Mobile Vulnerabilities and Threats

Keep Things in Perspective

- Our mission is to expose as many vulnerabilities as we can
  - It's fun!
- Keep a reasonable perspective about risk
  - What is the real-life risk associated with the vulnerability?

Mobile App vs. Traditional App Security

- Development
  - Rush to market
  - Focus on ease of use
  - Inexperienced developers
- Attack Surface
  - Fewer, but different attack surfaces than desktop machine
- Platform
  - Multiple sensors that gather information
- Network
  - Not connected to protected network
  - Wifi, LTE, Bluetooth, NFC, USB
- Not physically protected
  - Loss or theft of device

Example Exploits, Tools, and Techniques

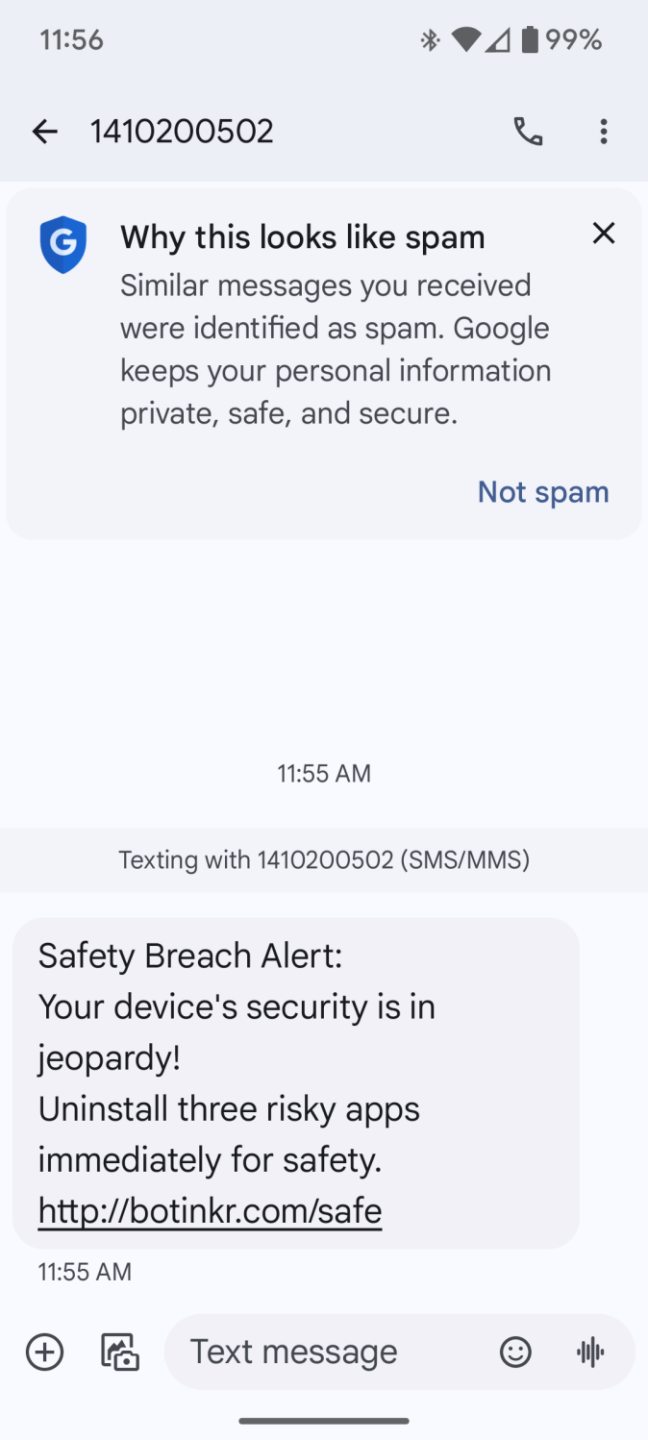
Examples of mobile vulnerabilities and exploits:

Surveillance vulnerabilities	Audio attack	This involves switching on the microphone to listen in on conversations.
Financial vulnerabilities	Stealing transaction codes	This technique is commonly used for man-in-the-middle attacks against online banking sites. Also vulnerable to NFC attacks.

Example Exploits, Tools, and Techniques (Cont.)

