#ZTW25

THREATLOCKER®

ZERO TRUST WORLD '25

Obfuscating Your C2

Nick Cottrell

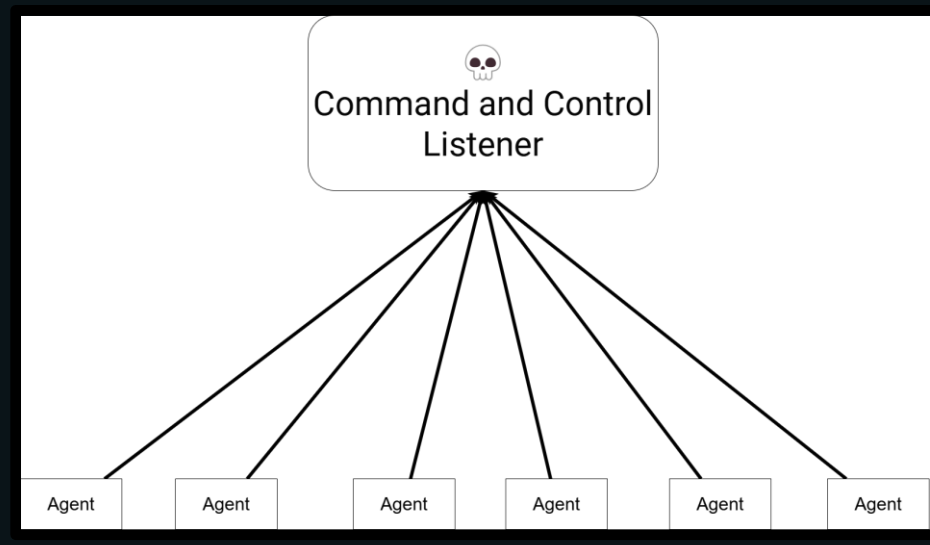
Threat Intelligence, ThreatLocker

What we will go over

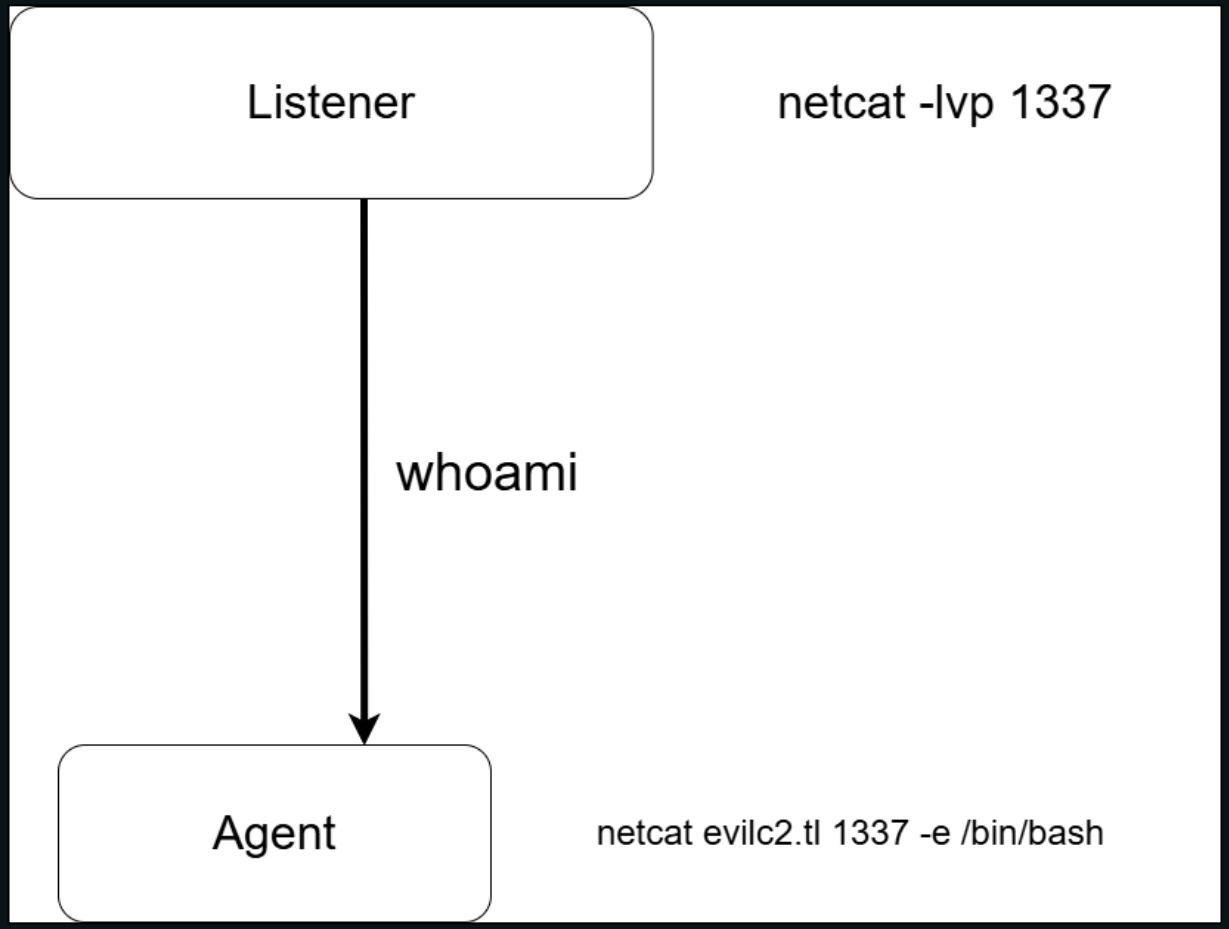
- What is a command and Control (C2)
  - Communication between the C2 and the endpoint
  - Problem: This is too obvious
- Communicating in Pig Latin
  - This is too suspicious
- Just act natural
- The ultimate reverse shell: The beacon
- I just don’t have time to write my own C2
- Writing your own C2!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

