Welcome to Auto-ISAC!

Monthly Virtual Community Call

December 6, 2023

This Session will be recorded.

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Antitrust Statement

As Members of the Auto-ISAC, we strictly comply with EU and US antitrust laws. Please do not discuss anything that your company considers commercially sensitive and/or confidential such as pricing or future product plans. A violation of any of the above-mentioned issues will result in us having to quickly terminate the meeting.

Finally, please remember to keep these deliberations confidential. Please do not discuss the substance of these meetings outside of this group.

This meeting is being held at

TLP:CLEAR

Disclosure is not limited.

Traffic Light Protocol (TLP)

Version 2.0 Definitions

Color		When Should It Be Used?	How May It Be Shared?
TLP:RED 🔴 ● ●	**Not for disclosure, restricted to participants only.**	Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. For the eyes and ears of individual recipients only, no further.	Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.
TLP:AMBER+STRICT ● 🟡 ●	**Limited disclosure, restricted to participants' and its organization.**	Sources may use TLP:AMBER+STRICT when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization.	Recipients may share TLP:AMBER+STRICT information only with members of their own organization on a need-to-know basis to protect their organization and prevent further harm.
TLP:AMBER ● 🟡 ●	**Limited disclosure, restricted to participants' organization and its clients on a need-to-know basis.**	Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Note that TLP:AMBER+STRICT should be used to restrict sharing to the recipient organization only.	Recipients may share TLP:AMBER information with members of their own organization and its clients on a need-to-know basis to protect their organization and its clients and prevent further harm.
TLP:GREEN ● ● 🟢	**Limited disclosure, restricted to the community.**	Sources may use TLP:GREEN when information is useful to increase awareness within their wider community.	Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. Unless otherwise specified, TLP:GREEN information may not be shared outside of the cybersecurity or cyber defense community.
TLP:CLEAR ○ ○ ○	**Disclosure is not limited.**	Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	Recipients may share this information without restriction. Information is subject to standard copyright rules.

Source: https://www.us-cert.gov/tlp

Agenda

Time (ET)	Topic
11:00	**Welcome** ➢ Why We're Here ➢ Expectations for This Community
11:05	**Auto-ISAC Update** ➢ Auto-ISAC Activities ➢ Heard Around the Community ➢ Intelligence Highlights
11:15	***DHS CISA Community Update*** ➢ **Jeff Terra, Consulting Support, Joint Cyber Defense Collaborative (JCDC), Cybersecurity and Infrastructure Security Agency (CISA)**
11:20	**Featured Speaker:** ➢ **Dan Barahona, Founder, APIsec University** ➢ **Title: *"API Security Risks for Connected Cars"***
11:55	**Q&A & Closing Remarks**

Welcome - Auto-ISAC Community Call!

Purpose: **These monthly Auto-ISAC Community Meetings are an opportunity for you, our Members & connected vehicle ecosystem Partners, to:**

- ✓ ***Stay informed of Auto-ISAC activities***
- ✓ ***Share information on key vehicle cybersecurity topics***
- ✓ ***Learn about exciting initiatives within the automotive community from our featured speakers***

Participants: **Auto-ISAC Members, Potential Members, Strategic Partners, Academia, Industry Stakeholders and Government –** ***the whole of the automotive industry***

Classification Level: **TLP:GREEN - May be shared within the Auto-ISAC Community and "off the record"**

How to Connect: **For further info, questions or to add other POCs to the invite, please contact us!**

(sharmilakhadka@automotiveisac.com)

Engaging in the Auto-ISAC Community

- **Join**
  - If your organization is eligible, apply for Auto-ISAC Membership
  - If you aren't eligible for Membership, connect with us as a Partner
  - Get engaged – *"Cybersecurity is everyone's responsibility!"*

- **Participate**
  - Participate in monthly virtual conference calls (1st Wednesday of month)
  - If you have a topic of interest, let us know!
  - Engage & ask questions!

- **Share** – *"If you see something, say something!"*
  - Submit threat intelligence or other relevant information
  - Send us information on potential vulnerabilities
  - Contribute incident reports and lessons learned
  - Provide best practices around mitigation techniques

30 *OEM Members*

21 *Navigator Partners*

47 *Supplier & Commercial Vehicle Members*

20 *Innovator Partners*

Membership represents **99%** *of cars and trucks on the road in North America*

Coordination with **26** *critical infrastructure ISACs through the National Council of ISACs (NCI)*

2023 Board of Directors

Thank you for your Leadership!

Josh Davis
Chair *of the*
Board of the Directors
Toyota

Kevin Tierney
Vice Chair *of the*
Board of the Directors
GM

Stephen Roberts
Secretary *of the*
Board of the Directors
Honda

Tim Geiger
Treasurer *of the*
Board of the Directors
Ford

Andreas Ebert
Chair *of the EuSC*
Volkswagen

Andrew Hillery
Chair *of the CAG*
Cummins

Ravi Puvvala
Chair *of the SAG*
Fleet Defender

Monica Mitchell
Polaris

Bob Kaster
Bosch

Brian Witten
Aptiv

Auto-ISAC Member Roster

As of December 1, 2023

80 Members + 5 Pending

Aisin	Ferrari	Lucid Motors	Qualcomm
Allison Transmission	Fleet Defender	Luminar	Renesas Electronics
Amazon	Flex	Magna	Rivian
American Axle & Manufacturing	Ford	MARELLI	Stellantis
Aptiv	Garrett	Mazda	Subaru
AT&T	General Motors (Cruise-Affiliate)	Mercedes-Benz	Sumitomo Electric
AVL List GmbH	Geotab	Mitsubishi Electric	thyssenkrupp
Blackberry Limited	Harman	Mitsubishi Motors	Tokai Rika
BMW Group	Hitachi	Mobis	Toyota (Woven-Affiliate)
BorgWarner	Honda	Motional	Valeo
Bosch (ETAS-Affiliate)	Hyundai	Navistar	Veoneer
Bose Automotive	Infineon	Nexteer Automotive Corp	Vitesco
ChargePoint	Intel	Nissan	Volkswagen (Cariad-Affiliate)
CNH Industrial	John Deere Electronic	Nuro	Volvo Cars
Continental (Argus-Affiliate)	JTEKT	Nuspire	Volvo Group
Cummins (Meritor-Affiliate)	Kia America, Inc.	NXP	Waymo
Daimler Truck	Knorr Bremse	Oshkosh Corp	Yamaha Motors
Denso	KTM	PACCAR	ZF
e:fs TechHub GmbH	Lear	Panasonic (Ficosa-Affiliate)	
Faurecia	LG Electronics	Polaris	

Pending: Dana Inc, Phinia Inc, Stoneridge, Jaguar Land Rover, Renault SAS

**All times are in ET

Auto-ISAC Business Updates and Events

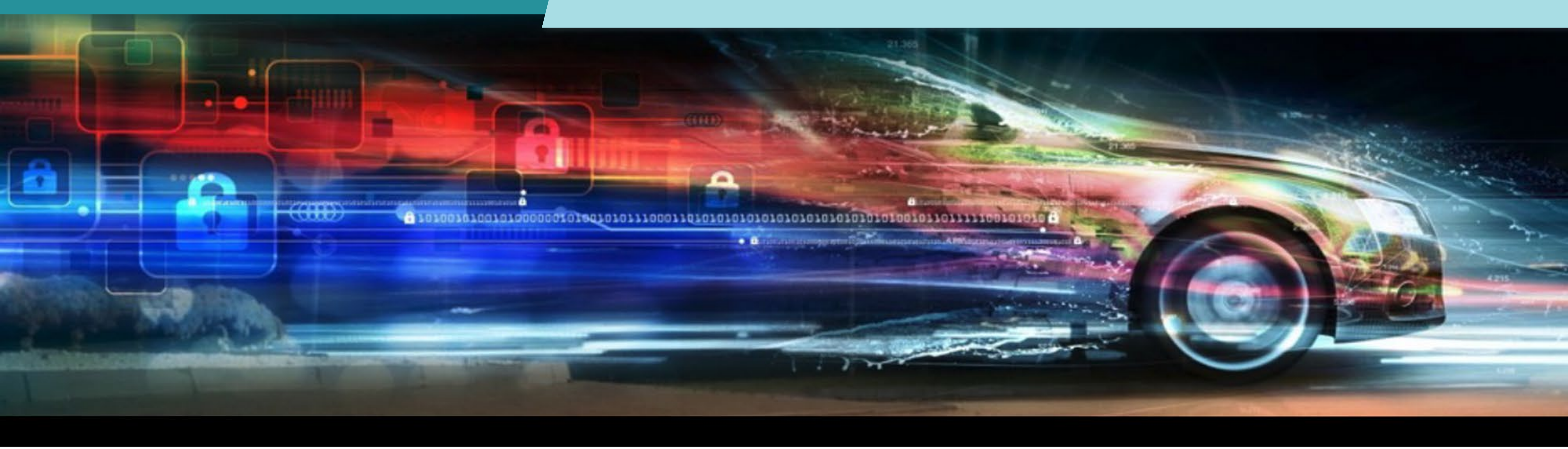
- **Community Call: Wednesday, January 10th Time: *11:00am – 12:00 p.m*. TLP:GREEN**
  - **Speaker: Ramiro Pareja Veredas, Principal Cybersecurity Consultant, IOActive; Yashin Mehaboobe, Senior Cybersecurity Consultant, Xebia**
  - **Title: "Scalable Attacks on Connected Vehicles"**

- **Auto-ISAC 2nd European Summit be held in Munich, Germany: June 12th – June 13th. The Titanium sponsor the 2024 event will be BMW. Stay tuned for more details.**

- **ACT Fundamental Course Block: Online, On-Demand, Anytime, Anywhere, and by Anyone $500/course**
  - **Cybersecurity Basics (32 hrs.) | Security Engineering (28 hrs.) | Security Operations/Management (22.5 hrs.)**

- **ACT Advanced Courses: ~~$4500 ($4k member pricing)~~**
  - ❑ **Cost: ***$2000 (Member Pricing), ($2250 Non-Member Pricing) with discount code.**
  - **Advanced Engineering: January 22 - 26, 2024**
  - **Wireless: February 5 - 9, 2024**
  - **EV and EV Infrastructure: March 4 - 8, 2024**
  - **Guided Attacks: April 29 - May 4, 2024**

NOTE: The January Community call rescheduled to January 10th. A New Community Call invite for Feb 2024- Jan 2025 will be sent soon. Please be on the lookout.



Auto-ISAC Intelligence Highlight

This document is Auto-ISAC Sensitive and Confidential.