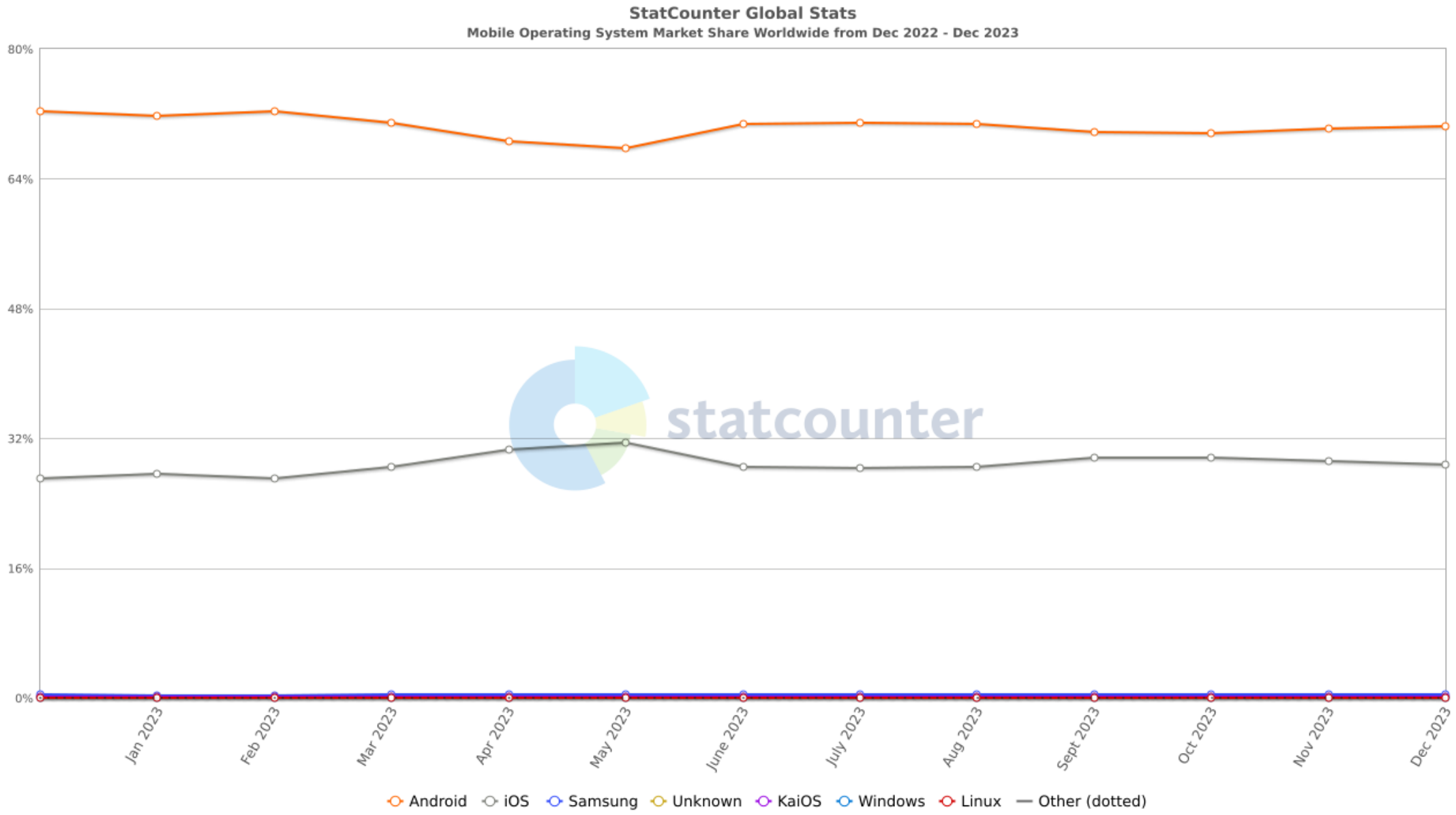
Botnet activity	Participating in distributed denial of service (DDoS) attacks and crypto mining	This involves hijacking the phone to participate in mass attacks on a third-party network—for example, by sending out Domain Name System (DNS) or Network Time Protocol (NTP) requests.
Data theft	Communications	E-mails and SMS messages are all open to theft.
Impersonation	Sending SMS messages	This involves sending false messages to collect information from contacts or to engage in illegal or illicit activities (including harassing the user).

