

Forum:[Hack Forums](#)

Thread: [\[DEVELOPING\] Hades Botnet](#)

Insane Developer - February 9, 2016, 6:38 pm

Welcome to Hades Botnet's development thread
Hades Botnet, the controller of the
souls.

DEVELOPEMENT HAVE STOPPED. PLEASE DO NOT POST HERE!!!! <=====

Virus Scan: <http://scan.majyx.net/scans/result/2ff322822ca1d5cdb0eb923901c4938ef00545e7>

Some pics:

<https://gyazo.com/9a71be271242b82725be75fe3582767a>

<https://gyazo.com/b15b25b99595442b0d81938407d6cf81>

<https://gyazo.com/0087f89b960b893583e2ebd36c67edcb>

<https://gyazo.com/db9dcb0c706cd841b0c3a41e821dc19f>

Features (Color indicates the progress, green=65-100%, red=0-25%, orange=25-65%, grey=Not worked on yet): Social engineering to get UAC

Botkiller

DDoS(GET, POST, UDP, TCP)

Password recovery

Download and execute

Download without execution

Run file

Remote Registry

Secured panel

Panel design

Backup host

Tor Support

Background changer (Advertisement?)

Stable

USB spreader

Encryption and protection

Protected Task, hiding,...

Ring0/3 rootkit

Shutdown

Grab computer name and Username

Block/Unblock user input

Message box

Restart

Removing ZoneID

Kill Antiviruses

Bitcoin miner

Advanced VM and debuggers detection, works even if VMware services, VirtualBox services and processes are killed/disabled prior to execution. When detected, it will do the best to destroy the VM/computer, causes noise to make the real trace unidentifiable from the fake trace, and removes itself

Hidden Startup

FUD scan: Spoiler [\(Click to View\)](#)<http://v2.scan.majyx.net/image.php?id=996894>

President Morty - February 9, 2016, 7:20 pm

Anything with hijacking bitcoin/currency I believe isn't allowed in any way on HF.

Bitcoin and Cryptocurrency Fraud

We consider crypto currency an excellent choice for payments here on HF. And while they have no official government backing we feel they have value to this community. As such any cryptocurrency fraud will be considered financial fraud. Discussion on stealing wallets including RATS will not be allowed on HF.

postingmail - February 9, 2016, 7:25 pm

How many times have these type of posts been spammed on here

Insane Developer - February 9, 2016, 10:26 pm

(Feb 9, 2016 08:20 PM)L_USER Wrote: [\[CITE\]](#) Anything with hijacking bitcoin/currency I believe isn't allowed in any way on HF.

Bitcoin and Cryptocurrency Fraud

We consider crypto currency an excellent choice for payments here on HF. And while they have no official government backing we feel they have value to this community. As such any cryptocurrency fraud will be considered financial fraud. Discussion on stealing wallets including RATS will not be allowed on HF.

Removed.

(Feb 9, 2016 08:25 PM)postingmail Wrote: [\[CITE\]](#) How many times have these type of posts been spammed on hereSo it is now considered spamming to post a thread asking for ideas?

Insane Developer - February 11, 2016, 1:15 am

Update: Panel is getting a redesign.Will post screenshots soon

fq23533 - February 11, 2016, 9:12 am

Which programming language?

modular system
web Injects
Hidden vnc/rdp planning?

Juggernaut - February 11, 2016, 9:16 am

Some more ddos options would probably be nice. I mean, a botnet is nothing without a good udp flood

Insane Developer - February 11, 2016, 6:17 pm

I will add UDP and slow HTTP after finish redesigning the web panel.

The language would be Autolt.

No web inject, since that may be used in financial crimes.

Maybe I will include a function to create a RDP, but will take some times and research.

?Xe - February 12, 2016, 7:36 am

When you're done developing & finishing it off for a final release, be sure to hmu with the download :D Thanks in advance!

Green Goblin - February 12, 2016, 7:59 am

(Feb 9, 2016 08:20 PM)L_USER Wrote: [\[CITE\]](#) Anything with hijacking bitcoin/currency I believe isn't allowed in any way on HF.

Bitcoin and Cryptocurrency Fraud

We consider crypto currency an excellent choice for payments here on HF. And while they have no official government backing we feel they have value to this community. As such any cryptocurrency fraud will be considered financial fraud. Discussion on stealing wallets including RATS will not be allowed on HF. fake projects shouldnt be allowed either

RoryMercury - February 12, 2016, 7:37 pm

Which language (stub)?

Unnecesary:

- CD Open, CD Close
- Shut Down, Lock, Sleep, Restart

Add:

Many types of DDos with timer, example, ddos an ip for 5 minutes.

Download & run (on a selected pc)

team viewer hidden.

Insane Developer - February 12, 2016, 7:57 pm

(Feb 12, 2016 08:37 PM)RoryMercury Wrote: [\[CITE\]](#) Which language (stub)?

Unnecessary:

- CD Open, CD Close
- Shut Down, Lock, Sleep, Restart

Add:

Many types of DDos with timer, example, ddos an ip for 5 minutes.

Download & run (on a selected pc)

team viewer hidden.

