
\*\*\*\*\*


Captcha  
v4c0nhmi  
v4c0nhmi

Submit

Upas - Login Screen

### Upas

- Map
- Bots
- Statistics
- Tools
- Logs
- Tasks
- Download logs
- Settings
- AdminCP
- LogOut



0.056023 sec.

Copyright © 2012 Upas Inc. All rights reserved.

### Upas - Map

### Upas

- Map
- Bots
- Statistics
- Tools
- Logs
- Tasks
- Download logs
- Settings
- AdminCP
- LogOut

IP	Country	OS	Arch	SP	Permissions	Version	Build	Socks	FirstKnock	LastKnock	Status
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	[redacted]	N/A	[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	[redacted]	N/A	[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	Admin	1.0.1.1	LNK	[redacted]	[redacted]	[redacted]	Online
[redacted]	[redacted]	Windows 7	[redacted]	0	[redacted]	1.0.1.1	MAIN	[redacted]	2012	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	MAIN	[redacted]	2012	[redacted]	Online
[redacted]	[redacted]	[redacted]	x86	2	Admin	1.0.1.1	MAIN	N/A	2012	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	[redacted]	Windows XP	x86	2	Admin	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	User	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	US	[redacted]	[redacted]	[redacted]	Admin	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]	x64	1	Admin	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	CA	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	User	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	DE	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]	1.0.1.1	MAIN	[redacted]	[redacted]	[redacted]	Online

Showing rows [redacted]

Pages [redacted] OK

0.048276 sec.

Copyright © 2012 Upas Inc. All rights reserved.

### Upas - Bots

# Upas

Map | Bots Online | Online Bots | Arch | Countries | Comparing mont | Spreading | Botkill | Ruskill | FTP

Bots | Passwords | Bots Summary statistics | Version | OS | Permissions

Statistics

Tools

Logs

Tasks

Download logs

Settings

AdminCP

LogOut

Bots Online

Online last 15 min:	
Online last 15 min:	
Online last 1 hr:	
Online last 6 hr:	
Online last 12 hr:	
Online last 24 hr:	
Online last 2 days:	
Online last 2 days:	
Online last 4 days:	
Online last 5 days:	
Online last 6 days:	
Online last 7 days:	

0.637772 sec.

Copyright © 2012 Upas Inc. All rights reserved.

Waiting for ajax.googleapis.com...

## Upas - Statistics - Bots Online

# Upas

Map | Bots Online | Online Bots | Arch | Countries | Comparing mont | Spreading | Botkill | Ruskill | FTP

Bots | Passwords | Bots Summary statistics | Version | OS | Permissions

Statistics

Tools

Logs

Tasks

Download logs

Settings

AdminCP

LogOut

Online Bots

Day	MAIN	LNK	Auton.inf
1	~800	0	0
2	~800	0	0
3	~800	0	0
4	~800	0	0
5	~800	0	0
6	~800	0	0
7	~800	0	0
8	~800	0	0
9	~800	0	0
10	~800	0	0
11	~800	0	0
12	~800	0	0
13	~800	0	0
14	~800	0	0
15	~800	0	0
16	~800	0	0
17	~800	0	0
18	~800	0	0
19	~800	0	0
20	~800	0	0
21	~800	0	0
22	~800	0	0
23	~800	0	0
24	~800	0	0
25	~800	0	0
26	~800	0	0
27	~800	0	0
28	~800	0	0
29	~800	0	0
30	~800	0	0
31	~800	0	0

0.669734 sec.

Copyright © 2012 Upas Inc. All rights reserved.

Waiting for ajax.googleapis.com...

## Upas - Statistics - Online Bots

### Upas

Map	Bots Online	Online Bots	Arch	Countries	Comparing month	Spreading	Botkill	Ruskill	FTP
Bots	Passwords	Bots Summary statistics		Version	OS	Permissions			

Arch

0.669734 sec.

Copyright © 2012 Upas Inc. All rights reserved.

