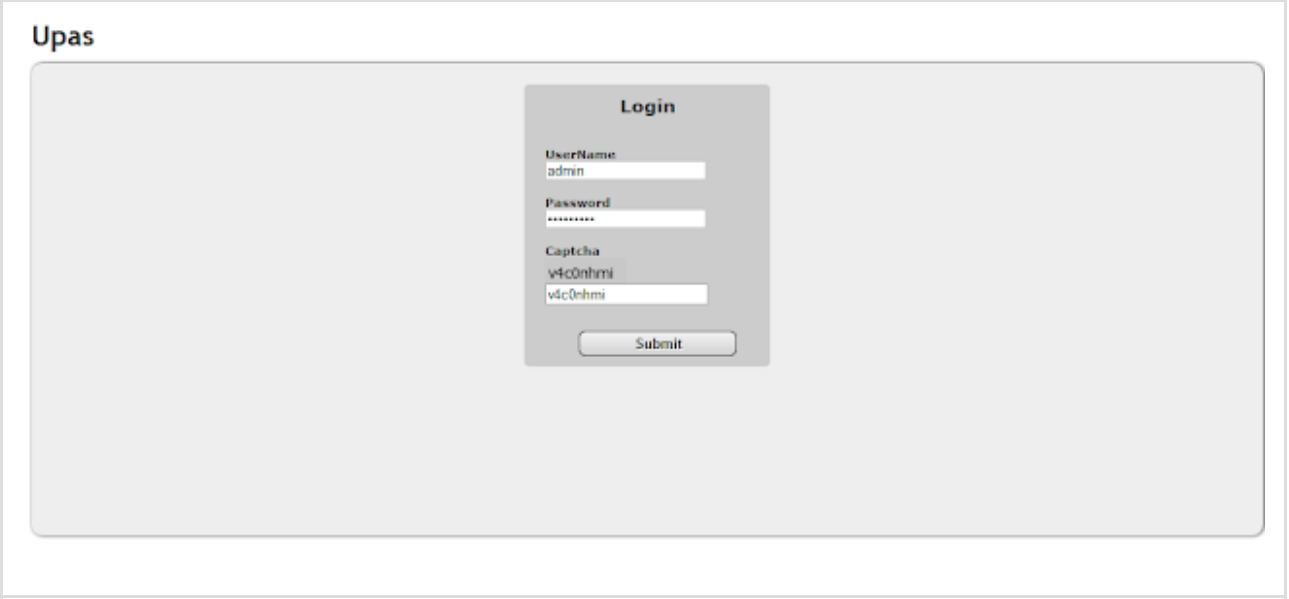
Inside Upas Kit (1.0.1.1) aka Rombrast C&C - Botnet Control Panel

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

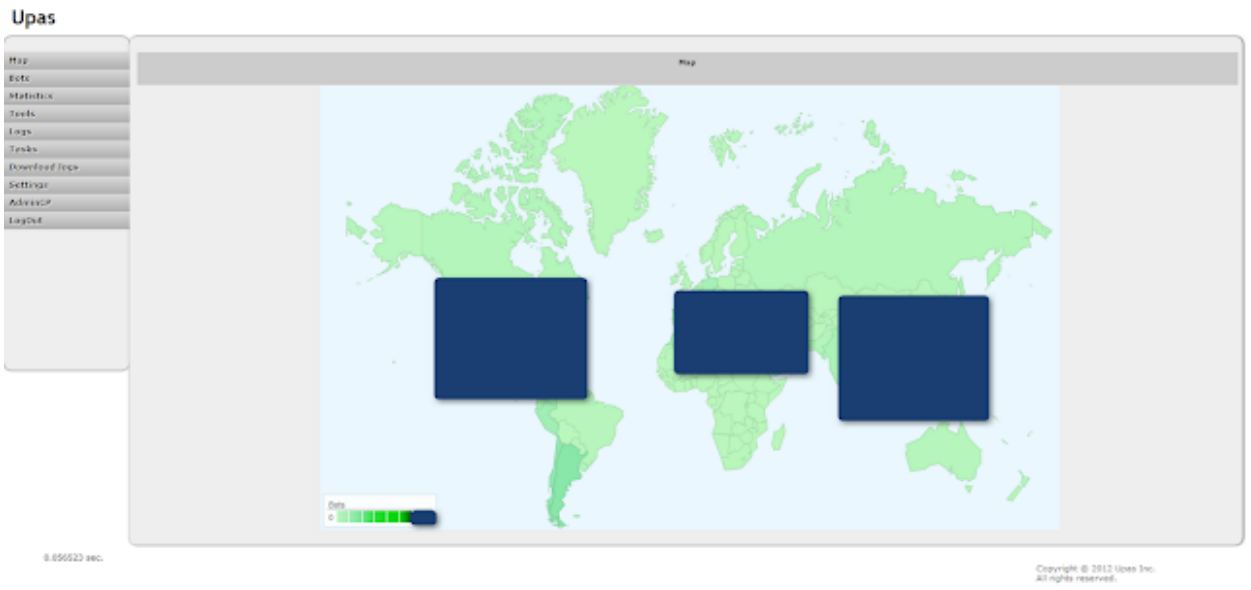
2012-08-16 - Panel

Upas

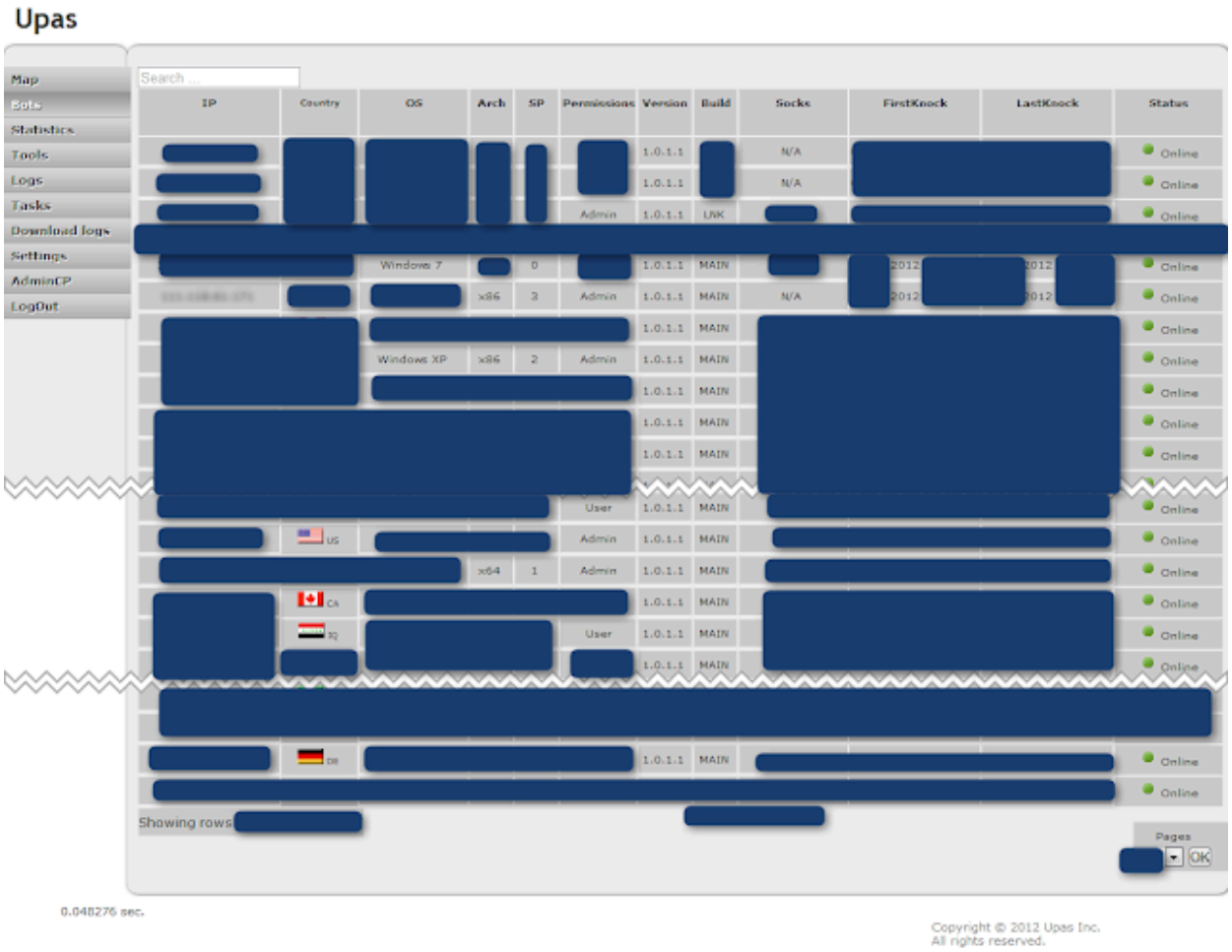
In middle of june a new botnet was advertised on underground forum as Upas Kit. (see end of this post for advert). Bot is recognized by Microsoft in Win32/Rombrast familly