What is a Command and Control (C2)

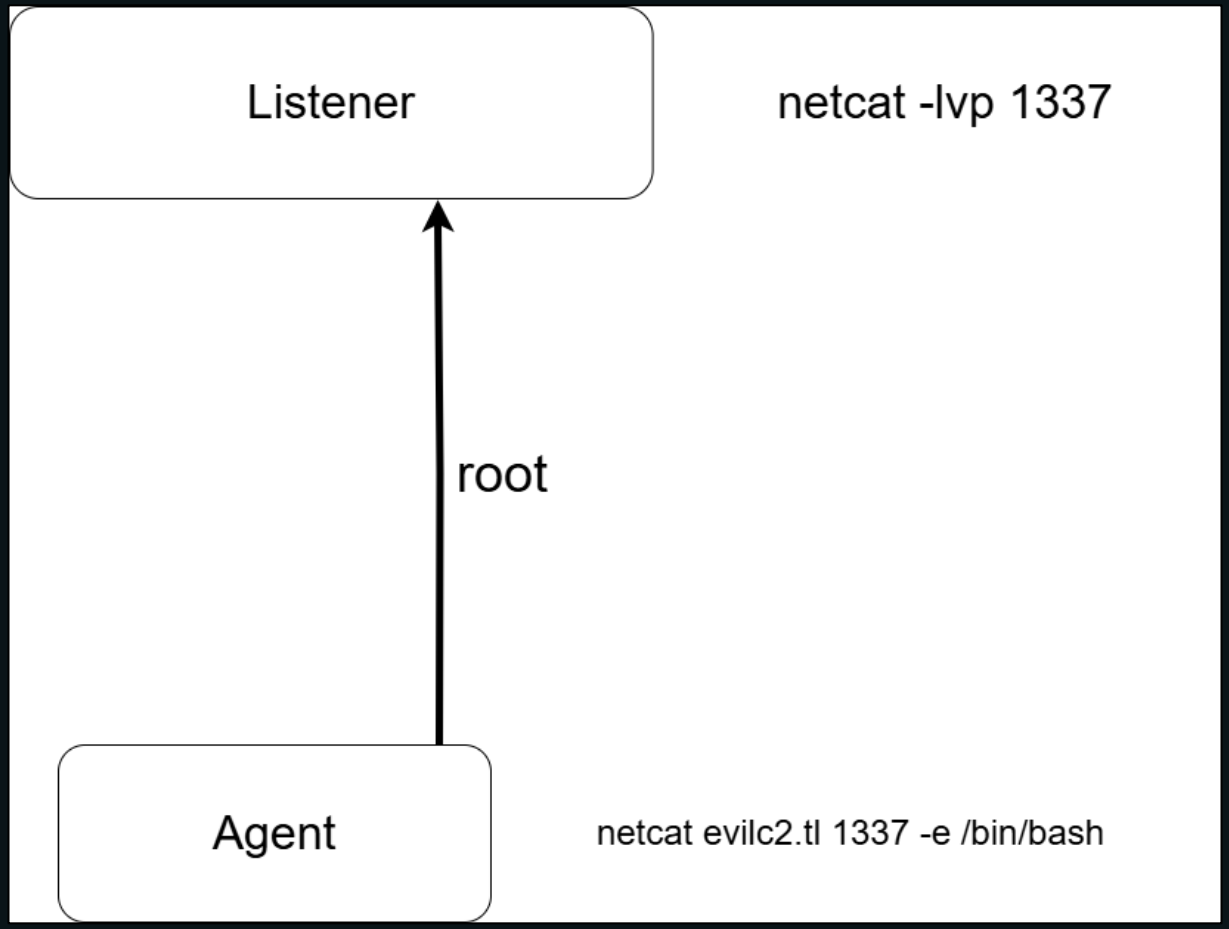
- Sends commands to an agent to act on and listens for responses
- Contains a listener and at least one agent
- Typically, agents talk back to listener
  - Example: netcat reverse shell



