“We are currently clean on OPSEC”: The Signalgate Saga

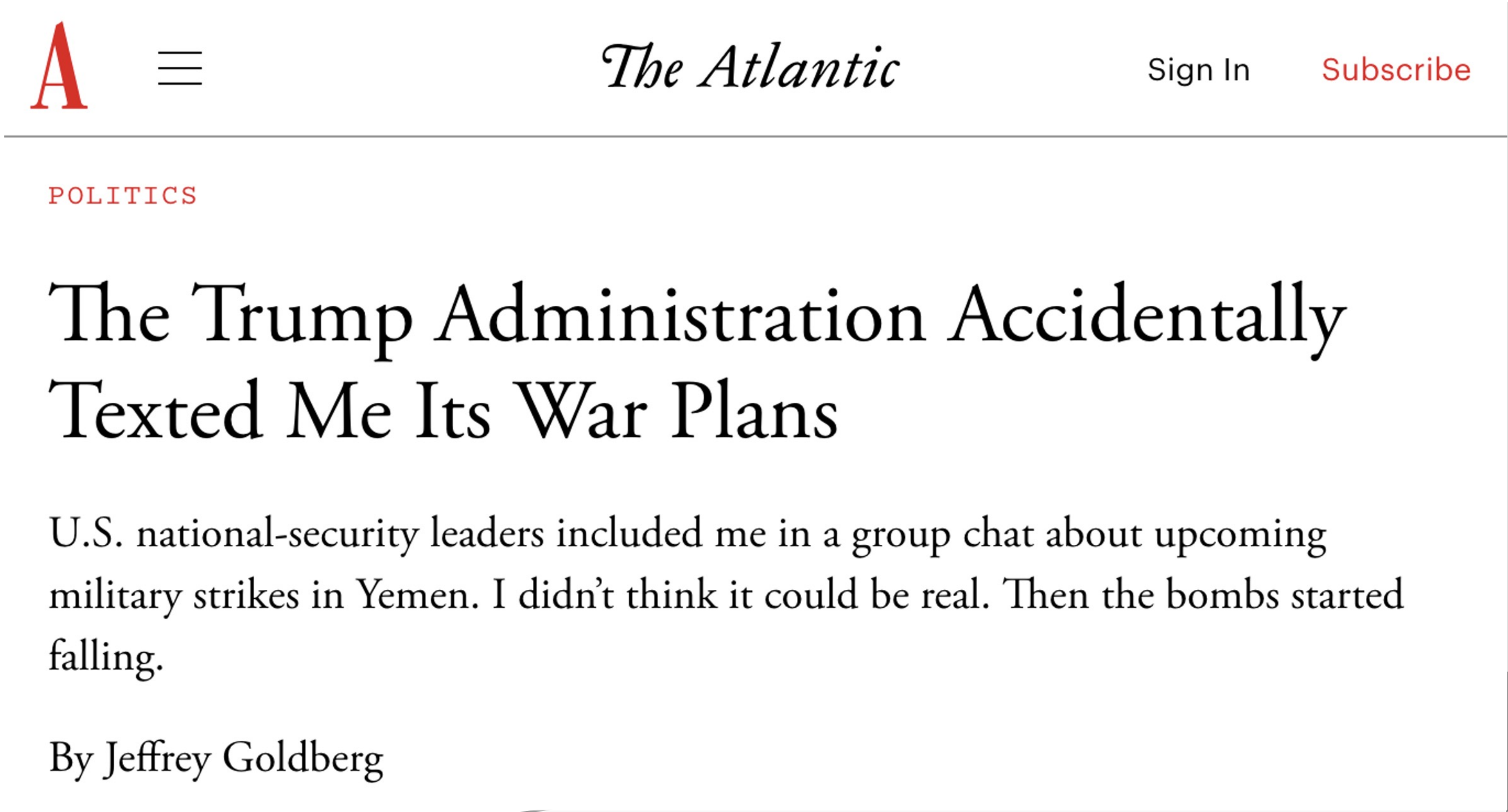
a presentation by Micah Lee

Chapters

1. Signalgate
2. Hey Sir
3. Mike Waltz is Bored
4. TM SGNL
5. Hacked in 15-20 Minutes
6. End-to-Middle-to-End Encryption
7. Drowning in Heap Dumps
8. TeleMessage Explorer
9. Clean on OPSEC

Chapter 1: Signalgate

- **Mike Walz**
  National Security Advisor



The Atlantic

POLITICS

The Trump Administration Accidentally Texted Me Its War Plans

U.S. national-security leaders included me in a group chat about upcoming military strikes in Yemen. I didn’t think it could be real. Then the bombs started falling.

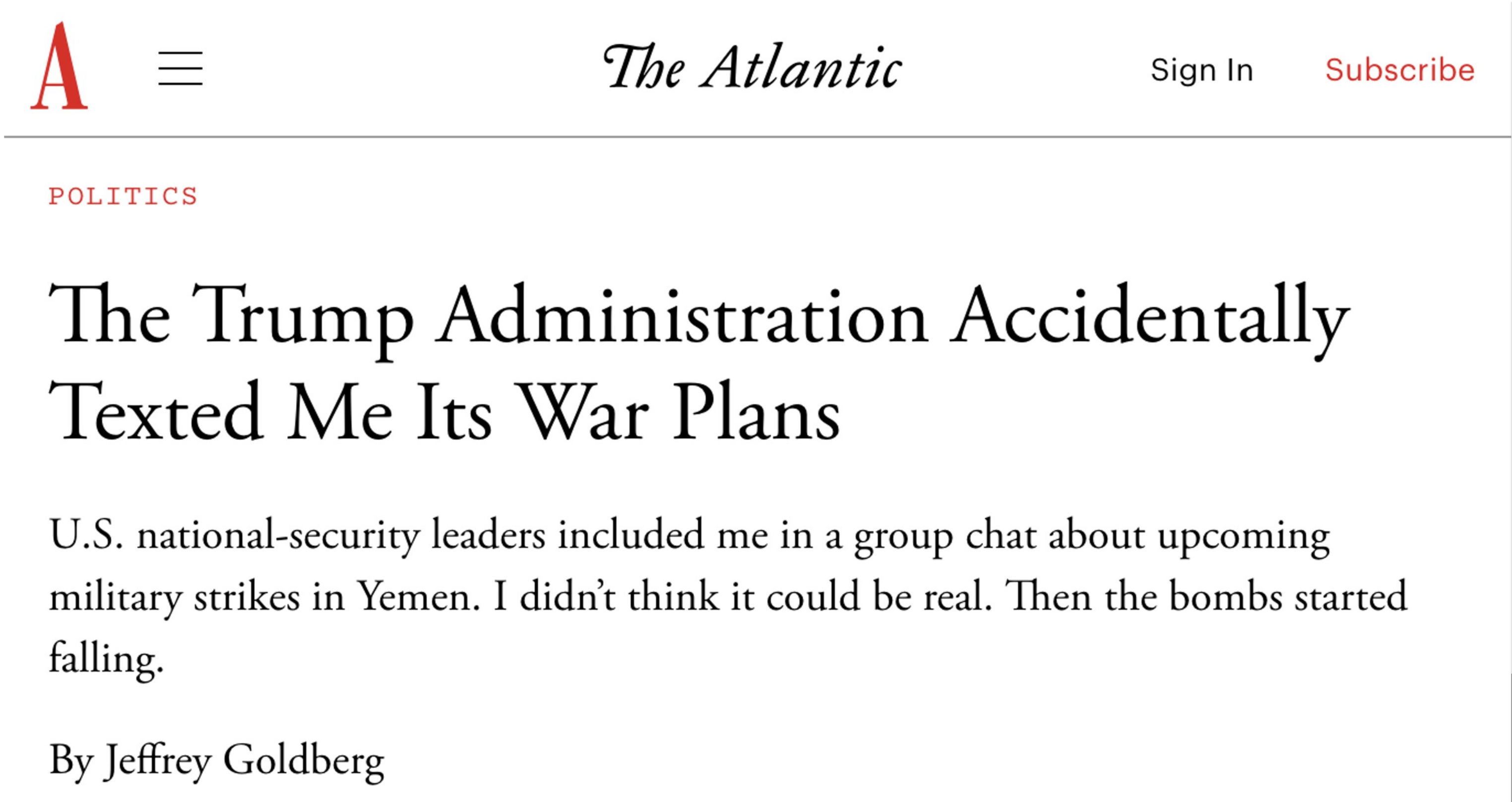
By Jeffrey Goldberg

March 24, 2025

https://archive.is/u5txN

Chapter 1: Signalgate

- **Mike Walz**
  National Security Advisor
- **Pete Hegseth**
  Secretary of Defense



POLITICS

The Trump Administration Accidentally Texted Me Its War Plans

U.S. national-security leaders included me in a group chat about upcoming military strikes in Yemen. I didn't think it could be real. Then the bombs started falling.

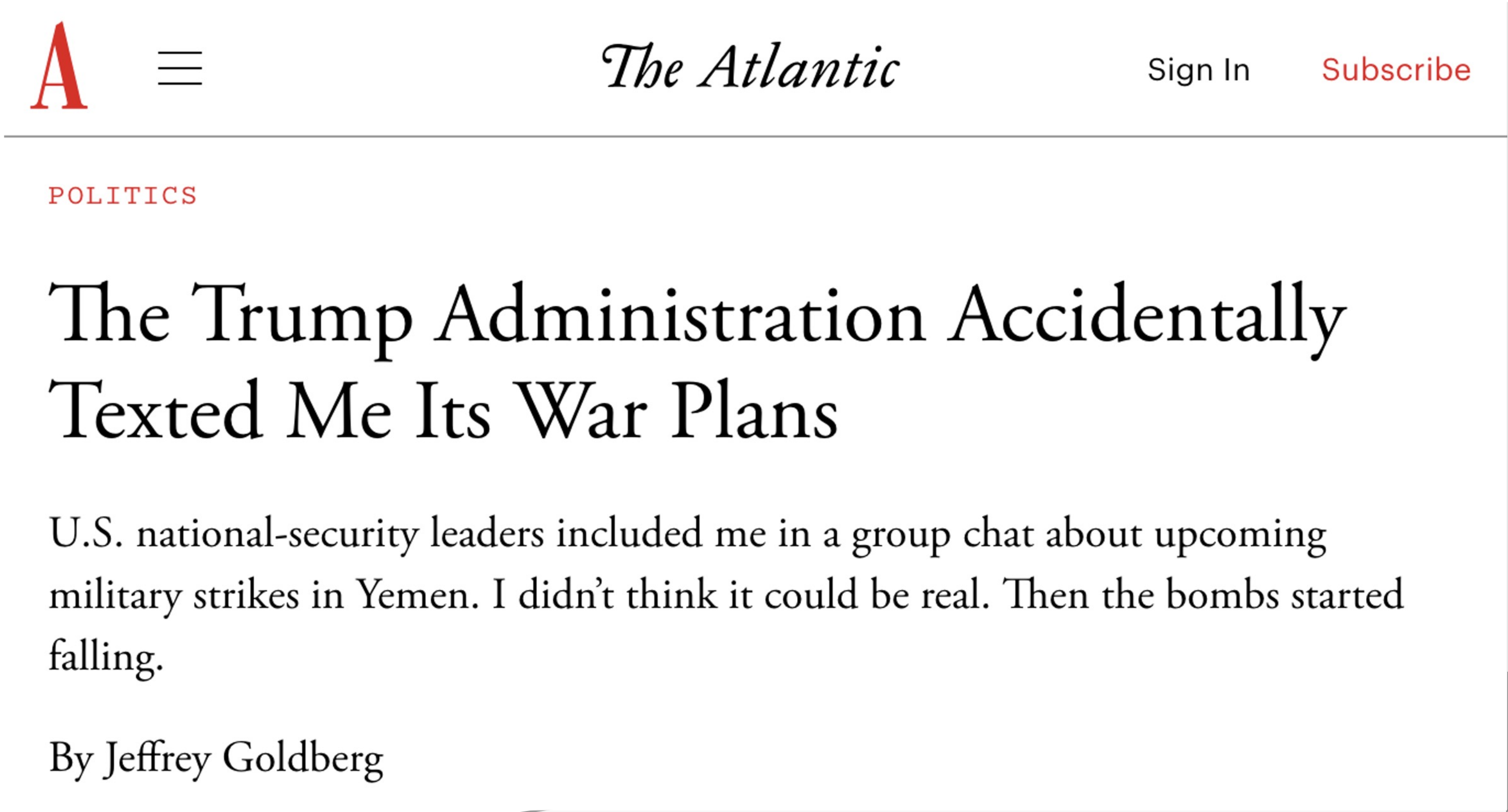
By Jeffrey Goldberg

March 24, 2025

https://archive.is/u5txN

Chapter 1: Signalgate

- **Mike Walz**
  National Security Advisor
- **Pete Hegseth**
  Secretary of Defense
- **John Radcliffe**
  Director of the CIA



POLITICS

The Trump Administration Accidentally Texted Me Its War Plans

U.S. national-security leaders included me in a group chat about upcoming military strikes in Yemen. I didn't think it could be real. Then the bombs started falling.

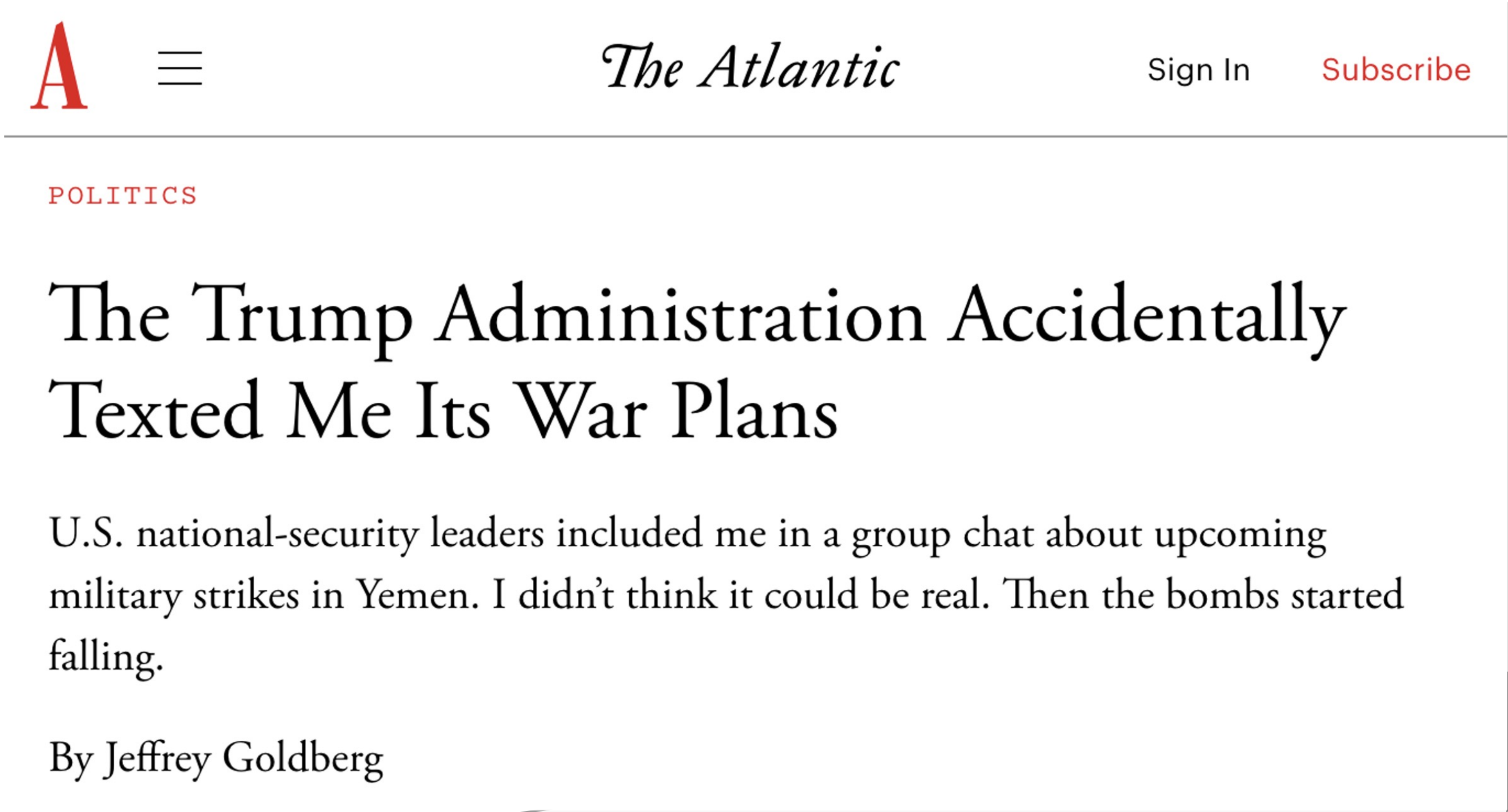
By Jeffrey Goldberg

March 24, 2025

https://archive.is/u5txN

Chapter 1: Signalgate

- **Mike Walz**
  National Security Advisor
- **Pete Hegseth**
  Secretary of Defense
- **John Radcliffe**
  Director of the CIA
- **Tulsi Gabbard**
  DNI



POLITICS

The Trump Administration Accidentally Texted Me Its War Plans

U.S. national-security leaders included me in a group chat about upcoming military strikes in Yemen. I didn't think it could be real. Then the bombs started falling.

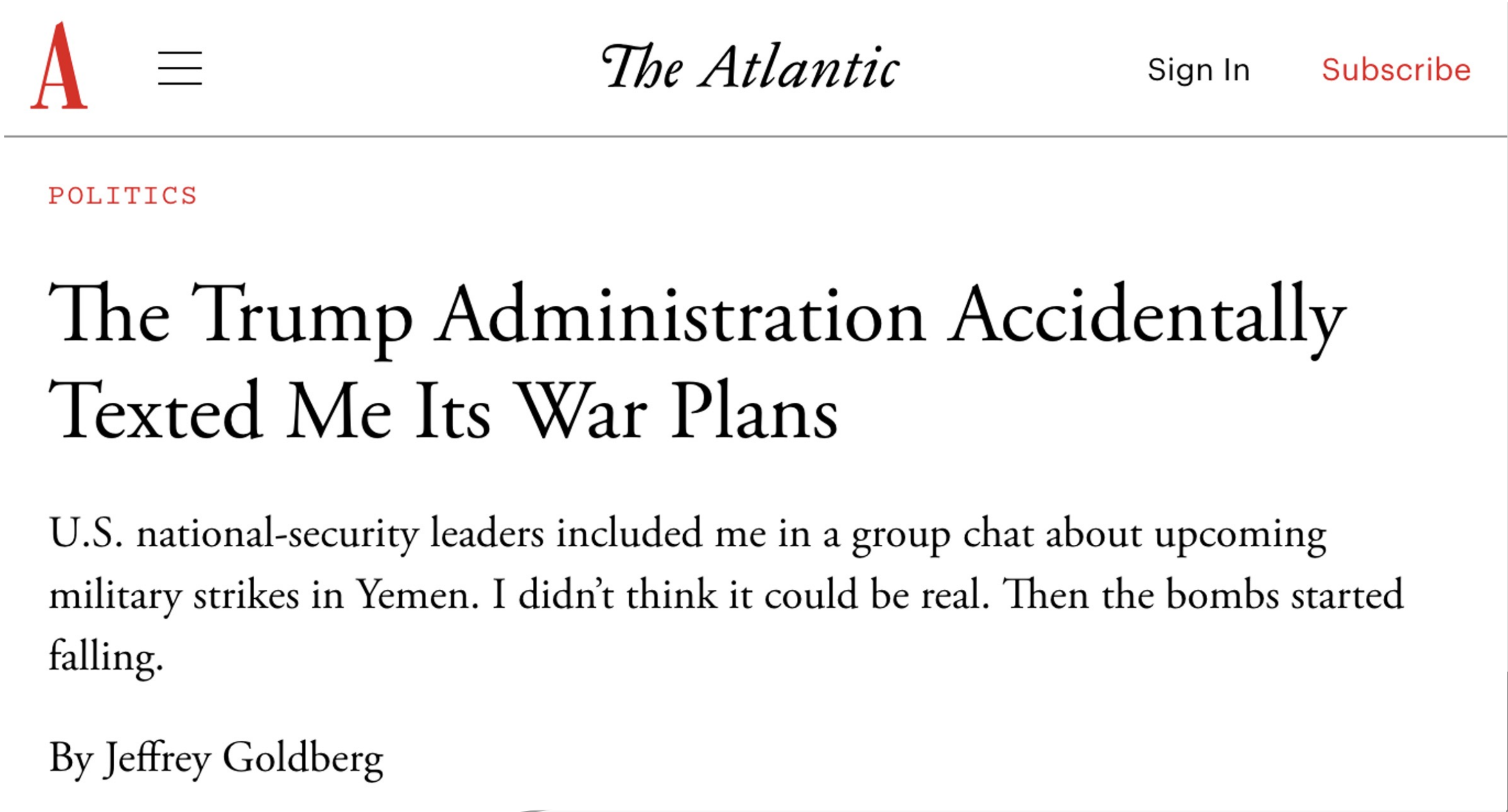
By Jeffrey Goldberg

March 24, 2025

https://archive.is/u5txN

Chapter 1: Signalgate

- **Mike Walz**
  National Security Advisor
- **Pete Hegseth**
  Secretary of Defense
- **John Radcliffe**
  Director of the CIA
- **Tulsi Gabbard**
  DNI
- **Stephen Miller**
  racist vampire



POLITICS

The Trump Administration Accidentally Texted Me Its War Plans

U.S. national-security leaders included me in a group chat about upcoming military strikes in Yemen. I didn't think it could be real. Then the bombs started falling.

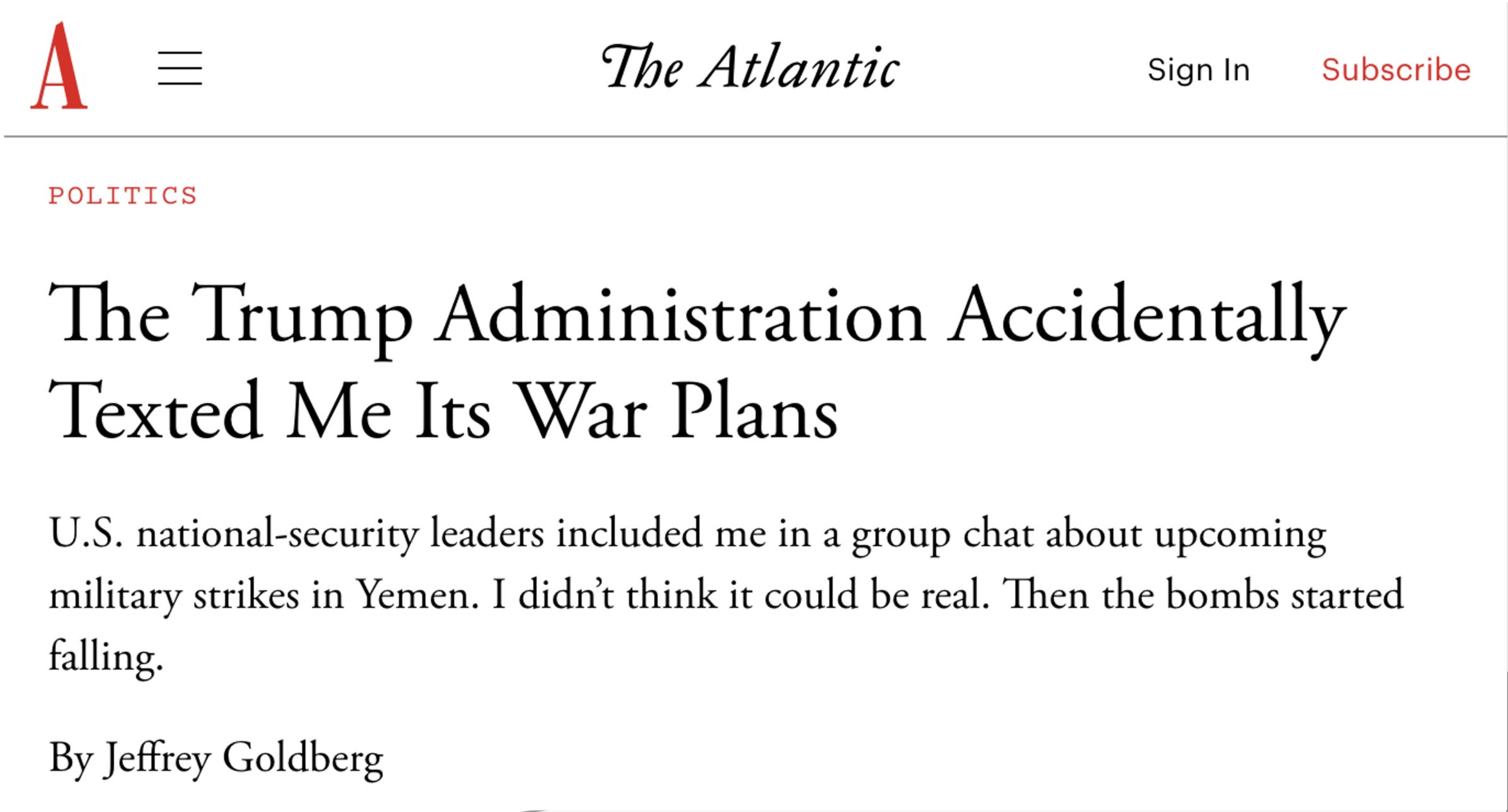
By Jeffrey Goldberg

March 24, 2025

https://archive.is/u5txN

Chapter 1: Signalgate

- **Mike Walz**
  National Security Advisor
- **Pete Hegseth**
  Secretary of Defense
- **John Radcliffe**
  Director of the CIA
- **Tulsi Gabbard**
  DNI
- **Stephen Miller**
  racist vampire
- **… and many more**



POLITICS

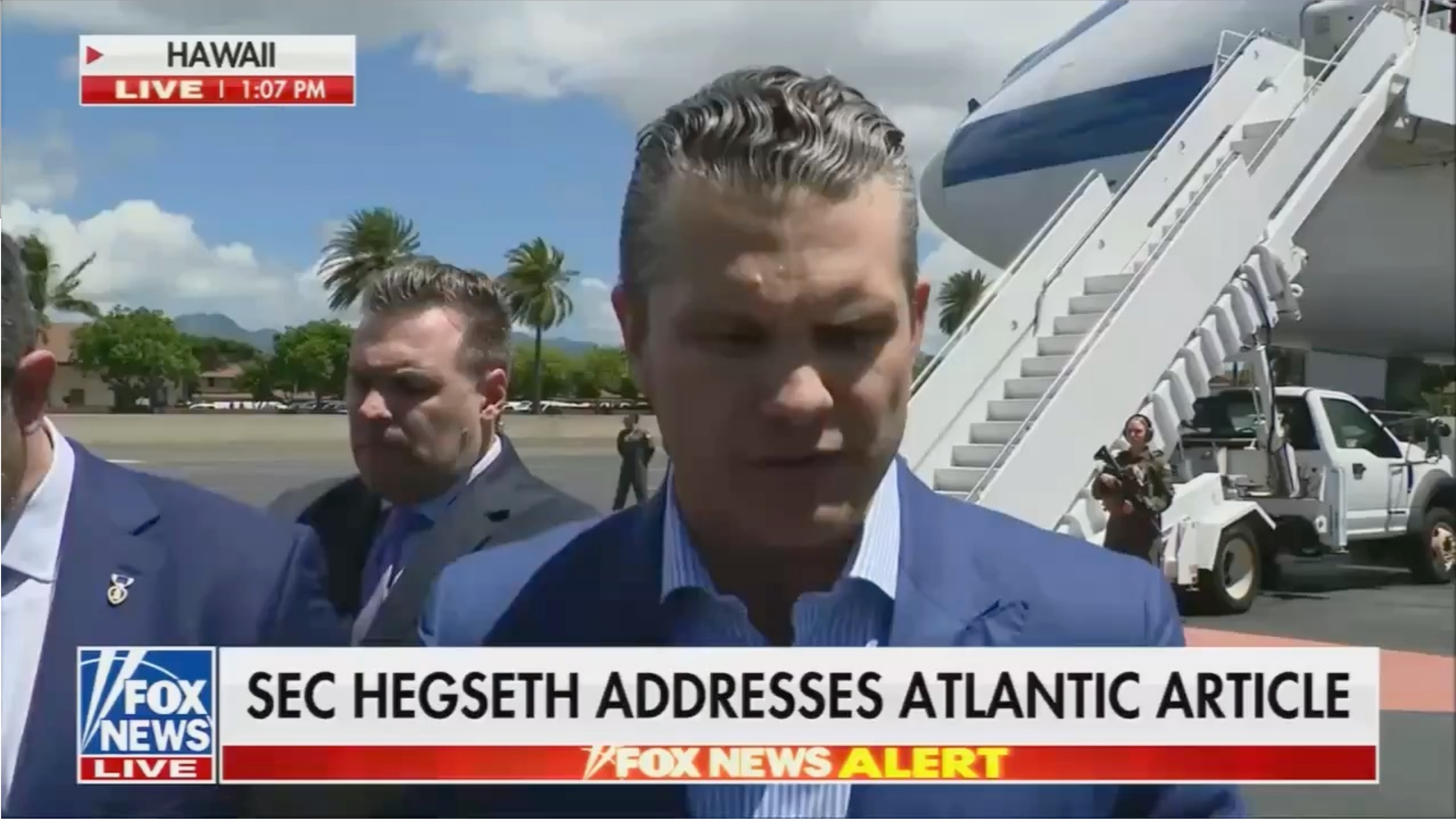
The Trump Administration Accidentally Texted Me Its War Plans

U.S. national-security leaders included me in a group chat about upcoming military strikes in Yemen. I didn't think it could be real. Then the bombs started falling.