TLP:CLEAR

AUTO-ISAC
Automotive Information Sharing and Analysis Center

Auto-ISAC Intelligence

- **Know what we track daily: subscribe to the DRIVEN; Auto-ISAC 2024 Threat Assessment is nearly complete; the TLP:GREEN version is expected early next year.**
  - **Send feedback, intelligence, or questions to analyst@automotiveisac.com**
- **Intelligence Notes**
  - **Geopolitical tensions involving Russia, China, North Korea, and Iran remain high with Russia-Ukraine and Israel-Hamas in crisis (Russia-Ukraine, China [1], North Korea [2] [3] [4] [5], Iran [6]). Regarding the Israel-Hamas War: (Note: We cannot rule out the war expanding to Iran)**
    - **No signs of state-sponsored destructive cyberattacks; however, cybercriminals have recently used at least one wiper to target entities in Israel (BleepingComputer).**
    - **Cybercriminals, including hacktivists, remain active with nuisance attacks, including beginning to target "Israel-nexus" entities outside the country (Check Point, Bleeping Computer, SecurityAffairs)**
  - **Ransomware [7] [8]* Groups Targeting Automotive: Medusa, INC Ransomware, 8Base, Akira, LockBit 3.0, Lorenz, Knight, Play, ALPHV**
  - **Notable TTPs and Tools: Exploiting CITRIX BLEED (CISA); Luring Software Developers and Malicious Actors Seeking Employment to Exploit Insider Threat Vector (Unit42); Exploiting Zyxel Firewalls (Sektorcert); Exploiting Unitronics Programmable Logic Controllers* (CISA); GPS Spoofing* (OpsGroup); SysJoker (Check Point); MultiLayer Wiper, PartialWasher Wiper, BFG Agonizer Wiper (Unit42) *.**

CISA Resource Highlights

- Joint Cyber Defense Collaborative

JOINT CYBER DEFENSE COLLABORATIVE

Jeff Terra
12/6/2023

CISA Releases Guidance for Addressing Citrix NetScaler ADC and Gateway Vulnerability CVE-2023-4966, Citrix Bleed

- The CSA details activity by cyber actors, known as BlackTech, linked to the People's Republic of China (PRC).
- The advisory provides BlackTech tactics, techniques, and procedures (TTPs) and urges multinational corporations to review all subsidiary connections, verify access, and consider implementing zero trust models to limit the extent of a potential BlackTech compromise.
- BlackTech has demonstrated capabilities in modifying router firmware without detection and exploiting routers' domain-trust relationships to pivot from international subsidiaries to headquarters in Japan and the United States, which are the primary targets.

#StopRansomware: Snatch Ransomware

- The FBI and CISA are releasing this joint CSA to disseminate known ransomware IOCs and TTPs associated with the Snatch ransomware variant identified through FBI investigations as recently as June 1, 2023.
- Since mid-2021, Snatch threat actors have consistently evolved their tactics to take advantage of current trends in the cybercriminal space and leveraged successes of other ransomware variants' operations.
- Mitigations include:
  - Secure and closely monitor Remote Desktop Protocol (RDP)
  - Maintain offline backups of data
  - Enable and enforce phishing-resistant multifactor authentication

CISA Releases its Open-Source Software Security Roadmap

- CISA released an Open-Source Software Security Roadmap to lay out—in alignment with the National Cybersecurity Strategy and the CISA Cybersecurity Strategic Plan—how we will partner with federal agencies, open-source software (OSS) consumers, and the OSS community, to secure OSS infrastructure.

- The roadmap details four key goals:

  - Establish CISA's role in supporting the security of OSS
  - Understand the prevalence of key open-source dependencies
  - Reduce risks to the federal government
  - Harden the broader OSS ecosystem

Security/Software Updates

For September 2023:

- Apple Releases Multiple Security Updates
- Atlassian Releases Security Updates
- Fortinet Releases Security Updates
- Adobe Releases Security Updates
- Microsoft Releases Security Updates
- Mozilla Releases Security Updates
- CISCO Releases Security Updates
- VMWare Releases Security Updates
- Drupal Releases Security Guidance

- **Best practices:**
  - Leverage automatic updates for all operating systems and third-party software
  - Implement security configurations for all hardware and software assets
  - Remove unsupported or unauthorized hardware and software from systems

Please note all information provided is TLP Amber

CISA Releases Industrial Control Advisories

- These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.
- For the period of 9/1/23- 9/30/23 approximately 35 advisories have been issued.
- Affected systems include Fujitsu Limited, Drover Fueling Solutions, Phoenix Contact TC Router, Rockwell Automation (multiple products), Siemens (multiple products), Omron Engineering, Real Time Automation, DEXMA DexGate and many others.
- For current ICS advisories please check CISA.gov regularly

Please note all information provided is TLP Amber

KEVs Catalogue

CISA strongly urges all organizations to reduce their exposure to cyberattacks by prioritizing timely remediation of Catalog vulnerabilities as part of their vulnerability management practice.

CISA added 23 new vulnerabilities to its Known Exploited Vulnerabilities (KEV) Catalog in the month of September. These types of vulnerabilities are a frequent attack vector for malicious cyber actors and pose significant risk to the federal enterprise.

Please note all information provided is TLP Amber

Additional Resources from CISA

- □ CISA Homepage - https://www.cisa.gov/
- □ CISA NCAS – https://cisa.gov/resources-tools/all-resources-tools
- □ CISA Shields Up - https://www.cisa.gov/shields-up
- □ Free Cybersecurity Services and Tools - https://www.cisa.gov/free-cybersecurity-services-and-tools
- □ CISA News Room - https://www.cisa.gov/cisa/newsroom
- □ CISA Blog - https://www.cisa.gov/blog-list
- □ CISA Publications Library - https://www.cisa.gov/publications-library
- □ CISA Cyber Resource Hub - https://www.cisa.gov/cyber-resource-hub
- □ CISA Cybersecurity Directives - https://cyber.dhs.gov/directives/

JOINT CYBER DEFENSE
COLLABORATIVE

For more information:

cisa.gov

Questions?

Central@cisa.dhs.gov

1-888-282-0870

Auto-ISAC Community Meeting

Why Do We Feature Speakers?

- These calls are an opportunity for information exchange & learning
- Goal is to educate & provide awareness around cybersecurity for the *connected vehicle*

What Does it Mean to Be Featured?

- Perspectives across our ecosystem are shared from Members, government, academia, researchers, industry, associations and others.
- Goal is to showcase a rich & balanced variety of topics and viewpoints
- *Featured speakers are not endorsed by Auto-ISAC nor do the speakers speak on behalf of Auto-ISAC*

30+ *Featured Speakers to date*

How Can I Be Featured?

- If you have a topic of interest you would like to share with the broader Auto-ISAC Community, then we encourage you to contact us!

7 *Best Practice Guides available on website*

2000+ *Community Participants*

Featured Speaker

Meet the Speaker

Dan Barahona

Dan is a 20+ year cybersecurity executive, and most recently the founder of APIsec University – a site that offers free, non-vendor courses on API security. The site, launched in August 2022, now has over 50,000 students enrolled, including over half the Fortune 100. Dan has held executive roles in Products, Marketing, Business Development, and Sales at companies including APIsec.ai, Qualys, Anomali, and ArcSight.

Dan hosts regular educational webinars on APIs and API Security. Recent topics include Hacking Cars, and Why APIs are the Weakest Link, which received over 2,500 attendees. He's a frequent speaker at API and cybersecurity conferences.

Dan's career started in the automotive industry, where he spent 3 years at General Motors in Safety and Crashworthiness. He has mechanical engineering degrees from Rensselaer Polytechnic Institute and Cornell University and an MBA from the University of Michigan.

API Security 101

Dan Barahona
Co-founder, APIsec University
dan@apisecuniversity.com

APISEC UNIVERSITY

HACKING APIs
HAPI HACKER

API Explosion

83%

of all Internet traffic is API traffic

Akamai

APIs Under Attack

2022

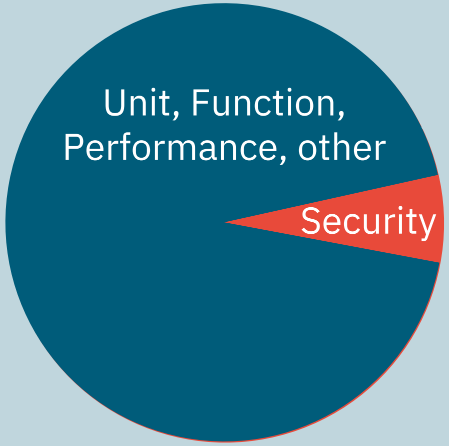
“API attacks will become the **most frequent attack vector”**

