Kamran Saifullah

Cyber Security Enthusiast

Qatar

Email

Twitter

LinkedIn

GitHub

Utilizing BTunnel For Data Exfiltration

5 minute read

On this page

Initials

I have been working on `DevTunnels`, `CloudFlared` and they have always amazed me based on their usage i.e. providing ease to developers to expose their local codebases/applications over the internet and possibly by IT Team for troubleshooting and support. However, i always knew that threat actors are not taking a u-turn from LOLBins, Living Off Other Binaries etc. But, today it has happened in a research article covered by `Unit 42` where they uncovered a threat actor targeting `Asia` and utilizing developers systems i.e. installed `Visual Studio Code` devtunnels for data exfiltrations.

Reference: https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage/

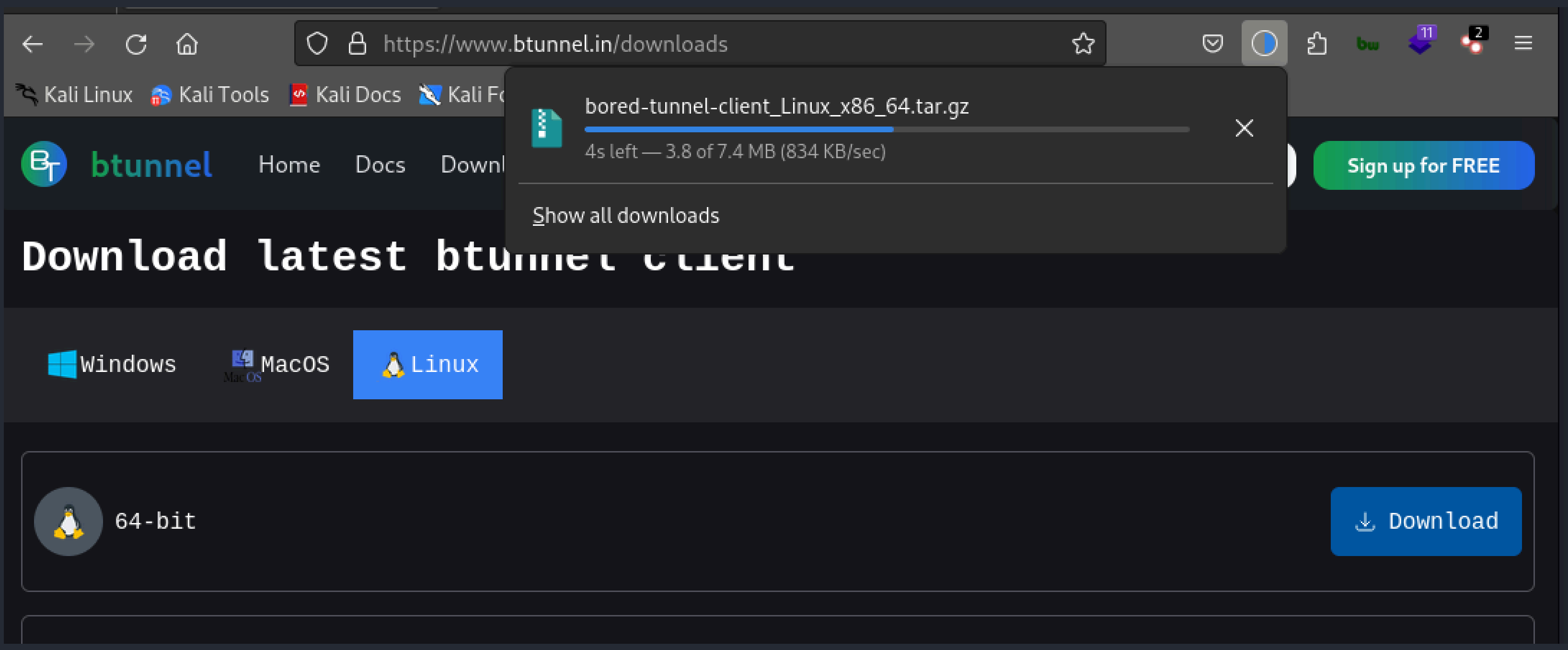
As organizations in most of the cases are not that much taking a look into the developers tools but threat actors have always been and have been trying to get into the system and findings simple ways to exfiltrate the data outside of the organizations. These tools have proven to be worth it for threat actors.