By Jeffrey Goldberg

March 24, 2025

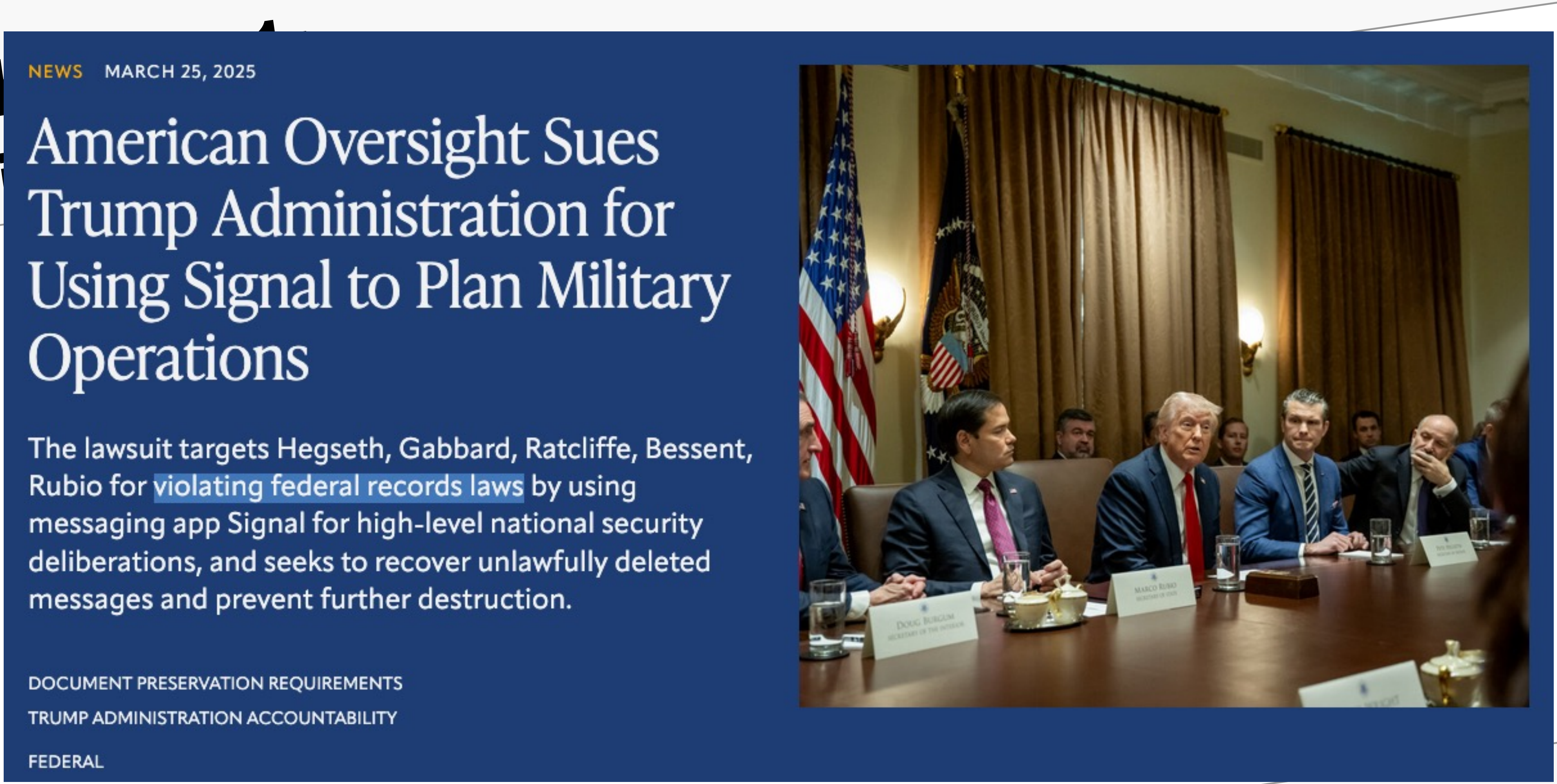
https://archive.is/u5txN



SEC HEGSETH ADDRESSES ATLANTIC ARTICLE

Cl

S



NEWS MARCH 25, 2025

American Oversight Sues Trump Administration for Using Signal to Plan Military Operations

The lawsuit targets Hegseth, Gabbard, Ratcliffe, Bessent, Rubio for violating federal records laws by using messaging app Signal for high-level national security deliberations, and seeks to recover unlawfully deleted messages and prevent further destruction.

DOCUMENT PRESERVATION REQUIREMENTS

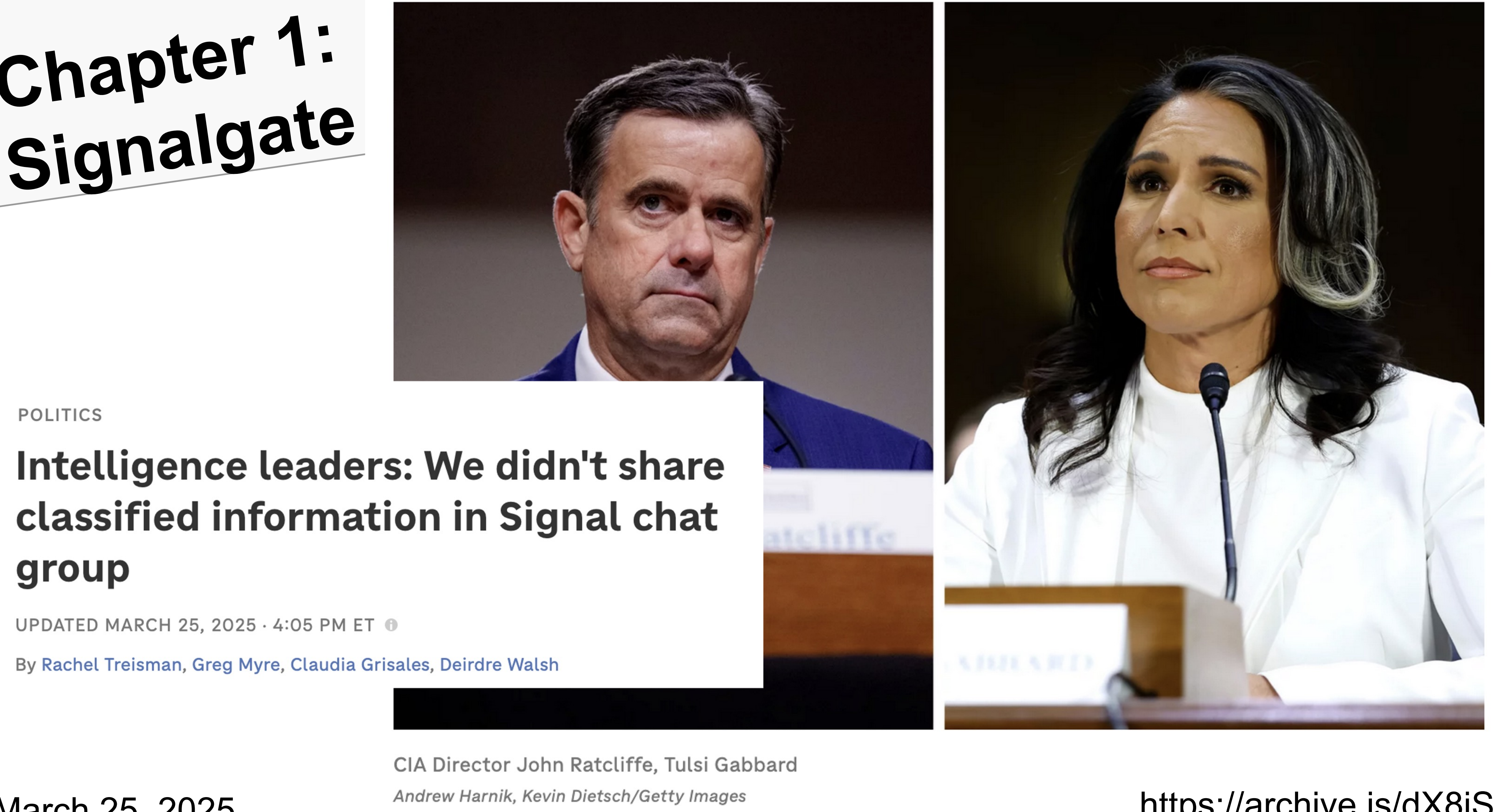
TRUMP ADMINISTRATION ACCOUNTABILITY

FEDERAL

March 25, 2025

https://americanoversight.org/american-oversight-sues-trump-administration-for-using-signal-to-plan-military-operations/

Chapter 1: Signalgate



POLITICS

Intelligence leaders: We didn't share classified information in Signal chat group

UPDATED MARCH 25, 2025 · 4:05 PM ET

By Rachel Treisman, Greg Myre, Claudia Grisales, Deirdre Walsh

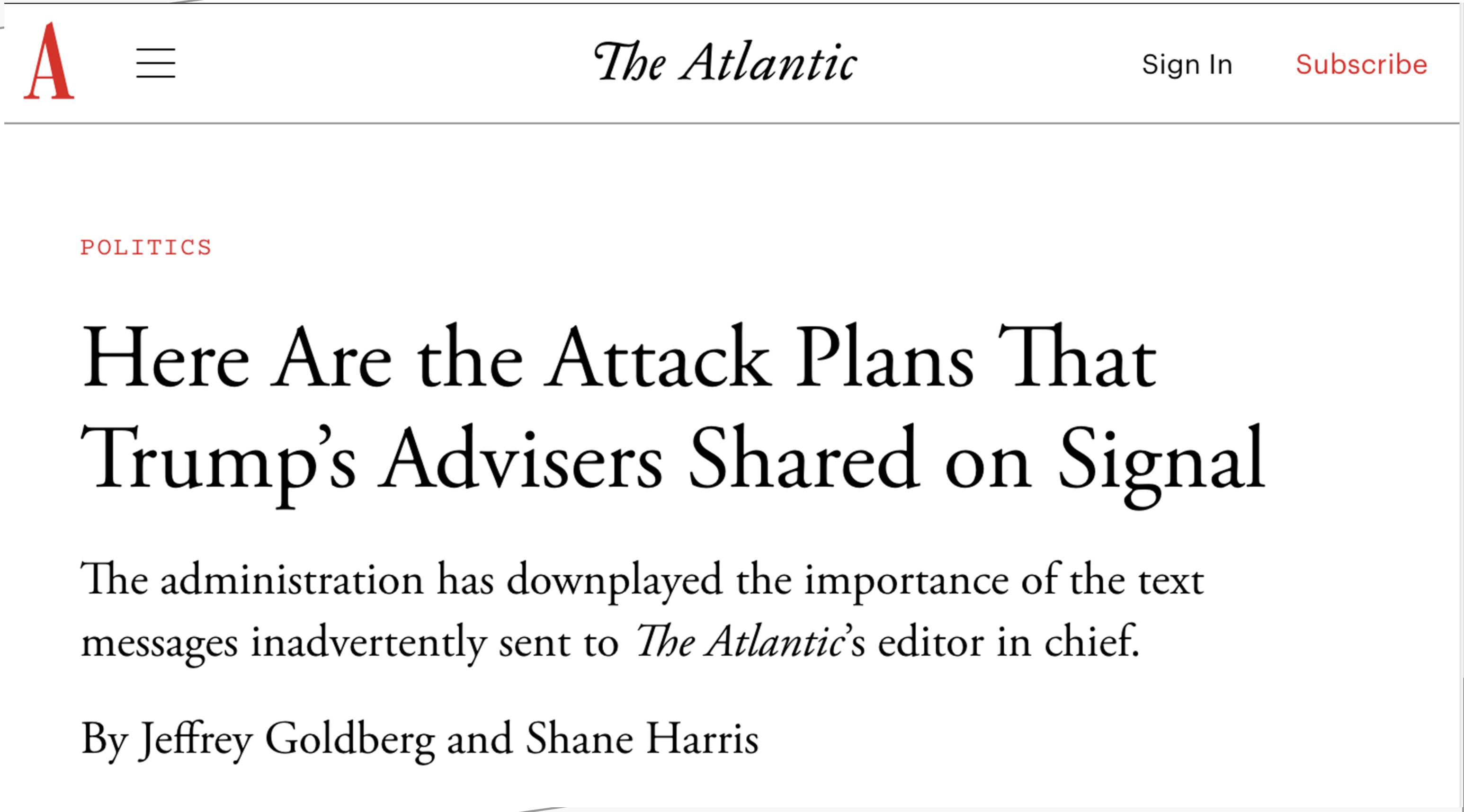
CIA Director John Ratcliffe, Tulsi Gabbard

Andrew Harnik, Kevin Dietsch/Getty Images

March 25, 2025

https://archive.is/dX8jS

Chapter 1: Signalgate



POLITICS

Here Are the Attack Plans That Trump's Advisers Shared on Signal

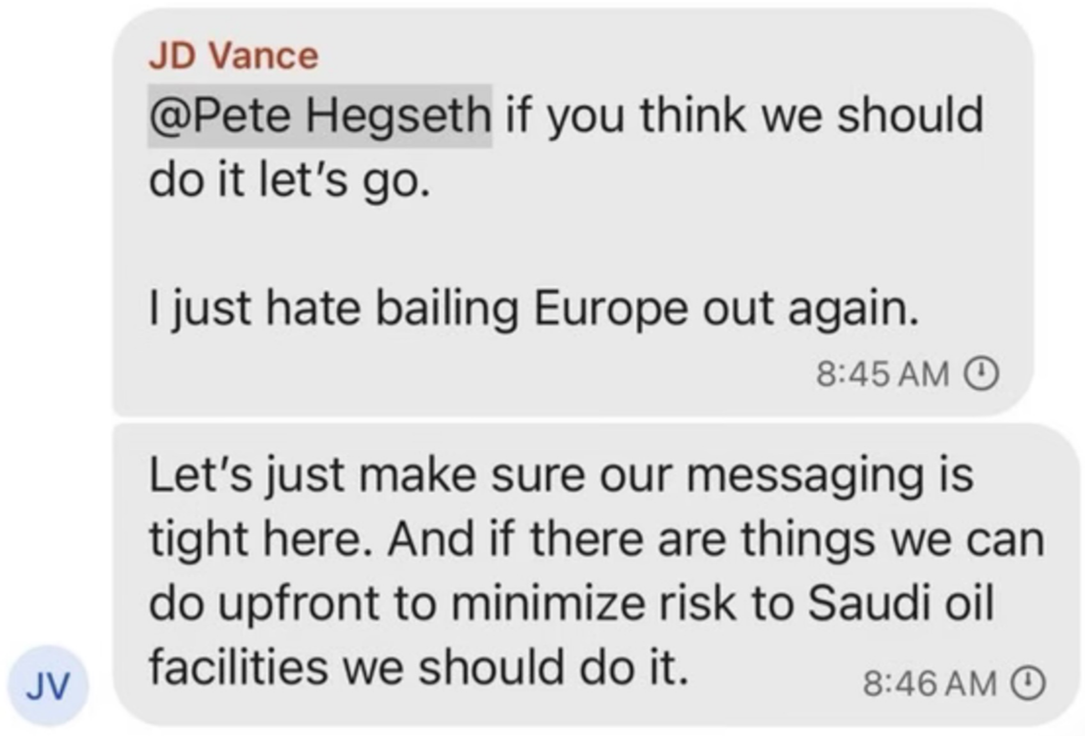
The administration has downplayed the importance of the text messages inadvertently sent to *The Atlantic*'s editor in chief.

By Jeffrey Goldberg and Shane Harris

March 26, 2025

https://archive.is/vnPIk

Chapter 1: Signalgate



JD Vance

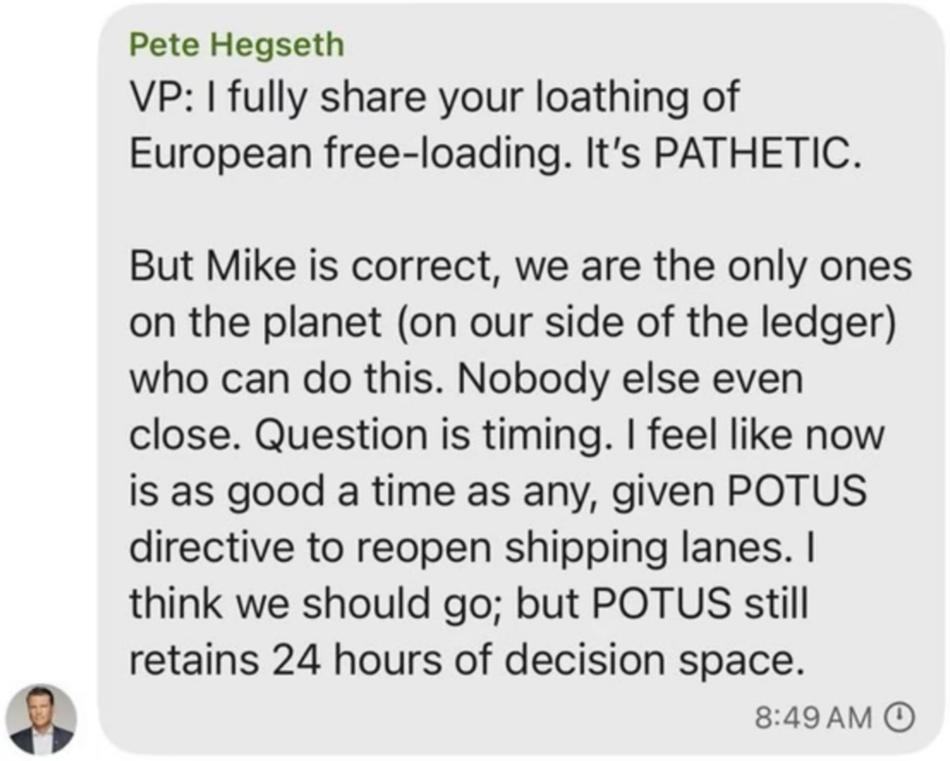
@Pete Hegseth if you think we should do it let's go.

I just hate bailing Europe out again.

8:45 AM

Let's just make sure our messaging is tight here. And if there are things we can do upfront to minimize risk to Saudi oil facilities we should do it.

8:46 AM



Pete Hegseth

VP: I fully share your loathing of European free-loading. It's PATHETIC.

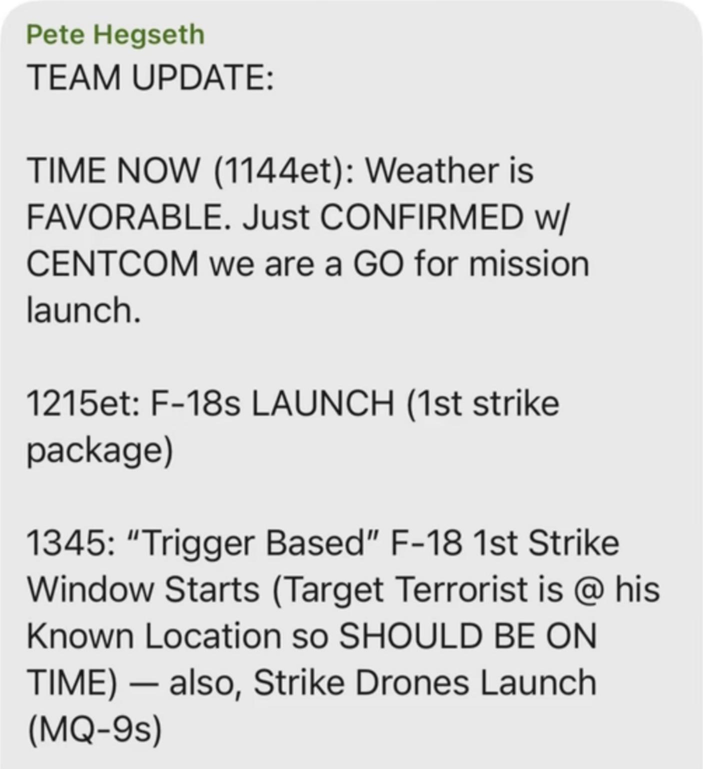
But Mike is correct, we are the only ones on the planet (on our side of the ledger) who can do this. Nobody else even close. Question is timing. I feel like now is as good a time as any, given POTUS directive to reopen shipping lanes. I think we should go; but POTUS still retains 24 hours of decision space.

8:49 AM

Chat logs from March 15, 2025

https://archive.is/vnPIk

Chapter 1: Signalgate



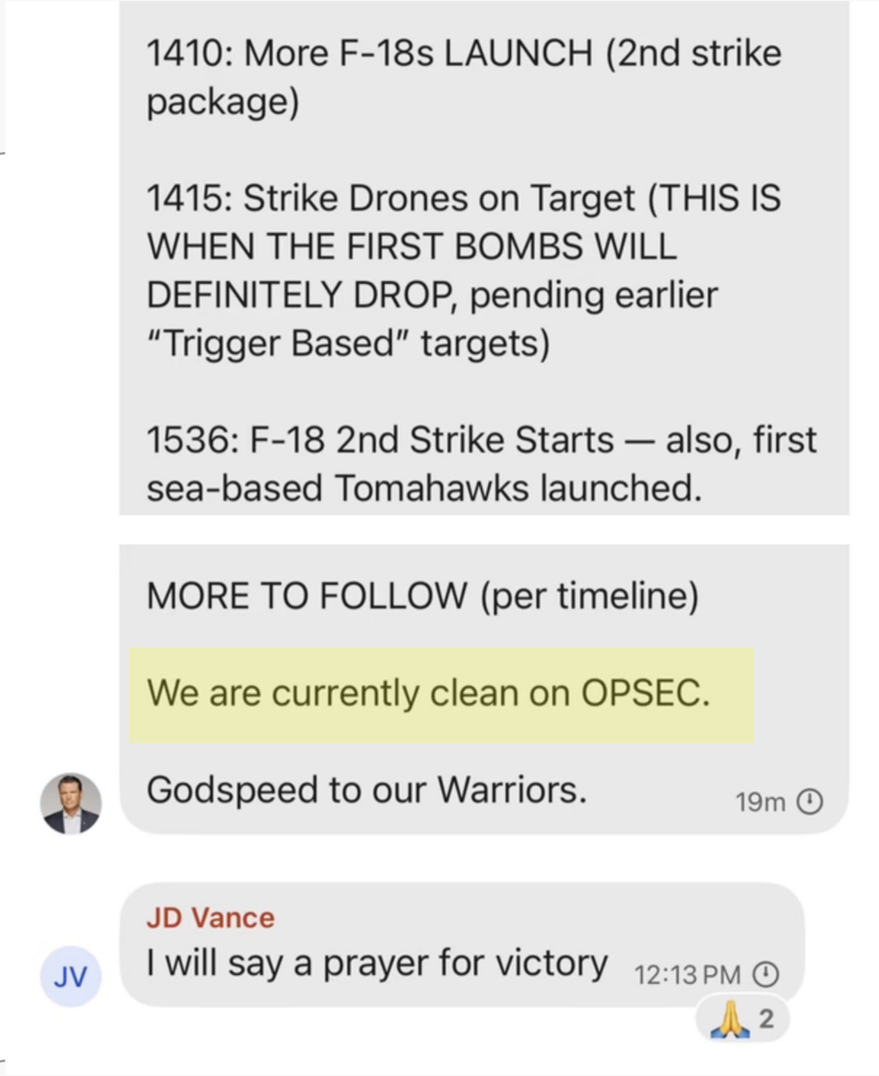
Pete Hegseth

TEAM UPDATE:

TIME NOW (1144et): Weather is FAVORABLE. Just CONFIRMED w/ CENTCOM we are a GO for mission launch.

1215et: F-18s LAUNCH (1st strike package)

1345: “Trigger Based” F-18 1st Strike Window Starts (Target Terrorist is @ his Known Location so SHOULD BE ON TIME) — also, Strike Drones Launch (MQ-9s)



1410: More F-18s LAUNCH (2nd strike package)

1415: Strike Drones on Target (THIS IS WHEN THE FIRST BOMBS WILL DEFINITELY DROP, pending earlier “Trigger Based” targets)

1536: F-18 2nd Strike Starts — also, first sea-based Tomahawks launched.

MORE TO FOLLOW (per timeline)

We are currently clean on OPSEC.

Godspeed to our Warriors. 19m

JV

JD Vance

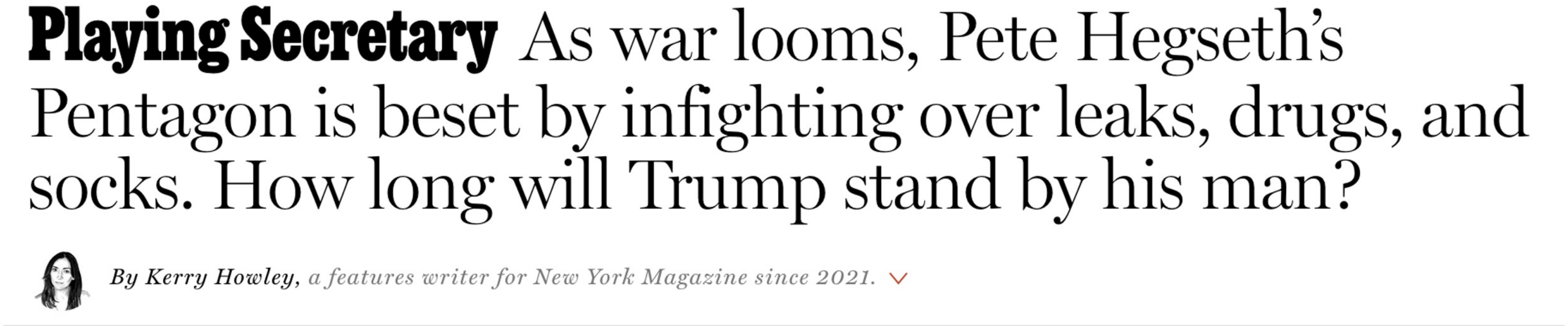
I will say a prayer for victory 12:13 PM

🙏 2

Chat logs from March 15, 2025

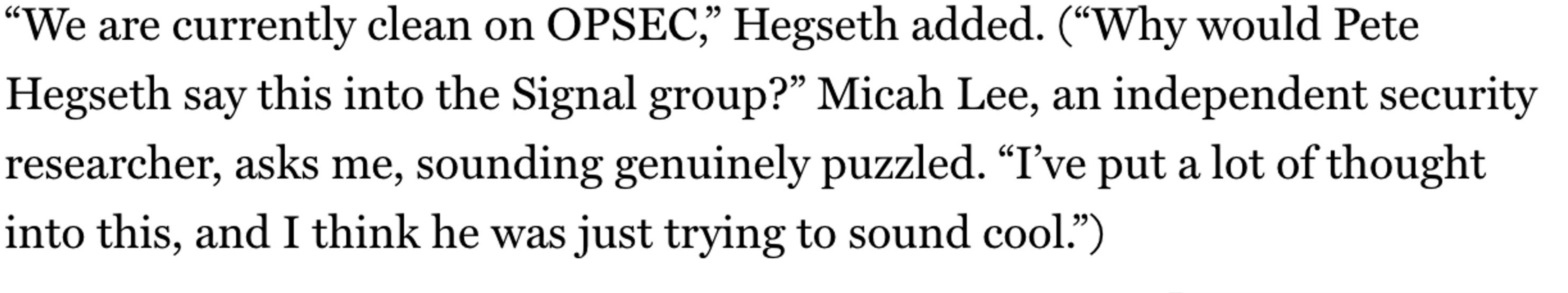
https://archive.is/vnPIk

Chapter 1: Signalgate



Playing Secretary As war looms, Pete Hegseth's Pentagon is beset by infighting over leaks, drugs, and socks. How long will Trump stand by his man?

By Kerry Howley, a features writer for New York Magazine since 2021.

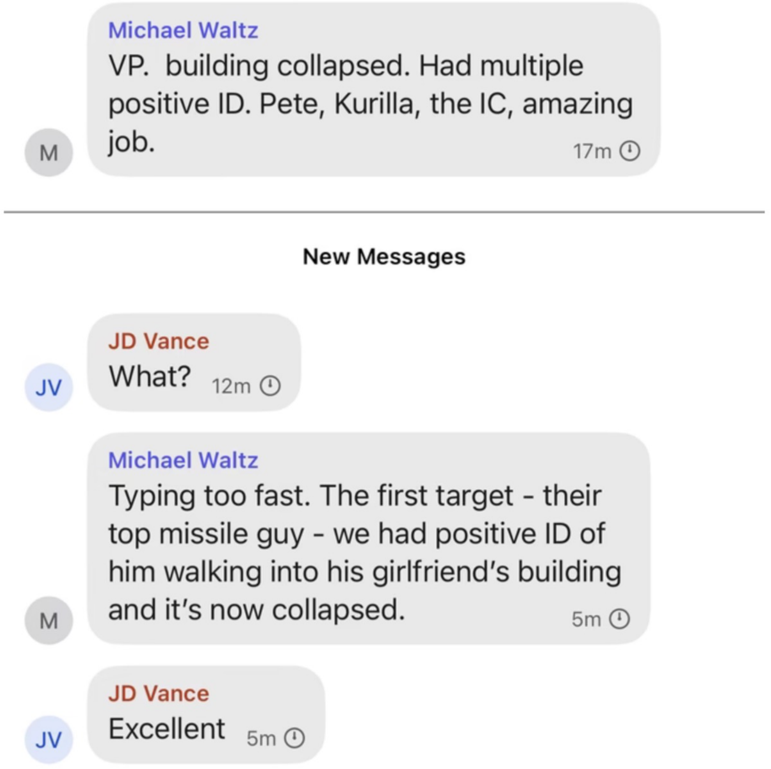


"We are currently clean on OPSEC," Hegseth added. ("Why would Pete Hegseth say this into the Signal group?" Micah Lee, an independent security researcher, asks me, sounding genuinely puzzled. "I've put a lot of thought into this, and I think he was just trying to sound cool.")