Gartner

APIs Under-Secured

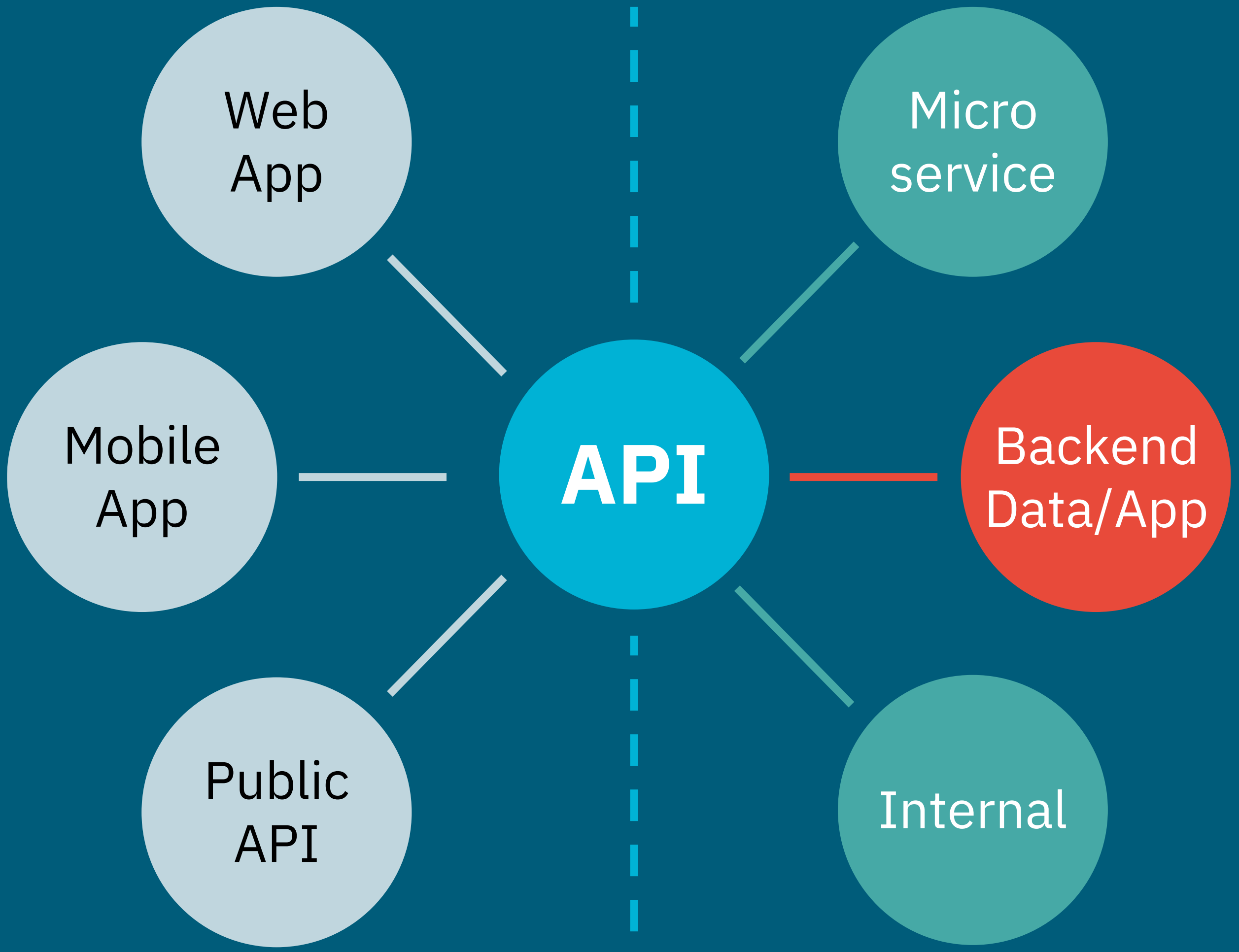
4%

of API testing is Security



Source: stateofapis.com

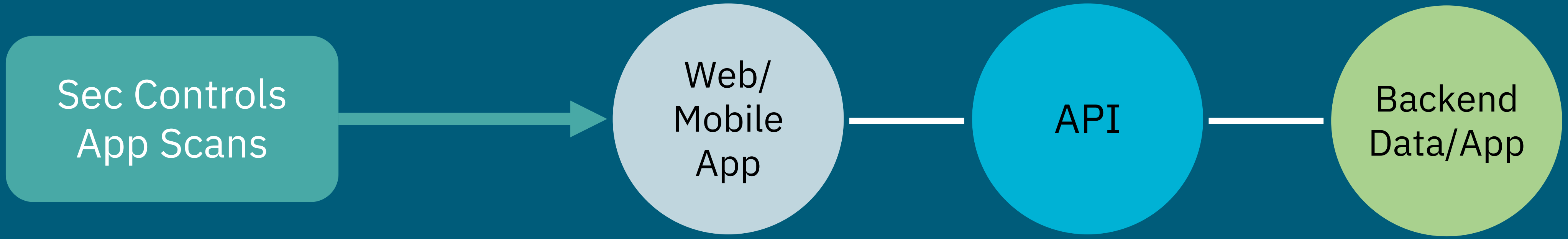
Why Attackers Target APIs



APIs:

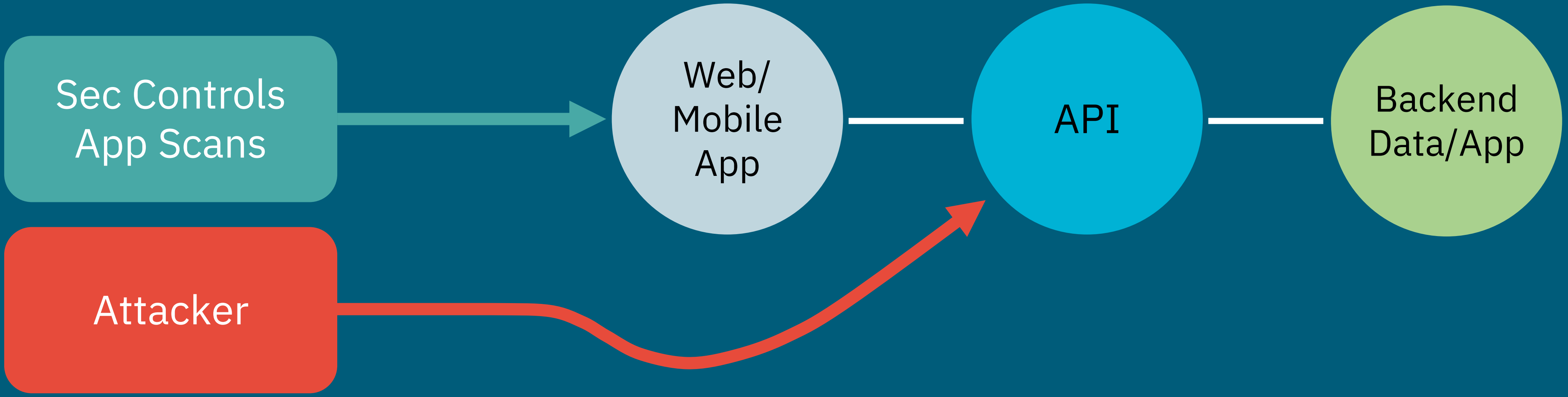
- Power web/mobile UIs
- Often exposed externally
- Also used internally
- Provide direct access to data
- Can be discovered, even if unpublished

API Attacks are Different



- Security controls often enforced at UI layer
- Traditional app scanners focus on UIs, common vulnerabilities

API Attacks are Different

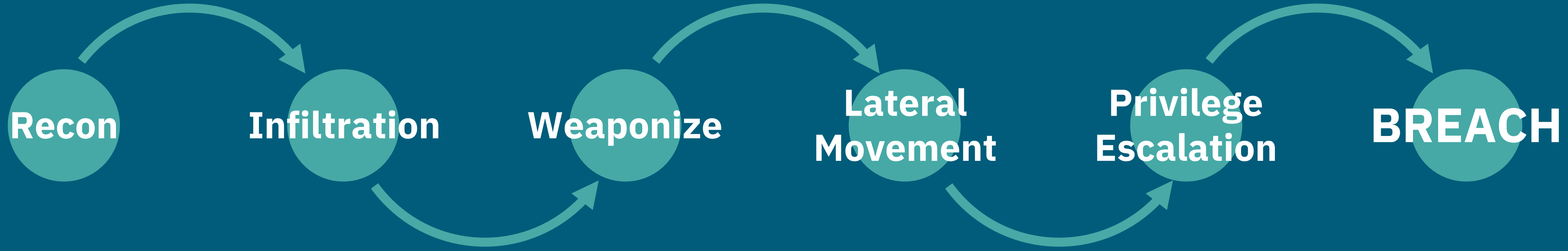


- Attackers bypass UIs and target APIs
- Direct access to backend data

- Often over-permissioned
- Vulnerable to logic flaws

Pro Tip: Your UI is NOT part of your security stack

“Classic” Cyber Attack



Recon

Infiltration

Weaponize

Lateral Movement

Privilege Escalation

BREACH

API Attack

Find Vulnerability

BREACH

Regulatory Landscape

U.S. SECURITIES AND EXCHANGE COMMISSION

- Breach notification requirement
- Public disclosure of risk management, processes, strategies
- Must include APIs if part of risk exposure

PCI DSS COMPLIANT

- New DSS 4.0 regulation – compliance by March 2024
- Includes APIs specifically for first time
- Detection of abuse of “business logic,” “manipulation of APIs”

European Commission GDPR General Data Protection Regulation

- Privacy rules being adopted in all geos (CCPA, PIPEDA, …)
- PII breaches frequently result of vulnerable APIs
- Fines in excess of $1B have been imposed

HIPAA

- Health orgs have competing Privacy and Interoperability mandates
- Consumers have right to data access – via APIs
- But orgs must still maintain privacy

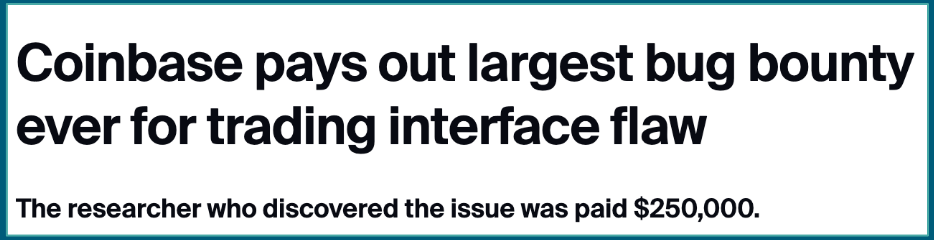
API Attack Examples

coinbase	Unauthorized trading
UNITED STATES POSTAL SERVICE	Account data harvesting
venmo	Excess data exposure
Instagram	Account takeover
bumble	Account tampering
T Mobile	SEC reporting
OPTUS	Ransom
experian	3rd party exposure

Examples highlight:

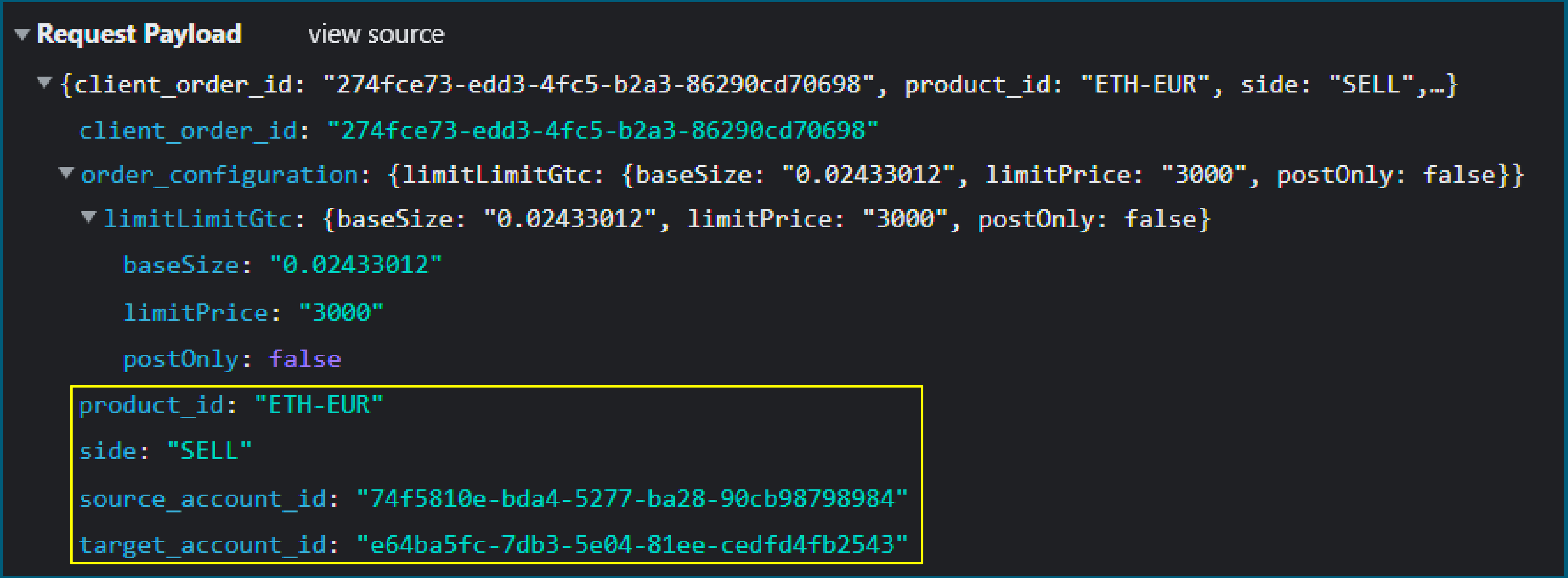
- Attacks are new/different
- Difficult to detect
- Traditional appsec tools failed to prevent
- Need to involve Dev in Security