These tools are very simple to use yet very effective and kind of dificult to find whether any data exfiltration activity is happening as the tunnels created and hosted are on official website i.e. Microsoft, CloudFlare which are normally whitelisted everywhere.

While doing more research and finding out other possible solutions which work in the same way, one organization from `India` had my eyes on i.e. `BTunnels`. This works completely in similar fashion where the difference is that the `Authentication` of the session is based on `API KEY`. As well as very simple to configure `Username` and `Password` for authentication. But what will happen if API KEYs of someone else is exposed and is used by threat actors to exfiltrate the data? That still remains the question on how important it is to keep the API keys safe and secure.

BTunnels

It is fairly simple to use this tool as its a pre-compiled binary and is not required to be installed on the local system. Simple,y by hopping onto the downdloads sections we can download our required binary for `Mac, Windows & Linux`. For the sake of this article, i will be using `Linux` binary.

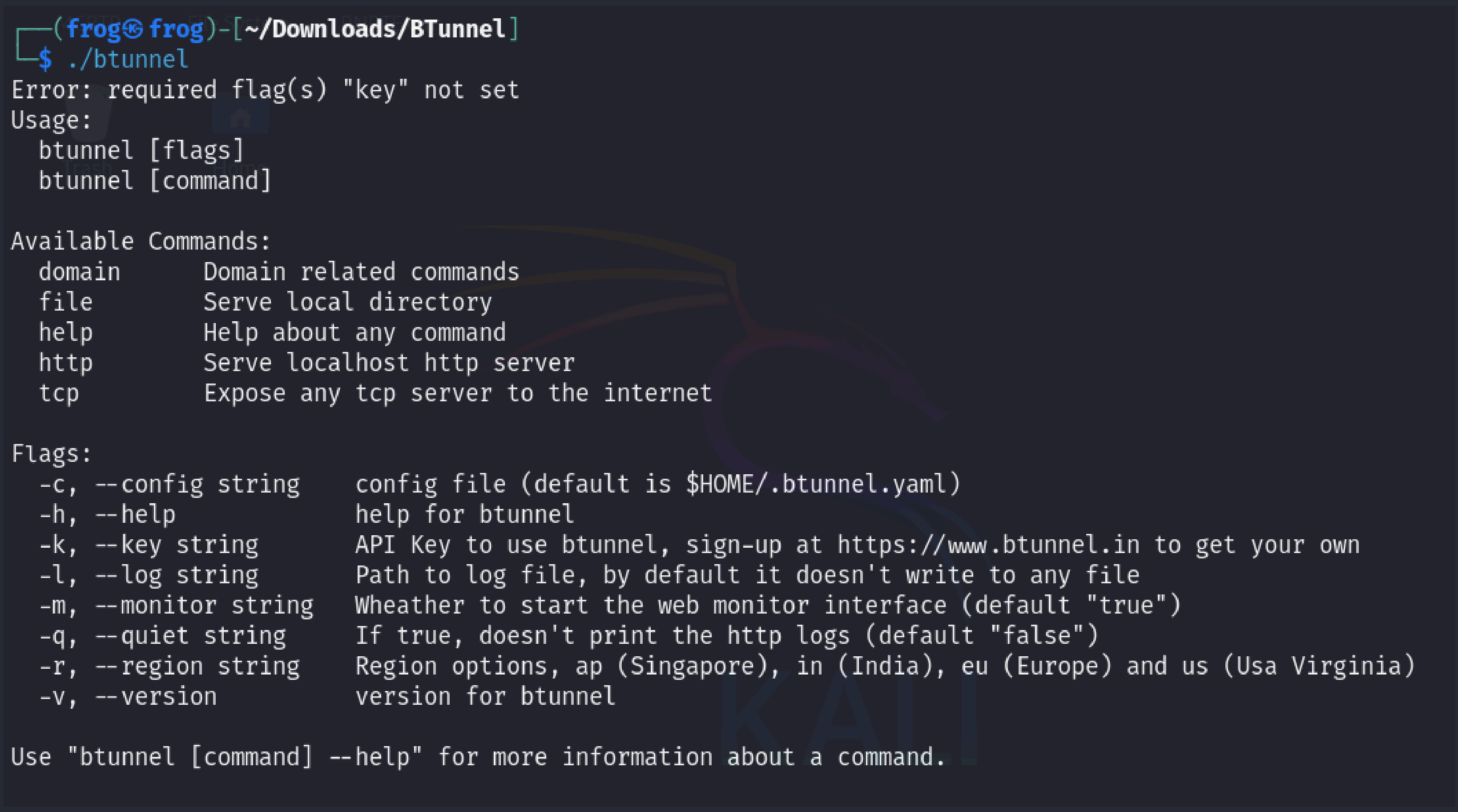

https://www.btunnel.in/downloads
Kali Linux
Kali Tools
Kali Docs
Kali Fo
btunnel
Home
Docs
Downl
Sign up for FREE
bored-tunnel-client_Linux_x86_64.tar.gz
4s left — 3.8 of 7.4 MB (834 KB/sec)
Show all downloads
Download latest btunnel client
Windows
MacOS
Linux
64-bit
Download

