Turning the table:

Honeypots 'Flawed Logic' and Counter-Intelligence

Sheila A. Berta (@UnaPibaGeek)

DREAMLAB
TECHNOLOGIES

WHO AM I

- Sheila A. Berta - (@UnaPibaGeek)
- Security Researcher (+15 years)
- Head of Research at Dreamlab Technologies 🇨🇭
- Review Board member at Black Hat USA
- Speaker at Black Hat, DefCon, HITB, Eko and more

DREAMLAB TECHNOLOGIES

AGENDA

01 Honeypots Inner-workings

02 Honeypots “Flawed Logic” issues

03 Statistics & Counter-Intelligence

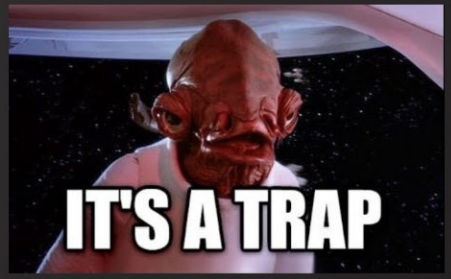
01

HONEYPOTS INNER-WORKINGS

QUICK OVERVIEW OF HOW HONEYPOTS WORK

HONEYPOTS OBJECTIVES

- Mimic real systems to attract attackers
- Allow defenders to study attackers' TTP
- Gather threat intelligence, statistics, improve security



ARCHITECTURE OVERVIEW

Attacker

Honeypot mimicking a real system
(E.g: database, SMB service, web server...)

Log processing, database and dashboard
(E.g: elastic stack)

Defender

REAL VS EMULATION

REAL SERVICES

- Pros: Full capabilities, quite difficult to identify
- Cons: High effort, hard maintenance, difficult attack logging

EMULATED SERVICES

- Pros: Low effort, easy maintenance, ready-to-use
- Cons: Limited capabilities, sometimes poorly written, easier to identify

LEVELS OF INTERACTION

- LOW INTERACTION
- MEDIUM INTERACTION
- HIGH INTERACTION

02

HONEYPOTS "FLAWED LOGIC" ISSUES

DETECTING HONEYPOTS
VIA 'FLAWED LOGIC' ISSUES

PRIOR RESEARCH

HONEYPOTS DETECTION BASED ON:

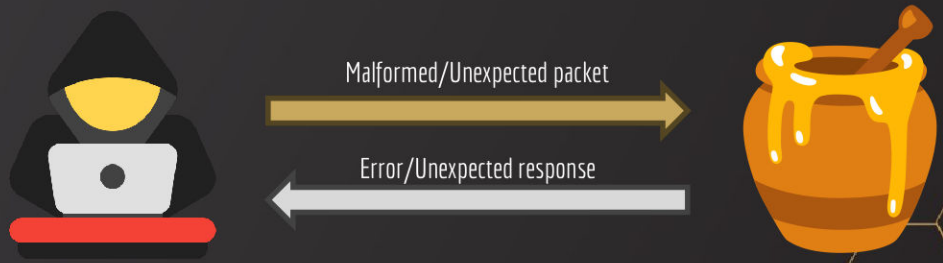
- Default service banners (E.g.: 220 mailrelay.local ESMTP Exim 4.81 #1 Thu, 29 Jul 2010 05:13:48 -0700)
- Default response to commands (E.g.: cat /etc/passwd shows user “Phil California”)
- Certificates configuration (E.g.: Organization issuer/subject: “dionaea.carnivore.it”)
- Suspicious number of open ports in the host (E.g.: All ports are open)
- Suspicious hosting provider (E.g.: ICS honeypots on Cloud hosting)

RESEARCH MOTIVATION

HONEYPOTS DETECTION BASED ON:

- Flawed logic in their packet-handling functions (errors/unexpected responses)
- Minimal interaction with the honeypot (1-2 network packets)

Bypass honeypots detection countermeasures!