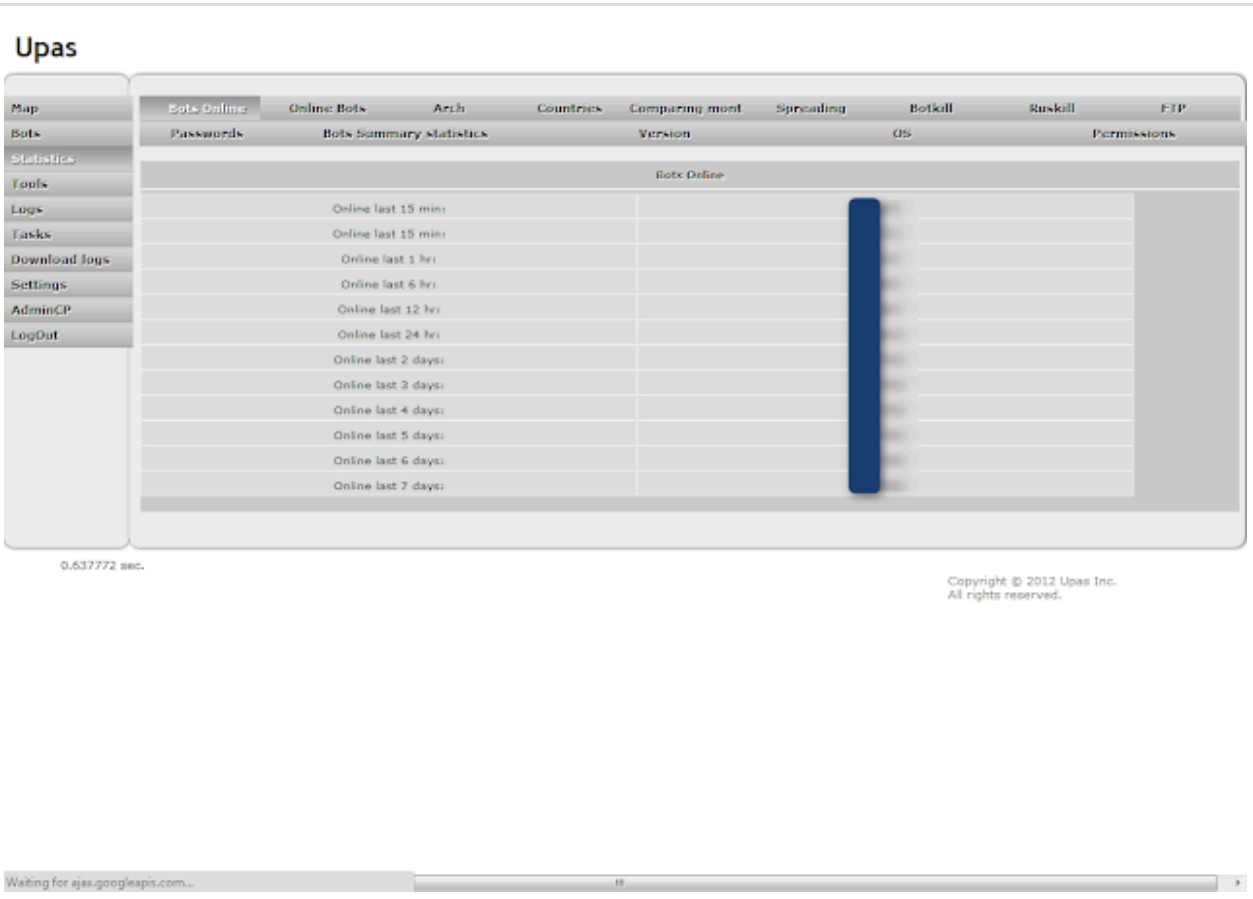
Upas - Login Screen



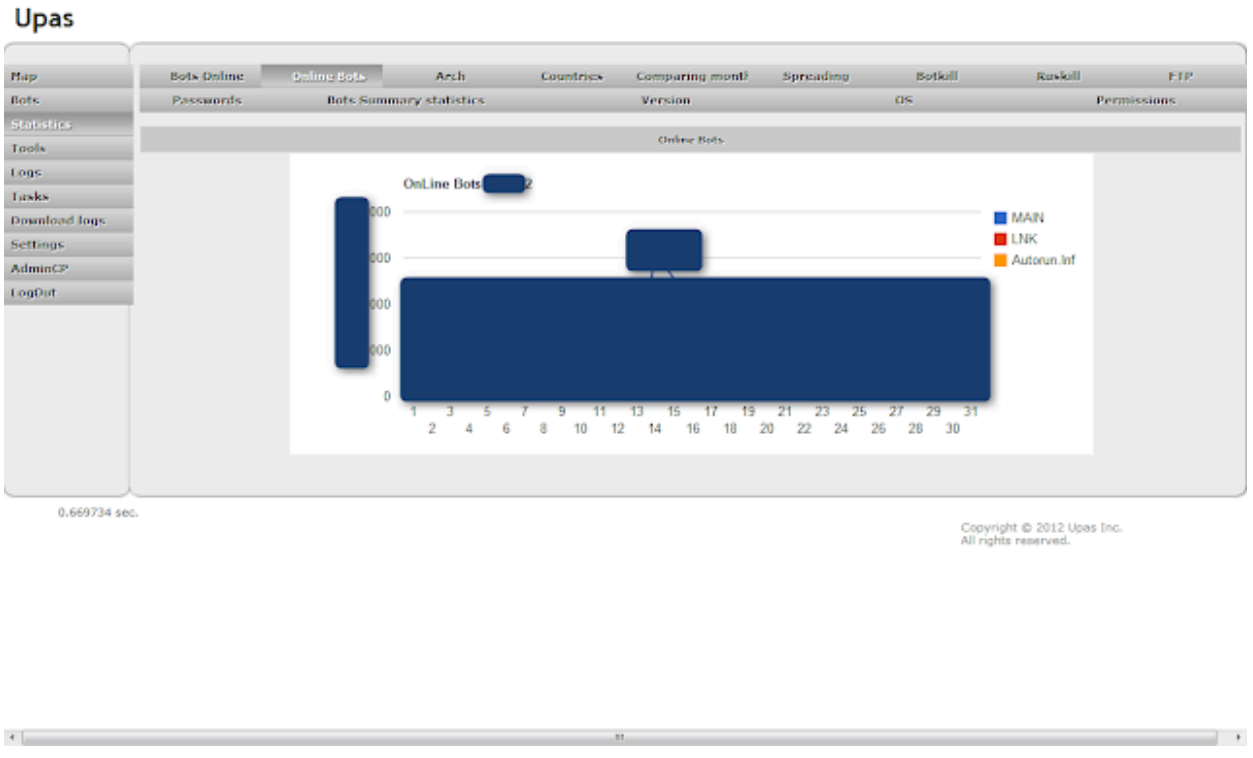
Upas - Map



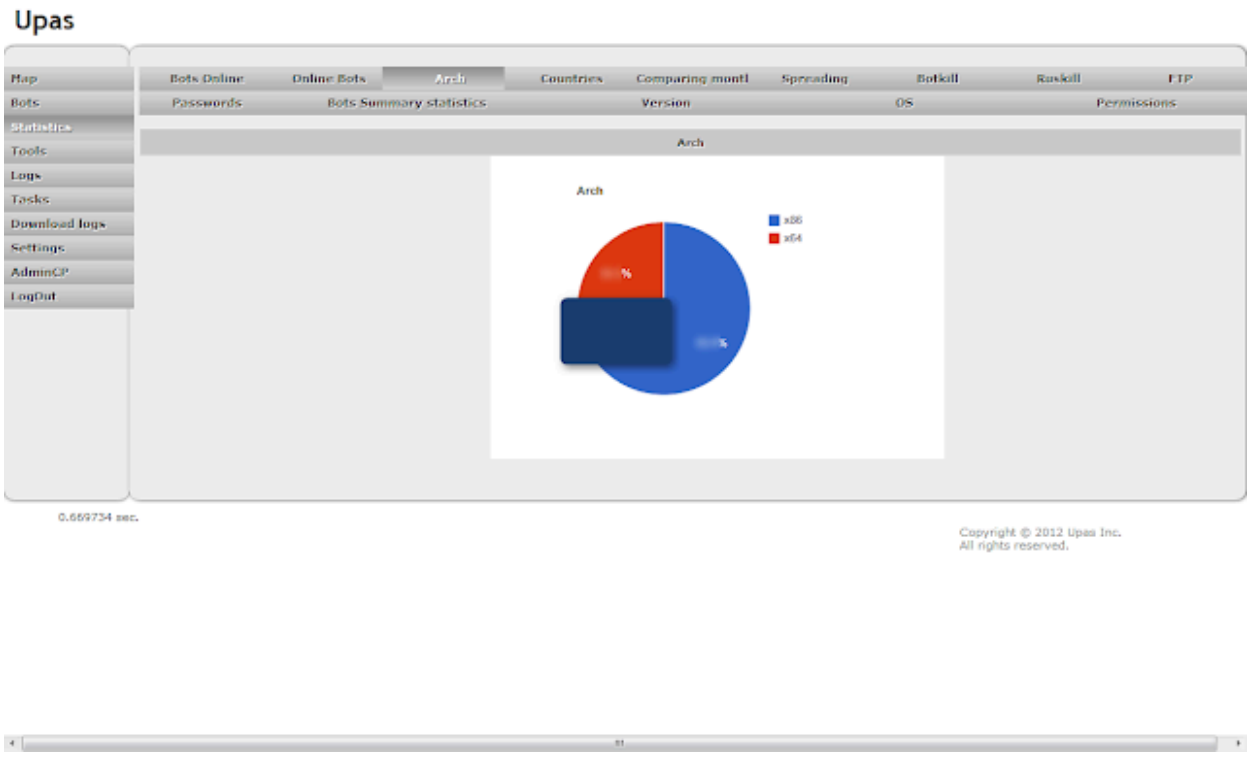
Upas - Bots



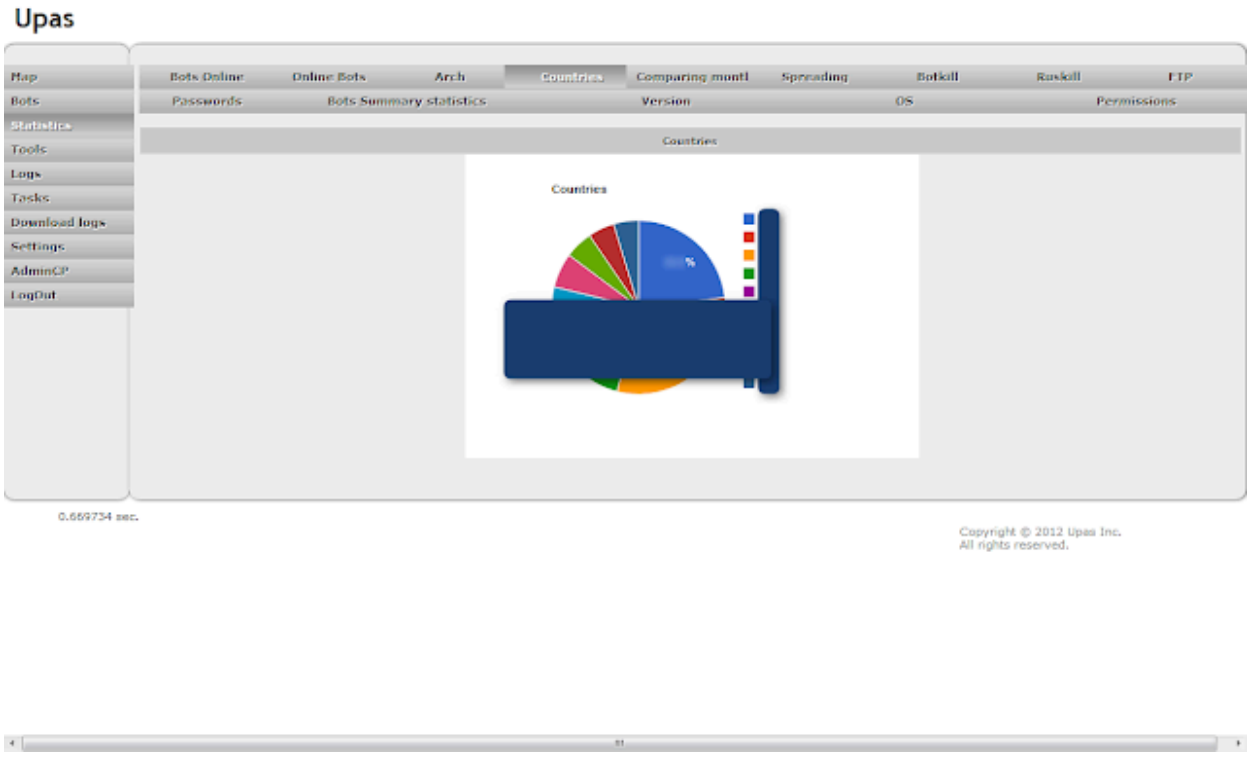
Upas - Statistics - Bots Online