Message Received Today

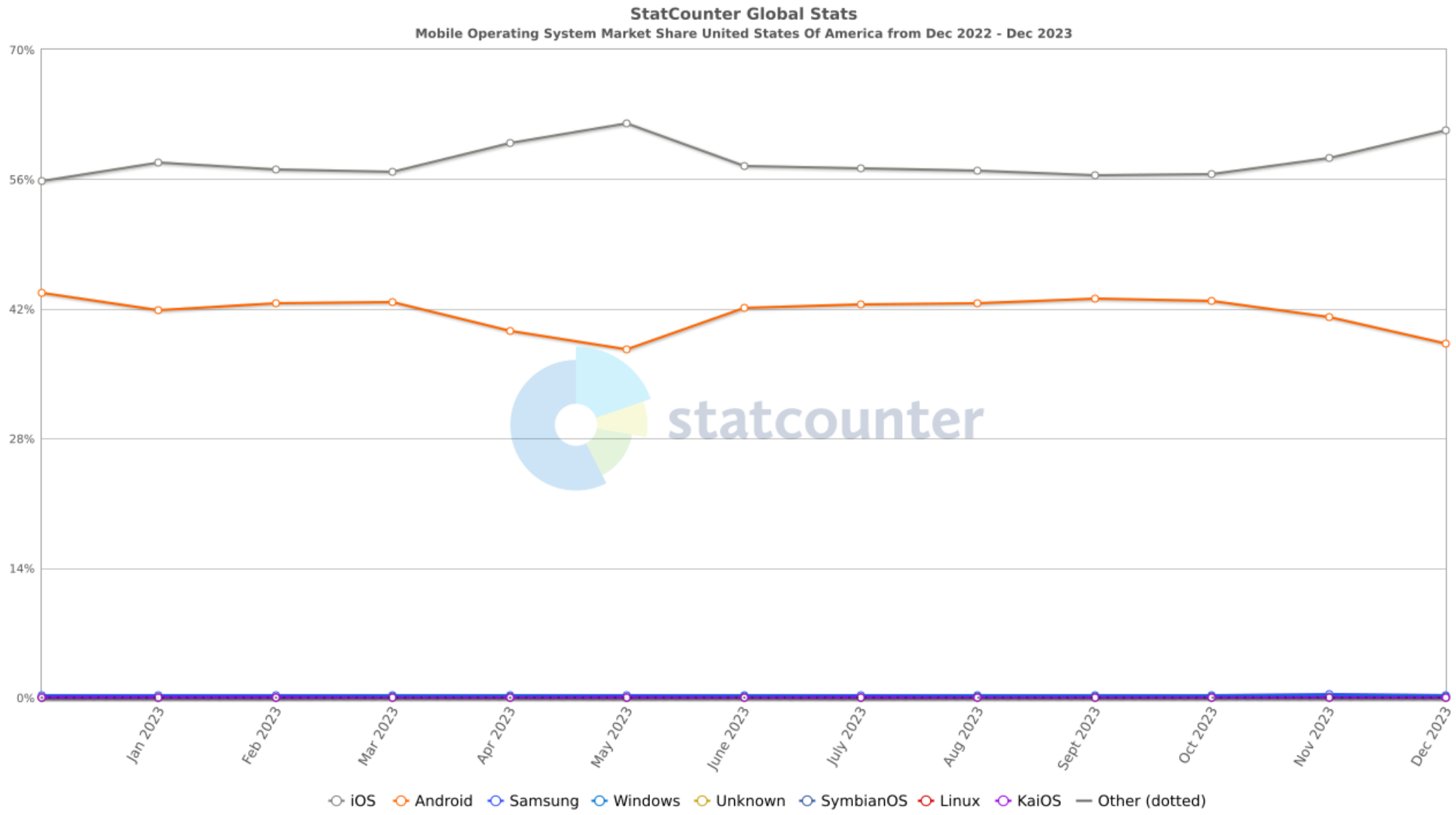


Mobile Vulnerabilities

Identified Weaknesses in the OS

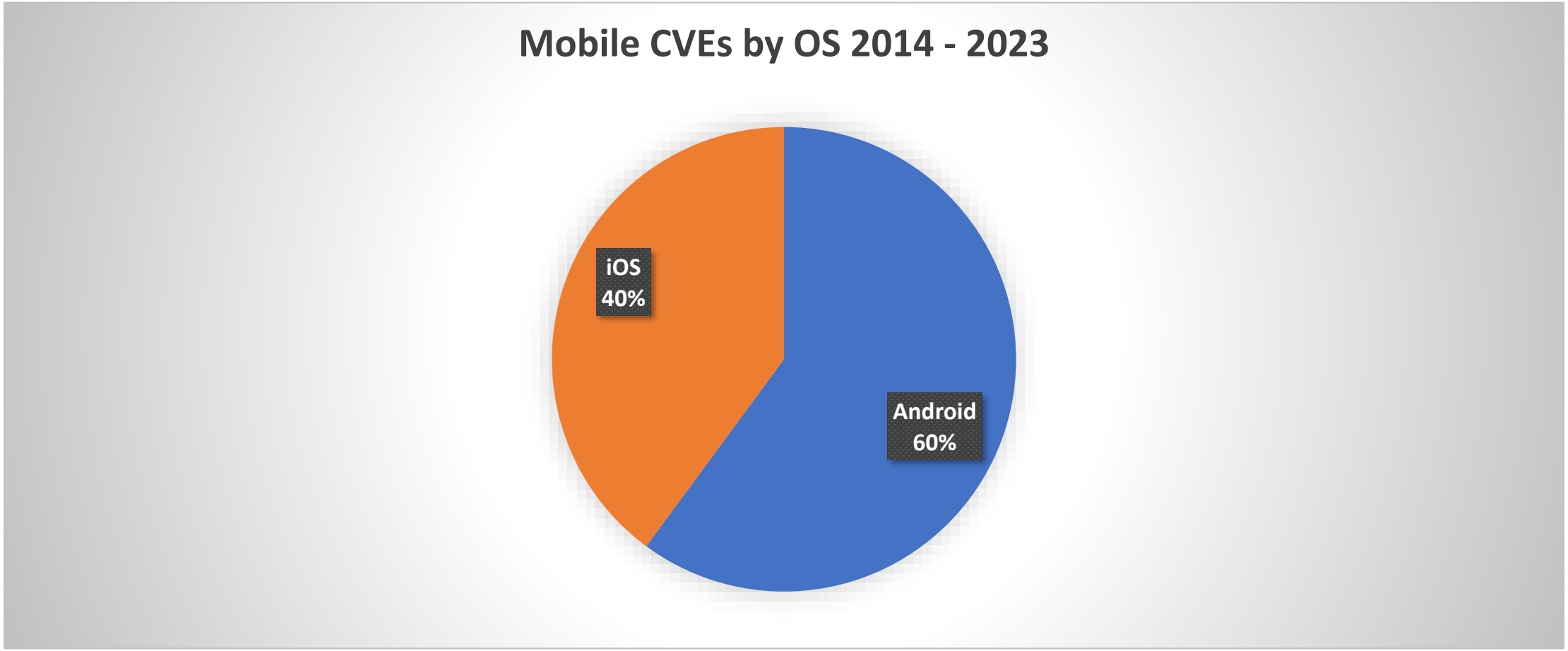


Source: https://gs.statcounter.com/os-market-share/mobile/worldwide



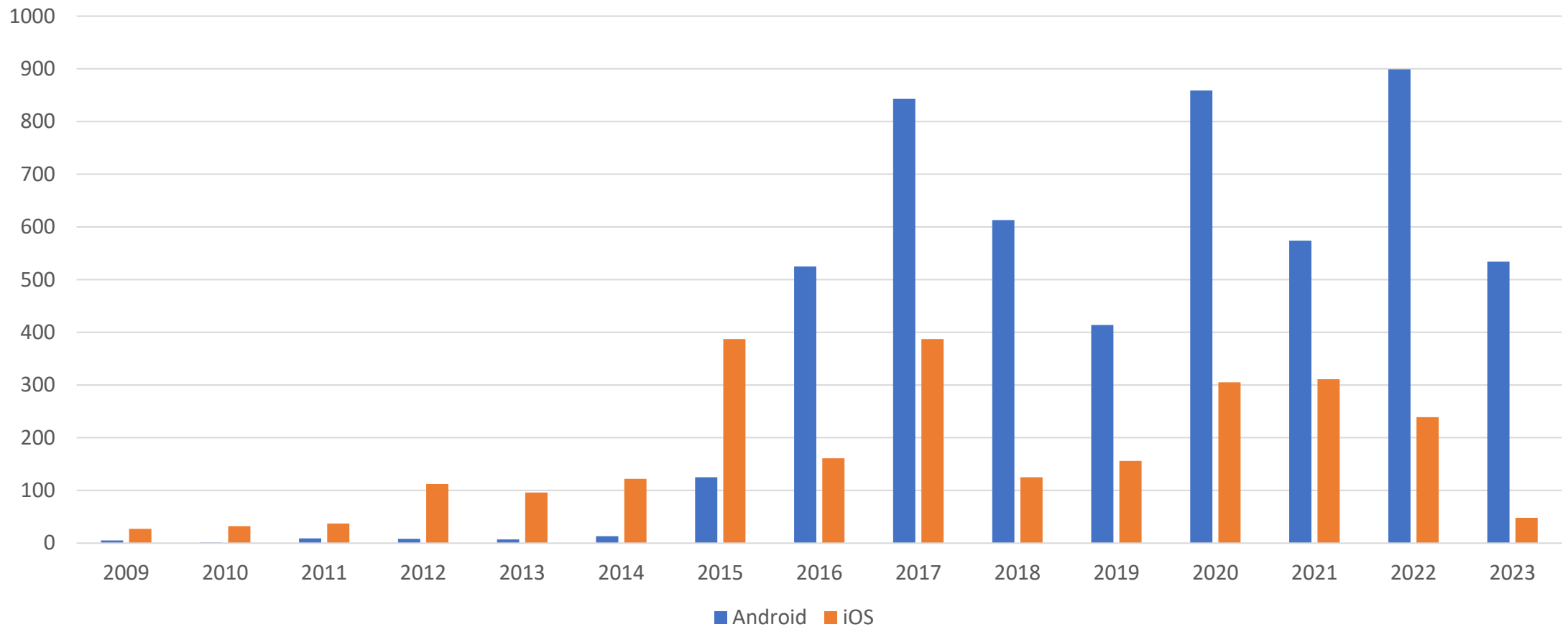
Source: https://gs.statcounter.com/os-market-share/mobile/united-states-of-america