I will keep those "Unnecessary features" (Which you spelled wrong btw) and I am working on the hidden RDP feature.

(Feb 12, 2016 08:59 AM)Green Goblin Wrote: [\[CITE\]](#) fake projects shouldnt be allowed either Who says it is fake? I am working on it for real.

Update: New DDoS function: TCP and UDP flood. Working on the web panel now.

Insane Developer - February 13, 2016, 1:18 am

(Feb 13, 2016 02:09 AM)NTTITONV327 Wrote: [\[CITE\]](#) Any sugestions?

Yeah, have a messagebox during execution asking the user if he wants junk on his pc

I already have the fake message box feature?

And junking? Nah. This is made for "educational purposes" only and must not be used for any "malicious purposes" including but not limited to "fraud, ddos, infecting people without their permission". The author of this product does not "endorse the use of this product" for "malicious purposes" and will "suspend anyone who is found to be doing so"

Jeffnickels - February 13, 2016, 1:19 am

This seems very basic.

A "embedded downloader" is just download a file and starting the process.

What's it coded in?

Stub size? Encryption for responses on the requests?

Jeffnickels - February 13, 2016, 1:25 am

(Feb 13, 2016 02:23 AM)NTTITONV327 Wrote: [\[CITE\]](#) I'm talking about RIGHT ON EXECUTION

```
int main()
{
    MsgBox(0,"Do you want junk installed on your computer?",0,0); //This is where we assume no

    return 0; //this is our reaction
}
```

It's coded in vb6 with inline .NET

Ah vb is still lower execution rate than a true native lang.

I'm interested in seeing where this is going.

Yet to see proof of panel or anything.

Insane Developer - February 13, 2016, 1:31 am

(Feb 13, 2016 02:19 AM)Jeffnickels Wrote: [\[CITE\]](#) This seems very basic.

A "embedded downloader" is just download a file and starting the process.

What's it coded in?

Stub size? Encryption for responses on the requests?

It is coded in Autolt, Python and I will be making more complicated modules in other languages. Encryption will be done with SHA 256 with a long random key, and maybe another encryption layer with base64,pgp or something (almost done with this).

It seems basic because I just started this. Didn't have much time but it will evolve into something a lot more.

Stub size is 717kb (will be worked on), but I will provide a FUD downloader which will probably be around 10kb.

(Feb 13, 2016 02:23 AM)NTTITONV327 Wrote: [\[CITE\]](#) I'm talking about RIGHT ON EXECUTION

```
int main()
```

```
{  
  MessageBox(0,"Do you want junk installed on your computer?",0,0); //This is where we assume no
```

```
  return 0; //this is our reaction
```

```
}
```

It's coded in vb6 with inline .NET

Well, I will not use .NET and have dependencies. However, you can feel free to get out of my thread.

[br]

Oops, see you already are banned.

Jeffnickels - February 13, 2016, 10:34 pm

(Feb 13, 2016 02:31 AM)haigiang02 Wrote: [\[CITE\]](#) It is coded in Autolt, Python and I will be making more complicated modules in other languages. Encryption will be done with SHA 256 with a long random key, and maybe another encryption layer with base64,pgp or something (almost done with this).

It seems basic because I just started this. Didn't have much time but it will evolve into something a lot more.

Stub size is 717kb (will be worked on), but I will provide a FUD downloader which will probably be around 10kb.

Well, I will not use .NET and have dependencies. However, you can feel free to get out of my thread.

[br]

Oops, see you already are banned.717KB?

Waste of time don't even sell.

A fud downloader? You said embedded downloader which is download and execute which makes you seem stupid.

If you're having trouble with understanding download and execute and embedded downloader is I doubt it'll be anymore advanced.

It's made in auto it? Please just kill yourself.

Good god auto it has a bad execution rate you'd be better off using .net lmao.

Spare us all the bullshit.

Edit

Also please show us a picture of the panel.

Insane Developer - February 14, 2016, 12:34 am

(Feb 13, 2016 11:34 PM)Jeffnickels Wrote: [\[CITE\]](#) 717KB?

Waste of time don't even sell.

A fud downloader? You said embedded downloader which is download and execute which makes you seem stupid.

If you're having trouble with understanding download and execute and embedded downloader is I doubt it'll be anymore advanced.

It's made in auto it? Please just kill yourself.

Good god auto it has a bad execution rate you'd be better off using .net lmao.

Spare us all the bullshit.

Edit

Also please show us a picture of the panel. I don't see why it reduces execution rate, it has no dependencies at all once compiled. Ofc it won't be the au3 file.

The external downloader is so that you can upload the stub to direct download sites, and link it.

And it is not only in AutoIt, it contains Python and some C as well. AutoIt is just used as the frame for the botnet.

Will post panel's screenshot once I finish redesigning it

NTTITONV332 - February 14, 2016, 12:45 am

You guys should try vb6 with inline .net

Insane Developer - February 14, 2016, 1:02 am

(Feb 14, 2016 01:45 AM)NTTITONV332 Wrote: [\[CITE\]](#) You guys should try vb6 with inline .net

Oh hi! Congrats on your 332nd account!

And maybe, but probably not.