COMMON SERVICES

DIONAEA FTP

REQUEST:

"/n" character as a password

RESPONSE:

"500 Syntax error: PASS requires an argument"

REAL SERVICE:

```
🚀 ~ ftp [redacted]
Connected to [redacted].
220 ProFTPD 1.3.4a Server (Debian) [redacted]
Name ([redacted]):
331 Password required for shei
Password:
530 Login incorrect.
ftp: Login failed.
ftp> bye
221 Goodbye.
```

HONEYPOT:

```
🚀 ~ ftp [redacted]
Connected to [redacted].
220 DiskStation FTP server ready.
Name ([redacted]):
331 Password required for shei.
Password:
500 Syntax error: PASS requires an argument
ftp: Login failed.
ftp> bye
503 Incorrect sequence of commands: PASS required after USER
```

COWRIE SSH

REQUEST:

"SSH-1337-OpenSSH_9.0\r\n"

RESPONSE:

"Protocol major versions differs" or
"bad version 1337"

REAL SERVICE:

```
[DBG] [cowrie-honeypot-detect] Dumped Network response for [redacted]:22

00000000  53 53 48 2d 32 2e 30 2d  4f 70 65 6e 53 53 48 5f  |SSH-2.0-OpenSSH_|
00000010  37 2e 39 70 31 20 44 65  62 69 61 6e 2d 31 30 2b  |7.9p1 Debian-10+|
00000020  64 65 62 31 30 75 33 0d  0a 50 72 6f 74 6f 63 6f  |deb10u3..Protoco|
00000030  6c 20 6d 69 73 6d 61 74  63 68 2e 0a              |l mismatch..|
```

HONEYPOT:

```
[DBG] [ssh-honeypot-detection] Dumped Network response for [redacted]:22

00000000  53 53 48 2d 32 2e 30 2d  4f 70 65 6e 53 53 48 5f  |SSH-2.0-OpenSSH_|
00000010  36 2e 30 70 31 20 44 65  62 69 61 6e 2d 34 2b 64  |6.0p1 Debian-4+d|
00000020  65 62 37 75 32 0d 0a 00  00 00 24 06 01 00 00 00  |eb7u2.....$.....|
00000030  08 00 00 00 10 62 61 64  20 76 65 72 73 69 6f 6e  |.....bad version|
00000040  20 31 33 33 37 00 00 00  00 f3 1a f4 86 37 9c     | 1337........7.|
```

MAILONEY SMTP

REQUEST:

"HELP" or "NON-EXISTENT"

RESPONSE:

"502 Error: command "HELP" not implemented"

REAL SERVICE:

```
~ telnet 127.0.0.1 25
Trying 127.0.0.1...
Connected to 127.0.0.1.
Escape character is '^]'.
220 example.org ESMTP Exim 4.93 Ubuntu Mon, 28 Aug 2023 19:43:00 +0000
HELP
214-Commands supported:
214 AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
AAAA
500 unrecognized command
```

HONEYPOT:

```
~ telnet [redacted] 25
Trying [redacted]...
Connected to [redacted].
Escape character is '^]'.
220 mailrelay.local ESMTP Exim 4.81 #1 Thu, 29 Jul 2010 05:13:48 -0700
HELP
502 Error: command "HELP" not implemented
AAAA
502 Error: command "AAAA" not implemented
```

DIONAEA HTTP

REQUEST:

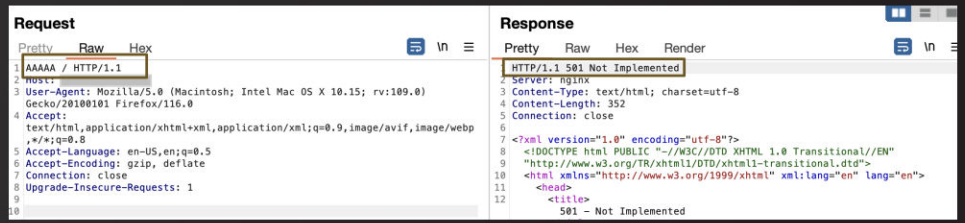
"AAAA / HTTP/1.1"

RESPONSE:

"501 - Not Implemented"

REAL SERVICE:

HONEYPOT:



SNARE HTTP

REQUEST:

"GET / HTTP/1337"

RESPONSE:

"Bad status line 'Expected dot'"

REAL SERVICE:

Request

Pretty Raw Hex \n

```
1 GET / HTTP/1337
2 Host:
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0)
  Gecko/20100101 Firefox/116.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp
  ,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 505 HTTP Version Not Supported
2 Server: nginx/1.14.0 (Ubuntu)
3 Date: Mon, 28 Aug 2023 12:28:42 GMT
4 Content-Type: text/html
5 Content-Length: 212
6 Connection: close
7
8 <html>
9   <head>
      <title>
        505 HTTP Version Not Supported
      </title>
```

HONEYPOT:

Request

Pretty Raw Hex \n

```
1 GET / HTTP/1337
2 Host:
3 User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
  rv:109.0) Gecko/20100101 Firefox/116.0
4 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
  mage/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.0 400 Bad Request
2 Content-Type: text/plain; charset=utf-8
3 Content-Length: 30
4 Date: Mon, 28 Aug 2023 12:20:55 GMT
5 Server: Python/3.10 aiohttp/3.8.3
6
7 Bad status line 'Expected dot'
```

DIONAEA SMB

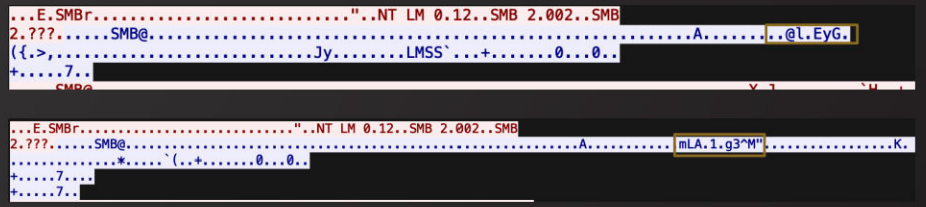
REQUEST:

Starts SMB negotiation

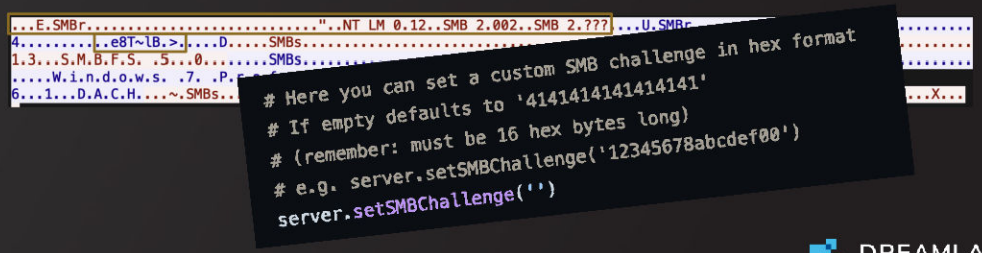
RESPONSE:

“\x65\x38\x54\x7e\x6c\x42” (e8T~lB)

REAL SERVICE:



HONEYPOT:



DATABASES

DIONAEA MYSQL

REQUEST:

Starts MYSQL connection (Protocol 'Hello')

RESPONSE:

"5.7.16 (...) aaaaaaaa..."

REAL SERVICE:

```
[DBG] [mysql-honeypot-detect] Dumped Network response for [redacted]3306

00000000  49 00 00 00 0a 38 2e 31  2e 30 00 0b 00 00 00 0f  |I....8.1.0......|
00000010  15 7d 55 2d 01 22 25 00  ff ff ff 02 00 ff df 15  |.}U-."%.........|
00000020  00 00 00 00 00 00 00 00  00 00 72 07 64 5b 21 3e  |..........r.d[!>|
00000030  14 68 57 34 3b 74 00 63  61 63 68 69 6e 67 5f 73  |.hW4;t.caching_s|
00000040  68 61 32 5f 70 61 73 73  77 6f 72 64 00           |ha2_password.|
```

HONEYPOT:

```
[DBG] [mysql-honeypot-detect] Dumped Network response for [redacted]:3306

00000000  34 00 00 00 0a 35 2e 37  2e 31 36 00 00 00 12 67  |4....5.7.16....g|
00000010  61 61 61 61 61 61 61 61  00 2c a2 21 02 00 00 00  |aaaaaaaa.,.!....|
00000020  00 00 00 00 00 00 00 00  00 00 00 20 20 20 20 20  |........... .....|
00000030  20 20 20 20 20 20 20 00                           |       .|
```