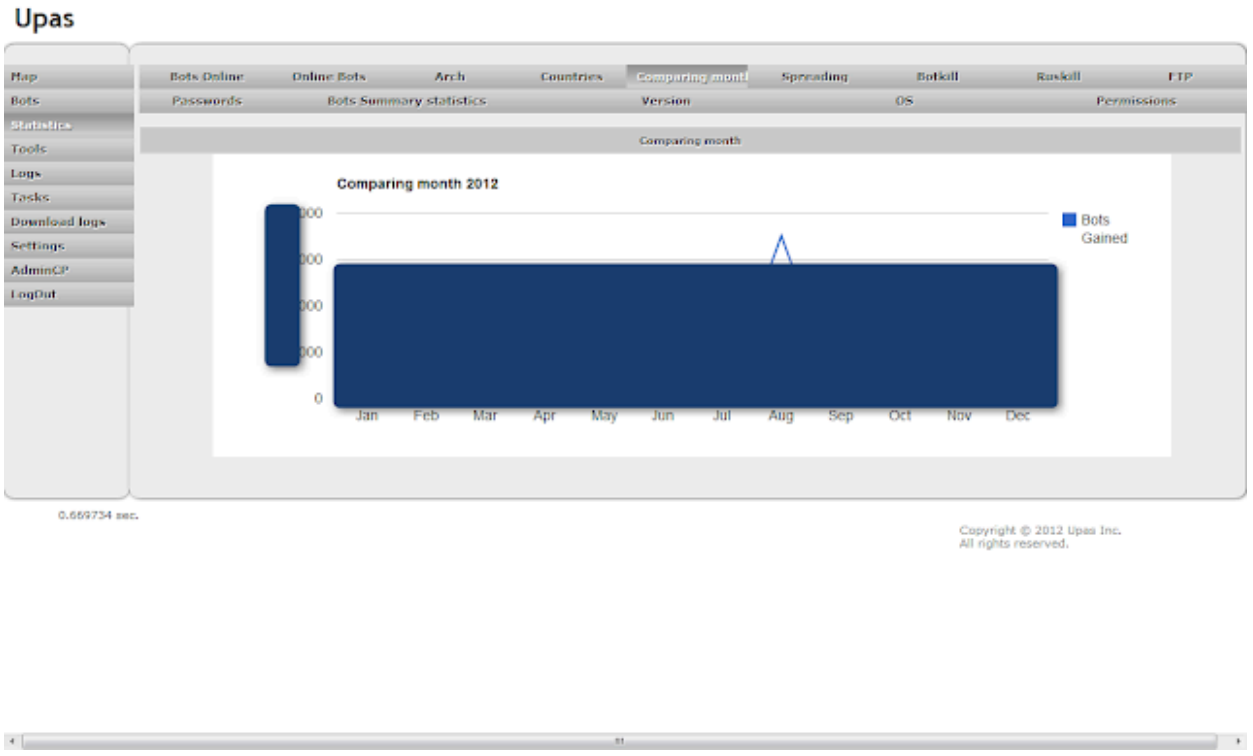
Upas - Statistics - Online Bots



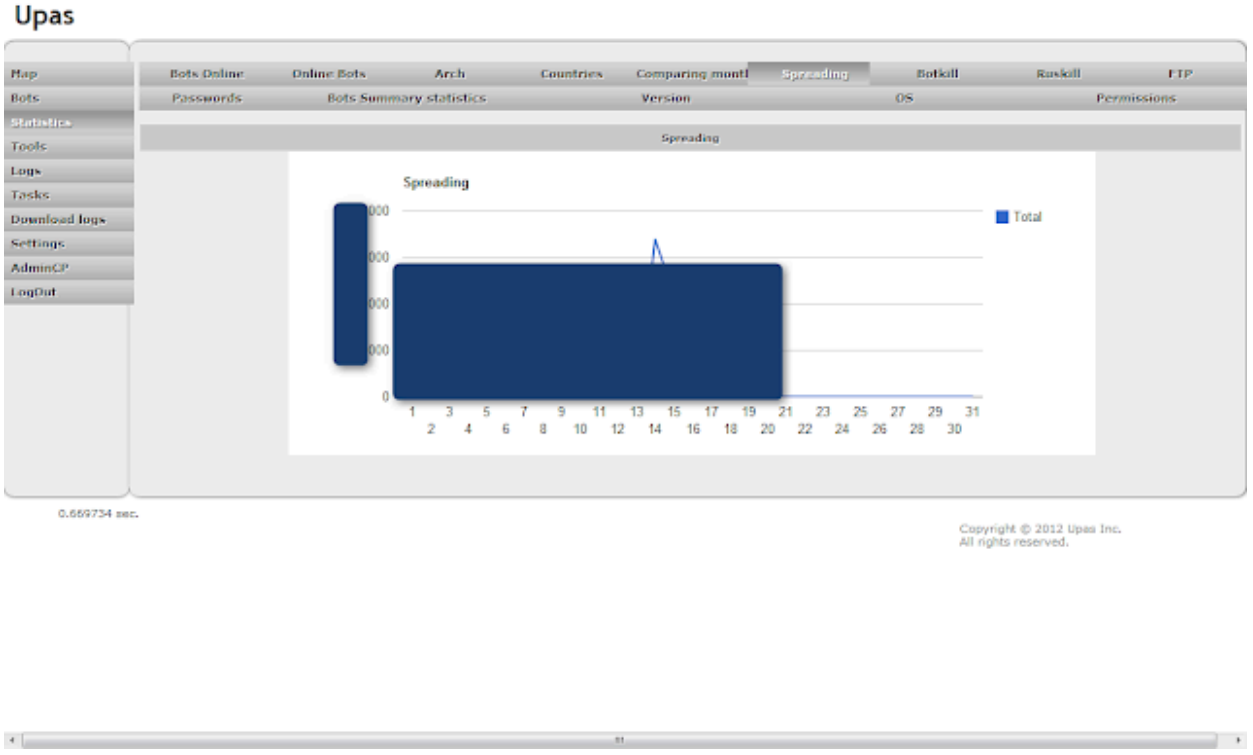
Upas - Statistics - Arch



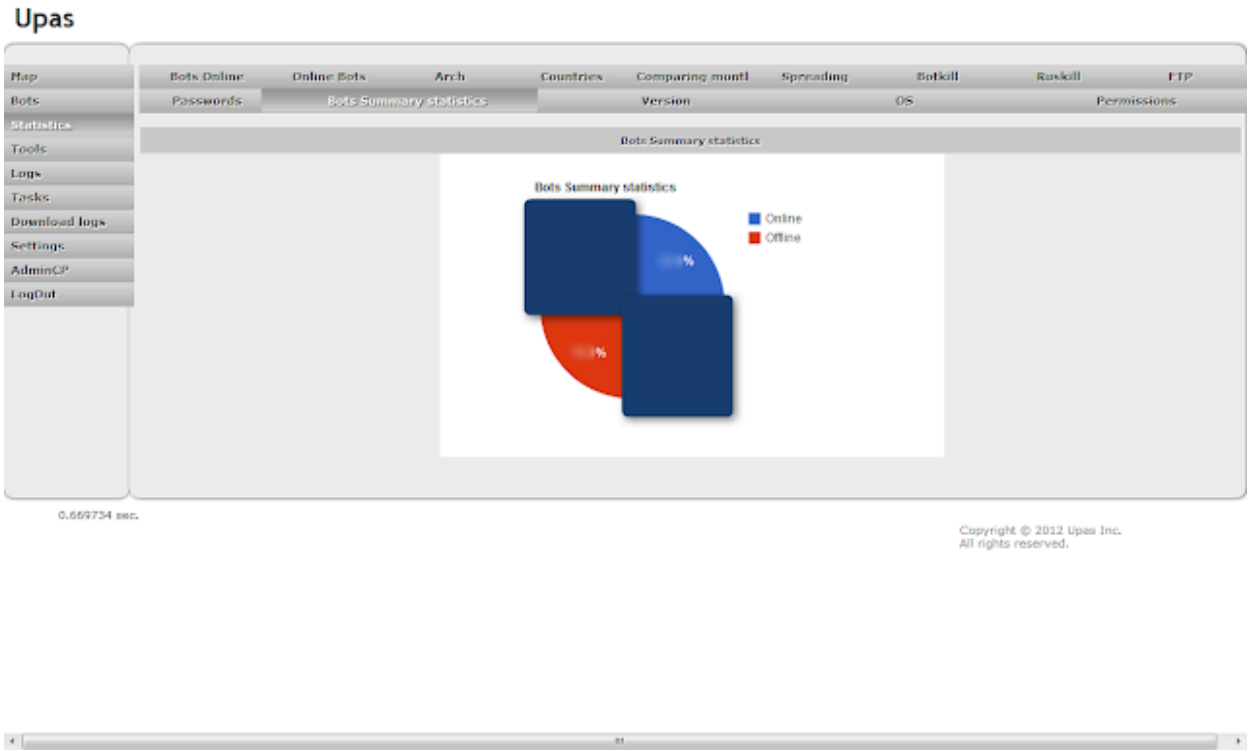
Upas - Statistics - Countries