coinbase

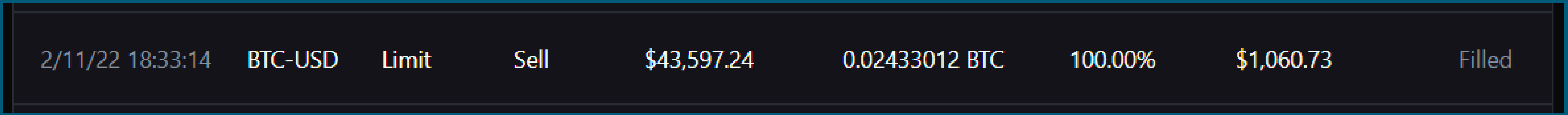


Coinbase pays out largest bug bounty ever for trading interface flaw

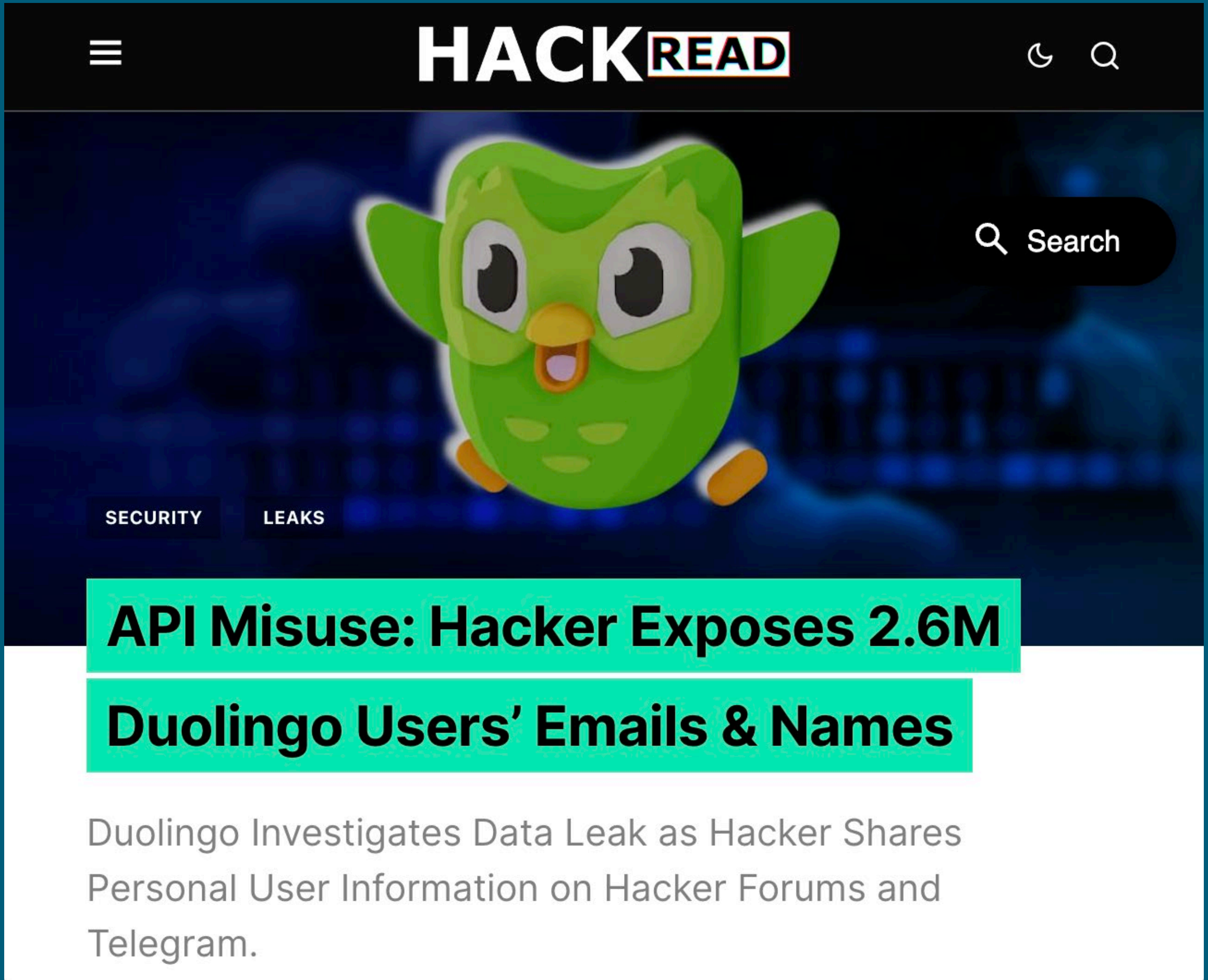
The researcher who discovered the issue was paid $250,000.



```
▼ Request Payload      view source
  ▼ {client_order_id: "274fce73-edd3-4fc5-b2a3-86290cd70698", product_id: "ETH-EUR", side: "SELL",…}
     client_order_id: "274fce73-edd3-4fc5-b2a3-86290cd70698"
    ▼ order_configuration: {limitLimitGtc: {baseSize: "0.02433012", limitPrice: "3000", postOnly: false}}
      ▼ limitLimitGtc: {baseSize: "0.02433012", limitPrice: "3000", postOnly: false}
         baseSize: "0.02433012"
         limitPrice: "3000"
         postOnly: false
     product_id: "ETH-EUR"
     side: "SELL"
     source_account_id: "74f5810e-bda4-5277-ba28-90cb98798984"
     target_account_id: "e64ba5fc-7db3-5e04-81ee-cedfd4fb2543"
```

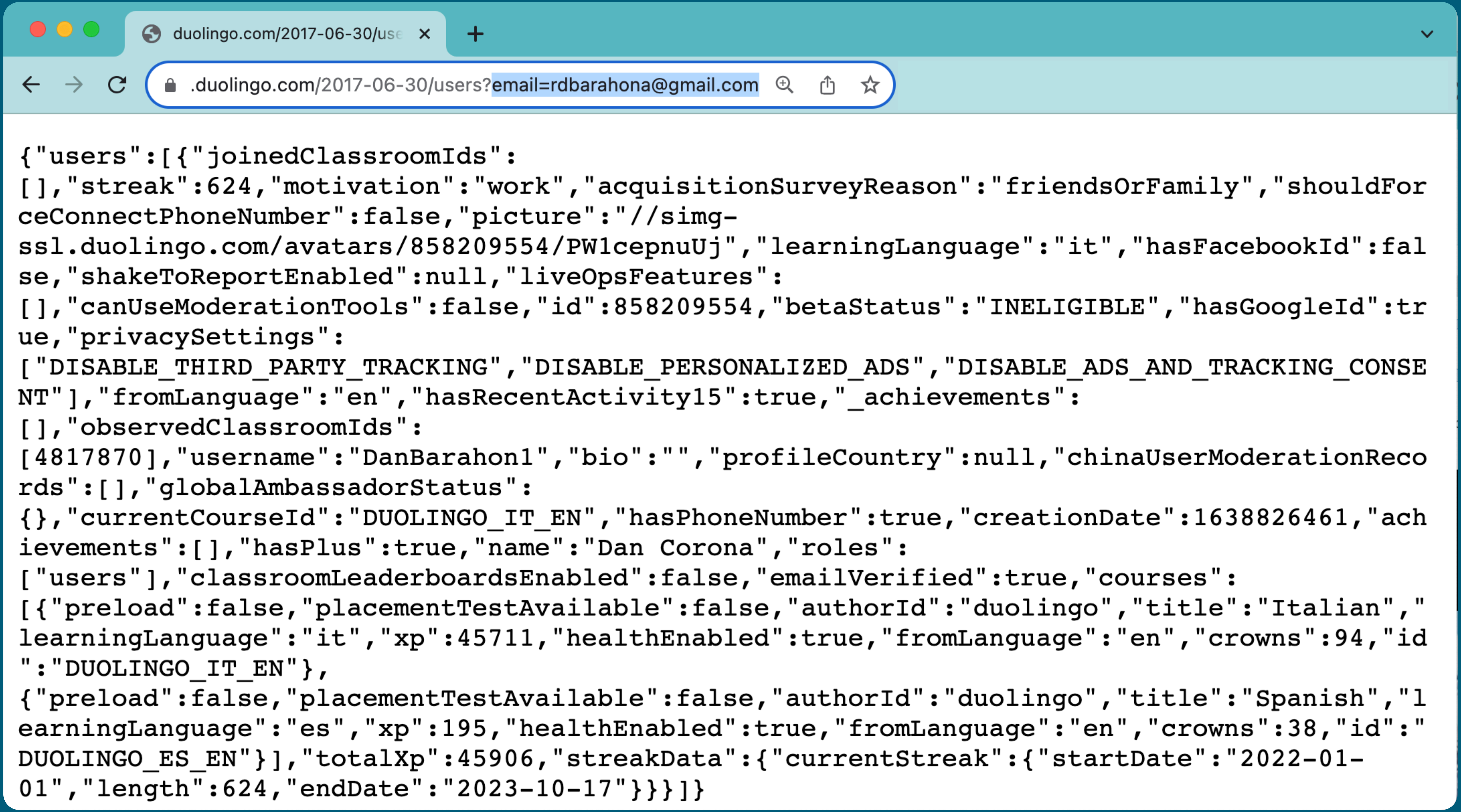


```
2/11/22 18:33:14   BTC-USD   Limit   Sell   $43,597.24   0.02433012 BTC   100.00%   $1,060.73   Filled
```



