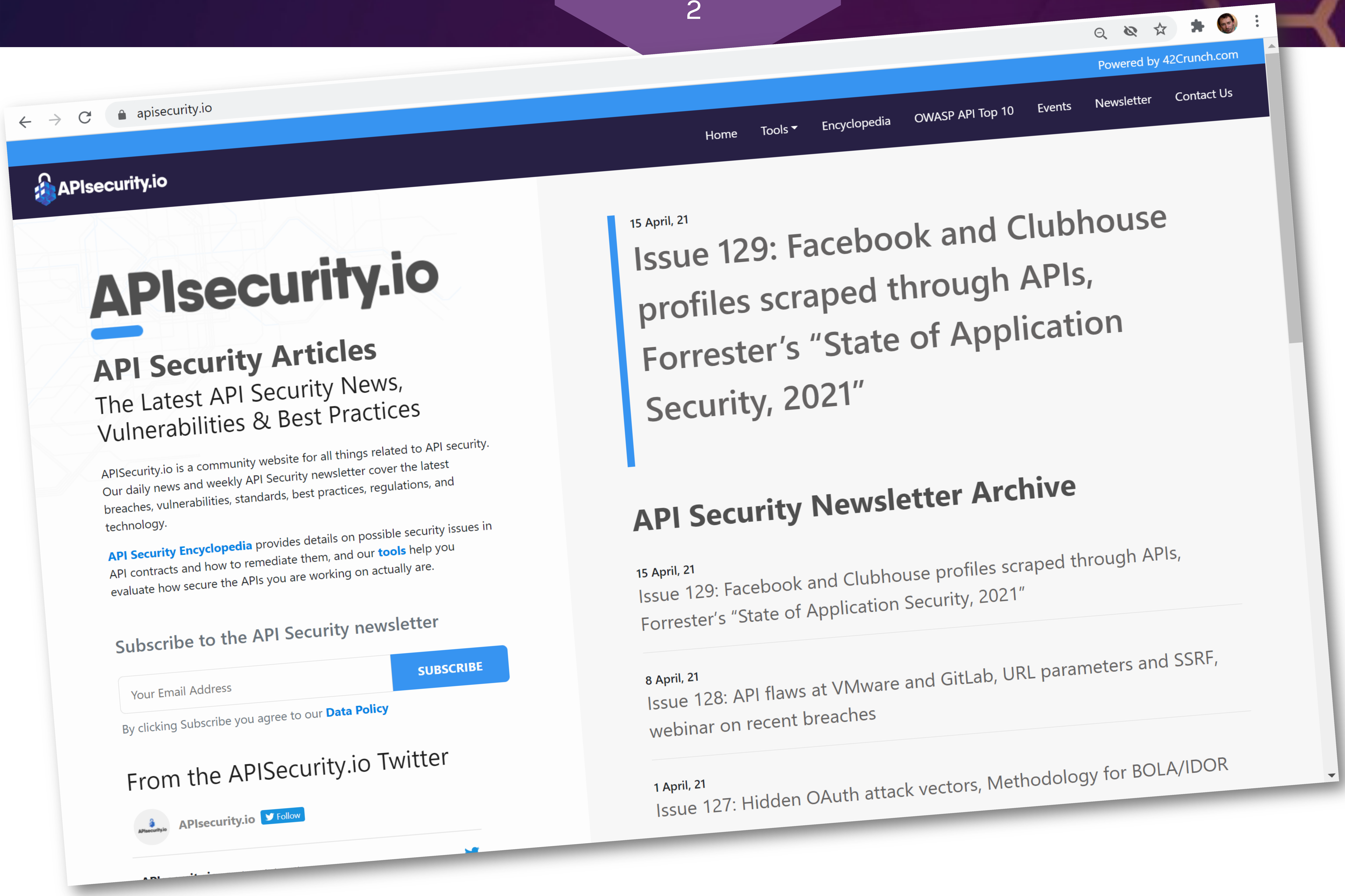
42crunch

Dissecting the Biggest API Breaches from Q1 2021

Dmitry Sotnikov, 42Crunch CPO, Curator of APIsecurity.io



apisecurity.io

Powered by 42Crunch.com

APIsecurity.io

API Security Articles

The Latest API Security News, Vulnerabilities & Best Practices

APISecurity.io is a community website for all things related to API security. Our daily news and weekly API Security newsletter cover the latest breaches, vulnerabilities, standards, best practices, regulations, and technology.

API Security Encyclopedia provides details on possible security issues in API contracts and how to remediate them, and our **tools** help you evaluate how secure the APIs you are working on actually are.

Subscribe to the API Security newsletter

Your Email Address

SUBSCRIBE

By clicking Subscribe you agree to our **Data Policy**

From the APISecurity.io Twitter

APIsecurity.io Follow

15 April, 21

Issue 129: Facebook and Clubhouse profiles scraped through APIs, Forrester’s “State of Application Security, 2021”

API Security Newsletter Archive

15 April, 21
Issue 129: Facebook and Clubhouse profiles scraped through APIs, Forrester’s “State of Application Security, 2021”

8 April, 21
Issue 128: API flaws at VMware and GitLab, URL parameters and SSRF, webinar on recent breaches

1 April, 21
Issue 127: Hidden OAuth attack vectors, Methodology for BOLA/IDOR

42CRUNCH API SECURITY PLATFORM

INTEGRATED

AUTOMATED

SCALABLE

Develop

Developers document the API contract with OpenAPI/Swagger.

*API Contract security is **audited** from IDEs (VSCode, Intellij) using 42Crunch plugins.*

Integrate & Test

*API Contract security is **audited** via CI/CD pipeline, enforcing security **compliance**.*