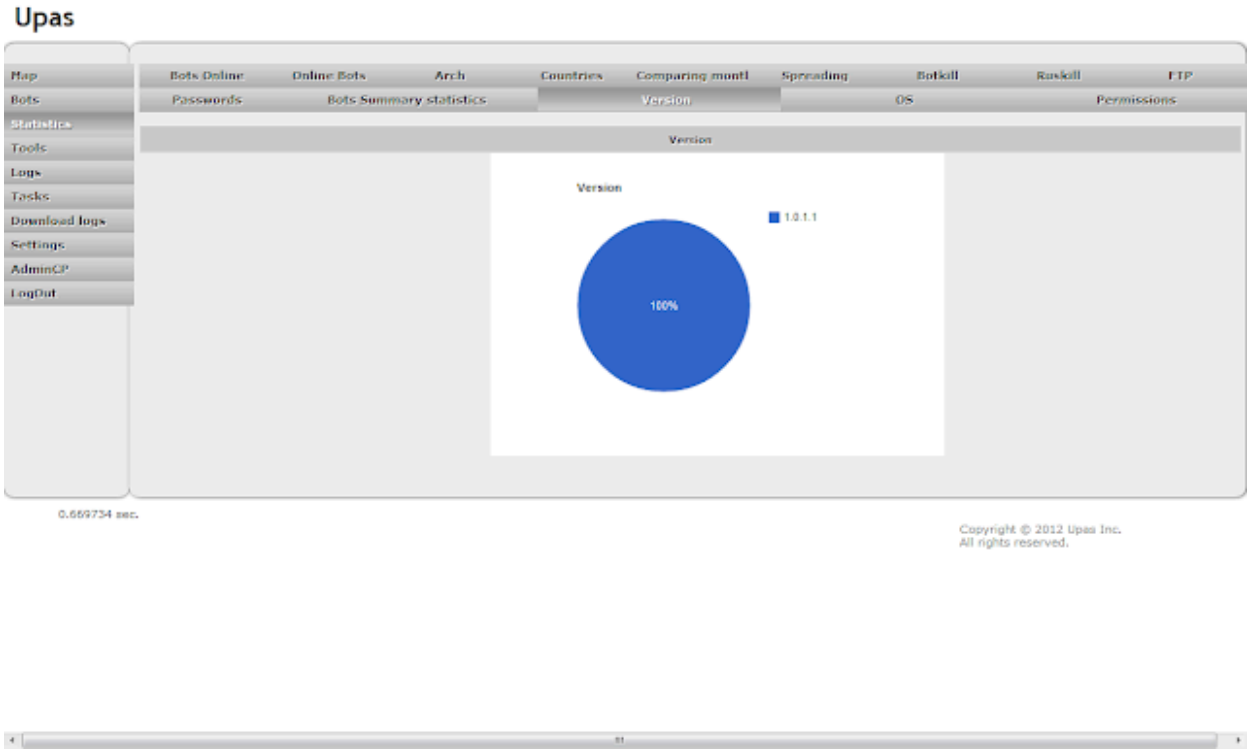
Upas - Statistics - Comparing months



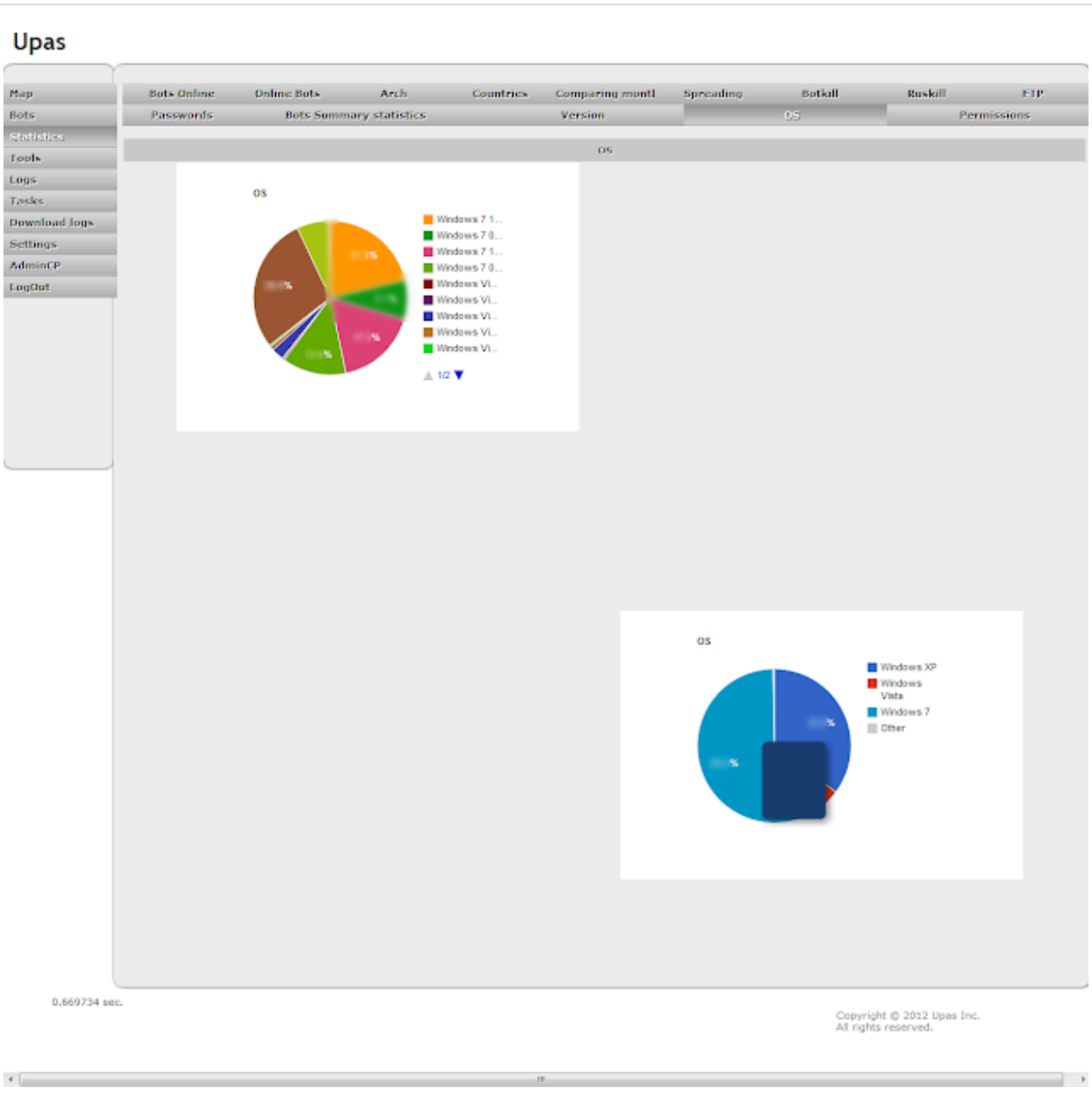
Upas - Statistics - Spreading



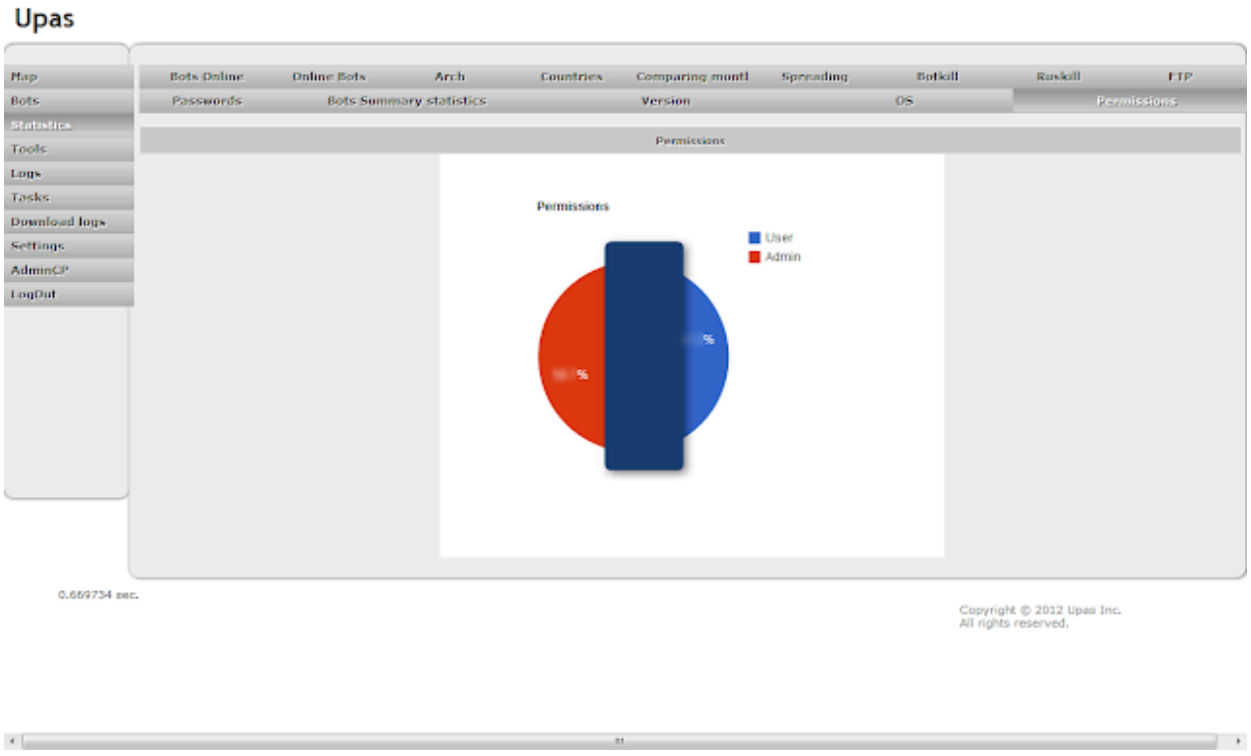
Upas - Statistics - Bots Summary statistics