API Misuse: Hacker Exposes 2.6M Duolingo Users' Emails & Names

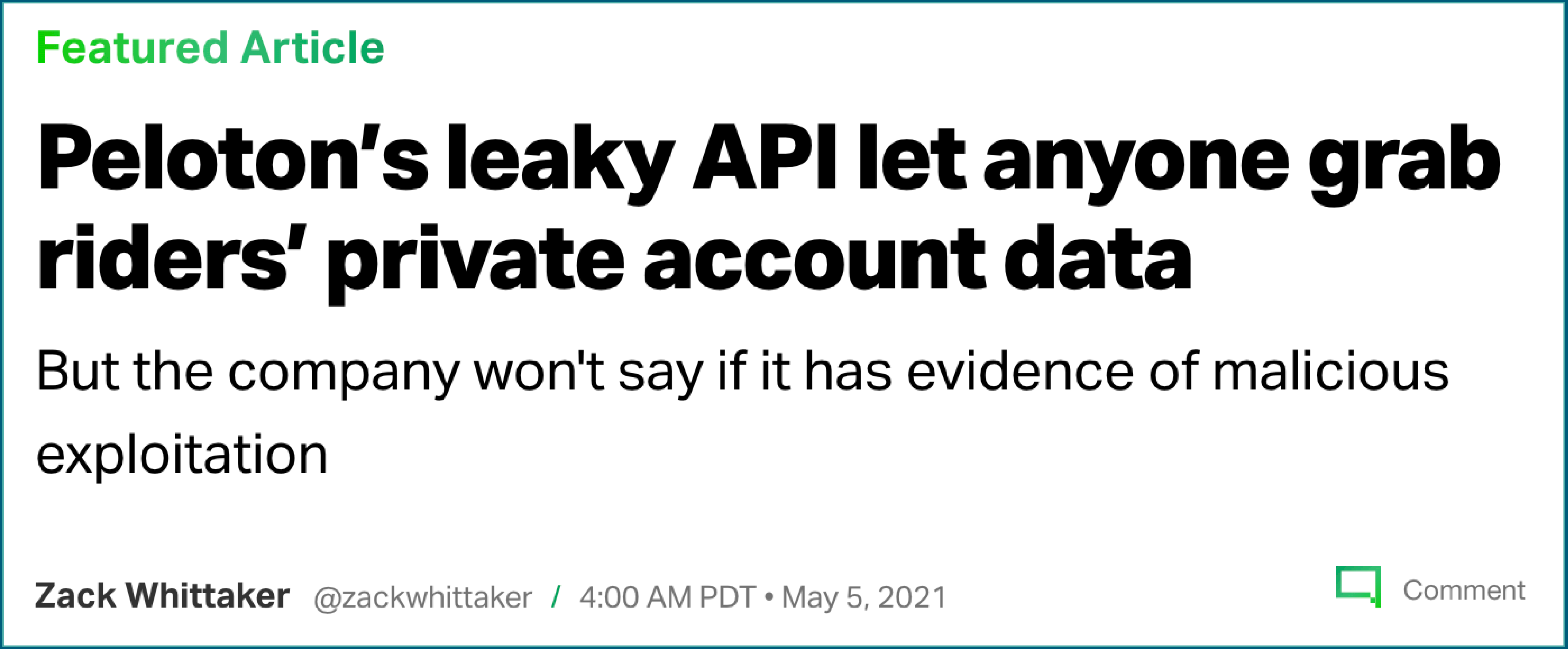
Duolingo Investigates Data Leak as Hacker Shares Personal User Information on Hacker Forums and Telegram.



duolingo.com/2017-06-30/use
.duolingo.com/2017-06-30/users?email=rdbarahona@gmail.com

```
{"users":[{"joinedClassroomIds":
[],"streak":624,"motivation":"work","acquisitionSurveyReason":"friendsOrFamily","shouldFor
ceConnectPhoneNumber":false,"picture":"//simg-
ssl.duolingo.com/avatars/858209554/PW1cepnuUj","learningLanguage":"it","hasFacebookId":fal
se,"shakeToReportEnabled":null,"liveOpsFeatures":
[],"canUseModerationTools":false,"id":858209554,"betaStatus":"INELIGIBLE","hasGoogleId":tr
ue,"privacySettings":
["DISABLE_THIRD_PARTY_TRACKING","DISABLE_PERSONALIZED_ADS","DISABLE_ADS_AND_TRACKING_CONSE
NT"],"fromLanguage":"en","hasRecentActivity15":true,"_achievements":
[],"observedClassroomIds":
[4817870],"username":"DanBarahon1","bio":"","profileCountry":null,"chinaUserModerationReco
rds":[],"globalAmbassadorStatus":
{},"currentCourseId":"DUOLINGO_IT_EN","hasPhoneNumber":true,"creationDate":1638826461,"ach
ievements":[],"hasPlus":true,"name":"Dan Corona","roles":
["users"],"classroomLeaderboardsEnabled":false,"emailVerified":true,"courses":
[{"preload":false,"placementTestAvailable":false,"authorId":"duolingo","title":"Italian","
learningLanguage":"it","xp":45711,"healthEnabled":true,"fromLanguage":"en","crowns":94,"id
":"DUOLINGO_IT_EN"},
{"preload":false,"placementTestAvailable":false,"authorId":"duolingo","title":"Spanish","l
earningLanguage":"es","xp":195,"healthEnabled":true,"fromLanguage":"en","crowns":38,"id":"
DUOLINGO_ES_EN"}],"totalXp":45906,"streakData":{"currentStreak":{"startDate":"2022-01-
01","length":624,"endDate":"2023-10-17"}}}]}
```

PELOTON



Featured Article

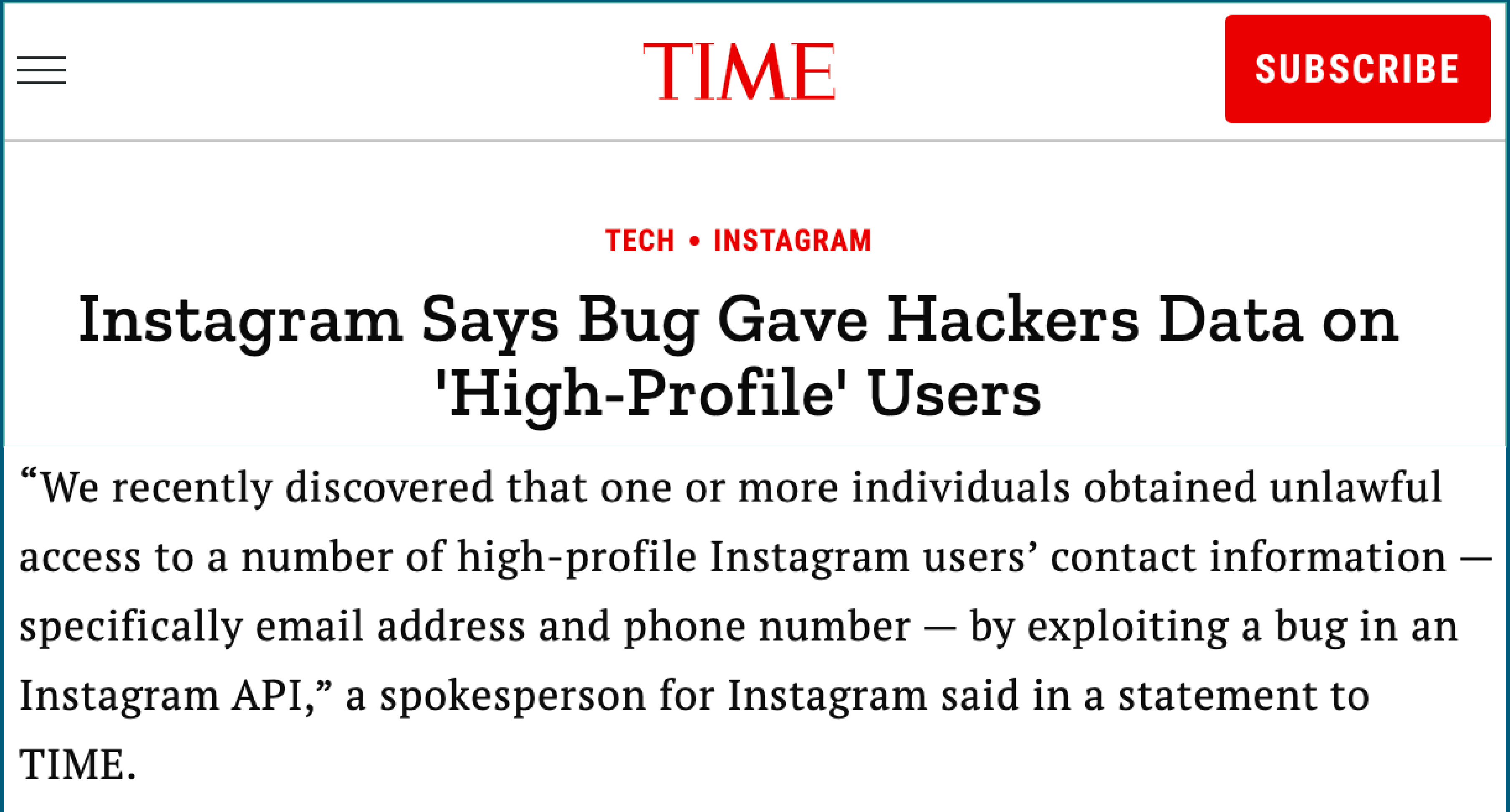
Peloton’s leaky API let anyone grab riders’ private account data

