

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

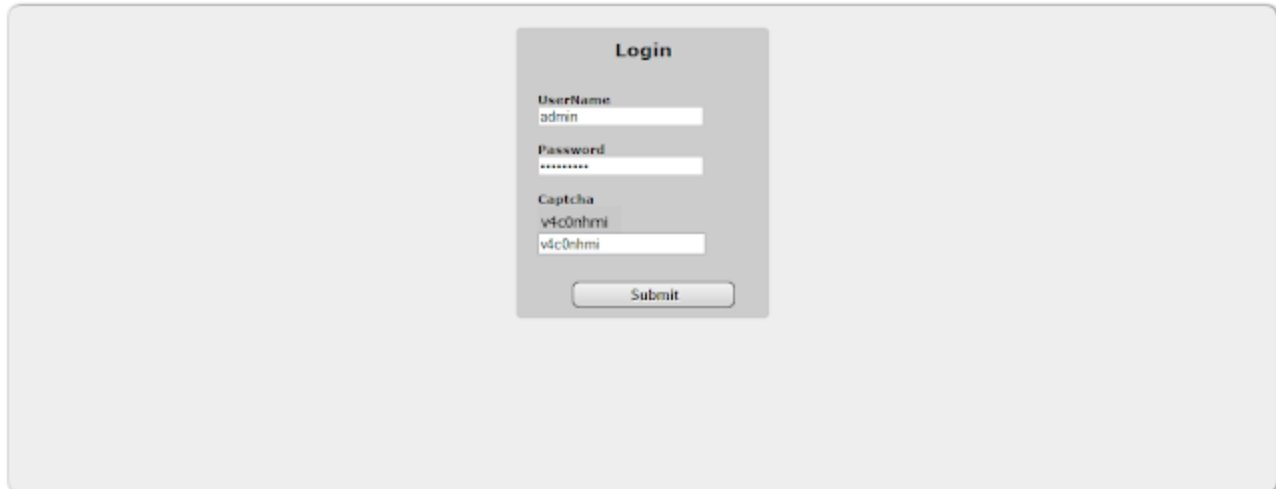
 malware.dontneedcoffee.com/2012/08/inside-upas-kit1.0.1.1.html

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
v4c0thmi
v4c0thmi

Submit

Upas - Login Screen

Upas

Upas - Map

Upas

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	2012	Online
[Redacted]	[Redacted]	[Redacted]	x86	2	Admin	1.0.1.1	MAIN	N/A	2012	2012	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]	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]	IQ	[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]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	[Redacted]	Online

Upas - Bots

Upas

Map	Bots Online	Online Bots	Arch	Countries	Comparing most	Spreading	Botkill	Ruskill	FTP
Bots	Passwords	Bots Summary Statistics			Version		OS	Permissions	
Statistics	Bots Online								
Tools									
Logs		Online last 15 min:							
Tasks		Online last 15 min:							
Download logs		Online last 1 hr:							
Settings		Online last 6 hr:							
AdminCP		Online last 12 hr:							
LogOut		Online last 24 hr:							
		Online last 2 days:							
		Online last 3 days:							
		Online last 4 days:							
		Online last 5 days:							
		Online last 6 days:							
		Online last 7 days:							

0.637772 sec.

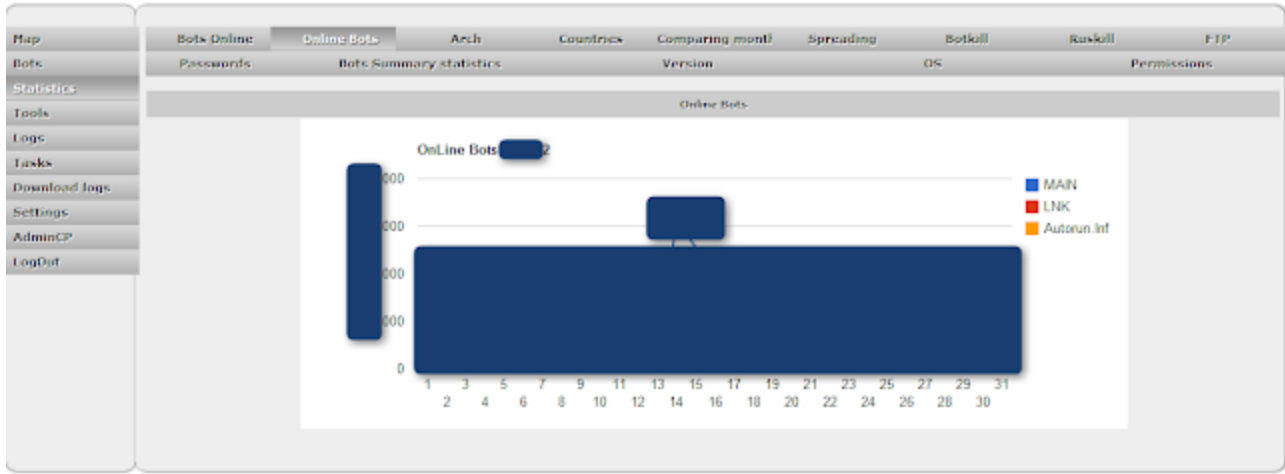
Copyright © 2012 Upas Inc.
All rights reserved.

