

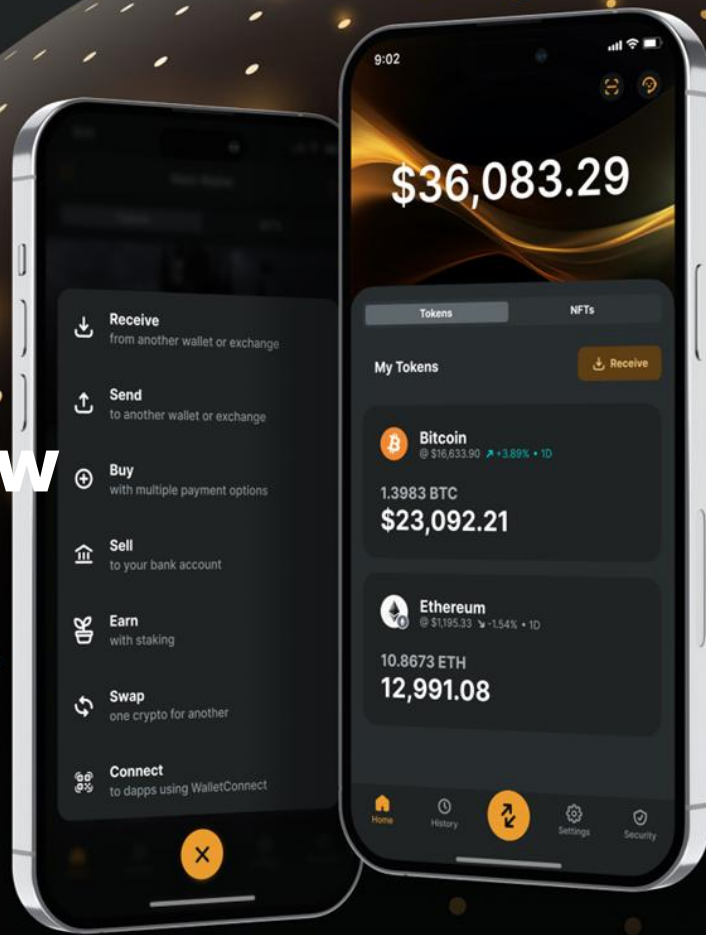


4 Exploits and a Funeral

Exploring WhatsApp's "View Once" Media



Troopers 26

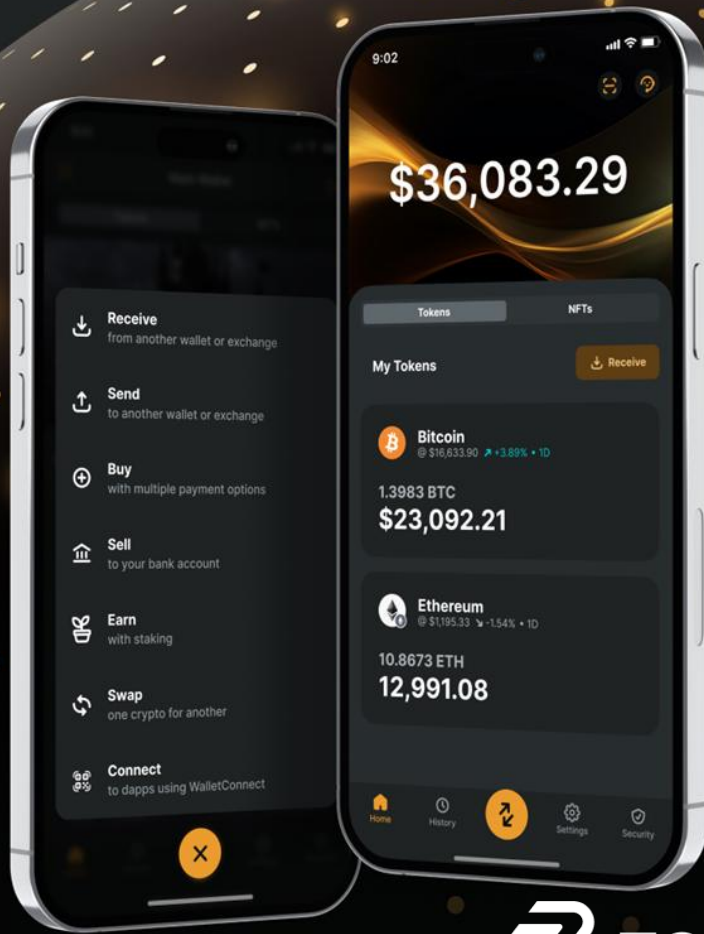


👋 Hi, I'm Tal Be'ery

- Co-Founder, CTO @ Zengo
- Recently, acquired by eToro
- 20+ years cyber security
- 10 times Black Hat Speaker
- 1st time Troopers speaker!
- [@talbeerysec](https://twitter.com/talbeerysec)



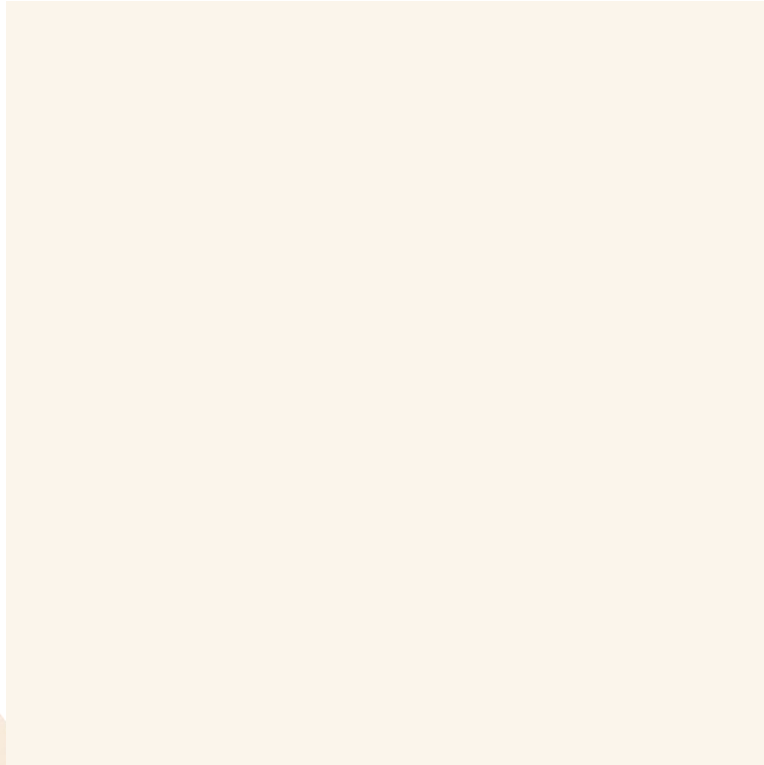
eToro



zengo

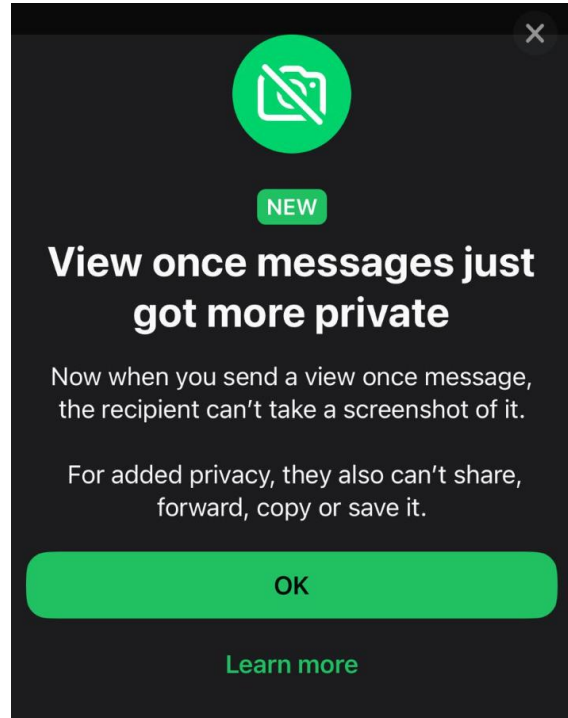
TL;DR

View Once: presented by WhatsApp



<https://x.com/WhatsApp/status/1617578925022138369>

View Once: Privacy!