But the company won't say if it has evidence of malicious exploitation

Zack Whittaker @zackwhittaker / 4:00 AM PDT • May 5, 2021

Pro Tip: Authentication != Authorization

Instagram

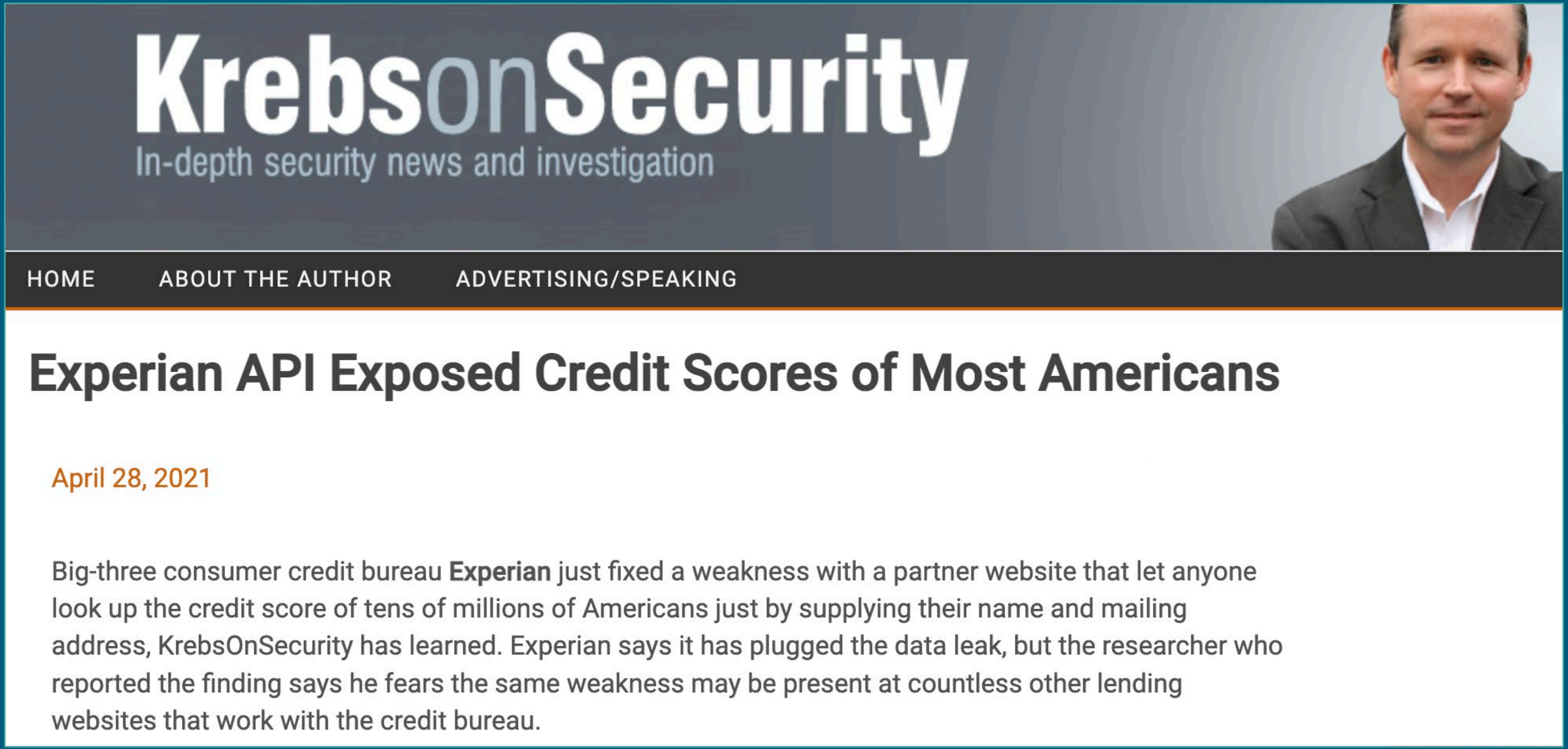


TECH • INSTAGRAM

Instagram Says Bug Gave Hackers Data on 'High-Profile' Users

“We recently discovered that one or more individuals obtained unlawful access to a number of high-profile Instagram users’ contact information — specifically email address and phone number — by exploiting a bug in an Instagram API,” a spokesperson for Instagram said in a statement to TIME.

experian™

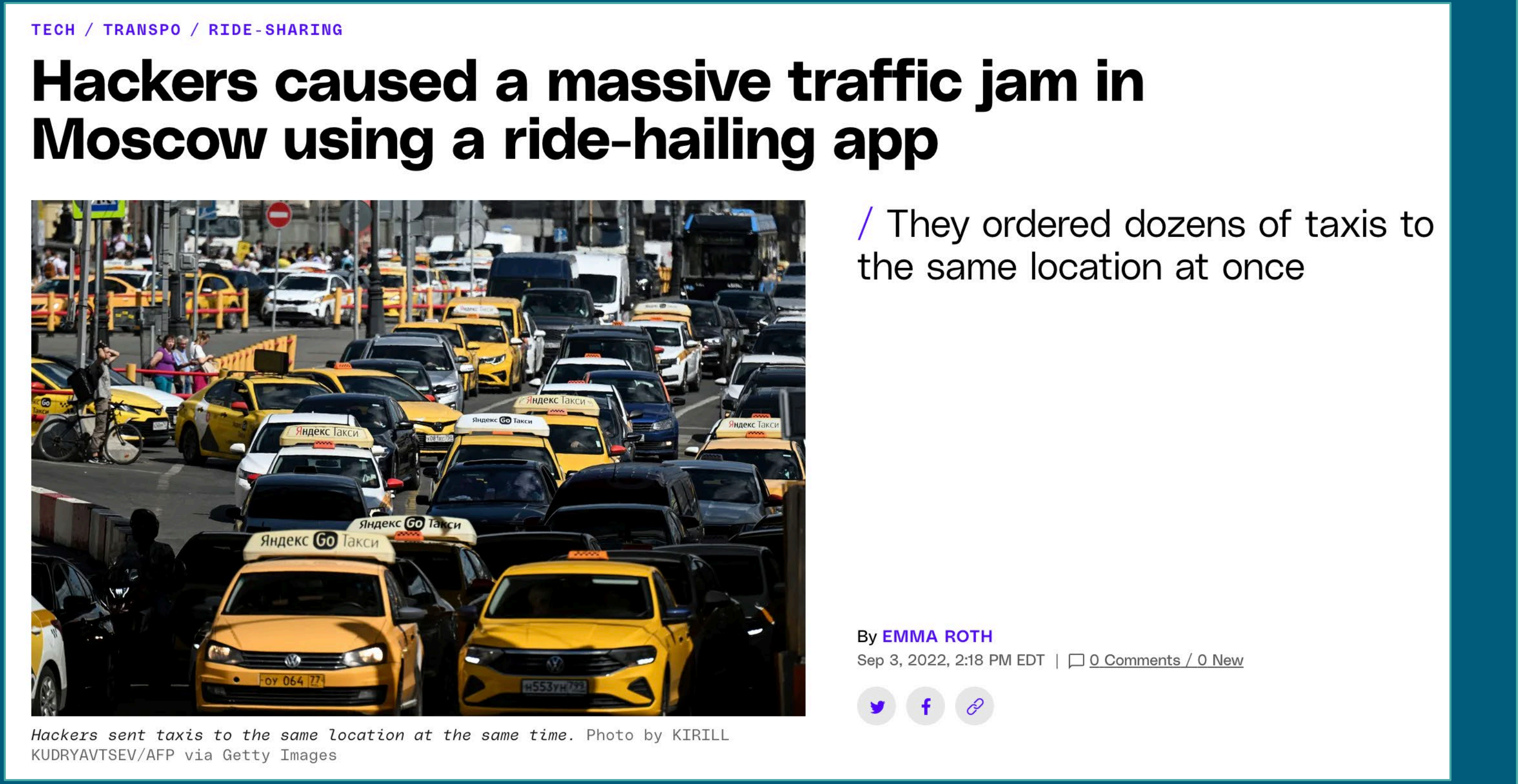


Experian API Exposed Credit Scores of Most Americans

April 28, 2021

Big-three consumer credit bureau **Experian** just fixed a weakness with a partner website that let anyone look up the credit score of tens of millions of Americans just by supplying their name and mailing address, KrebsOnSecurity has learned. Experian says it has plugged the data leak, but the researcher who reported the finding says he fears the same weakness may be present at countless other lending websites that work with the credit bureau.

Yandex



TECH / TRANSPO / RIDE-SHARING

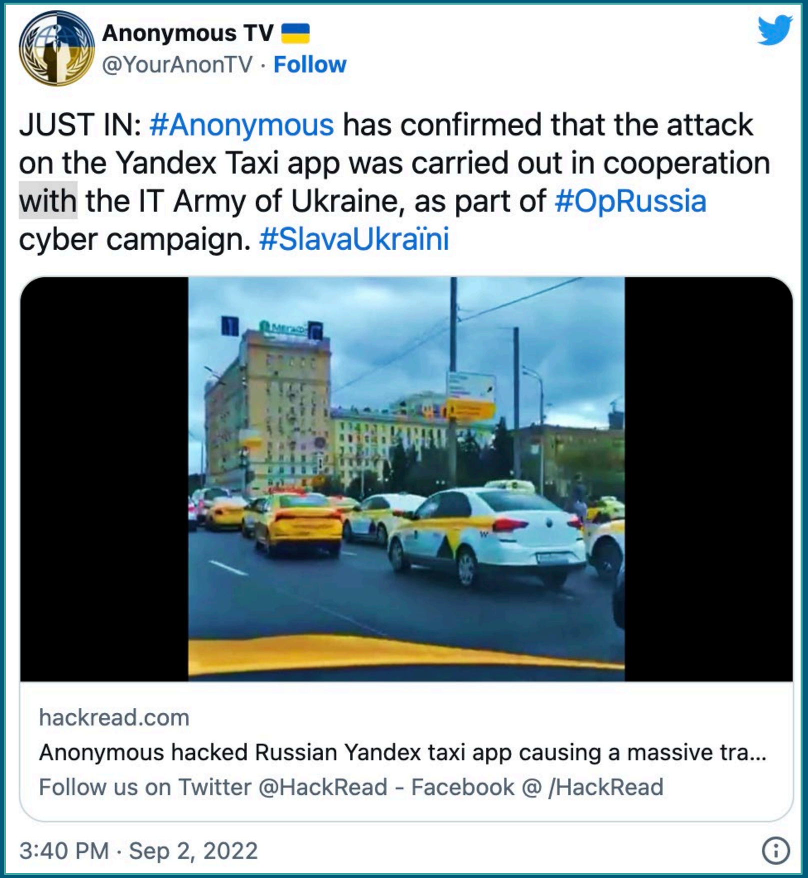
Hackers caused a massive traffic jam in Moscow using a ride-hailing app

/ They ordered dozens of taxis to the same location at once

Hackers sent taxis to the same location at the same time. Photo by KIRILL KUDRYAVTSEV/AFP via Getty Images

By EMMA ROTH

Sep 3, 2022, 2:18 PM EDT | 0 Comments / 0 New



Anonymous TV 🇺🇦
@YourAnonTV · Follow

JUST IN: #Anonymous has confirmed that the attack on the Yandex Taxi app was carried out in cooperation with the IT Army of Ukraine, as part of #OpRussia cyber campaign. #SlavaUkraïni

hackread.com
Anonymous hacked Russian Yandex taxi app causing a massive tra...
Follow us on Twitter @HackRead - Facebook @ /HackRead

3:40 PM · Sep 2, 2022

OWASP API Security Top 10 (2023)

API1	Broken Object Level Authorization
API2	Broken Authentication
API3	Broken Object Property Level Authorization
API4	Unrestricted Resource Consumption
API5	Broken Function Level Authorization
API6	Unrestricted Access to Sensitive Business Flows
API7	Server Side Request Forgery
API8	Security Misconfiguration
API9	Improper Inventory Management
API10	Unsafe Consumption of APIs

What’s Missing from Top 10?

- Injections
- Logging & Monitoring
- Business Logic

Which OWASP Stood Out in Breaches?

API1	Broken Object Level Authorization
API2	Broken Authentication
API3	Broken Object Property Level Authorization
API4	Unrestricted Resource Consumption
API5	Broken Function Level Authorization
API6	Unrestricted Access to Sensitive Business Flows
API7	Server Side Request Forgery
API8	Security Misconfiguration
API9	Improper Inventory Management
API10	Unsafe Consumption of APIs

What's Missing from Top 10?