Waiting for ajax.googleapis.com...

18

Upas - Statistics - Bots Online

Upas

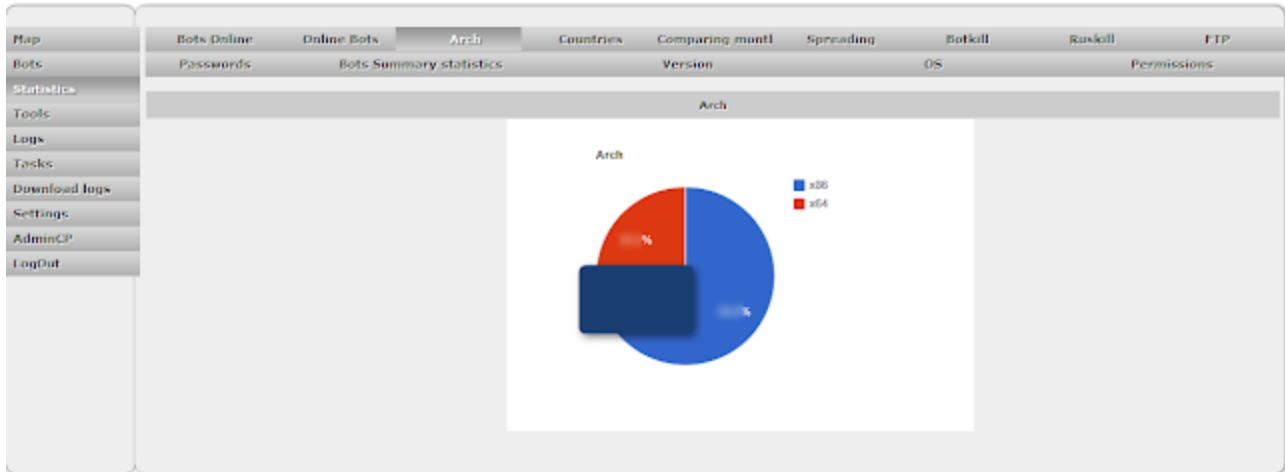


0.669734 sec.

Copyright © 2012 Upas Inc. All rights reserved.