OS Vulnerabilities



Sources:
https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224
https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49

OS Vulnerabilities



Sources:
https://www.cvedetails.com/product/19997/Google-Android.html?vendor_id=1224
https://www.cvedetails.com/product/15556/Apple-Iphone-Os.html?vendor_id=49

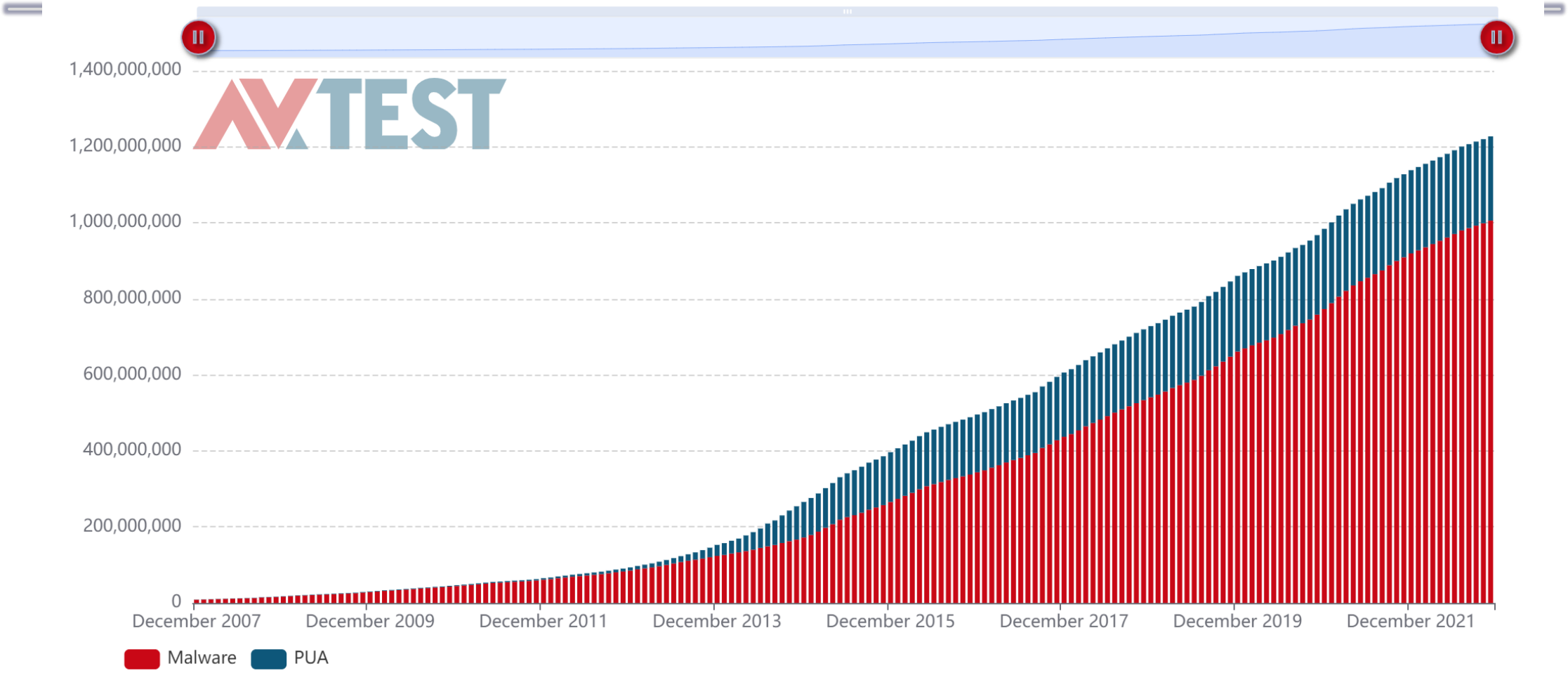
Latest CVEs

- https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/Google-Android.html
- https://www.cvedetails.com/vulnerability-list/vendor_id-49/product_id-15556/Apple-Iphone-Os.html

Malware on Android Devices

- Main driver is that the Android OS is an open source system
- Android OS is actually very secure
- Susceptibility to malware is more a function of software fragmentation among vendors, poor user administration, and poor update-management practices
- Google must identify vulnerabilities and engineer security patches, make them available to device manufacturers that host Android
  - Device manufacturers must test with their equipment/network and add their bloatware