New York Magazine article from June 13, 2025

https://archive.is/eIo90

Chapter 1: Signalgate



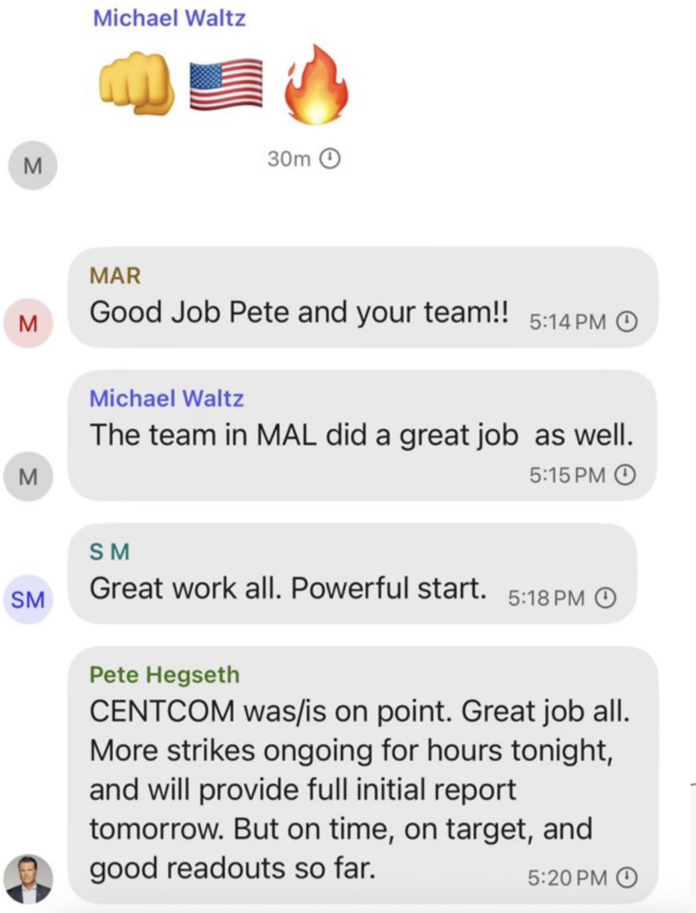
Michael Waltz
VP. building collapsed. Had multiple positive ID. Pete, Kurilla, the IC, amazing job. 17m

New Messages

JD Vance
What? 12m

Michael Waltz
Typing too fast. The first target - their top missile guy - we had positive ID of him walking into his girlfriend's building and it's now collapsed. 5m

JD Vance
Excellent 5m



Michael Waltz
👊🇺🇸🔥
30m

MAR
Good Job Pete and your team!! 5:14 PM

Michael Waltz
The team in MAL did a great job as well. 5:15 PM

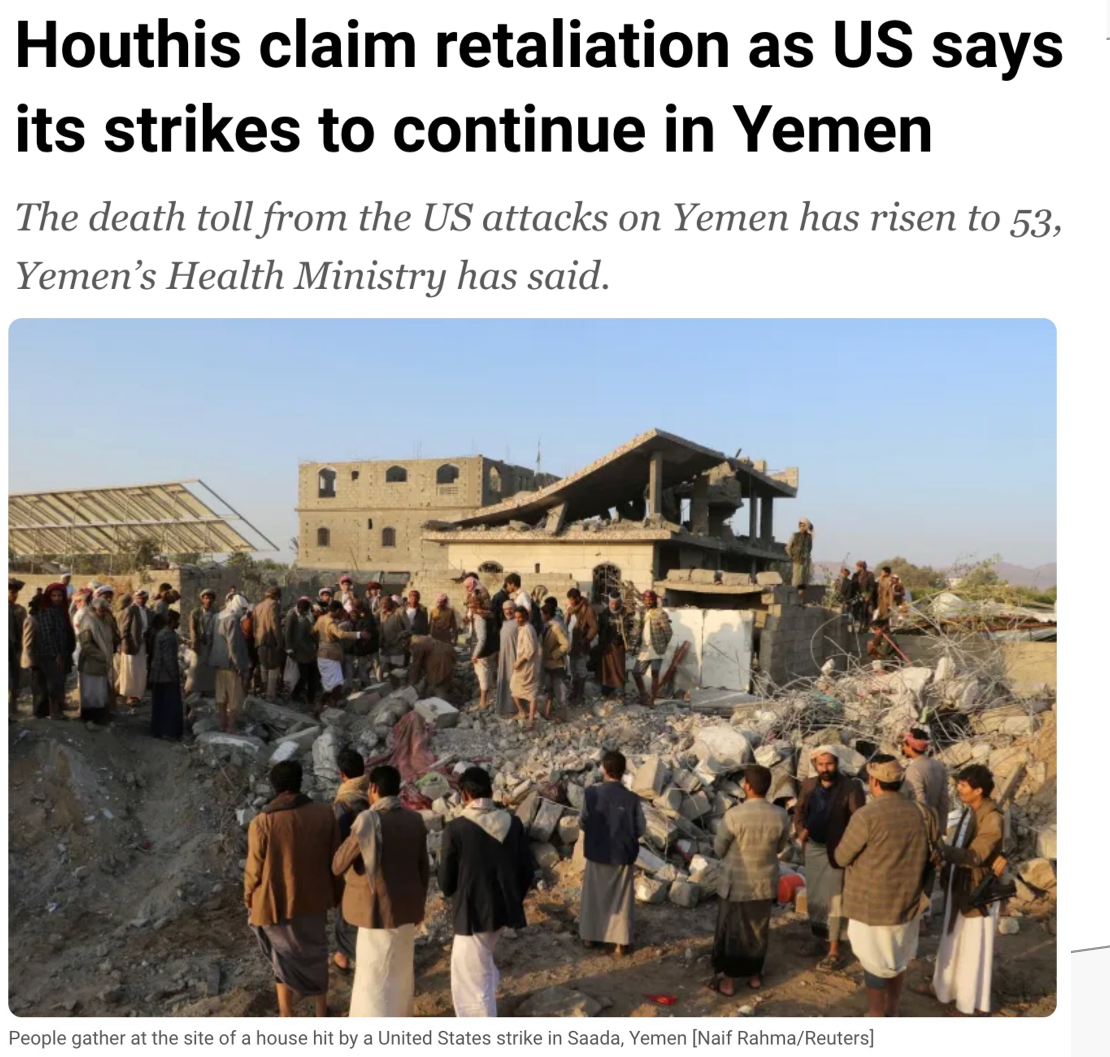
S M
Great work all. Powerful start. 5:18 PM

Pete Hegseth
CENTCOM was/is on point. Great job all. More strikes ongoing for hours tonight, and will provide full initial report tomorrow. But on time, on target, and good readouts so far. 5:20 PM

Chat logs from March 15, 2025

https://archive.is/vnPIk

Chapter 1: Signalgate



Houthis claim retaliation as US says its strikes to continue in Yemen

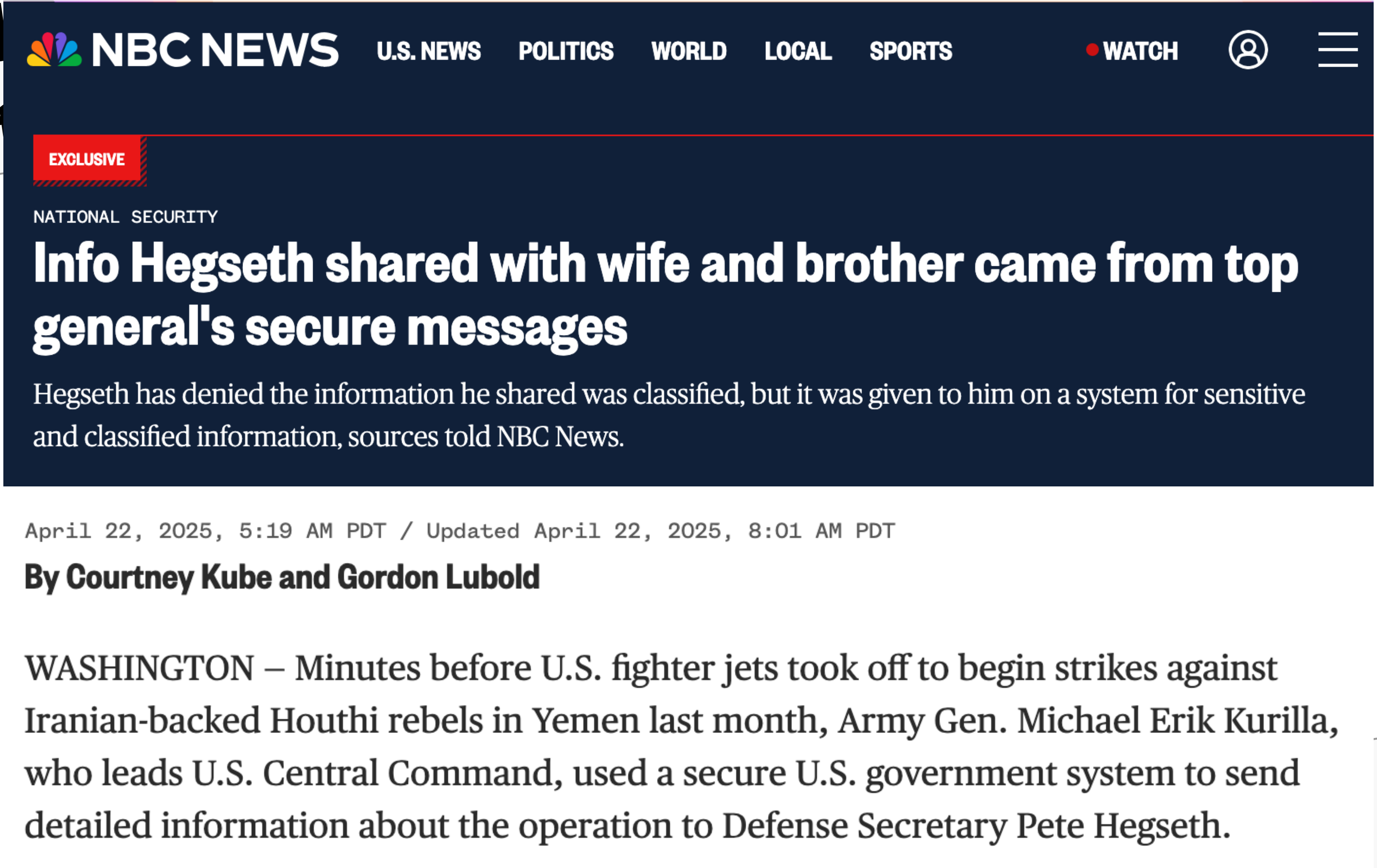
The death toll from the US attacks on Yemen has risen to 53, Yemen’s Health Ministry has said.

People gather at the site of a house hit by a United States strike in Saada, Yemen [Naif Rahma/Reuters]

Al Jazeera article from March 16, 2025

https://archive.is/ODHDb

Chapter 1
Signalgat



EXCLUSIVE

NATIONAL SECURITY

Info Hegseth shared with wife and brother came from top general's secure messages

Hegseth has denied the information he shared was classified, but it was given to him on a system for sensitive and classified information, sources told NBC News.

April 22, 2025, 5:19 AM PDT / Updated April 22, 2025, 8:01 AM PDT

By Courtney Kube and Gordon Lubold

WASHINGTON – Minutes before U.S. fighter jets took off to begin strikes against Iranian-backed Houthi rebels in Yemen last month, Army Gen. Michael Erik Kurilla, who leads U.S. Central Command, used a secure U.S. government system to send detailed information about the operation to Defense Secretary Pete Hegseth.

April 22, 2025

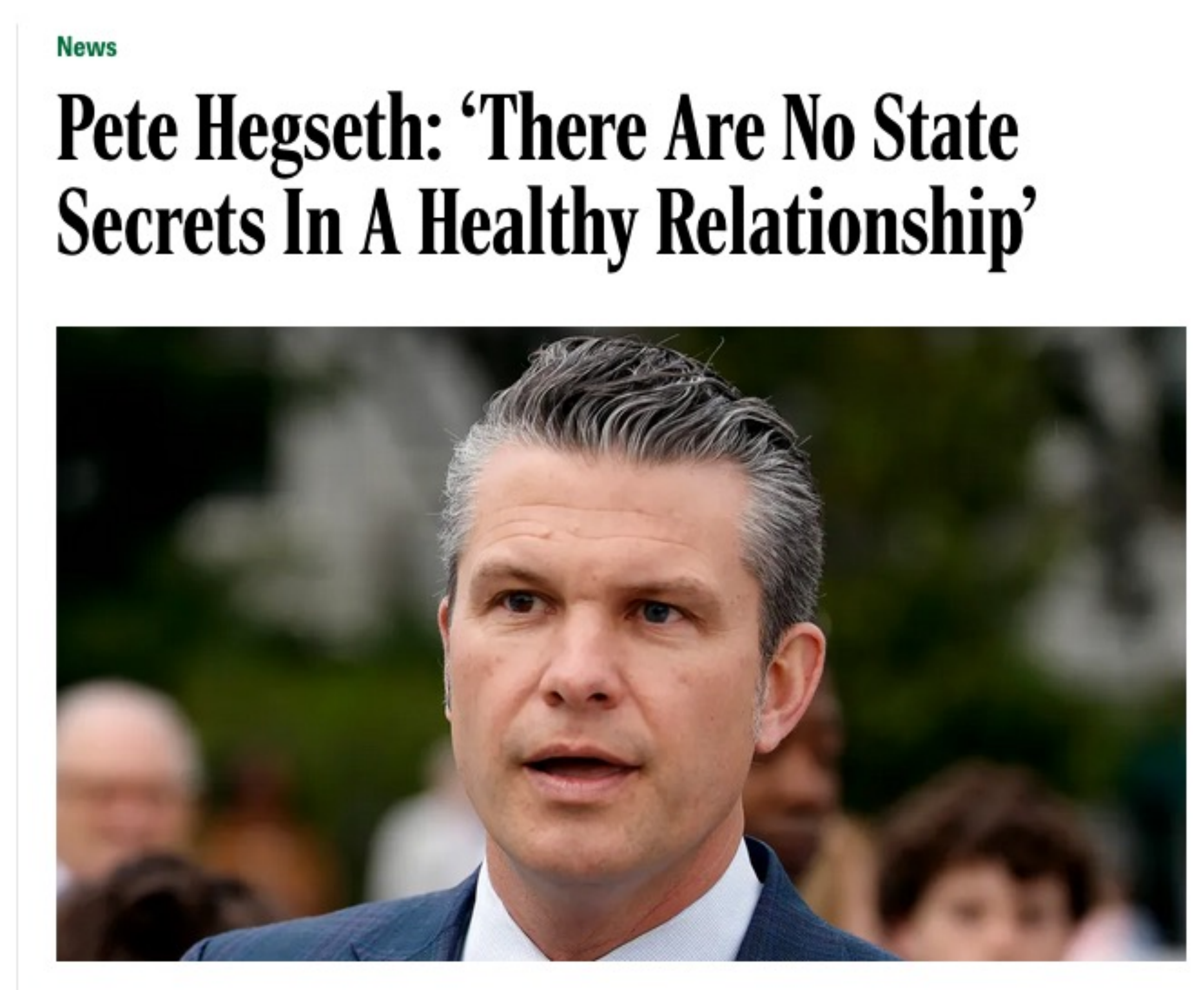
https://archive.is/u0BoI

FILE
504
NBC NEWS

Chapter 1: Signalgate

the ONION

America's Finest News Source



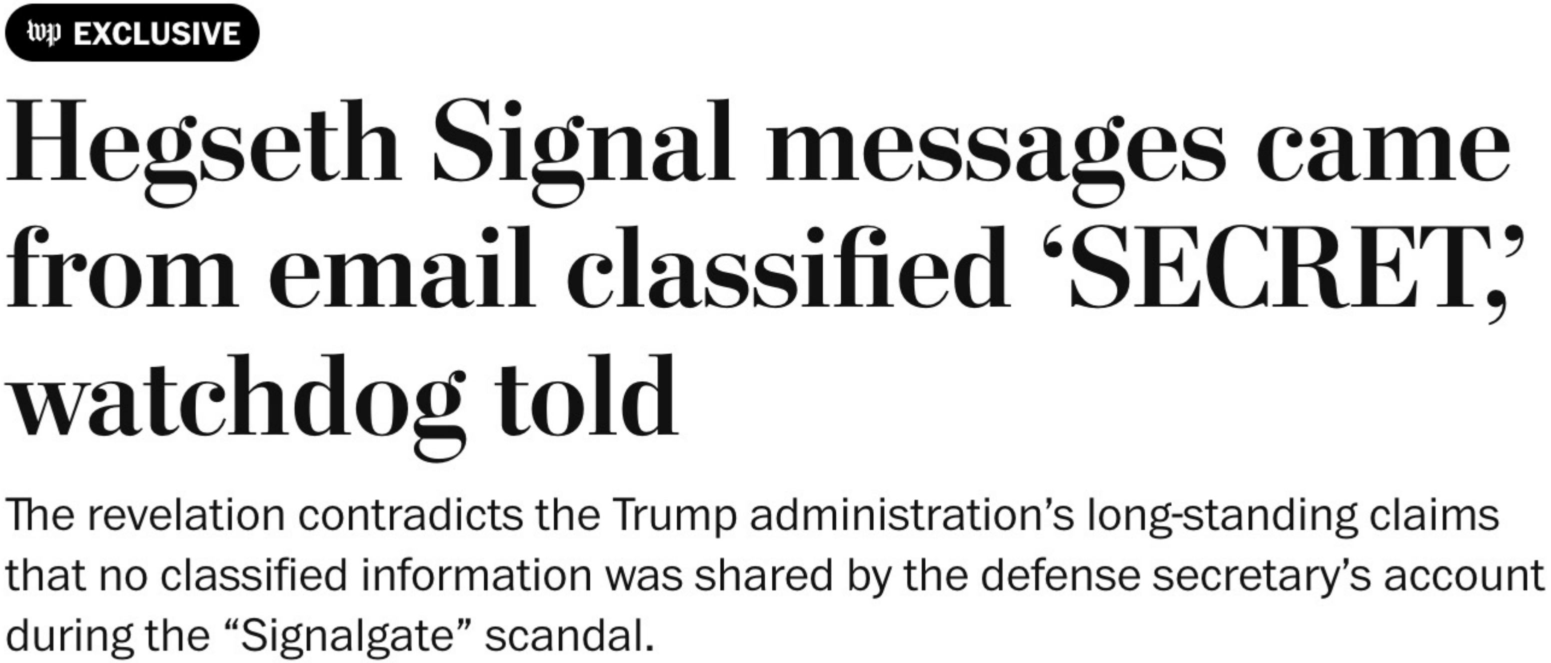
News

Pete Hegseth: 'There Are No State Secrets In A Healthy Relationship'

April 21, 2025

https://theonion.com/pete-hegseth-there-are-no-state-secrets-in-a-healthy-relationship/

Chapter 1: Signalgate



wp EXCLUSIVE

Hegseth Signal messages came from email classified ‘SECRET,’ watchdog told

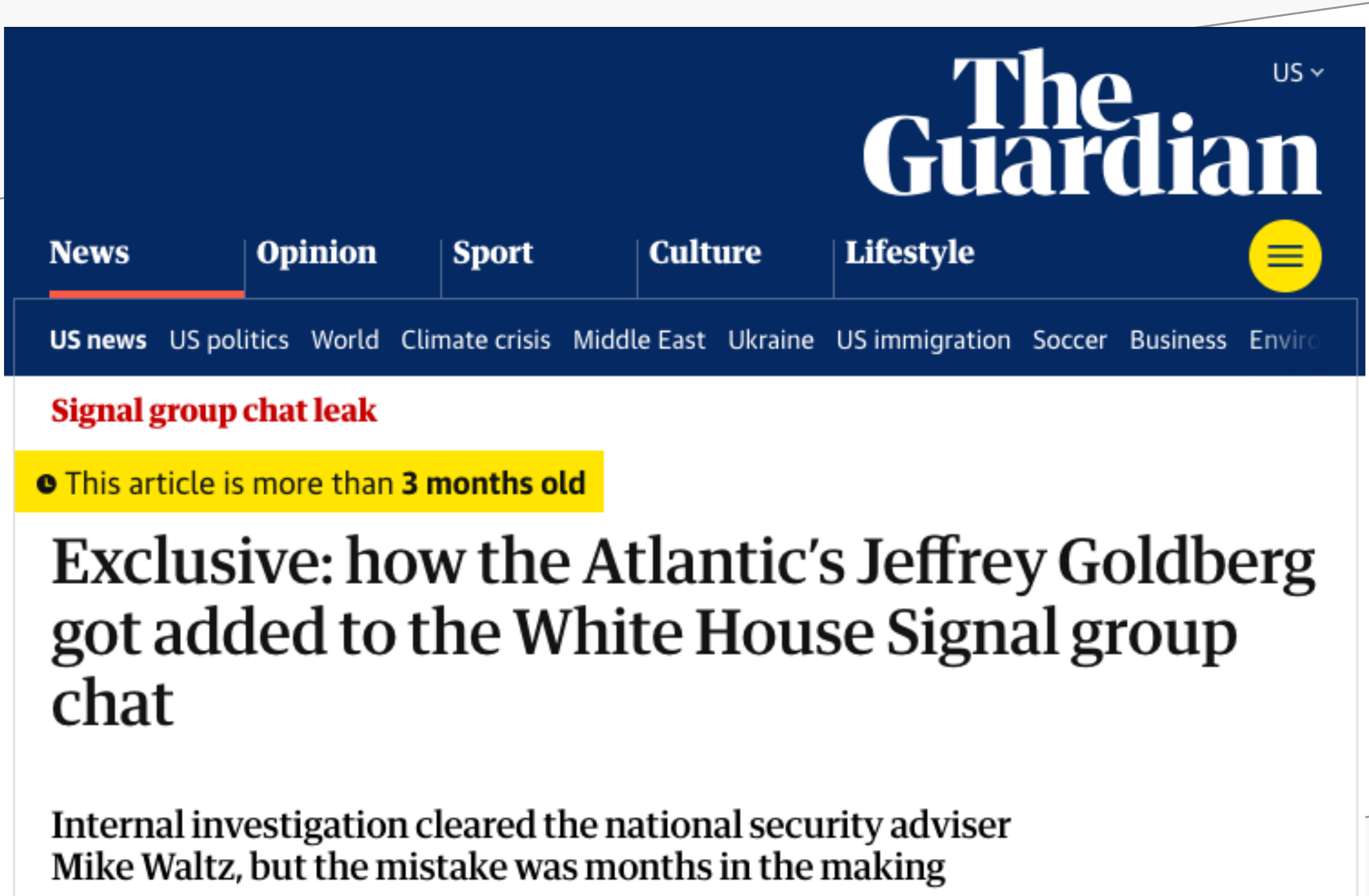
The revelation contradicts the Trump administration’s long-standing claims that no classified information was shared by the defense secretary’s account during the “Signalgate” scandal.

July 23, 2025

https://archive.is/aDIyn

Chapter 2: Hey Siri

October 2024, before Trump was elected…



The Guardian

US

News | Opinion | Sport | Culture | Lifestyle

US news | US politics | World | Climate crisis | Middle East | Ukraine | US immigration | Soccer | Business | Enviro

Signal group chat leak

This article is more than **3 months old**

Exclusive: how the Atlantic's Jeffrey Goldberg got added to the White House Signal group chat

Internal investigation cleared the national security adviser Mike Waltz, but the mistake was months in the making

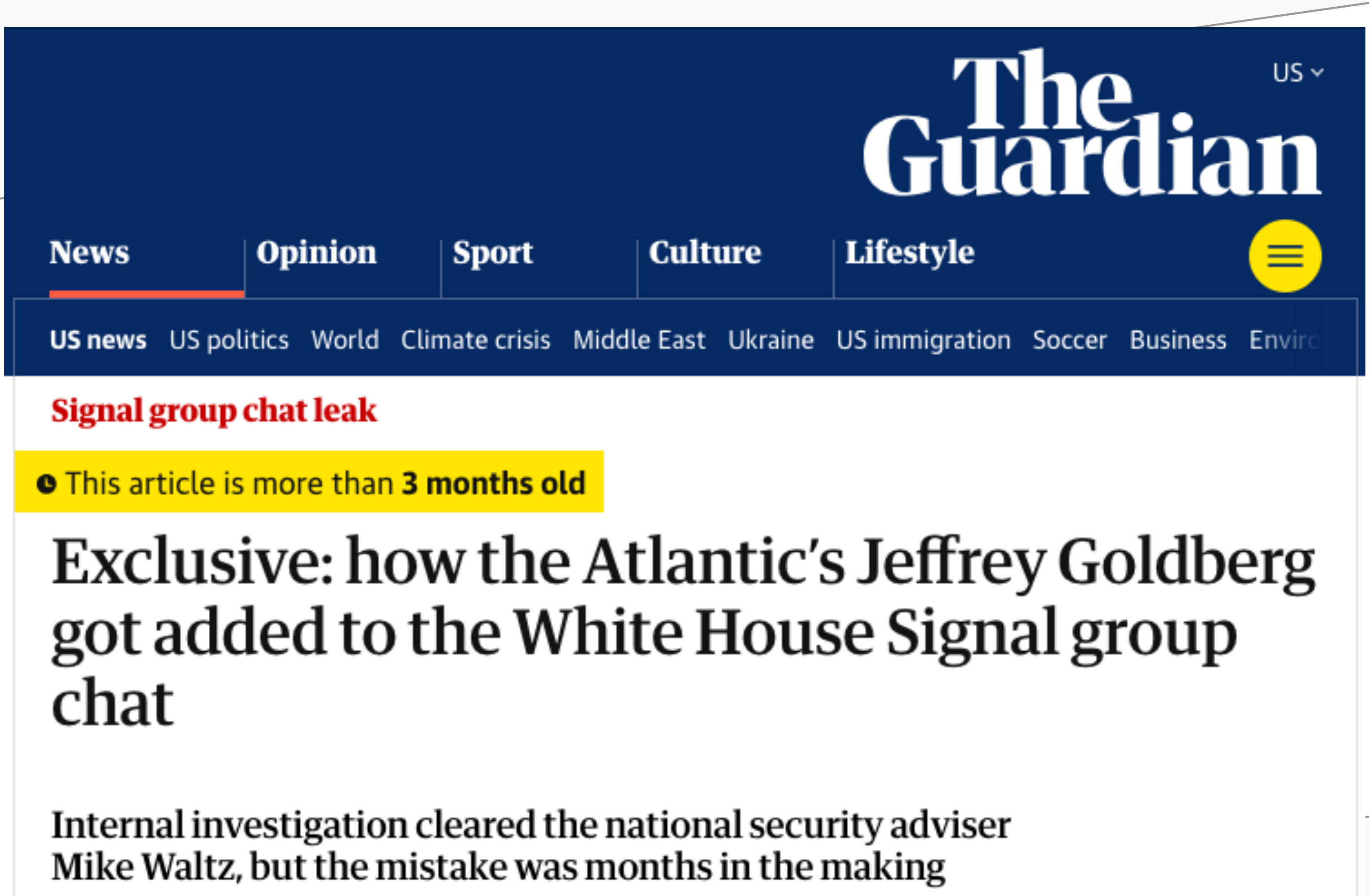
The Guardian article from April 6, 2025

https://archive.is/CnT25

Chapter 2: Hey Siri

October 2024, before Trump was elected:

- **Jeffrey Goldberg** The Atlantic editor-in-chef



Signal group chat leak

This article is more than **3 months old**

Exclusive: how the Atlantic's Jeffrey Goldberg got added to the White House Signal group chat

Internal investigation cleared the national security adviser Mike Waltz, but the mistake was months in the making