Upas - Statistics - Online Bots

Upas

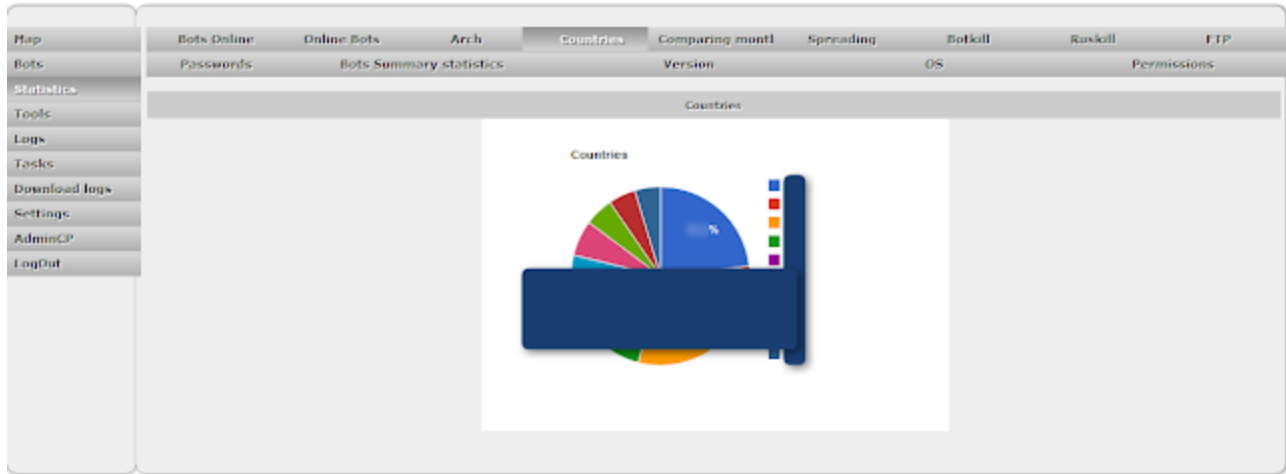


0.669734 sec.

Copyright © 2012 Upas Inc. All rights reserved.

Upas - Statistics - Arch

Upas



0.669734 sec.

Copyright © 2012 Upas Inc.
All rights reserved.

Upas - Statistics - Countries

Upas

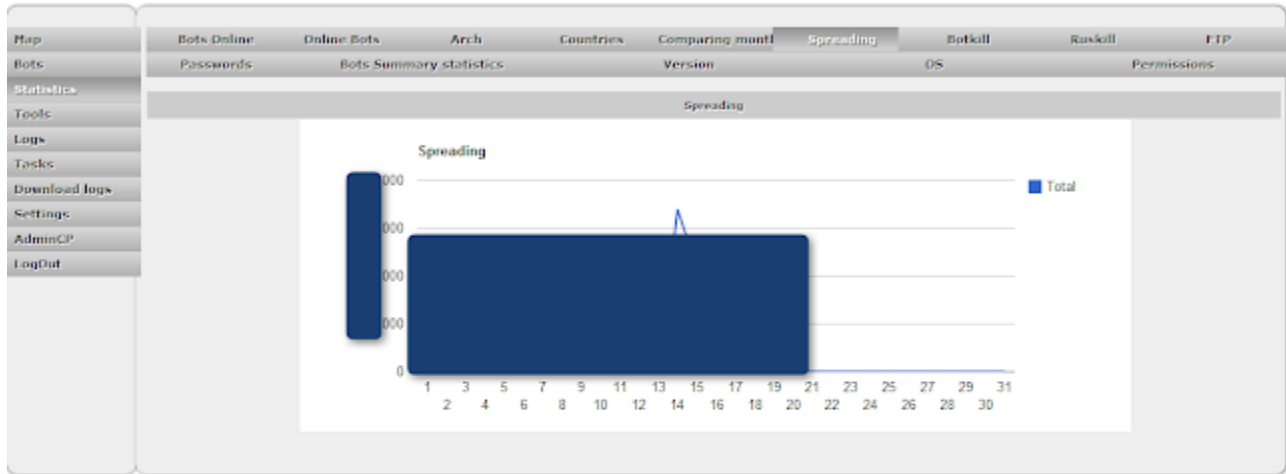


0.669734 sec.

Copyright © 2012 Upas Inc.
All rights reserved.

