

## Forum:[Hack Forums](#)

Thread: [Developing a HTTP BOT](#)

**Vonful** - June 18, 2018, 11:57 am

So thought I'd talk about what i've been up to recently. As you can guess form the title I've been making a HTTP Botnet.

The way mine works is a bit different (I think) from everyone elses in the terms of not using sockets and/or any reliability on tcp connections through external ports to a server.

My bot works 90% on php where payloads and Download and Execute urls are done in mysql database. The stub is C# and is very basic. When I release it people can use crypters or some shit. Or I might make a builder depending on how bored I get.

So why did I post this? Purely because I want feedback. Please tell me if you think what I've done is pure retardation or anything along them lines. I do ask tho that you don't be nasty about anything as in insults. I take HF as a place of learning not insulting.

P.S: If I got anything technically wrong in the way other botnets funcion please don't burn me at the stake because to be fair I just pulled an assumision with no real research on how they funcion. But from what I saw of liteHTTP it uses sockets? Juding from the includes on the c# stub but again I didnt look at anything else just kinda gave in and looked how it worked, and then sockets are long then I was like fuck that lmao. Im rambling but you get me I guess.

**A Kitty** - June 18, 2018, 12:45 pm

(Jun 18, 2018 11:57 AM)Vonful Wrote: [\[CITE\]](#) So thought I'd talk about what i've been up to recently. As you can guess form the title I've been making a HTTP Botnet.

The way mine works is a bit different (I think) from everyone elses in the terms of not using sockets and/or any reliability on tcp connections through external ports to a server.

My bot works 90% on php where payloads and Download and Execute urls are done in mysql database. The stub is C# and is very basic. When I release it people can use crypters or some shit. Or I might make a builder depending on how bored I get.

So why did I post this? Purely because I want feedback. Please tell me if you think what I've done is pure retardation or anything along them lines. I do ask tho that you don't be nasty about anything as in insults. I take HF as a place of learning not insulting.

P.S: If I got anything technically wrong in the way other botnets funcion please don't burn me at the stake because to be fair I just pulled an assumision with no real research on how they funcion. But from what I saw of liteHTTP it uses sockets? Juding from the includes on the c# stub but again I didnt look at anything else just kinda gave in and looked how it worked, and then sockets are long then I was like fuck that lmao. Im rambling but you get me I guess.

Yours is no different to other HTTP botnets. The use of TCP connections is mostly used in IRC botnets, where a constant link is made.

**Vonful** - June 18, 2018, 12:50 pm

(Jun 18, 2018 12:45 PM)A Kitty Wrote: [\[CITE\]](#) Yours is no different to other HTTP botnets. The use of TCP connections is mostly used in IRC botnets, where a constant link is made.

Thanks for the correction. :D

**int** - June 19, 2018, 7:26 am

(Jun 18, 2018 12:45 PM)A Kitty Wrote: [\[CITE\]](#) Yours is no different to other HTTP botnets. The use of TCP connections is mostly used in IRC botnets, where a constant link is made.

literally this. What is the point of making a botnet if it has the same features as everything else public.

EDIT: also, most people say c# isnt good for malware due to its dependencies.

**Vonful** - June 19, 2018, 12:25 pm

(Jun 19, 2018 07:26 AM)Jukeboxhook Wrote: [\[CITE\]](#) literally this. What is the point of making a botnet if it has the same features as everything else public.

EDIT: also, most people say c# isnt good for malware due to its dependencies.

Well, for the first thing: pure fun. Why make anything? Just depressing thinking otherwise.

Two, thanks for the advice. Might make a c++ one but rn c# is fine for what i've been doing.

**int** - June 19, 2018, 12:36 pm

(Jun 19, 2018 12:25 PM)Vonful Wrote: [\[CITE\]](#) Well, for the first thing: pure fun. Why make anything? Just depressing thinking otherwise.

Two, thanks for the advice. Might make a c++ one but rn c# is fine for what i've been doing.

Yeah, that makes sense, but try to make something new. Atleast try to make new features

**Vonful** - June 19, 2018, 12:42 pm

(Jun 19, 2018 12:36 PM)Jukeboxhook Wrote: [\[CITE\]](#) Yeah, that makes sense, but try to make something new. Atleast try to make new features

Well, the whole premise of my idea is just to create something stable to load our other malware onto it. For example, if we wanna mine shitcoin we can mine shitcoin with a silent miner and load it onto the bot.

Forgot to thank you for the TIP about the c++ btw, thanks :+1:

**Vanilla** - June 19, 2018, 12:45 pm

(Jun 19, 2018 07:26 AM)Jukeboxhook Wrote: [\[CITE\]](#) literally this. What is the point of making a botnet if it has the same features as everything else public.

EDIT: also, most people say c# isnt good for malware due to its dependencies.

Haha, not only its dependencies but the fact that it leaves metadata, allowing anyone and their mom to open the stub up in something like iISpy and go to town.

(Jun 19, 2018 12:42 PM)Vonful Wrote: [\[CITE\]](#) Well, the whole premise of my idea is just to create something stable to load our other malware onto it. For example, if we wanna mine shitcoin we can mine shitcoin with a silent miner and load it onto the bot.

Forgot to thank you for the TIP about the c++ btw, thanks :+1:

Yeah, then you want to create a stable loader, relatively easy. Create the panel front end with something like HTML/CSS, the back end in PHP or Go (my personal favorite) Then, I would recommend you code the stub in a language that compiles to machine code. Don't just go and choose C++ as coding in it can be difficult and take much longer than using a language like Rust which is native.