After this, simply create an account, hop over to `Dashboard` and grab your `API KEY`.

Finally, running the command to see what capabilities we have. As of writing this article, we have the following options.

1. Domain
2. File
3. Http
4. TCP

Well, as its very clear and all 4 can be abused/illegimiate use of the functionality for data exfiltration.



```
┌──(frog㉿frog)-[~/Downloads/BTunnel]
└─$ ./btunnel
Error: required flag(s) "key" not set
Usage:
  btunnel [flags]
  btunnel [command]

Available Commands:
  domain      Domain related commands
  file        Serve local directory
  help        Help about any command
  http        Serve localhost http server
  tcp         Expose any tcp server to the internet

Flags:
  -c, --config string     config file (default is $HOME/.btunnel.yaml)
  -h, --help              help for btunnel
  -k, --key string        API Key to use btunnel, sign-up at https://www.btunnel.in to get your own
  -l, --log string        Path to log file, by default it doesn't write to any file
  -m, --monitor string    Wheather to start the web monitor interface (default "true")
  -q, --quiet string      If true, doesn't print the http logs (default "false")
  -r, --region string     Region options, ap (Singapore), in (India), eu (Europe) and us (Usa Virginia)
  -v, --version           version for btunnel

Use "btunnel [command] --help" for more information about a command.
```

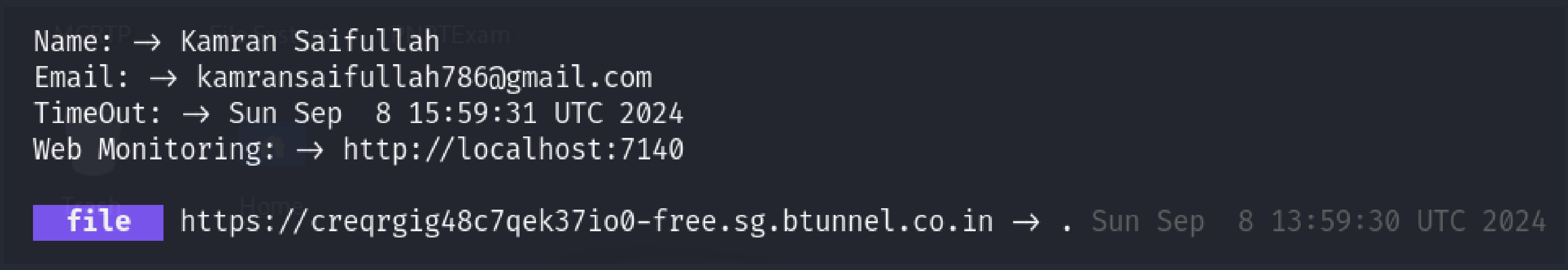
Lets take a look few of these.