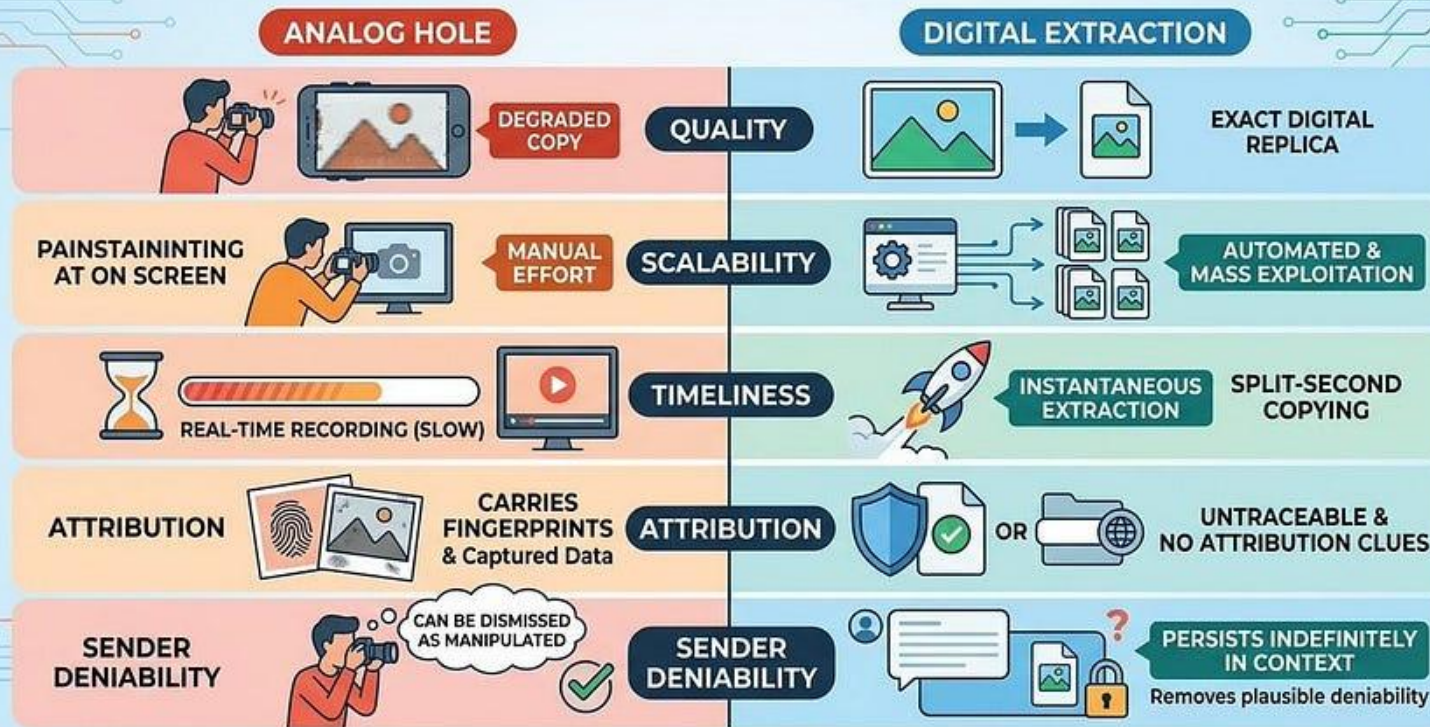


TL;DR:

- **We broke Meta's WhatsApp's View Once 4 times 2024-26:**
 - **Creating an instant digital copy with no restrictions**
 - **As easy as installing a browser extension**
- Meta fixed 3, WONT FIX 4th

But you can still photo it with another camera"

WHY DIGITAL EXTRACTION IS FAR MORE DANGEROUS THAN THE ANALOG HOLE: 5 KEY REASONS



DIGITAL EXTRACTION is Instantaneous, Exact, Untraceable, Infinitely Scalable, and Legally Irreversible.

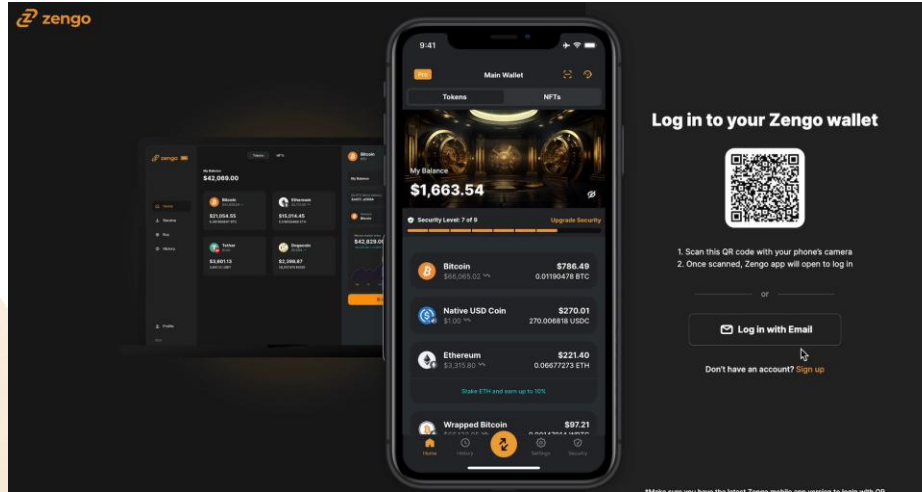
Agenda

- WhatsApp intro: threat modelling, security, E2EE
- WhatsApp over the wire: With a new Open-Source research tool
- Exploits 1,2,3,4
- Funeral: Meta's WONT FIX
- Resurrection: How it should work
- Q&A

Cryptowallets → View Once ???

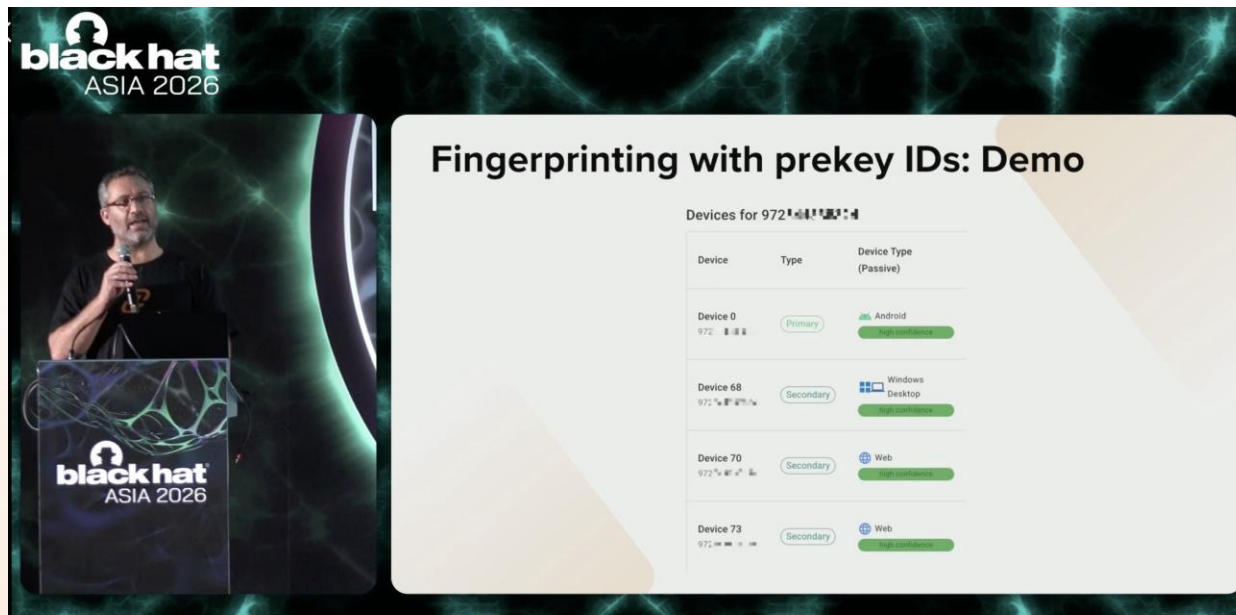
IM: Wallet's brother from another mother