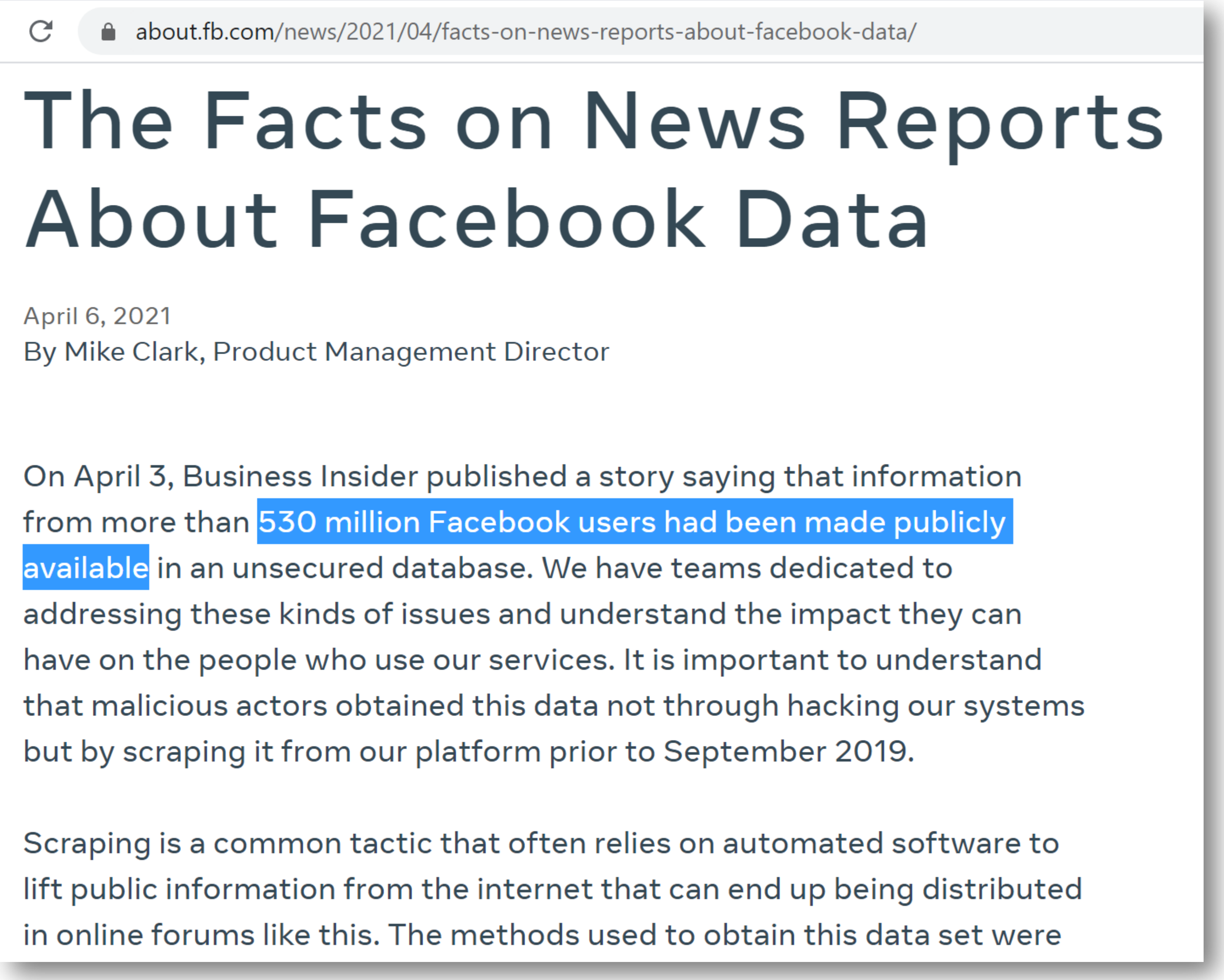
*API implementation is tested for vulnerabilities/discrepancies via **Conformance Scan**.*

Deploy & Protect

*API is automatically protected from OAS file with our **API Firewall**, deployed in line of traffic.*

*Unique **positive security model**, based on OpenAPI. No manual rules to write and maintain.*

#1: Facebook 530 million profiles leak



about.fb.com/news/2021/04/facts-on-news-reports-about-facebook-data/

The Facts on News Reports About Facebook Data

April 6, 2021
By Mike Clark, Product Management Director

On April 3, Business Insider published a story saying that information from more than 530 million Facebook users had been made publicly available in an unsecured database. We have teams dedicated to addressing these kinds of issues and understand the impact they can have on the people who use our services. It is important to understand that malicious actors obtained this data not through hacking our systems but by scraping it from our platform prior to September 2019.

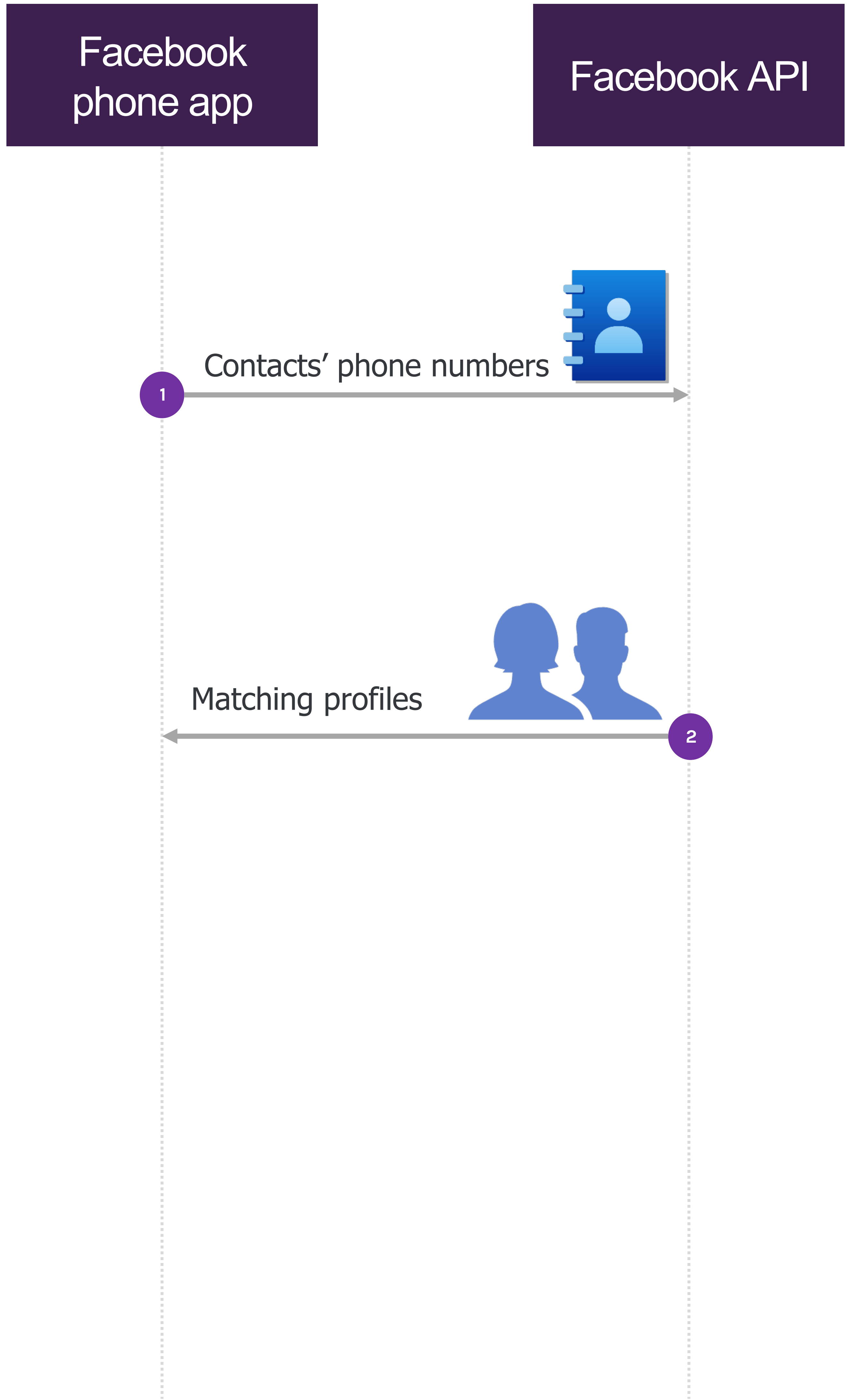
Scraping is a common tactic that often relies on automated software to lift public information from the internet that can end up being distributed in online forums like this. The methods used to obtain this data set were

https://apisecurity.io/issue-129-facebook-clubhouse-profiles-scraped-apis-forresters-state-application-security-2021/