DIONAEA MONGODB

REQUEST:

Sends 'BuildInfo' command

RESPONSE:

Version is not present

REAL SERVICE:

```
[DBG] [mongodb-honeypot-detection] Dumped Network response for [redacted]27017

00000000  93 05 00 00 3c 9f 06 00  3c 30 00 00 01 00 00 00  |....<...<0......|
00000010  08 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000020  01 00 00 00 6f 05 00 00  02 76 65 72 73 69 6f 6e  |....o....version|
00000030  00 07 00 00 00 34 2e 30  2e 32 33 00 02 67 69 74  |.....4.0.23..git|
00000040  56 65 72 73 69 6f 6e 00  29 00 00 00 30 37 63 36  |Version.)...07c6|
00000050  36 31 31 62 33 38 64 32  61 61 63 62 64 62 31 38  |611b38d2aacbdb18|
00000060  34 36 62 36 38 38 64 62  37 30 62 33 32 37 33 31  |46b688db70b32731|
00000070  37 30 66 62 00 04 6d 6f  64 75 6c 65 73 00 05 00  |70fb..modules...|
```

HONEYPOT:

```
[DBG] [mongodb-honeypot-detection] Dumped Network response for [redacted]:27017

00000000  c9 00 00 00 00 00 00 00  3c 30 00 00 01 00 00 00  |........<0......|
00000010  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000020  01 00 00 00 a5 00 00 00  08 69 73 6d 61 73 74 65  |.........ismaste|
00000030  72 00 01 10 6d 61 78 42  73 6f 6e 4f 62 6a 65 63  |r...maxBsonObjec|
00000040  74 53 69 7a 65 00 00 00  00 01 10 6d 61 78 4d 65  |tSize......maxMe|
00000050  73 73 61 67 65 53 69 7a  65 42 79 74 65 73 00 00  |ssageSizeBytes..|
00000060  6c dc 02 10 6d 61 78 57  72 69 74 65 42 61 74 63  |l...maxWriteBatc|
00000070  68 53 69 7a 65 00 e8 03  00 00 09 6c 6f 63 61 6c  |hSize......local|
00000080  54 69 6d 65 00 7e b9 35  47 8b 01 00 00 10 6d 61  |Time.~.5G.....ma|
00000090  78 57 69 72 65 56 65 72  73 69 6f 6e 00 05 00 00  |xWireVersion....|
000000a0  00 10 6d 69 6e 57 69 72  65 56 65 72 73 69 6f 6e  |..minWireVersion|
000000b0  00 00 00 00 00 08 72 65  61 64 4f 6e 6c 79 00 00  |......readOnly..|
000000c0  10 6f 6b 00 01 00 00 00  00                       |.ok......|
```


DREAMLAB TECHNOLOGIES

ELASTICPOT

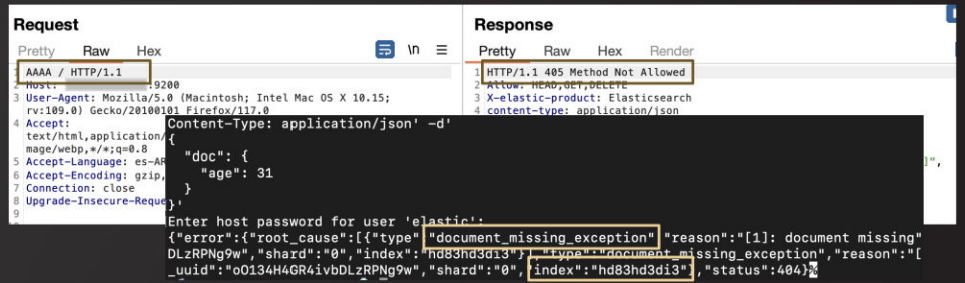
REQUEST:

"AAAA / HTTP/1.1" or
"GET /_cluster/settings" or
Update a document

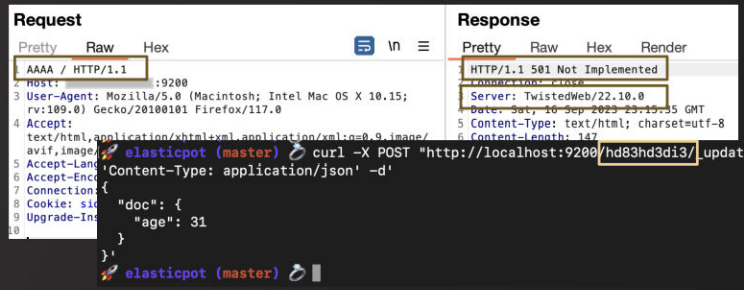
RESPONSE:

"501 - Huh?" or
"index_not_found" or
"OK"

REAL SERVICE:



HONEYPOT:



DREAMLAB TECHNOLOGIES

REDIS HONEYPOT

REQUEST:

"QUIT" or "NON-EXISTENT"

RESPONSE:

"ERR unknown command `QUIT`, with args beginning with:)"

REAL SERVICE:

```
🚀 ~ nc -vv 127.0.0.1 6379
Connection to 127.0.0.1 port 6379 [tcp/*] succeeded!
NONEXISTENT
-ERR unknown command 'NONEXISTENT', with args beginning with:
QUIT
+OK
🚀 ~
```

HONEYPOT:

```
🚀 ~ nc -vv 138.68.179.61 6379
Connection to 138.68.179.61 port 6379 [tcp/*] succeeded!
NONEXISTENT
-ERR unknown command `NONEXISTENT`, with args beginning with:
QUIT
-ERR unknown command `QUIT`, with args beginning with:
^C
🔥 ~
```

APPLICATIONS

CISCO ASA

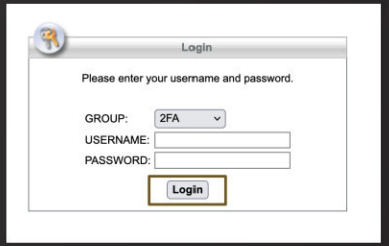
REQUEST:

"GET /+CSCOE+/logon.html HTTP/1.1"

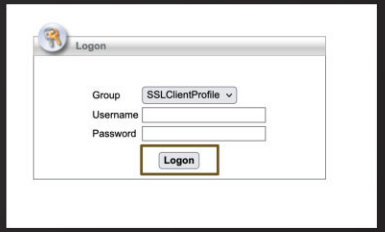
RESPONSE:

Shows "Logon" instead of "Login"

REAL SERVICE:



HONEYPOT:



CITRIX HONEYPOT

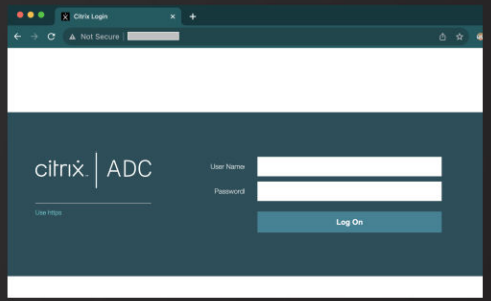
REQUEST:

"GET / HTTP/1.1" (normal)

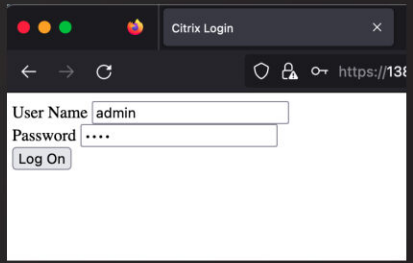
RESPONSE:

Shows "Citrix Login" but no real content

REAL SERVICE:



HONEYPOT:



ICS

CONPOT

REQUEST:

Starts Siemens negotiation (first packet)

RESPONSE:

"\x03\x00\x00... \xc2\x02\x00\x00"

REAL SERVICE:


```
{
  "data": "\u0003\u0000\u0000\u0016\u0011\ufffd\u0000\u0000\u0000\u0004\u0000\ufffd\u0002\u0001\u0000\
ufffd\u0002\u0001\u0002\ufffd\u0001\n",
  "hex": "0300001611e00000000400c1020100c2020102c0010a",
  "request": true
}
{
  "data": "\u0003\u0000\u0000\u0016\u0011\ufffd\u0000\u0000\u0000\u0004\u0000\ufffd\u0002\u0001\u0000\
ufffd\u0002\u0002\u0000\ufffd\u0001\n",
  "hex": "0300001611e00000000400c1020100c2020200c0010a",
  "request": true
}
```