- Sending digital money is yet another format of P2P comms
- Public Key cryptography
- Started Mobile, went Multi-Device



WhatsApp some other research

BlackHat ASIA 2026: [Your Number Is Up: When 3.5 Billion Strangers Can Exploit Your WhatsApp Devices](#)



The slide features a presentation from BlackHat ASIA 2026. On the left, a speaker is shown at a podium with the BlackHat ASIA 2026 logo. The main content area is titled "Fingerprinting with prekey IDs: Demo" and displays a table of devices for a specific phone number (9721111111111111).

black hat
ASIA 2026

black hat
ASIA 2026

Fingerprinting with prekey IDs: Demo

Devices for 9721111111111111

Device	Type	Device Type (Passive)
Device 0 9721111111111111	Primary	Android High Confidence
Device 68 9721111111111111	Secondary	Windows Desktop High Confidence
Device 70 9721111111111111	Secondary	Web High Confidence
Device 73 9721111111111111	Secondary	Web High Confidence



**ME TRYING
TO DO
A NORMAL
PRODUCTIVE
E2EE IN THE
WILD RESEARCH**

**WHATSAPP
PRIVACY
ISSUES**



WhatsApp Security

Intro

WHATSAPP IS THE IM GORILLA

A Giant in Instant Messaging



▲ 201 bm
▲ 126%

▼ 150%
l.l.l

▲ 401
▲ 381



OVER 3 BILLION
MONTHLY ACTIVE USERS WORLDWIDE



100 MILLION
MONTHLY ACTIVE USERS IN THE US



RANKED MOST USED
MOBILE MESSENGER APP IN THE WORLD



**MORE THAN
100 BILLION**
MESSAGES SENT
EACH DAY



**MORE THAN
7 BILLION**
VOICE MESSAGES
SENT DAILY





I rob banks because that's where the
money is.

— *Willie Sutton* —

AZ QUOTES



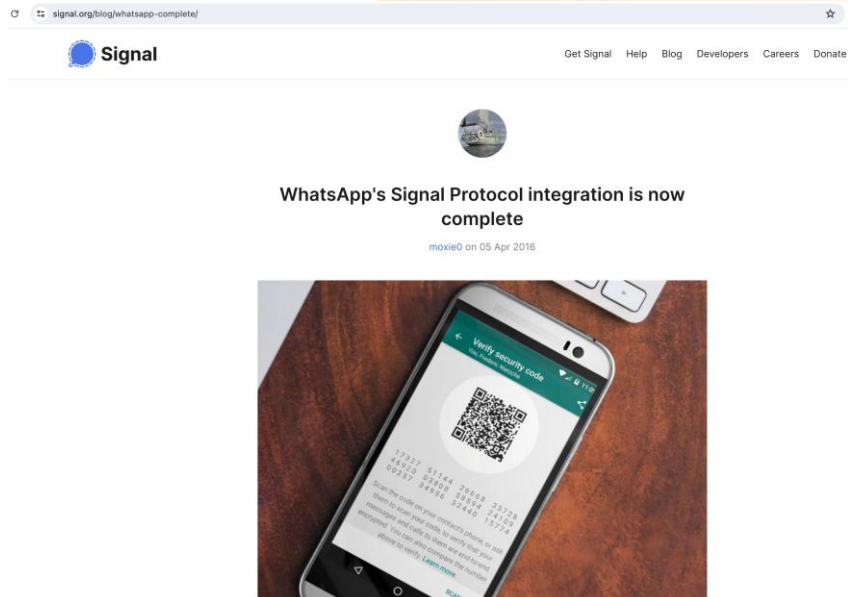
I hack WhatsApp because that's
where the data is.

— *Willie Sutton* —



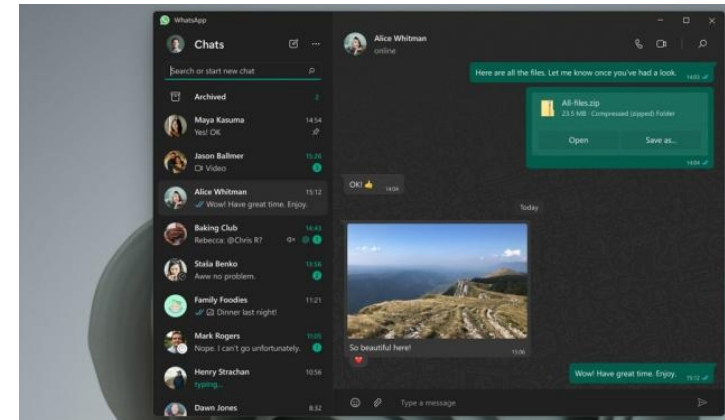
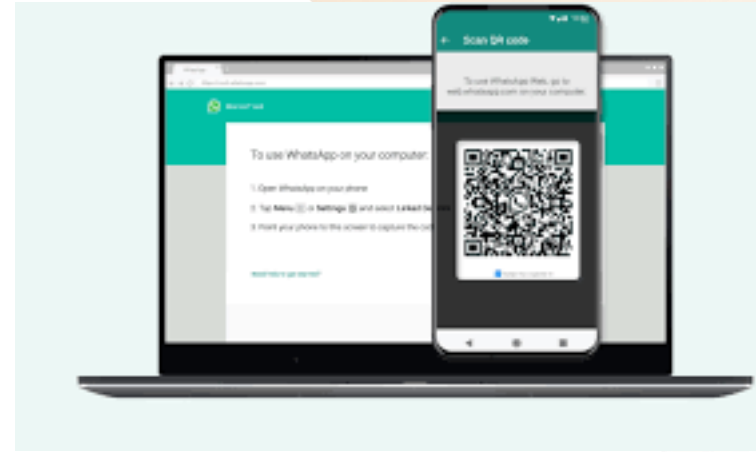
WhatsApp Signal E2EE

- Introduced in 2016
- Based on Signal Protocol
- <https://signal.org/blog/whatsapp-complete/>
- <https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf>



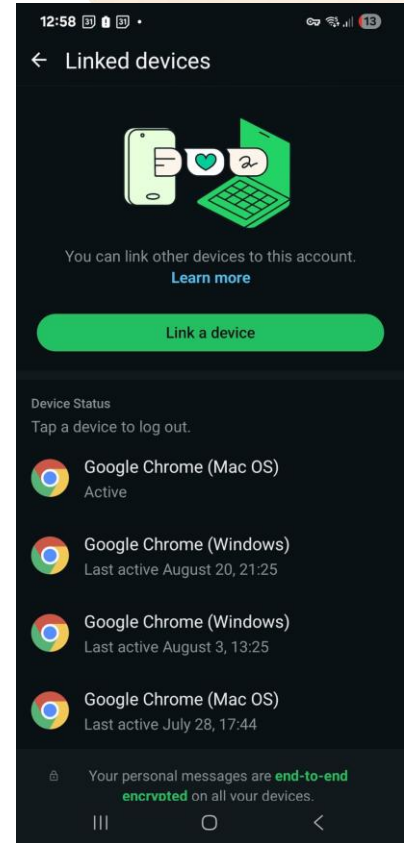
WhatsApp Multi-device

- Primary device: mobile
- Identity: phone #
- Companions: Web, desktops, another mobile, ...
- To add, scan primary's QR



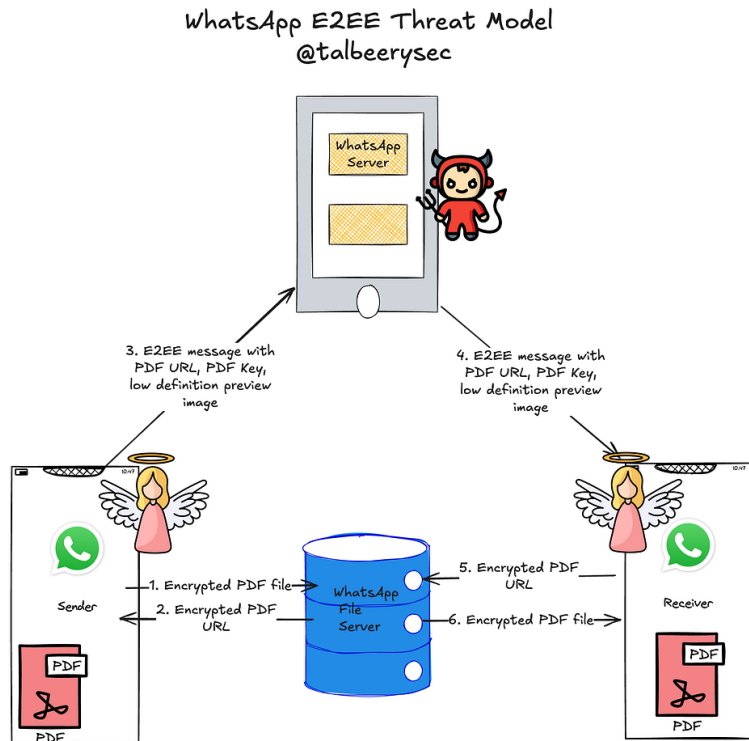
How to E2EE with Multi-devices?