1. File

The command for this is going to be as below.

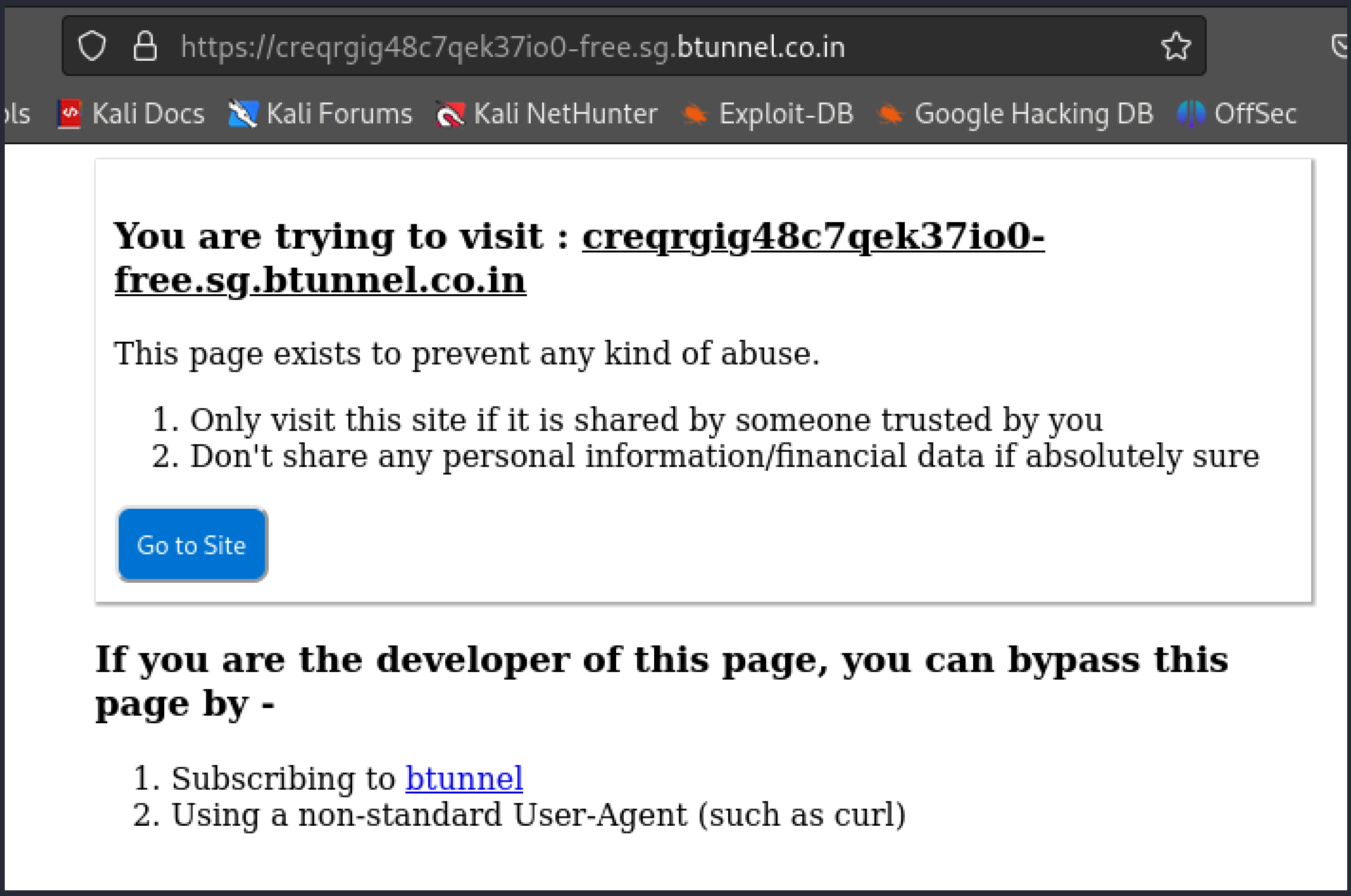
```
./btunnel file --key <API-KEY>
```

Once we execute the command, we are provided with the `Tunnel Link` to access the the local file system over the internet directly.



```
Name: → Kamran Saifullah
Email: → kamransaifullah786@gmail.com
TimeOut: → Sun Sep  8 15:59:31 UTC 2024
Web Monitoring: → http://localhost:7140

 file  https://creqrgig48c7qek37io0-free.sg.btunnel.co.in → . Sun Sep  8 13:59:30 UTC 2024
```

Using the tunnel link as i am not subscribed yet, we are provided with the warning.