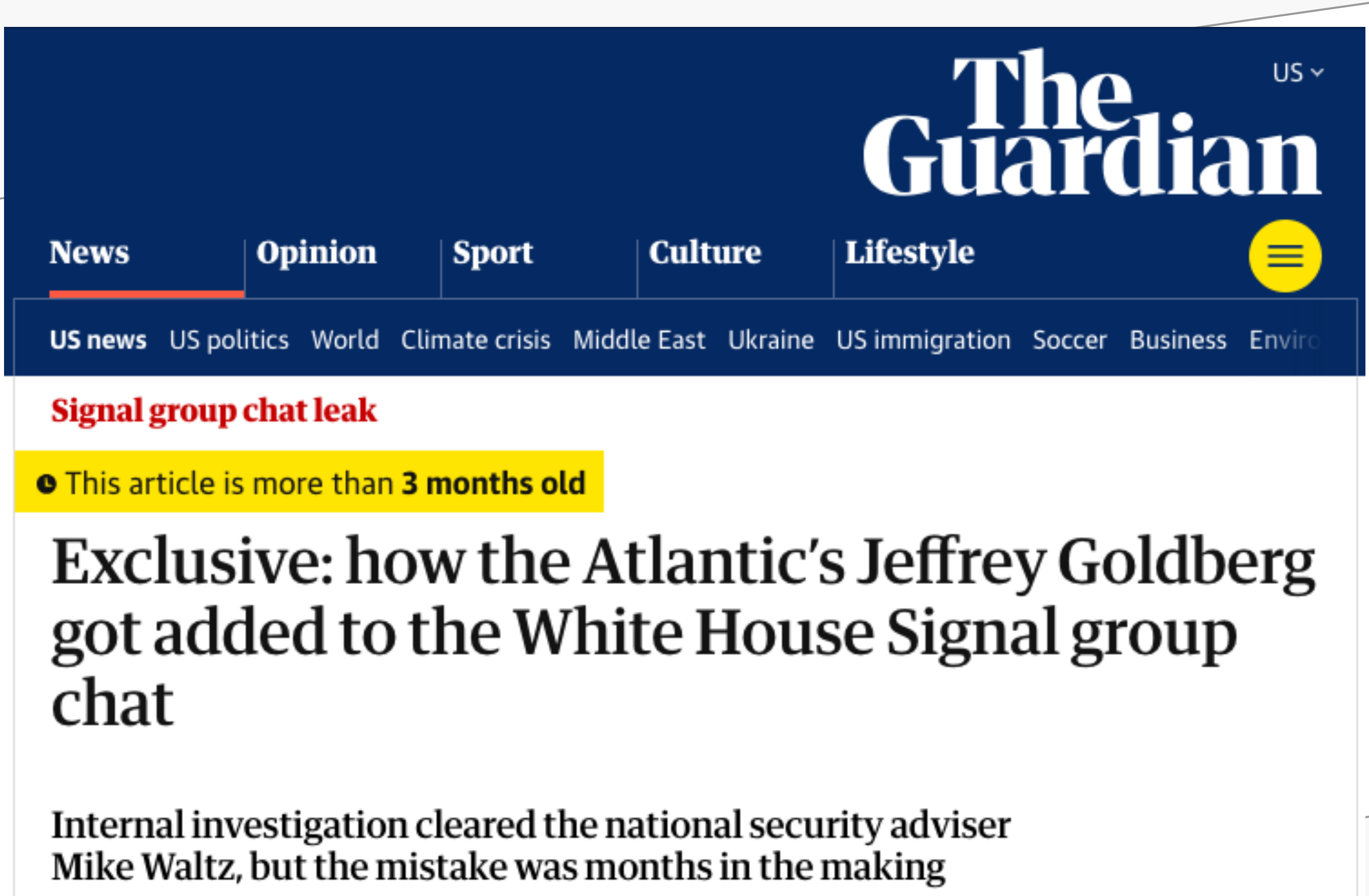
The Guardian article from April 6, 2025

https://archive.is/CnT25

Chapter 2: Hey Siri

October 2024, before Trump was elected:

- **Jeffrey Goldberg**
  The Atlantic editor-in-chef
- **Brian Hughes**
  Trump campaign spokesperson



Signal group chat leak

This article is more than **3 months old**

Exclusive: how the Atlantic's Jeffrey Goldberg got added to the White House Signal group chat

Internal investigation cleared the national security adviser Mike Waltz, but the mistake was months in the making

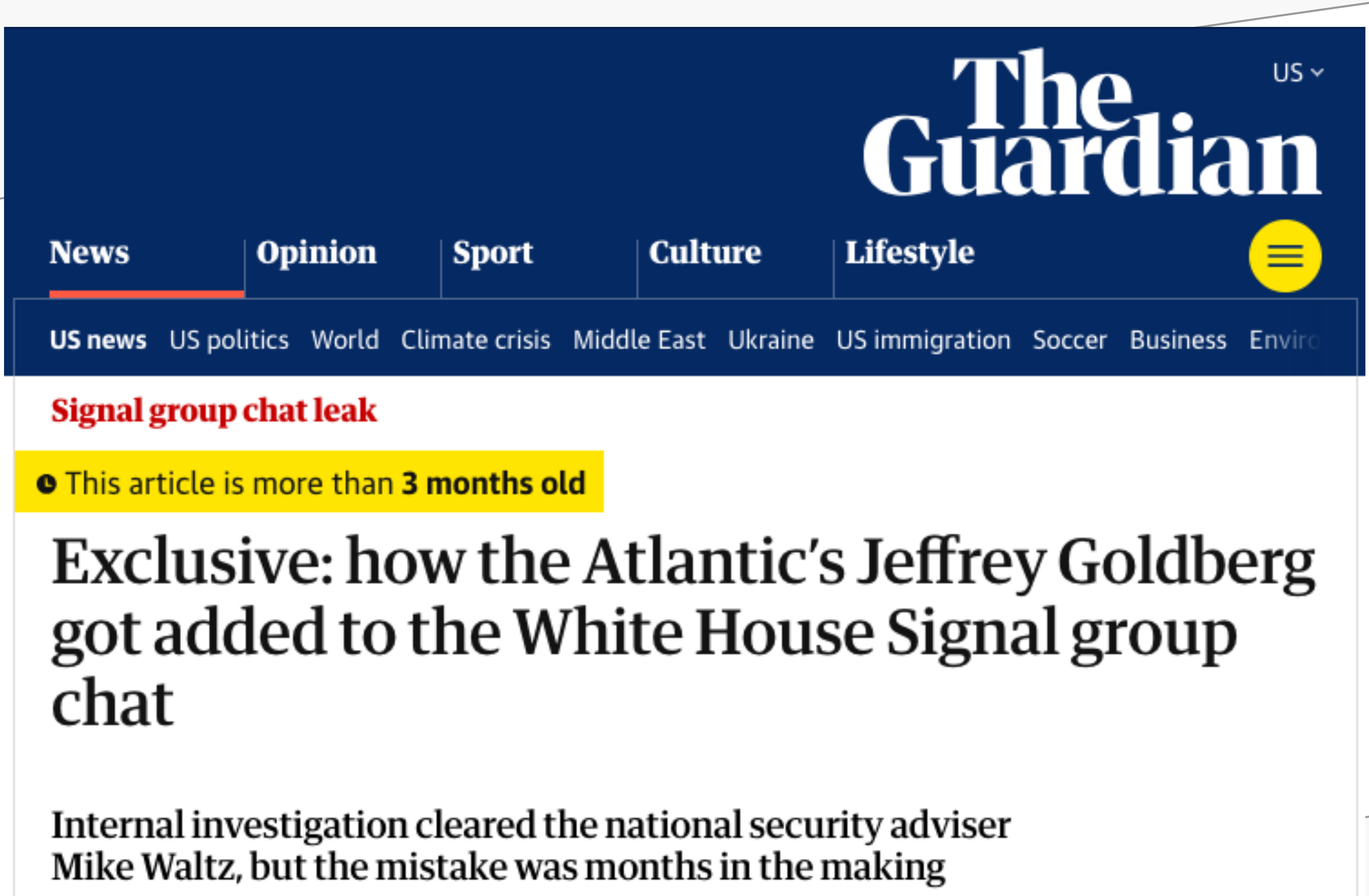
The Guardian article from April 6, 2025

https://archive.is/CnT25

Chapter 2: Hey Siri

October 2024, before Trump was elected:

- **Jeffrey Goldberg**
  The Atlantic editor-in-chief
- **Brian Hughes**
  Trump campaign spokesperson
- **Mike Waltz**
  Trump campaign national security surrogate



Signal group chat leak

This article is more than **3 months old**

Exclusive: how the Atlantic's Jeffrey Goldberg got added to the White House Signal group chat

Internal investigation cleared the national security adviser Mike Waltz, but the mistake was months in the making

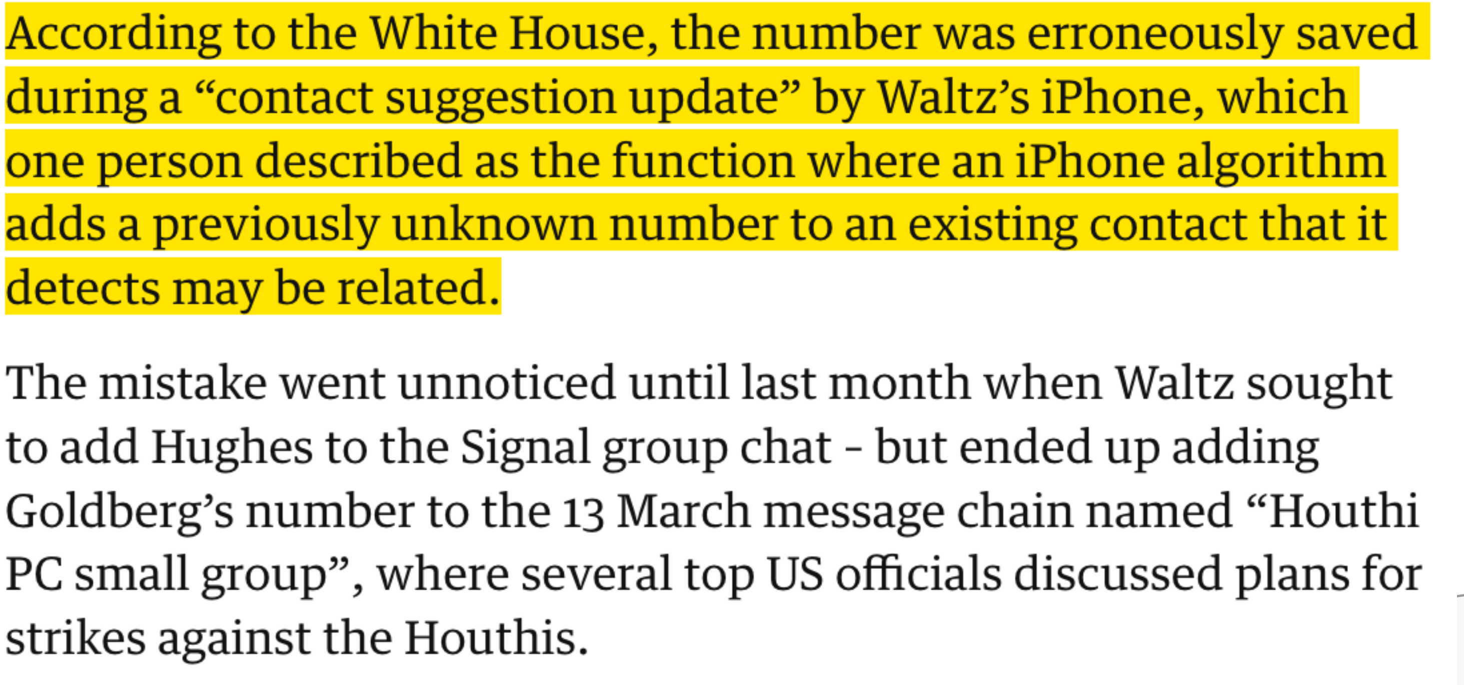
The Guardian article from April 6, 2025

https://archive.is/CnT25

Chapter 2: Hey Siri

October 2024, before Trump was elected:

- **Jeffrey Goldberg**
  The Atlantic editor-in-chief
- **Brian Hughes**
  Trump campaign spokesperson
- **Mike Waltz**
  Trump campaign national security surrogate



According to the White House, the number was erroneously saved during a “contact suggestion update” by Waltz’s iPhone, which one person described as the function where an iPhone algorithm adds a previously unknown number to an existing contact that it detects may be related.

The mistake went unnoticed until last month when Waltz sought to add Hughes to the Signal group chat - but ended up adding Goldberg’s number to the 13 March message chain named “Houthi PC small group”, where several top US officials discussed plans for strikes against the Houthis.

The Guardian article from April 6, 2025

https://archive.is/CnT25

Chapter 2: Hey Siri

October 2024, before Trump was elected:

- **Jeffrey Goldberg**
  The Atlantic editor-in-chef
- **Brian Hughes**
  Trump campaign spokesperson
- **Mike Waltz**
  Trump campaign national security surrogate

After Trump was elected:

- **Jeffrey Goldberg**
  The Atlantic editor-in-chef
- **Brian Hughes**
  National Security Council spokesperson
- **Mike Waltz**
  National Security Advisor
  (but still using the same phone)

The Guardian article from April 6, 2025

https://archive.is/CnT25

Chapter 2: Hey Siri

October 2024, before Trump was elected:

- **Jeffrey Goldberg**
  The Atlantic editor-in-chef
- **Brian Hughes**
  Trump campaign spokesperson
- **Mike Waltz**
  Trump campaign national security surrogate

After Trump was elected:

- **Jeffrey Goldberg**
  The Atlantic editor-in-chef
- **Brian Hughes**
  National Security Council spokesperson
- **Mike Waltz**
  National Security Advisor
  (but still using the same phone)

Waltz's war crimes Signal group:

- He tried to add Brian Hughes
- He actually added Jeffrey Goldberg

The Guardian article from April 6, 2025

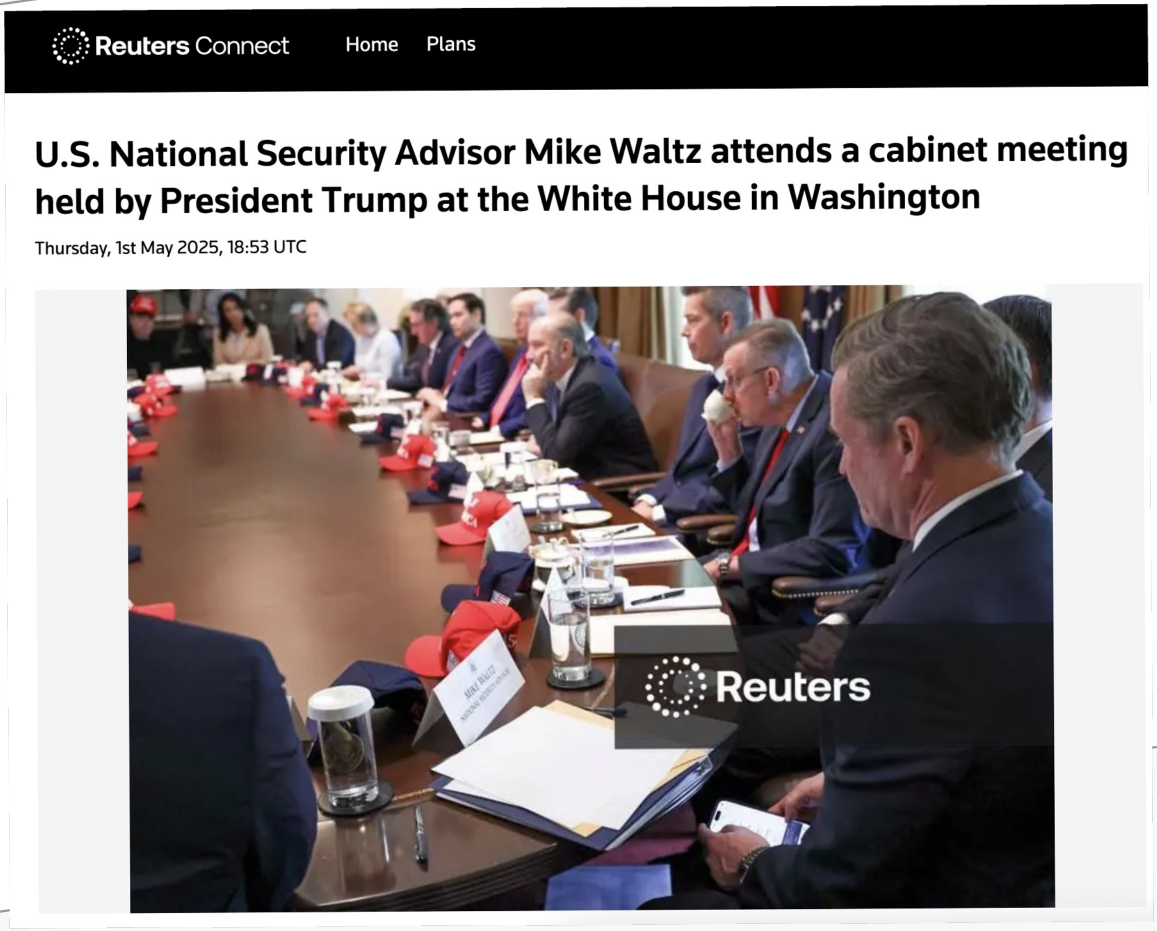
https://archive.is/CnT25

Chapter 2: Hey Siri

Teen Warned Not To Accept Group Chat Invites From National Security Advisors She Doesn’t Know

the ONION

Chapter 3: Mike Waltz is Bored

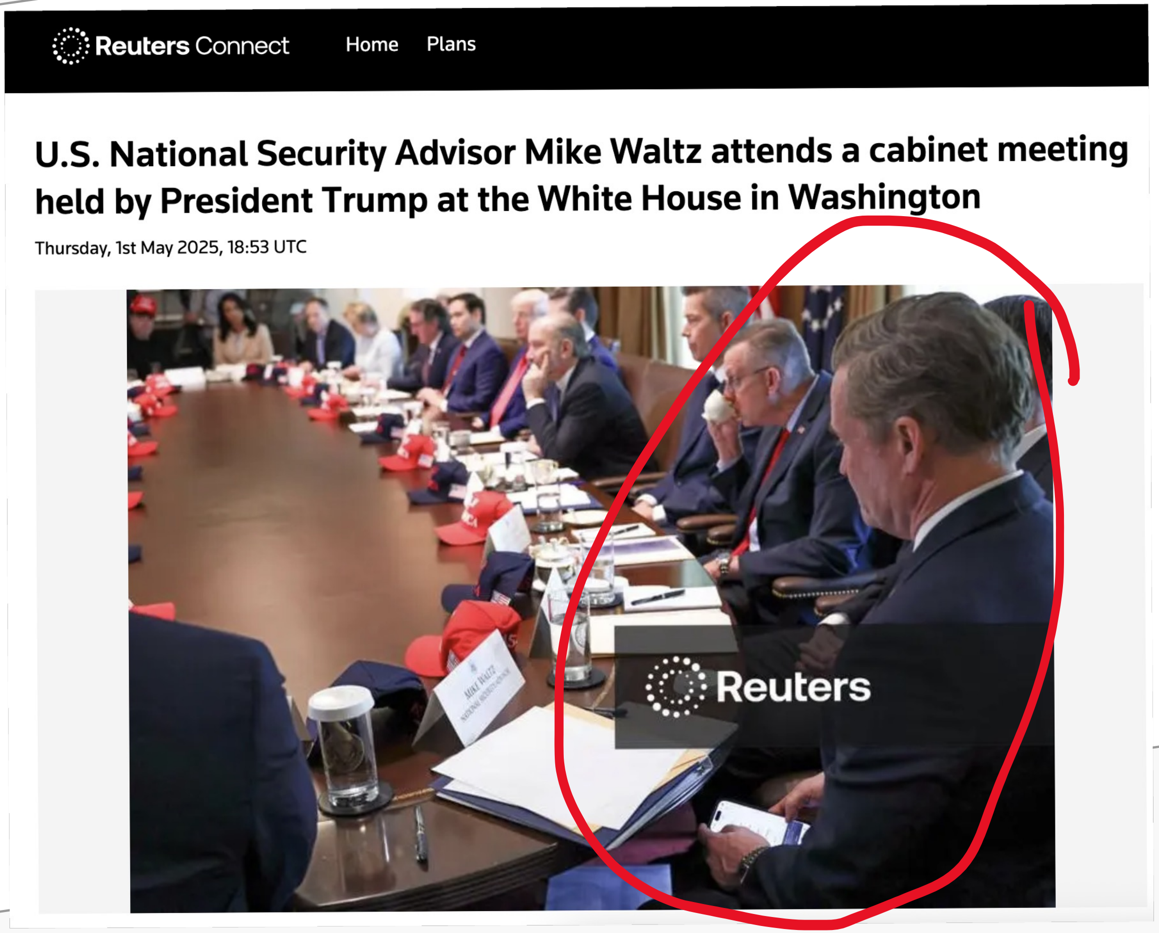


U.S. National Security Advisor Mike Waltz attends a cabinet meeting held by President Trump at the White House in Washington

Thursday, 1st May 2025, 18:53 UTC

May 1, 2025

Chapter 3:
Mike Waltz is Bored

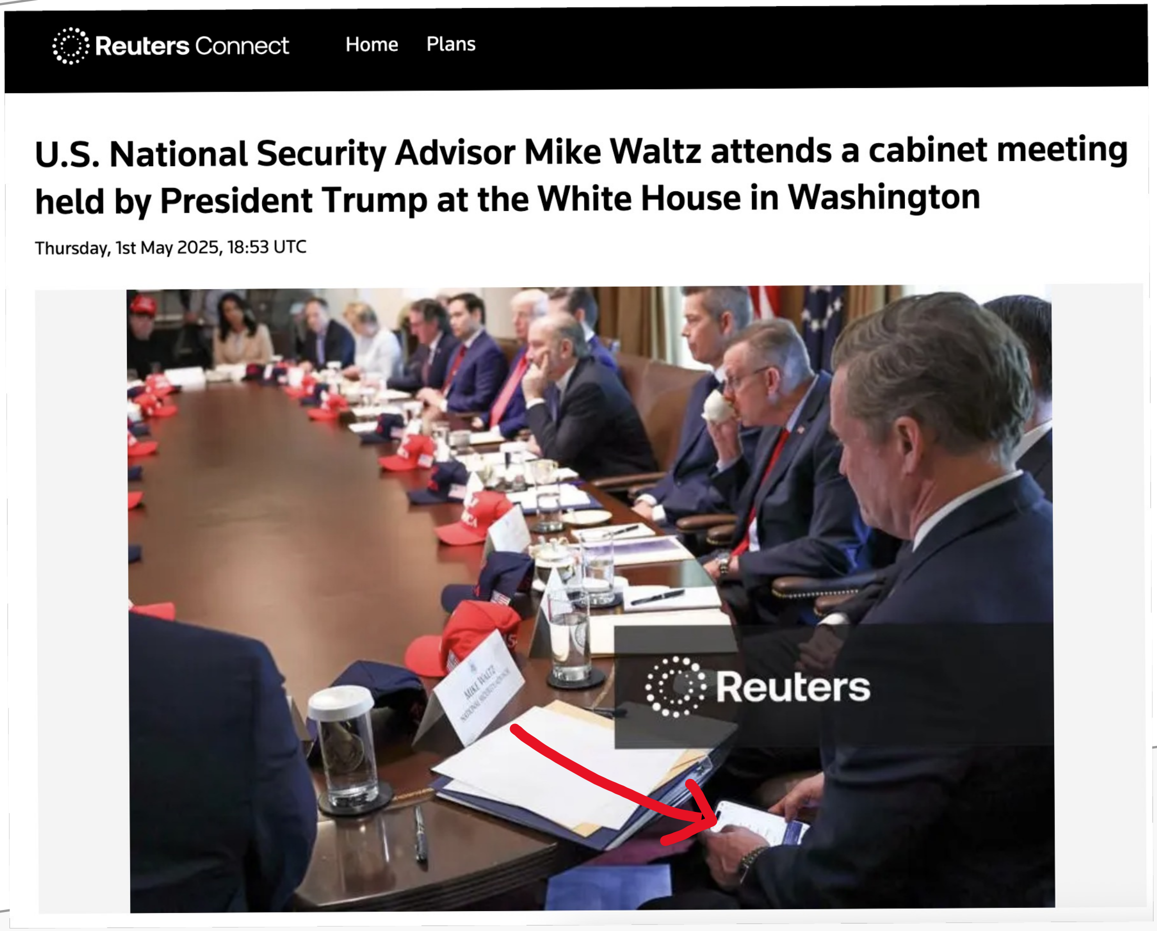


U.S. National Security Advisor Mike Waltz attends a cabinet meeting held by President Trump at the White House in Washington

Thursday, 1st May 2025, 18:53 UTC

May 1, 2025

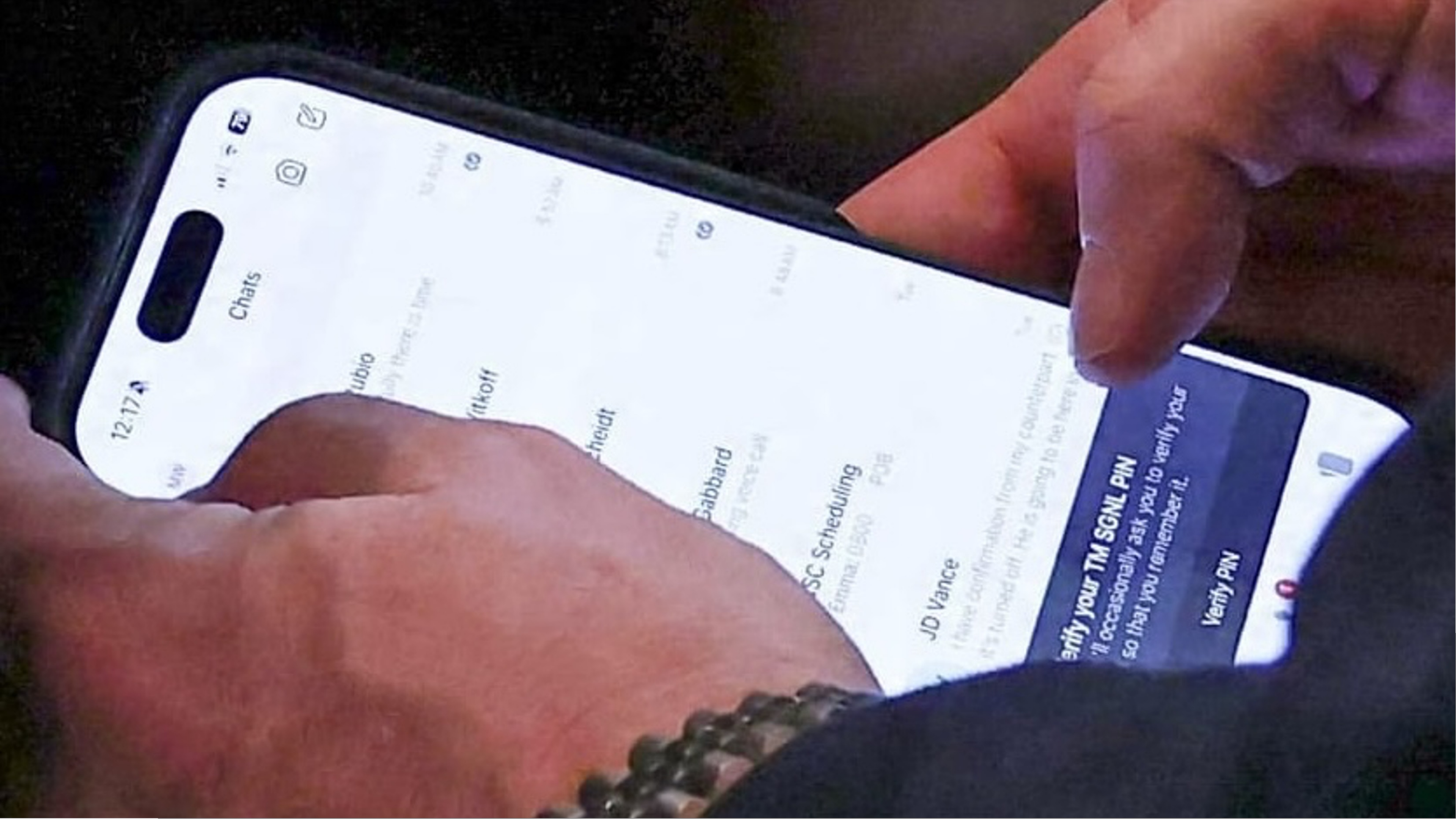
Chapter 3:
Mike Waltz is Bored



U.S. National Security Advisor Mike Waltz attends a cabinet meeting held by President Trump at the White House in Washington

Thursday, 1st May 2025, 18:53 UTC

May 1, 2025



12:17

Chats

ubio
ally there is time

itkoff

cheidt

Gabbard
ng voice cal

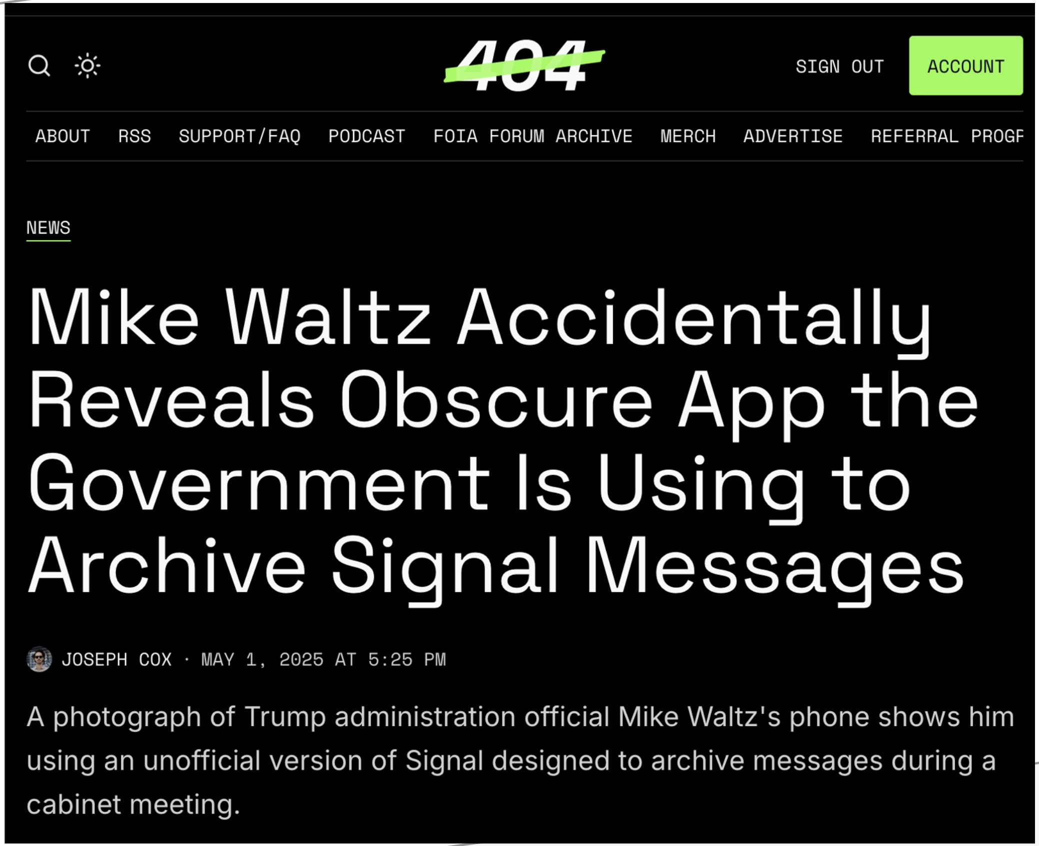
SC Scheduling
Emma: 0500 POB

JD Vance
I have confirmation from my counterpart
it's turned off. He is going to be here

erify your TM SGNL PIN
'll occasionally ask you to verify your
so that you remember it.