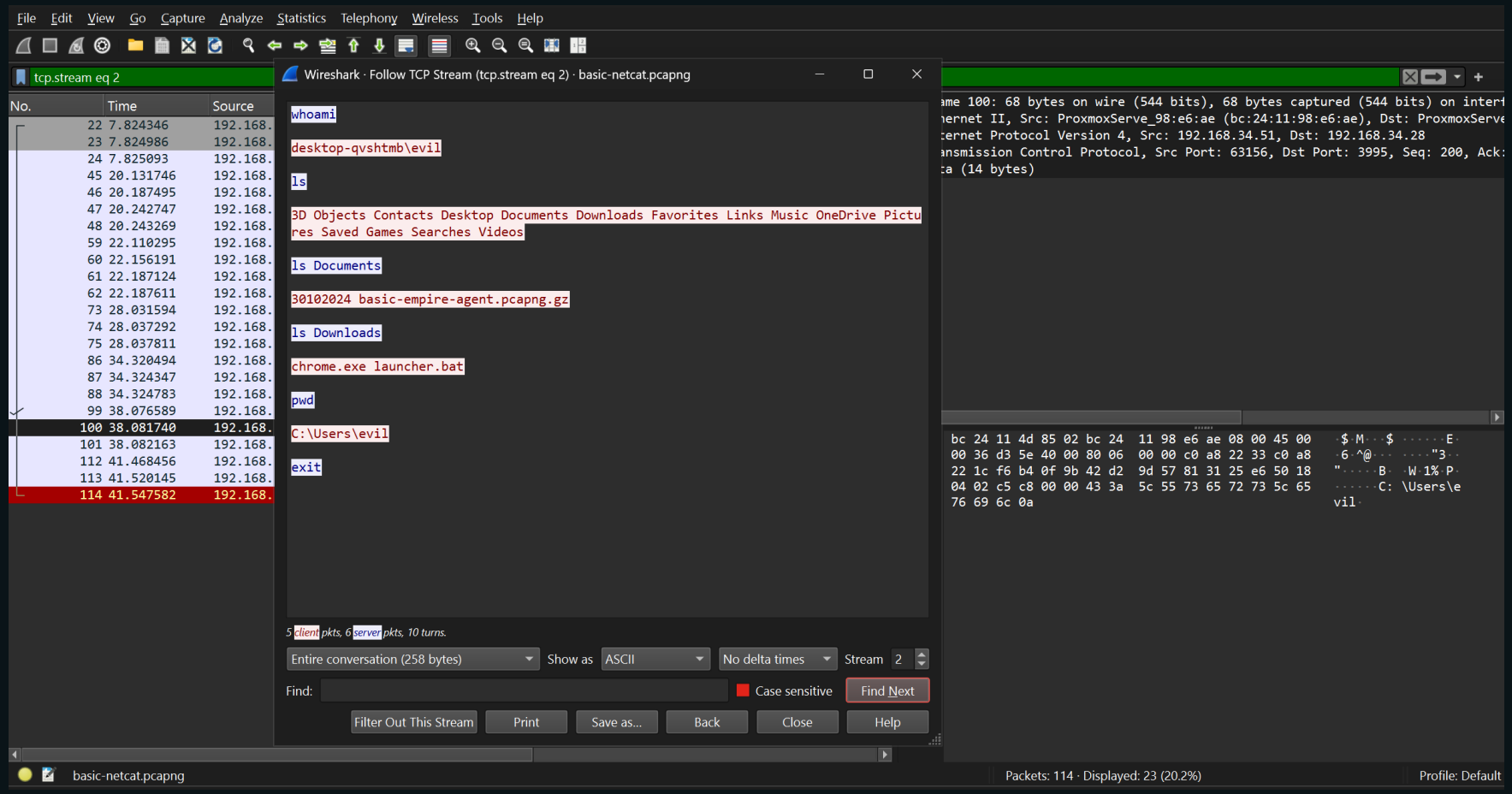
Communication between the C2 and the endpoint