You are trying to visit : creqrgig48c7qek37io0-free.sg.btunnel.co.in

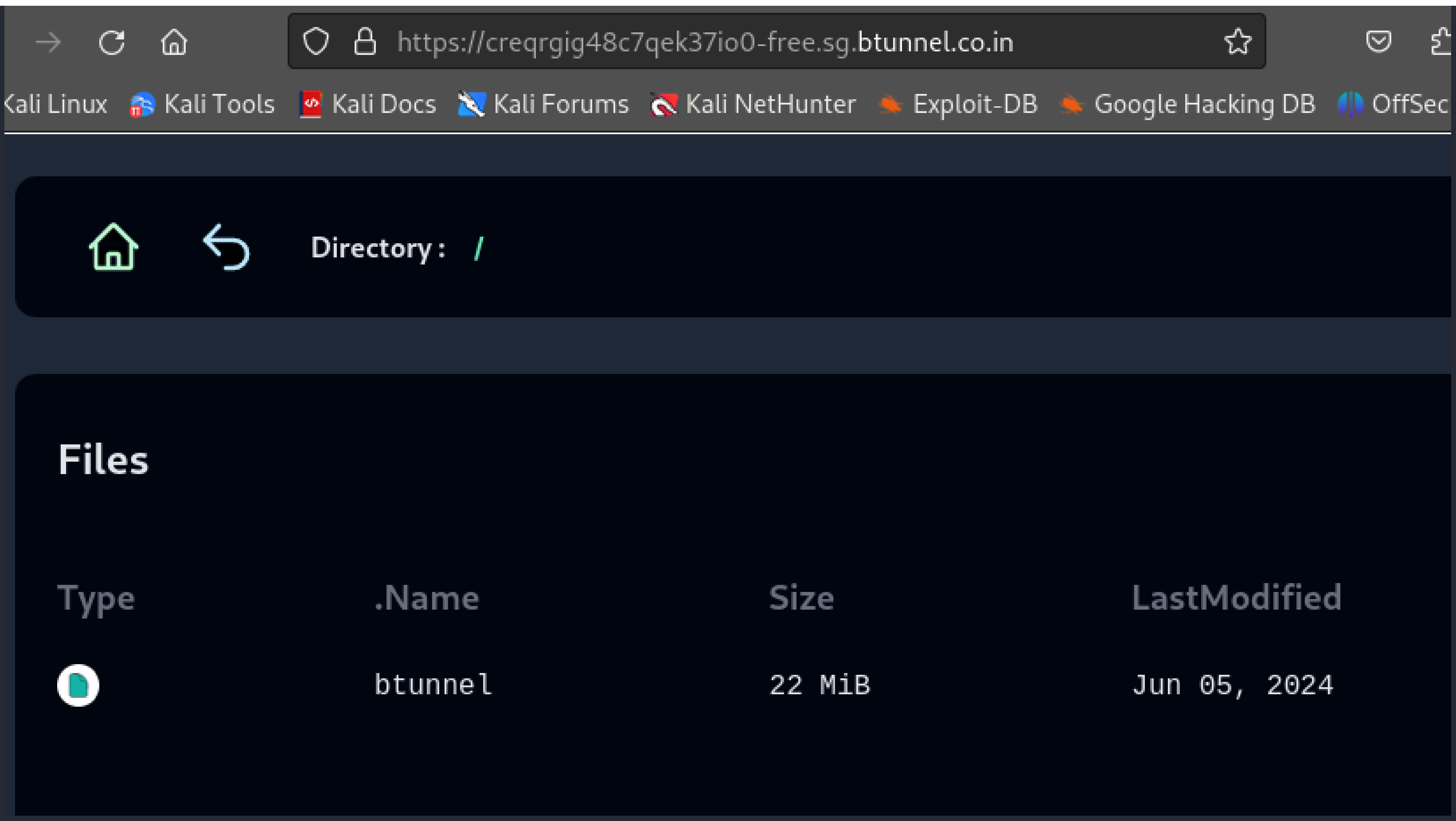
This page exists to prevent any kind of abuse.