### Upas - Statistics - Arch

### Upas

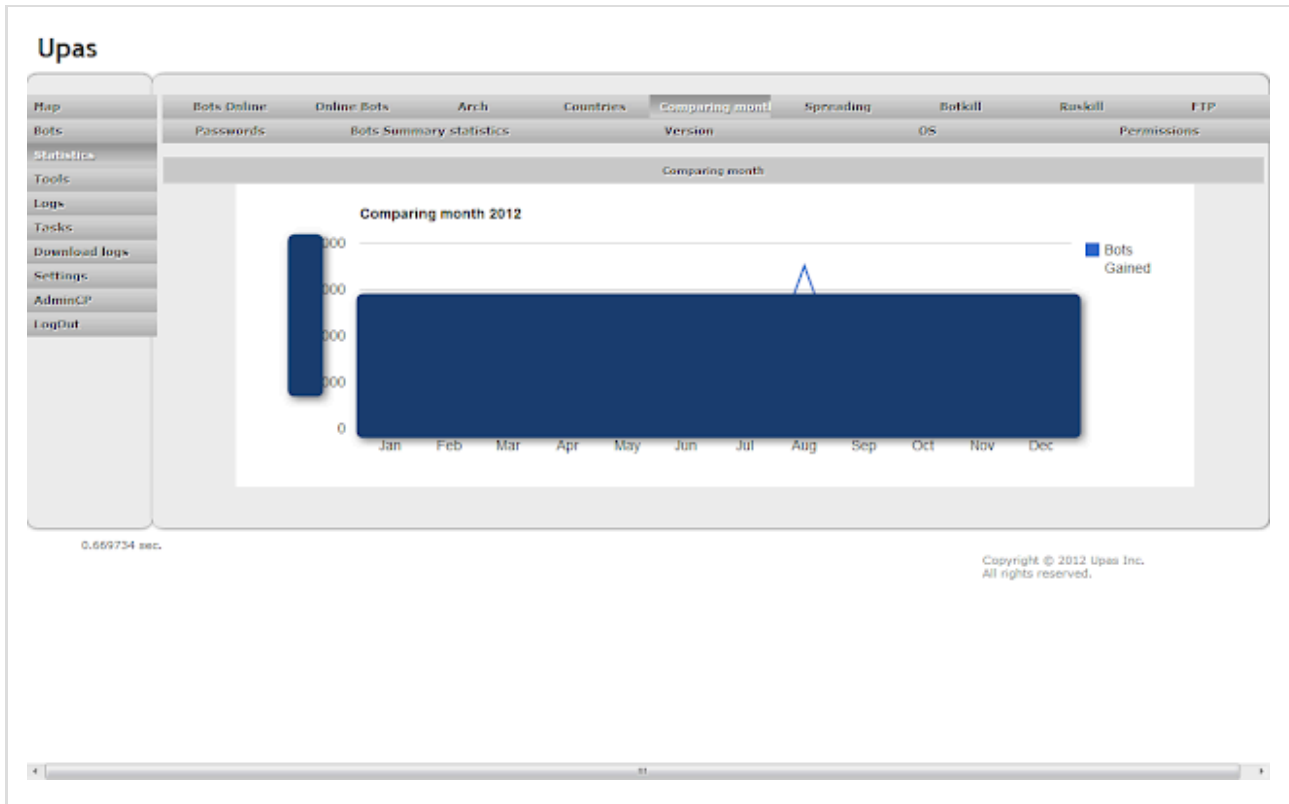
Map	Bots Online	Online Bots	Arch	Countries	Comparing month	Spreading	Botkill	Ruskill	FTP
Bots	Passwords	Bots Summary statistics		Version	OS	Permissions			

Countries

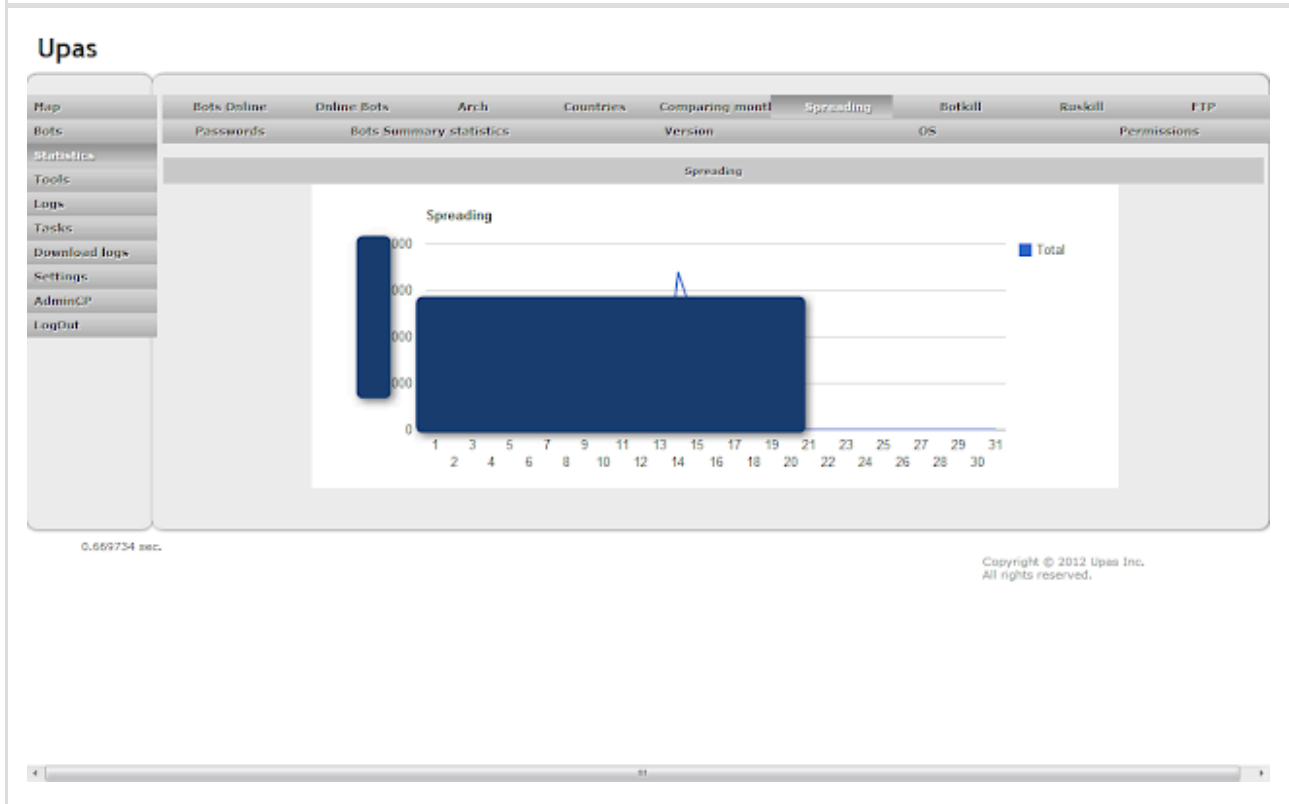
0.669734 sec.