- Signal [Sesame](#) : Multiple sessions
- Each device generates Key bundles
- Sender creates a session with:
 - Each receiver device
 - All other sender devices
- Sender sends message on all sessions

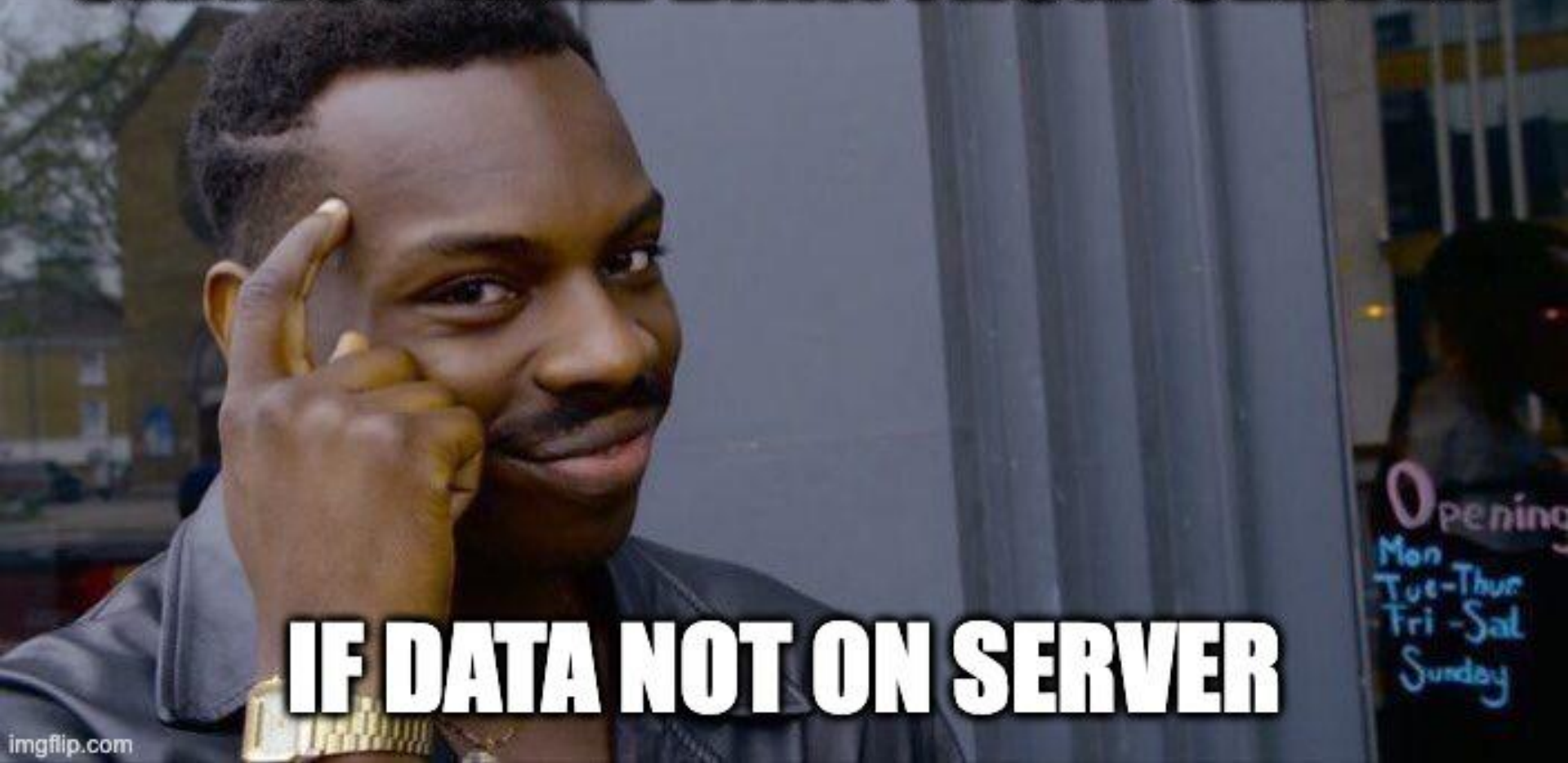


WhatsApp Threat Model: Rogue Server

- No data on server
 - Metadata remains
- Prevents mass surveillance
- Server is a less attractive target now