1. Only visit this site if it is shared by someone trusted by you
2. Don't share any personal information/financial data if absolutely sure

If you are the developer of this page, you can bypass this page by -

1. Subscribing to btunnel
2. Using a non-standard User-Agent (such as curl)

After clicking `Go To Site`, we can easily access the local file system over the internet.



Directory : /

Files

Type	.Name	Size	LastModified
●	btunnel	22 MiB	Jun 05, 2024

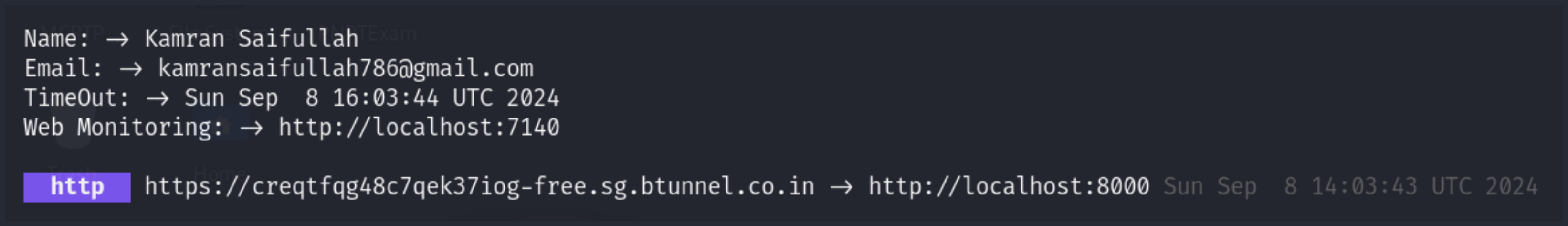
Now, this is one usecase where we can easily expose the local file system over the internet.

2. Http

In order to forward the local port over the internet, we can use the following command where port number can vary.

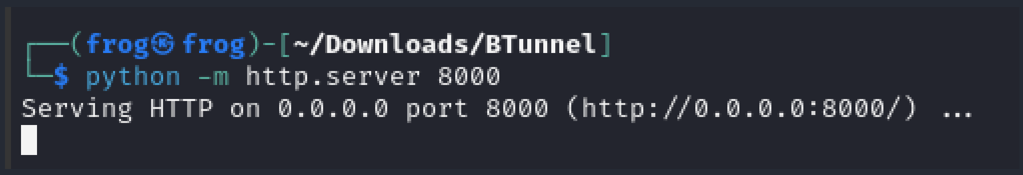
```
./btunnel http -p 8000 --key <API-KEY>
```

We can clearly see in the below screenshot that our local port is being forwarded to Btunnels. So, we have to make sure that a server/service is running on localhost.



