

Forum:[Hack Forums](#)

Thread: [· A?u?is Sca??er ``Tutorial`` ·](#)

iBoNeT - May 29, 2011, 11:38 am

What'z Up All?

Ok today's I'll show you how to explore .exe {Windows application} file if the file is a server or viruses.

1.

Visit : <http://anubis.iseclab.org/index.php>

2.

Here is the interface that we have needed :

[img]http://localhostr.com/file/OtDDOQp/Capture.PNG[/img]

Click the Browse button or upload and choose your application.

For application we'll create a server with DDoSeR 4.2 or other...

3.

Choose your file :

[img]http://localhostr.com/file/LLmj7GT/Capture2.PNG[/img]

4.

Go down and apply the option to be faster :

[img]http://localhostr.com/file/KUusKC7/Capture3.PNG[/img]

5.

Click "Submit for Analysis"

6.

Click the link :

[img]http://localhostr.com/file/441mHmU/Capture4.PNG[/img]

7. The site scans your file, it may take a few minutes...

[img]http://localhostr.com/file/Bsek6BD/Capture5.PNG[/img]

8.

You must choose what format you want the report (HTML, XML, PDF, Text) We will choose the HTML.

9.

You can now browse your file... We will check the IP address and DNS server.

10.

DDoSeR_4.2 = Is detected as the client server

svchost.exe = Is detected as an application created it or the virus directly

[img]<http://localhostr.com/file/ScsmnOw/Capture6.PNG>[/img]

11.

"Processes Created:" This is what he created.

[img]<http://localhostr.com/file/aju5lcJ/Capture7.PNG>[/img]

12.

DNS Queries" this is where you'll see the IP address, DNS server.

[img]<http://localhostr.com/file/xR0B8Zk/Capture8.PNG>[/img]

--

This tutorial is made by me, if you want to share it on another site please ask my permission.

Thank you for watching.

Conch - May 29, 2011, 3:46 pm

Very Interesting Post indeed.

I never knew you could query DNS/IP addresses, and other processes the infected file creates.
I will use Anubis more often in the future now after reading this :)

Thank you.

iBoNeT - June 1, 2011, 6:24 pm

Thank you for your comment.

I found several IP with this site ..

quintz - June 2, 2011, 6:03 pm

Haha, sweet...

This is just as good as Sandboxie ;D

NlZ - June 3, 2011, 6:16 pm

Thanks you very much. :)

-NlZ

iBoNeT - July 15, 2011, 10:49 pm

(Jun 3, 2011 06:16 PM)NlZ Wrote: [\[CITE\]](#) Thanks you very much. :)

-NlZ

Thanks you, I appreciate.

Joey Tribbiani - July 16, 2011, 6:51 am

Good job. However, there is a lot more to analyzing the anubis result to determine if the file is really clean or not (and it's not even easy).

iBoNeT - July 16, 2011, 11:40 am

(Jul 16, 2011 06:51 AM)Joey Tribbiani Wrote: [\[CITE\]](#) Good job. However, there is a lot more to analyzing the anubis result to determine if the file is really clean or not (and it's not even easy). Yes indeed, but the things I like is that we can see the communication with the file.

Eminent - July 16, 2011, 11:10 pm

Just a couple suggestions to make your thread better:

1. Change the title so it isn't a bunch of special characters (it looks more professorial)
2. Put the pictures in spoilers

iBoNeT - July 16, 2011, 11:20 pm

(Jul 16, 2011 11:10 PM)Eminent Wrote: [\[CITE\]](#) Just a couple suggestions to make your thread better:

1. Change the title so it isn't a bunch of special characters (it looks more professorial)
2. Put the pictures in spoilers

I had thought of this. But I can not :

Sorry but you cannot edit your post. The Administrator has set it so that posts can only be edited within 1440 minutes of posting.

Eminent - July 17, 2011, 10:04 am

(Jul 16, 2011 11:20 PM)iBoNeT Wrote: [\[CITE\]](#) I had thought of this. But I can not :

Sorry but you cannot edit your post. The Administrator has set it so that posts can only be edited within 1440 minutes of posting.

Oh yeah. Sorry, it slips my mind sometimes that you have to be l33t or UB3R in order to do that.

iBoNeT - July 17, 2011, 11:09 am

(Jul 17, 2011 10:04 AM)Eminent Wrote: [\[CITE\]](#) Oh yeah. Sorry, it slips my mind sometimes that you have to be l33t or UB3R in order to do that.

Yes indeed, I'll change it when I will be l33t/Ub3r, thank you for your proposal.