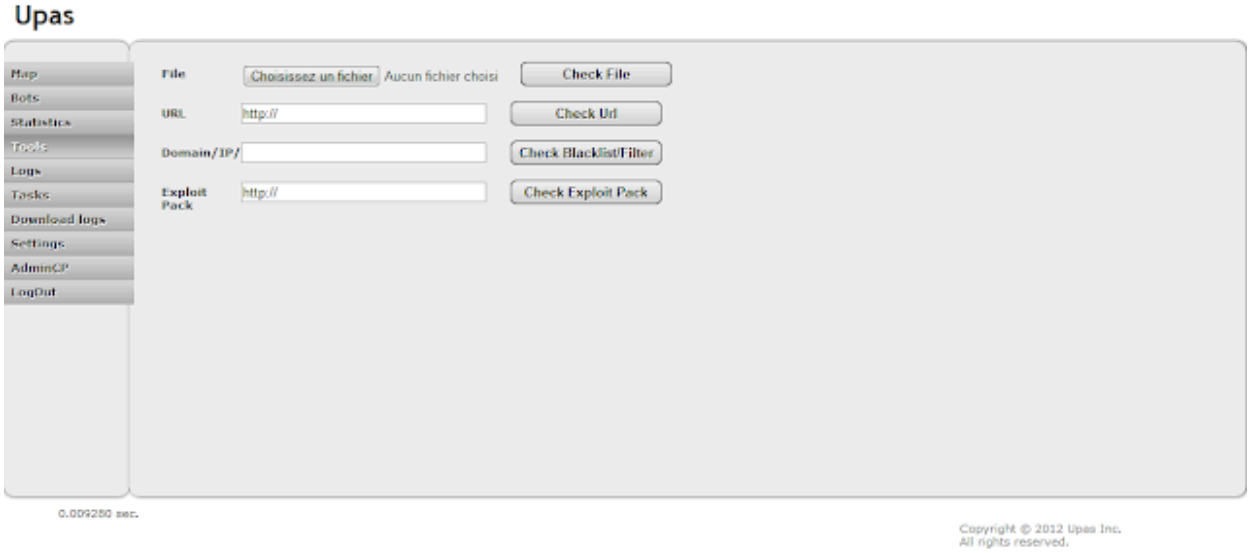
Upas - Statistics - Version



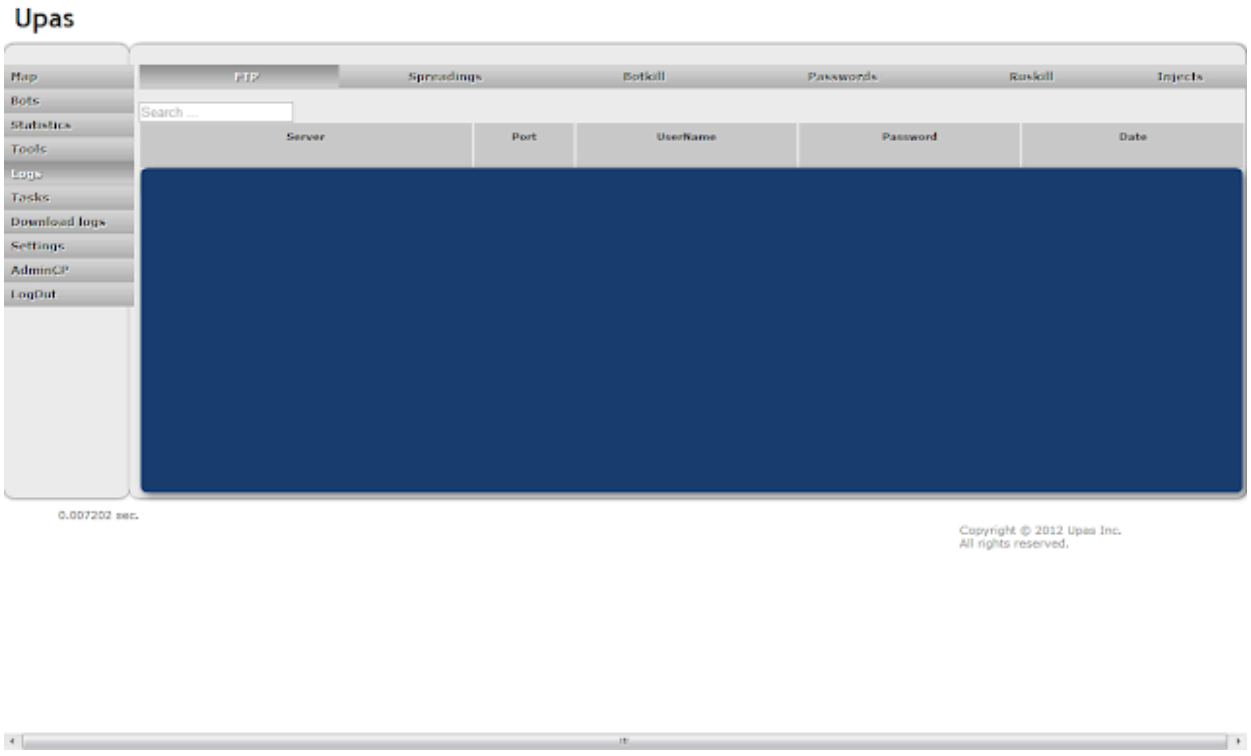
Upas - Statistics - OS



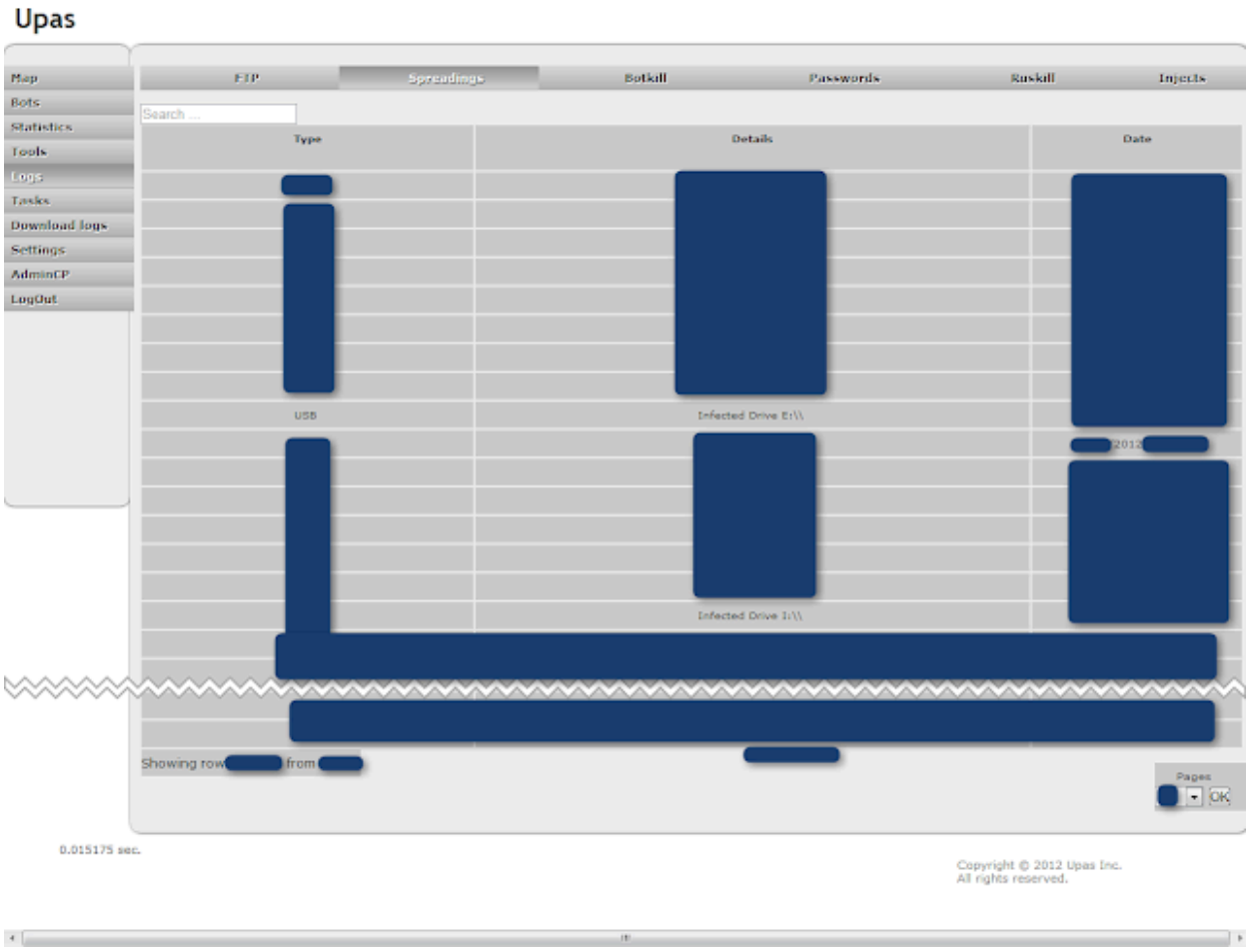
Upas - Statistics - Permissions



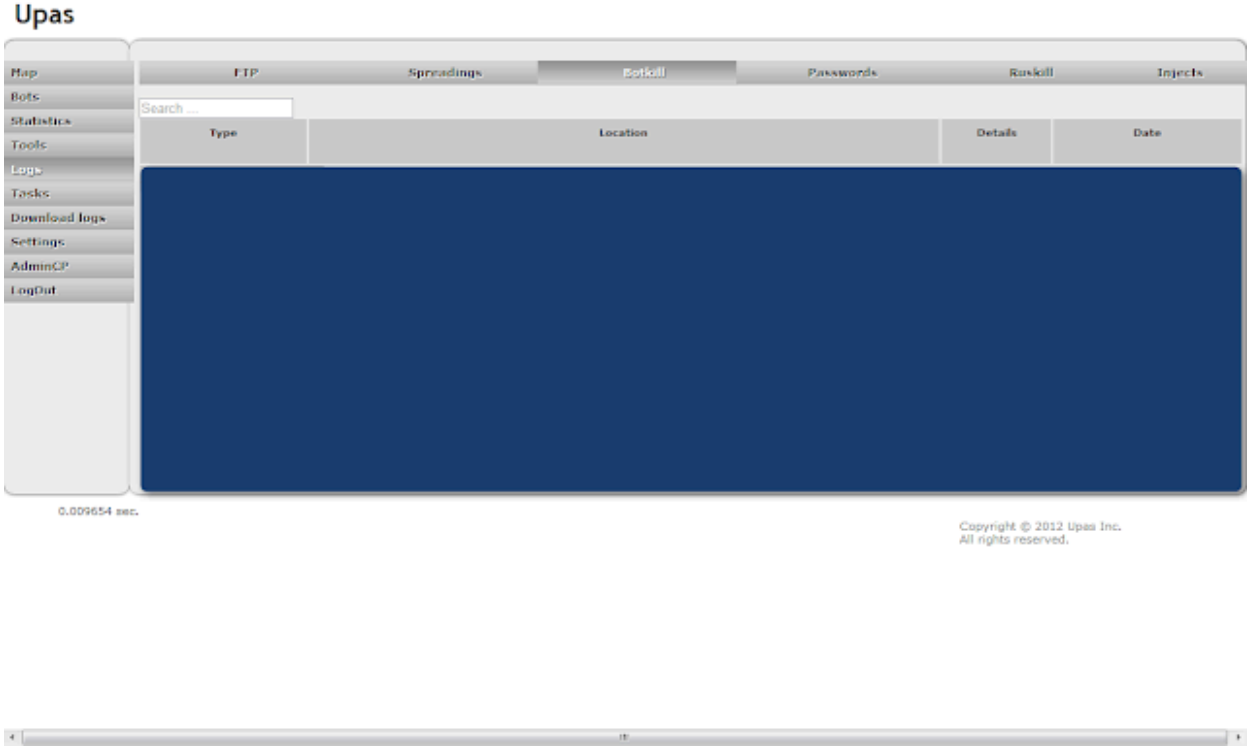
Upas - Stats



Upas - Logs - FTP

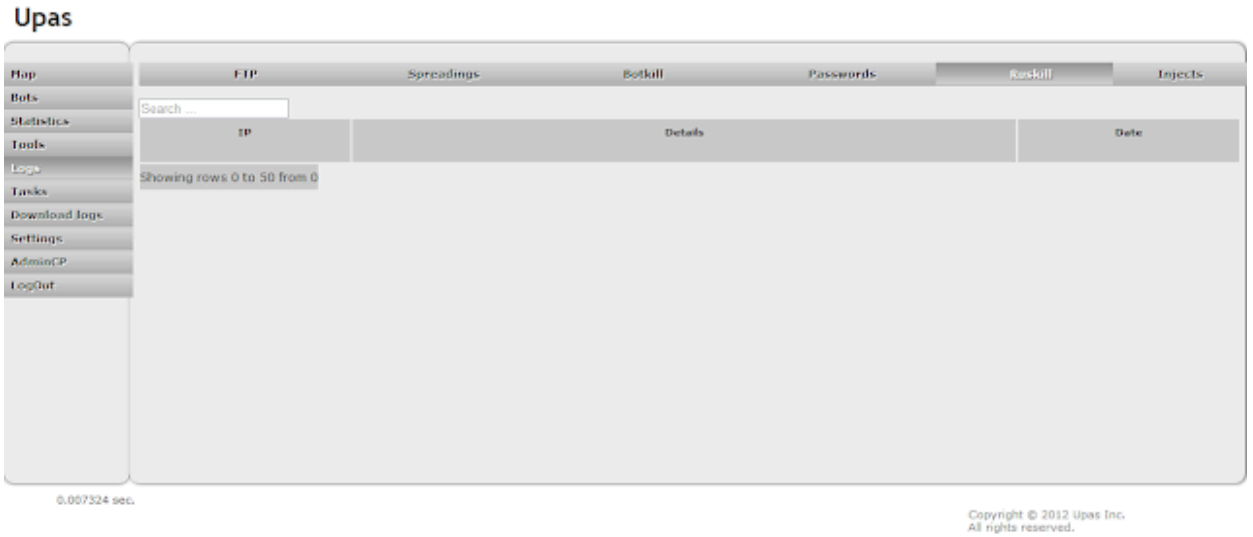


Upas - Logs - Spreadings

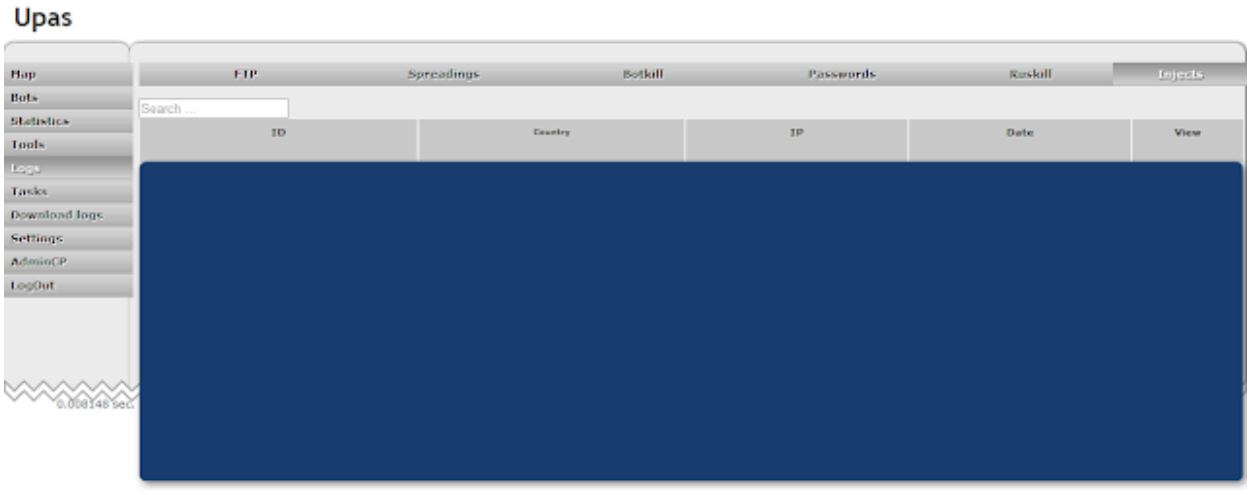


Upas - Logs - Botkill

Upas - Logs - Passwords

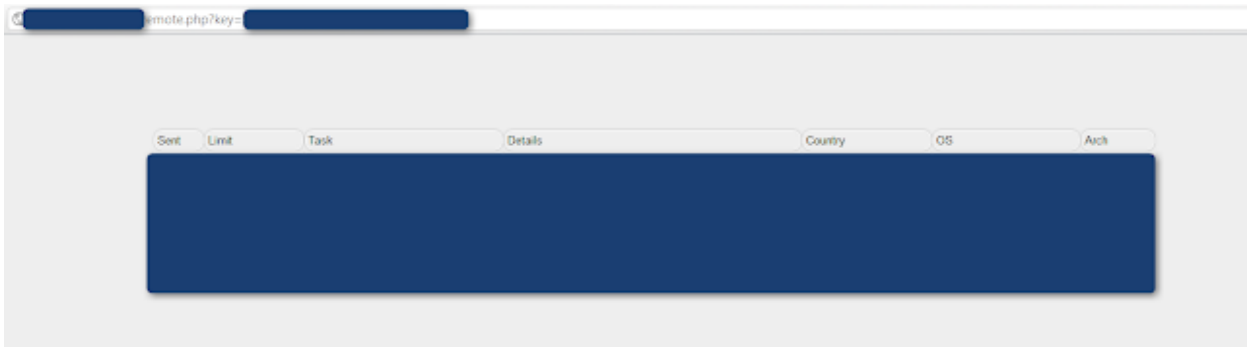


Upas - Logs - Ruskill