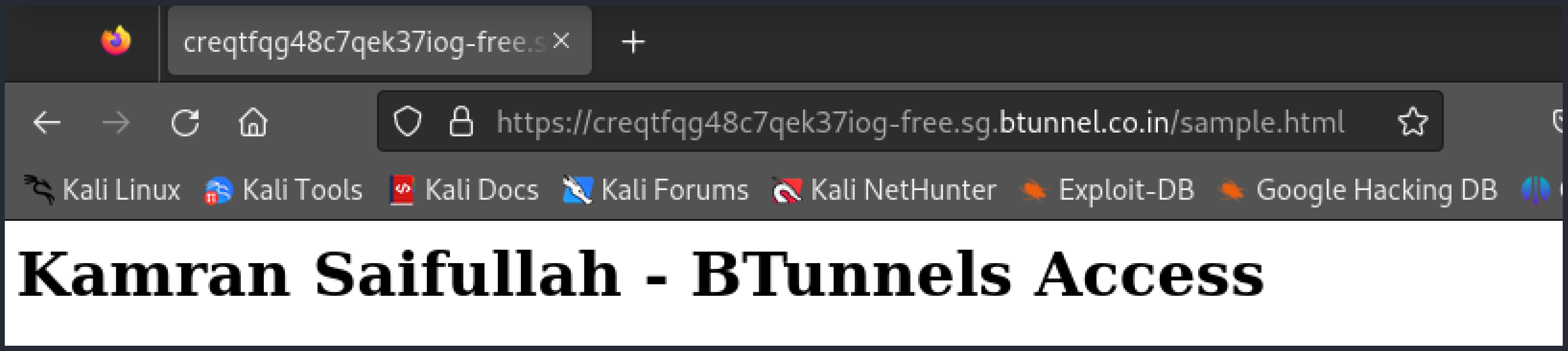
```
Name: → Kamran Saifullah
Email: → kamransaifullah786@gmail.com
TimeOut: → Sun Sep  8 16:03:44 UTC 2024
Web Monitoring: → http://localhost:7140

 http  https://creqtfqg48c7qek37iog-free.sg.btunnel.co.in → http://localhost:8000 Sun Sep  8 14:03:43 UTC 2024
```

I have created a simple file and started a `Python Server` on the localhost hosting one `sample.html` file.



```
┌──(frog㉿frog)-[~/Downloads/BTunnel]
└─$ python -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
█
```

Using the same link provided to us, we can access the file over the `Tunnel`.


creqtfqg48c7qek37iog-free.s ×
+
https://creqtfqg48c7qek37iog-free.sg.btunnel.co.in/sample.html
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB

Kamran Saifullah - BTunnels Access

3. TCP

This is one of the crazy parts where it does not looks malicious but what can happen here is?

We can redirect the network traffic and create backdoors and also port forward the RDP/SSH/FTP etc. connection over the internet and connect back to them using the `BTunnels`.

While testing this part, i received an error of not being a pro user but the command is so simple.

```
./btunnel tcp -p 22 --key <API-KEY>
```

Similarly, we can forward the RDP by running the following command.

```
./btunnel tcp -p 3389 --key <API-KEY>
```

and we can keep on going and can forward many other forts as required.

4. Domain

This command allows to persist the domains/subdomains created for the BTunnel for the current user. More information can be found on this at the below link.

https://www.btunnel.in/docs/commands/btunnel_domain

Conclusion

As simple as these tools are and the level of ease they bring for the developers (technical/non-technical). This can fairly be used by the threat actors to exfiltrate the data and not just that but also for C2 communications as well as Phishing/Spear Phishing. As most of these tools are not malicious by default/behavior wise, these can easily be brought onto the compromised machines, where when executed, the created tunnel can be used for malicious purposes.

It is equally important to keep an eye on these kind of ttols and to ensure these are blocked by default by having `Application Whitelisting` policies or else at-least the `Tunnels` links are monitored.

This only has 1 `Network IOC` and i.e. as below.

- https://*.btunnel.co.in

However, its recommended to add the following into monitoring as well.

- https://*.btunnel.in

Including the main domaind and subdomains.

Additional

One more thing which i have noticed is that anyone can create an account on the website without the need to email verification or 2FA/MFA neither the accounts are verified. Thus, opening it for a great opportunity for the threat actors to use the registration for bulk registrations and taking out bulk APIs which can be used for malicious purposes.

Also, one thing to note here is, this tool can not only be used to exfiltrate the data but also as a way in i.e. Phishing Campaigns as well as hosting binaries/tools/malwares and downloading them onto the compromised machines while the information of where it is connecting from remains within the orgnizations. Thus, giving away very less information of who the threat actor really is.

Tags: Research

Categories: Research

Updated: September 8, 2024

Previous Next

FOLLOW: FEED