Copyright © 2012 Upas Inc. All rights reserved.

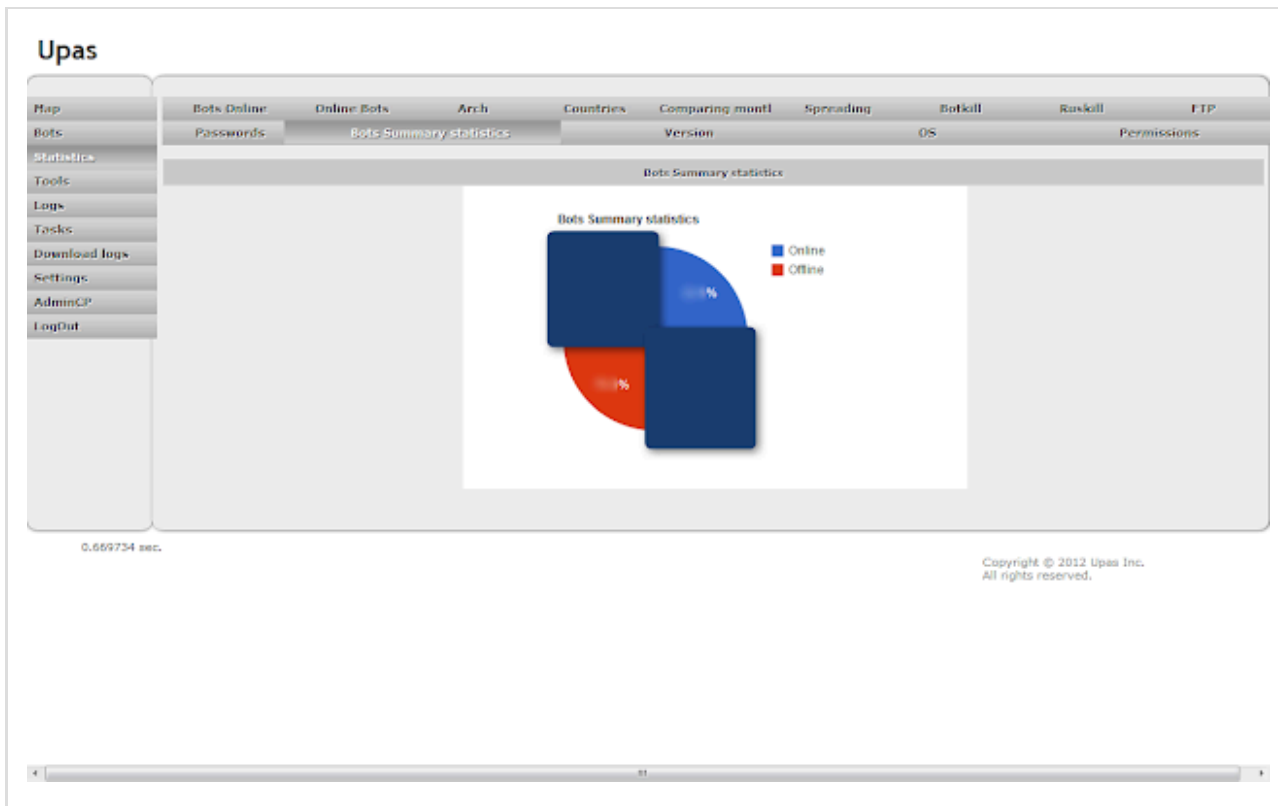
### Upas - Statistics - Countries



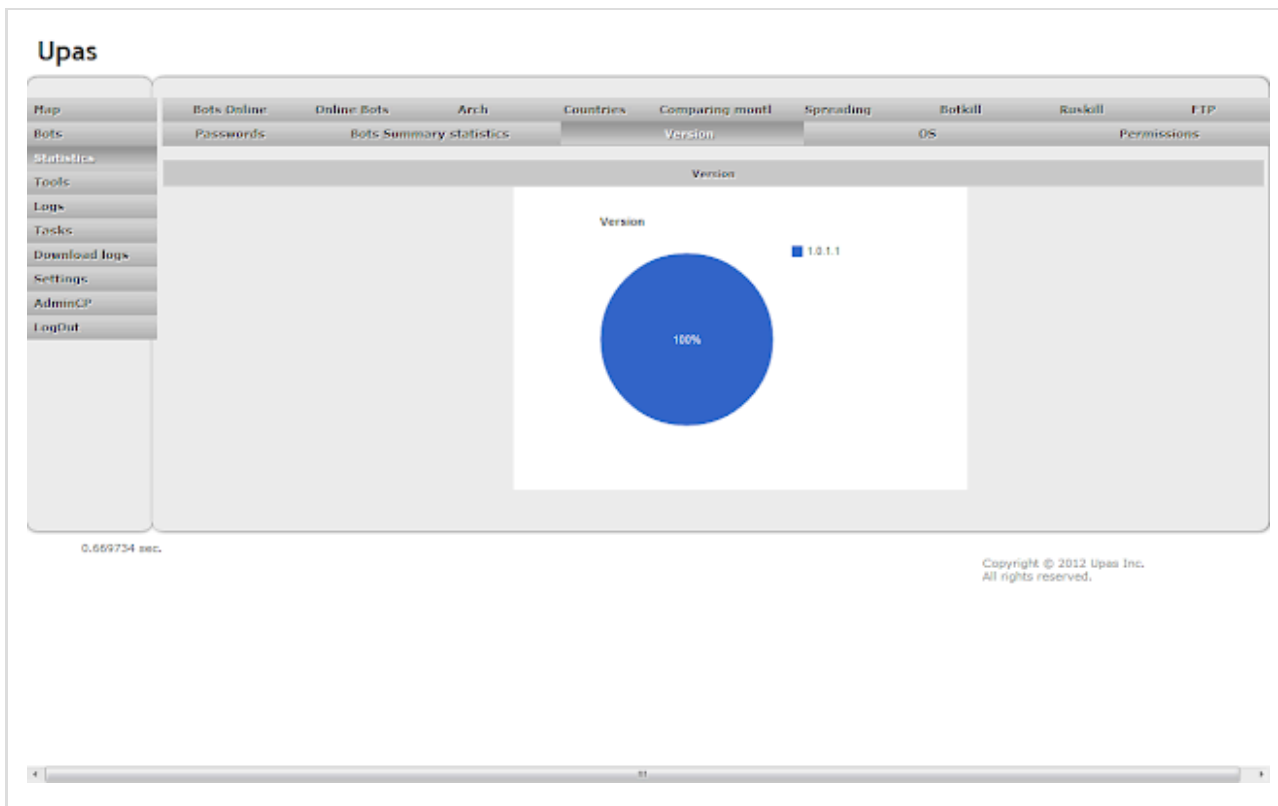
Upas - Statistics - Comparing months



Upas - Statistics - Spreading



Upas - Statistics - Bots Summary statistics



Upas - Statistics - Version

# Upas

Map | Bots Online | Online Bots | Arch | Countries | Comparing month | Spreading | Botkill | Ruskill | FTP  
Bots | Passwords | Bots Summary Statistics | Version | OS | Permissions  
Statistics  
Tools  
Logs  
Tasks  
Download logs  
Settings  
AdminCP  
LogOut

OS

OS

0.669734 sec.

Copyright © 2012 Upas Inc. All rights reserved.

Upas - Statistics - OS

### Upas

- Map
- Bots
- Statistics
- Tools
- Logs
- Tasks
- Download logs
- Settings
- AdminCP
- LogOut

Bots Online   Online Bots   Arch   Countries   Comparing month   Spreading   Botkill   Ruskill   FTP

Passwords   Bots Summary statistics   Version   OS   Permissions

#### Permissions

0.669734 sec.

Copyright © 2012 Upas Inc. All rights reserved.

### Upas - Statistics - Permissions

### Upas

- Map
- Bots
- Statistics
- Tools
- Logs
- Tasks
- Download logs
- Settings
- AdminCP
- LogOut

File:  Aucun fichier choisi

URL:

Domain/IP:

Exploit Pack:

0.009280 sec.

Copyright © 2012 Upas Inc. All rights reserved.

### Upas - Stats

# Upas

- Map
- Bots
- Statistics
- Tools
- Logs
- Tasks
- Download logs
- Settings
- AdminCP
- LogOut

- FTP
- Spreadings
- Botkill
- Passwords
- Ruskill
- Injects

Search ...

Server	Port	UserName	Password	Date
--------	------	----------	----------	------

0.007202 sec.

Copyright © 2012 Upas Inc.  
All rights reserved.