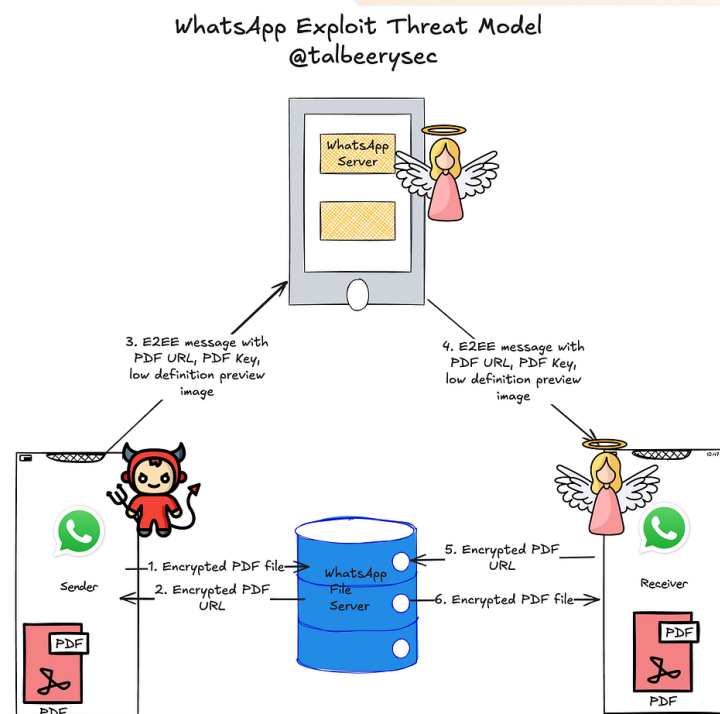
CANNOT TAKE DATA FROM SERVER



IF DATA NOT ON SERVER

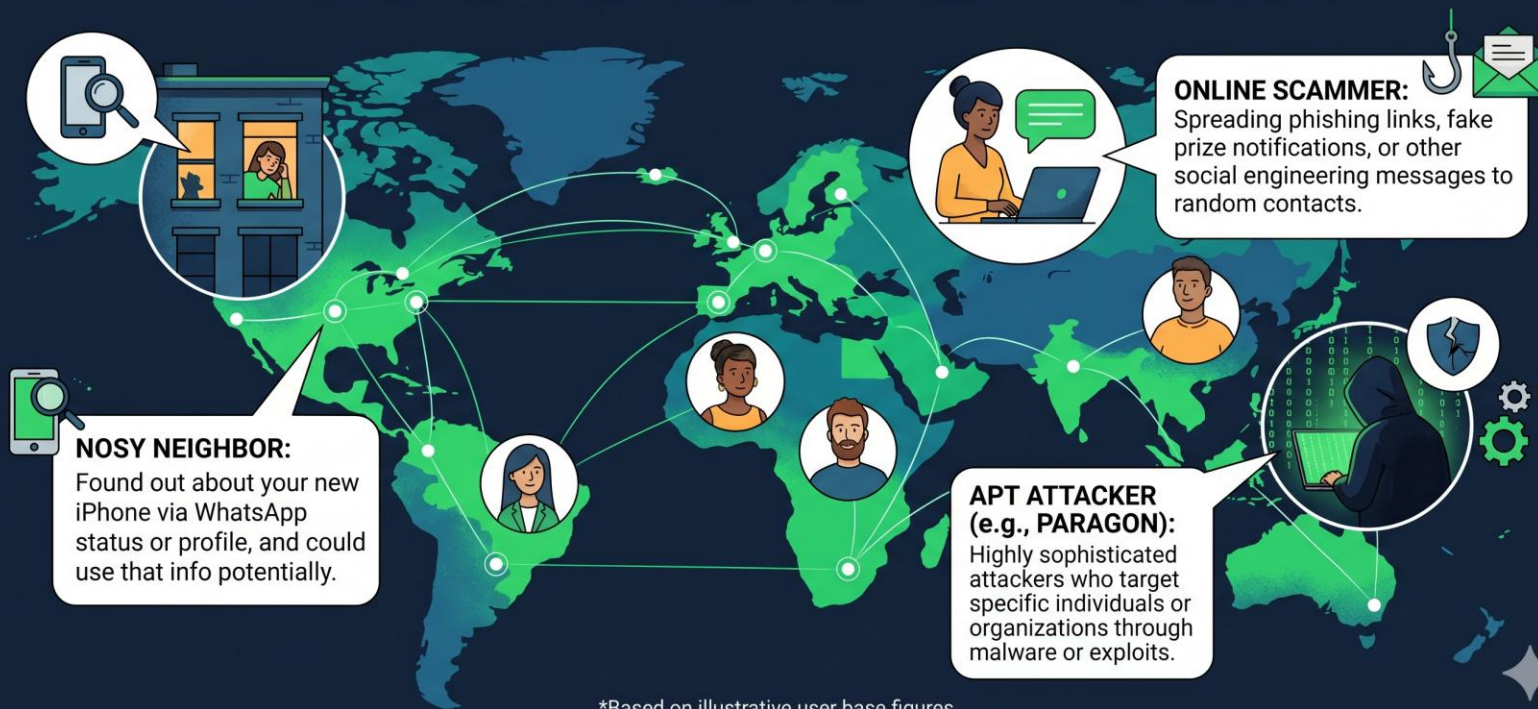
WhatsApp Threat Model: Rogue Client

- Server is a less attractive target now
 - Client is a more attractive target
- Server is a “dumb pipe”
 - Cannot see malicious traffic
 - Cannot terminate sessions: Client is directly “exposed”



WhatsApp Threat Model: Rogue Client

ANYONE OF **WHATSAPP'S 3.5B*** USER BASE
CAN POTENTIALLY BE A WHATSAPP ATTACKER



*Based on illustrative user base figures.

WhatsApp

Over the wire



wiresharkfoundation.org

Looking under the hood

- The client does not let us see all the action
- We need a client that does!
- Based on Baileys open-source project
- <https://github.com/WhiskeySockets/Baileys>
- New client is added as another companion device





SAY HELLO TO MY LITTLE FRIEND

A CENTURY OF
SCARFACE

Author of The Exorcist Legacy: 50 Years of Fear

NAT SEGALOFF

FOREWORD BY STEVEN BAUER,
ON HIS STAR-MAKING ROLE AS MANNY RIBERA

WhatsApp Bailey's Device Toolkit

Baileys Web UI

Dashboard
Overview and status

Send Messages
Send messages and reactions

Chats
View and manage chats

Contacts
Contact management

Devices
Device management

Prekey Bundles
View device prekey bundles

Presence
Presence control

Developer
Advanced tools

Settings
Client configuration

Logout

WhatsApp Web Interface

OPEN REFRESH

Dashboard

Welcome to the Baileys WhatsApp Web Interface. Monitor your connection status and manage your WhatsApp operations.

WhatsApp Connection

Connected

Unknown

Baileys v6.7.21

Last updated: 4/17/2026, 12:09:42 PM

Quick Stats

50

Total Chats

1934

Total Contacts

3

Unread Chats

Recent Chats

WhatsApp Group

1

WhatsApp Group

0

WhatsApp Group

1

WhatsApp Group

1

WhatsApp Group

0

System Status

WhatsApp State

open

Authenticated

User Account

Unknown

Baileys Version

6.7.21

Last Update

4/17/2026, 12:09:42 PM

github.com/talbeerysec/WhatsApp-baileys-device-toolkit

Say hello to my eldest son



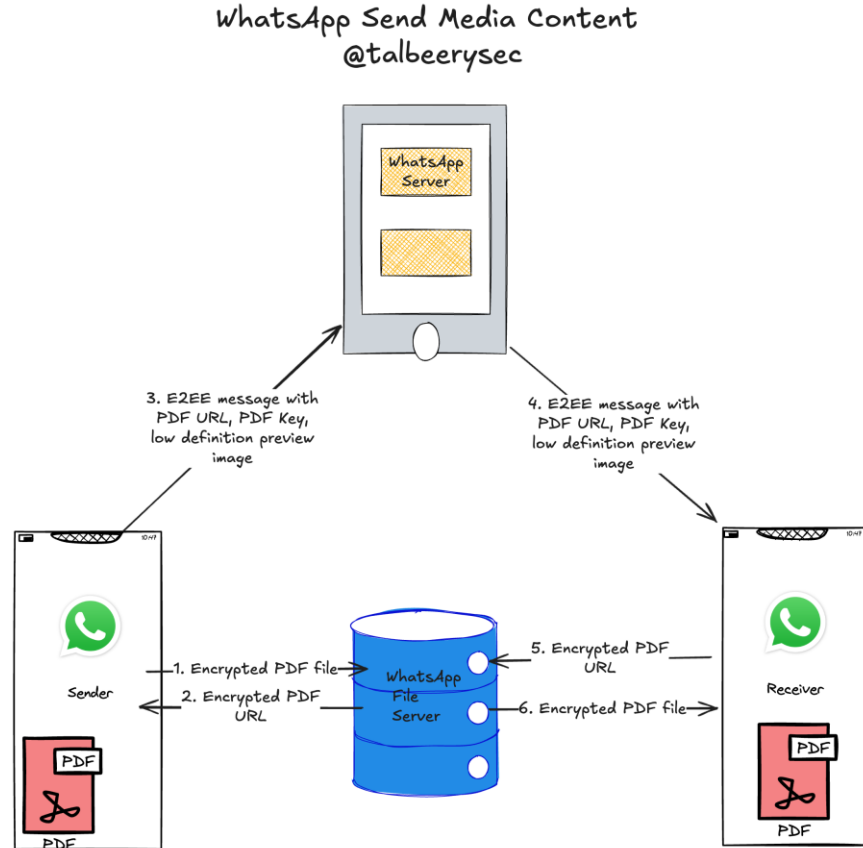
Encrypted message on wire

- XMPP envelope
 - Extensible Messaging and Presence Protocol
 - Originally named Jabber (hence JID)
- Metadata in plaintext
- Content E2EE

```
<message>
  @from: "972[REDACTED]:8@s.whatsapp.net"
  @type: "media"
  @id: "[REDACTED]1932[REDACTED]"
  @recipient: "44[REDACTED]@s.whatsapp.net"
  @notify: "Tal"
  @t: "1724775174"
  "\n\t\t"
  <enc>
    @v: "2"
    @type: "pkmsg"
    @mediatype: "video"
    "\n\t\t\t3[REDACTED]"
    "\n\t\t"
  <device-identity>
    "\n\t\t\t[REDACTED]"
```

Media message send and receive

- Sender generates a random key
- Encrypt + upload file to file server
- Sends URL + key under E2EE
- Receiver: download + decrypt