Update: Here is the screenshot of the current panel:

<https://gyazo.com/4522af1541f5235a2432cfc654b0d94c>

I know it is shit, that's why I am redesigning it.

And the name is wrong as well since that was my old name for it.

Lucifer Morningstar - February 14, 2016, 3:10 am

(Feb 14, 2016 02:02 AM)haigiang02 Wrote: [\[CITE\]](#) Oh hi! Congrats on your 332nd account!

And maybe, but probably not.

Update: Here is the screenshot of the current panel:

<https://gyazo.com/4522af1541f5235a2432cfc654b0d94c>

I know it is shit, that's why I am redesigning it.

And the name is wrong as well since that was my old name for it.

He had more than 332 accounts.

Also why are you releasing pictures of a broken panel? You should be ashamed to say the least.

FurfUksake - February 14, 2016, 3:24 am

(Feb 9, 2016 07:38 PM)haigiang02 Wrote: [\[CITE\]](#) Any sugestions?

I have some constructive criticism if you are interested in hearing it:

1) Focus less on thinking up cool names and creating aesthetically pleaseing graphics for your control panel and focus more on developing new methods and techniques to achieve your goals.

2) Do something that has never been done.

3) If you must regurgitate the same old functions then try to accomplish it using a modified approach, preferably improved.

You are always going to get heat from creating a thread of this nature the main reason being that if you aren't creative enough to even think of a concept you will never be creative enough to think of the solution to the problem created from the concept.

Best of luck on your endeavors.

Insane Developer - February 14, 2016, 6:40 am

(Feb 14, 2016 04:24 AM)Veto Wrote: [\[CITE\]](#) I have some constructive criticism if you are interested in hearing it:

1) Focus less on thinking up cool names and creating aesthetically pleaseing graphics for your control panel and focus more on developing new methods and techniques to achieve your goals.

2) Do something that has never been done.

3) If you must regurgitate the same old functions then try to accomplish it using a modified approach, preferably improved.

You are always going to get heat from creating a thread of this nature the main reason being that if you aren't creative enough to even think of a concept you will never be creative enough to think of the solution to the problem created from the concept.

Best of luck on your endeavors.Thanks for the suggestions! I am redesigning the panel, since the other one was just a temporary solution. I currently am working on the hidden RDP feature, will probably finish it in a week. I also am around 25% finish with homepage changer.

(Feb 14, 2016 04:10 AM)Tx707 Wrote: [\[CITE\]](#) He had more than 332 accounts.
Also why are you releasing pictures of a broken panel? You should be ashamed to say the least. The panel is not broken, it shows that because I didn't upload the PHP file to a webhost but just opened it from the local file. My bad.
Also I am working on a new panel from scratch, so the old one doesn't really matter.

Zettabit - February 14, 2016, 10:16 am

I can shit out a bot in .NET that's 10 times better than this piece of shit in 2 days.

Insane Developer - February 14, 2016, 5:17 pm

(Feb 14, 2016 11:16 AM)Zettabit Wrote: [\[CITE\]](#) I can shit out a bot in .NET that's 10 times better than this piece of shit in 2 days.
Feel free to ?

Update: Stub size reduced to 543 KB, Almost finished with RDP

Added Silent Bitcoin Miner in, which is written in Delphi.

v4p3 - February 15, 2016, 2:45 am

I'd move away from autoit for the client as it's easily decompiled, go for something like C or C++ as they are much better languages

Insane Developer - February 15, 2016, 3:07 am

(Feb 15, 2016 03:45 AM)v4p3 Wrote: [\[CITE\]](#) I'd move away from autoit for the client as it's easily

decompiled, go for something like C or C++ as they are much better languages

I have around 20 obfuscators and will use a crypter. I also have other methods to prevent exe2Aut. and this Botnet is multi-lingual. I will probably use C for more complex functions and use Autolt for simple stuffs.

Staunching - February 15, 2016, 3:53 am

if you make a password recovery try and make it as much browsers as possible atleast do the main four people use (google chrome, internet explorer, firefox/mozilla, opera)

NTTITONV336 - February 15, 2016, 3:59 am

52. At the end of this sequence of instructions, how many bytes separate esp and the stored return address on the program's stack? Assume that we called this function using standard 32-bit x86 calling conventions.

```
804847c functionname:
804847c: push %ebp
804847d: mov %esp,%ebp
804847f: sub $0x34,%esp
8048482: movl $0x0,0x4(%esp)
804848a: movl $0x8048580,(%esp)
```

61. At the end of this sequence of instructions, what is the value in eax? Assume that we are using standard 32-bit x86 calling conventions.

```
80484f0 functionname:
80484f0: push %ebp
80484f1: mov %esp,%ebp
80484f3: sub $0x28,%esp
80484f6: call $+5
80484fb: pop $eax
```

Insane Developer - February 15, 2016, 4:53 am

(Feb 15, 2016 04:59 AM)NTTITONV336 Wrote: [\[CITE\]](#) 52. At the end of this sequence of instructions, how many bytes separate esp and the stored return address on the program's stack? Assume that we called this function using standard 32-bit x86 calling conventions.

```
804847c functionname:
804847c: push %ebp
804847d: mov %esp,%ebp
804847f: sub $0x34,%esp
8048482: movl $0x0,0x4(%esp)
804848a: movl $0x8048580,(%esp)
```

61. At the end of this sequence of instructions, what is the value in eax? Assume that we are using standard 32-bit x86 calling conventions.

```
80484f0 functionname:
80484f0: push %ebp
80484f1: mov %esp,%ebp
```

80484f3: sub \$0x28,%esp

80484f6: call \$+5

80484fb: pop \$eaxWow I am deeply confused I do NOT know what you mean.