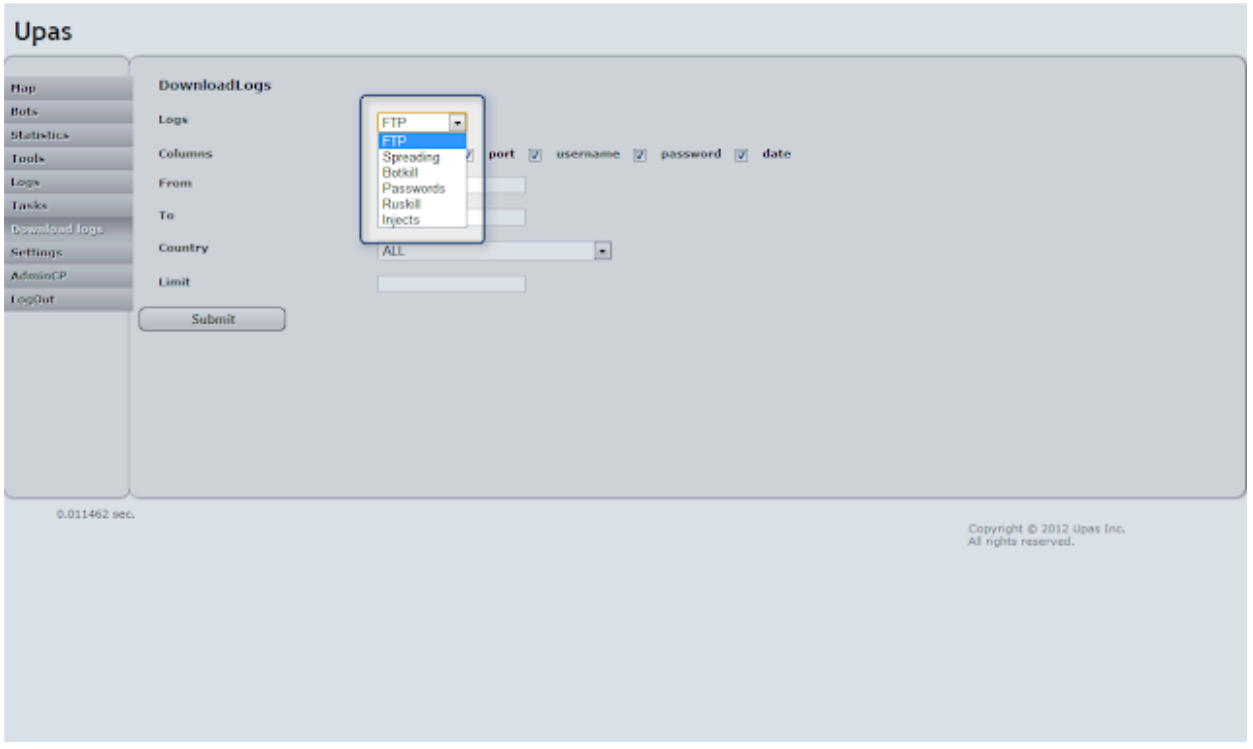


Upas - Logs - Injects

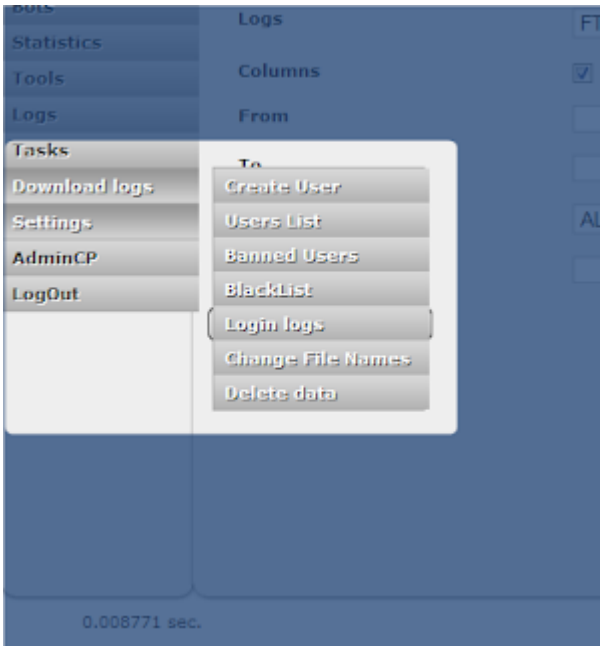
Upas - Tasks



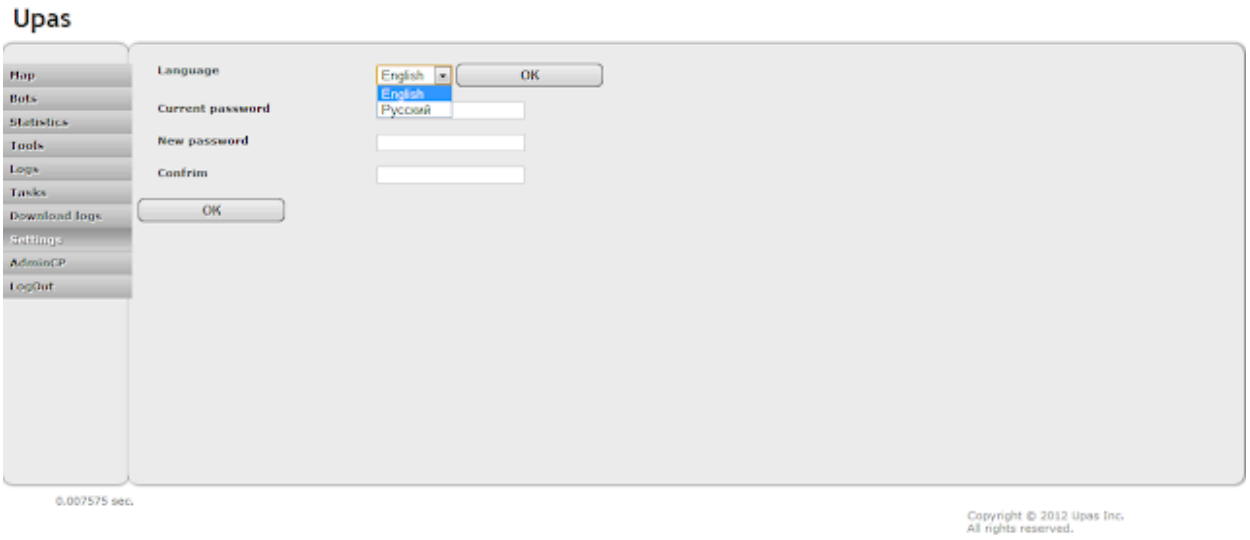
Upas - Public Link to tasks



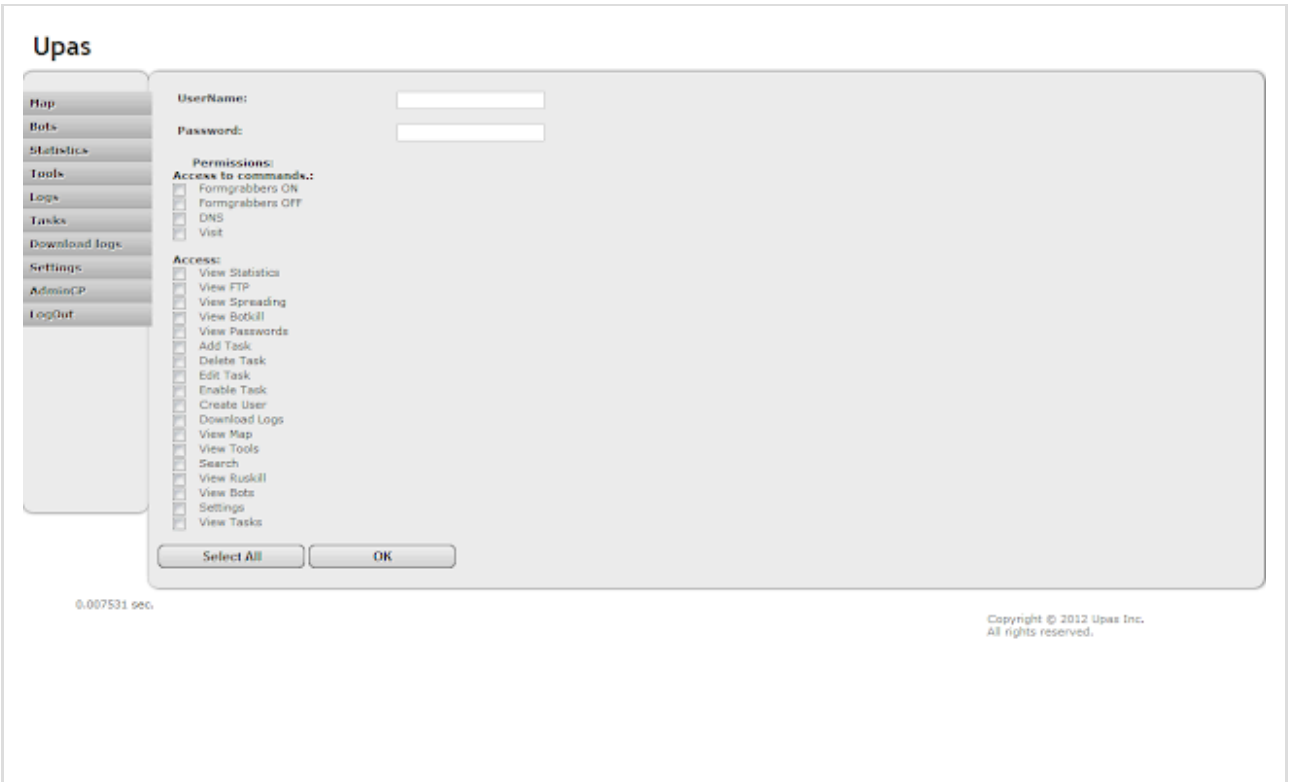
Upas - Download logs



Upas - Settings list

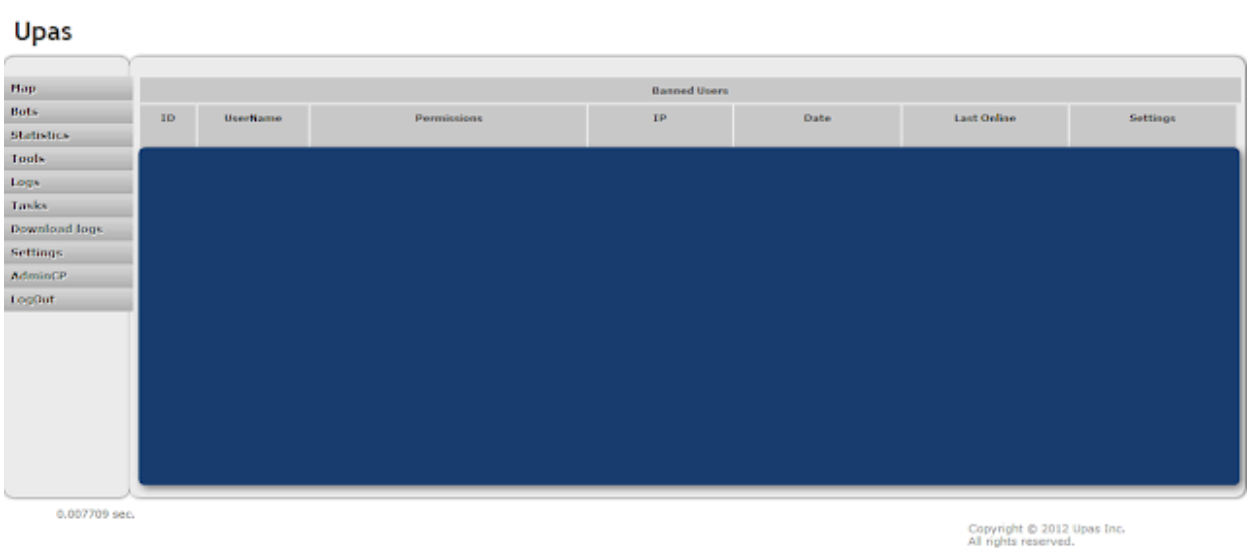


Upas - Settings

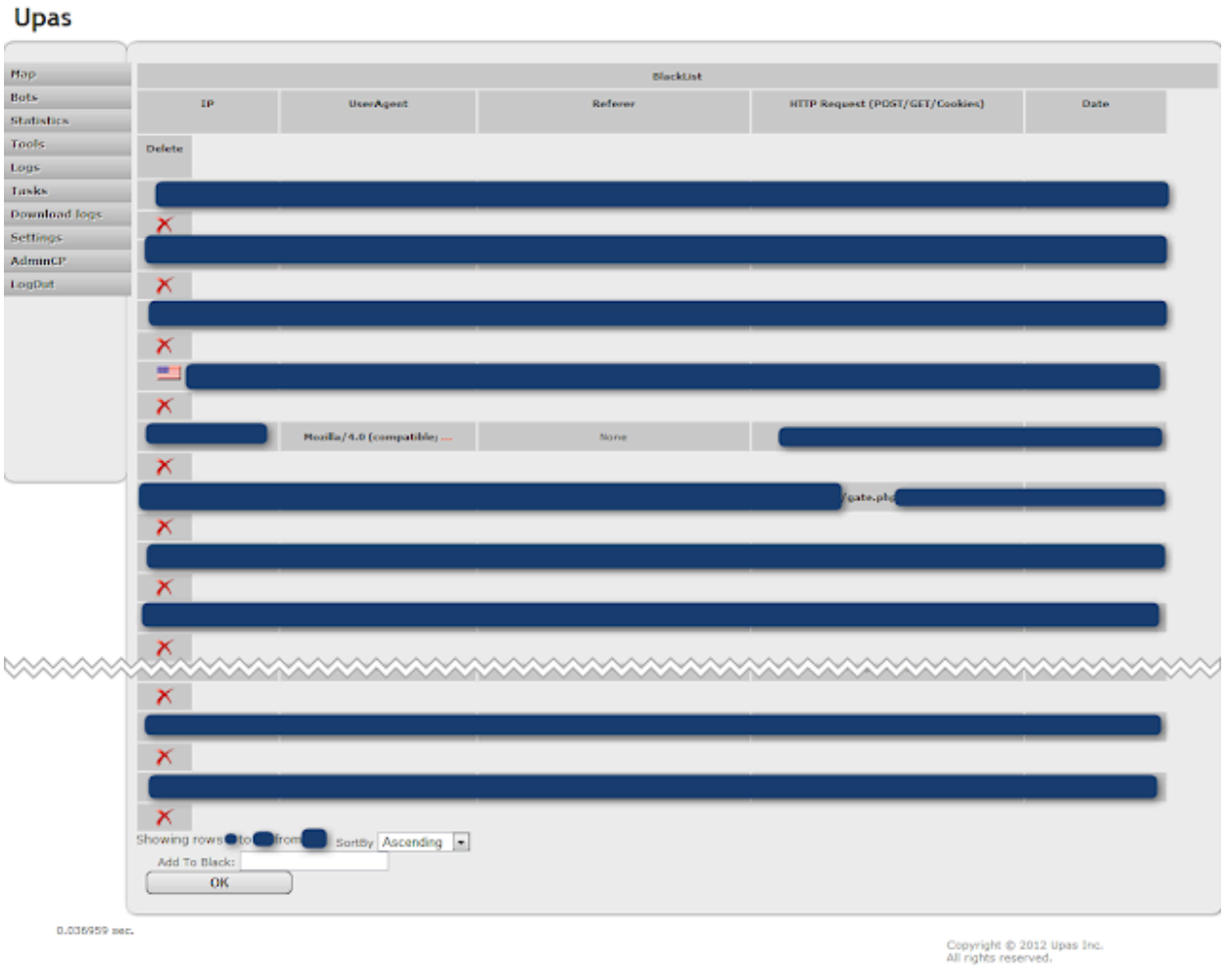


Upas - Settings - Create user

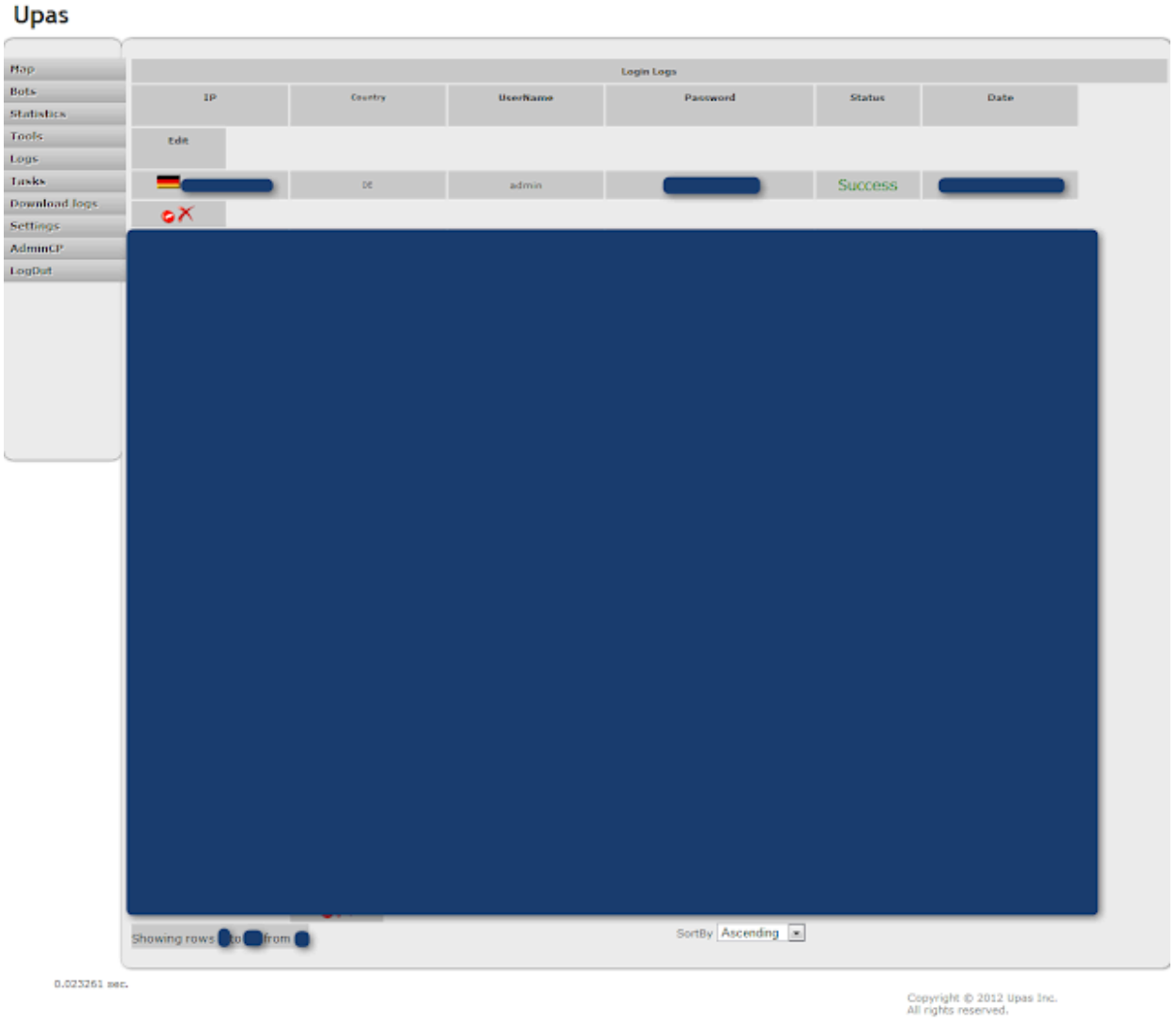
Upas - Settings - Users list



Upas - Settings - Banned Users



