

Forum:[Hack Forums](#)

Thread: [Secur v1.0 || Malware reversal tool/Botkiller \[FIXED\]](#)

IcYSeptember - September 20, 2014, 6:02 pm

At the moment, this is just a standard botkiller, which searches heuristically for malware. Even though it's just that, it does its job well.

I intend to add useful tools to it such as an infected shortcut fixer, AV killer fix, and a few more tools.

[Video: https://www.youtube.com/watch?v=_Ol81fUytw]

Here's the malware it has been tested with and is working perfectly against:

LoadHTTP
DarkComet
Cybergate
IPKiller
Coiner HTTP
IcYYou IRC
CryptoWall

Got more malware? Test it and let me know how it goes!
Find any bugs? Post them here and I'll fix them!

Fixed download link:

<https://mega.co.nz/#!kFUGhCaJ!ftMXiWJ389GcQVDc5azYEv6-oZOw99SXfacJ2KVNvH4>

Cammy - September 21, 2014, 8:31 am

It looks good but it crashes for me.

Tried running as admin, compability mode doesn't do anything either.

IcYSeptember - September 21, 2014, 8:59 am

(Sep 21, 2014 08:31 AM)RAJVH Wrote: [\[CITE\]](#) It looks good but it crashes for me.

Tried running as admin, compability mode doesn't do anything either.
I had that problem too, earlier. I think it's a reference error.
I'll fix it and update.

Hire - September 21, 2014, 9:02 am

Thanks, But it is also crashing for me :(
Hopefully i can use it soon!

IcYSeptember - September 21, 2014, 11:37 am

I fixed the program. Hopefully it works well now.

Cammy - September 21, 2014, 12:17 pm

Yup, downloaded it again (Now you need to fix your URL ?) and kills my DC stub just fine. Good job.

BigBill2 - September 21, 2014, 12:18 pm

Havent Tried it but watched the Youtube video and looks good!!

One suggestion can you add a loading bar or something to show that it is running and hasnt crashed on Later build / Verison?

IcYSeptember - September 21, 2014, 12:31 pm

(Sep 21, 2014 12:17 PM)RAJVH Wrote: [\[CITE\]](#) Yup, downloaded it again (Now you need to fix your URL ?) and kills my DC stub just fine. Good job.

That's good. And I fixed it

(Sep 21, 2014 12:18 PM)seedy21 Wrote: [\[CITE\]](#) Havent Tried it but watched the Youtube video and looks good!!

One suggestion can you add a loading bar or something to show that it is running and hasnt crashed on Later build / Verison?

Yes, I can add this. I'll add it now.

Mmka - September 21, 2014, 1:14 pm

Crashed for me too...

Win 8 x64 in Parallels - with admin privileges

IcYSeptember - September 21, 2014, 2:20 pm

(Sep 21, 2014 01:14 PM)Mmka Wrote: [\[CITE\]](#) Crashed for me too...

Win 8 x64 in Parallels - with admin privileges

Odd. What version of the .NET framework do you have installed?

And what error message did you get?

Guess what guys? It kills LoadHTTP!

(The second botkill was run about a minute after the first, to see if it came back)

SIM-1809171 - September 21, 2014, 3:06 pm

Great program and great coder. Thank for this release man

Hunting Rifle - September 22, 2014, 9:11 am

I got a BSOD when running this, critical process died.

IcYSeptember - September 22, 2014, 10:25 am

(Sep 22, 2014 09:11 AM)Hunting Rifle Wrote: [\[CITE\]](#) I got a BSOD when running this, critical process died.

I'll try to fix this to set the critical flag off on malicious processes.

Sparkfear - September 22, 2014, 3:32 pm

Looks very promising!

Will follow this topic on the development.

SIM-2223238 - September 23, 2014, 12:20 pm

Well, Thank you for sharing mate ;)

Guys dont download this, After I downloaded this it gave me a BSOD, Then it removed my malwarebytes and netgear genie, I dont trust this.

IcYSeptember - September 23, 2014, 5:15 pm

(Sep 23, 2014 12:20 PM)?????123 Wrote: [\[CITE\]](#) Well, Thank you for sharing mate ;)

Guys dont download this, After I downloaded this it gave me a BSOD, Then it removed my malwarebytes and netgear genie, I dont trust this.

It must have terminated a critical process. And can you tell me more about it removing Malwarebytes?

Also, along with adding an way of setting the "critical" flag off on processes, I'm going to add something to keep logs of what the program does before it does it, just in case an error occurs.

Austerity - September 24, 2014, 5:08 am

Good work!

I will take use in this once I feel that I'm infected.

Keep it up!