- Injections
- Logging & Monitoring
- Business Logic

The 3 Pillars of API Security

Governance

Developing secure APIs

Testing

Ensuring APIs are free of flaws

Monitoring

Detecting threats in production

Governance

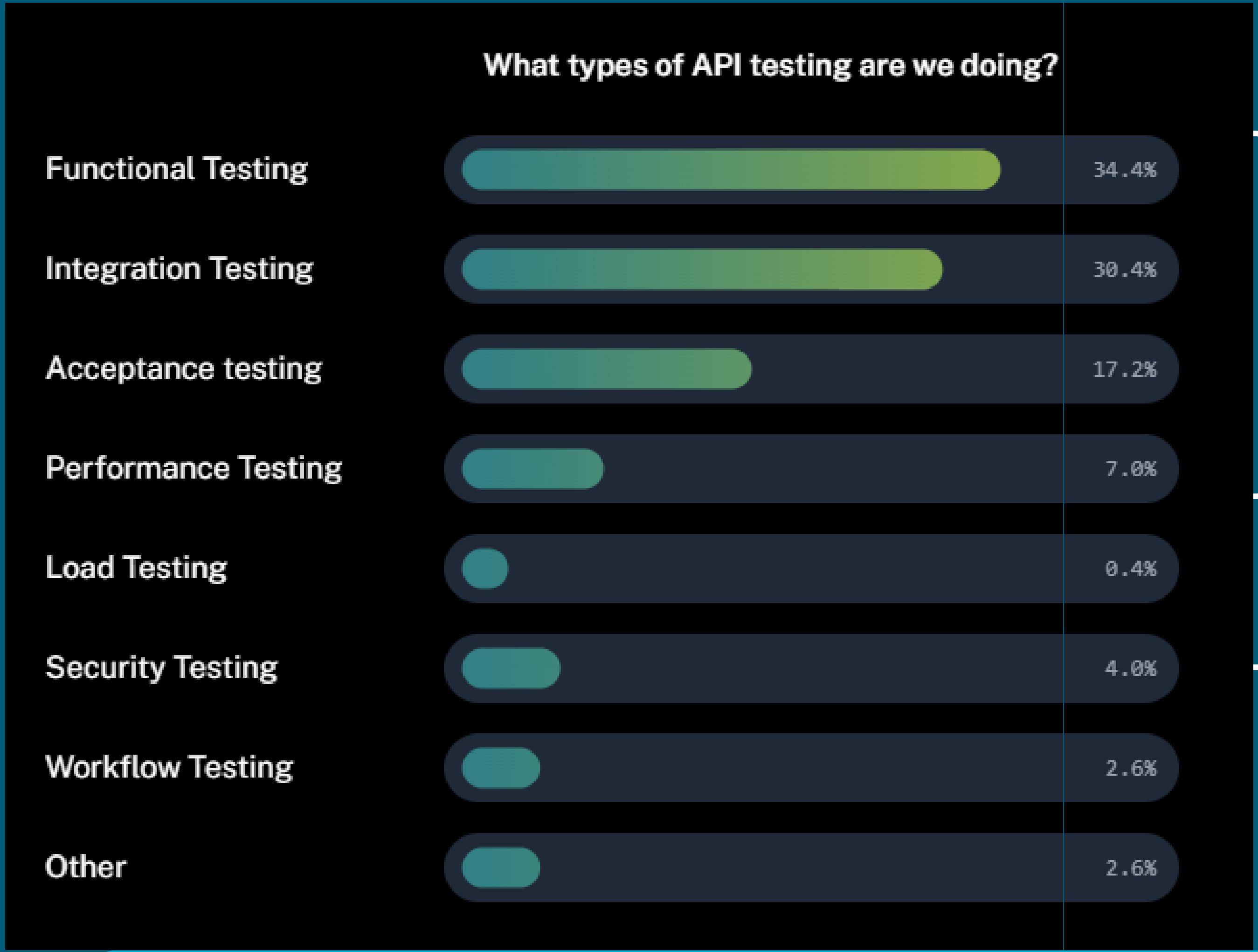
Awareness

- Know your APIs
- Know your data
- Know your risks

Policy & Process

- API Dev process
- API documentation
- Style guides

Testing



Does it do what it’s designed to do

Does it not do what it’s not designed to do

Pro Tip: train Devs on API risks & testing

Testing Categories

Security

- Unsecured Endpoints
- Authentication exploits
- Incremental IDs
- App DOS, rate limiting
- Missing TLS, SSL issues
- Injection, XSS
- Fuzzing, input validation
- Server-side request forgery
- Server properties leaks

Data

- Access control
- Excessive data exposure
- Sensitive data exposure
- Personal, health, bank data
- File, directory exposure
- Encryption at rest
- Data exfiltration

Logic

- Object ID manipulation
- Cross-account access
- API function abuse
- Role-based access control
- Authorization gaps

Monitoring

Runtime Protection

- Policy enforcement
- Authentication
- Traffic filtering

Threat Detection

- Fraudulent traffic
- Volumetric attacks
- Incident response

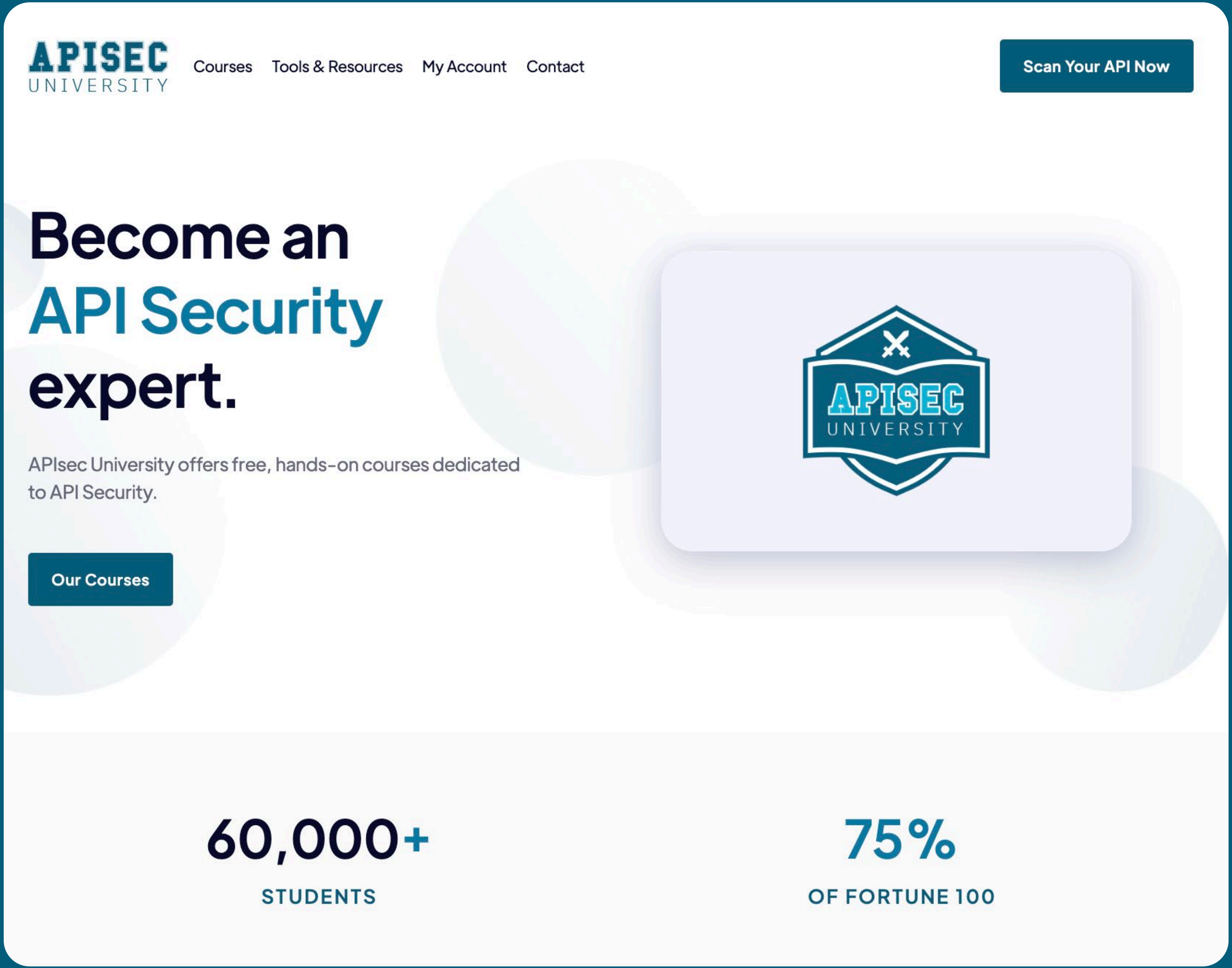
Control Validation

- Verify API controls
- Uncover anomalies

Pro Tip: Monitoring is reactive, can’t detect all API attacks

API Security Best Practices – Top 10

1. Start with Governance
2. Know Your APIs Ecosystem
3. Get Sec & Dev talking
4. API Docs Non-Negotiable
5. Train API Devs/Owners
6. Centralize API Management
7. Don’t Trust Anything
8. Don’t rely on UIs for Security
9. Authentication != Authorization
10. Automate Pre-Prod Testing



APISEC UNIVERSITY

Courses Tools & Resources My Account Contact

Scan Your API Now

Become an API Security expert.

APIsec University offers free, hands-on courses dedicated to API Security.