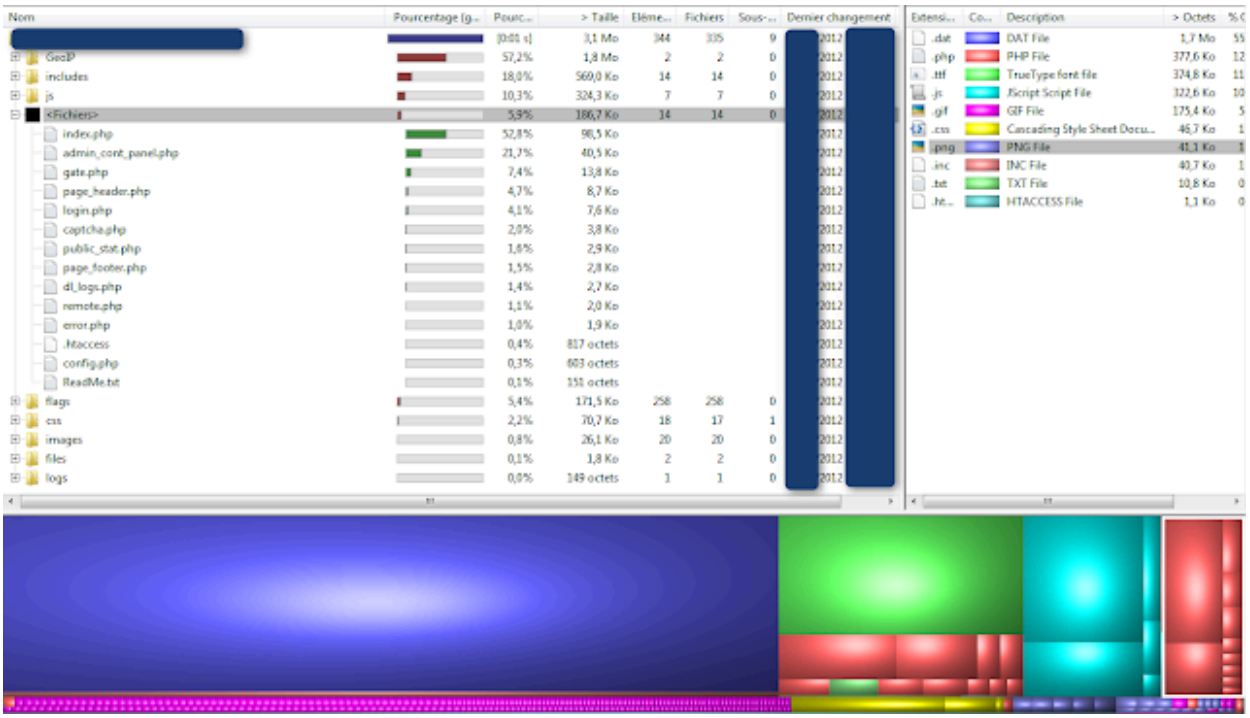
Upas - Settings - Blacklist



Upas - Settings - Login logs

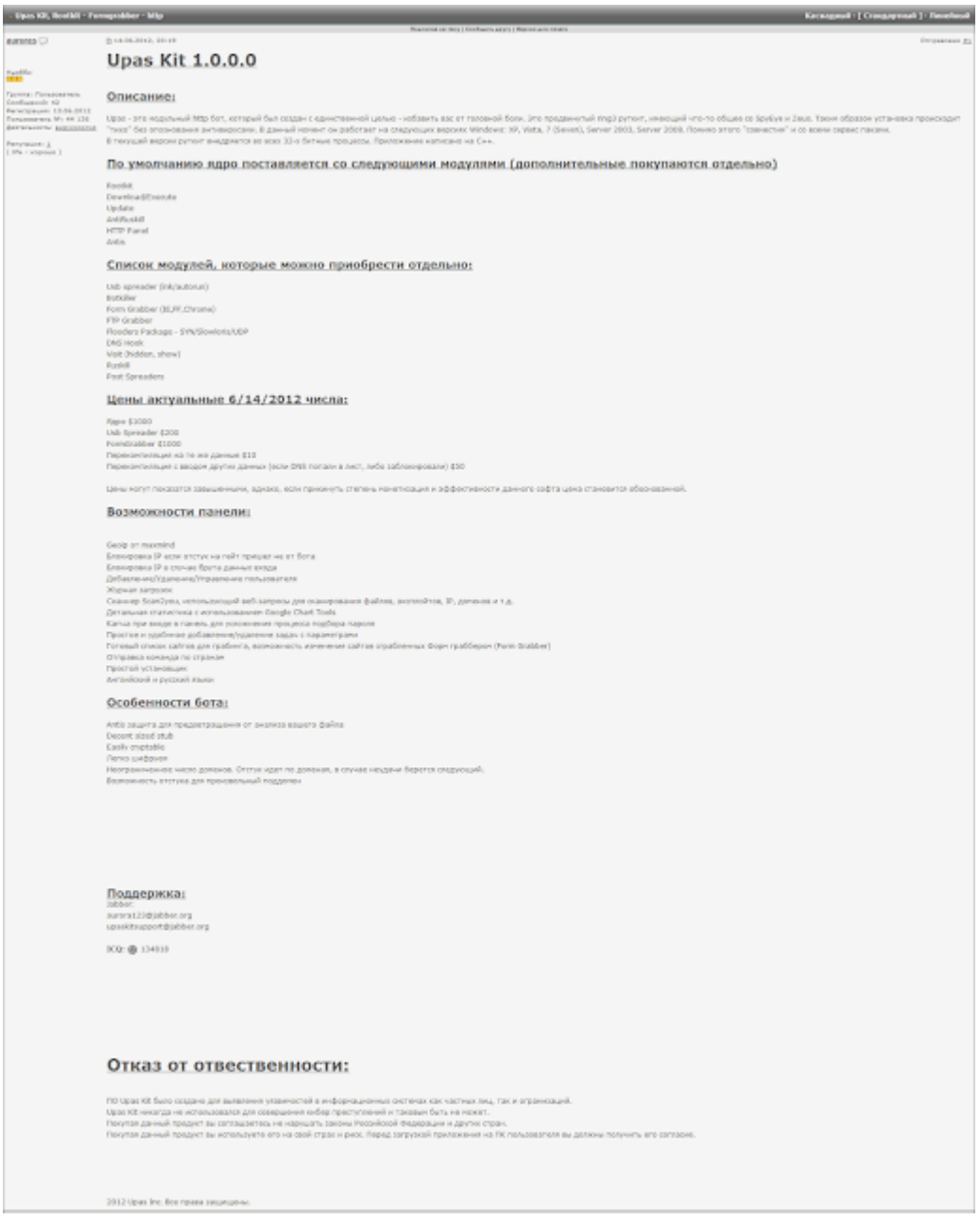
Upas - Settings - Change files name

Upas - AdminCP



Upas - Server Side Tree

Here is the initial advert on Exploit.In :



Upas Kit 1.0.0.0

Описание:

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

Список модулей, которые можно приобрести отдельно:

Цены актуальные 6/14/2012 числа:

Возможности панели:

Особенности бота:

Поддержка:

Отказ от ответственности:

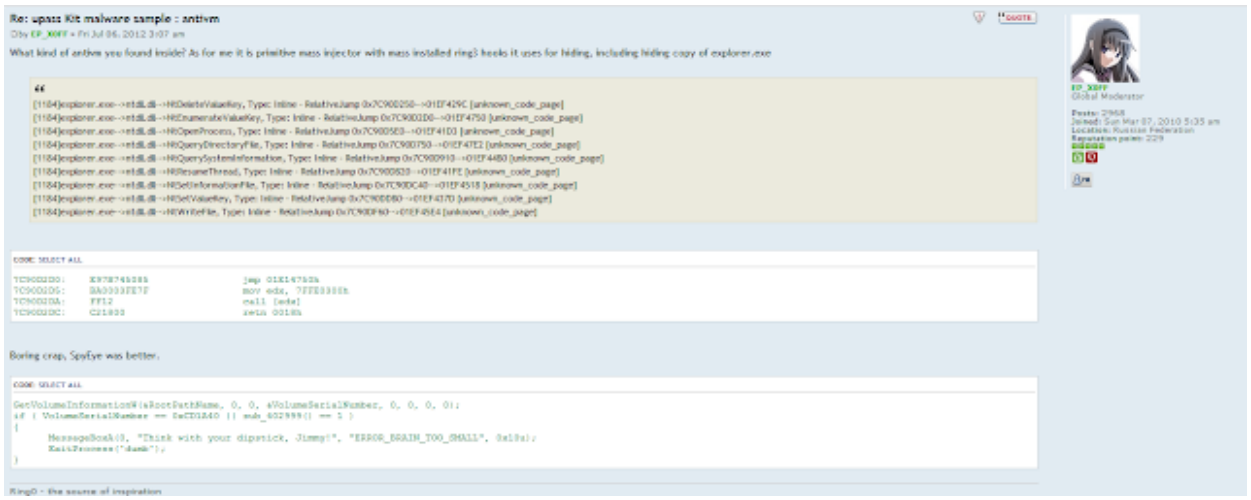
Upas Kit 1.0.0.0 as adverted by auroras on Exploit.in on the 14th of june 2012

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

http://pastebin.com/T8b0FMGA

And its Google Translation here :

http://pastebin.com/RCN0wYez

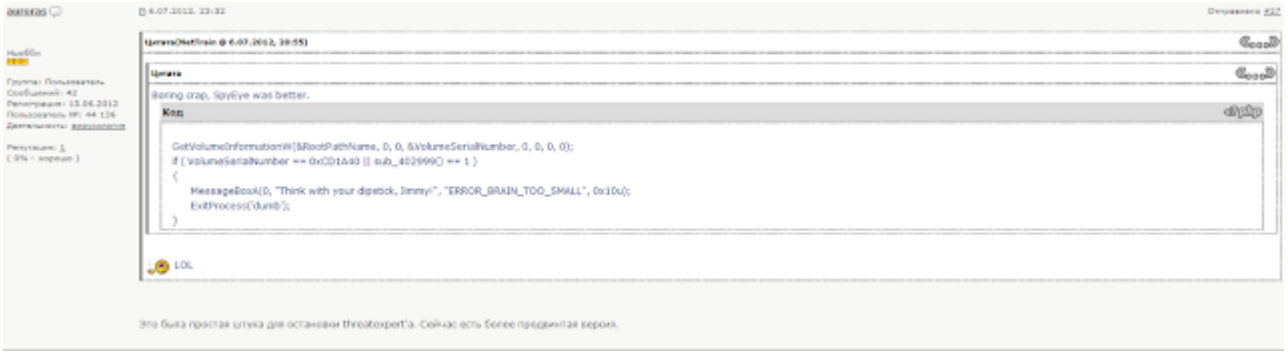


AntiVM analysis by EP_X0FF:

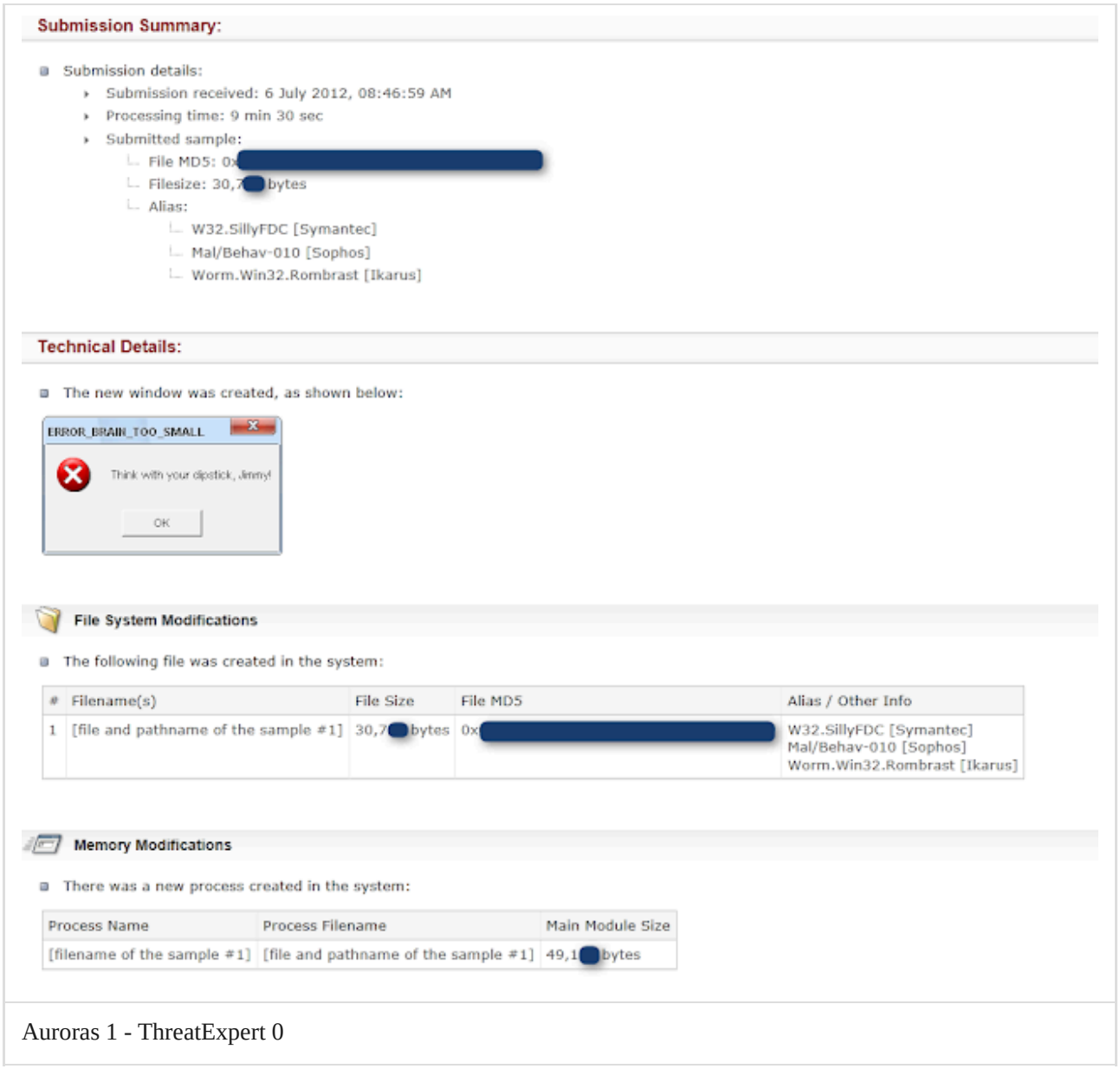
You'll find it here :

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 :



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