Decrypted Media message

- Protobuf encoded

→ URL

→ TYPE

→ Dimensions (for image)

→ Key

→ Preview

```
url: https://mmg.whatsapp.net/o1/v/  
mimetype: image/jpeg  
fileSha256: yrMsiJCqdcAr8XOKoFHhmmI  
fileLength: 224990  
height: 1600  
width: 1131  
mediaKey: 4kBhJcDhmOCEcsGvHSaxM/f05  
fileEncSha256: 3oHQG8nJkpfP/rhZdWis  
directPath: /o1/v/t62.7118-24/f1/m2  
mediaKeyTimestamp: 1725144638  
jpegThumbnail: /9j/4AAQSkZJRgABAQAA
```

Decrypting Media: DIY

- CURL URL
- HKDF(base64(media key))
 - IV
 - KEY
 - MAC
- openssl enc -aes-256-cbc -d

```
url: https://mmg.whatsapp.net/o1/v/  
mimetype: image/jpeg  
fileSha256: yrMsiJCqdcAr8XOKoFHhmmI  
fileLength: 224990  
height: 1600  
width: 1131  
mediaKey: 4kBhJcDhmOCEcsGvHSaxM/f05  
fileEncSha256: 3oHQG8nJkpfP/rhZdWis  
directPath: /o1/v/t62.7118-24/f1/m2  
mediaKeyTimestamp: 1725144638  
jpegThumbnail: /9j/4AAQSkZJRgABAQAA
```


View Once in mobile

- **WhatsApp relies on mobile OS to block screenshots**

Android Developers > Design & Plan > Security > Fraud prevention > Guides

Was this helpful?  

Secure sensitive activities



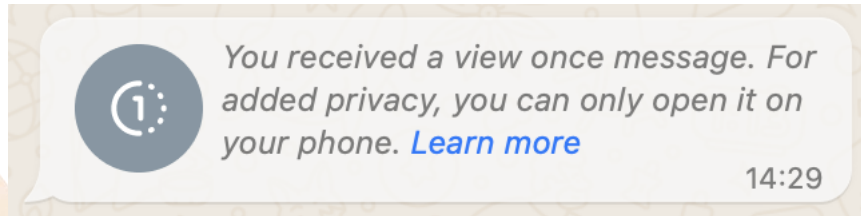
This document details ways to monitor sensitive activities, such as user logins and online purchases.

FLAG_SECURE

`FLAG_SECURE` is a [Window flag](#) that tells Android not to allow screenshots or to display the window view on a non-secure display (such as Casting the screen). This is useful for applications that need to protect sensitive information, like banking apps or password managers. When a window is flagged with `FLAG_SECURE`, Android prevents screenshots from being taken and prevents the window from being displayed on a non-secure display, such as a TV or projector. This helps to protect the information that is being displayed in the window from being accessed by unauthorized people.

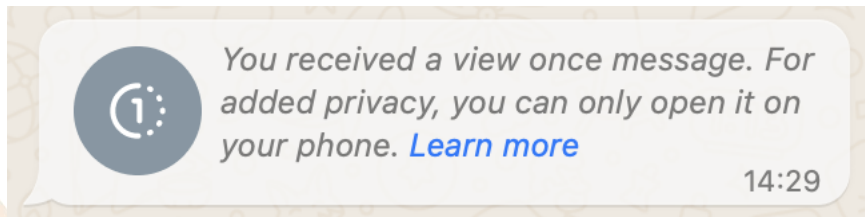
View Once + Multiple device

- WhatsApp allows receiving View Once only in devices in which the app can control screenshots
- In other devices (e.g. Web) users are told to open it on supporting devices



View Once: Device fingerprinting potential?

- Hypothesis: WhatsApp server tells sender to which devices it can send View Once and to which it cannot
- If true, a fingerprinting potential!



View Once message JSON



View Once message JSON analysis

- **Contains**

- Media URL
- Media key material
- Thumbnail (???)
- View once = true

- Regular media message + View Once = True



Exploit 1

Aug 24: View ~~Once~~ stored messages

Let's view infinitely.... #1

- WhatsApp Web stores View Once in chat history, as is
→ Display is blocked by the ViewOnce flag
- Let's make a Chrome Extension to toggle it!
- Let's check WhatsApp Chrome extension in GitHub...
- <https://github.com/Schwartzblat/WhatsApp-Web-Plus> !

Code

```
const view_once_handler = (message) => {
  if (!message?.isViewOnce) {
    return false;
  }
  message.isViewOnce = false;
};

const initialize_renderer_hook = () => {
  const handle_message = (message) => {
    if (message?.isViewOnce !== true) {
      return;
    }
    console.log(message);
    message.isViewOnce = false;
  };

  const original_function = mR.modules[WA_MODULES.MESSAGES_RENDERER].default;
  mR.modules[WA_MODULES.MESSAGES_RENDERER].default = function () {
    handle_message(arguments[0]?.msg);
    return original_function(...arguments);
  }
};
```



אבא

Normal WhatsApp Web Sender



Hadar Be'ery

Manipulated WhatsApp Web Receiver



Responsible disclosure to Meta

[View once: uploaded media is not deleted from server after 14 days](#)

Informative · Last updated 7 weeks ago · #122174562572159209

[WhatsApp view once - file URL issues](#)

Informative · Last updated 7 weeks ago · #122173211618159209

[WhatsApp View once image message includes preview information](#)

Informative · Last updated 7 weeks ago · #122171855396159209

[View once media privacy issues](#)

Informative · Last updated 7 weeks ago · #122171558132159209

Exploited in the wild!

- Let's check if such extensions exist in Chrome Store
- Boom! Since 2023 (chrome-stats.com)

The screenshot shows the Chrome Web Store page for the extension 'View Once Photos Bypass for Whatsapp Web'. The page includes a header with the extension name and a brief description: 'Open view once media in the browser.' Below this are tabs for 'Overview', 'Download', 'Source', 'Reviews', and 'Trends'. The main content area features two identical preview images showing a WhatsApp message interface with a 'View Once' photo of a sticky note that says 'My Password 123456'. A red arrow points from the message to the photo. Below the previews, there is a section titled 'What is View Once Photos Bypass for Whatsapp Web?' followed by a description: 'View Once Photos Bypass for Whatsapp Web is a Chrome extension that allows you to open and save view once media in the browser, so you can view them as many times as you want until you open the media on your cell phone. A subscription is required for usage.' At the bottom of the main content area are buttons for 'Download', 'Compare with', and 'Add to favorites'. Below the main content is a section titled 'EXTENSION STATS' which lists various metrics: 'By: ops.json', 'View on Chrome Web Store', 'Users: 10,000+', 'Rating: 3.00 (188)', 'Version: 2.5.1 (Last updated: 2024-09-19)', 'Creation date: 2023-12-11', 'Risk impact: Low risk impact', 'Risk likelihood: Moderate risk likelihood', 'Manifest version: 3', 'Size: 23.08K', and 'Email: c*****@gmail.com'. To the right of the 'EXTENSION STATS' section is a 'Ranking' box showing the extension's rank as #7614, along with other rankings for different keywords and a button to 'Upgrade to see more rankings'.

View Once Photos Bypass for Whatsapp Web

Open view once media in the browser.

Overview Download Source Reviews Trends

View Once Photos Bypass

You received a view once message. For added privacy, you can only open it on your phone. [Learn more](#)

22:19

View Once Photos Bypass

You received a view once message. For added privacy, you can only open it on your phone. [Learn more](#)

22:19

What is View Once Photos Bypass for Whatsapp Web?

View Once Photos Bypass for Whatsapp Web is a Chrome extension that allows you to open and save view once media in the browser, so you can view them as many times as you want until you open the media on your cell phone. A subscription is required for usage.