What happened

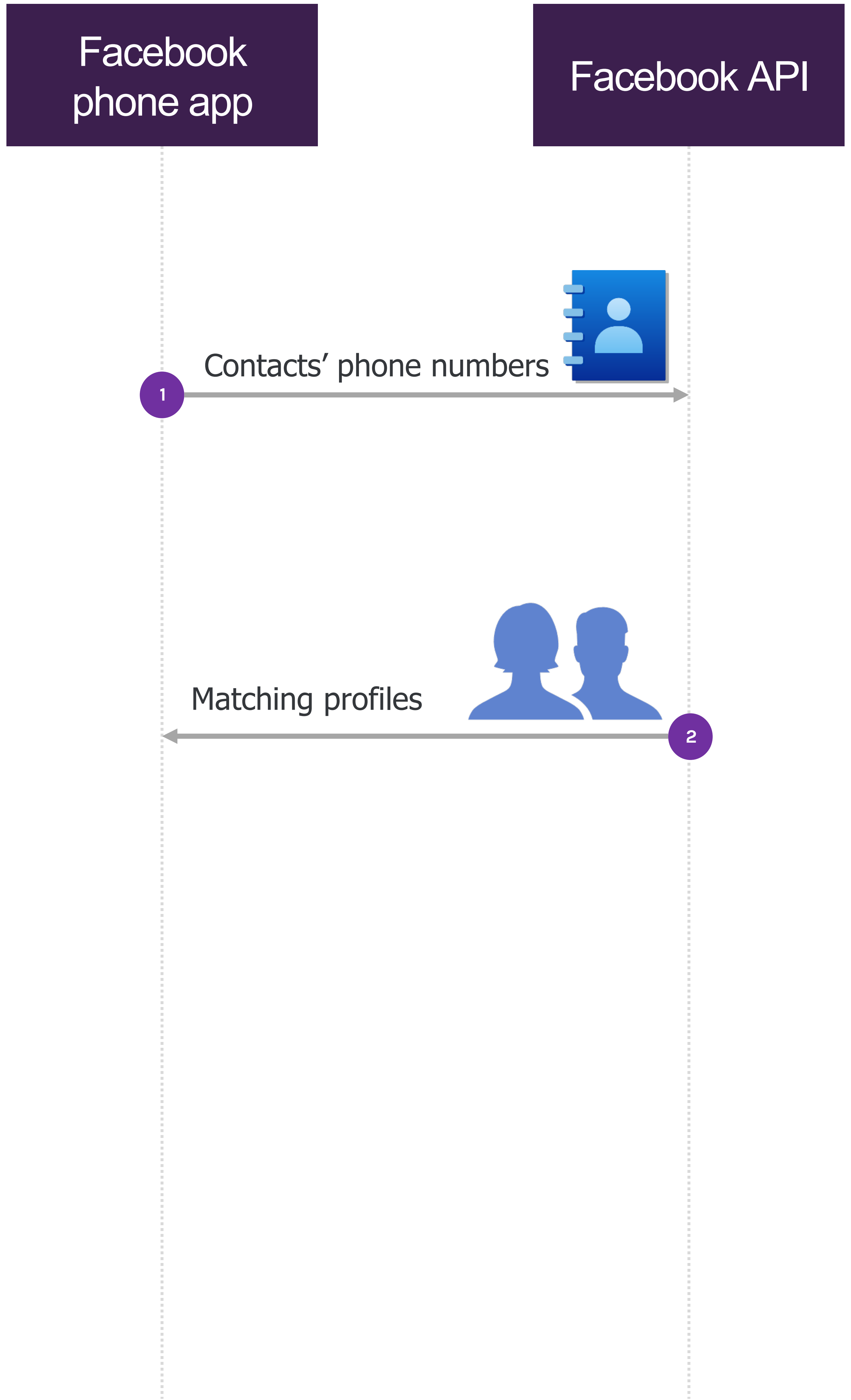
- API to find “friends” by contacts’ phone numbers
- Attackers could submit generated numbers:

  e.g. +1 (000) 000-0000 to +1 (999) 999-9999
- Up to 10,000 entries were accepted per call
- Leaked data includes names, Facebook IDs, phone numbers, email addresses, page likes
- Looks like Facebook had been receiving reports of the vulnerability for years before fixing it in 2019



Business impact

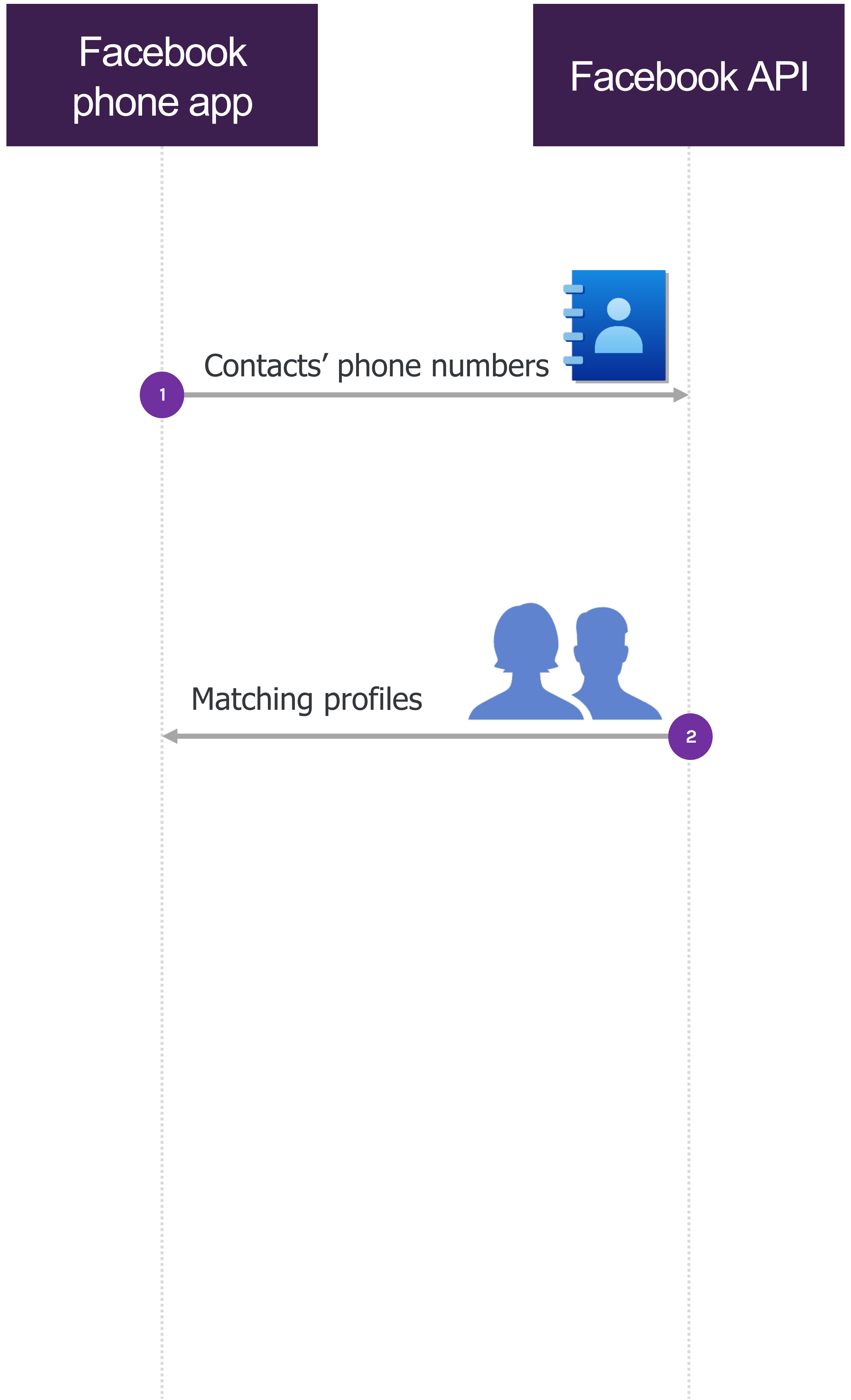
- Private phone numbers (including ones for MFA) leaked too
- Big privacy violation
- Potentially enabling phishing and social engineering attacks
- Likely with legal consequences for Facebook