Communication between the C2 and the endpoint



Problem: This is too obvious

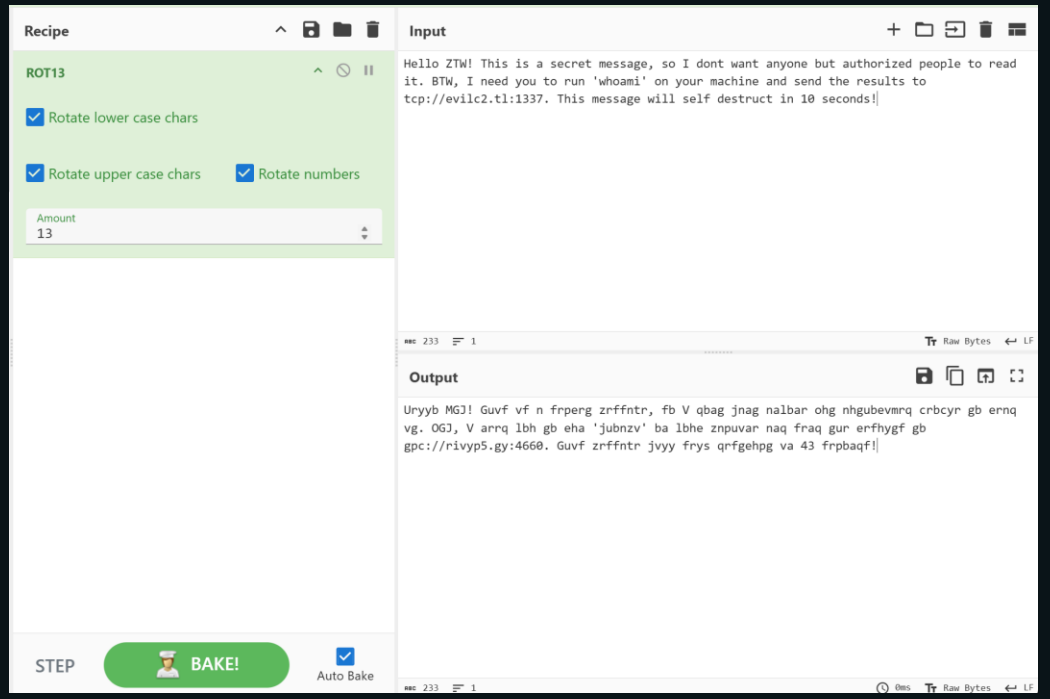


ZTW25

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

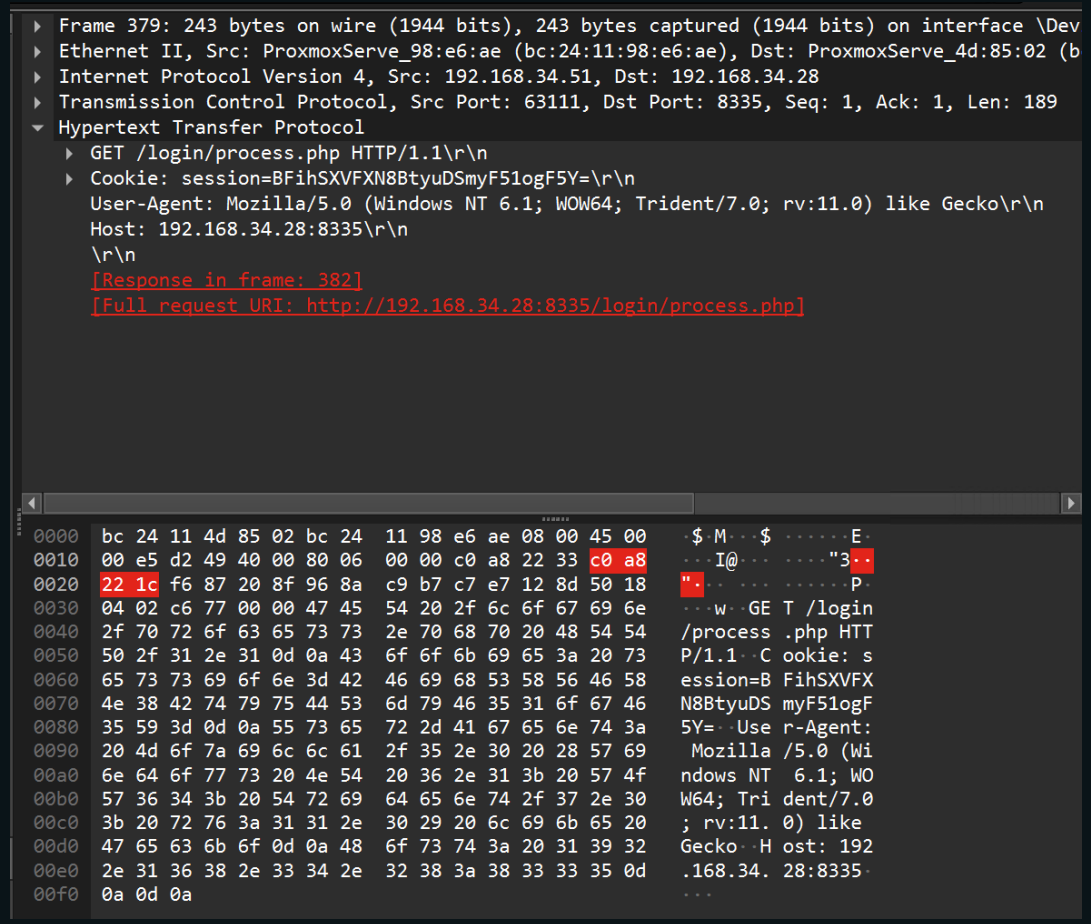
- Encoding
  - Hex
  - Octal
  - binary
  - Base64
  - unicode

