**Ports of Cicada onions**

**Cicada uses different port for every onion**

onion 1 Apache Server at auqgnxjtvdbll3pv.onion Port 5240

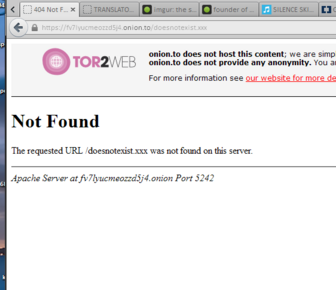
onion 2 Apache Server at cu343l33nqaekrnw.onion Port 5241

onion 3 Apache Server at fv7lyucmeozzd5j4.onion Port 5242

onion 4 Apache Server at avowyfgl5lkzfj3n.onion Port 5243

onion 5 We didnt get same error anymore [http://q4utgdi2n4m4uim5.onion](http://q4utgdi2n4m4uim5.onion/)

To see PORT number just enter nonexisten link after valid onion url

[](https://static.wikia.nocookie.net/uncovering-cicada/images/f/f6/97sfcnM.png/revision/latest?cb=20140109023245)

Maybe the same Server? Would make sense from cicadas view

Onion 5: [http://q4utgdi2n4m4uim5.onion](http://q4utgdi2n4m4uim5.onion/)

We dont have port number.

More about why we dont have it in this log:

Collapsed log

More about why we dont have it in this log:

[02:31] <NiceLurk> also nobod y checked the port number

[02:31] <r2dliu> it wasn't availalbe

[02:31] <NiceLurk> [http://uncovering-cicada.wikia.com/wiki/Ports\_of\_Cicada\_onions](https://uncovering-cicada.fandom.com/wiki/Ports_of_Cicada_onions)

[02:31] <NiceLurk> To see PORT number just enter nonexisten link after valid onion url

[02:31] <r2dliu> yea that part was missing from onion5

[02:32] <NiceLurk> but i guess we can assume it was Port 5244

[02:32] <akame> lol

[02:32] <-- Anoniem4l (c7feeeae@gateway/web/freenode/ip.199.254.238.174) has quit (Ping timeout: 245 seconds)

[02:32] <akame> can we

[02:33] --> ksihkehe\_ (48bdf90d@gateway/web/freenode/ip.72.189.249.13) has joined #cicadasolvers

[02:33] <NiceLurk> or if error mesage was different, it menas that cicada saw that we are noting those ports and manually chanhged error mesages in apache

[02:33] <dead> while it was up

[02:33] <dead> we tried to hit port 9133/3319 etc..

[02:33] <NiceLurk> yeah it works only while it was up

[02:33] <dead> nothing

[02:33] <akame> note that these are just arbitrary address tag texts in a static error page or header

[02:33] <NiceLurk> yeah

[02:33] <akame> not clear any actual port is involved

[02:33] <NiceLurk> it doesnt mean it is really this port

[02:33] <ext> NiceLurk: since all urls was serving the string the port number could not be observed

[02:34] <NiceLurk> but apparently its another "signture" of cicada, for every onion that port should be higher by one

[02:34] <NiceLurk> ext: of it was lobal redirect?

[02:34] <r2dliu> was that true for previous years?

[02:34] <-- ksihkehe (48bdf90d@gateway/web/freenode/ip.72.189.249.13) has quit (Ping timeout: 245 seconds)

[02:34] <NiceLurk> r2dliu: idk

[02:34] <akame> but this is all just a playful ordering technique

[02:35] --> Slipknot- (~flashdr@c-24-6-178-40.hsd1.ca.comcast.net) has joined #cicadasolvers

[02:35] <ext> NiceLurk: no redirect, it served the string directly

[02:35] <ext> or what do you mean "local redirect"? url rewriting?

[02:36] <akame> that is not possible to find out

[02:36] --> logikal (~logikal@30.sub-70-208-71.myvzw.com) has joined #cicadasolvers

[02:36] <NiceLurk> ext xeah but if you entered <http://avowyfgl5lkzfj3n.onion/somethingdirty.xxx> then you aso got string?

[02:36] <ext> what we should have tried was passing an invalid method or something

[02:36] <ext> NiceLurk: yes

[02:36] <-- gigart (46b9d742@gateway/web/freenode/ip.70.185.215.66) has quit (Quit: Page closed)

[02:36] <akame> y i think i tried index or smth

[02:37] <NiceLurk> yeah isnt that coalled global redirect? idk, our guys call it like this

[02:37] <ext> it was not a HTTP redirect

[02:37] <-- D\_Synapse (~flashdr@c-24-6-178-40.hsd1.ca.comcast.net) has quit (Ping timeout: 272 seconds)

[02:38] --> OzWiSkeptic (cb278aaa@gateway/web/freenode/ip.203.39.138.170) has joined #cicadasolvers

[02:39] <ext> a possible way to get the port would be to use a bad method (e.g. not GET or POST), but I don't think to try that at the time

[02:39] <ShadowFix> I am off see you tomorow> good night and good luck..

[02:39] <OzWiSkeptic> Good aftermorn everyone, how are we travelling today?