Congrats on another new account btw?

(Feb 15, 2016 04:53 AM)Staunching Wrote: [\[CITE\]](#) if you make a password recovery try and make it as much browsers as possible atleast do the main four people use (google chrome, internet explorer, firefox/mozilla, opera)

I got those 4 browsers already. I also have implemented a large amount of other passwords from other application.

Added hiding task from Task Manager, gonna try to make it less visible to user

Insane Developer - February 17, 2016, 2:13 am

Added Advanced VM detections, capable of detecting VM even when VMware service and tools is not installed.

Insane Developer - February 18, 2016, 7:52 am

Added extra persistence using 4 watchdogs.

Changed install dir

Staunching - February 18, 2016, 2:25 pm

this will be the next http botnet :)

Insane Developer - February 19, 2016, 6:54 am

Working on reFUDing as well as finishing the hidden RDP feature!

[\[IMG\]http://v2.scan.majyx.net/image.php?id=988479\[/IMG\]](http://v2.scan.majyx.net/image.php?id=988479)

RoryMercury - February 19, 2016, 8:17 pm

will you sell it? im interesed on beta-testing it if you want..

The Unusual Hunter - February 19, 2016, 8:25 pm

When is this out and would I recommend you do a beta test and if you do I would love to be a part of it.

How much do you think you will be selling this for please give me an estimate so I can start saving :)

Kicking - February 19, 2016, 9:33 pm

I've been looking for a botnet, PM me if you're interested in selling!

Insane Developer - February 20, 2016, 5:41 am

Update: I am not working on RDP anymore, managed to create hidden admin user but it was too complicated. Working on the design now

The Unusual Hunter - February 20, 2016, 5:54 am

Hidden RDP would make this the best botnet out there

Killertip - February 20, 2016, 10:50 am

oh dude i am doing a botnet too and your looks so dope i am doing a c# controller because web hosts put it down plus it only uses web page to send commands to the bot and back but i havent worked on the bot application i am too lazy lol

i will post a preview of my botnet now

h t t p s:// s content-fra3-1 .
xx.fbcdn.net/hphotos-xtp1/v/t35.0-12/12751890_774343399333172_1282297565_o.jpg?oh=185eb5
f1954051fa8b9af882b54b3f3b&oe=56CA696A

there it is and also i found something cool when i was searching about image exploits

there is nothing much but it tells you how to run code with images its old but i think you can still use it

h t t p s:/ /w w w . defcon.org/images/defcon-15/dc15-presentations/dc-15-schrenk.pdf

hope i helped and hope you liked my botnet design

(Just remove the spaces)

Arsenic_ - February 20, 2016, 12:16 pm

Other rats have cryptocurrency mining, so I dont see why talking about it is such a problem. If you state that you are using it for fraud then yes obviously thats not allowed. Its all in the wording my friend.

I dont know if you've seen the member Hades, but he has quite a large botnet and is a bot seller. Might be worth teaming up with him or asking his opinion of what works and what doesnt, or what he would like to have.

<https://hackforums.net/showthread.php?tid=4533479>

Insane Developer - February 20, 2016, 7:05 pm

(Feb 20, 2016 01:16 PM)Arsenic_ Wrote: [\[CITE\]](#) Other rats have cryptocurrency mining, so I dont see why talking about it is such a problem. If you state that you are using it for fraud then yes obviously thats not allowed. Its all in the wording my friend.

I dont know if you've seen the member Hades, but he has quite a large botnet and is a bot seller. Might be worth teaming up with him or asking his opinion of what works and what doesnt, or what he would like to have.

<https://hackforums.net/showthread.php?tid=4533479>

What he said was not allowed was my feature to detect when a BTC address is in the clipboard, and change it to another address that you specified.

I don't want to take risk so I probably won't do it.

And the bitcoin mining feature is already done. It was written in Delphi

Kristofferson - February 20, 2016, 8:51 pm

>No Rootkit

>No botkill

[img]http://orig02.deviantart.net/5338/f/2008/352/6/3/tanaka____ho_ho_ho_____by_kendoka602.jpg[/img]

Insane Developer - February 20, 2016, 9:52 pm

(Feb 20, 2016 09:51 PM)Kristofferson Wrote: [\[CITE\]](#) >No Rootkit

>No botkill

-big image-I am working on botkill, it is almost functional. And no Rootkit atm, but it is very persistent.

Added registry writer, CMD, File Deleting

Added another layer of obfuscation, it is now extremely difficult if not impossible to get the Panel URL.

Insane Developer - February 23, 2016, 4:38 am

Working on reducing stub size, more obfuscation on already completed functions and general protection against decompiling.