How to prevent

- **OWASP API1:2019** Broken Object-Level Authorization
- **OWASP API3:2019** Excessive Data Exposure
- **OWASP API4:2019** Lack of resources and rate limiting

- Enforce and test authorization even on internal APIs (42Crunch Conformance Scan)
- Define/test/enforce limits on incoming and returned payloads including number of elements (42Crunch Security Audit, Conformance Scan, Protection)
- Implement rate limiting (42Crunch rate limit protections)
- Implement monitoring (SIEM integration of 42Crunch Protection)



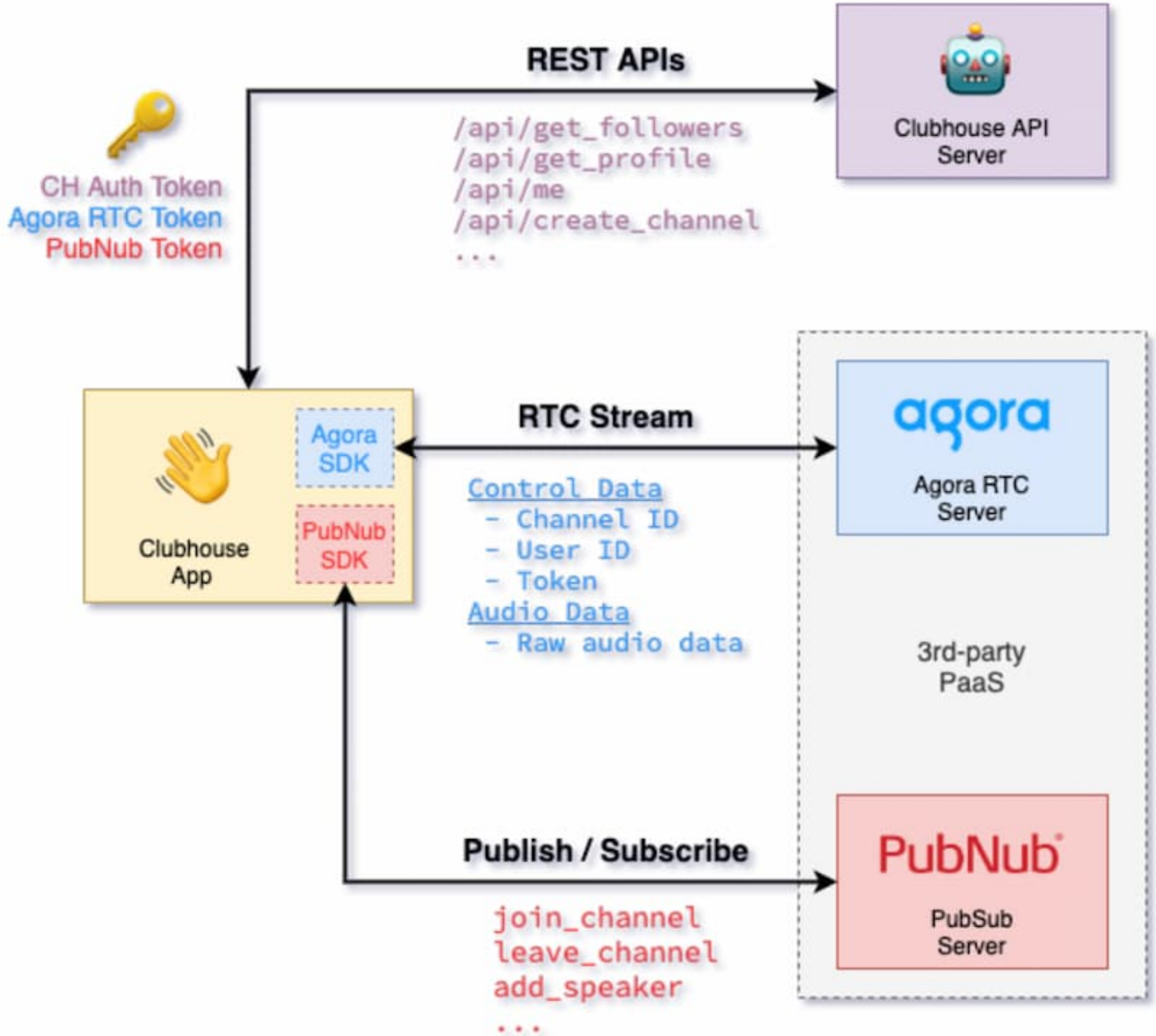
Other similar leaks: Parler, Clubhouse

- Parler posts got scraped: sequential IDs, open API, photo and video in RAW formats with metadata

- 1.3 Clubhouse user profiles scraped: sequential IDs, included links to private Twitter and Instagram accounts

#2: Clubhouse data spill

- Attackers were enumerating rooms, getting Agora tokens to join, and then "leaving" the room, but keeping access through Agora