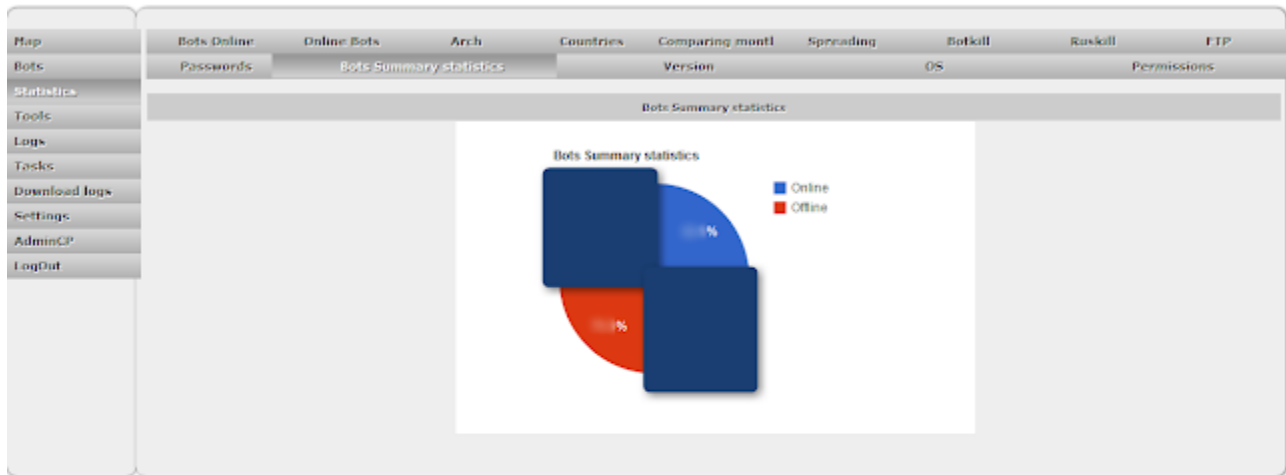
Upas - Statistics - Comparing months

Upas



Upas - Statistics - Spreading

Upas



Upas - Statistics - Bots Summary statistics

Upas

Map Bots Online Online Bots Arch Countries Comparing monthl Spreading Botkill Raskill FTP

Bots Passwords Bots Summary statistics Version OS Permissions

Statistics

Tools

Logs

Tasks


Download logs

Settings

AdminCP

LogOut

Version



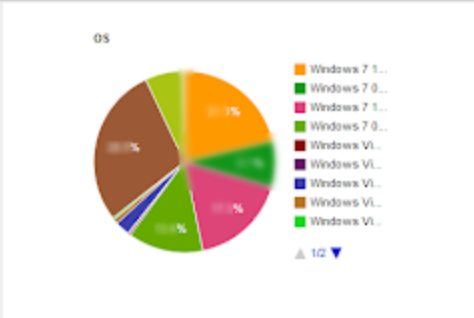
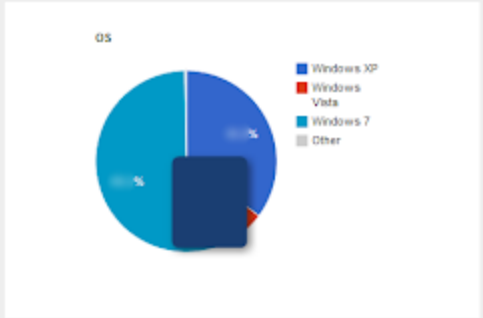
A pie chart titled "Version" showing a single blue slice representing 100% of the data. A legend to the right of the chart shows a blue square next to the text "1.0.1.1".

Version	Percentage
1.0.1.1	100%

0.059734 sec.

Copyright © 2012 Upas Inc.
All rights reserved.

Upas - Statistics - Version

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

0.669734 sec.

Copyright © 2012 Upas Inc. All rights reserved.

Upas - Statistics - OS

Upas

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

Bots Online: Online Bots Arch Countries Comparing month Spreading Botkill Raskill FTP
Passwords Bots Summary statistics Version OS Permissions

Permissions

A pie chart titled 'Permissions' showing the distribution of permissions between 'User' (blue) and 'Admin' (red). The chart is divided into two equal halves, each representing 50%. A vertical blue bar is overlaid on the chart.

Role	Percentage
User	50%
Admin	50%

0.669734 sec.

Copyright © 2012 Upas Inc.
All rights reserved.

Upas - Statistics - Permissions

Upas

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

File Aucun fichier choisi

URL

Domain/IP/

Exploit Pack

0.009250 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 Riskill 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 | Ruskill | InjectIs

Search ...

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

Showing row [] from []

Pages [] OK

0.015175 sec.

Copyright © 2012 Upas Inc.
All rights reserved.

Upas - Logs - Spreadings

Upas

Map FTP Spreadings **Botkill** Passwords Riskill Injects

Bots

Statistics

Tools

Logs

Tasks

Download logs

Settings

AdminCP

LogOut

Search ...

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

0.009654 sec.

Copyright © 2012 Upas Inc.
All rights reserved.



Upas - Logs - Botkill

Upas

Map FTP Spreading Botkill Passwords Riskill Injects

Search

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 1 to 13 from [redacted] Next

Pages [redacted] OK

0.009745 sec. Copyright © 2012 Upas Inc. All rights reserved.

Upas - Logs - Passwords

Upas

Map
Bots
Statistics
Tools
Logs
Tasks
Download logs
Settings
AdminCP
LogOut

FTP Spreadings Botkill Passwords **Ruskill** Injects

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

Map
Bots
Statistics
Tools
Logs
Tasks
Download logs
Settings
AdminCP
LogOut

FTP Spreadings Botkill Passwords Ruskill **Injects**

Search ...