Upas - Logs - FTP

# Upas

- Map
- Bots
- Statistics
- Tools
- Logs
- Tasks
- Download logs
- Settings
- AdminCP
- LogOut

FIP   Spreadings   Botkill   Passwords   Ruskall   Injects

Search ...

Type	Details	Date
USB	Infected Drive E:\	2012
USB	Infected Drive I:\	

Showing row ... from ...

Pages: [ ] OK

0.015175 sec.

Copyright © 2012 Upas Inc. All rights reserved.

## Upas - Logs - Spreadings

# Upas

- Map
- Bots
- Statistics
- Tools
- Logs
- Tasks
- Download logs
- Settings
- AdminCP
- LogOut

- FTP
- Spreadings
- Botkill**
- Passwords
- Ruskill
- Injects

Search ...

Type	Location	Details	Date
------	----------	---------	------

0.009654 sec.

Copyright © 2012 Upas Inc.  
All rights reserved.

Upas - Logs - Botkill

### Upas

- Map
- Bots
- Statistics
- Tools
- Logs
- Tasks
- Download logs
- Settings
- AdminCP
- Logout

FTP	Spreadings	Botkill	Passwords	Rootkit	Injects
IP	Country	Browser	URL	UserName	Password
[REDACTED]	[REDACTED]	Firefox	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	2012	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	www.facebook	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	accounts.google.com	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	login.live.com	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	Chrome	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	Chrome	login.yahoo.com	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	IE/Explore	www.facebook	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	Firefox	[REDACTED]	[REDACTED]	[REDACTED]

Showing rows 10 from [REDACTED] Next

Page 1 of 1

0.099745 sec. Copyright © 2012 Upas Inc. All rights reserved.