Communicating in pig latin

- RSA
- RC4
- AES

- HTTP -> HTTPS
- DNS -> DNS Over HTTPS (DoH)

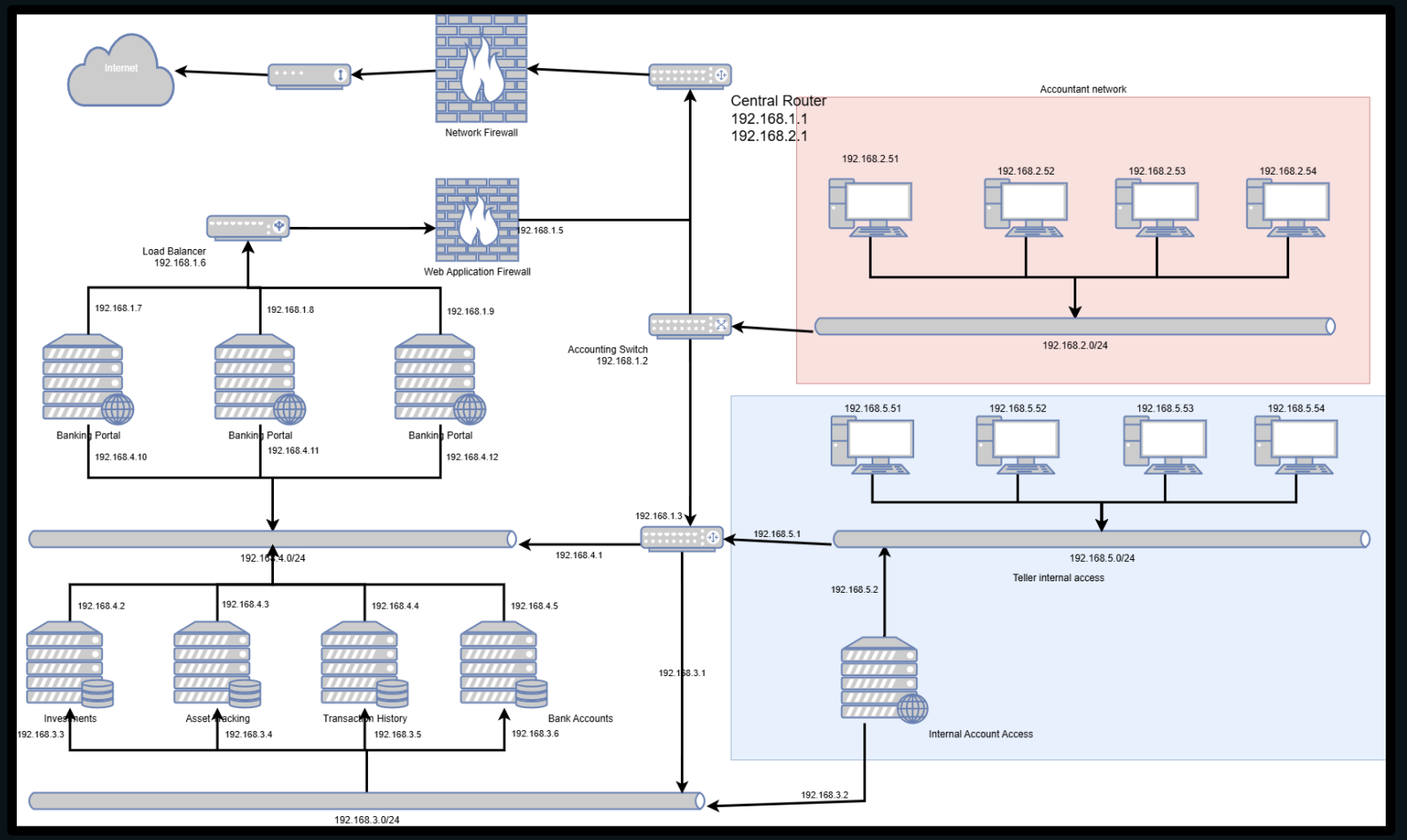
This is too suspicious...