Android Malware Development



Source: https://www.av-test.org/en/statistics/malware/

iOS Malware

- Statistics may be limited as it is difficult to find with scans
- Amount of iOS malware is small, but growing
  - https://theapplewiki.com/wiki/Malware_for_iOS
- Most infections are due to clicking a link or state-sponsored applications
- Malware uses sideloading from unauthorized app stores and progressive web apps
  - Apple contends sideloading will increase malware
  - Apple claims it will still monitor and charge for sideloading
- Malware tends to focus on older versions of iOS or jailbroken phones
- Roughly 50 percent of iPhones in China have been jailbroken

iOS Malware Examples

- https://www.jamf.com/blog/ios-trojan-malware/
- https://macpaw.com/how-to/most-common-iphone-viruses

Mobile Threat Models

Open Web Application Security Project (OWASP) Top 10

- Mobile Top 10
  - https://owasp.org/www-project-mobile-top-10/

NIST Mobile Threat Categories

- Mobile Threat Catalogue

MITRE ATTACK Mobile

- https://attack.mitre.org/versions/v12/matrices/mobile/

Mobile Threat Actors and Malware

Criminal and Developer Collaboration

- Security experts suspect broad collaboration between cybercriminals and dubious Android developers who focus their attention on Android malware
- Potentially unwanted applications (PUAs) and commercial mobile adware (madware)
  - Things we would love to find!
- Popular goals are:
  - Mining crypto currency
  - Gaining control of phone file systems to steal data, photos, and the like, or to lock out the user for ransom
  - Gaining control of features, such as the camera and microphone, for surveillance or location tracking—prevalent in commercial and business espionage and cyberstalking

Criminal and Developer Collaboration

- Typical targets:
  - Unsecure data storage
  - Weak server-side controls
  - Insufficient Transport Layer protection
  - Poor authorization and authentication
  - Improper session handling
  - Data leakage
  - Poorly implemented encryption
  - Sensitive data disclosure

Madware

- A form of aggressive adware that is prevalent on mobile devices
- Developers consider madware to be harmless and legitimate
- Some free applications are not; they run background processes that access GPS information, scan address books, and send out stolen data via HTTP to third-party APIs
- Developers maintain that terms of use have been stated and user's permission has been granted; but few users read terms and conditions in their entirety

Madware Example

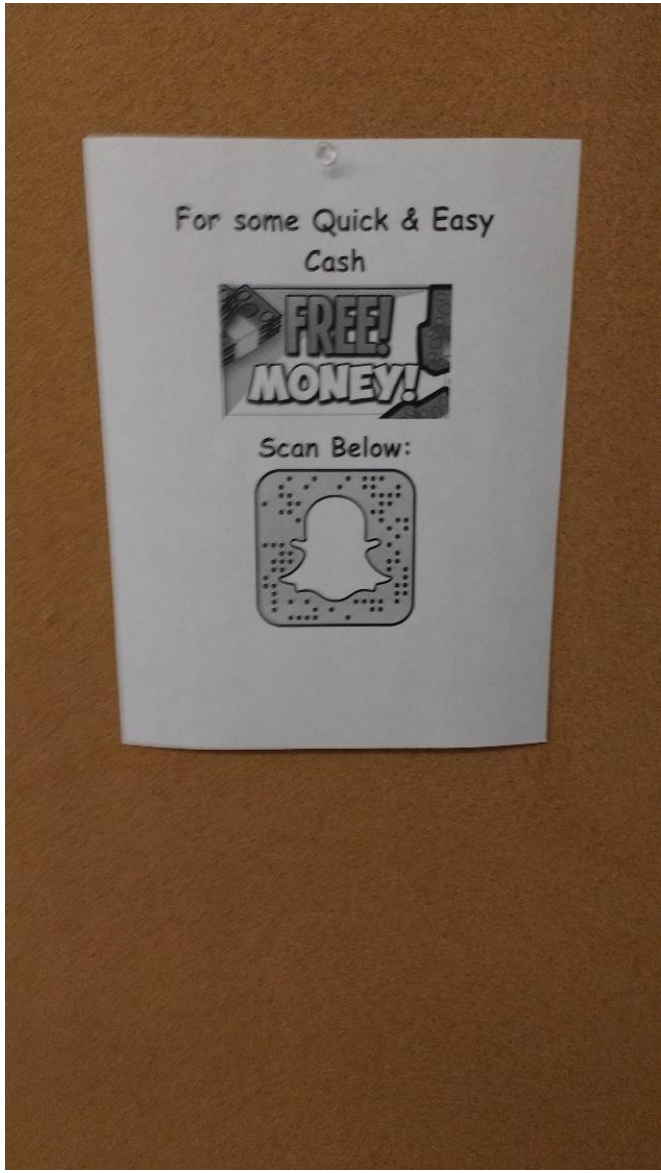
- https://www.humansecurity.com/learn/blog/traffic-signals-the-vastflux-takedown?utm_source=businesswire.com&utm_medium=press_release&utm_campaign=vastflux_2022&utm_content=link

Mobile Malware Delivery Methods

- Binding an application to a genuine popular free app available in Google Play or the App Store
- Loading malware to the many third-party stores
- Creating a Web page infected with a drive-by download
- Using a hybrid attack with a dual payload to target both PCs and smartphones
- Using social engineering
- Creating malicious QR codes for malware distribution

QR and Other Scan Codes

https://blog.pradeo.com/quishing-when-qr-code-becomes-trap



Captive Portals

- Cybercriminal launches and advertises an attractive free Wi-Fi portal
- Users join, click on links
- Takes them from captive portal to a phishing Web site, which uses JavaScript (or other means) to perform a drive-by browser attack

Drive-by Attacks

- Involves injecting malicious code into Web sites to exploit browser vulnerabilities
- The result: A user's device can be infected simply by visiting site
- Can occur on hacker Web sites specifically created to launch an attack, and on legitimate sites that have been hacked and infected with malicious code