### Upas - Logs - Passwords

### Upas

Navigation menu: Map, Bots, Statistics, Tools, Logs, Tasks, Download logs, Settings, AdminCP, LogOut

Sub-headers: FTP, Spreadings, Botkill, Passwords, **Ruskill**, Injects

Search: Search ...

IP	Details	Date
Showing rows 0 to 50 from 0		

0.007324 sec.

Copyright © 2012 Upas Inc. All rights reserved.

### Upas - Logs - Ruskill

### Upas

Navigation menu: Map, Bots, Statistics, Tools, Logs, Tasks, Download logs, Settings, AdminCP, LogOut

Sub-headers: FTP, Spreadings, Botkill, Passwords, **Ruskill**, Injects

Search: Search ...

ID	Country	IP	Date	View
----	---------	----	------	------

0.008148 sec.

### Upas - Logs - Injects

### Upas

0.01086 sec.

Task: Update  
Limit: [input]  
Mode: Continuous  
Country: All  
OS: All  
Arch: All

Public Link

Task	Details	Mode	Limit	Country	OS	Arch	Status	Task
download and execute		Continuous			ALL	ALL	Active	

Copyright © 2012 Upas Inc. All rights reserved.

### Upas - Tasks

remote.php?key=

Sort	Limit	Task	Details	Country	OS	Arch
------	-------	------	---------	---------	----	------

### Upas - Public Link to tasks

### Upas

0.011462 sec.

DownloadLogs

Logs: FTP  
Columns: Spreading, Botkill, Passwords, Ruskil, Injects  
From: [input]  
To: [input]  
Country: All  
Limit: [input]

Submit

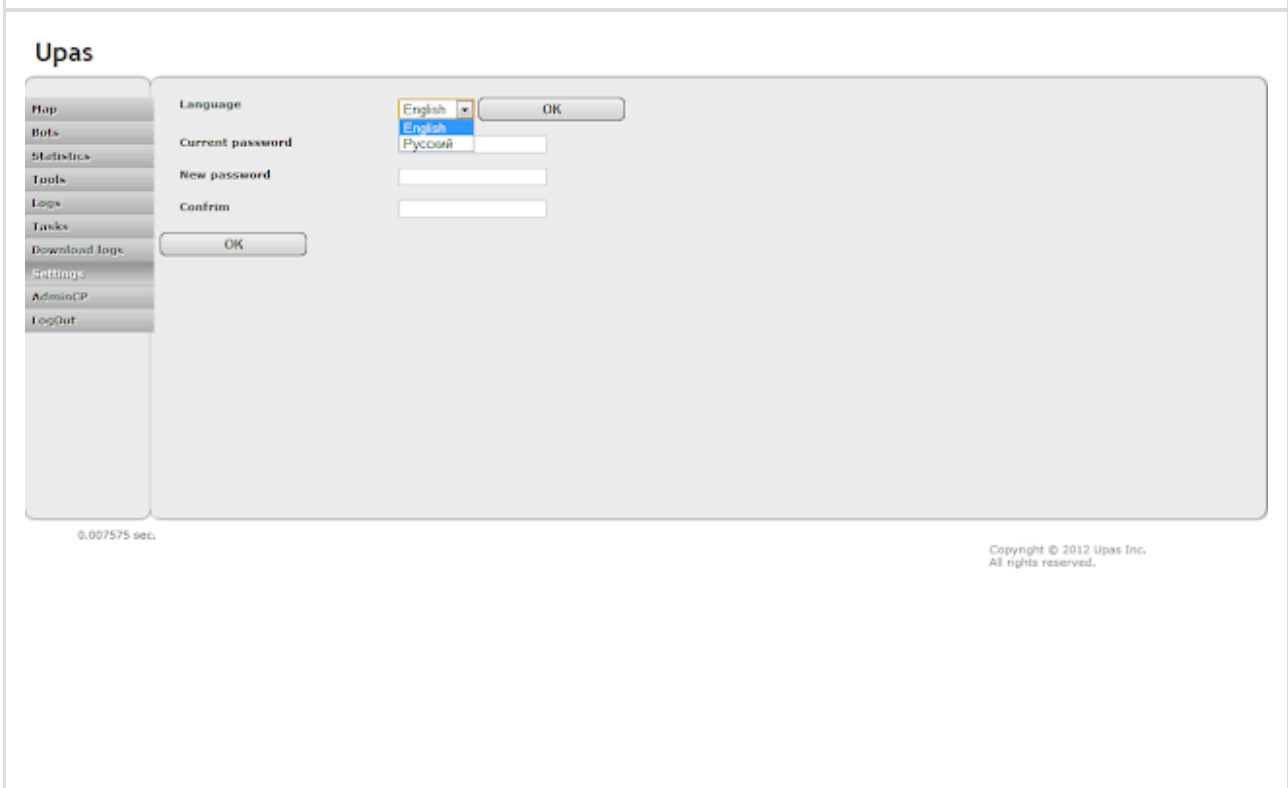
port  username  password  date

Copyright © 2012 Upas Inc. All rights reserved.