ID	Country	IP	Date	View
[Large blue rectangular area]				

0.000148 sec.

Upas - Logs - Injects

Upas

The screenshot shows the Upas interface with a sidebar on the left containing menu items: Map, Bots, Statistics, Tools, Logs, Tasks, Download logs, Settings, AdminCP, and LogOut. The main area is titled "Task" and contains several configuration fields: "Task" (a dropdown menu with "Update" selected and a sub-menu open showing "Update", "Download and execute", "Details", and "Uninstall"), "Limit", "Mode" (set to "Continuous"), "Country" (set to "All"), "OS" (set to "All"), and "Arch" (set to "All"). A "Submit" button is located below these fields. On the right side, a blue box labeled "Public Link" has an arrow pointing to a small icon in the bottom right corner of the task table. Below the configuration fields is a table with the following columns: Task, Details, Mode, Cost, Link, Country, OS, Arch, Status, and Edit. The table contains one row with the task "Download and execute", a red minus sign in the Details column, "Continuous" in the Mode column, and "ALL" in the OS, Arch, and Status columns. The bottom left corner shows "0.01086 sec" and the bottom right corner shows "Copyright © 2012 Upas Inc. All rights reserved."

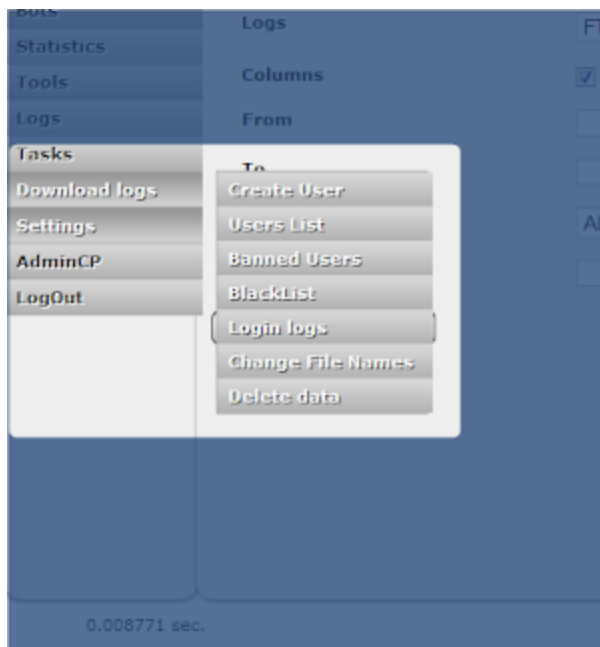
Upas - Tasks

The screenshot shows a browser window with the address bar containing "remote.php?key=". Below the address bar is a table with the following columns: Sent, Limit, Task, Details, Country, OS, and Arch. The table body is currently empty, represented by a large dark blue rectangular area.