Clickjacking

- Purpose is to confuse victim by creating a Web page with a background of invisible frames
- Attacker superimposes another set of frames or buttons visible to victim
- Some mouse clicks appear to be unresponsive, causes victim to swipe mouse around, triggering the exploit

Likejacking

- An invisible frame or button is placed directly on top of a Facebook Like button
- Clicking button works as normal, but also infects the device
- Usually successful on smartphones due to smaller screens, which are more difficult to see

Plug-and-Play Scripts

- Small screen on smartphone makes it difficult to use navigation controls
- Malware developers use JavaScript to cause any mouse click to activate target button, which infects device
- If user inadvertently clicks in wrong place (easy to do on a smartphone), causes a malware script to run

Mobile Malware and Social Engineering

- End user is weak link
  - Little security awareness
  - Equipped with powerful and intelligent smartphone
- Cybercriminals are highly collaborative
  - Able to disseminate information through own networks more quickly than information is spread in many corporations with well-defined information-dissemination processes

Mobile Threat Defense

Mitigating Mobile Browser Attacks

- Best practices:
  - Practicing due diligence
  - Using HTTPS when entering credentials
  - Maintaining robust anti-malware software – questionable on mobile devices
  - Blocking pop-ups
  - Checking app permissions
  - Removing unwanted apps
  - Switching off auto-fill dialog boxes and JavaScript
  - **Enabling fraud warnings on accounts**
  - Clearing cookies, history, and cache

Enterprise Mobile Malware Defense

- Advice for computer users is to run anti-malware and antivirus software
  - Antivirus apps on mobile devices are restricted to their sandbox and questionable value
- Follow best practices:
  - Adhere to policy using mobile device management
  - Prohibit the unlocking or jailbreaking of devices and the side-loading of apps
  - Install security patches and updates
  - Provide security-awareness training for end users
  - Prohibit applications from noncertified developers and third-party marketplaces
  - Restrict users to vetted applications

Mobile Antivirus Issues

- https://cybernews.com/security/free-cleaning-apps-put-millions-at-risk-of-hacking-says-research/

Example Insecure Apps

Source: The Worst Mobile Apps – DEFCON 28, August 2020

FTC Lawsuit Settlement

https://www.ftc.gov/news-events/press-releases/2014/03/fandango-credit-karma-set

Home » News & Events » Press Releases » Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Faili
Personal Information

Fandango, Credit Karma Settle FTC Charges that They Deceived Consumers By Failing to Securely Transmit Sensitive Personal Information

Mobile Apps Placed Credit Card Details, Credit Report Data, Social Security Numbers at Risk

SHARE THIS PAGE

FOR RELEASE

March 28, 2014

TAGS: deceptive/misleading conduct | Technology | Bureau of Consumer Protection | Consumer Protection | Privacy and Security | Consumer Privacy | Data Security

Two companies have agreed to settle Federal Trade Commission charges that they misrepresented the security of their mobile apps and failed to secure the transmission of millions of consumers' sensitive personal information from their mobile apps.

Equity Pandit

equitypandit
INVESTMENT ADVISOR

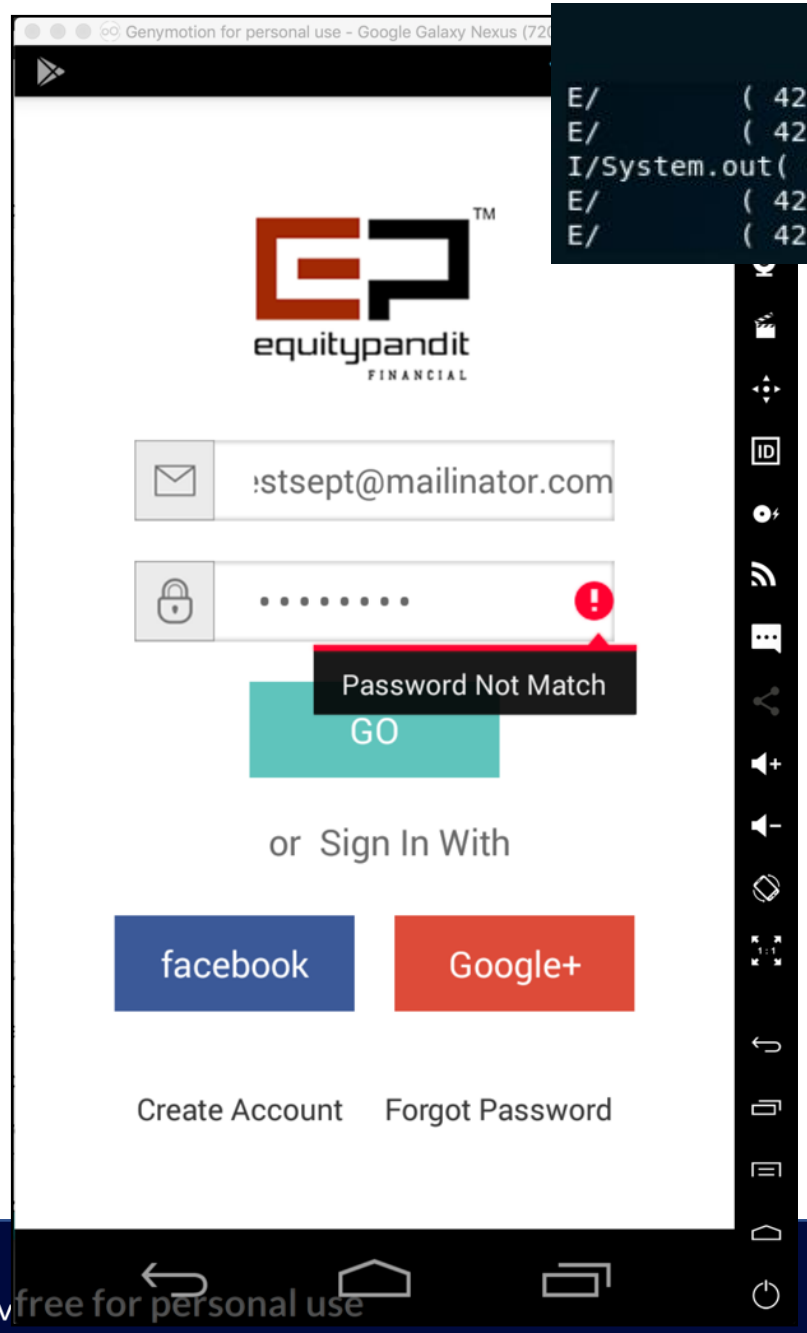
EquityPandit Featured as 'Highly Recommended Financial Advisors For 2020' by Enterprise World