Our Courses

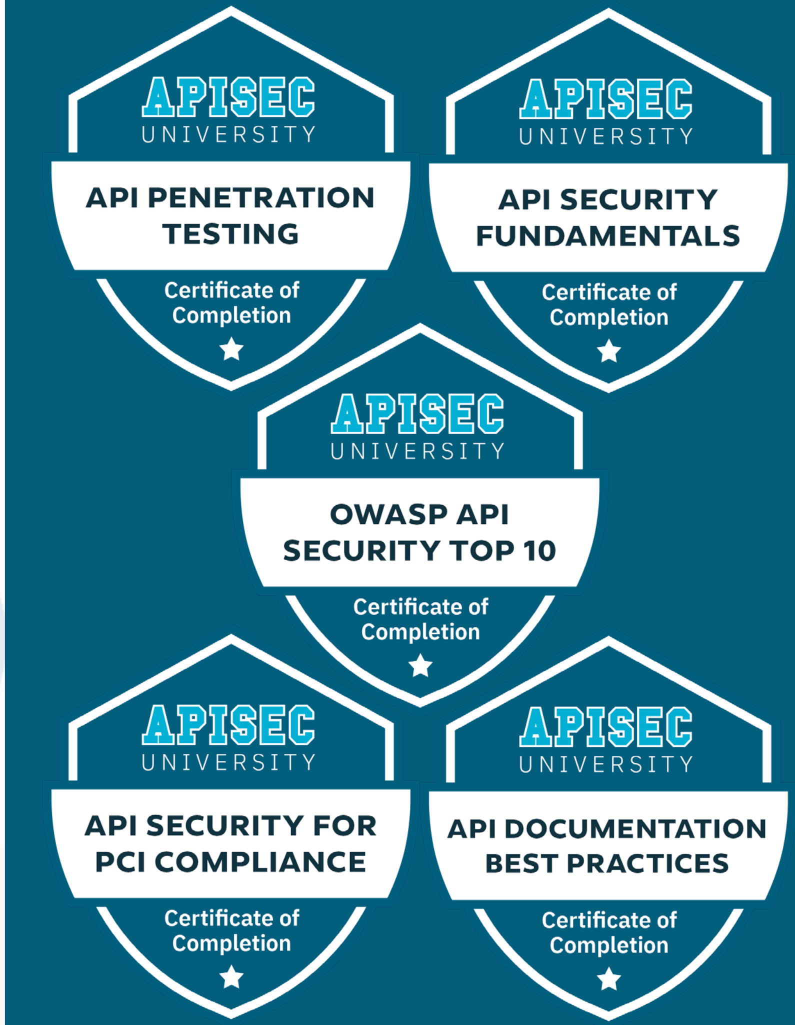
APISEC UNIVERSITY

60,000+

STUDENTS

75%

OF FORTUNE 100


APISEC UNIVERSITY
API PENETRATION TESTING
Certificate of Completion
APISEC UNIVERSITY
API SECURITY FUNDAMENTALS
Certificate of Completion
APISEC UNIVERSITY
OWASP API SECURITY TOP 10
Certificate of Completion
APISEC UNIVERSITY
API SECURITY FOR PCI COMPLIANCE
Certificate of Completion
APISEC UNIVERSITY
API DOCUMENTATION BEST PRACTICES
Certificate of Completion

Thank you!

Dan Barahona
dan@apisecuniversity.com

APISEC
UNIVERSITY

Open Discussion

Any questions about the Auto-ISAC or future topics for discussion?

How to Get Involved: Membership

If you are an OEM, supplier or commercial vehicle, Carrier or Fleet, please join the Auto-ISAC!

- *Real-time Intelligence Sharing*
- *Intelligence Summaries*
- *Regular intelligence meetings*
- *Crisis Notifications*
- *Member Contact Directory*
- *Development of Best Practice Guides*
- *Exchanges and Workshops*
- *Tabletop exercises*
- *Webinars and Presentations*
- *Annual Auto-ISAC Summit Event*

To learn more about Auto-ISAC Membership and Partnership, please contact melissacromack@automotiveisac.com.

Auto-ISAC Partnership Programs

Strategic Partnership

- **For-profit** companies such as "Solutions Providers" that sell connected vehicle cybersecurity products & services.
- **Examples:** *Hacker ONE, Upstream, IOActive, Karamba, Grimm*

1. **Must be approved** by Executive Director and the Membership & Benefit Standing Committee (MBSC).
2. Formal agreements: **NDA, SPA, SoW, CoC** required.
3. **In-kind contributions** allowed. Currently no fee.
4. **Does not** overtly sell or promote product or service.
5. Commits to **support the Auto-ISAC's mission.**
6. Engages with the automotive ecosystem, **supporting & educating Auto-ISAC Members and its Community.**
7. **Develops value added Partnership Projects** to engage with the Auto-ISAC, its Member, and Community.
8. **Summit Sponsorship** allowed for promotion. Summit Booth **priority**.
9. Engagement **must provide Member awareness, education, training, and information sharing**
10. **Builds relationships, shares, and participates** in information sharing Auto-ISAC activities.
11. Supports our mission through **educational webinars and sharing of information.**

Community Partnership

- **Community Partners** are companies, individuals, or organizations with a complementary mission to the Auto-ISAC, with the interest in engaging with the automotive ecosystem, supporting, and educating Members and the community.
- Includes ***Industry Associations, Government Partners, Academia, Research Institution, Standards Organizations, Non- Profit, Technical Experts, Auto-ISAC Sponsors*****.**
- **Examples:** *Autos Innovate, ATA, ACEA, JAMA, MEMA,CLEPA, CISA, DHS, FBI, NHTSA, NCI, UDM etc.*

1. **No formal agreement** required.
2. **No approval** required.
3. Added to **Auto-ISAC Community Distro** List to stay engaged in Community events and activities.
4. Participate in **Auto-ISAC Monthly Community Calls.**
5. Learn **what is trending** in the ISACs and hear from key leaders during the **special topic of interest** presentation.
6. Added to **Auto-ISAC DRIVEN** list to receive our **daily cyber automotive newsletter.**
7. Part of the Network with **Automotive Community and the extended automotive ecosystem.**
8. Invitation to **attend and support** our yearly Summit.

Current Partnerships

Many organizations engaging

Thanks for your Support to our Many Partners

Community Partners

INNOVATOR

Strategic Partnership (20)

ArmorText
BlockHarbor
Cybellum
Deloitte
FEV
GRIMM
HackerOne
Irdeto
Itemis
Karamba Security
KELA
Pen Testing Partners
Red Balloon Security
Regulus Cyber
Saferide
Security Scorecard
Trustonic
Upstream
VicOne
Vultara

NAVIGATOR

Support Partnership

AAA
ACEA
ACM
American Trucking Associations (ATA)
ASC
ATIS
Auto Alliance
EMA
Global Automakers
IARA
IIC
JAMA
MEMA
NADA
NAFA
NMFTA
RVIA
SAE
TIA
Transport Canada

COLLABORATOR

Coordination Partnership

AUTOSAR
Billington Cybersecurity
Cal-CSIC
Computest
Cyber Truck Challenge
DHS CSVI
DHS HQ
DOT-PIF
FASTR
FBI
GAO
ISAO
Macomb Business/MADCAT
Merit (training, np)
MITRE
National White Collar Crime Center
NCFTA
NDIA
NHTSA
NIST
Northern California Regional Intelligence Center (NCRIC)
NTIA
OASIS
ODNI
Ohio Turnpike & Infrastructure Commission
SANS
The University of Warwick
TSA
University of Tulsa
USSC
VOLPE
W3C/MIT
Walsh College

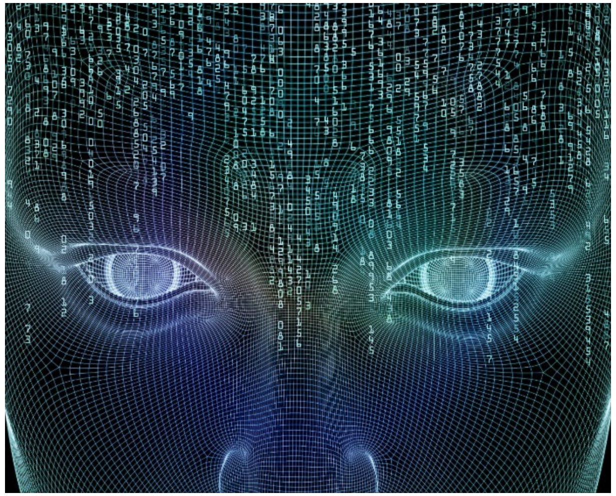
BENEFACTOR

Sponsorship Partnership

2022 Summit Sponsors-
Argus
BGNetworks
Bosch
Blackberry
Block Harbor
BlueVoyant
Booz Allen Hamilton
C2A
Cybellum
CyberGRX
Cyware
Deloitte
Denso
Finite State
Fortress
Itemis
Keysight Technologies
Micron
NXP
Okta
Sandia
Securonix
Tanium
UL
Upstream
VicOne

Auto-ISAC Benefits

- Focused Intelligence Information/Briefings
- Cybersecurity intelligence sharing
- Vulnerability resolution
- Member to Member Sharing
- Distribute Information Gathering Costs across the Sector
- Non-attribution and Anonymity of Submissions
- Information source for the entire organization
- Risk mitigation for automotive industry
- Comparative advantage in risk mitigation
- Security and Resiliency

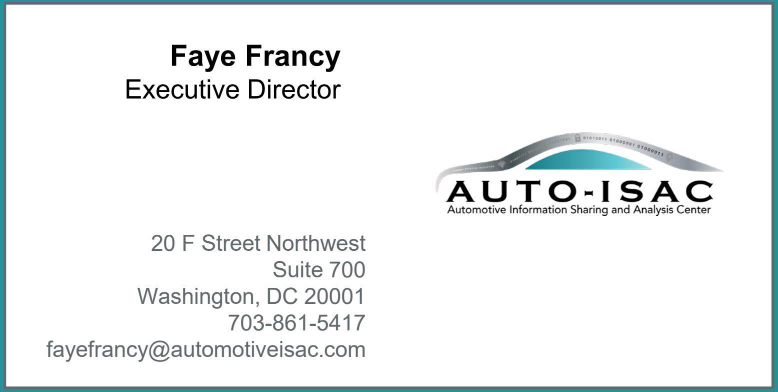


Building Resiliency Across the Auto Industry

Thank You

THANK
YOU
MAAKE
JUSPAXAR
OBRIGADO
MATONDO
SALAMAT
KIITOS
MOCHCHAKKERAM
KIA ORA
MULTUMESC
CHOKRANE
TERMA KASIH
RAIBH MAITH AGAT
GRAZIE
MULTUMESC
MERCI
SALAMAT
CAM ON BAN
MERCI
RAIBH MAITH AGAT
MERCI
MOCHCHAKKERAM
OBRIGADO
MOCHCHAKKERAM
GRAZIE
ASANTE
CHOKRANE
MATUR NUWUN
UA TSAUG RAU KOJ
MOCHCHAKKERAM
MATONDO
WELALIN
KIITOS
CHOKRANE
UA TSAUG RAU KOJ
DANK JE
RAIBH MAITH AGAT
SPASIBO
SPASIBO
MAAKE
OBRIGADO
ARIGATO
KIITOS
DANKON
MOCHCHAKKERAM
NIRRINGRAZZJAK
MOCHCHAKKERAM
OBRIGADO
SPASIBO
MULTUMESC
VINAKA
NIRRINGRAZZJAK
MAMANA
OBRIGADO
DANK JE

Our Contact Info



Faye Francy
Executive Director

AUTO-ISAC
Automotive Information Sharing and Analysis Center

20 F Street Northwest
Suite 700
Washington, DC 20001
703-861-5417
fayefrancy@automotiveisac.com

AUTO-ISAC
Automotive Information Sharing and Analysis Center

AUTOMOTIVEISAC.COM