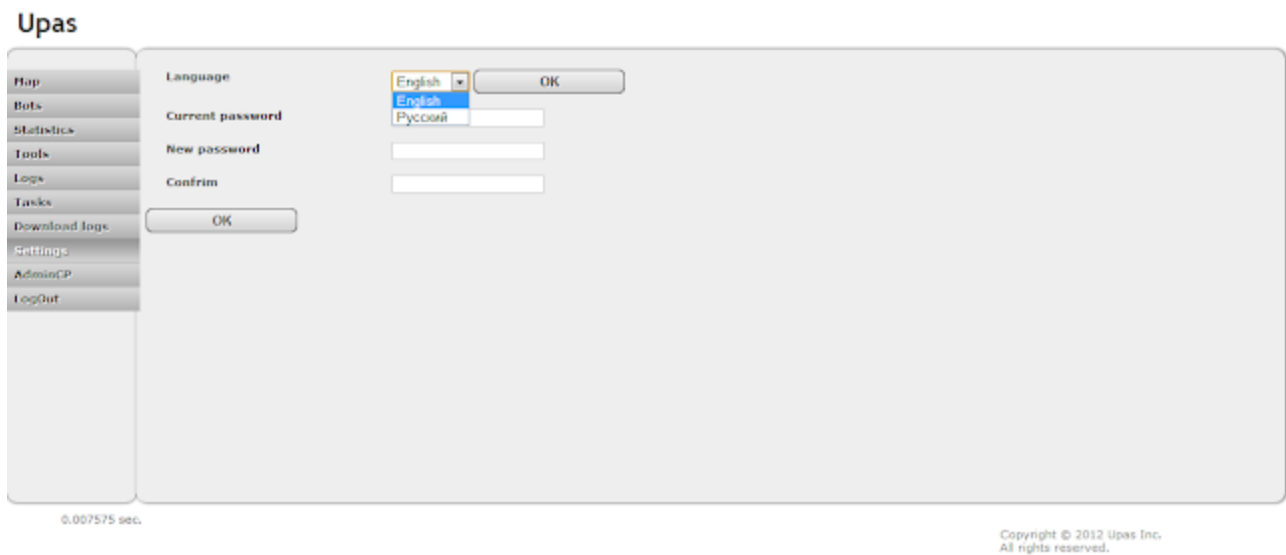
Upas - Public Link to tasks

The screenshot shows the Upas interface with the sidebar on the left containing menu items: Map, Bots, Statistics, Tools, Logs, Tasks, Download logs, Settings, AdminCP, and LogOut. The main area is titled "DownloadLogs" and contains several configuration fields: "Logs" (a dropdown menu with "FTP" selected and a sub-menu open showing "FTP", "Spreading", "Betkill", "Passwords", "Ruskill", and "Injects"), "Columns" (checkboxes for "port", "username", "password", and "date", all of which are checked), "From", "To", "Country" (set to "ALL"), and "Limit". A "Submit" button is located below these fields. The bottom left corner shows "0.011462 sec" and the bottom right corner shows "Copyright © 2012 Upas Inc. All rights reserved."

Upas - Download logs



Upas - Settings list



Upas - Settings

Upas

Map
Bots
Statistics
Tools
Logs
Tasks
Download logs
Settings
AdminCP
LogOut

UserName:
Password:

Permissions:
Access to commands:
 Formgrabbers ON
 Formgrabbers OFF
 DNS
 Visit

Access:
 View Statistics
 View FTP
 View Spreading
 View Botkill
 View Passwords
 Add Task
 Delete Task
 Edit Task
 Enable Task
 Create User
 Download Logs
 View Map
 View Tools
 Search
 View Ruskill
 View Bots
 Settings
 View Tasks

0.007531 sec.

Copyright © 2012 Upas Inc.
All rights reserved.

Upas - Settings - Create user

Upas

Map
Bots
Statistics
Tools
Logs
Tasks
Download logs
Settings
AdminCP
LogOut

Users List

ID	UserName	Permissions	IP	Date	Last Online	Settings
1	admin	Admin				

0.008939 sec.

Copyright © 2012 Upas Inc.
All rights reserved.

Upas - Settings - Users list

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

0.007709 sec.

Copyright © 2012 Upas Inc.
All rights reserved.



Upas - Settings - Banned Users

Upas

Navigation menu:

- Map
- Bofs
- Statistics
- Tools
- Logs
- Tasks
- Download logs
- Settings
- AdminCP
- LogDat

Table: Login Logs

IP	Country	Username	Password	Status	Date
ede					
	DE	admin	<input type="password"/>	Success	<input type="text"/>
					

Showing rows: from SortBy: Ascending

0.023261 sec.

Copyright © 2012 Upas Inc.
All rights reserved.

Upas - Settings - Login logs

Upas

Map	AdminCP	<input type="text" value="admin_conf_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