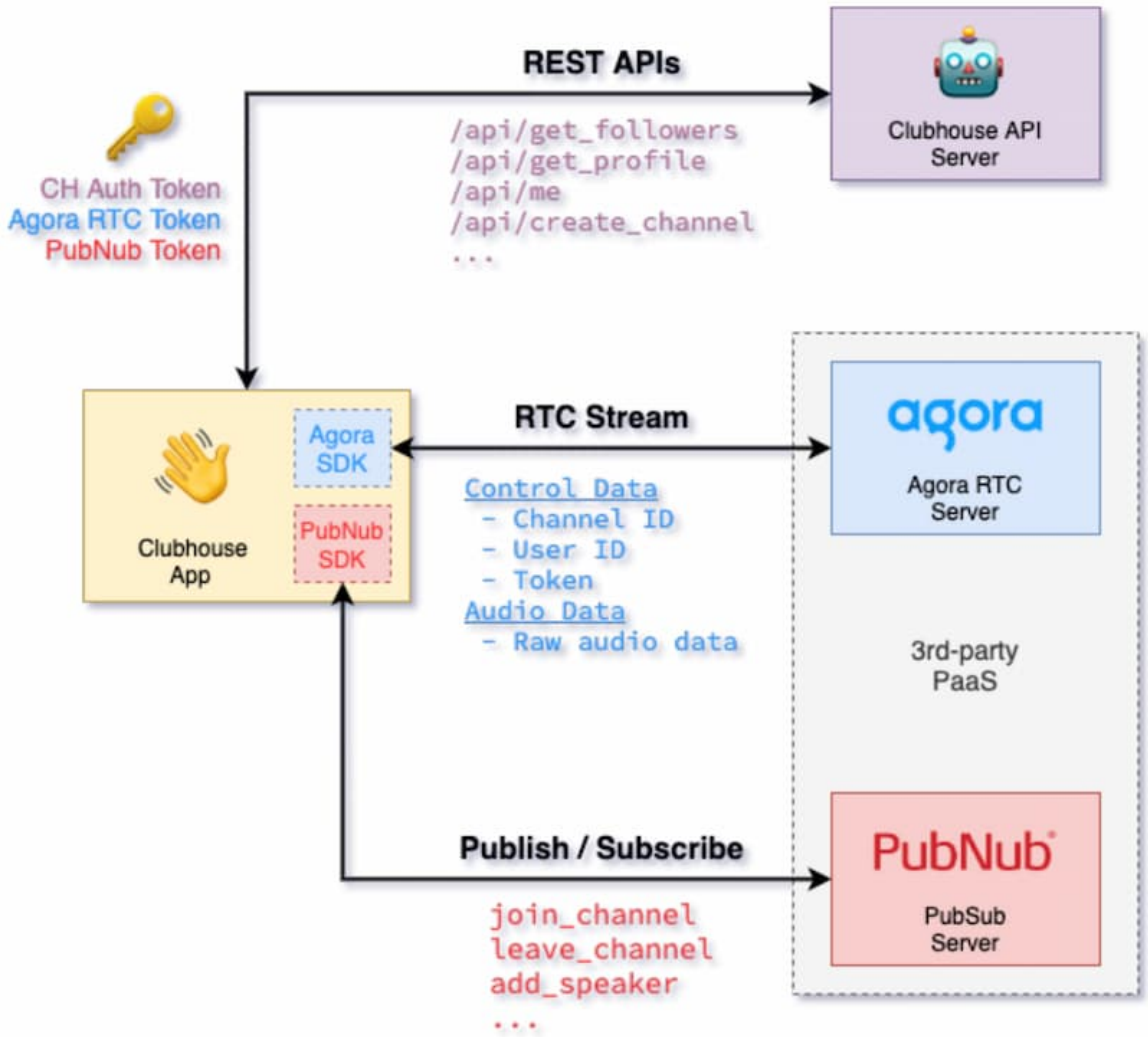


https://apisecurity.io/issue-122-api-issues-clubhouse-healthcare-apps-scope-based-recon-oas-v3-1-0/

How to prevent

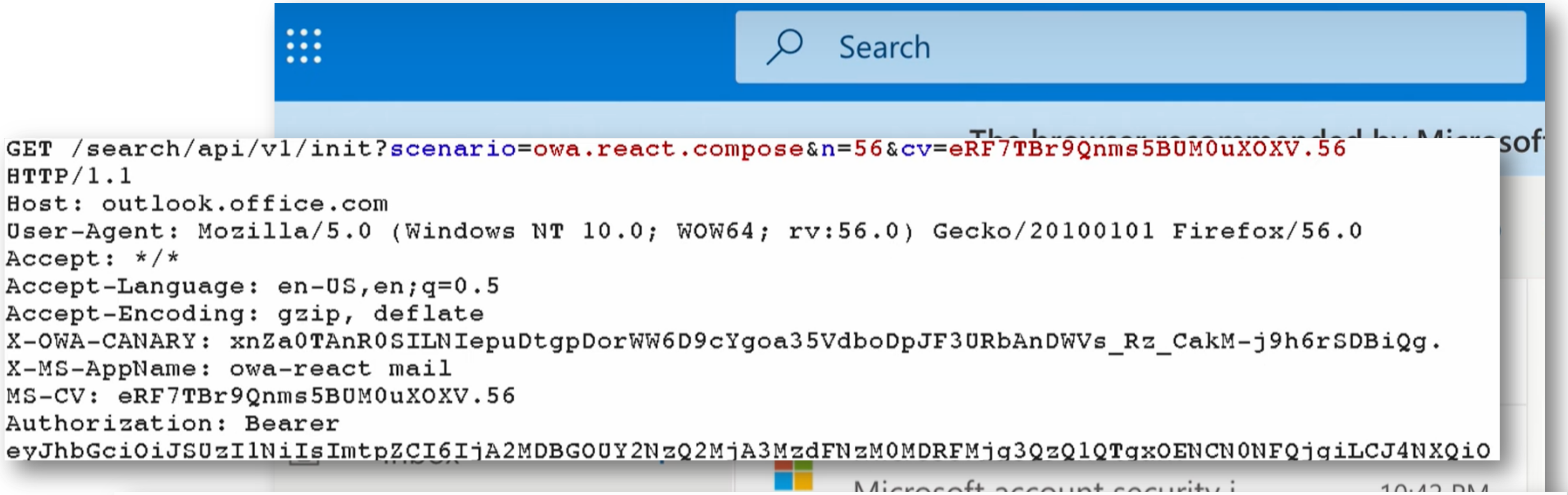
- **OWASP API2:2019:** Broken Authentication

- Use standard authentication and delegation mechanisms such as OAuth and short-lived tokens (42Crunch Security Audit)
- Use signed JWT tokens and prevent token reuse (42Crunch JWT Protections)