Verify PIN

Chapter 3:
Mike Waltz is Bored



NEWS

Mike Waltz Accidentally Reveals Obscure App the Government Is Using to Archive Signal Messages

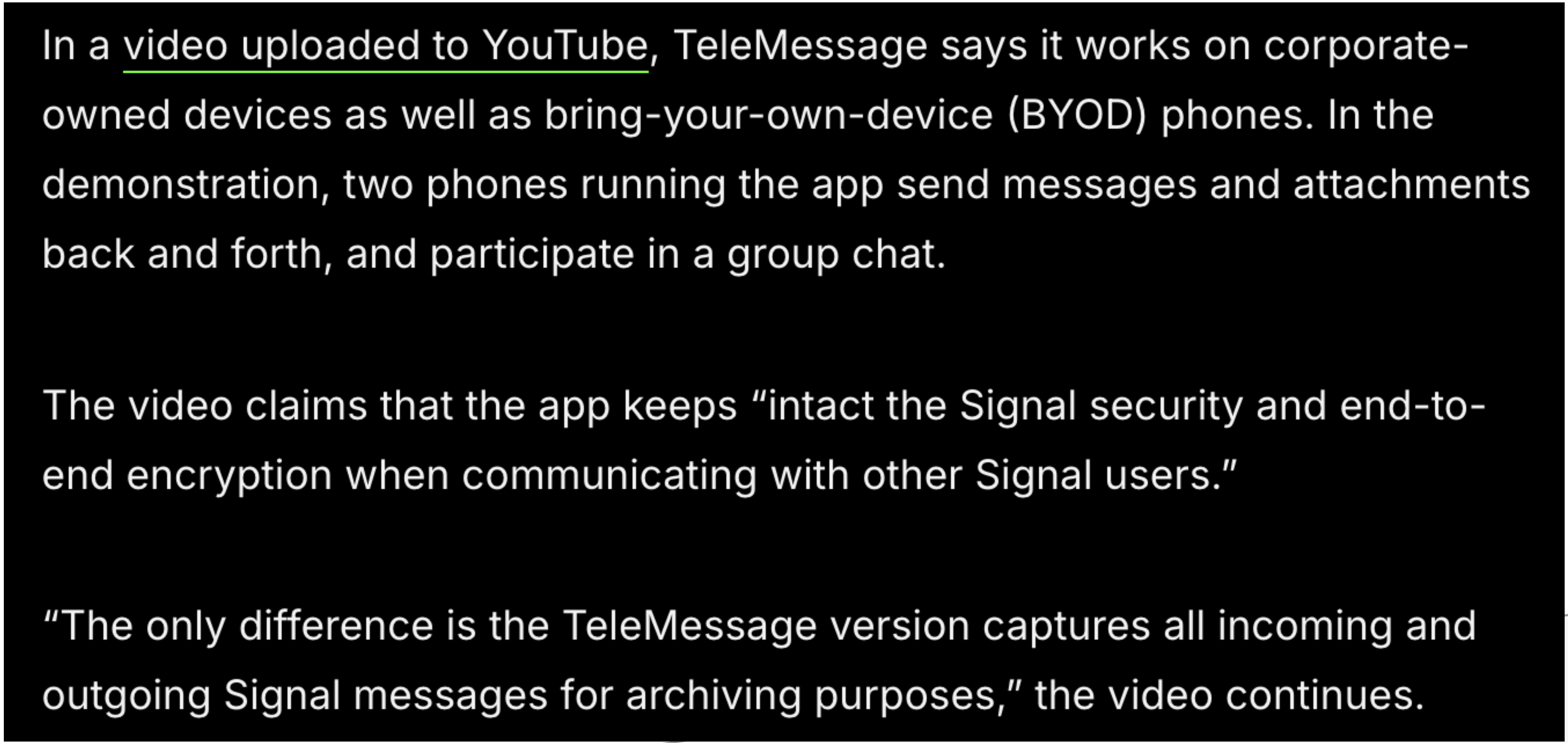
JOSEPH COX · MAY 1, 2025 AT 5:25 PM

A photograph of Trump administration official Mike Waltz's phone shows him using an unofficial version of Signal designed to archive messages during a cabinet meeting.

May 1, 2025

https://archive.ph/rpSNc

Chapter 3:
Mike Waltz is Bored



In a video uploaded to YouTube, TeleMessage says it works on corporate-owned devices as well as bring-your-own-device (BYOD) phones. In the demonstration, two phones running the app send messages and attachments back and forth, and participate in a group chat.

The video claims that the app keeps “intact the Signal security and end-to-end encryption when communicating with other Signal users.”

“The only difference is the TeleMessage version captures all incoming and outgoing Signal messages for archiving purposes,” the video continues.

May 1, 2025

https://archive.ph/rpSNc

Chapter 4: TM SGNL

TeleMessage

A Smarsh Company

Chapter 4: TM SGNL

Guy Levit, CEO

Guy has served as TeleMessage's CEO since July 2002 after co-founding TeleMessage in 1999. Prior to his current position he held various sales, marketing and operational positions within the company. **From 1996 until 1999, Guy served as the head of the planning and development of one of the IDF's Intelligence elite technical units.** In this role Mr. Levit was in charge of project management, budgets, and the design, development, implementation and maintenance of organizational, managerial and logistical information systems. Mr. Levit holds a B.Sc. in Industrial Engineering from the Technion, Israel's Institute of Technology and an MBA from Tel Aviv University.

from an archive of https://www.telemessage.com/team/

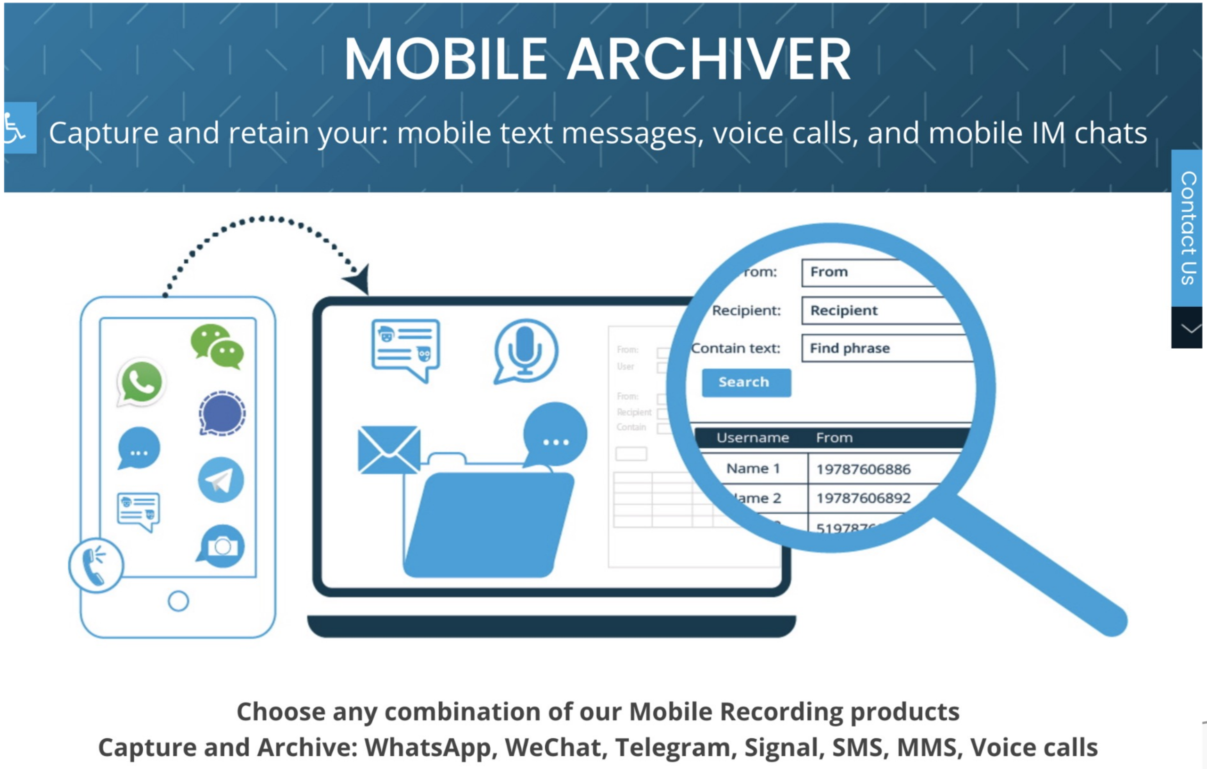
Chapter 4: TM SGNL

Gil Shapira, Vice President Business Development

Mr. Shapira is one of TeleMessage's co-founders. Between 1999 and 2005, he held various sales, marketing, operational positions in the company, as well as ran the company's European office. **Mr. Shapira served in the Israeli Air Force from 1993 – 1999 as a computer programmer, project manager and team leader of the IAF's special R&D software development unit.** Mr. Shapira holds a B.Sc. in Aerospace Engineering from the Technion, Israel's Institute of Technology and a M.Sc. in Industrial Engineering from Tel Aviv University.

from an archive of https://www.telemessage.com/team/

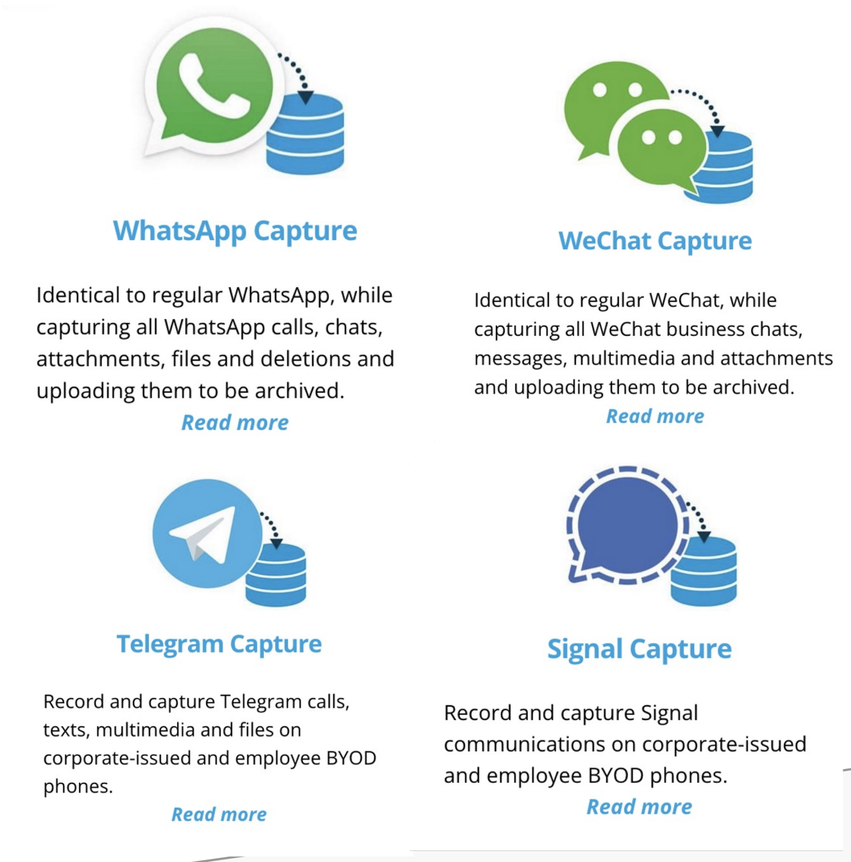
Chapter 4: TM SGNL



MOBILE ARCHIVER

Capture and retain your: mobile text messages, voice calls, and mobile IM chats

Choose any combination of our Mobile Recording products
Capture and Archive: WhatsApp, WeChat, Telegram, Signal, SMS, MMS, Voice calls



WhatsApp Capture

Identical to regular WhatsApp, while capturing all WhatsApp calls, chats, attachments, files and deletions and uploading them to be archived.

Read more

WeChat Capture

Identical to regular WeChat, while capturing all WeChat business chats, messages, multimedia and attachments and uploading them to be archived.

Read more

Telegram Capture

Record and capture Telegram calls, texts, multimedia and files on corporate-issued and employee BYOD phones.

Read more

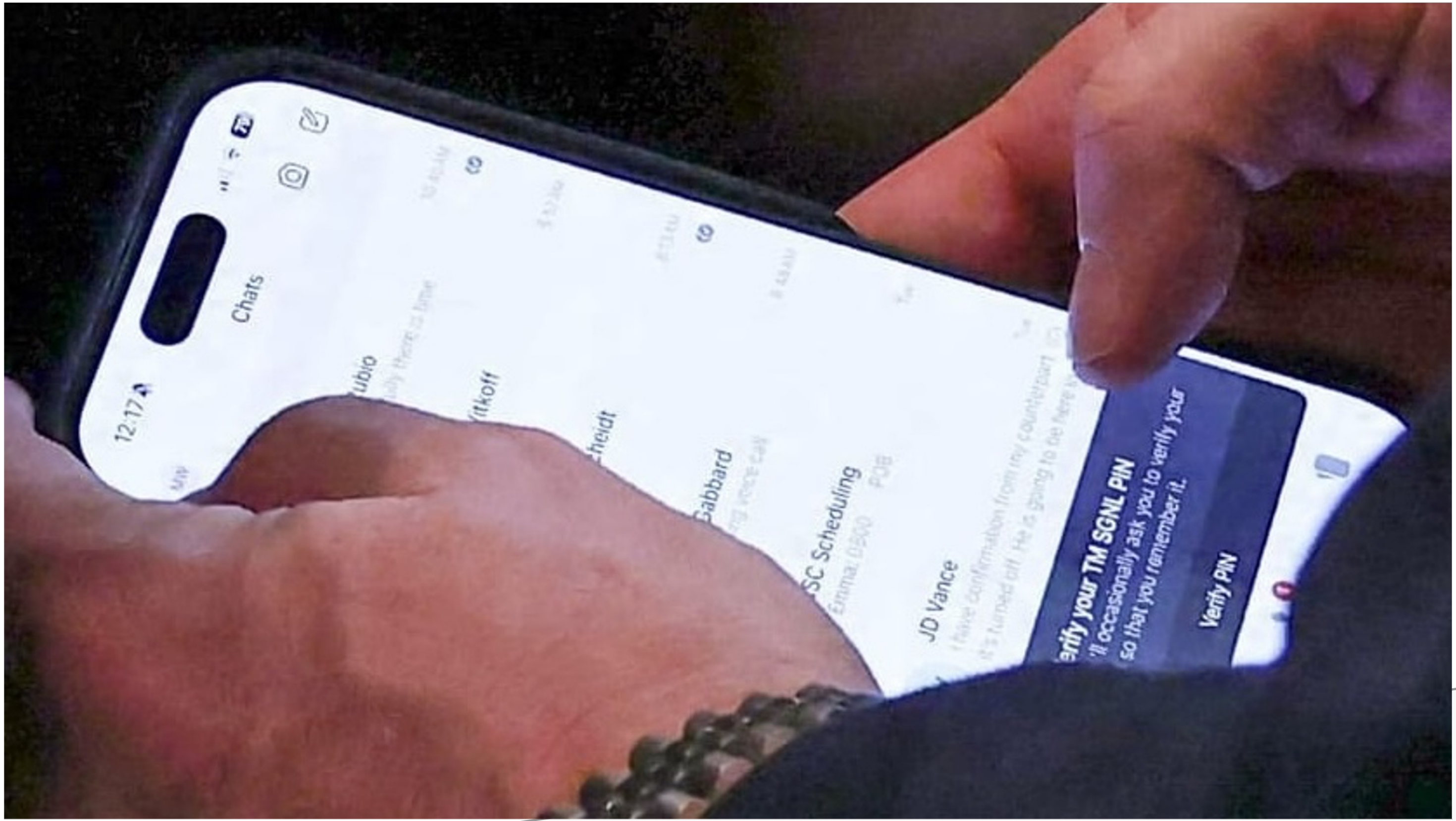
Signal Capture

Record and capture Signal communications on corporate-issued and employee BYOD phones.

Read more

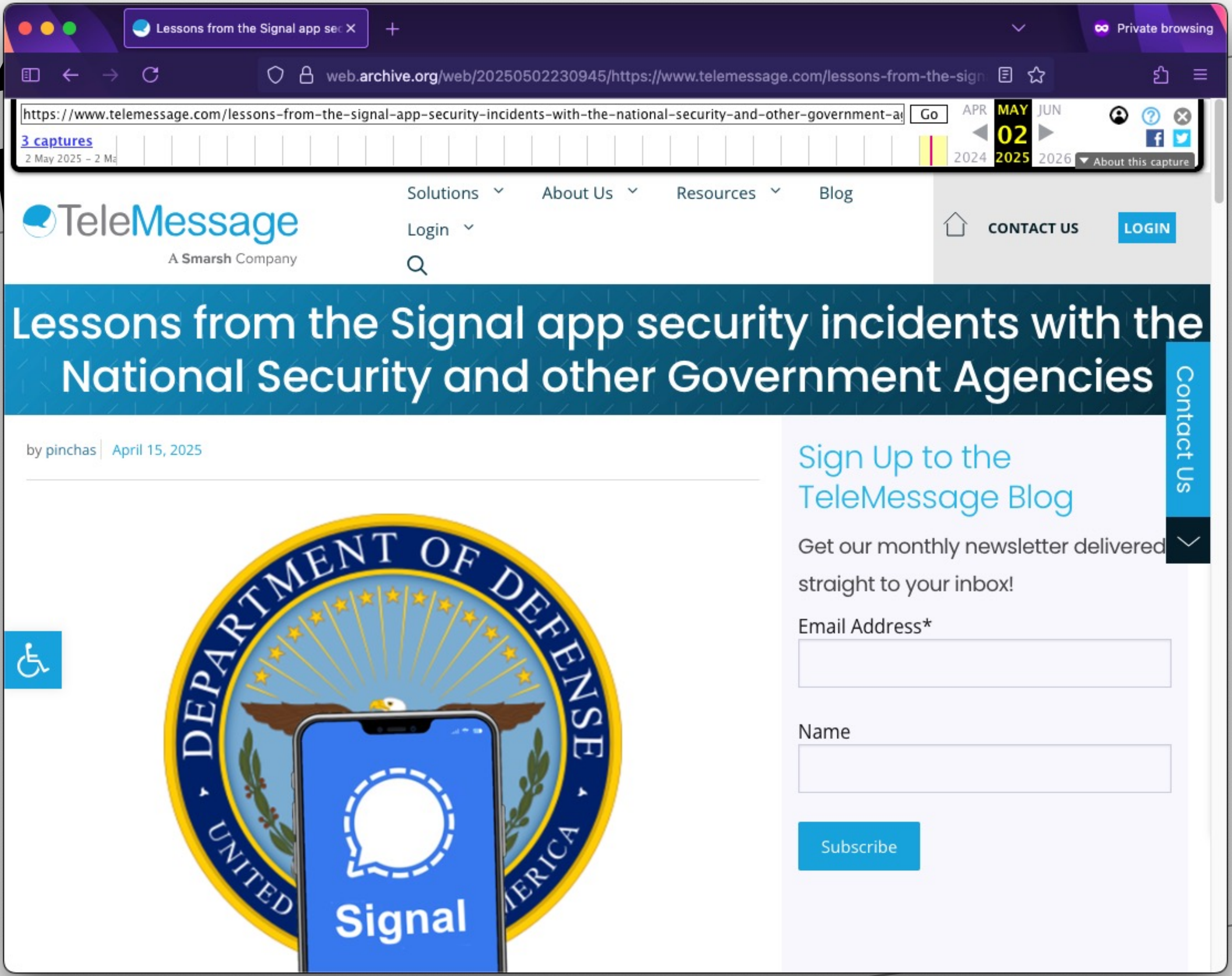
from an archive of https://www.telemessage.com/mobile-archiver/

Chapter 4: TM SGNL



May 1, 2025

Chapter
TM SGN



Lessons from the Signal app se

Private browsing

web.archive.org/web/20250502230945/https://www.telemessage.com/lessons-from-the-sign

https://www.telemessage.com/lessons-from-the-signal-app-security-incidents-with-the-national-security-and-other-government-a Go

3 captures

2 May 2025 - 2 Ma

APR MAY JUN

02

2024 2025 2026

About this capture

Solutions · About Us · Resources · Blog · Login

TeleMessage

A Smarsh Company

CONTACT US LOGIN

Lessons from the Signal app security incidents with the National Security and other Government Agencies

by pinchas | April 15, 2025

Sign Up to the TeleMessage Blog

Get our monthly newsletter delivered straight to your inbox!

Email Address*

Name

Subscribe

Contact Us

from an archive of https://www.telemessage.com/lessons-from-the-signal-app-security-incidents-with-the-national-security-and-other-government-agencies/

Chapter 4: TM SGNL

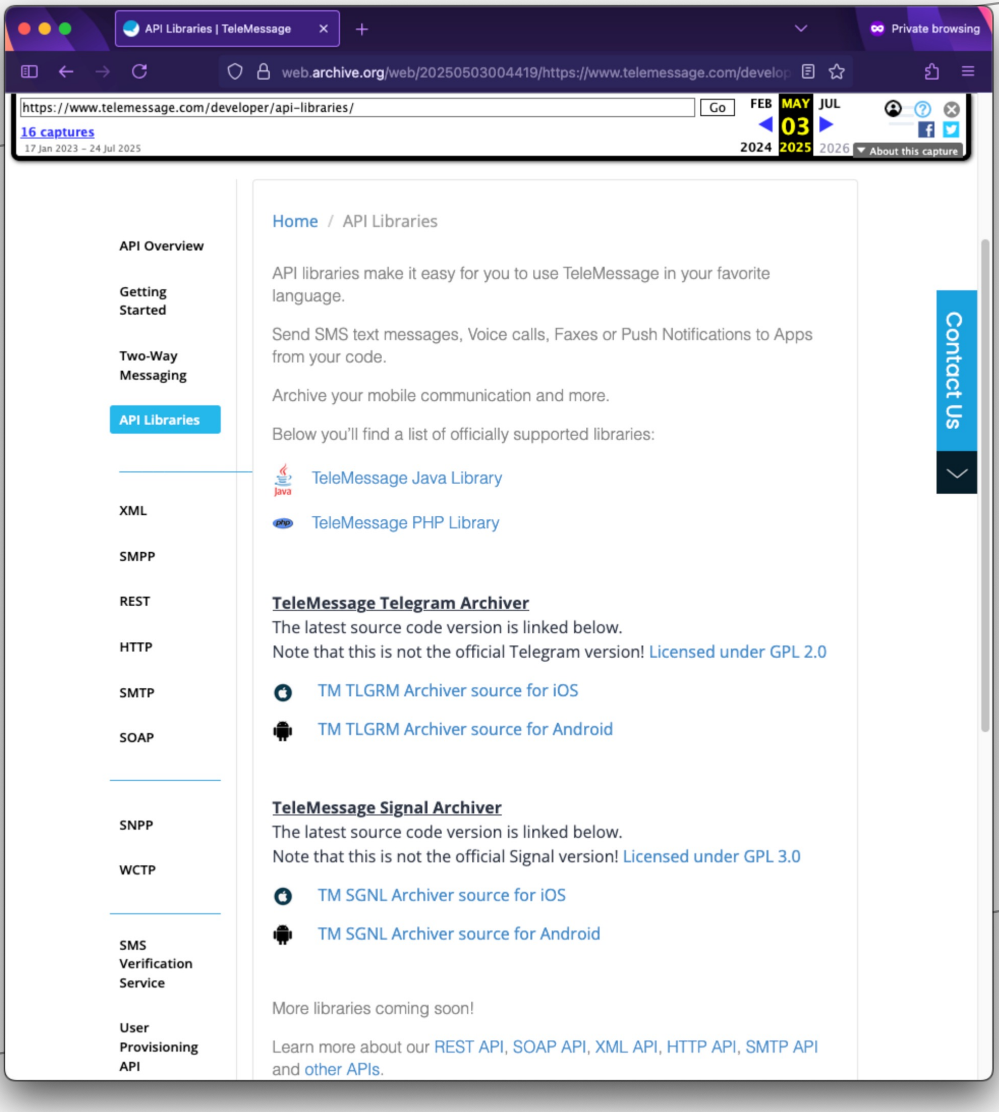
When did the Trump administration start using TeleMessage?

- March 13: Mike Waltz invites journalist to Signal group
- March 15: US bombs Yemen
- March 24: The Atlantic publishes first article
- **March 25: Senate hearing, and American Oversight lawsuit**
- March 26: House hearing, and the Atlantic publishes second article
- **April 15: TeleMessage blogs about Signalgate**
- May 1: Mike Waltz is photographed using TM SGNL

Chapter 4: TM SGNL

iOS source code link:
https://telemessage.com/wp-content/uploads/2024/12/Signal-iOS-main.zip

Android source code link:
https://www.telemessage.com/wp-content/uploads/2024/12/Signal.zip



Home / API Libraries

API libraries make it easy for you to use TeleMessage in your favorite language.

Send SMS text messages, Voice calls, Faxes or Push Notifications to Apps from your code.

Archive your mobile communication and more.

Below you'll find a list of officially supported libraries:

- TeleMessage Java Library
- TeleMessage PHP Library

TeleMessage Telegram Archiver
The latest source code version is linked below.
Note that this is not the official Telegram version! Licensed under GPL 2.0

- TM TLGRM Archiver source for iOS
- TM TLGRM Archiver source for Android

TeleMessage Signal Archiver
The latest source code version is linked below.
Note that this is not the official Signal version! Licensed under GPL 3.0

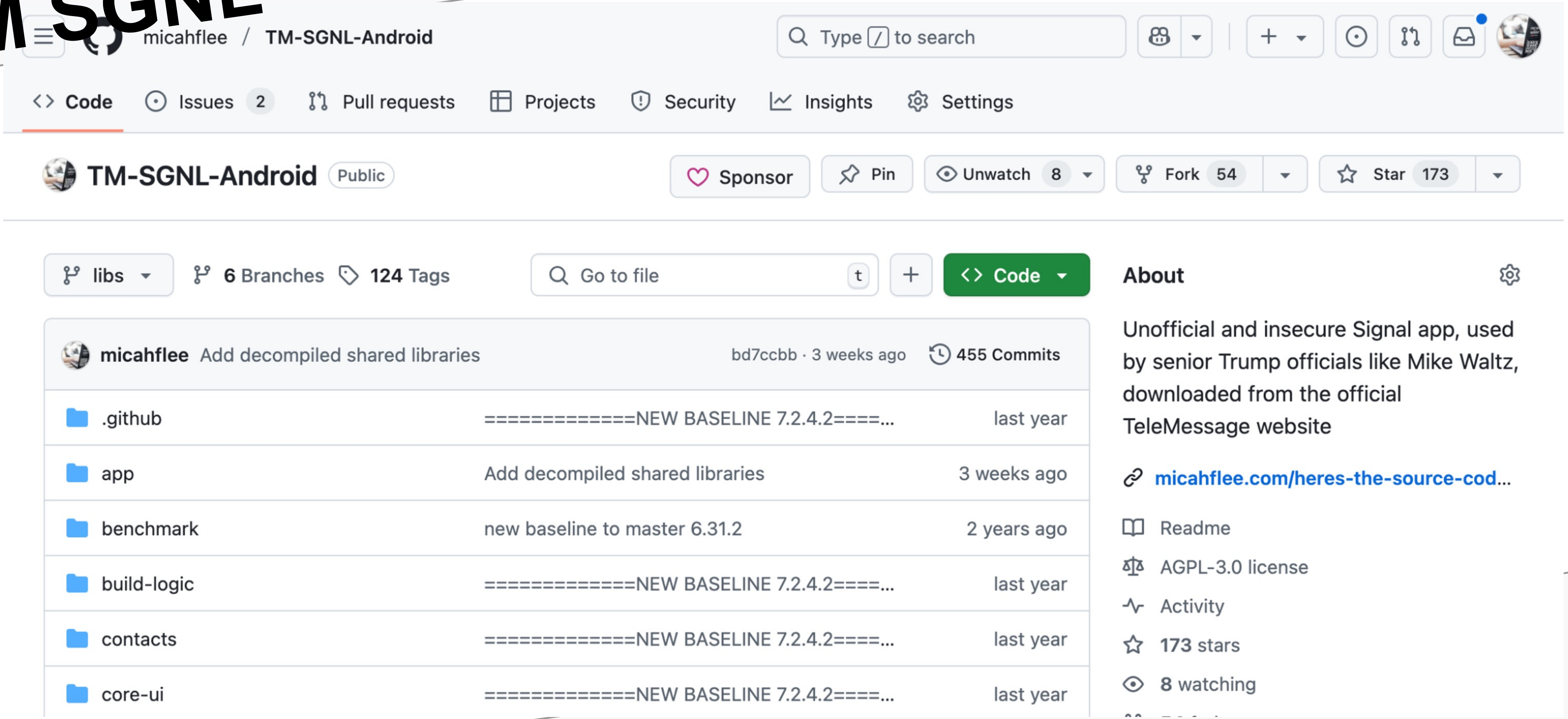
- TM SGNL Archiver source for iOS
- TM SGNL Archiver source for Android

More libraries coming soon!

