The neonazis are now using Tor, and that’s fine (Online Article)

Historical Note

This online article was published in October of 2017 by the website Kontrasusta.

Content

The neonazis are now using Tor, and that’s fine

published on October 22, 2017 by nvp

The title requires a lot of unpacking, so bear with me. Please also note that there’s more technical details I decided not to go into, I’m giving an extremely simplified overview of the technology discussed.

Tor is a free-as-in-freedom software project which implements an encryption technology known as *onion routing*. It gets that name because it uses multiple layers of encryption to route a request between the initial client and the final server, *like layers of an onion*. The Tor software creates ephemeral circuits of intermediary computers (called *relay nodes*) which take turns requesting the web resource the initial client wants to access, in a way that no node knows where the request is coming from originally, and where it must terminate – each node only knows who the immediately adjacent node to them in the circuit was.

There are two ways Tor can be used. One is to access websites on the Internet we know, the *somewebsite.org* kind of websites. This manner of use requires some *exit nodes*, that is some Tor nodes which are connected to the Internet, and fetch websites that some client which is unknown to them requested. Then there is what is called “hidden services”, or “onion services”. Those are websites that are only accessible over Tor, but not from the Internet as we know it. Onion services do not have traditional web addresses, and since they are inside the Tor network, they can hide their location in the same way Tor nodes don’t know anything but their immediately adjacent notes in the ephemeral circuit they find themselves in.

Of course, if the Onion service website wants to be accessible, it does need to tell at least one node where it can be found. Tor could develop a system that works like the somewebsite.org addresses we know, but they decided not to.

The traditional web addresses use something called DNS, *Domain Name System*. DNS uses tables which translate word-based addresses to numerical *IP* addresses which correspond to the position where the server is connected to the Internet. For example www.eff.org is located at 69.50.232.54.

DNS is hierarchical. Different governmental bodies and private businesses can assign different levels of the domain name, and they provide the look-up tables to help a computer convert the word-based address into the numerical location. In very simple terms, the highest authority delegates the Top

Lever Domains (.org, .com, .info, .cy, .fr, .ca, and so on) to the Registrars (private businesses, public organisations, or governments; for example .cy is administered by University of Cyprus, while .info is administered by a private company in Ireland). Those Registrars can also have sub-Registrars which they are allowed to sell the domains they own. For example you can buy a .info domain (lets say somewebsite.info) from the US-based private company GoDaddy, who have reseller rights for .info domains. Once you have that website address, you are now the next chain in the hierarchy, and you can assign subdomains for your use, or for others. For example you can create the subdomain *projects.somewebsite.info*.

Skipping over some implementation details, what we need to know is that the hierarchical way of DNS means that if someone in that chain of command decides to remove you from their look-up tables, your website address will not be translated to the numerical address, and users will not be able to visit you. For example, this is what happens when your domain name expires and you don't renew it. It starts to be erased from the look-up tables, if the look-up tables preferred by the computers of your readers are among those who erased your expired domain, they won't be able to find you.

And this is where we get to the Nazis. After the neonazi attack in Charlottesville USA —which appears to be a decisive moment similar to the murder of Fyssas in Greece— a lot of previously "neutral" political groups (the various kinds of liberals and radical centrists), as well as amoral corporations who would have preferred to continue businesses as usual, are forced to take a stance and pick a side. The domain name registrar GoDaddy was thus forced to cancel the domain name of a famous white supremacist blog and forum. To counter this, the neonazis decided to make their website accessible again as an Onion service, to resist any further attempts to be rendered inaccessible.

They are practically certain not to be blocked while on Tor, because here the routing happens over special onion circuits, which advertise their *knowledge of where the Onion service is hosted*. The advertisement is in turn picked up by various independently operated nodes which perform look-up table duties, and arrange a "blind date" at a rendezvous-point (where the last link of the client-side onion circuit connects to the randezvous node, which in turn connects to the last link of the server-side circuit, securing this way that neither the client, nor the server, nor the match-maker randezvous-point know the location of each-other).

This lead to a few voices from the various anti-nazi coalitions (the non-entirely-pushover liberals, the antifas, the anarchists, the US antiracist movements and so on) urging Tor, the software project, to kick off the nazis from the Onion network.

This is impossible, and we should be glad it is. Not because neonazis deserve free speech. They don't. But because it means that the software the Tor community maintains works as intended. It was designed to be censorship-resilient and without having any single computer in a position of authority that allows them to control which websites are accessible and which are, in effect, un-routable. It's a political decision baked right into the source code of the Tor software.

This is not the first time Tor was asked to remove access to content. For one, there were neonazis on the Onion network for years already. And there's more vile content on Tor, which includes child pornography and revenge porn, covert slavery markets, hitmen for hire and so on. Black markets also exist as Onion services. Not to mention that FBI and other state-agencies own and operate many of those vile websites as honeypot traps.

But on the Onion network you can also find projects like the Debian GNU/Linux distribution (sejnfjrq6szgca7v.onion), the Sci-Hub academic journal liberator (scihub22266oqcxt.onion), or the radical tech collective Riseup (nzh3fv6jc6jskki3.onion), which use Onion services to provide their

users with extra security and defence against hackers (freelancer or state-sponsored ones) and censorship.

So, am I saying that there is nothing the Tor Project can do? Not quite. But there’s nothing meaningful to do. The Tor Project could send an update that will make nodes pretend a certain Onion service doesn’t exist. The only thing this would achieve is to make everyone lose trust on Tor’s promises, but in practical terms, the neonazis can simply create a new Onion service. Users and node operators can skip that update. And because Tor is a software that is free-as-in-freedom, even if all existing nodes agree that neonazis can fuck off Tor, the neonazis can simply take the source code and build their own Onion network.

Does that mean that we have to tolerate neonazis online? Hell no. There’s still a lot more than can be done to attack their forum. A dynamic website is an application, even when accessible over Tor. Applications can be hacked. What neonazis seem to really fear is their private details leaking. No doubt they share a lot of identifying information all over their website. Malware can be injected in their forum software that will inflect their computers and further facilitate exposing them. Their website can be bombarded with access requests so that their network connection melts down (this is called a Denial of Service attack). **But we have to avoid self-defeating tactics.** We cannot break Tor for the symbolism of kicking of the nazis (it will be purely symbolic but ultimately pointless, as already explained). Without a working Onion network we are also in the same danger. We cannot demand that effective encryption is outlawed because fascists can also use it. If it’s outlawed, we will also have to face the consequences of insisting on using it, because we *need* encryption. We cannot insert flaws in the software that only we can know about them and only use them for good reasons. Those are always independently discovered by others, with different agendas than us. And very importantly, free-as-in-freedom software is not a problem, neither in this case, nor ever: if Tor was not freedom-respecting and opensource, we wouldn’t have any trust in it in the first place. Because it is free-libre software, we know that we too can resist if ever the Tor Project decides to push an update that targets us.

In conclusion, bash the fash, not encryption.

Needs Turkish Translation, Kontrasusta (Website), Online Articles, Decade 2010-2019, 2017, Undefined Location