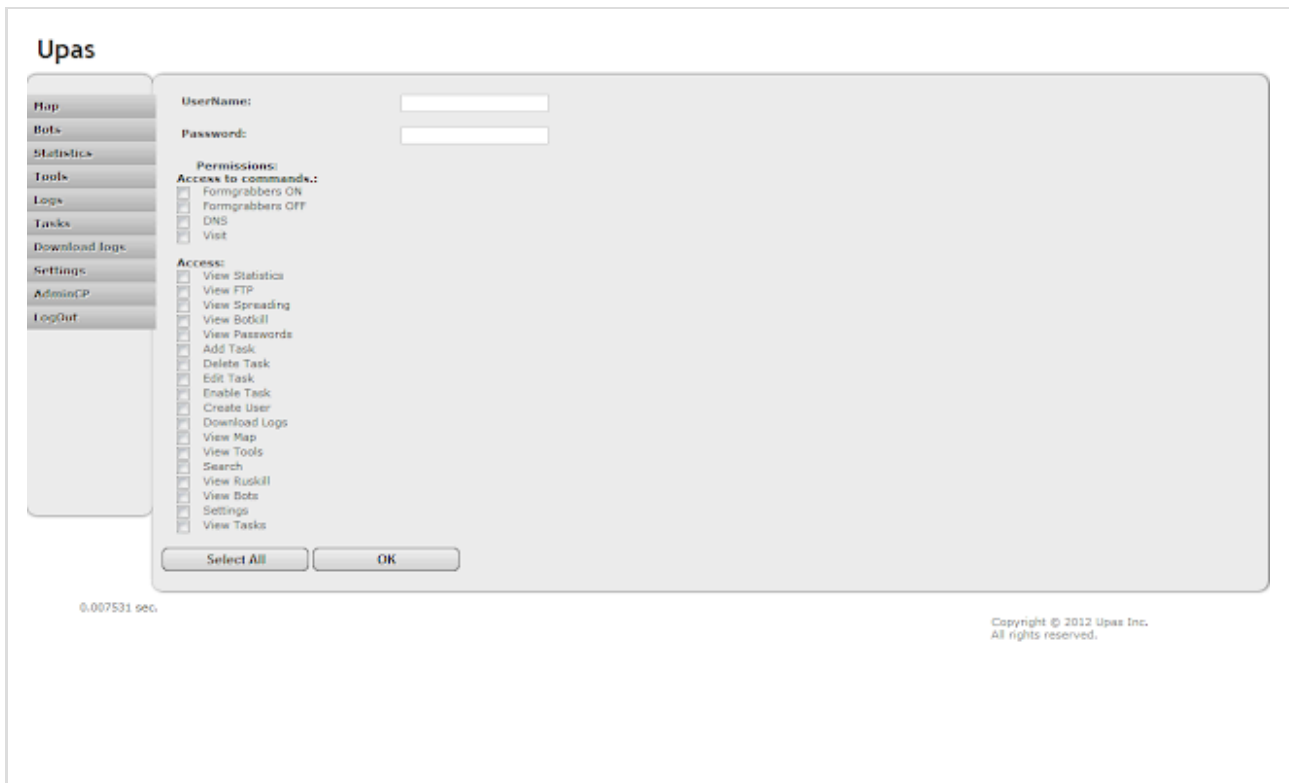
### Upas - Download logs



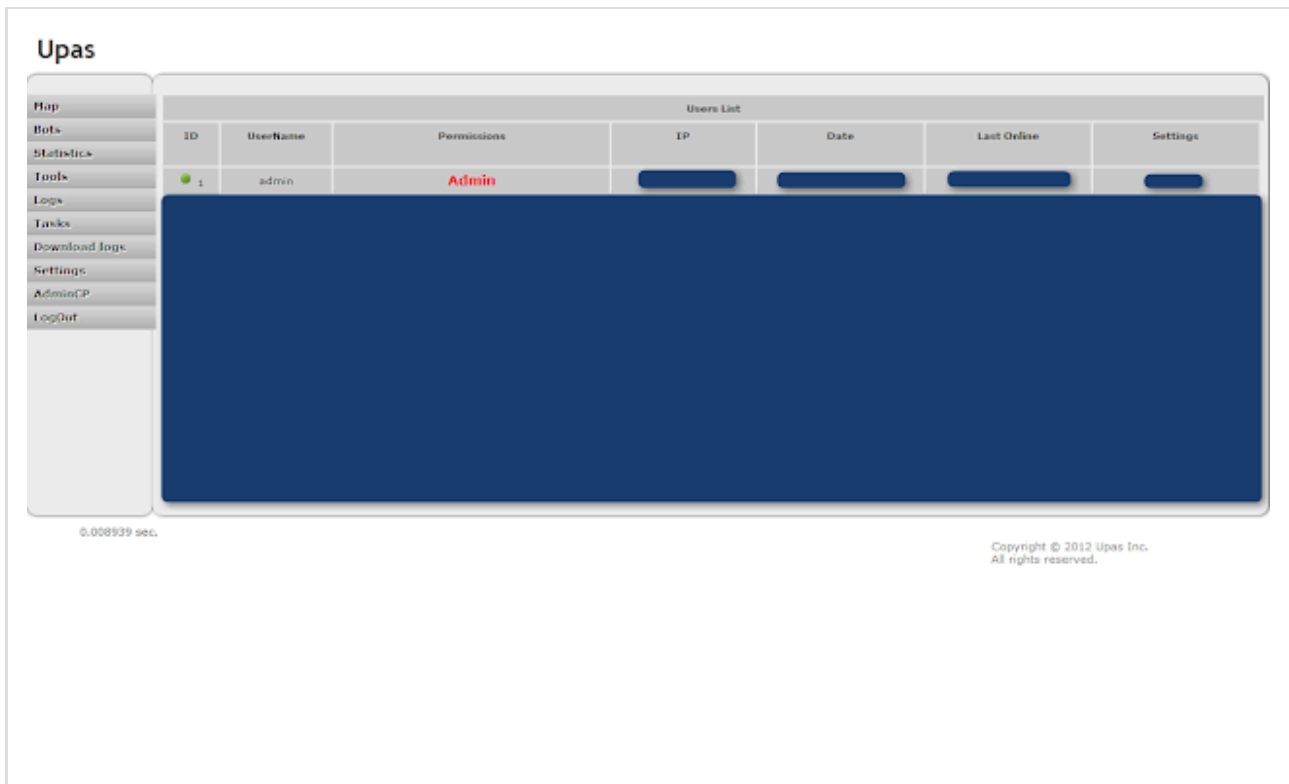
### Upas - Settings list



### Upas - Settings



Upas - Settings - Create user



Upas - Settings - Users list

# Upas

Banned Users							
ID	UserName	Permissions	IP	Date	Last Online	Settings	
[Redacted Content]							

- Home
- Bots
- Statistics
- Tools
- Logs
- Tasks
- Download logs
- Settings
- AdminCP
- LogOut

0.007709 sec.

Copyright © 2012 Upas Inc.  
All rights reserved.

Upas - Settings - Banned Users



# Upas

- Map
- Bots
- Statistics
- Tools
- Logs
- Tasks
- Download logs
- Settings
- AdminCP
- LogOut

## Login Logs

IP	Country	UserName	Password	Status	Date
edit					
	DE	admin		Success	
					

Showing rows  to  from

SortBy Ascending ▾

0.023261 sec.

Copyright © 2012 Upas Inc. All rights reserved.

### Upas - Settings - Login logs

### Upas

Home	AdminCP	<input type="text" value="admin_cont_panel"/>	<input type="button" value="Change"/>
Bots	Gate	<input type="text" value="gate"/>	<input type="button" value="Change"/>
Statistics	PublicStat	<input type="text" value="stat"/>	<input type="button" value="Change"/>
Tools	Captcha	<input type="text" value="captcha"/>	<input type="button" value="Change"/>
Logs	Index	<input type="text" value="index"/>	<input type="button" value="Change"/>
Tasks	Login	<input type="text" value="login"/>	<input type="button" value="Change"/>
Download logs			
Settings			
AdminCP			
LogOut			

0.006674 sec.

Copyright © 2012 Upas Inc. All rights reserved.

### Upas - Settings - Change files name

### Upas

Home	Max login attempts	<input type="text" value="5"/>
Bots	Max items on page	<input type="text" value="50"/>