Learn more about our REST API, SOAP API, XML API, HTTP API, SMTP API and other APIs.

from an archive of https://www.telemessage.com/developer/api-libraries/

Chapter 4: TM SGNL



TM-SGNL-Android Public

micahflee Add decompiled shared libraries	bd7ccbb · 3 weeks ago	455 Commits
.github	============NEW BASELINE 7.2.4.2====...	last year
app	Add decompiled shared libraries	3 weeks ago
benchmark	new baseline to master 6.31.2	2 years ago
build-logic	============NEW BASELINE 7.2.4.2====...	last year
contacts	============NEW BASELINE 7.2.4.2====...	last year
core-ui	============NEW BASELINE 7.2.4.2====...	last year

About

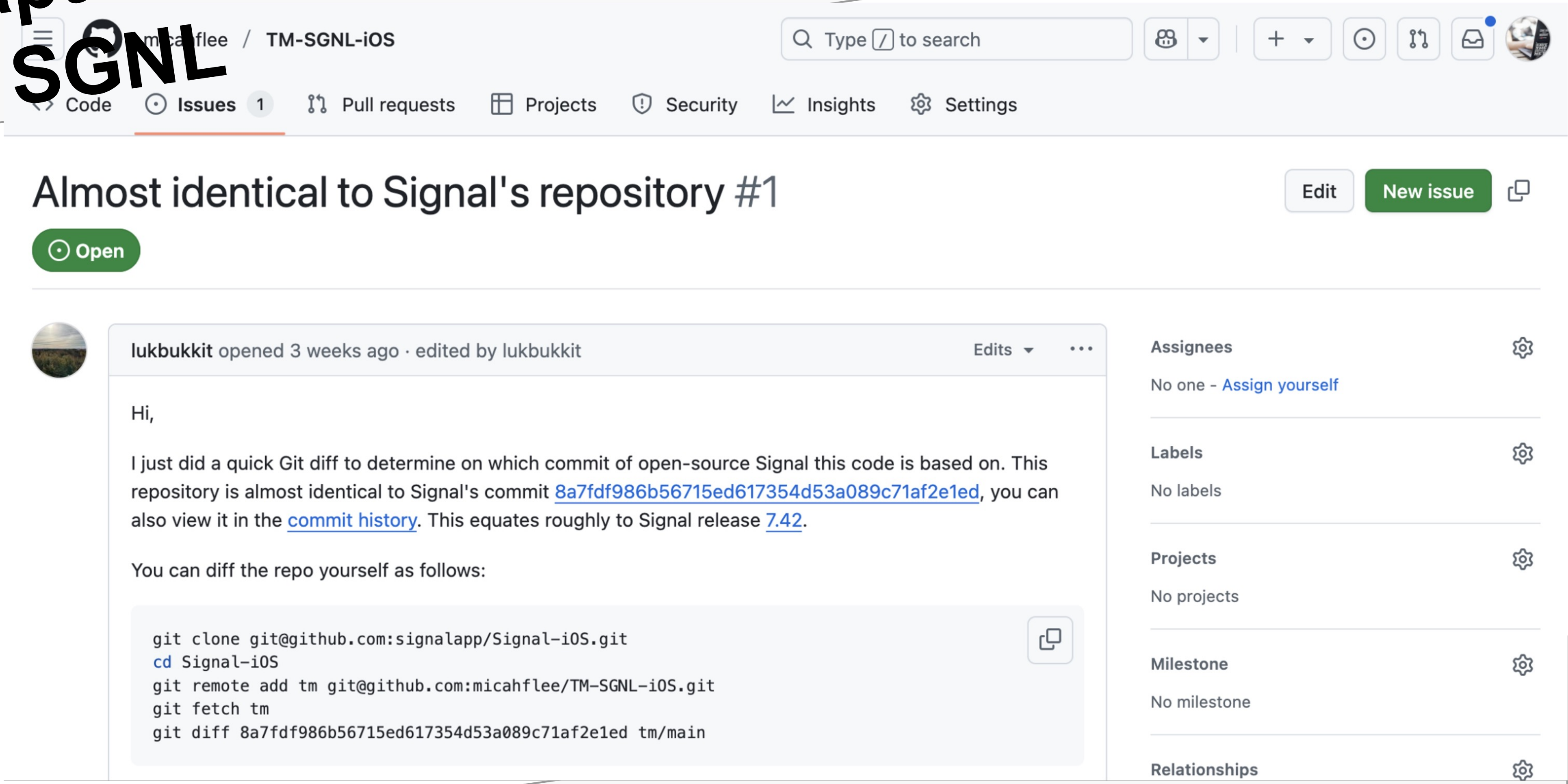
Unofficial and insecure Signal app, used by senior Trump officials like Mike Waltz, downloaded from the official TeleMessage website

micahflee.com/heres-the-source-cod...

- Readme
- AGPL-3.0 license
- Activity
- 173 stars
- 8 watching

https://github.com/micahflee/TM-SGNL-Android

Chapter 4: TM SGNL



Almost identical to Signal's repository #1

lukbukkit opened 3 weeks ago · edited by lukbukkit

Hi,

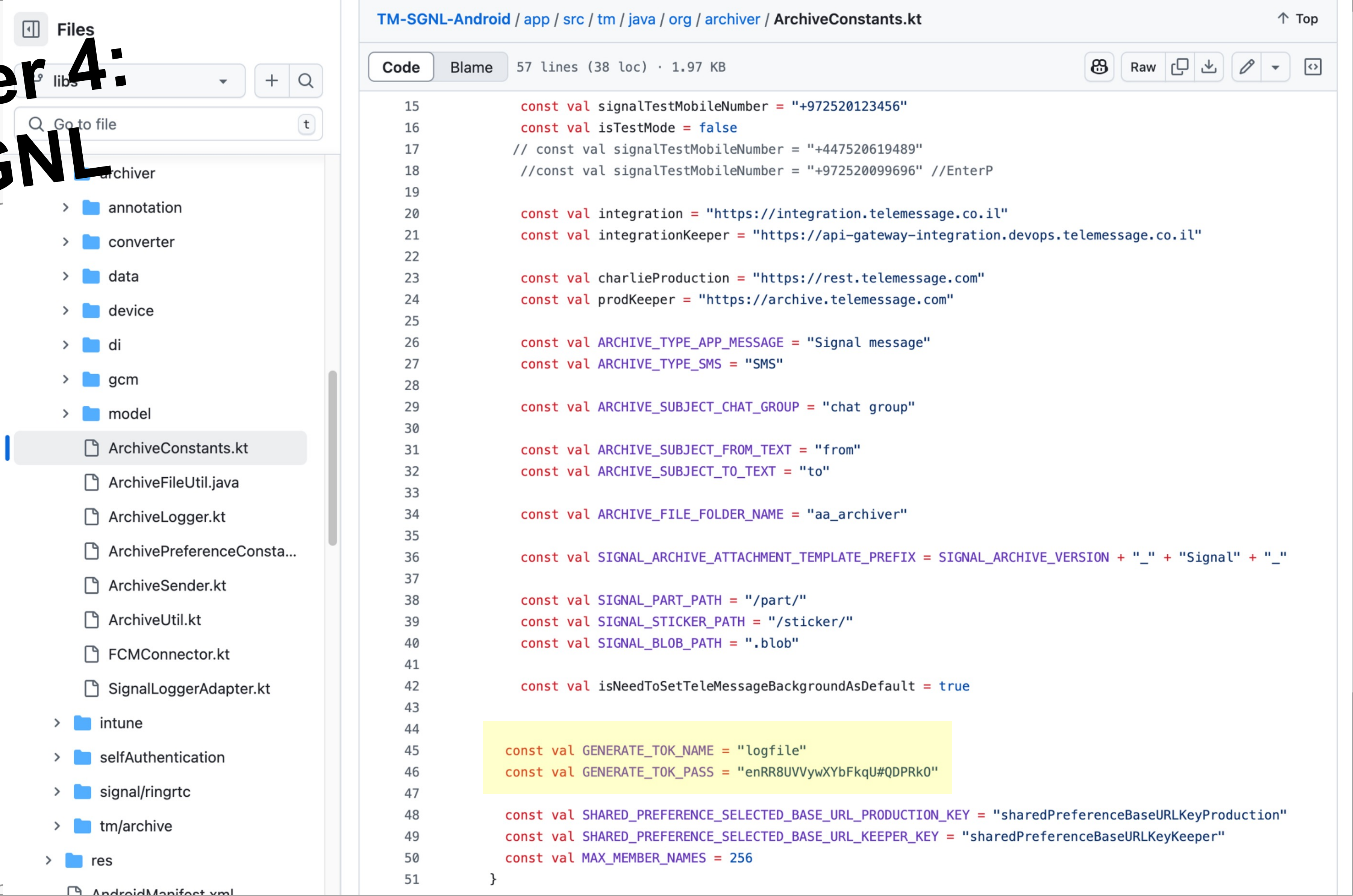
I just did a quick Git diff to determine on which commit of open-source Signal this code is based on. This repository is almost identical to Signal's commit 8a7fdf986b56715ed617354d53a089c71af2e1ed, you can also view it in the commit history. This equates roughly to Signal release 7.42.

You can diff the repo yourself as follows:

```
git clone git@github.com:signalapp/Signal-iOS.git
cd Signal-iOS
git remote add tm git@github.com:micahflee/TM-SGNL-iOS.git
git fetch tm
git diff 8a7fdf986b56715ed617354d53a089c71af2e1ed tm/main
```

https://github.com/micahflee/TM-SGNL-iOS/issues/1

Chapter 4: TM SGNL

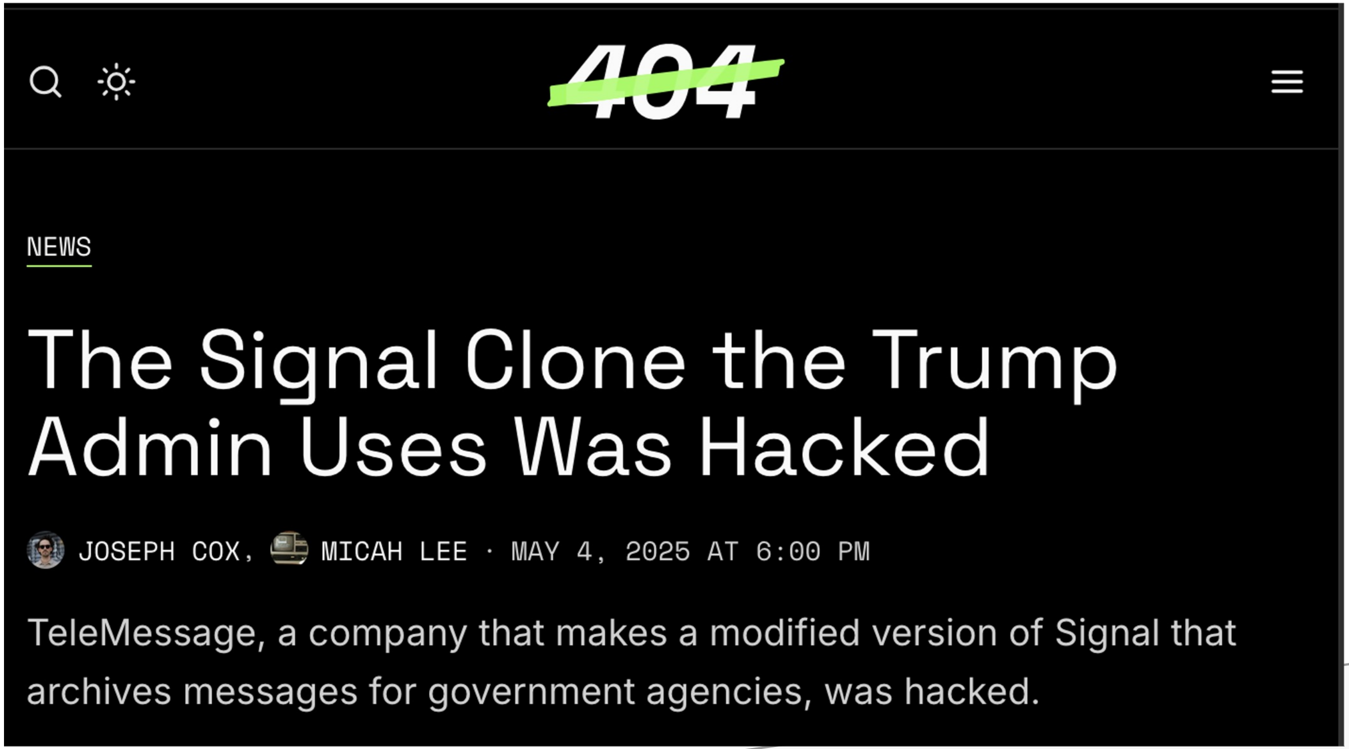


TM-SGNL-Android / app / src / tm / java / org / archiver / ArchiveConstants.kt

57 lines (38 loc) · 1.97 KB

```
      const val signalTestMobileNumber = "+972520123456"
      const val isTestMode = false
     // const val signalTestMobileNumber = "+447520619489"
      //const val signalTestMobileNumber = "+972520099696" //EnterP

      const val integration = "https://integration.telemessage.co.il"
      const val integrationKeeper = "https://api-gateway-integration.devops.telemessage.co.il"

      const val charlieProduction = "https://rest.telemessage.com"
      const val prodKeeper = "https://archive.telemessage.com"

      const val ARCHIVE_TYPE_APP_MESSAGE = "Signal message"
      const val ARCHIVE_TYPE_SMS = "SMS"

      const val ARCHIVE_SUBJECT_CHAT_GROUP = "chat group"

      const val ARCHIVE_SUBJECT_FROM_TEXT = "from"
      const val ARCHIVE_SUBJECT_TO_TEXT = "to"

      const val ARCHIVE_FILE_FOLDER_NAME = "aa_archiver"

      const val SIGNAL_ARCHIVE_ATTACHMENT_TEMPLATE_PREFIX = SIGNAL_ARCHIVE_VERSION + "_" + "Signal" + "_"

      const val SIGNAL_PART_PATH = "/part/"
      const val SIGNAL_STICKER_PATH = "/sticker/"
      const val SIGNAL_BLOB_PATH = ".blob"

      const val isNeedToSetTeleMessageBackgroundAsDefault = true


     const val GENERATE_TOK_NAME = "logfile"
     const val GENERATE_TOK_PASS = "enRR8UVVywXYbFkqU#QDPRkO"

     const val SHARED_PREFERENCE_SELECTED_BASE_URL_PRODUCTION_KEY = "sharedPreferenceBaseURLKeyProduction"
     const val SHARED_PREFERENCE_SELECTED_BASE_URL_KEEPER_KEY = "sharedPreferenceBaseURLKeeper"
     const val MAX_MEMBER_NAMES = 256
    }
```

Chapter 5:
Hacked in 15-20 Minutes



NEWS

The Signal Clone the Trump Admin Uses Was Hacked

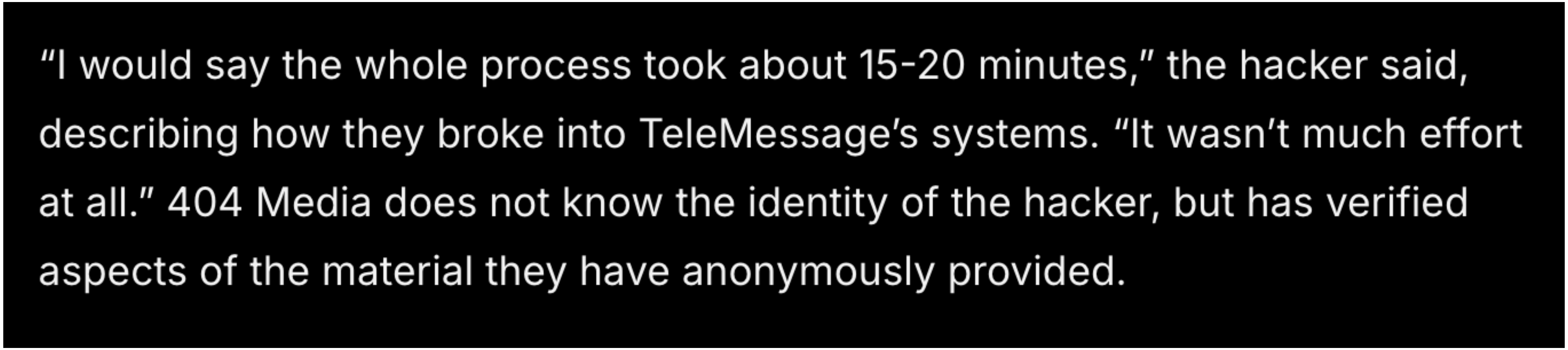
JOSEPH COX, MICAH LEE · MAY 4, 2025 AT 6:00 PM

TeleMessage, a company that makes a modified version of Signal that archives messages for government agencies, was hacked.

May 4, 2025

https://archive.ph/yyyLg

Chapter 5: Hacked in 15-20 Minutes

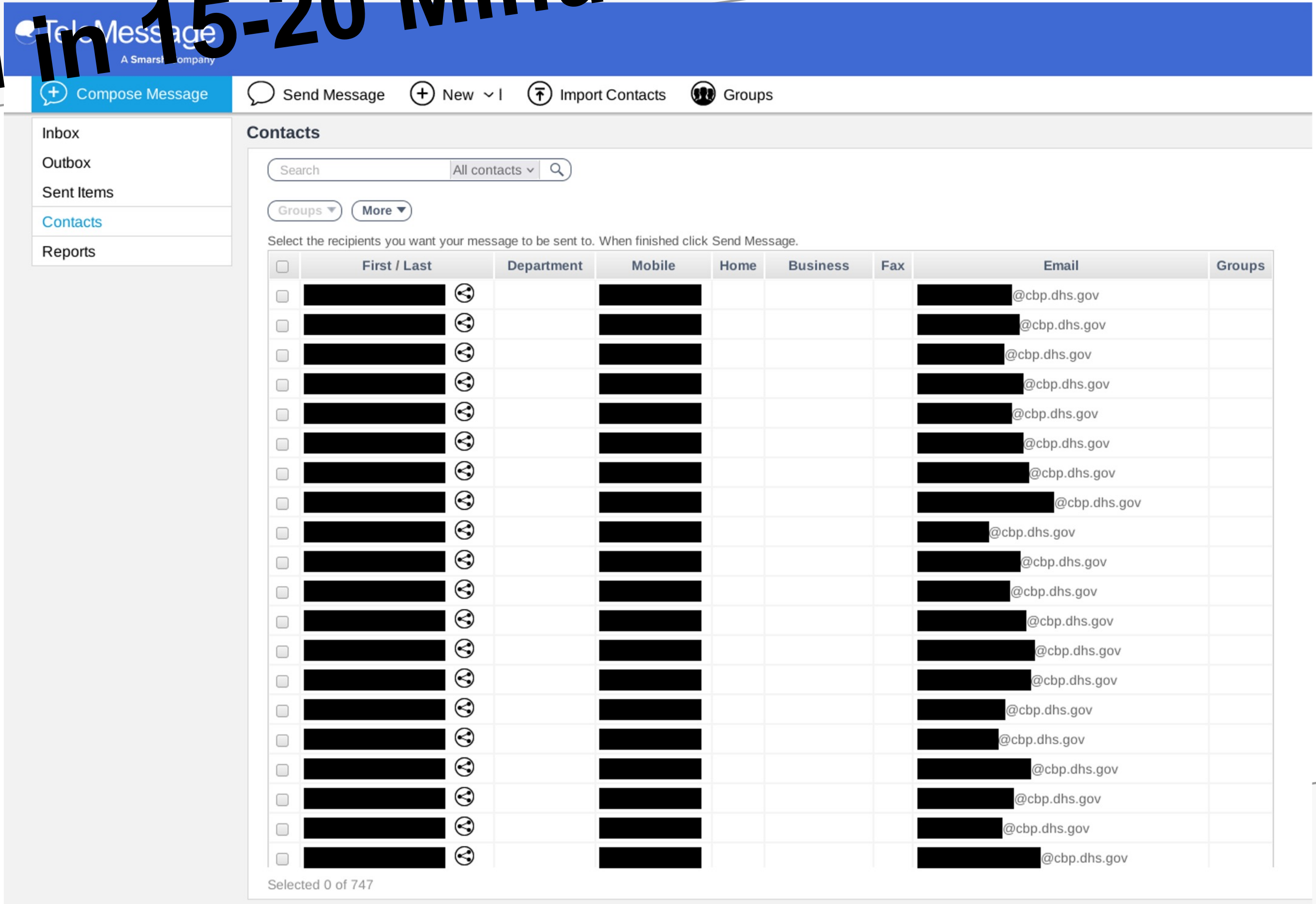


"I would say the whole process took about 15-20 minutes," the hacker said, describing how they broke into TeleMessage's systems. "It wasn't much effort at all." 404 Media does not know the identity of the hacker, but has verified aspects of the material they have anonymously provided.

May 4, 2025

https://archive.ph/yyyLg

Chapter 5: Hacked in 15-20 Minutes



Contacts

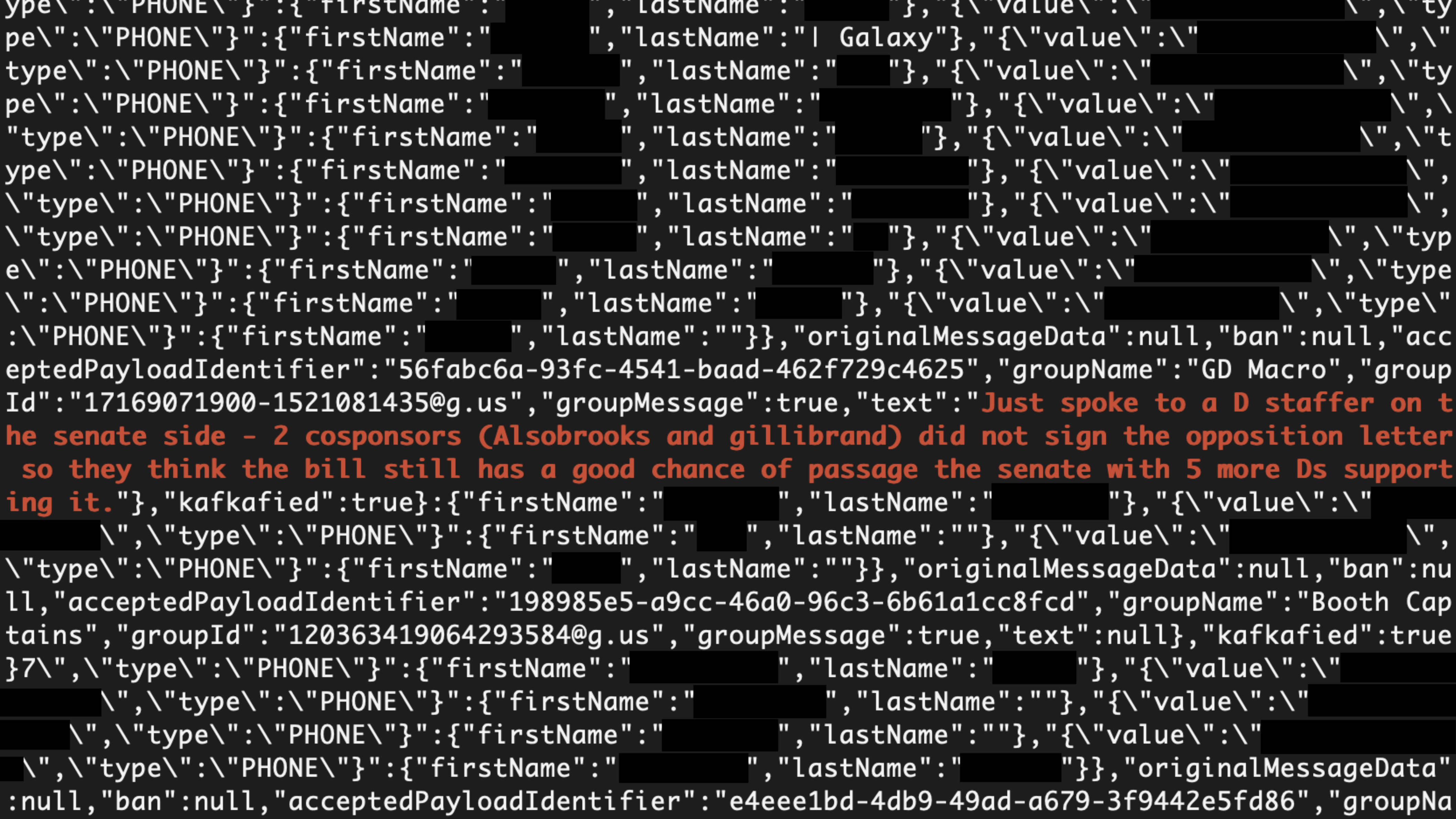
Select the recipients you want your message to be sent to. When finished click Send Message.

□	First / Last	Department	Mobile	Home	Business	Fax	Email	Groups
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	
□	[redacted]		[redacted]				[redacted]@cbp.dhs.gov	

Selected 0 of 747

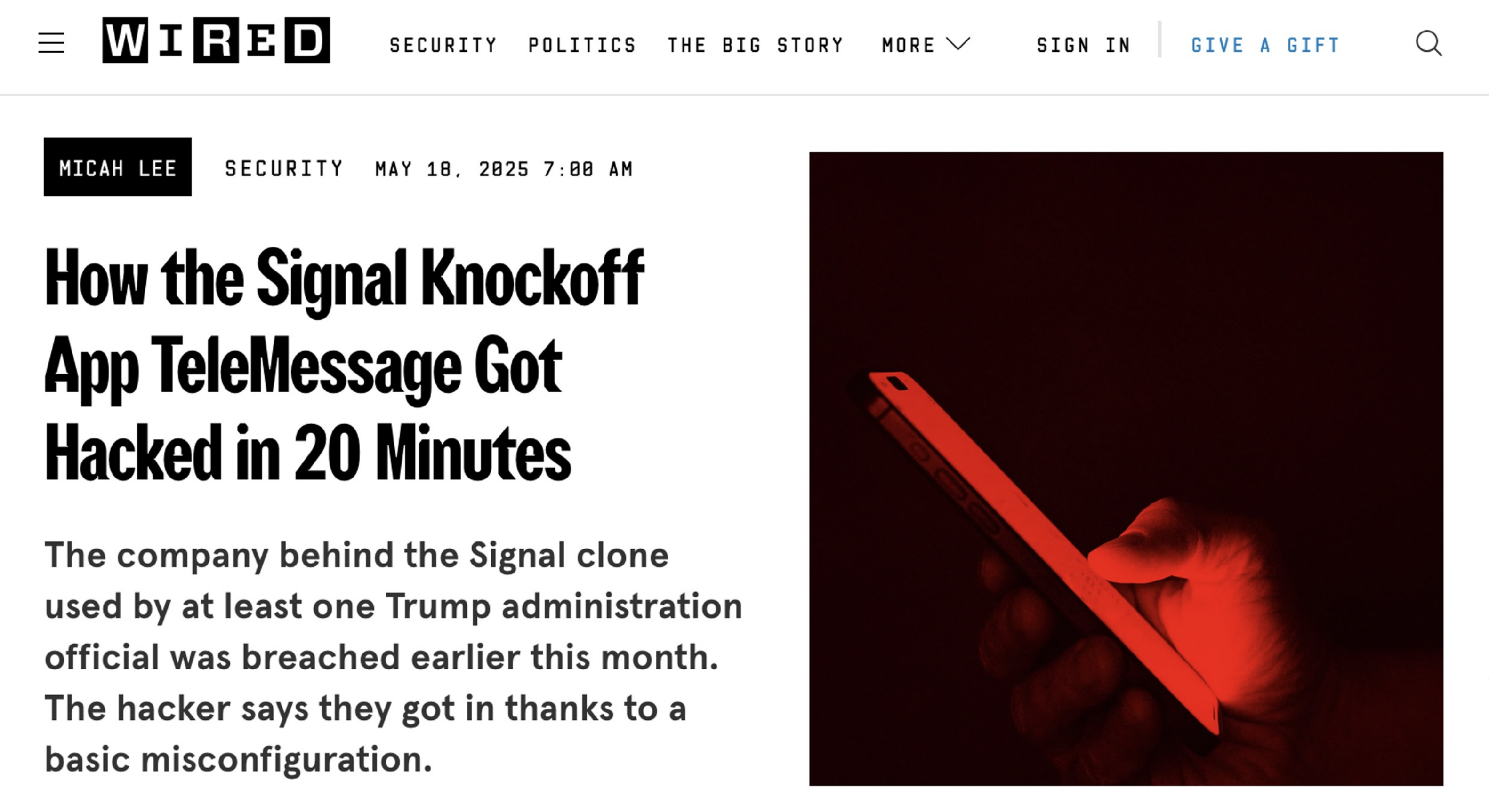
May 4, 2025

https://archive.ph/yyyLg



```
ype\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"[redacted]"},"{\"value\":\"[redacted]\",\"ty
pe\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"| Galaxy"},"{\"value\":\"[redacted]\",\"
type\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"[redacted]"},"{\"value\":\"[redacted]\",\"ty
pe\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"[redacted]"},"{\"value\":\"[redacted]\",\
"type\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"[redacted]"},"{\"value\":\"[redacted]\",\"t
ype\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"[redacted]"},"{\"value\":\"[redacted]\",
\"type\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"[redacted]"},"{\"value\":\"[redacted]\",
\"type\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"[redacted]"},"{\"value\":\"[redacted]\",\"typ
e\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"[redacted]"},"{\"value\":\"[redacted]\",\"type
\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"[redacted]"},"{\"value\":\"[redacted]\",\"type\"
:\"PHONE\"}":{"firstName":"[redacted]","lastName":""}},"originalMessageData":null,"ban":null,"acc
eptedPayloadIdentifier":"56fabc6a-93fc-4541-baad-462f729c4625","groupName":"GD Macro","group
Id":"17169071900-1521081435@g.us","groupMessage":true,"text":"Just spoke to a D staffer on t
he senate side - 2 cosponsors (Alsobrooks and gillibrand) did not sign the opposition letter
 so they think the bill still has a good chance of passage the senate with 5 more Ds support
ing it."},"kafkafied":true}:{"firstName":"[redacted]","lastName":"[redacted]"},"{\"value\":\"[redacted]
[redacted]\",\"type\":\"PHONE\"}":{"firstName":"[redacted]","lastName":""},"{\"value\":\"[redacted]\",
\"type\":\"PHONE\"}":{"firstName":"[redacted]","lastName":""}},"originalMessageData":null,"ban":nu
ll,"acceptedPayloadIdentifier":"198985e5-a9cc-46a0-96c3-6b61a1cc8fcd","groupName":"Booth Cap
tains","groupId":"120363419064293584@g.us","groupMessage":true,"text":null},"kafkafied":true
}7\",\"type\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"[redacted]"},"{\"value\":\"[redacted]
[redacted]\",\"type\":\"PHONE\"}":{"firstName":"[redacted]","lastName":""},"{\"value\":\"[redacted]
[redacted]\",\"type\":\"PHONE\"}":{"firstName":"[redacted]","lastName":""},"{\"value\":\"[redacted]
[redacted]\",\"type\":\"PHONE\"}":{"firstName":"[redacted]","lastName":"[redacted]"}},"originalMessageData"
:null,"ban":null,"acceptedPayloadIdentifier":"e4eee1bd-4db9-49ad-a679-3f9442e5fd86","groupNa
```