Botkilling is now capable of killing 75% of the malwares I threw at it.

sdsdsdsdsd - February 23, 2016, 7:27 am

Just curious, what is the language that you are writing HADES in?

Insane Developer - February 23, 2016, 6:56 pm

(Feb 23, 2016 08:27 AM)sdsdsdsdsd Wrote: [\[CITE\]](#) Just curious, what is the language that you are writing HADES in?

As stated multiple times on the thread, it is in Autolt

This project is now merged with [Roughnet](#)

This is now the developmental thread

martypacn - February 24, 2016, 4:32 pm

Sounds good fpnweffrewaffwfefwf

SIM-2198759 - February 24, 2016, 4:47 pm

(Feb 20, 2016 09:51 PM)Kristofferson Wrote: [\[CITE\]](#) >No Rootkit

>No botkill

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

[img]http://orig02.deviantart.net/5338/f/2008/352/6/3/tanaka____ho_ho_ho_____by_kendoka602.jpg[/img]

We may not get along, but that BB refrence gave me a giggle m8, Even heard the laugh in his "Voice"

Insane Developer - February 24, 2016, 5:26 pm

(Feb 24, 2016 05:32 PM)martypacn Wrote: [\[CITE\]](#) Sounds good fpnweffrewaffwfefwf

Spamming is not a good way to increase post count

(Feb 24, 2016 05:47 PM)?DeathStr0ke Wrote: [\[CITE\]](#) We may not get along, but that BB refrence gave me a giggle m8, Even heard the laugh in his "Voice"

We might even get along, since the laugh had the deep voice of an old man.?

Binary Ghoul - February 24, 2016, 5:51 pm

Can you post some pictures of it?

Insane Developer - February 25, 2016, 6:44 pm

(Feb 24, 2016 06:51 PM)Binary Ghoul Wrote: [\[CITE\]](#) Can you post some pictures of it?

Already did

?euces - February 25, 2016, 9:00 pm

This looks like its turning out pretty dope, keep it up dude and goodluck if u need any help with interfaces let me know

HADE? - February 26, 2016, 2:46 am

Are you making this in my honor ? :)

Insane Developer - February 26, 2016, 4:05 am

(Feb 26, 2016 03:46 AM)HADË? Wrote: [\[CITE\]](#) Are you making this in my honor ? :)

LMAO It was a pretty funny coincidence. If you want I can change the name so it won't be in "Your honor"?

Adding my legendary tool "The Silencer" to it to improve DDoS power

Binary Ghoul - February 26, 2016, 3:26 pm

Why is it called roughnet in the pics but hades on the thread

Insane Developer - February 26, 2016, 8:32 pm

(Feb 26, 2016 04:26 PM)Binary Ghoul Wrote: [\[CITE\]](#) Why is it called roughnet in the pics but hades on the thread

It was merged with Roughnet a few days ago since Roughnet had no binary, and Hades had no panel.

We will change it soon.

Mouser - February 26, 2016, 8:33 pm

(Feb 26, 2016 09:32 PM)Insane Developer Wrote: [\[CITE\]](#) It was merged with Roughnet a few days ago since Roughnet had no binary, and Hades had no panel.

We will change it soon.

aids bot

Erock - February 27, 2016, 6:09 am

Can i get this once it's done? Are you going to be selling it for 1000000 dollars? Because i'm poor and can't afford shit. I PM'd you.

Insane Developer - February 27, 2016, 7:10 am

(Feb 27, 2016 07:09 AM)Erock Wrote: [\[CITE\]](#) Can i get this once it's done? Are you going to be selling it for 1000000 dollars? Because i'm poor and can't afford shit. I PM'd you.

Add 7 zeros to that and you will get the price ?

Update: Now it will collect Username, PC name as well.

Working on CPU and GPU info.

FurfUksake - February 27, 2016, 9:24 am

(Feb 23, 2016 05:38 AM)Insane Developer Wrote: [\[CITE\]](#) Working on reducing stub size, more obfuscation on already completed functions and general protection against decompiling.

Botkilling is now capable of killing 75% of the malwares I threw at it.

Just out of interest how small did you manage to reduce your bin to? (excluding packing)

Insane Developer - February 27, 2016, 8:35 pm

(Feb 27, 2016 10:24 AM)Veto Wrote: [\[CITE\]](#) Just out of interest how small did you manage to reduce your bin to? (excluding packing)

975kb without packing. I am making a downloader which will come with it.

However, I honestly don't see large stub size as an issue since normally you pump it as well to make it look real. and 1mb isn't THAT large.

FurfUksake - February 28, 2016, 12:54 am

(Feb 27, 2016 09:35 PM)Insane Developer Wrote: [\[CITE\]](#) 975kb without packing. I am making a downloader which will come with it.

However, I honestly don't see large stub size as an issue since normally you pump it as well to make it look real. and 1mb isn't THAT large.

With AutoIT you are always going to get a lot of bloat which is why I prefer C, that said it could be a lot worse I have seen people peddling bins which are anywhere up to 5MB.

There are some instances where bin size does matter, normally when it is intended to be installed without the knowledge of the user rather than bound to or disguised as another application.

