The Hidden Internet

Josh Michaels, 2012-19-11

Recently, a manager, let's call him Rob, overheard me talking with Sam about an issue he was having with his automobile. The auto had an inboard dash diagnostic system, but it was pass coded. The dealership and mechanics stated they were not allowed to divulge the code, lest they be terminated/punished. I thought it sounded a little silly and told Sam that I would look around to see if someone might have a clue about accessing it. Rob, always the jester, called out of his office asking "if I was going to locate some information on my ***super secret special internets***".

It was a good jest, but it got me thinking.. and the answer was Yes.. yes I was going to use my super secret hidden internet.

Among my network, we often joke that "we're going to go back to our internet now, as the other one has gotten (silly|stupid|full of ludites| etc). We kid about "having stared into darkness at the end of the internet, and found it staring back" While we laugh about it, there is some truth to the statement.

> *** NOTE* The data being shared below is can be dangerous, as some of the accessible items are of gray legal areas, even to access. Others are completely illegal, immoral. Please read and use this information responsibly.**

What is the "hidden internet"? Easy, it's networks that are not general public access. Whether they are user access restricted, skill level restricted, or just obfuscated. Everything from Darknets (invite only systems, often file shares, message boards, irc's. Possibly some form of floating VPN access) to the TOR network.

TOR

The easiest one to show you is the TOR network. Everyone knows TOR as the anonymizer. It is supposed to allow people to bounce their connections through multiple nodes, hiding who they are. In reality, it is very easy in most cases to determine the identity of someone bouncing along the TOR nodes. Also, the exit node (last node the connection goes through before it hits the destination) is capable of reading all unencrypted traffic. There are multiple documented cases of researchers, evils, and governments running exit nodes simply to capture data.

Beyond just an anonymizer, TOR also houses an underground. There is an entire TLD called .ONION. Housed here are "hidden services", sites that live on the TOR network and can only be accessed from TOR. The launch pad for the ONION is typically the TORDIR. This is a directory page for some sites within the ONION network.

While TORDIR can potentially be mostly informative data and actually has some fully legal services/content, it also can contain more dark and possibly nefarious links.

Beyond TORDIR, there is a darker site. The "Hidden Wiki". The address floats a bit, but a google search will always return it.

What's the Hidden wiki?

It's less than legal central. From whistle blowing, credit card sales (selling stolen numbers) , narcotics, ripped movies, anonymizers, and other items of even darker natures. These are listed on the hidden wiki.
The hidden wiki, it's not a nice, happy fluffy bunny sort of place, but sometimes security engineers have to sift through the garbage to find the data needed to save something.

If you are interested in exploring the ONION network:

> If you have access to TOR, kick it on and access:
> ****NOTICE:**
> **ALWAYS RUN WITH NO SCRIPT**
> **USE A BROWSER IN A RESEARCH VM (A clean VM, that you delete at the end of research. Hopefully run from an isolated unit that only has outbound network access)**
> ********
>
> http://dppmfxaacucguzpc.onion
> This is the TORDIR. It's rather safe (the top level anyways). Here you can access different sites, etc through TOR onion links.
> ****NOTICE:**
> **BEWARE THE PINK LINKS. (Hostile and offensive content ranging from illegal images to illegal business options.**
> ******
>
> ---

Hope this was informative in some way or another.

Respectfully,
Josh Michaels
Devcentral Security Solutions Developer

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc. Corporate Headquarters info@f5.com	F5 Networks Asia-Pacific apacinfo@f5.com	F5 Networks Ltd. Europe/Middle-East/Africa emeainfo@f5.com	F5 Networks Japan K.K. f5j-info@f5.com