Chapter 5: Hacked in 15-20 Minutes



MICAH LEE SECURITY MAY 18, 2025 7:00 AM

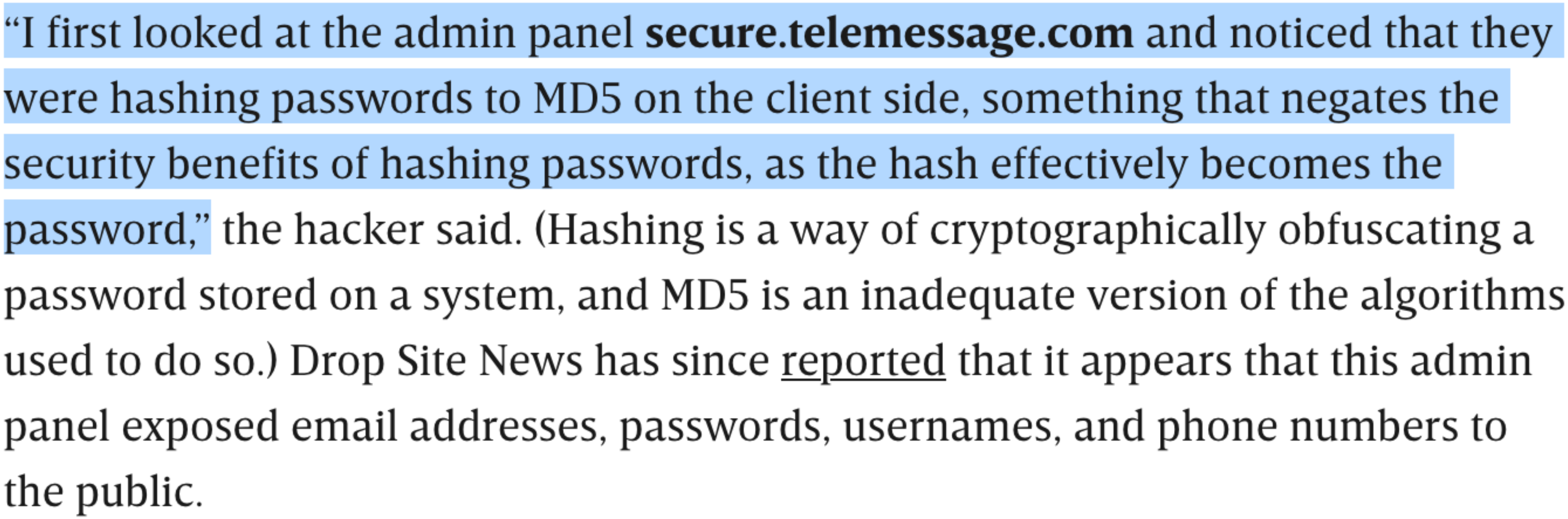
How the Signal Knockoff App TeleMessage Got Hacked in 20 Minutes

The company behind the Signal clone used by at least one Trump administration official was breached earlier this month. The hacker says they got in thanks to a basic misconfiguration.

May 18, 2025

https://archive.ph/5WcRT

Chapter 5:
Hacked in 15-20 Minutes

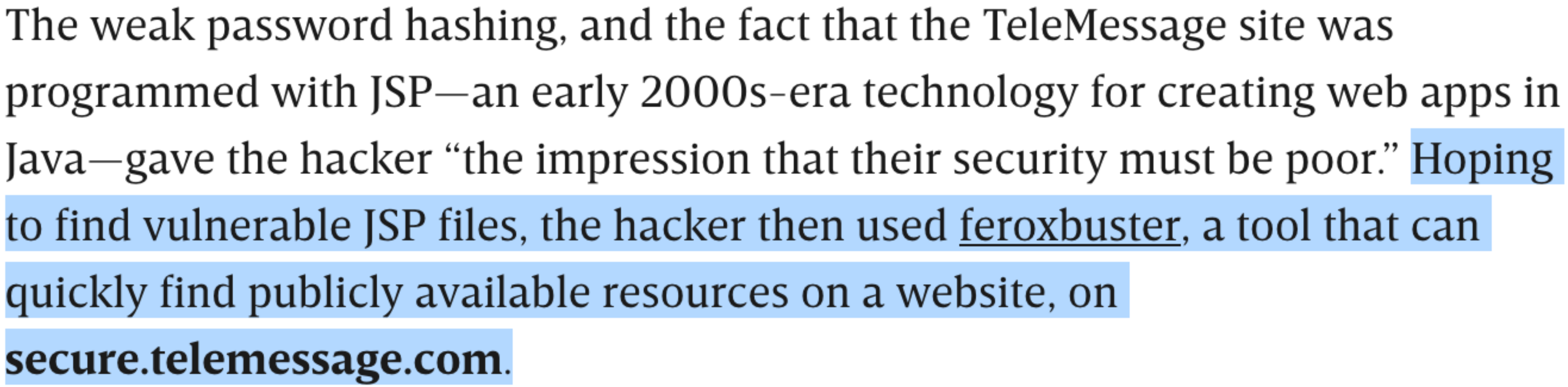


“I first looked at the admin panel **secure.telemessage.com** and noticed that they were hashing passwords to MD5 on the client side, something that negates the security benefits of hashing passwords, as the hash effectively becomes the password,” the hacker said. (Hashing is a way of cryptographically obfuscating a password stored on a system, and MD5 is an inadequate version of the algorithms used to do so.) Drop Site News has since reported that it appears that this admin panel exposed email addresses, passwords, usernames, and phone numbers to the public.

May 18, 2025

https://archive.ph/5WcRT

Chapter 5:
Hacked in 15-20 Minutes

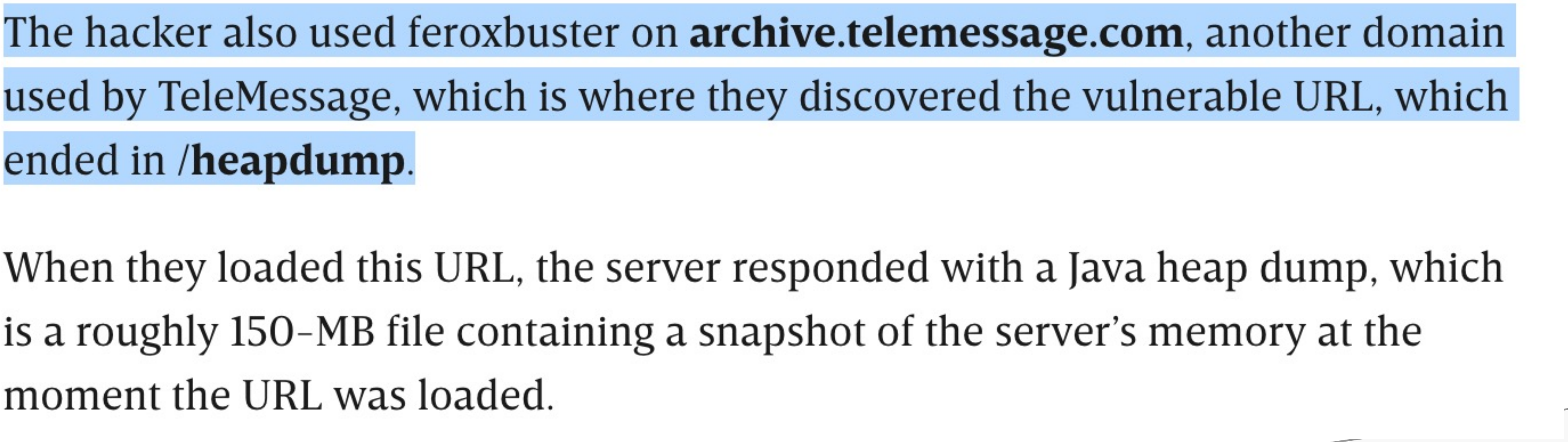


The weak password hashing, and the fact that the TeleMessage site was programmed with JSP—an early 2000s-era technology for creating web apps in Java—gave the hacker “the impression that their security must be poor.” Hoping to find vulnerable JSP files, the hacker then used feroxbuster, a tool that can quickly find publicly available resources on a website, on **secure.telemessage.com**.

May 18, 2025

https://archive.ph/5WcRT

Chapter 5: Hacked in 15-20 Minutes



The hacker also used feroxbuster on **archive.telemessage.com**, another domain used by TeleMessage, which is where they discovered the vulnerable URL, which ended in /**heapdump**.

When they loaded this URL, the server responded with a Java heap dump, which is a roughly 150-MB file containing a snapshot of the server's memory at the moment the URL was loaded.

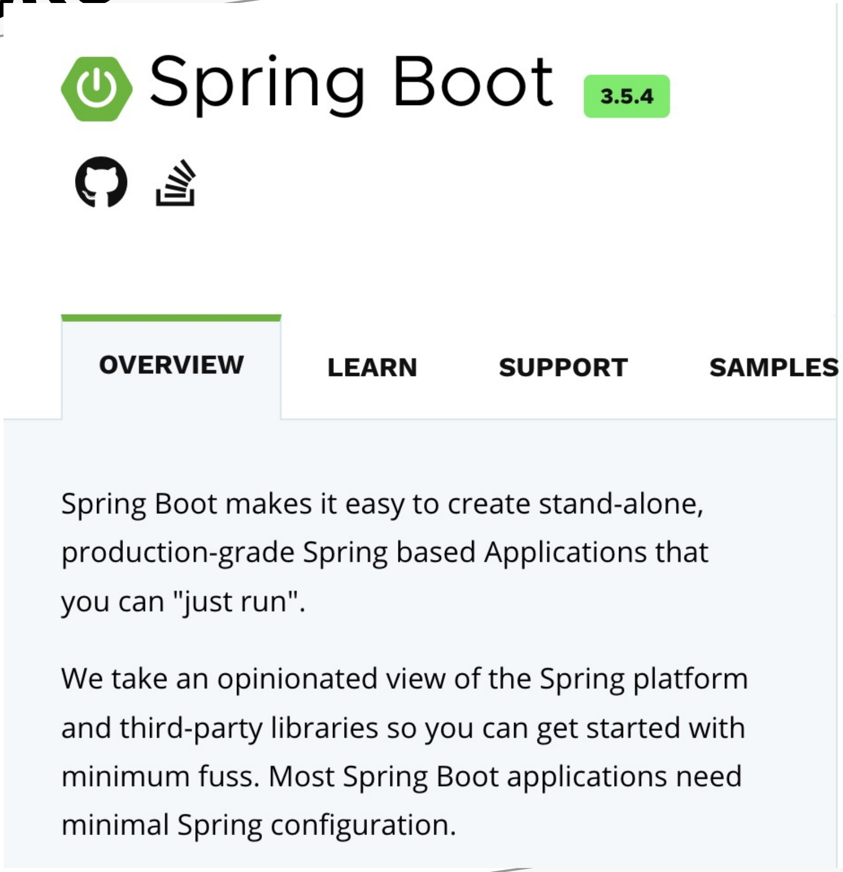
May 18, 2025

https://archive.ph/5WcRT

Chapter 5: Hacked in 15-20 Minutes

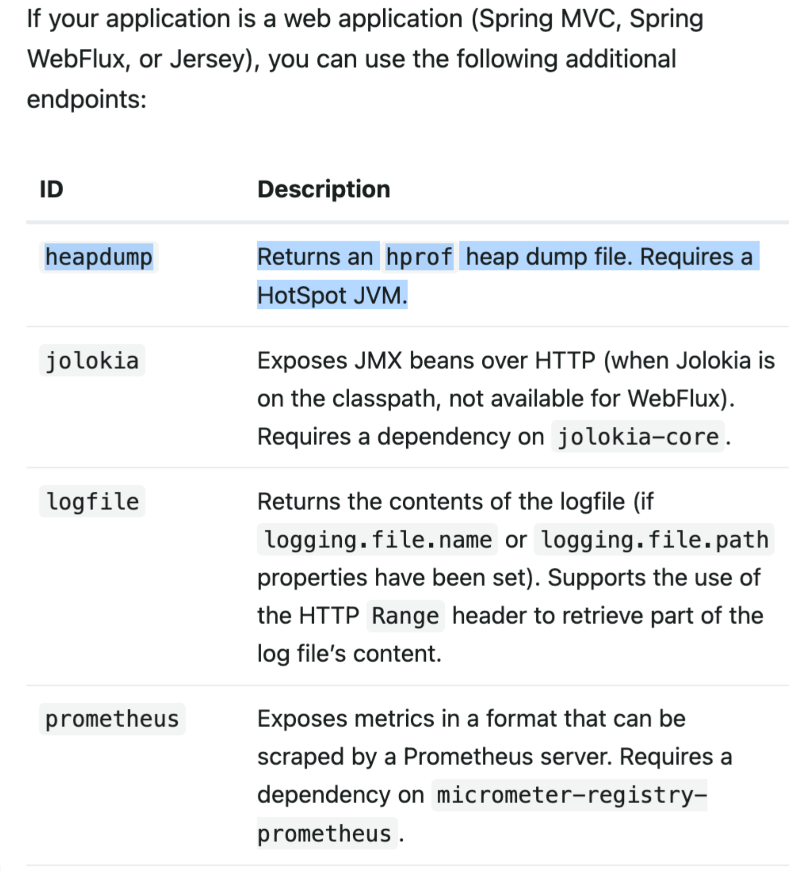
https://archive.telemessage.com/management/heapdump

Chapter 5: Hacked in 15-20 Minutes



Spring Boot makes it easy to create stand-alone, production-grade Spring based Applications that you can "just run".

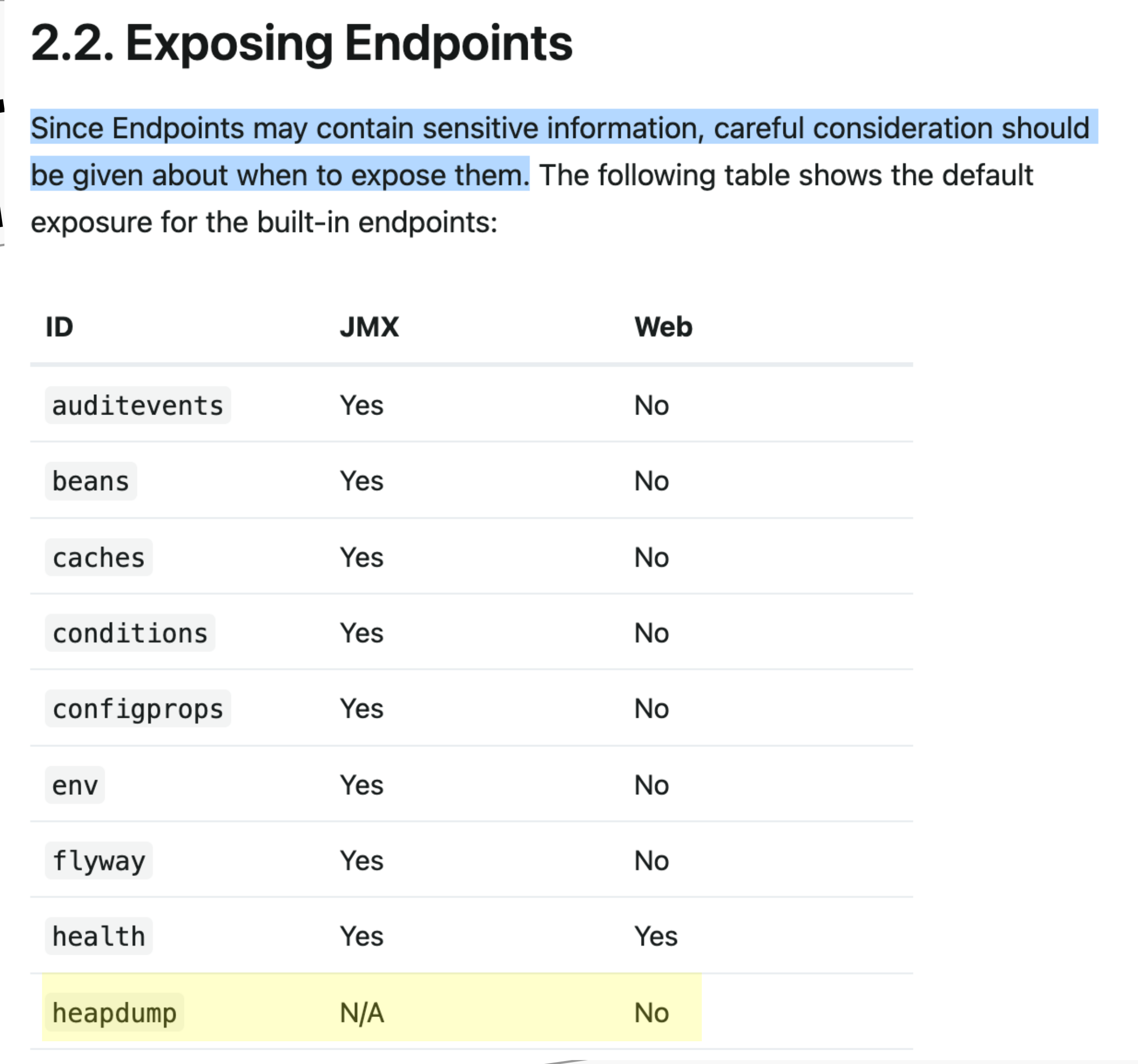
We take an opinionated view of the Spring platform and third-party libraries so you can get started with minimum fuss. Most Spring Boot applications need minimal Spring configuration.



If your application is a web application (Spring MVC, Spring WebFlux, or Jersey), you can use the following additional endpoints:

ID	Description
`heapdump`	Returns an `hprof` heap dump file. Requires a HotSpot JVM.
`jolokia`	Exposes JMX beans over HTTP (when Jolokia is on the classpath, not available for WebFlux). Requires a dependency on `jolokia-core`.
`logfile`	Returns the contents of the logfile (if `logging.file.name` or `logging.file.path` properties have been set). Supports the use of the HTTP `Range` header to retrieve part of the log file's content.
`prometheus`	Exposes metrics in a format that can be scraped by a Prometheus server. Requires a dependency on `micrometer-registry-prometheus`.

Chapter 5: Hacked in



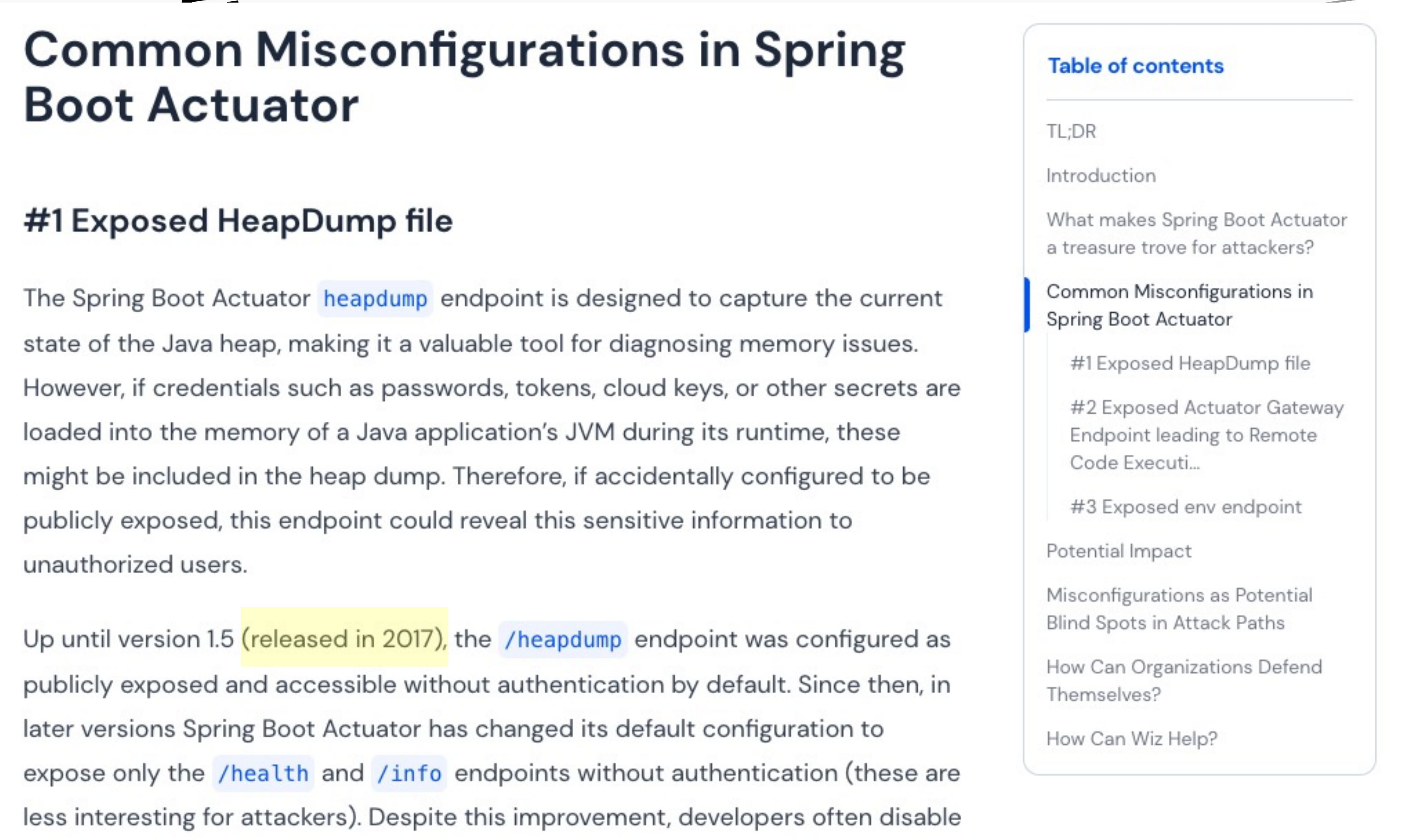
2.2. Exposing Endpoints

Since Endpoints may contain sensitive information, careful consideration should be given about when to expose them. The following table shows the default exposure for the built-in endpoints:

ID	JMX	Web
`auditevents`	Yes	No
`beans`	Yes	No
`caches`	Yes	No
`conditions`	Yes	No
`configprops`	Yes	No
`env`	Yes	No
`flyway`	Yes	No
`health`	Yes	Yes
`heapdump`	N/A	No

https://docs.spring.io/spring-boot/docs/2.5.6/reference/html/actuator.html

Cha
Hac



Common Misconfigurations in Spring Boot Actuator

#1 Exposed HeapDump file

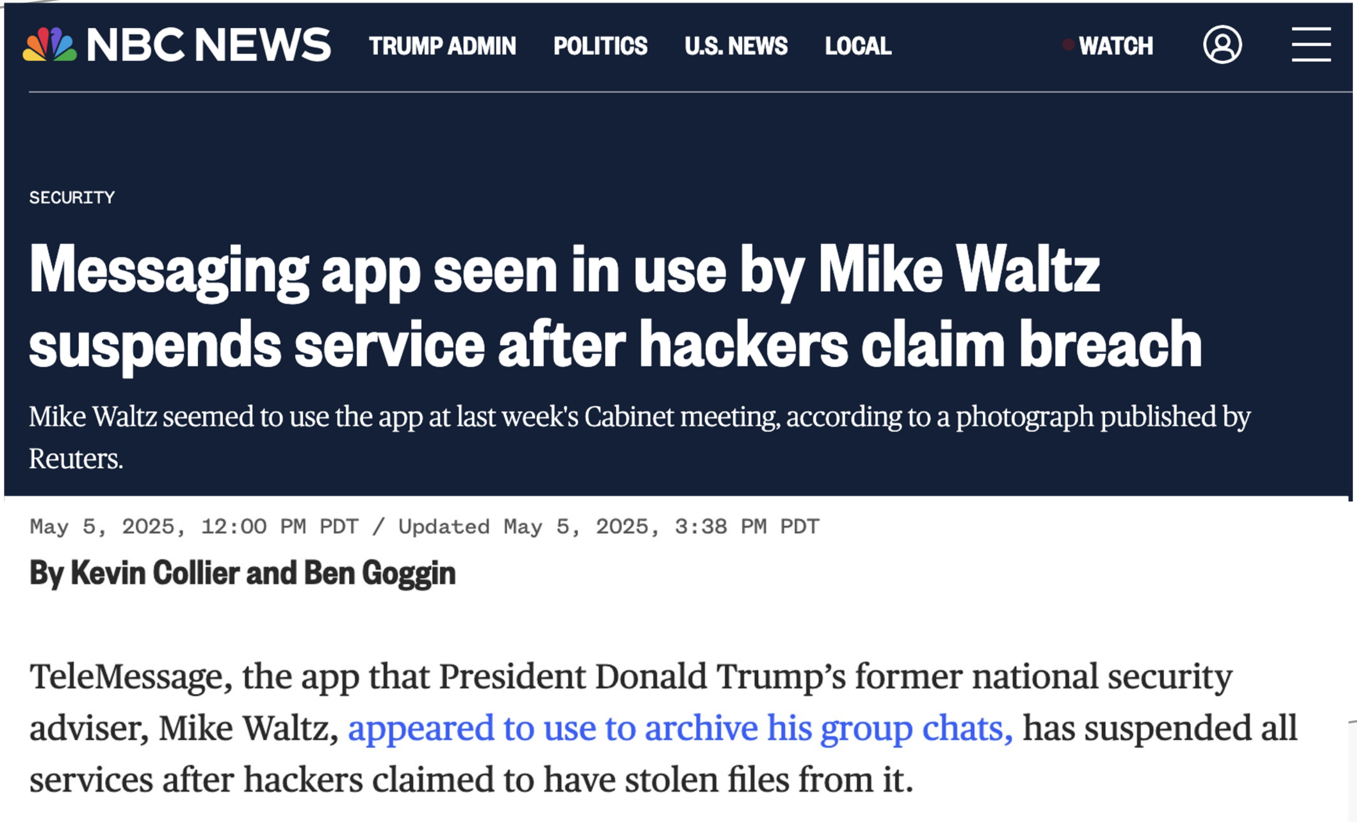
The Spring Boot Actuator `heapdump` endpoint is designed to capture the current state of the Java heap, making it a valuable tool for diagnosing memory issues. However, if credentials such as passwords, tokens, cloud keys, or other secrets are loaded into the memory of a Java application's JVM during its runtime, these might be included in the heap dump. Therefore, if accidentally configured to be publicly exposed, this endpoint could reveal this sensitive information to unauthorized users.

Up until version 1.5 (released in 2017), the `/heapdump` endpoint was configured as publicly exposed and accessible without authentication by default. Since then, in later versions Spring Boot Actuator has changed its default configuration to expose only the `/health` and `/info` endpoints without authentication (these are less interesting for attackers). Despite this improvement, developers often disable

Table of contents

https://www.wiz.io/blog/spring-boot-actuator-misconfigurations

Chapter 5: Hacked in 15-20 Minutes



SECURITY

Messaging app seen in use by Mike Waltz suspends service after hackers claim breach

Mike Waltz seemed to use the app at last week's Cabinet meeting, according to a photograph published by Reuters.