Download Compare with Add to favorites

EXTENSION STATS

By: ops.json

View on Chrome Web Store

Users: 10,000+

Rating: 3.00 (188)

Version: 2.5.1 (Last updated: 2024-09-19)

Creation date: 2023-12-11

Risk impact: Low risk impact

Risk likelihood: Moderate risk likelihood

Manifest version: 3

Size: 23.08K

Email: c*****@gmail.com

Ranking

#7614

Other rankings

#2520 in Tools

#18 in whatsapp extension keyword

#32 in photo keyword

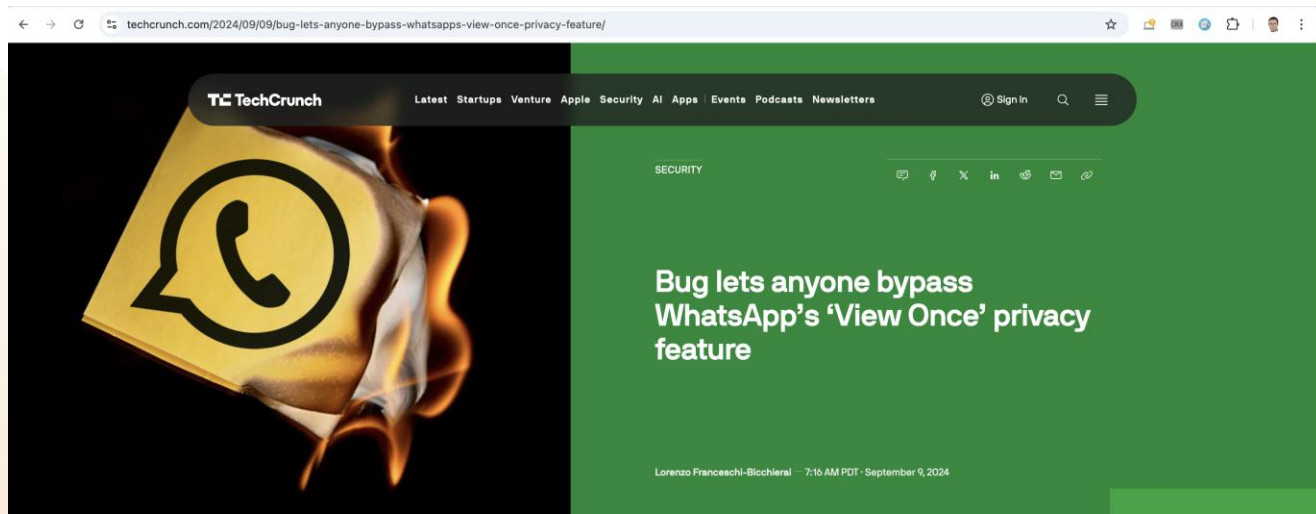
#38 in whatsapp keyword

#74 in subscription keyword

Upgrade to see more rankings

Publish

- No word from Meta for a while
- Exploited in the wild
- Published in [TechCrunch](https://techcrunch.com/2024/09/09/bug-lets-anyone-bypass-whatsapp-view-once-privacy-feature/) , others (9.9.24)



Meta response



Informative · Wednesday, September 18, 2024 at 6:55 PM

Our reply

Hi Tal,

Thank you for your bug bounty submission.

We appreciate your research and have reviewed your findings, which were informative. Prior to your submission, we were already in the process of rolling out updates to view once on Web. Those updates are forthcoming and will be rolled out soon. Given that, your submission does not qualify for a monetary reward.

Additionally, we would like to remind you of our guidance that we provide immediately after a submission is made to the program, which is a requirement that we also outline on our website's Program Terms: "Please give us reasonable time to investigate and mitigate the issue before sharing information with others." In the future, please give us reasonable time to investigate and respond to your report prior to sharing your report with others.

Thanks,

Meta Bug Bounty Team

Meta's fix

- **12.9.24 update to web app**
- **WhatsApp Web redacts ViewOnce in chat history**
 - **URL, Key are not saved**
- **Saved messages are safe now!**

Exploit 2

Sept 24: View ~~Once~~ received messages

Let's view infinitely.... #2

- WhatsApp Web redacts View Once in chat history
 - URL, Key are not saved
- Let's toggle ViewOnce "upstream" on message itself, before it gets saved, so it will not get redacted
- Contributed code to [WhatsApp-Web-Plus](#) extension
- [Blogpost](#)

Code

```
const initialize_protobuf_hook = () => {
  const handle_message = (message) => {
    if (message?.viewOnceMessageV2?.message?.imageMessage?.viewOnce === true) {
      message.viewOnceMessageV2.message.imageMessage.viewOnce = false;
    } else if (message?.viewOnceMessageV2?.message?.videoMessage?.viewOnce === true) {
      message.viewOnceMessageV2.message.videoMessage.viewOnce = false;
    } else if (message?.viewOnceMessageV2Extension?.message?.audioMessage?.viewOnce === true) {
      message.viewOnceMessageV2Extension.message.audioMessage.viewOnce = false;
    }
    return message;
  };

  const original_processor = MODULES.PROTOBUF_HOOK.verifyProtobufMessageObjectKeys;
  MODULES.PROTOBUF_HOOK.verifyProtobufMessageObjectKeys = function (message) {
    const modified_message = handle_message(message);
    return original_processor(modified_message);
  };
};
```

Responsible disclosure to Meta



Monday, September 16, 2024 at 2:22 PM

What you submitted

Title

View Once is vulnerable even after 12.924 fix

Vuln Type

Read Data Improperly

Product Area

Web

Description/Impact

The original issue is that the View Once media messages are identical to ordinary media messages, with the addition of a single field that tells the client this media should be viewed once. Once received, these messages are stored in the app's database, just like ordinary media messages.

As a result, exploiting extensions could just change the View Once field to false in the database and make the official WhatsApp web app show them.

Circa 12.9.2024, WhatsApp released an update to their Web App, that changes the way View Once media messages are saved to the application's databases and redact some of the information that enables the media viewing. As a result, the media becomes technically unviewable even if the View Once field was set to false.

To bypass the fix, exploiters just need to go "upstream" and toggle the View Once flag to false when it is received by the app and before it is stored in the database.

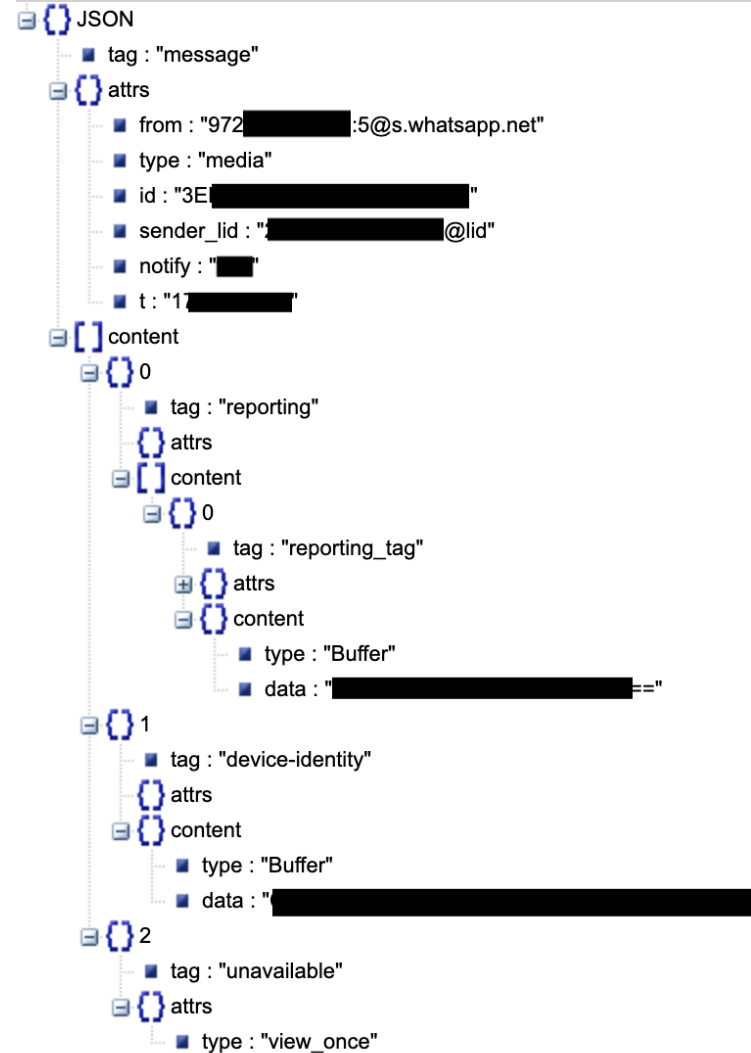
See

<https://medium.com/@TalBeerySec/whatsapp-view-once-privacy-issue-initial-fix-assessment-the-good-the-bad-and-the-ugly-be97ec1cc2e5>