March 26, 2020 AT 3:24 PM

India's leading equity research company EquityPandit, has been covered by The Enterprise World as The Highly Recommended Financial Advisor For 2020 and is been featured in the cover story of the magazine. Addressing EquityPandit as the leading equity research company of India, the Enterprise World credited it for making a better financial tomorrow. The magazine also mentioned EquityPandit as a company that is one of the biggest players with a dominant position in both Institutional and Retail.

(see more...)

An ISO 9001:2008 Certified Company




```
E/        ( 4256): Cgeck email data result: user already exist
E/        ( 4256): false case
I/System.out( 4256): EP_Login_Details checking all email
E/        ( 4256): same_id: not match
E/        ( 4256): db_password, password: P@ssw0rd, AAaa22@@
```

- Stores passwords locally
- Transmits them in plaintext
- Exposes every user's password in the API

University of Houston Alumni App Data Exposure

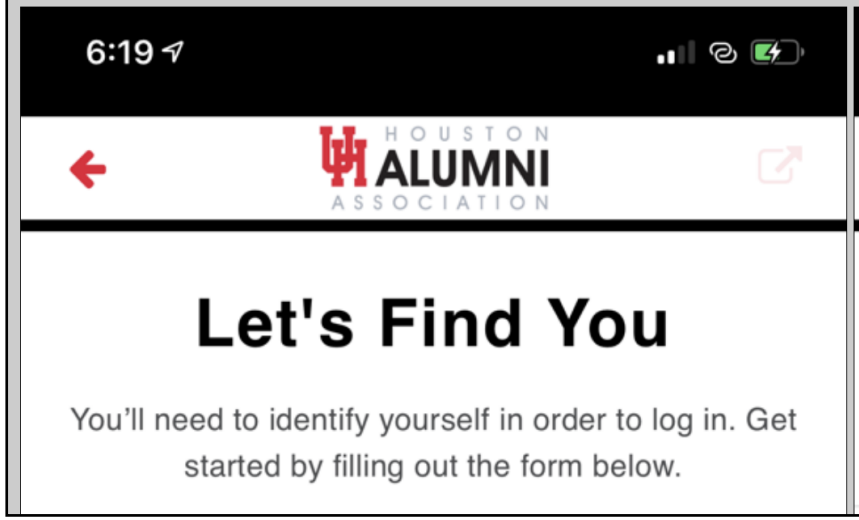
Executive Summary

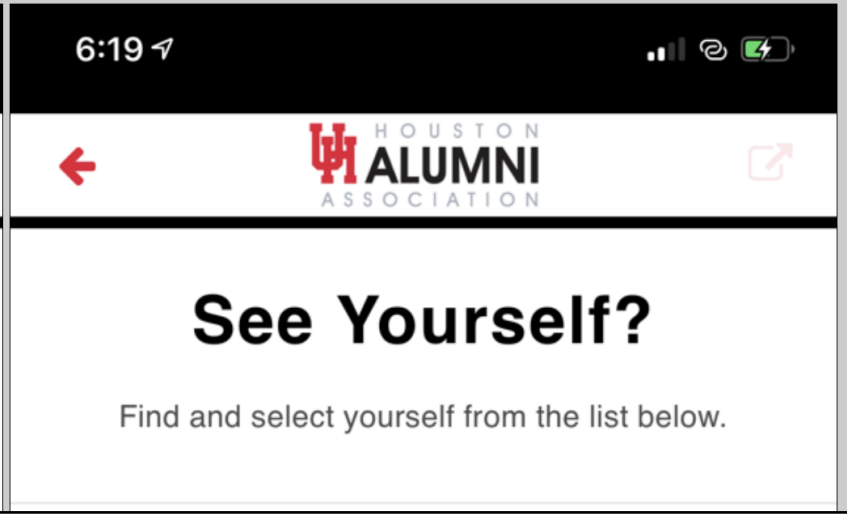
The University of Houston Alumni iOS App exposes data about alumni to everyone, and sends authentication data over the Internet without proper encryption.

These privacy violations appear to be violations of Federal regulations. Publishing the alumni data may violate FERPA, and failure to validate TLS cerificates has led to lawsuits from the FTC.

Detailed Findings

The app contains a "Let's Find You" page, which allows a search to find user records, as shown below. This allows anyone to view a list of alumni names, cities, and gradiation years.