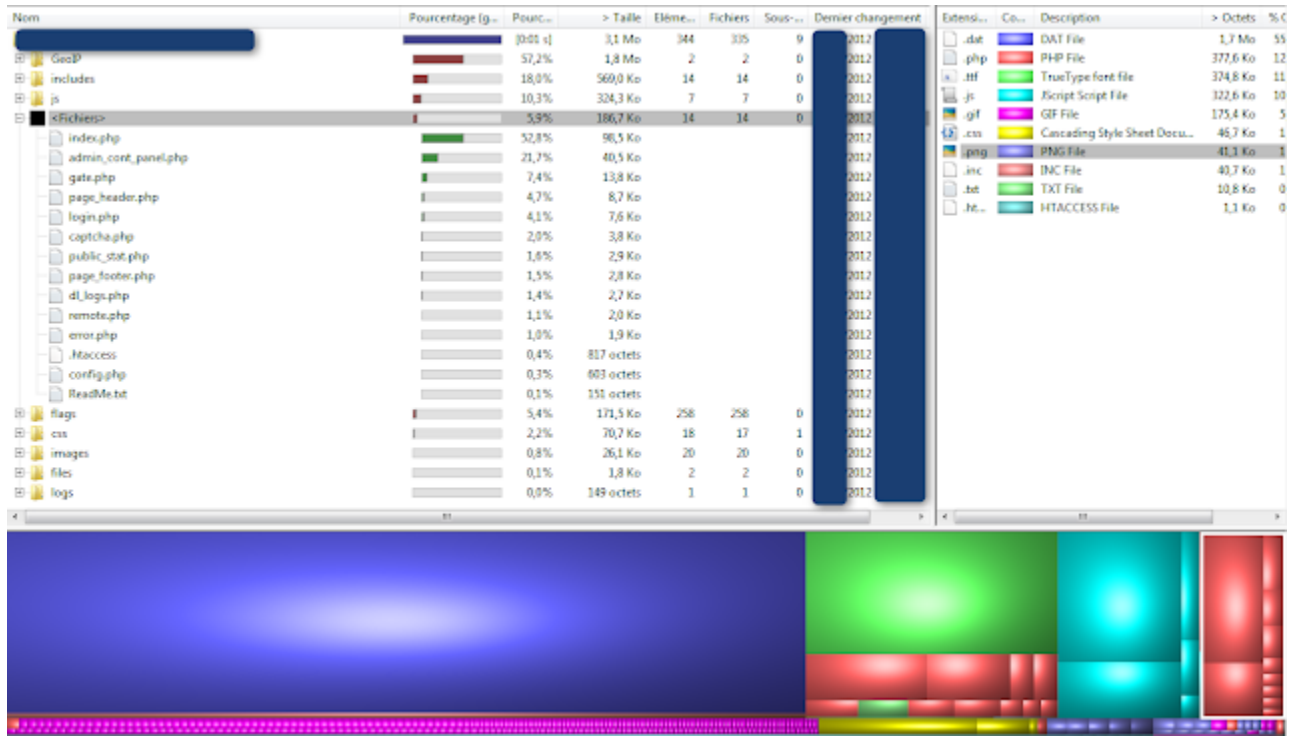
Upas

Map	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	Scantyou Login	<input type="password"/>
Download logs	Scantyou Password	<input type="password"/>
Settings		
AdminCP		
LogOut		
	<input type="button" value="Submit"/>	

0.009441 sec.

Copyright © 2012 Upas Inc.
All rights reserved.

Upas - AdminCP



Upas - Server Side Tree

Here is the initial advert on Exploit.In :

Exploit Kit 1.0.0.0

Описание:

Uras - это модный MITM бот, который был создан с единственной целью - добавить вас от главной боли. Это продвинутый MITM руглет, имеющий что-то общее со Zruba и Ziva. Точно образом установка происходит "как" без опознавания активности. В данный момент он работает на следующих версиях Windows: XP, Vista, 7 (Service Pack 2003, Service 2009). Помимо этого "известен" и со всеми версиям пакета. В текущей версии руглет выводится на все 32-х битные процессоры. Приложение написано на C++.

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

- EvilWin
- DenialofService
- UrasBot
- AntiVirus
- HTTP Flood
- DoS

Список модулей, которые можно приобрести отдельно:

- Uras evildoer (UK/US/DM)
- BotKill
- Root Grabber (S/PK/OS/MS)
- IP Grabber
- Rootkit Packard - S/PK/OS/MS/UDF
- OS Hook
- Uras (Hook, Shell)
- UrasBot
- Uras BotGrabber

Цены актуальные 6/14/2012 числа:

- Uras - \$2000
- Uras BotGrabber - \$200
- Uras evildoer - \$1000
- Uras BotKill - на по не данные \$10
- Uras BotKill - с входом другим данным (Uras BotKill посылать в лист, либо забронировать) \$50

Цены могут показаться завышенными, однако, если принять во внимание надежность и эффективность данного софта цена становится обоснованной.