[02:39] --> grazzaB (~grazzab@wcnat-108-170.wheaton.edu) has joined #cicadasolvers

[02:39] \*\*\* Mode #cicadasolvers +o grazzaB by ChanServ

[02:39] <ext> didn\*t

[02:39] <akame> shadowfix: nighty

[02:40] <NiceLurk> ext: we will se on next onion, if it will be up long enough

[02:40] <NiceLurk> i serioulsy thing cicada is removing onions so fact to prevent us disecting them

[02:40] <ShadowFix> I will be back tomorrow and be able to be on all weekend, goodnight and thanks..

[02:41] <ShadowFix> NiceLurk: yes, I agree

[02:41] <ShadowFix> bye

[02:41] <erfwerf> one thing: why cicada pic on jpg4 is different from all cicadas seen till now?

[02:42] <ext> if using curl to fetch the page, use "-X foo" to pass an invalid method which will result in HTTP 405 Method Not Allowed

[02:42] <-- ShadowFix (56b2e2dc@gateway/web/freenode/ip.86.178.226.220) has quit (Quit: Page closed)

[02:42] <ext> and the port will be in the description

[02:42] <ext> unless they disabled error pages ofcourse

[02:43] <-- Surtri (~surtri@gateway/tor-sasl/surtri) has quit (Remote host closed the connection)

[02:43] --> Anoniem4l (bc7e4bfa@gateway/web/freenode/ip.188.126.75.250) has joined #cicadasolvers

[02:44] --> Discordia\_ (4b900d1e@gateway/web/freenode/ip.75.144.13.30) has joined #cicadasolvers

[02:45] <-- neziru (41621811@gateway/web/freenode/ip.65.98.24.17) has quit (Ping timeout: 245 seconds)

[02:46] <SheCalledMeSleep> what i miss, anything

[02:47] <-- Slipknot- (~flashdr@c-24-6-178-40.hsd1.ca.comcast.net) has quit (Ping timeout: 245 seconds)

[02:48] --> gig\_ (46b9d742@gateway/web/freenode/ip.70.185.215.66) has joined #cicadasolvers

[02:50] <akame> ext: curl -w %{remote\_port} ??

[02:51] <-- brotherBox (~brotherBo@ip-178-203-85-56.unitymediagroup.de) has quit (Ping timeout: 240 seconds)

[02:52] <NiceLurk> erfwerf: it is not actually

[02:52] <NiceLurk> i f you are talking about jpg4 from onion 4

[02:52] <erfwerf> i've missed something i suppose then

[02:52] <SheCalledMeSleep> NiceLurk, anything from like 4:30 ish?

[02:53] <NiceLurk> erfwerf:

[02:53] <NiceLurk> same cicada was twice on warning page (not sure itf that is page 2 or 3 though)

[02:53] <erfwerf> cool thanks :)

[02:54] <erfwerf> i was wrong, happens

[02:54] <NiceLurk> it just wanst place in the middle so it was much harder to spot

[02:54] <erfwerf> and well, it happens a lot of times if cicada is around lol

[02:54] <NiceLurk> sometime best place to hid things is in plain sight

[02:54] <akame> anyone got a link of all five onion addresses?

[02:54] <NiceLurk> i also tought i saw that new cicada first time whne i looked at jpg4 from onion 4

[02:54] <-- nbka (~nbk@2.82.17.108) has quit (Ping timeout: 240 seconds)

[02:55] <NiceLurk> akame: 4 are there

[02:55] <NiceLurk> <NiceLurk> [http://uncovering-cicada.wikia.com/wiki/Ports\_of\_Cicada\_onions](https://uncovering-cicada.fandom.com/wiki/Ports_of_Cicada_onions)

[02:55] <-- OzWiSkeptic (cb278aaa@gateway/web/freenode/ip.203.39.138.170) has quit (Quit: Page closed)

[02:55] <NiceLurk> [http://q4utgdi2n4m4uim5](http://q4utgdi2n4m4uim5/) - 9133

[02:55] <-- logikal (~logikal@30.sub-70-208-71.myvzw.com) has quit (Ping timeout: 245 seconds)

[02:56] <NiceLurk> thats fifth one

[02:56] <ext> akame: "-x foo" changes the http method to an invalid which will cause an error no matter what, the only question is if an error page is rendered or not

[02:56] <-- Discordia\_ (4b900d1e@gateway/web/freenode/ip.75.144.13.30) has quit (Ping timeout: 245 seconds)

[02:57] <-- nopd (~nopd@gateway/tor-sasl/nopd) has quit (Ping timeout: 240 seconds)

[02:57] <NiceLurk> ext: was that redirect from all pages to index html done by htaccess?

[02:58] <NiceLurk> like this: <http://stackoverflow.com/questions/17709500/how-to-redirect-all-pages-only-to-index-html-using-htaccess-file-and-not-redirec>

[02:58] <ext> either using .htaccess or using the host configuration

[02:58] <ext> but no, not as SO

[02:58] <ext> they cause a HTTP redirect

[02:59] <ext> <http://httpd.apache.org/docs/2.2/mod/mod_alias.html#aliasmatch> <-- more like that

[03:01] <ext> the major difference is that a http redirect sends a reply to you "hey, the new url is over here: ..." and your client automatically fetch the new

[03:01] <ext> while an alias is transparent to you

[03:02] <NiceLurk> cool thx