Interested to see how you get on with it.

Insane Developer - February 28, 2016, 3:02 am

(Feb 28, 2016 01:54 AM)Veto Wrote: [\[CITE\]](#) With AutoIT you are always going to get a lot of bloat which is why I prefer C, that said it could be a lot worse I have seen people peddling bins which are anywhere up to 5MB.

There are some instances where bin size does matter, normally when it is intended to be installed without the knowledge of the user rather than bound to or disguised as another application.

Interested to see how you get on with it.

I will also have a FUD downloader to go with it, in case the customers want it. It is almost done.

morph - February 28, 2016, 7:01 am

Sorry, but I have to assume this is shit. It's AutoIt.. ?

Insane Developer - February 28, 2016, 7:10 am

(Feb 28, 2016 08:01 AM)Zymbiotic Wrote: [\[CITE\]](#) Sorry, but I have to assume this is shit. It's AutoIt.. ?

You are underestimating the power of AutoIt.

The only limit is your imagination and your skills.

Volty - February 28, 2016, 7:37 am

It seems your focusing a lot on the FUD downloader instead of the botnet itself. Downloaders aren't really worth it. But all in all, this is pretty nice. Have you set a price?

Insane Developer - February 28, 2016, 10:55 pm

(Feb 28, 2016 08:37 AM)Volty Wrote: [\[CITE\]](#) It seems your focusing a lot on the FUD downloader instead of the botnet itself. Downloaders aren't really worth it. But all in all, this is pretty nice. Have you set a price?

I am focusing on the botnet, not the downloader.

AnonymousBuffalo - February 29, 2016, 1:21 am

Do note that his is not working on the downloader I volunteered to do it for him.

Insane Developer - February 29, 2016, 1:41 am

(Feb 29, 2016 02:21 AM)AnonymousBuffalo Wrote: [\[CITE\]](#) Do note that his is not working on the downloader I volunteered to do it for him.

This is true.

Insane Developer - March 2, 2016, 8:03 pm

Removed G-Data's detection using advanced code obfuscation and encryption method.

[\[IMG\]http://v2.scan.majyx.net/image.php?id=996894\[/IMG\]](#)

<https://pscan.xyz/results.php?id=GOvdCTEbUSdtFCr>

morph - March 3, 2016, 4:09 am

(Feb 28, 2016 08:10 AM)Insane Developer Wrote: [\[CITE\]](#) You are underestimating the power of AutoIt.

The only limit is your imagination and your skills.

You are overestimating the power of AutoIt.

What you're doing is the equivalent to building a car with wood.

Conscious - March 3, 2016, 4:18 am

(Mar 3, 2016 05:09 AM)Zymbiotic Wrote: [\[CITE\]](#) You are overestimating the power of AutoIt.

What you're doing is the equivalent to building a car with wood.

For a more or less newbie, can you explain further why AutoIT is that bad compared to the other languages being mentioned (C#, Vb.net, C etc)

Thanks in advance!

crm1234 - March 3, 2016, 4:40 am

design and Features :>

glws

.fn. - March 3, 2016, 6:52 am

If you get or want help with getting Tor support working hit me up. I don't know AutoIT too well but from what I've seen it doesn't look too difficult to pick up and you could just improve what I give you anyway

Insane Developer - March 3, 2016, 8:22 am

(Mar 3, 2016 05:09 AM)Zymbiotic Wrote: [\[CITE\]](#) You are overestimating the power of AutoIt.

What you're doing is the equivalent to building a car with wood.

Well it is not. It is just the matter of filling your stomach with Bread or Rice.

SREE - March 3, 2016, 8:28 am

form grabbing module will be good.

Insane Developer - March 3, 2016, 10:23 pm

(Mar 3, 2016 09:28 AM)SREE Wrote: [\[CITE\]](#) form grabbing module will be good.

I will consider it, however the RDP grabber is still the priority.

Dotexe - March 4, 2016, 7:40 am

aww looks really promising :P

-Cheers

ghostdog77 - March 6, 2016, 8:47 am

u did it with AutoIT i'm impressed

Pikachu95 - March 6, 2016, 2:25 pm

Sorry where can I find the download?

Insane Developer - March 6, 2016, 4:13 pm

(Mar 6, 2016 03:25 PM)Pikachu95 Wrote: [\[CITE\]](#) Sorry where can I find the download?

After we release it AND you pay \$50 ?

Pikachu95 - March 6, 2016, 5:00 pm

(Mar 6, 2016 05:13 PM)Insane Developer Wrote: [\[CITE\]](#) After we release it AND you pay \$50 ?No problem, I would talk better with you on Skype... If you have Skype can you send me a MP? TY.

Insane Developer - March 6, 2016, 7:25 pm

(Mar 6, 2016 06:00 PM)Pikachu95 Wrote: [\[CITE\]](#) No problem, I would talk better with you on Skype... If you have Skype can you send me a MP? TY.