**Vonful** - June 19, 2018, 12:58 pm

(Jun 19, 2018 12:45 PM)Airy Wrote: [\[CITE\]](#) Haha, not only its dependencies but the fact that it leaves metadata, allowing anyone and their mom to open the stub up in something like iISpy and go to town.

Yeah, then you want to create a stable loader, relatively easy. Create the panel front end with

something like HTML/CSS, the back end in PHP or Go (my personal favorite) Then, I would recommend you code the stub in a language that compiles to machine code. Don't just go and choose C++ as coding in it can be difficult and take much longer than using a language like Rust which is native.

Thanks for the advice. I have already wrote everything basiclly. Got a front end (i[dot]imgur[dot]com/xEGN5OU.png) which I wrote in HTML, CSS, and PHP as backend. The bots are stored in a mysql database and everything functions correctly. Well, mostly. Can run commands and what not. But yeah I will take your advice and look into rust. Thanks for the input mate :)

**Vanilla** - June 19, 2018, 1:00 pm

(Jun 19, 2018 12:58 PM)Vonful Wrote: [\[CITE\]](#) Thanks for the advice. I have already wrote everything basiclly. Got a front end (i[dot]imgur[dot]com/xEGN5OU.png) which I wrote in HTML, CSS, and PHP as backend. The bots are stored in a mysql database and everything functions correctly. Well, mostly. Can run commands and what not. But yeah I will take your advice and look into rust. Thanks for the input mate :)

Glad to be of help ?

**inyourmemory** - June 19, 2018, 1:13 pm

C# botnet is very bad idea. Dependencies, big stub, easy reversal and anti debug etc other tricks like memory stuff become lot harder

**Vonful** - June 19, 2018, 1:14 pm

(Jun 19, 2018 01:00 PM)Airy Wrote: [\[CITE\]](#) Glad to be of help ?  
dont suppose you have discord?

(Jun 19, 2018 01:13 PM)Win64Worm Wrote: [\[CITE\]](#) C# botnet is very bad idea. Dependencies, big stub, easy reversal and anti debug etc other tricks like memory stuff become lot harder

Ye I realize that one now mate LMAO was just for fun but now I wanna see how far i can take it. Thanks for the advice my man <3

**Theslayer** - June 23, 2018, 12:05 pm

Get rid of that c# crap

Build a loader and store the client dll as a encrypted resource, decrypt it at runtime and inject it on several processes (chrome,firefox etc if you have formgrabber functionality, default process is explorer.exe but I have no idea if it works straight out on newer windows 10 builds)

Injection method should be NtQueueApcThread or RtlCreateUserThread , dont use CreateRemoteThread , its flagged by av

**Vonful** - June 23, 2018, 1:10 pm

(Jun 23, 2018 12:05 PM)Theslayer Wrote: [\[CITE\]](#) Get rid of that c# crap

Build a loader and store the client dll as a encrypted resource, decrypt it at runtime and inject it on several processes (chrome,firefox etc if you have formgrabber functionality, default process is explorer.exe but I have no idea if it works straight out on newer windows 10 builds)

Injection method should be NtQueueApcThread or RtlCreateUserThread , dont use CreateRemoteThread , its flagged by av

Thanks man, does help. But chances are I won't be making a c++ stub anytime soon as they're annoying to faf around with.

**Toxicique** - June 23, 2018, 2:35 pm

(Jun 23, 2018 12:05 PM)Theslayer Wrote: [\[CITE\]](#) Get rid of that c# crap

Build a loader and store the client dll as a encrypted resource, decrypt it at runtime and inject it on

several processes (chrome,firefox etc if you have formgrabber functionality, default process is explorer.exe but I have no idea if it works straight out on newer windows 10 builds)

Injection method should be NtQueueApcThread or RtlCreateUserThread , dont use CreateRemoteThread , its flagged by av  
Great post. thank you!

**inyourmemory** - June 23, 2018, 2:48 pm

(Jun 23, 2018 12:05 PM)Theslayer Wrote: [\[CITE\]](#) Get rid of that c# crap  
Build a loader and store the client dll as a encrypted resource, decrypt it at runtime and inject it on several processes (chrome,firefox etc if you have formgrabber functionality, default process is explorer.exe but I have no idea if it works straight out on newer windows 10 builds)

Injection method should be NtQueueApcThread or RtlCreateUserThread , dont use CreateRemoteThread , its flagged by av  
QueueUserApc is just as detected as CreateRemoteThread. same with RtlCreateUserthread

**Toxicique** - June 23, 2018, 2:50 pm

(Jun 23, 2018 02:48 PM)Win64Worm Wrote: [\[CITE\]](#) QueueUserApc is just as detected as CreateRemoteThread. same with RtlCreateUserthread  
how would you call those functions then?

**inyourmemory** - June 23, 2018, 2:59 pm

(Jun 23, 2018 02:50 PM)Toxicique Wrote: [\[CITE\]](#) how would you call those functions then?  
by loading clean copy of ntdll from disk and calling them from there, unhooking or using direct syscalls

**Toxicique** - June 24, 2018, 5:53 am

(Jun 23, 2018 02:59 PM)Win64Worm Wrote: [\[CITE\]](#) by loading clean copy of ntdll from disk and calling them from there, unhooking or using direct syscalls  
nice, have you gotten any open-source projects that implement this, or any resource where I can learn this on a practical level?

Thank you!

**P4r4517** - June 25, 2018, 11:29 am

(Jun 23, 2018 02:59 PM)Win64Worm Wrote: [\[CITE\]](#) by loading clean copy of ntdll from disk and calling them from there, unhooking or using direct syscalls  
AntiVirus may monitor the creation of remote thread via PsSetCreateThreadNotifyRoutine but thats better than using these api calls straight up.