HONEYPOT:


```
{
  "data": "\u0003\u0000\u0000\u0016\u0011\ufffd\u0000\u0000\u0000\u0004\u0000\ufffd\u0002\u0001\u0000\
ufffd\u0002\u0001\u0002\ufffd\u0001\n",
  "hex": "0300001611e00000000400c1020100c2020102c0010a",
  "request": true
}
{
  "data": "\u0003\u0000\u0000\u0013\u000c\ufffd\u0000\u0000\u0000\u0000\u0000\ufffd\u0002\u0000\u0000\
ufffd\u0002\u0000\u0000",
  "hex": "03000013ed00000000000c1020000c2020000",
  "response": true
}
```

OTHERS

DIONAEA MQTT

REQUEST:

"mosquitto_pub -V mqttv5... (...) "

RESPONSE:

"\x20\x02\x00\x00" (MQTT v3.11)

REAL SERVICE:

```
~ mosquitto_pub -d -p 1883 -V mqttv5 -t "test/topic" -m "1337"
Client null sending CONNECT
Client auto-7F20CBCD-03CD-51C4-7BFC-BAF8735B1BCE received CONNACK (0)
Client auto-7F20CBCD-03CD-51C4-7BFC-BAF8735B1BCE sending PUBLISH (d0, q0, r0, m1, 'test
/topic', ... (
Client auto-7F
~
```

```
{
  "data": "\u0010\u0010\u0000\u0004MQTT\u0005\u0002\u0000\u003c\u0003!\u0000\u0014\u0000\u0000",
  "hex": "101000044d515454050200 3c032100140000",
  "request": true
}
{
  "data": "  5\u0000\u0000\u0002\"\u0000\n\u0012\u0000)auto-DF8FAD8B-D257-3C51-C037-9D9B026ED3FB!\u0000\u0014",
  "hex": "203500003222000a12002961757 46f2d4446384644144384 22d443235372d33433531 2d433033372d3944394230323645
44334442210014",
  "response": true
}
```

HONEYPOT:

```
~ mosquitto_pub -d -h [redacted] -p 1883 -V mqttv5 -t "test/topic" -m "1337"
Client null sending CONNECT
Error: Unknown error.
~
```

```
{
  "data": "\u0010\u0010\u0000\u0004MQTT\u0005\u0002\u0000\u003c\u0003!\u0000\u0014\u0000\u0000",
  "hex": "101000044d515454050200 3c032100140000",
  "request": true
}
{
  "data": "  \u0002\u0000\u0000",
  "hex": "20020000",
  "response": true
}
```