Statistics	Loader dead after	<input type="text" value="7"/> Days
Tools	Admin Name	<input type="text" value="admin"/>
Logs	Admin Password	<input type="password" value="*****"/>
Tasks	Scan4you Login	<input type="password" value=""/>
Download logs	Scan4you Password	<input type="password" value=""/>
Settings		
AdminCP		
LogOut		

0.009441 sec.

Copyright © 2012 Upas Inc. All rights reserved.

### Upas - AdminCP

Nom	Pourcentage (g...)	Pourc...	> Taille	Éléme...	Fichiers	Sous...	Dernier changement
GeoIP	100%		3,1 Mo	344	335	9	2012
includes	57,2%		1,8 Mo	2	2	0	2012
js	18,0%		560,0 Ko	14	14	0	2012
js	10,3%		324,3 Ko	7	7	0	2012
!Fichiers>	5,9%		186,7 Ko	14	14	0	2012
index.php	52,8%		96,5 Ko				2012
admin_cont_panel.php	21,7%		40,5 Ko				2012
gate.php	7,4%		13,8 Ko				2012
page_header.php	4,7%		8,7 Ko				2012
login.php	4,1%		7,6 Ko				2012
captcha.php	2,0%		3,8 Ko				2012
public_stat.php	1,6%		2,9 Ko				2012
page_footer.php	1,5%		2,8 Ko				2012
dl_log.php	1,4%		2,7 Ko				2012
remote.php	1,1%		2,0 Ko				2012
error.php	1,0%		1,9 Ko				2012
.htaccess	0,4%		817 octets				2012
config.php	0,3%		603 octets				2012
ReadMe.txt	0,1%		151 octets				2012
flags	5,4%		171,5 Ko	258	258	0	2012
css	2,2%		70,7 Ko	18	17	1	2012
images	0,8%		26,1 Ko	20	20	0	2012
files	0,1%		1,8 Ko	2	2	0	2012
logs	0,0%		149 octets	1	1	0	2012

Extensi...	Co...	Description	> Octets	% C
.dat		DAT File	1,7 Mo	55
.php		PHP File	377,6 Ko	12
.ttf		TrueType font file	374,8 Ko	11
.js		JScript Script file	322,6 Ko	10
.gif		GIF File	175,4 Ko	5
.css		Cascading Style Sheet Docu...	46,7 Ko	1
.png		PNG File	41,1 Ko	1
.inc		INC File	40,7 Ko	1
.txt		TXT File	10,8 Ko	0
.ht...		HTACCESS File	1,1 Ko	0