My skype is publicly available. Add me: haigiang7

ZwClose - March 6, 2016, 7:26 pm

Isn't that galaxy's web panel :_), and how can vm decetion be advanced :_), and how do you get both ring0 & 3 :_____)

Insane Developer - March 6, 2016, 11:53 pm

(Mar 6, 2016 08:26 PM)Cute Little Girl Wrote: [\[CITE\]](#) Isn't that galaxy's web panel :_), and how can vm decetion be advanced :_), and how do you get both ring0 & 3 :_____)

Never heard of galaxy, but I am not in charge of the panel, another guy is making it. And most VM detection just kill itself if it sense VMwareservice.exe running, and mine detects it even when all of the services are disabled, and sense virtual box and hyperVM as well.

Magnumpies - March 7, 2016, 3:40 pm

This sounds interesting. Time for a closer look.

Insane Developer - March 9, 2016, 7:02 am

Working on our API system, miner and password recovery. Sales should start soon!

sotacan - March 9, 2016, 9:20 pm

Interesting, curious on the quality of each component. Normally these things are patched together so I would be very impressed by custom coded Rootkit, Botkiller, and Anti-virus evasion. Though, I'm not naive, I understand these things are normally impossible without a team or an extremely experienced individual. Anyways, If you can provide more details on that type of stuff it would be great. (Will read all thread pages soon, sorry if a lot was already mentioned!)

Also, I'd love to chat with anyone involved/interested with development of this stuff, have not been on HF in years and want some new perspective. ?

Russ. - March 9, 2016, 9:38 pm

(Mar 7, 2016 12:53 AM)Insane Developer Wrote: [\[CITE\]](#) Never heard of galaxy, but I am not in charge of the panel, another guy is making it. And most VM detection just kill itself if it sense VMwareservice.exe running, and mine detects it even when all of the services are disabled, and sense virtual box and hyperVM as well.

Shit which VM is it where you can escape and escalate privs? I'll edit this when I check my other comp.

Quick Edit: Also lets talk via xmpp and fix your "social engineer UAC" thing.

Insane Developer - March 9, 2016, 10:08 pm

(Mar 9, 2016 10:38 PM)Watson. Wrote: [\[CITE\]](#) Shit which VM is it where you can escape and escalate privs? I'll edit this when I check my other comp.

Quick Edit: Also lets talk via xmpp and fix your "social engineer UAC" thing.

It does not escape, only detects, and then it does it's best to wreck the VM and removes itself.

desmond88 - March 10, 2016, 4:53 am

It looks nice, iam very interested how it is.

Insane Developer - March 11, 2016, 5:39 am

Added "Explosion" feature, will uninstall and leaves fake traces, and attempt to destroy the computer when it detects debuggers or VM.

adige1431 - March 11, 2016, 9:31 am

Price is about how much ? I wanna buy it, it looks awesome

Russ. - March 11, 2016, 10:16 am

(Mar 11, 2016 10:31 AM)adige1431 Wrote: [\[CITE\]](#) Price is about how much ? I wanna buy it, it looks awesome

\$50 I think. I would have Insane clarify.

adige1431 - March 11, 2016, 1:49 pm

(Mar 11, 2016 11:16 AM)Watson. Wrote: [\[CITE\]](#) \$50 I think. I would have Insane clarify.
If this be 50\$ I'll definitely buy one :)

Insane Developer - March 11, 2016, 5:05 pm

Currently I want \$50 but my partner wants 200 due to the fact that "Spectral is 300 bucks and have less features!"

True story fam

Abathur - March 11, 2016, 5:20 pm

Business partner with Insane and have to say this product is amazing. Hades is everything you wanted in an HTTP botnet. Cerberus Crypter coming out soon as a bundle with Hades!

Look out for them soon!

Uiqueblhats - March 11, 2016, 9:27 pm

(Mar 11, 2016 06:05 PM)Insane Developer Wrote: [\[CITE\]](#) Currently I want \$50 but my partner wants 200 due to the fact that "Spectral is 300 bucks and have less features!"

True story famWell its coded in autoit so only basic stub will be 800kb-1mb and crypting it with autoit crypter.... Yeah you can imagine so i think \$50 is fine as a start.

Insane Developer - March 12, 2016, 1:23 am

(Mar 11, 2016 10:27 PM)Uiqueblhats Wrote: [\[CITE\]](#) Well its coded in autoit so only basic stub will be 800kb-1mb and crypting it with autoit crypter.... Yeah you can imagine so i think \$50 is fine as a start.

Well the stub is FUD by default, and the stub size is around 700kb to 800kb only.

Uiqueblhats - March 12, 2016, 7:01 am

(Mar 12, 2016 02:23 AM)Insane Developer Wrote: [\[CITE\]](#) Well the stub is FUD by default, and the stub size is around 700kb to 800kb only.Nobody in his right mind will not spread his bin even its default FUD and i think you know what i mean.

Insane Developer - March 12, 2016, 10:13 pm

(Mar 12, 2016 08:01 AM)Uiqueblhats Wrote: [\[CITE\]](#) Nobody in his right mind will not spread his bin even its default FUD and i think you know what i mean.

The crypter is for other stubs, so if the guy wants to drop a RAT on there or something, the crypter will come in handy.

hackerdelite - March 12, 2016, 10:18 pm

I want in!! I would love to test and see what the Tool is all about! Thx!