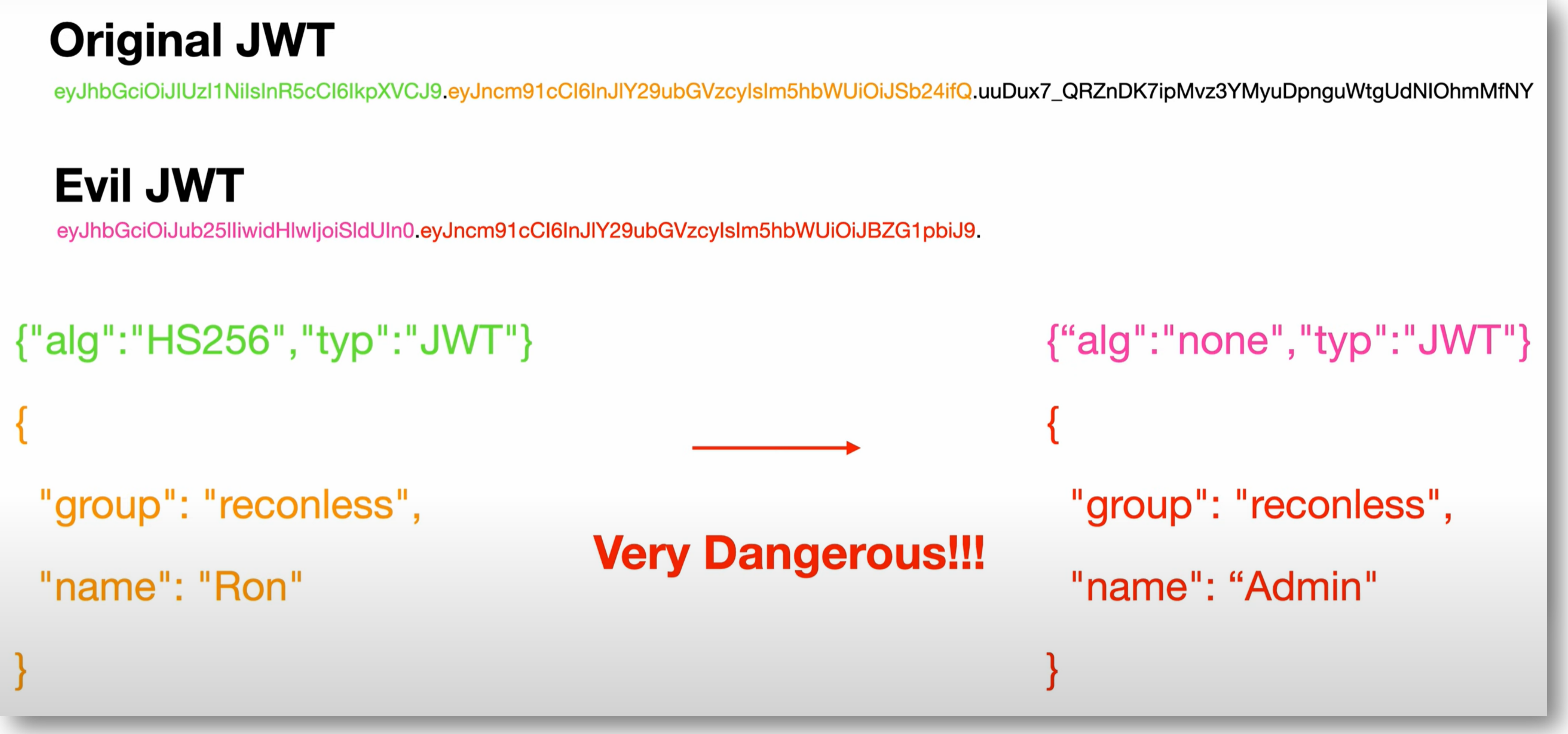


#3: Office 365 Outlook

- Microsoft Office 365 Outlook used JWT tokens for API authentication
- It accepted JWTs without signature
- Thus, attackers could construct tokens with other users' IDs and access their email



```
GET /search/api/v1/init?scenario=owa.react.compose&n=56&cv=eRF7TBr9Qnms5BUM0uXOXV.56
HTTP/1.1
Host: outlook.office.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-OWA-CANARY: xnZa0TAnR0SILNIepuDtgpDorWW6D9cYgoa35VdboDpJF3URbAnDWVs_Rz_CakM-j9h6rSDBiQg.
X-MS-AppName: owa-react mail
MS-CV: eRF7TBr9Qnms5BUM0uXOXV.56
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsImtpZCI6IjA2MDBGOUY2NzQ2MjA3MzdFNzM0MDRFMjg3QzQ1QTgxOENCN0NFQjgiLCJ4NXQiO
```



Original JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJncm91cCI6InJlY29ubGVzcyIsIm5hbWUiOiJSb24ifQ.uuDux7_QRZnDK7ipMvz3YMyuDpnguWtgUdNIOhmMfNY

Evil JWT

eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJncm91cCI6InJlY29ubGVzcyIsIm5hbWUiOiJBZG1pbiJ9.

```
{"alg":"HS256","typ":"JWT"}
{
 "group": "reconless",
 "name": "Ron"
}
```

Very Dangerous!!!

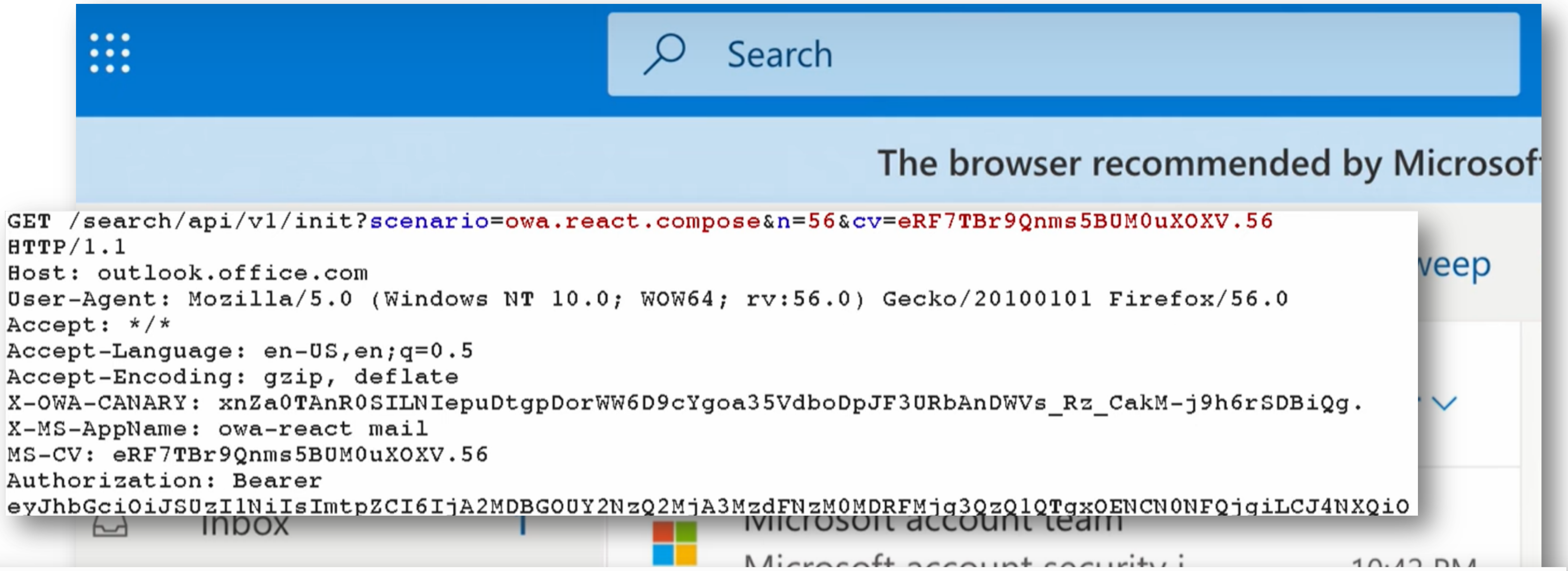
```
{“alg":"none","typ":"JWT"}
{
 "group": "reconless",
 "name": “Admin"
}
```

https://apisecurity.io/issue-115-vulnerabilities-solarwinds-ledger-outlook-new-plugin-jetbrains-ides/

How to prevent

- **OWASP API2:2019:** Broken Authentication
- Externalize JWT policies

  (42Crunch JWT Protections)


Search
The browser recommended by Microsof
veep
Inbox
Microsoft account team
Microsoft account security i
10:42 PM

```
GET /search/api/v1/init?scenario=owa.react.compose&n=56&cv=eRF7TBr9Qnms5BUM0uXOXV.56
HTTP/1.1
Host: outlook.office.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0) Gecko/20100101 Firefox/56.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
X-OWA-CANARY: xnZa0TAnR0SILNIepuDtgpDorWW6D9cYgoa35VdboDpJF3URbAnDWVs_Rz_CakM-j9h6rSDBiQg.
X-MS-AppName: owa-react mail
MS-CV: eRF7TBr9Qnms5BUM0uXOXV.56
Authorization: Bearer
eyJhbGciOiJSUzI1NiIsImtpZCI6IjA2MDBGOUY2NzQ2MjA3MzdFNzM0MDRFMjg3QzQ1QTgxOENCN0NFQjgiLCJ4NXQiO
```