Возможности панели:

- Сбор от packetflood
- Вывод IP адресов на сайт прилетев на от бота
- Вывод IP в случае бота данных входа
- Добавление/удаление/управление пользователями
- Журнал запросов
- Скрипты бан/убит, индивидуальный веб-дизайн для маскировки файла, включение, ID, домена и т.д.
- Детальная статистика с использованием Google Analytics
- Вывод при входе в панель для размещения рекламы на сайте
- Практика и управление добавлением/удалением модулей с параметрами
- Полный список сайтов для кражи, возможность изменения сайта на кражиных форм (Uras Grabber)
- Отправка команды по страницам
- Простой интерфейс
- Английский и русский языки

Особенности бота:

- Авто загрузка для предоставления от анализа своего файла
- Скорость 1000 rps
- Сайт-оператор
- Легко крафтить
- Неограниченное число доменов. Страница идет по доменам, в случае недачи берет следующий.
- Возможность вставки для произвольной подмены

Поддержка:

2009-
uras@exploit.in
uras@exploit.in
uras@exploit.in

ICQ: 134819

Отказ от ответственности:

Uras Kit было создано для выявления уязвимостей в информационных системах как частных лиц, так и организаций. Uras Kit никогда не использовался для сознательной кражи информации и должен быть не может. Покупая данный продукт вы соглашаетесь не наносить вреда физической инфраструктуре и другим странам. Покупая данный продукт вы соглашаетесь использовать его на свой страх и риск. Перед загрузкой приложения на ПК пользователи должны получить его согласие.

2012 Uras Inc. Все права защищены.

Uras 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>

Re: upass kit malware sample : antivm
 By EP_XOFF • Fri Jul 06, 2012 3:07 am

What kind of antivirus you found inside? As for me it b primitive mass injector with mass installed ring3 hooks it uses for hiding, including hiding copy of explorer.exe

```

##
[1184]explorer.exe-->HIDataValueKey, Type: Inline - RelativeJump 0x7C902250-->01F7429C [unknown_code_page]
[1184]explorer.exe-->HIDEnumerateValueKey, Type: Inline - RelativeJump 0x7C9031D0-->01F74750 [unknown_code_page]
[1184]explorer.exe-->HIOpenProcess, Type: Inline - RelativeJump 0x7C9025C3-->01F741D3 [unknown_code_page]
[1184]explorer.exe-->HIQueryDirectoryFile, Type: Inline - RelativeJump 0x7C902733-->01F74712 [unknown_code_page]
[1184]explorer.exe-->HIQuerySystemInformation, Type: Inline - RelativeJump 0x7C902913-->01F744B3 [unknown_code_page]
[1184]explorer.exe-->HIResumeThread, Type: Inline - RelativeJump 0x7C902623-->01F741FE [unknown_code_page]
[1184]explorer.exe-->HISetInformationFile, Type: Inline - RelativeJump 0x7C902C40-->01F74515 [unknown_code_page]
[1184]explorer.exe-->HISetValueKey, Type: Inline - RelativeJump 0x7C902660-->01F7437D [unknown_code_page]
[1184]explorer.exe-->HIWriteFile, Type: Inline - RelativeJump 0x7C902F40-->01F745E4 [unknown_code_page]

```

```

CODE SELECT ALL
TC9002D0:  X978744385      jmp 01K1675D8
TC9002D5:  BA3333FE7F      mov edi, 7FFE3338h
TC9002DA:  FF52           call [edi]
TC9002DC:  C21833        scasd 0018h

```

Boring crap, Sp0tIve was better.

```

CODE SELECT ALL
GetVolumeInformationW($RootPathName, 0, 0, $VolumeSerialNumber, 0, 0, 0, 0):
if ( $VolumeSerialNumber == 0xC01A93 || $A8_402999C == 1 )
{
    MessageBox(0, "Think with your dipstick, Jimmy!", "ERROR_BRAIN_TOO_SMALL", 0x10);
    ExitProcess($dumb);
}

```

Ring0 - the source of inspiration

AntiVM analysis by EP_XOFF:

You'll find it here :

<http://www.kernelmode.info/forum/viewtopic.php?f=16&t=1736&p=14437&hilit=upas#p14462>

Auroras "reply" on this code :

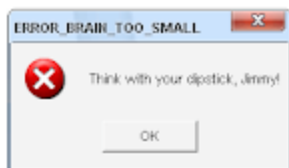
Which mean he did that fast to escape ThreatExpert. And it looks like it's pretty effective :

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 ;))