Insane Developer - March 12, 2016, 10:21 pm

(Mar 12, 2016 11:18 PM)hackerdelite Wrote: [\[CITE\]](#) I want in!! I would love to test and see what the Tool is all about! Thx!

Vouch for this HQ 4th post.

Insane Developer - March 14, 2016, 6:32 am

OK almost finished with miner, stub size is now 520kb (With packing)

0x42434e - March 14, 2016, 6:56 am

Quote:Advanced VM and debuggers detection, works even if VMware services, VirtualBox services and processes are killed/disabled prior to execution. When detected, it will do the best to destroy the VM/computer, causes noise to make the real trace unidentifiable from the fake trace, and removes itself

The fuck? Are you an idiot?

Insane Developer - March 14, 2016, 7:13 am

(Mar 14, 2016 06:56 AM)0x42434e Wrote: [\[CITE\]](#) The fuck? Are you an idiot?

I don't think I am, are you?

It is more advanced sine it detects BIOS and Hard Disk Drive as well.

Jorhead - March 14, 2016, 8:11 am

(Mar 14, 2016 06:56 AM)0x42434e Wrote: [\[CITE\]](#) The fuck? Are you an idiot?

I love how you had 0 idea to what he was talking about so you pretend you know with your ego

0x42434e - March 14, 2016, 9:37 am

(Mar 14, 2016 07:13 AM)Insane Developer Wrote: [\[CITE\]](#) I don't think I am, are you?

It is more advanced sine it detects BIOS and Hard Disk Drive as well.

Quote:When detected, it will do the best to destroy the VM/computer

Tell me why you do this even though I know your response will be stupid and riddled with arab logic.

(Mar 14, 2016 08:11 AM)Jorhead Wrote: [\[CITE\]](#) I love how you had 0 idea to what he was talking about so you pretend you know with your ego

What? If you knew anything about malware and read the function description I quoted then you would know it is idiocracy.

Clearly not though. Thanks for proving you have no knowledge about the subject at hand.

push rdx - March 14, 2016, 10:25 am

Trying to copy rombortik? ;s

FalconGreyHat - March 15, 2016, 6:08 am

I've been looking for a botnet as good as this. I'm really excited to see this developed further, and as soon as it's for sale I'll be buying.

milaeku - March 15, 2016, 2:40 pm

wants to add a rootkit, uses autoit. uses autoit in general. ugh

drogba - March 21, 2016, 5:13 pm

im interest for one where i contact you?

thx

m4z3 - March 28, 2016, 1:43 pm

interested in copy... pm me when avail

Russ. - March 28, 2016, 1:51 pm

His last visit to HF : 03-14-2016 08:41 AM

MarescaBot - March 28, 2016, 2:02 pm

Also silent visit on site?

AndreaEbbasta - March 28, 2016, 9:54 pm

Wow nice project. Cost ? ?

???? - March 28, 2016, 9:55 pm

(Mar 28, 2016 01:51 PM)Russ. Wrote: [\[CITE\]](#) His last visit to HF : 03-14-2016 08:41 AM
He get in trouble?

Phantom.exe - March 29, 2016, 9:30 pm

I'm interested. Nice project. Good job!

????ll?? - March 30, 2016, 12:39 am

meh i dont like the interface at all good luck anyways

Russ. - March 30, 2016, 1:23 am

Guy's he is gone. Stop commenting.

lorde123du75000 - March 31, 2016, 8:56 am

Hi I bought a encrypt here but the guy not answer how?
vendeur is MIKI

Insane Developer - April 7, 2016, 8:04 pm

(Mar 30, 2016 01:23 AM)Russ. Wrote: [\[CITE\]](#) Guy's he is gone. Stop commenting.
Now he's back. However, due to his changes in goal and wanting to spend more time on his site <http://zunzutech.com> and going more whitehat, the development will be a bit slower. It is already obfuscated to the point where even I cannot deobfuscate it. Stub size: 404kb (NOT FOUND CONFIRMED?)

(Mar 28, 2016 09:55 PM)ScorpiOn Wrote: [\[CITE\]](#) He get in trouble?
Nah he was busy

(Mar 14, 2016 10:25 AM)push rdx Wrote: [\[CITE\]](#) Trying to copy rombortik? ;s
No, MBR would be something of a low level, and I work in higher level. This one uses the Image File Execution option and creates large useless DLL files.

zharfan - April 8, 2016, 6:23 am

which program language do you use ?

Insane Developer - April 8, 2016, 6:52 am

(Apr 8, 2016 06:23 AM)zharfan Wrote: [\[CITE\]](#) which program language do you use ?
Posting on every single thread I have is not a good thing to do. Anyway it is Autolt and development is no longer active.

IBotnet - April 9, 2016, 7:07 am

If this bot was being fully developed then it looks good. If it's 75% copy/paste like most bots here then don't release it for a price, release it for free.

Very few coders know how to develop half of these features so...

hackdemon - *April 15, 2016, 5:40 am*

I need botnet that can caught google chrome & mozilla firefox, good sellers with website should contact me for me to buy

Skype: timothy.lipscomb1