Original JWT

eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJncm91cCI6InJlY29ubGVzcyIsIm5hbWUiOiJSb24ifQ.uuDux7_QRZnDK7ipMvz3YMyuDpnguWtgUdNIOhmMfNY

Evil JWT

eyJhbGciOiJub25lIiwidHlwIjoiSldUIn0.eyJncm91cCI6InJlY29ubGVzcyIsIm5hbWUiOiJBZG1pbiJ9.

```
{"alg":"HS256","typ":"JWT"}
{
  "group": "reconless",
  "name": "Ron"
}
```

→ **Very Dangerous!!!**

```
{“alg":"none","typ":"JWT"}
{
  "group": "reconless",
  "name": “Admin"
}
```

42crunch
How to Best Leverage JWTs for API Security
Isabelle Mauny, 42Crunch Field CTO and co-founder
Dmitry Sotnikov, 42Crunch CPO, Curator of APIsecurity.io
59:26

#4: iPhone Automatic Call Recorder

- The call to fetch recordings contained UserID parameter
- The API had no authentication or authorization
- Changing UserID to another user's ID (their phone number!) worked
- The API returned link to recordings in S3 storage

https://apisecurity.io/issue-125/

```
POST /fetch-sinch-recordings.php HTTP/1.1
Host: 167.88.123.157:80
Content-Type: application/json
Connection: close
Accept: */*
User-Agent: CallRecorder/2.25 (com.arun.callrecorderadvanced;
build:1; iOS 14.4.0) Alamofire/4.7.3
Accept-Language: en-IN;q=1.0, kn-IN;q=0.9, hi-IN;q=0.8, hi-Latn-
IN;q=0.7
Content-Length: 72
Accept-Encoding: gzip, deflate

{
 "UserID": "xxxxxx",
 "AppID": "xxx"
}
```

How to Prevent

- [API1:2019 — Broken object-level authorization]
- [API2:2019 — Broken authentication]

- Ensure that APIs have authentication (42Crunch Security Audit)
- Test against BOLA/IDOR attacks (42Crunch Conformance Scan)

```
POST /fetch-sinch-recordings.php HTTP/1.1
Host: 167.88.123.157:80
Content-Type: application/json
Connection: close
Accept: */*
User-Agent: CallRecorder/2.25 (com.arun.callrecorderadvanced; build:1; iOS 14.4.0) Alamofire/4.7.3
Accept-Language: en-IN;q=1.0, kn-IN;q=0.9, hi-IN;q=0.8, hi-Latn-IN;q=0.7
Content-Length: 72
Accept-Encoding: gzip, deflate

{
 "UserID": "xxxxxx",
 "AppID": "xxx"
}
```

#5: chess.com Account Takeover

- Chess.com has API to locate another user to exchange messages with your friends
- The API returned full user profile
- This included session_id which could be used to log in on the other user’s behalf
- For administrators, the session_id worked in the admin portal

https://apisecurity.io/issue-121-vulnerability-chess-com-graphql-security-playground-checklist/

```
GET
/v1/users?loginToken=98a161…&username=hikaru&signed=iOS3.9
.7
{
 "status": "success",
 "data": {
  "email": "REDACTED",
  "premium_status": 3,
  "id": 15448422,
  "uuid": "REDACTED",
  "country_id": 2,
  "avatar_url": "REDACTED",
  "last_login_date": REDACTED,
  "session_id": "REDACTED",
  "location": "Sunrise, Florida",
  "username": "Hikaru",
  "points": 52,
  "chess_title": "GM",
  "first_name": "Hikaru Nakamura",
  "last_name": null,
  "country_name": "United States",
  "member_since": REDACTED,
  "about": "",
  "is_blocked": false,
  "is_tracked": false,
  "are_friends": false,
  "friend_request_exists": true,
  "is_able_to_change_username": null,
  "flair_code": "diamond_traditional",
  ....
```

How to Prevent

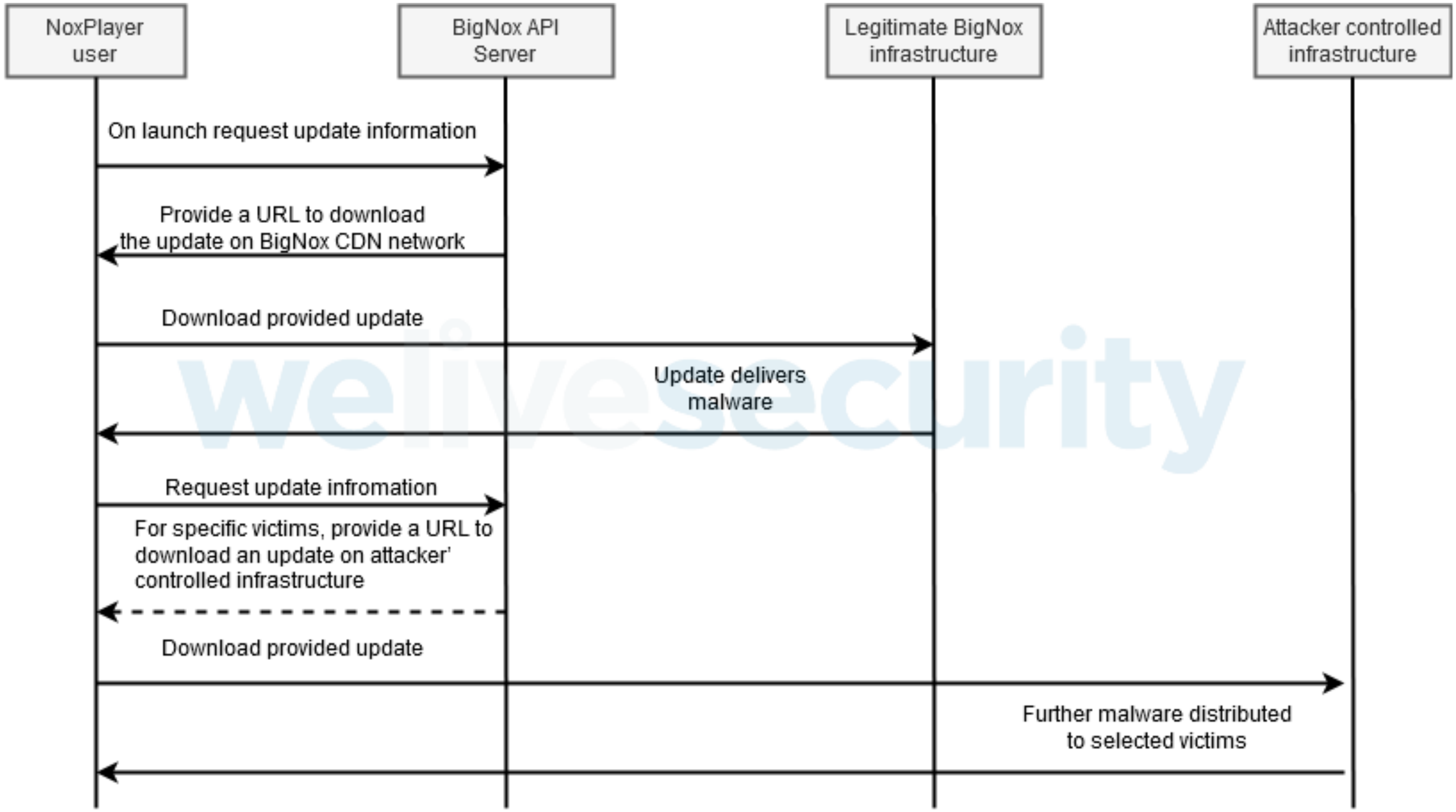
- OWASP API3:2019 — Excessive data exposure
- Strictly define API responses (42Crunch Security Audit)
- Enforce response definitions at runtime (42Crunch Protection)