DREAMLAB TECHNOLOGIES

AUTOMATION & DEMO

NUCLEI TEMPLATES

- One template per honeypot (+15)
- Ready-to-use with Nuclei

https://github.com/unapibageek

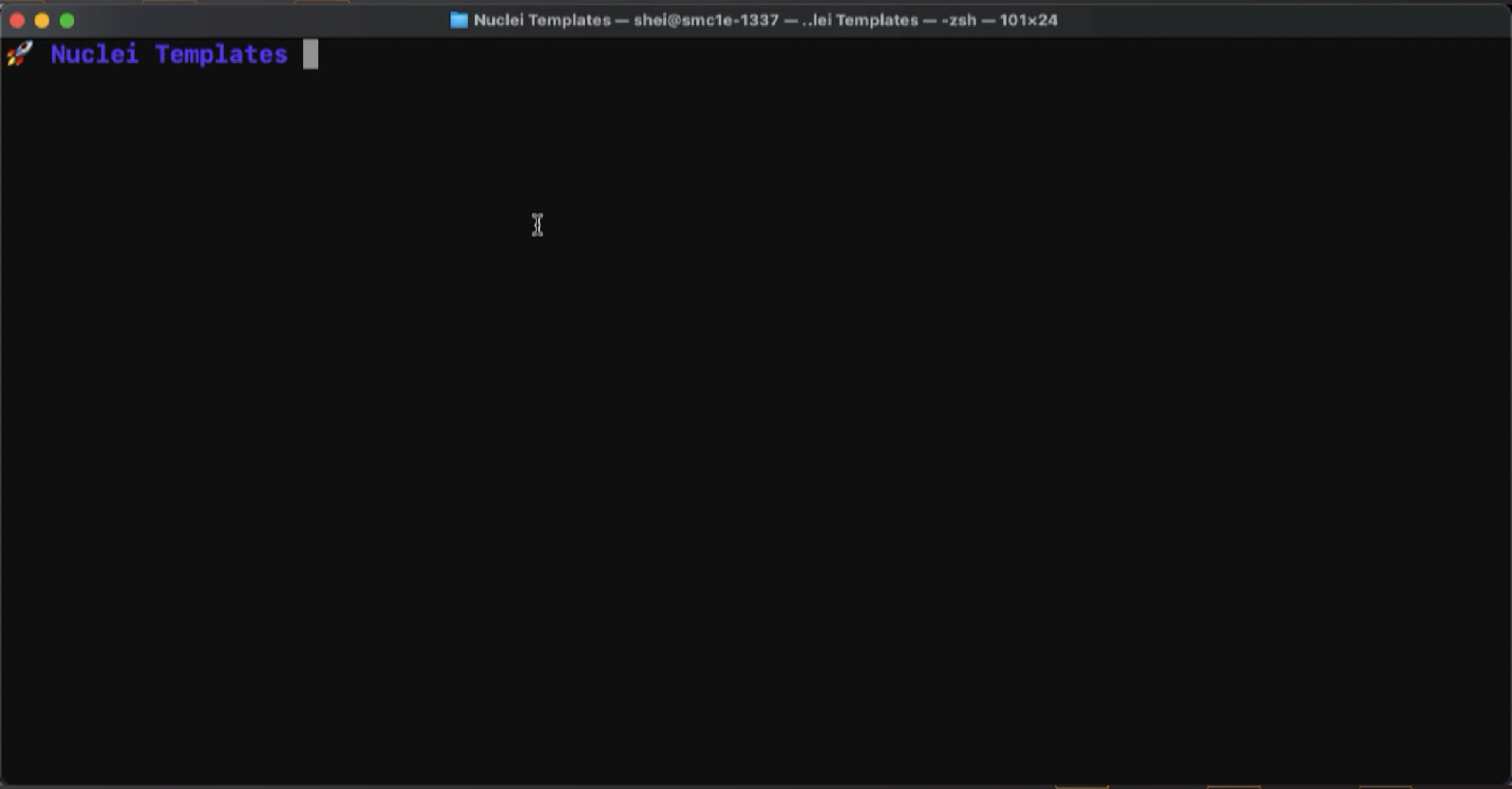
DEMO TIME!

```yaml
id: mqtt-honeypot-detection

info:
  name: Dionaea MQTT Honeypot Detection
  author: UnaPibaGeek
  severity: info
  description: |
    A Dionaea MQTT honeypot has been identified.
    The response to a MQTTv5 packet differs from real installations, signaling
  metadata:
    max-request: 2
    vendor: dionaea
    product: dionaea
  tags: dionaea,mqtt,honeypot

tcp:
  - host:
      - "{{Hostname}}"
      - "{{Host}}:1883"
    inputs:
      - data: "101000044d5154540502003c032100140000"
        type: hex

    read-size: 1024
    matchers:
      - type: binary
        binary:
          - "20020000"
```


Nuclei Templates — shei@smc1e-1337 — ..lei Templates — -zsh — 101×24
Nuclei Templates