ZTW25

Just act natural

Just act natural: Know your target



ZTW25

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

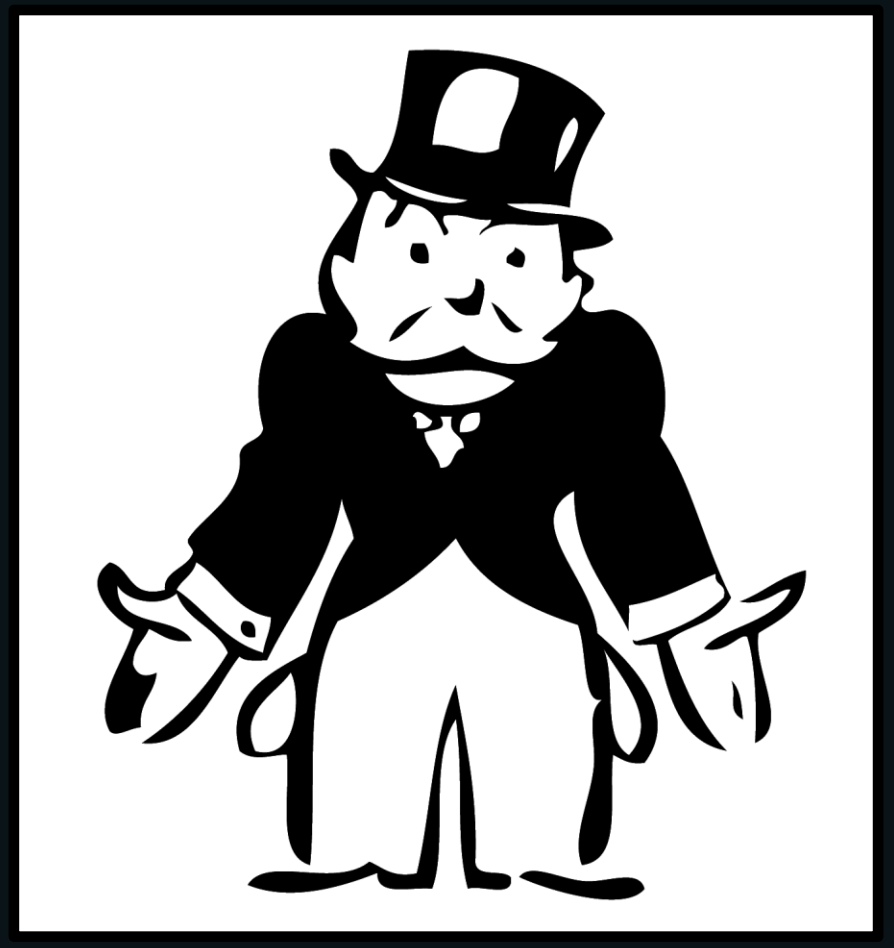
- Checks in periodically with listener
- Waits for commands to be received
- Can pivot through a middleman
- Checks for new tasks from listener
- Variable check-in rate