https://apisecurity.io/issue-121-vulnerability-chess-com-graphql-security-playground-checklist/

```
GET
/v1/users?loginToken=98a161…&username=hikaru&signed=iOS3.9
.7
{
 "status": "success",
 "data": {
  "email": "REDACTED",
  "premium_status": 3,
  "id": 15448422,
  "uuid": "REDACTED",
  "country_id": 2,
  "avatar_url": "REDACTED",
  "last_login_date": REDACTED,
  "session_id": "REDACTED",
  "location": "Sunrise, Florida",
  "username": "Hikaru",
  "points": 52,
  "chess_title": "GM",
  "first_name": "Hikaru Nakamura",
  "last_name": null,
  "country_name": "United States",
  "member_since": REDACTED,
  "about": "",
  "is_blocked": false,
  "is_tracked": false,
  "are_friends": false,
  "friend_request_exists": true,
  "is_able_to_change_username": null,
  "flair_code": "diamond_traditional",
  ....
```

#6: NoxPlayer Supply Chain Attack

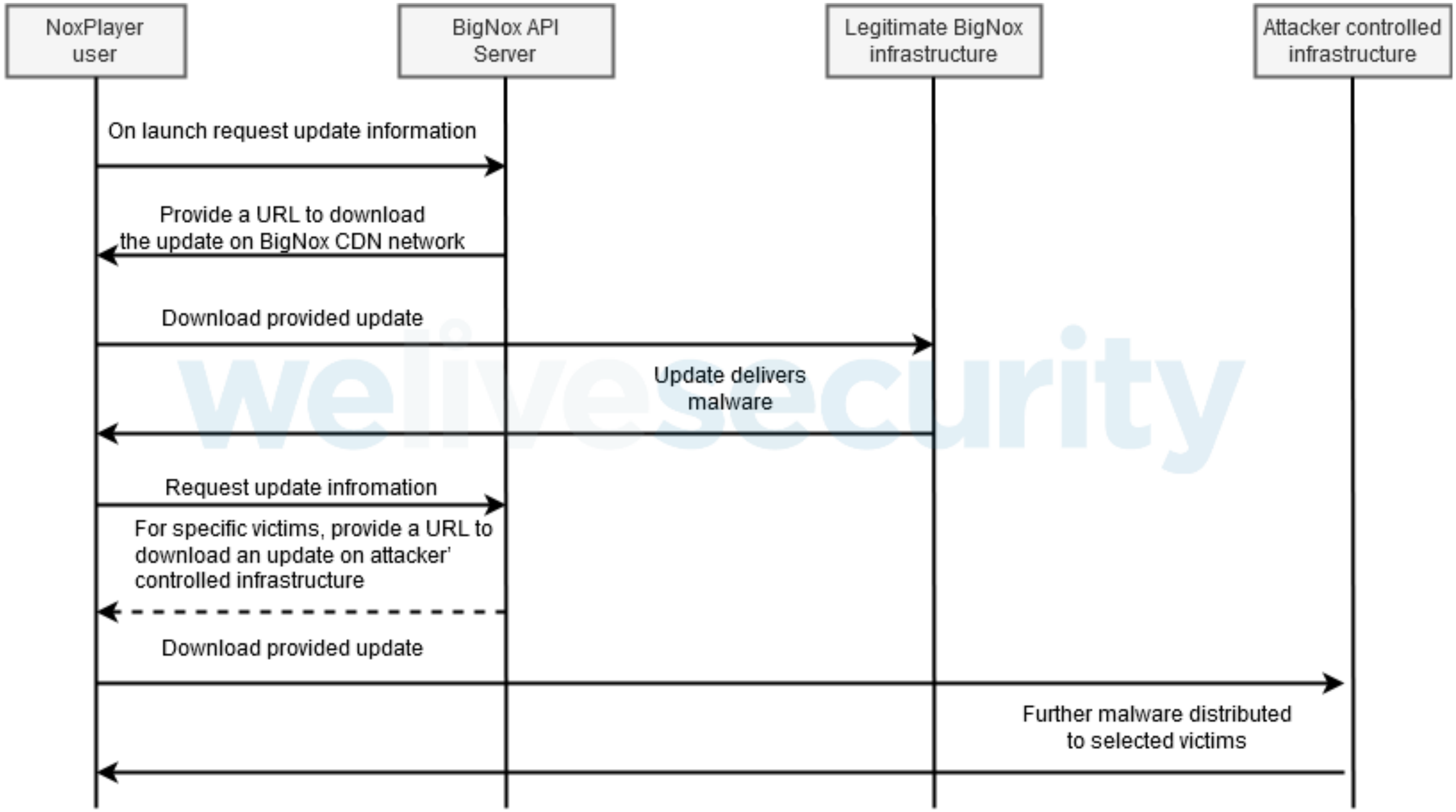
- Android emulator for PCs and Macs
- API hacked to deliver malware URLs instead of regular updates


NoxPlayer user
BigNox API Server
Legitimate BigNox infrastructure
Attacker controlled infrastructure
On launch request update information
Provide a URL to download the update on BigNox CDN network
Download provided update
Update delivers malware
Request update infromation
For specific victims, provide a URL to download an update on attacker' controlled infrastructure
Download provided update
Further malware distributed to selected victims
welivesecurity

https://apisecurity.io/issue-119-noxplayer-supply-chain-attack-hacked-api/

How to Prevent

- Define and enforce strict patterns on strings in API responses (42Crunch Security Audit, 42Crunch Protection)



NoxPlayer user

BigNox API Server

Legitimate BigNox infrastructure

Attacker controlled infrastructure

On launch request update information

Provide a URL to download the update on BigNox CDN network

Download provided update

Update delivers malware

Request update infromation

For specific victims, provide a URL to download an update on attacker' controlled infrastructure

Download provided update

Further malware distributed to selected victims

https://apisecurity.io/issue-119-noxplayer-supply-chain-attack-hacked-api/

Additional Resources

APIsecurity.io

- Sign up for the weekly newsletter that comes out every Thursday
- Follow us on social | Twitter | Linkedin Group

OWASP API Security Top 10

42Crunch.com

Follow us on social media to keep up with API news and new product and plugin releases!

Twitter | Linkedin | youtube

THANK YOU

- questions -