IcYSeptember - September 24, 2014, 10:14 am

To anyone who's getting bluescreen's, here why:

It's probably either killing a system process (which it shouldn't be, because it only searches in specific directories recursively and specific registry entries), or it's killing a malicious program that has the critical flag set on to prevent it from being killed.

Either way, I'm updating this with a logging feature, as well as a feature to set the critical flag off on malicious processes. This should stop the blue screens.

SIM-2223238 - September 24, 2014, 10:33 pm

(Sep 23, 2014 05:15 PM)IcYSeptember Wrote: [\[CITE\]](#) It must have terminated a critical process. And can you tell me more about it removing Malwarebytes?

Also, along with adding an way of setting the "critical" flag off on processes, I'm going to add something to keep logs of what the program does before it does it, just in case an error occurs.

Icy, When I try to open Netgear Genie or Malware bytes it tells me I dont have acces anymore to the program.

IcYSeptember - September 25, 2014, 8:57 am

(Sep 24, 2014 10:33 PM)?????123 Wrote: [\[CITE\]](#) Icy, When I try to open Netgear Genie or Malware bytes it tells me I dont have acces anymore to the program.

Are those stored in %appdata%, %temp%, %userprofile%, or any recursive directories?

Meow - September 25, 2014, 9:05 am

Downloaded it and it gave me BSOD..IcY why do you this mate?

Cybele - September 25, 2014, 9:09 am

Code Killed malicious file: C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSvcHost.exe

Killed malicious file: C:\Program Files\uTorrent\uTorrent.exe

BotKiller: Processes Killed: 1. Startup Items Killed: 0.Is my uTorrent infected, or is it just a false-positive lol?

Moon Rock - September 25, 2014, 9:12 am

Going to try to use this, hope I don't get BSOD. (I don't have a virus according to AVG)

IcYSeptember - September 25, 2014, 9:21 am

(Sep 25, 2014 09:09 AM)Cybele Wrote: [\[CITE\]](#) Code Killed malicious file:
C:\Windows\Microsoft.NET\Framework\v4.0.30319\SMSSvcHost.exe

Killed malicious file: C:\Program Files\uTorrent\uTorrent.exe

BotKiller: Processes Killed: 1. Startup Items Killed: 0.Is my uTorrent infected, or is it just a false-positive lol?

I'm adding a user-verification, along with a whitelist.

Moon Rock - September 25, 2014, 9:23 am

Okay, I just tried it and I got

Code BotKiller: Processes Killed: 0. Startup Items Killed: 0.
With no bsod, seems good to me.

Maori - September 25, 2014, 10:59 am

I'm not sure, but I think It's backdoored.

I don't want to accuse Icy, but it's strange that this is found by an AV.

It did even make crash my computer.

IcYSeptember - September 25, 2014, 11:17 am

(Sep 25, 2014 10:59 AM)ThePhantomBeast Wrote: [\[CITE\]](#) I'm not sure, but I think It's backdoored.

I don't want to accuse Icy, but it's strange that this is found by an AV.

It did even make crash my computer.

Feel free to decompile it, analyse it, anything.

This goes for anyone. Feel free. I'll even give the source to a trusted member.

Meow - September 25, 2014, 12:20 pm

(Sep 25, 2014 10:59 AM)ThePhantomBeast Wrote: [\[CITE\]](#) I'm not sure, but I think It's backdoored.

I don't want to accuse Icy, but it's strange that this is found by an AV.

It did even make crash my computer.

Nope,IcY gave me source code and I checked it,everything is good!

Here is proof that he gave it to me.

JakeFromStateFarm - September 26, 2014, 5:46 pm

First time running the application. Crashed my computer and asked for my machine to connect to 23.5.251.27:80 TCP. Why is this?

IcYSeptember - September 26, 2014, 6:15 pm

(Sep 26, 2014 05:46 PM)JakeFromStateFarm Wrote: [\[CITE\]](#) First time running the application. Crashed my computer and asked for my machine to connect to 23.5.251.27:80 TCP. Why is this?
23.5.251.27 = ocsp.verisign.com

Yeah, I decided to hack Verisign so I could infect a few members on Hack Forums /sarcasm.

Do some fucking digging before you accuse me, and don't say you haven't accused me because I know you are, of infecting members.

Aura - September 26, 2014, 9:59 pm

IcY's program is legit. We are talking about someone here who successfully found a 0 day in Sandboxie and reported it to the company instead of selling it. If you don't trust his product, don't download it. Don't accuse him of what he's not, simple as that.

Lord.Baltimore - November 5, 2014, 8:08 am

Good, very good job !

With the server that's present in my PC, it's a good tools haha !

Thanks iCy