See demo <https://www.youtube.com/watch?v=uEG0mldUSZ8>

Meta's fix

- Silent server fix 15.11.24
- ViewOnce flag was added to the unencrypted header
- WhatsApp Server redacts View Once message content that are sent to non-supporting devices

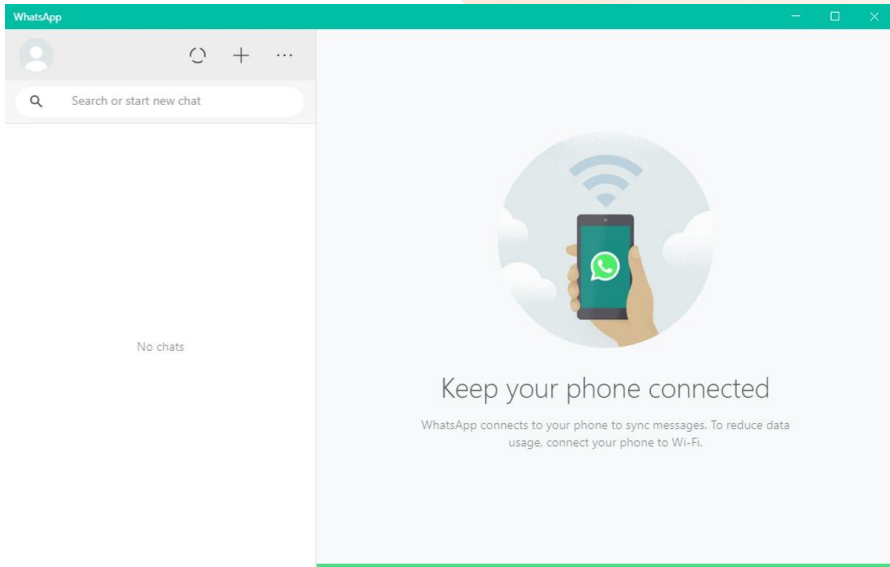


Exploit 3

Feb 25: View Once synced messages

What is history sync?

- **New device is added**
- **History resides on the primary device**
- **New device asks for it**



How it works?

- The primary device creates a file of chunked messages
- Pretty much like any other media
- Did Meta remember to redact view once there too?
- Apparently not!

```
"protocolMessage": {  
  "type": "HISTORY_SYNC_NOTIFICATION",  
  "historySyncNotification": {  
    "fileSha256": "imczkkPcrx1wCkf/J6d",  
    "fileLength": "1570203",  
    "mediaKey": "/2T+z2Eqnuaag6LQG/WFH",  
    "fileEncSha256": "11m+YPZCtWf5WJGz",  
    "directPath": "/v/t62.31111-24/306",  
    "syncType": "RECENT",  
    "chunkOrder": 4,  
    "progress": 100,  
    "oldestMsgInChunkTimestampSec": "1",  
  }  
}
```

Let's view infinitely.... #3

- **Create sync request**
- **View Once message are not redacted!**

Responsible disclosure to Meta



Thursday, February 6, 2025 at 2:34 PM

What you submitted

Title

View Once feature can still be bypassed with history sync

Vuln Type

Privacy / Authorization

Product Area

WhatsApp

Description/Impact

Following our previous research on WhatsApp View Once feature privacy and security, which led to WhatsApp multiple fixes, we have found yet another issue that was not addressed.

The gist of these fixes was to allow the view once message to reach only the primary mobile device of the recipient and prevent it from reaching to companion devices. This is due to the fact that on companion devices, such as WhatsApp Web, the bypass of the view once property is trivial and can be easily automated at scale with browser extensions.

We found a way to bypass this protection with WhatsApp history sync feature. A companion device can request to sync its history with messages from the primary device. This happens naturally when a device is added and needs to populate its history, or when older messages that were not previously synced are requested by the user. When such happens the primary device serializes the requested message and sends them to the companion device. When doing so the primary device fails to redact the View once message, which allows it to get to the companion device and allow its full abuse as before.

Meta response



Friday, March 21, 2025 at 1:11PM

Our reply

After reviewing this issue, we have decided to award you a bounty of \$500. Meta fulfills its bounty awards through Bugcrowd.

Thank you again for your report. We look forward to receiving more reports from you in the future!

Meta's fix

- **21.3.25**
- **View Once messages are redacted for non-supporting devices**

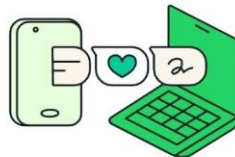
Exploit 4

Feb 26: View Once as Android

Device identification

- WhatsApp trusts Android with ViewOnce
 - Even if non-primary
- What prevents a client from lying?

← Linked devices



You can link other devices to this account.

[Learn more](#)

Link a device

DEVICE STATUS

Tap a device to rename it or log out.



Google Chrome (Mac OS)

Last active today at 10:48 AM



Android (Android)

Last active today at 10:48 AM

 Your personal messages are **end-to-end encrypted** on all your devices.

Device identification manipulation

WhatsApp Web Interface

WhatsApp Client Configuration

Configure how your client appears in WhatsApp's linked devices. Changes require logging out and reconnecting.

Platform Type

Custom...

Custom Platform Name

@TalBeerySec WhatsApp security research client

Enter a custom platform/OS name

Browser Name

blabla

The browser name to display

Version (Optional)

1.0.0

Leave empty to use preset defaults

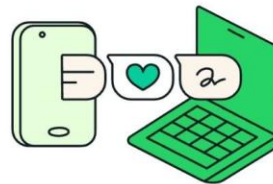
Preview

blabla (@TalBeerySec WhatsApp security research client)

This is how your device will appear in WhatsApp's linked devices

 SAVE CONFIGURATION

← Linked devices



You can link other devices to this account.

[Learn more](#)

[Link a device](#)

DEVICE STATUS

Tap a device to rename it or log out.



@TalBeerySec WhatsApp security resear...

Last active today at 2:07 PM



Google Chrome (Mac OS)

Last active today at 2:06 PM

Let's view infinitely.... #4

- **Set device type to Android via standalone app or Web extension**
- **View once is defeated**

Responsible disclosure to Meta



Monday, February 16, 2026 at 10:51PM

What you submitted

Title

Whatsapp viewonce bypass

Description/Impact

User can register their rogue client as Android companion. If so, this client gets view once messages and can ignore the viewonce flag.

view once can be viewed indefinitely

Meta response: WONT FIX



Not Applicable · Tuesday, March 10, 2026 at 12:13 PM

Our reply

Thank you for reaching out. From the security standpoint, we consider one-time-view media as a "best effort" feature, meaning that we do not consider our protections here to be hard security/privacy controls. This is because unfortunately there will always be ways to view/listen to a received media more than once. Some of these ways are outside of our control and we are unable to prevent (e.g. a person taking a photo/video of the media with another phone or capturing the media using a modified client). As such, we are unable to qualify this submission for our bug bounty program.

Although this issue does not qualify as a part of our bounty program, we appreciate your report. We will follow up with you on any security bugs or with any further questions we may have.

Meta response: WONT FIX



View Infinity → Lessons

A proper View Once solution: DRM

- This is a DRM problem
- Successfully (or at least to some extent) solved by Netflix, others
- Exploit 1,2: Solved with encryption + Hardware support
- Exploit 3: Solved with encryption
- Exploit 4: Solved with device attestation
- See [Blog](#)

General Vendors

- **Talk to security researchers reporting bugs**
- **Closing your eyes will not make it go away**



Users

- **View Once does not live to its promise**



Researchers

- **Responsibly disclose, but publish when it becomes irresponsible**
- **Be ready to be surprised when you are researching**



- [@talbeerysec](#)
- [Tal at Zengo dot com](#)
- [Talbe at etoro dot com](#)

 **TROOPERS**