Upas - Server Side Tree

Here is the initial advert on Exploit.In :

Upas Kit, Win32 - RemoteShell - MIT

Категории: | Стандартный | Раскрытый

14.06.2012, 09:48

Описание

Upas Kit - это модный MIT bot, который был создан с единственной целью - добавить азарт глорной боли. Это поданный MIT продукт, который не имеет ничего общего с Linux и Java. Также образом установка происходит "тихо" без опознаваемых антивирусами. В данный момент он работает на следующих версиях Windows: XP, Vista, 7 (32-bit), Server 2003, Server 2008. Помимо этого "привыкает" и со всеми версиями Linux. В текущей версии релиз выдвигается во все 32-битные процессоры. Проложенные кнопки на C++

**По умолчанию ядро поставляется со следующими модулями (дополнительные покупаются отдельно)**

- Kernel
- ExploitShellcode
- Crackmap
- AntiVM
- HTTP Fuzzer
- DoS

**Список модулей, которые можно приобрести отдельно:**

- LDAP grabber (LDAPGrabber)
- WinRM
- Form Grabber (SQLFuzzer)
- FTP Grabber
- Плохой Grabber - FTP/Smb/HTTP
- MSN Hook
- Win (Http, Http)
- Kernel
- Fast Breaker

**Цены актуальные 6/14/2012 числа:**

- Ядро \$200
- LDAP Grabber \$200
- FormGrabber \$1000
- Разрешение на 14 на даты \$10
- Разрешение на 14 на даты (если 2000 копий в акт, либо забронировать) \$20

Цены могут показаться завышенными, однако, если проанализировать сложность и эффективность данного софта цена становится обоснованной.

**Возможности панели:**

- Сюжет от машины
- Безопасность IP если доступ на сайт придет не от бота
- Безопасность IP в случае брота данных входа
- Детализация/Управление пользователями
- Управление сервером
- Сканер SQL-инъекций веб-сайтов для сканирования файлов, эксплойтов, IP, domains и т.д.
- Детальная статистика и использование Google Analytics
- Кнопка при входе в панель для локального процесса загрузки панели
- Панель и управление добавлением/удалением модулей и модулей ядра
- Полный список сайтов для крабов, возможность изменения сайтов крабовых форм крабов (Form Grabber) (Form Grabber)
- Список команд по странам
- Полный интерфейс
- Английский и русский языки

**Особенности бота:**

- Авто защита для предотвращения от анализа вашего файла
- Secure shell
- Сайт stealth
- Легко шифровать
- Многофункциональный домен. Сайт идет по домену, в случае неудачи берет следующий.
- Возможность вставки для произвольной подмены

**Поддержка:**

- 2009
- support@abbot.org
- www.kitrobot@abbot.org

ICQ: 134813

**Отказ от ответственности:**

Upas Kit было создано для выявления уязвимостей в информационных системах как частных лиц, так и организаций. Upas Kit никогда не использовался для совершения кибер-преступлений и таким быть не может. Покупая данный продукт вы соглашаетесь не нарушать законы Российской Федерации и других стран. Покупая данный продукт вы соглашаетесь что на свой страх и риск. Перед запуском приложения на ПК пользователи вы должны получить его согласие.

2012 Upas Inc. Все права защищены.

Upas Kit 1.0.0.0 as advertised by auroras on Exploit.in on the 14th of June 2012

You'll find the Original text of this advert here :

<http://pastebin.com/T8b0FMGA>

And its Google Translation here :

<http://pastebin.com/RCN0wYez>

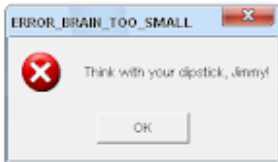


### Submission Summary:

- Submission details:
  - Submission received: 6 July 2012, 08:46:59 AM
  - Processing time: 9 min 30 sec
  - Submitted sample:
    - File MD5: 0x [REDACTED]
    - Filesize: 30,7 [REDACTED] bytes
    - Alias:
      - W32.SillyFDC [Symantec]
      - Mal/Behav-010 [Sophos]
      - Worm.Win32.Rombrast [Ikarus]

### Technical Details:

- The new window was created, as shown below:



### File System Modifications

- The following file was created in the system:

#	Filename(s)	File Size	File MD5	Alias / Other Info
1	[file and pathname of the sample #1]	30,7 [REDACTED] bytes	0x [REDACTED]	W32.SillyFDC [Symantec] Mal/Behav-010 [Sophos] Worm.Win32.Rombrast [Ikarus]

### Memory Modifications

- There was a new process created in the system:

Process Name	Process Filename	Main Module Size
[filename of the sample #1]	[file and pathname of the sample #1]	49,1 [REDACTED] bytes

Auroras 1 - ThreatExpert 0

For an analysis of Upas kit bot you can take a look at [Onthar's post](#).

Here one Anubis analysis : [149fd4bdae313f2e44d86cc9be7e2453a](#) - And here a Comodo IMA analysis : [7847d831a191833b7b845d95daf8d0c19f42322c53882c7814a0cb2cb7d9f195](#)

(no..these are not bots of the C&C shown here ;) )

Source: <https://malware.dontneedcoffee.com/2012/08/inside-upas-kit1.0.1.1.html>