Beacons being sneaky

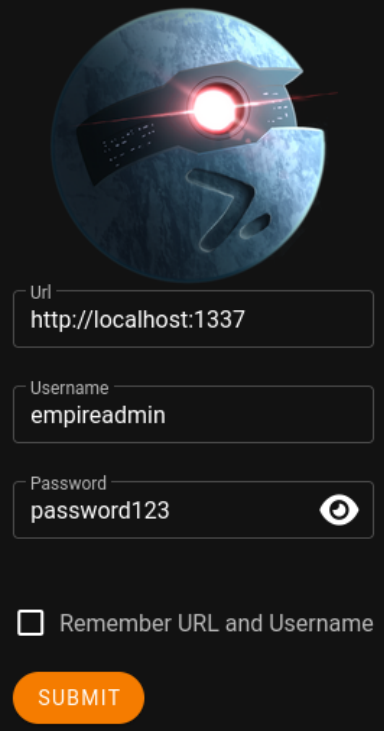
- Beacons will check in once per sleep interval
- Jitter provides random fluctuations in sleep interval
  - Counters patterns in check in time

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

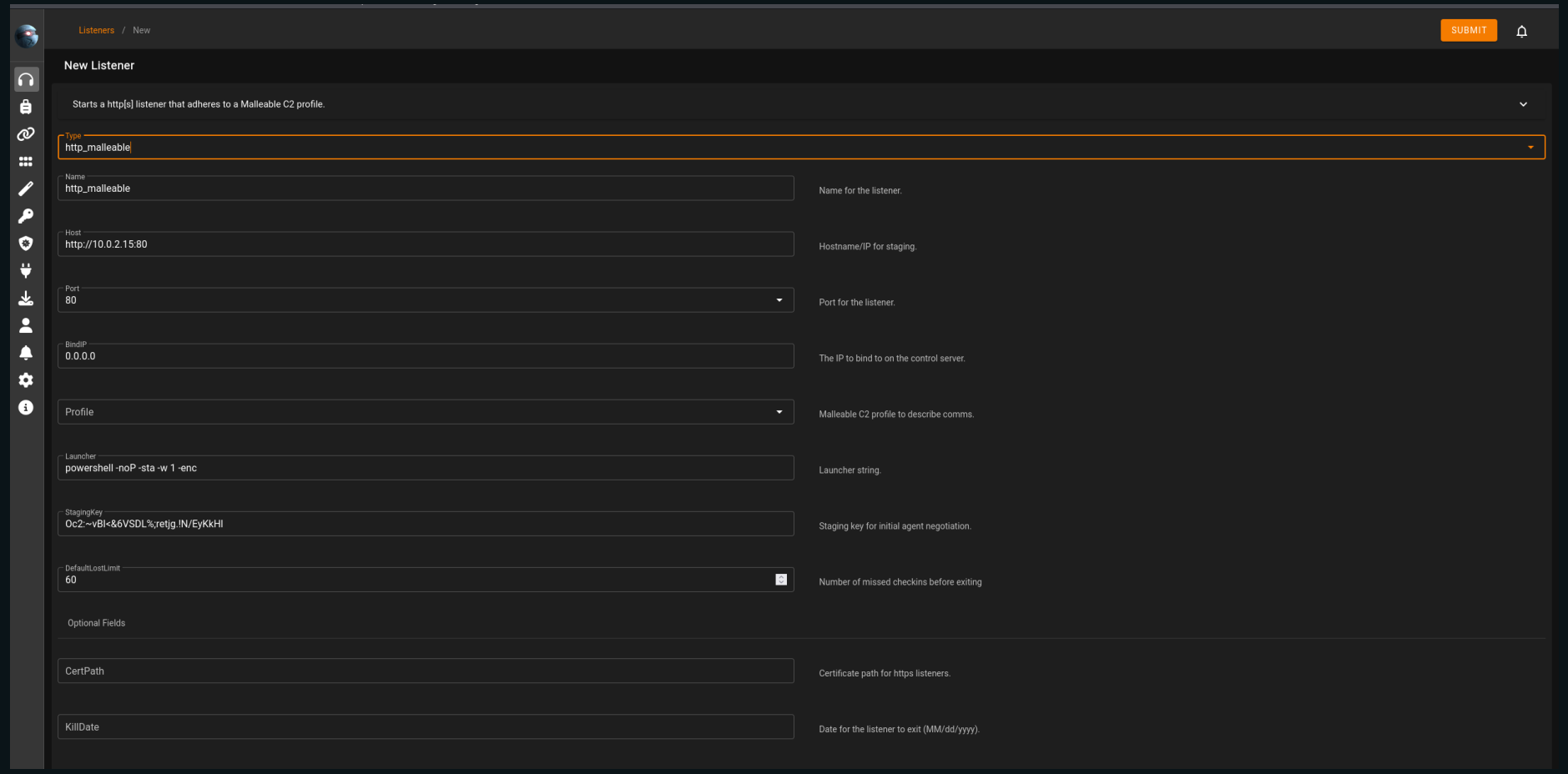
I just don’t have time to write my own C2