Transmits Entire Database

Burp Suite Community Edition v1.7.36 - Temporary Project

Burp Intruder Repeater Window Help

Target | Proxy | Spider | Scanner | Intruder | Repeater | Sequencer | Decoder | Comparer | Extender | Project options | User options | Alerts

Intercept | HTTP history | WebSockets history | Options

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extensic
935	https://api.essenzasoftware.com	POST	/v1/AzureProxy	✓		200	426	JSON	
936	https://api.essenzasoftware.com	POST	/v1/AzureProxy	✓		200	351484	JSON	

Request | Response

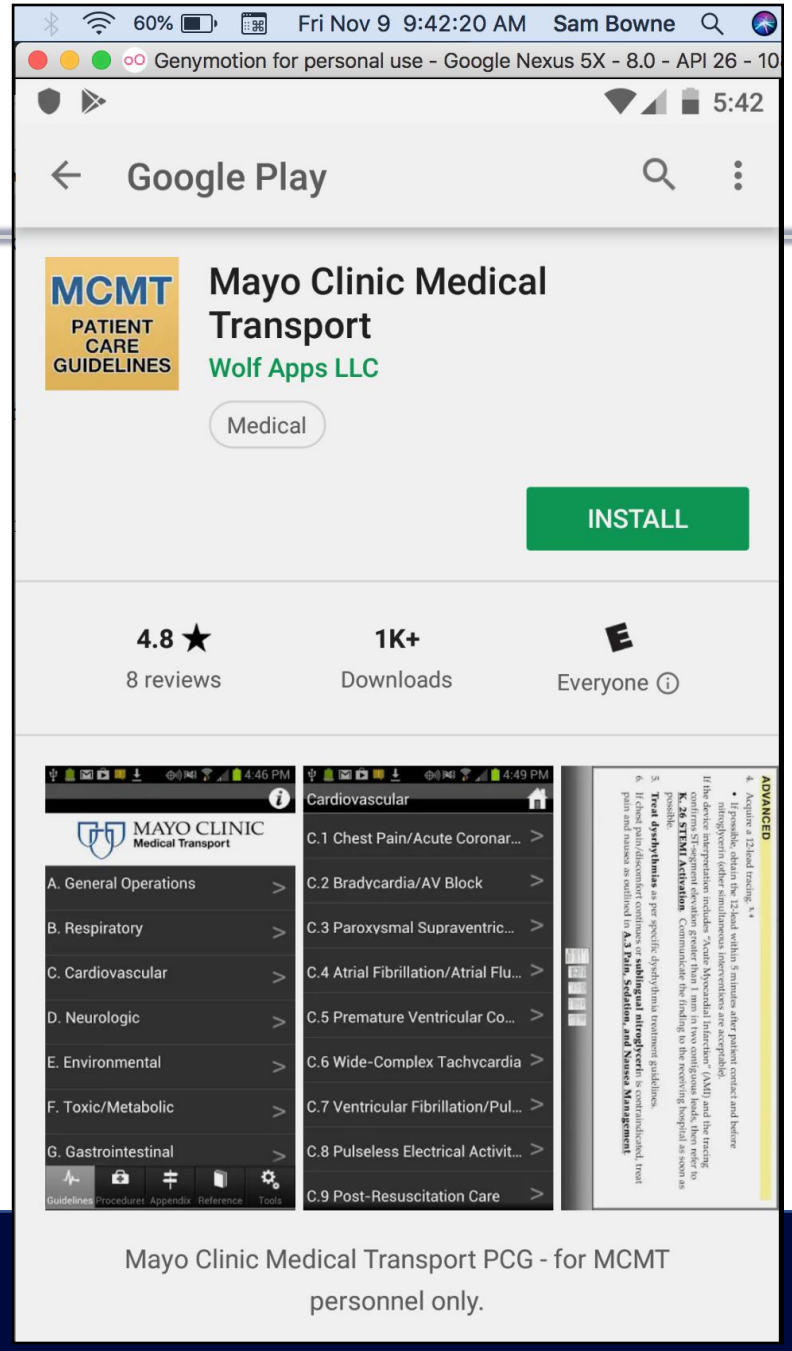
Raw | Headers | Hex

```
HTTP/1.1 200 OK
Cache-Control: no-cache
Pragma: no-cache
Content-Type: application/json; charset=utf-8
Expires: -1
Vary: Accept-Encoding
Server: Microsoft-IIS/10.0
Access-Control-Allow-Origin: file://
Access-Control-Allow-Credentials: true
Access-Control-Expose-Headers: Location,ETag
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Mon, 18 Feb 2019 15:38:57 GMT
Connection: close
Content-Length: 351055

[{"id":"000137E2-CD1A-4858-AC95-398609DC2EEC","createdOnApp":null,"isAdmin":null,"alertsCount":null,"purchasedMembership
Date":null,"EssenzaUniqueId":null,"lastNotified":null,"firstName":"Alison","lastName":[redacted],"memberID":"00[redacted],
"graduationYear":"2003","membershipStatus":"N","membershipPlan":null,"entity_middle_name":"A.","street1":"[redacted]
Jacinto
Dr","city":"Pasadena","state":"TX","email":"ydkk26@yahoo.com","dob":"[redacted],"foreign_cityzip":null,"country_name":n
ull,"zipcode":"[redacted]3426","Pref_Phone":"8326[redacted]
Work","degree_year_2":"2001","degree_major_2":"Psy[redacted],"degree_major_3":null,"directoryOptIn":
null,"EssenzaUserId":null},{"id":"00018953-CED3-4[redacted]3E135","createdOnApp":null,"isAdmin":null,"alertsCount
":null,"purchasedMembershipDate":null,"EssenzaUni[redacted]tNotified":null,"firstName":"[redacted],"lastName":"Ja
enicke","memberID":"[redacted],"graduationYear":[redacted]ipStatus":"N","membershipPlan":null,"entity_middle_nam
```

? < + > Type a search term 0 matches

Mayo Clinic Medical Transport



Mayo Clinic Medical Transport

- grep for **secretpassword**

```
[redacted]$ grep -ir secretpassword .
./assets/BT_config.txt:                                    {"itemId":"9B56BAB
431D90D2191114BD", "itemType":"Password_splash", "itemNickname":"pass spla
sh", "secretPassword":"G[redacted]", "secretPasswordWarning":"Access by unautho
rized personnel prohibited. Contact your supervisor with questions.", "rem
```

- **Disclosure**
  - Researcher notified the developer about this in June of 2015. He told researcher to get lost.

Binni Shah
@binitamshah

Following

We have patched the vulnerability you reported

Assignment 1: Exploring Mobile App Vulnerabilities

- See what app threats look like using an automated testing tool
  - Automated tools are good for quick scans, but generate many false positives