03

STATISTICS & COUNTER-INTELLIGENCE

CYOBS
SEE THE CYBER

UNVEILING WHO IS BEHIND
HONEYPOTS NETWORKS

SWITZERLAND STATISTICS

+280

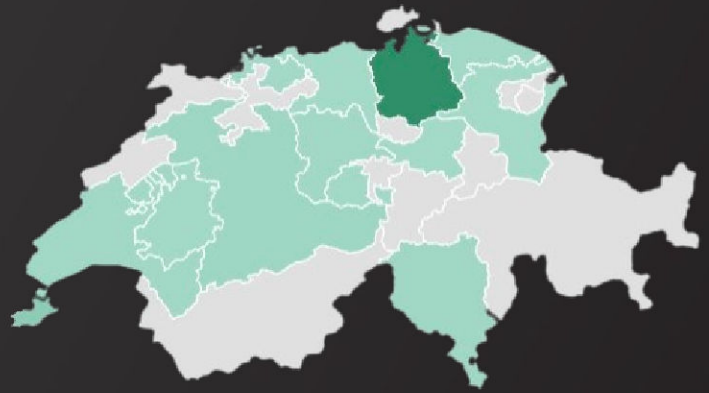
Honeypot Services

121

Unique Honeypots

14

Cantons



DREAMLAB TECHNOLOGIES

SWITZERLAND STATISTICS

TOP Locations

01 Zurich (79)

02 Geneve (15)

03 Bern (5)

04 Ticino (4)

05 Luzern (3)

TOP Organizations

01 Google Cloud (20)

02 Quickline AG (14)

03 Fiber (12)

04 Swisscom AG (8)

05 Green Floid LLC (5)

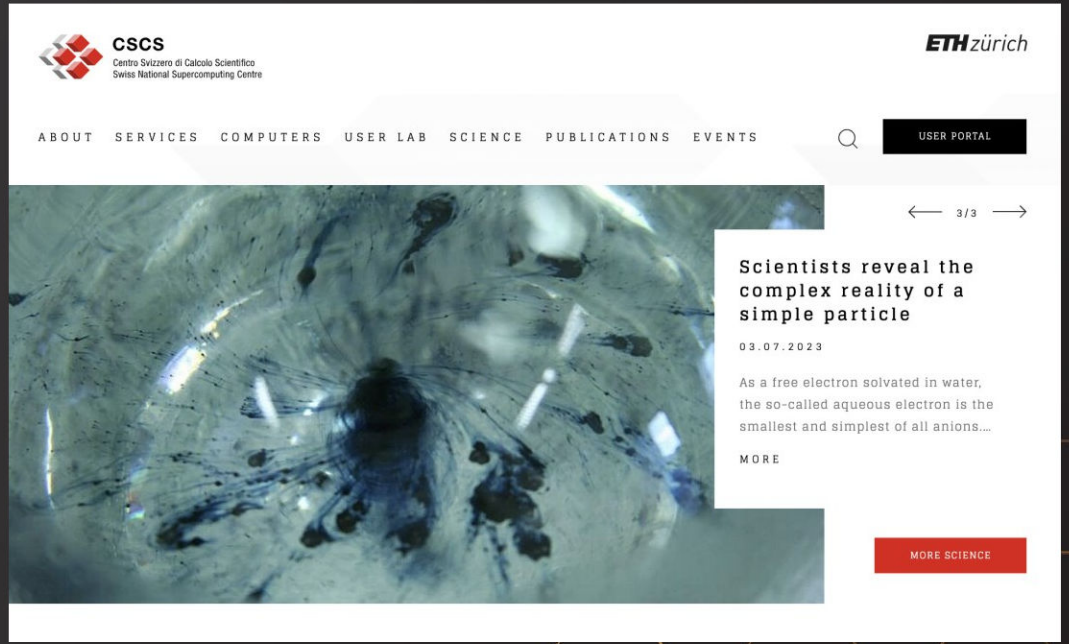
DREAMLAB TECHNOLOGIES

COUNTER-INTELLIGENCE EXAMPLE

CENTRO SVIZZERO
DI CALCOLO SCIENTIFICO

Lugano, Ticino, Switzerland

TPOT DETECTED!



DREAMLAB TECHNOLOGIES

CONCLUSIONS

CONCLUSIONS

- Customized honeypots can still be detected via ‘flawed logic’ issues
- Using real services as honeypots helps against detection techniques
- Do not run honeypots on your own network (too risky and allows intel)

THANK YOU!

Sheila A. Berta (@UnaPibaGeek)
sheila.berta@dreamlab.net

DREAMLAB
TECHNOLOGIES