Writing your own C2! (profile)

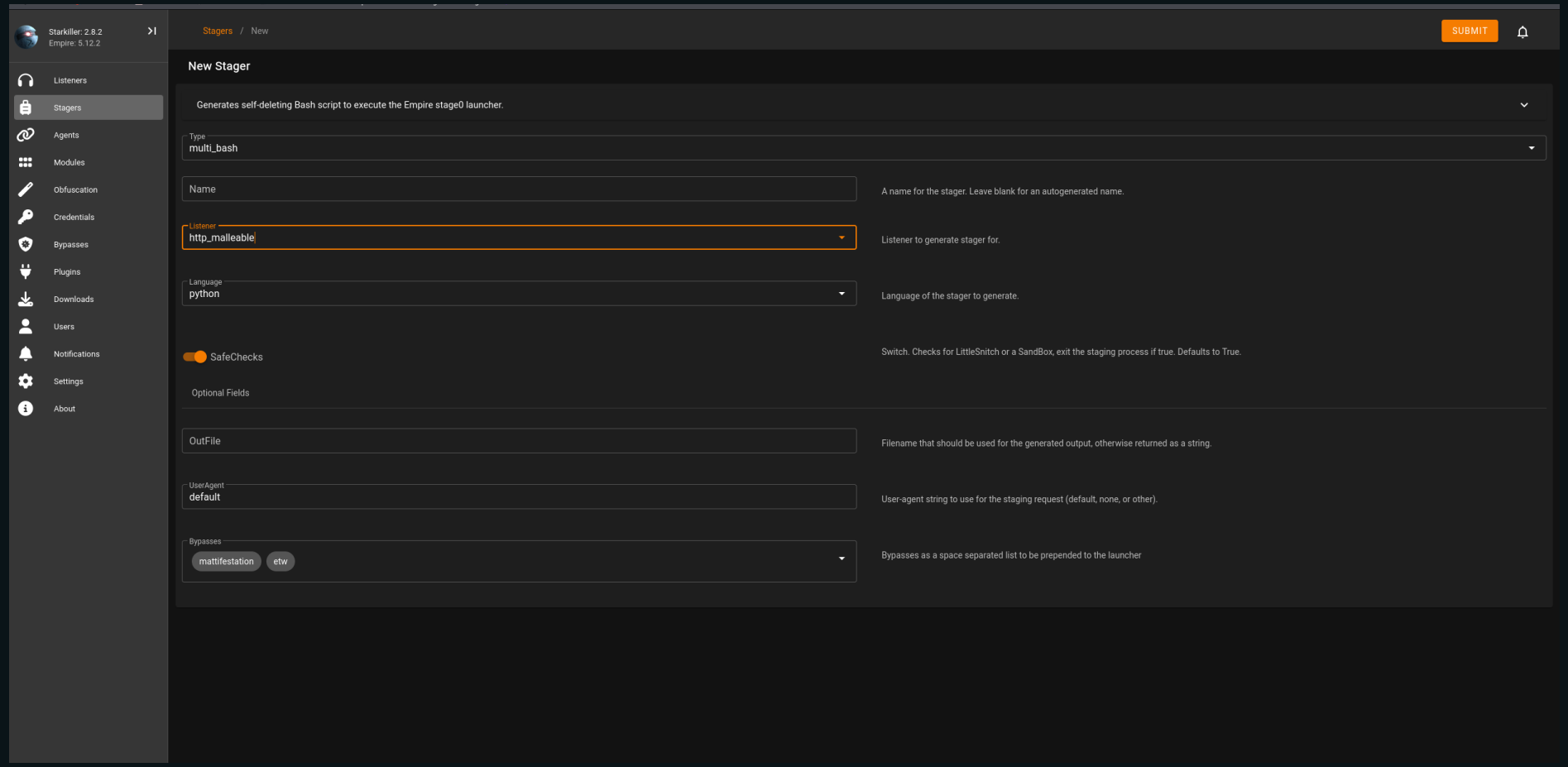


Writing your own C2! (profile)



ZTW25

Writing your own C2! (profile)



Writing your own C2! (profile)

```
# 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
```

Writing your own C2! (profile)

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

Writing your own C2! (profile)

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

Writing your own C2! (profile)

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 tcp header
Verb	Option between get or post
sample_name	Name to describe profile in IoC report

THREATLOCKER®

ZTW25

ZERO TRUST WORLD

The end

Go home