May 5, 2025, 12:00 PM PDT / Updated May 5, 2025, 3:38 PM PDT

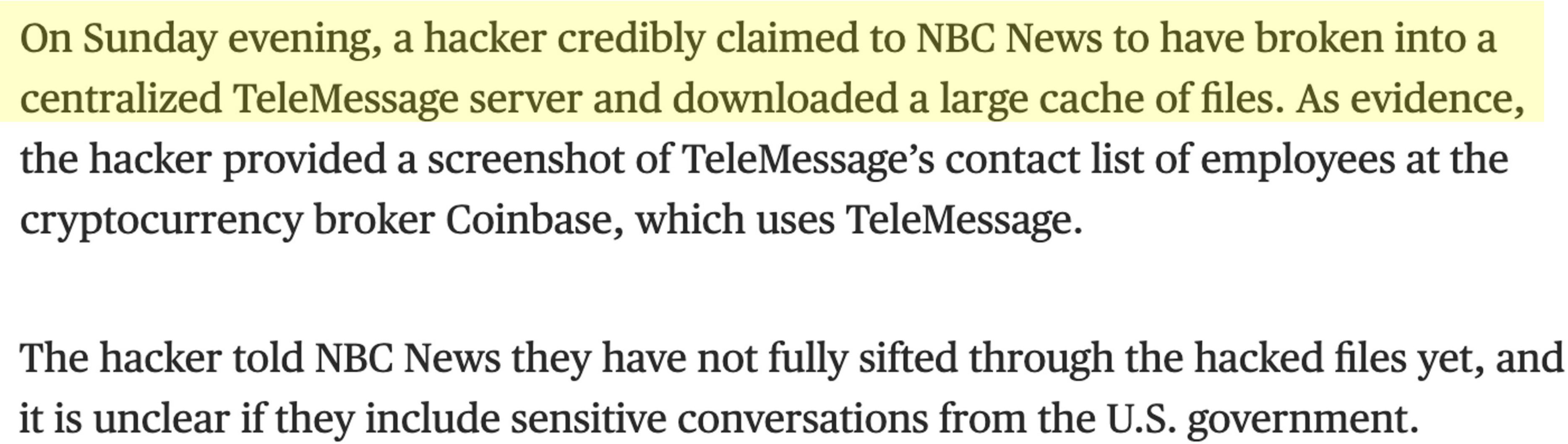
By Kevin Collier and Ben Goggin

TeleMessage, the app that President Donald Trump's former national security adviser, Mike Waltz, appeared to use to archive his group chats, has suspended all services after hackers claimed to have stolen files from it.

May 5, 2025

https://archive.ph/OFuGy

Chapter 5: Hacked in 15-20 Minutes



On Sunday evening, a hacker credibly claimed to NBC News to have broken into a centralized TeleMessage server and downloaded a large cache of files. As evidence, the hacker provided a screenshot of TeleMessage's contact list of employees at the cryptocurrency broker Coinbase, which uses TeleMessage.

The hacker told NBC News they have not fully sifted through the hacked files yet, and it is unclear if they include sensitive conversations from the U.S. government.

May 5, 2025

https://archive.ph/OFuGy

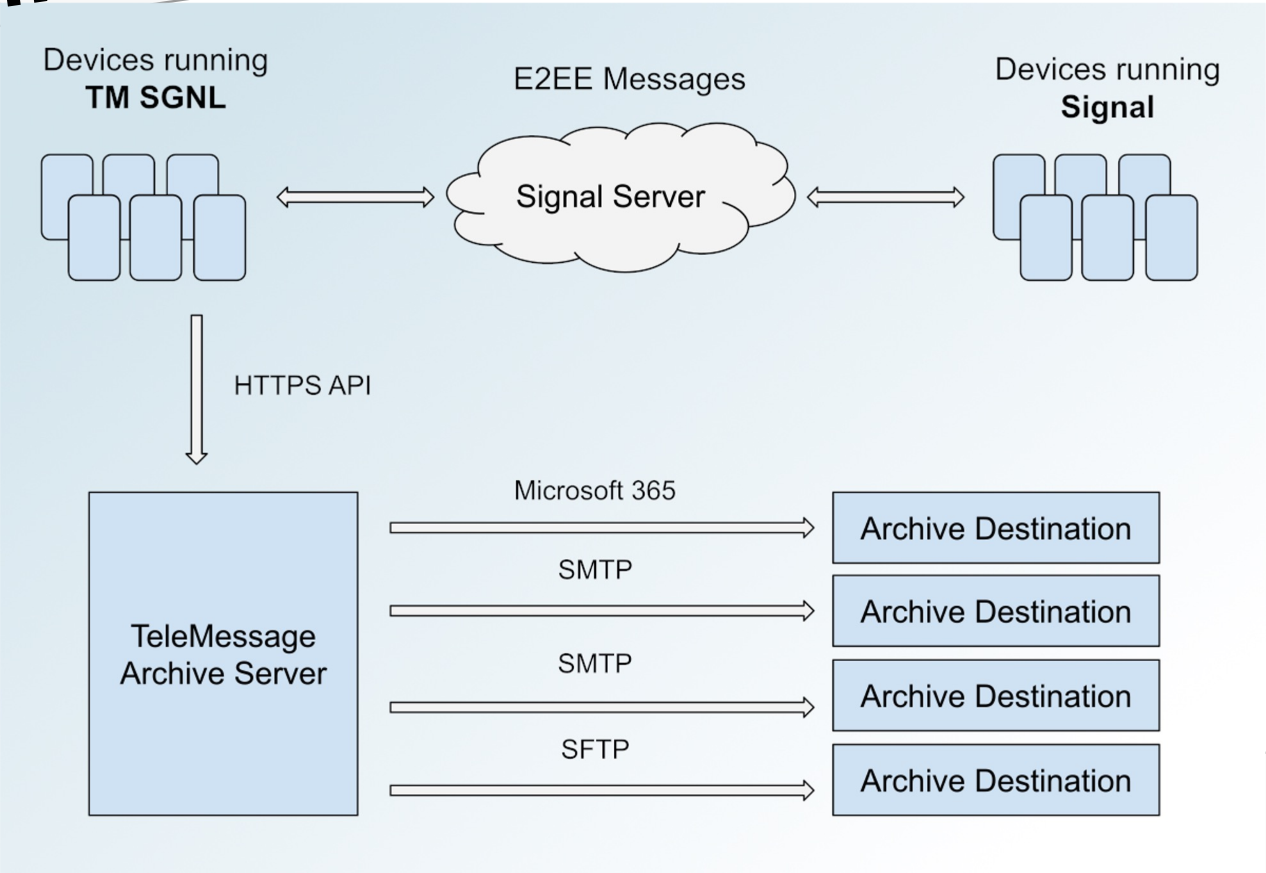
Chapter 6:
End-to-Middle-to-End Encryption

> “ Despite misleading marketing, Israeli company TeleMessage, used by Trump officials, can access plaintext chat logs ”

May 6, 2025

https://micahflee.com/telemessage-analysis/

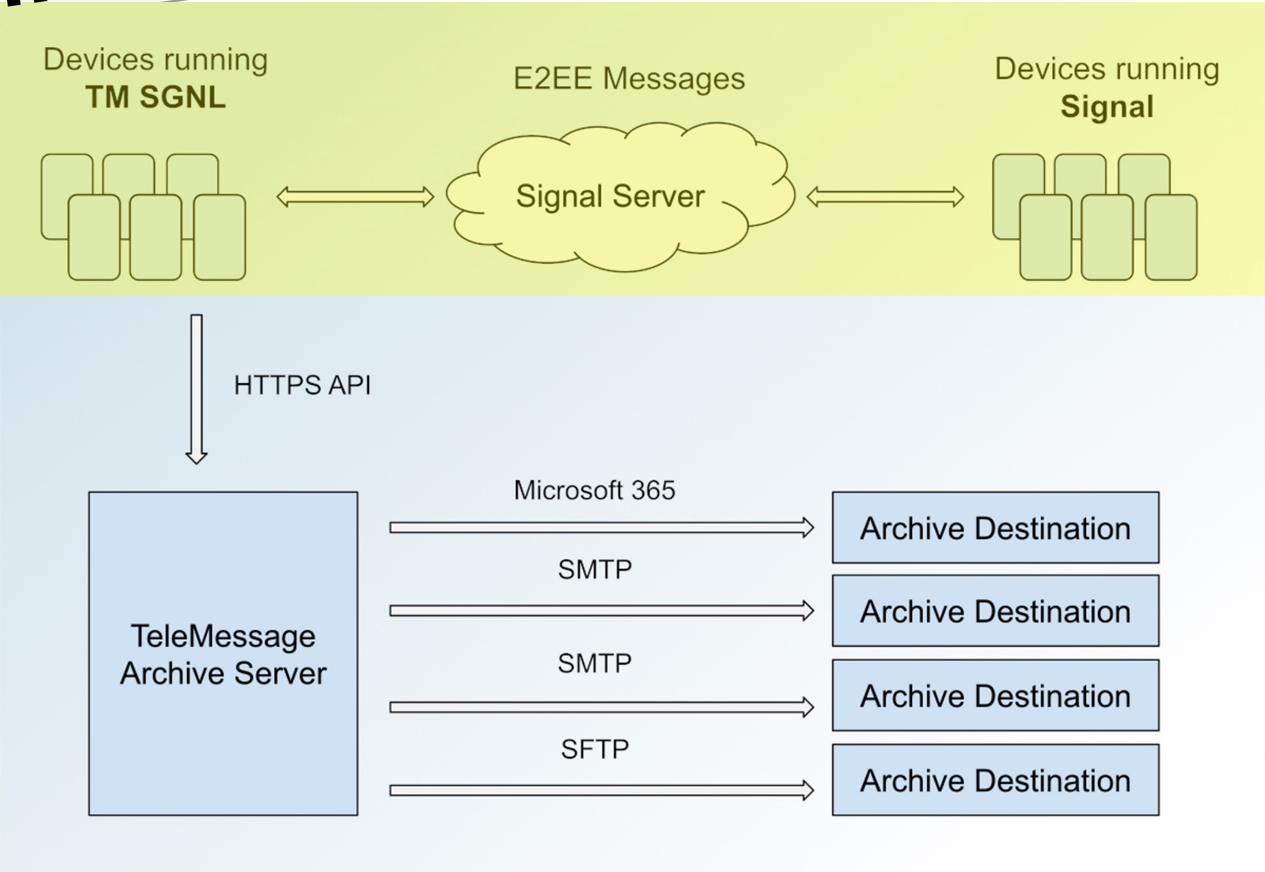
Chapter 6:
End-to-Middle-to-End Encryption



May 6, 2025

https://micahflee.com/telemessage-analysis/

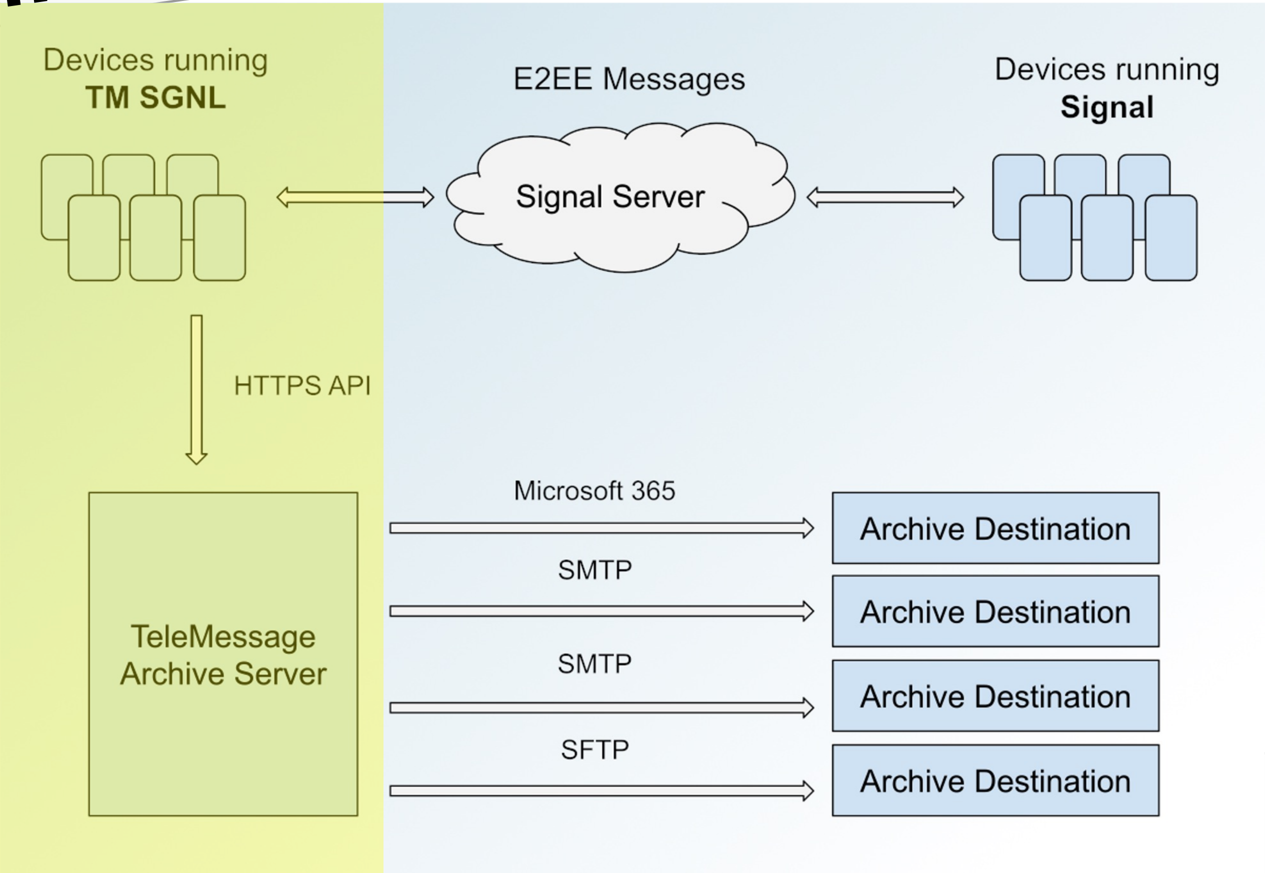
Chapter 6:
End-to-Middle-to-End Encryption



May 6, 2025

https://micahflee.com/telemessage-analysis/

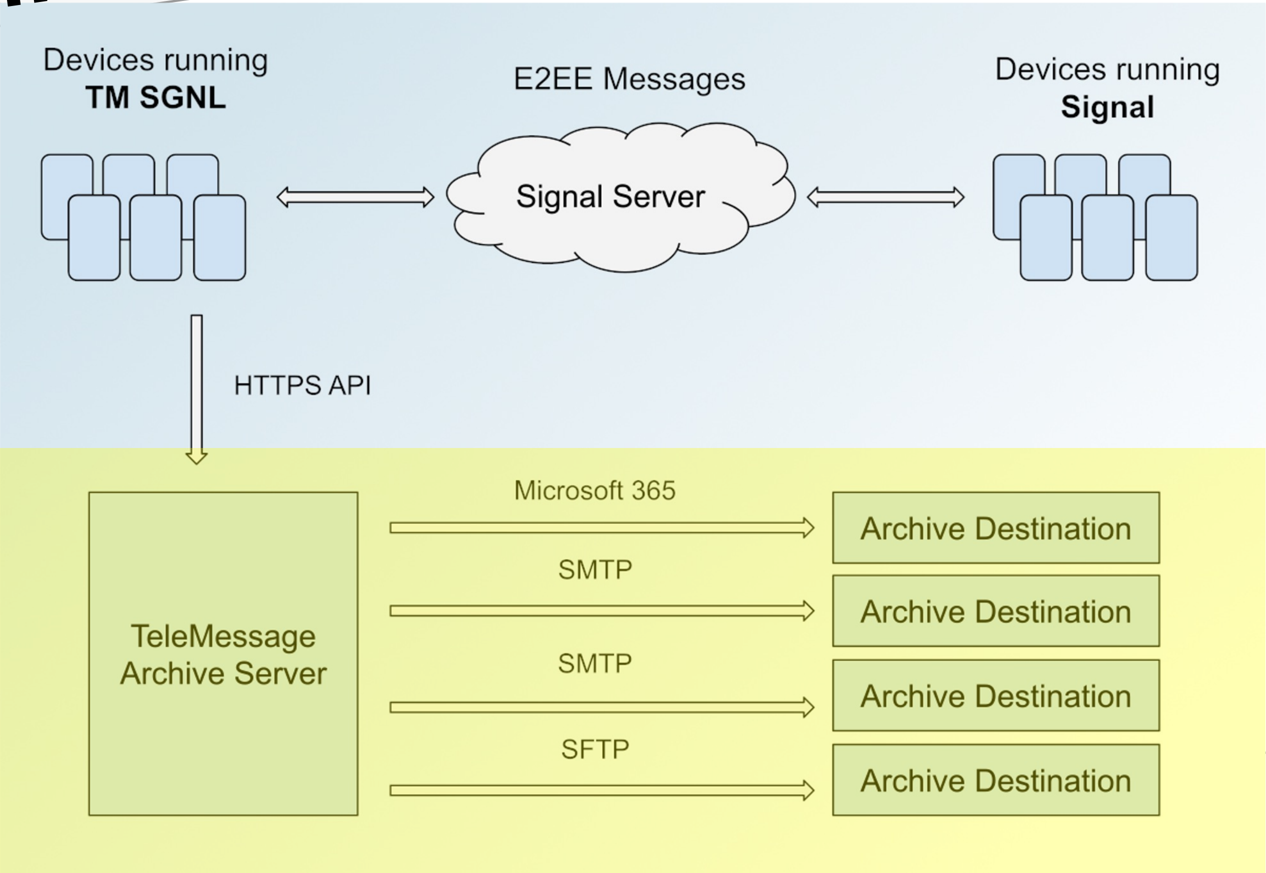
Chapter 6: End-to-Middle-to-End Encryption



May 6, 2025

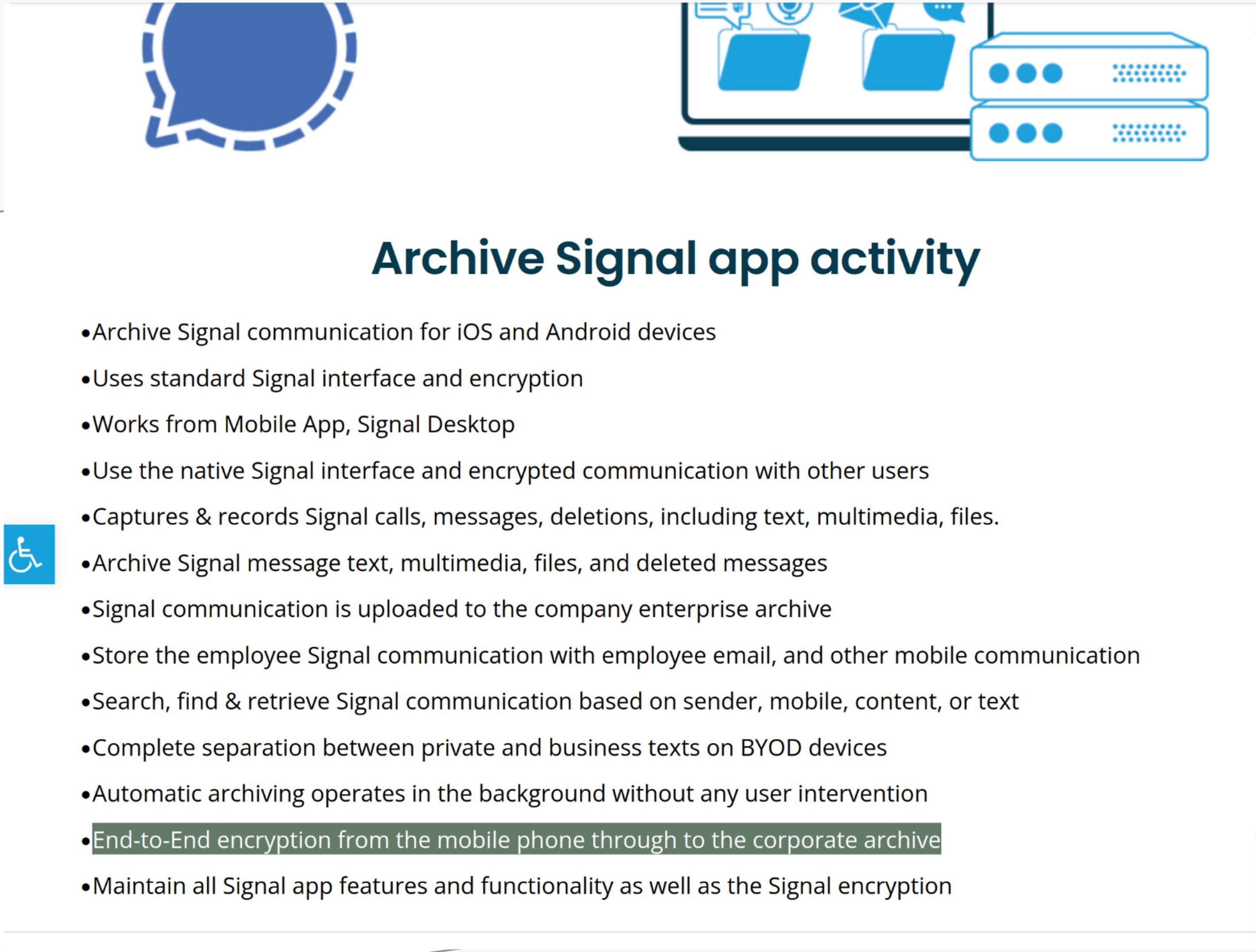
https://micahflee.com/telemessage-analysis/

Chapter 6:
End-to-Middle-to-End Encryption



May 6, 2025

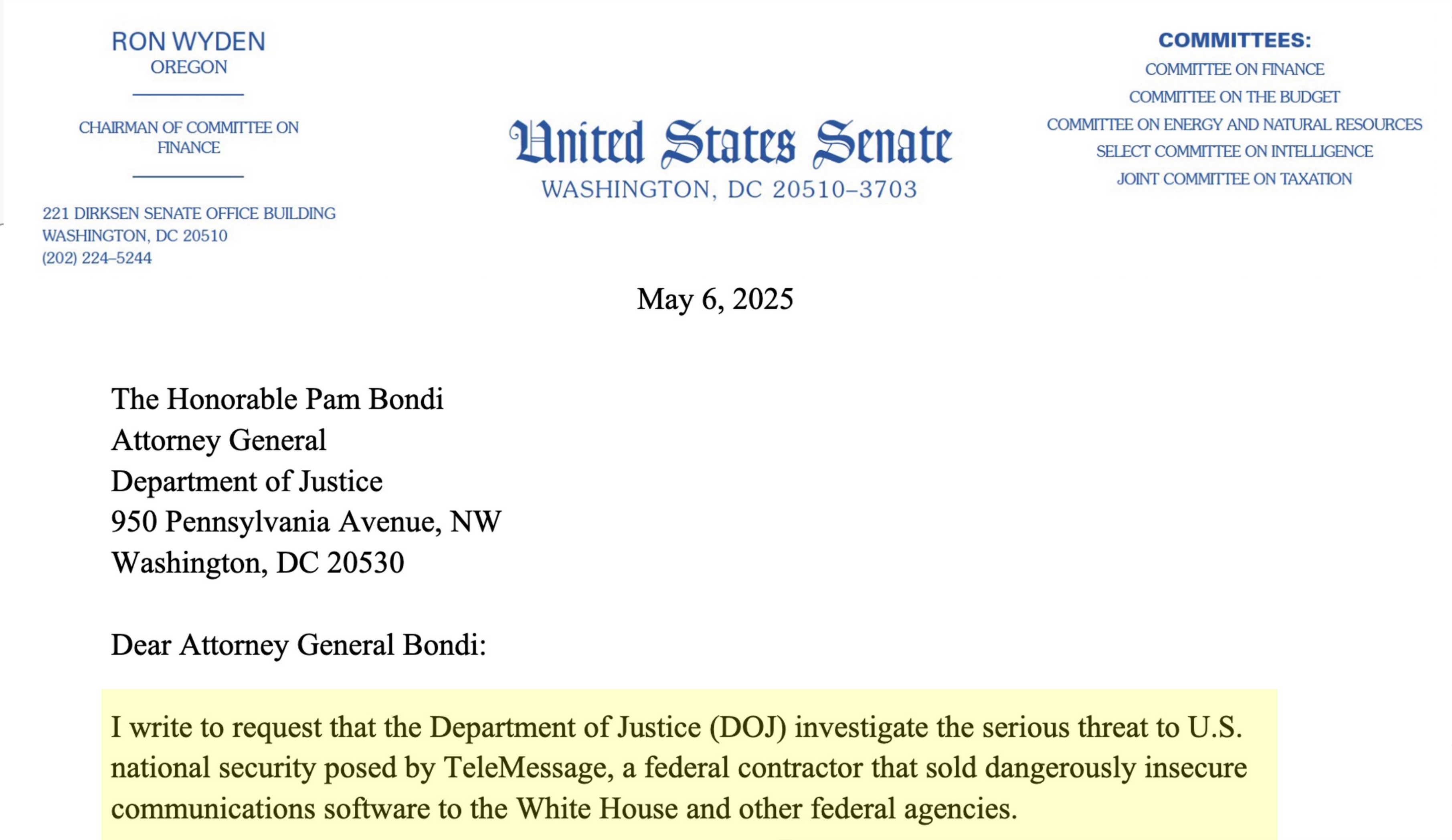
https://micahflee.com/telemessage-analysis/



Archive Signal app activity

- Archive Signal communication for iOS and Android devices
- Uses standard Signal interface and encryption
- Works from Mobile App, Signal Desktop
- Use the native Signal interface and encrypted communication with other users
- Captures & records Signal calls, messages, deletions, including text, multimedia, files.
- Archive Signal message text, multimedia, files, and deleted messages
- Signal communication is uploaded to the company enterprise archive
- Store the employee Signal communication with employee email, and other mobile communication
- Search, find & retrieve Signal communication based on sender, mobile, content, or text
- Complete separation between private and business texts on BYOD devices
- Automatic archiving operates in the background without any user intervention
- End-to-End encryption from the mobile phone through to the corporate archive
- Maintain all Signal app features and functionality as well as the Signal encryption

from an archive of https://www.telemessage.com/mobile-archiver/signal-archiver/



RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON
FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224–5244

United States Senate
WASHINGTON, DC 20510–3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL RESOURCES
SELECT COMMITTEE ON INTELLIGENCE
JOINT COMMITTEE ON TAXATION

May 6, 2025

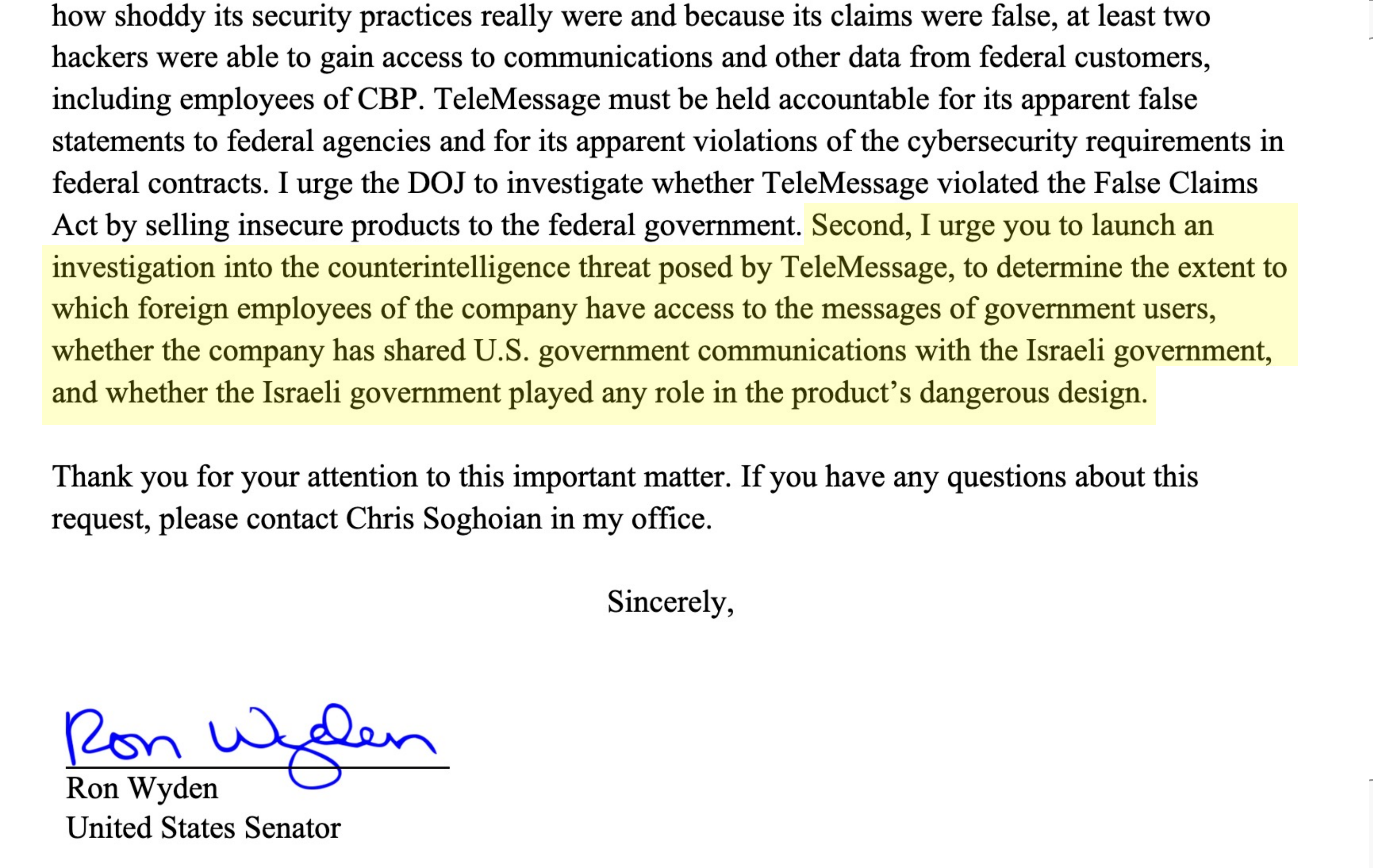
The Honorable Pam Bondi
Attorney General
Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Attorney General Bondi:

I write to request that the Department of Justice (DOJ) investigate the serious threat to U.S. national security posed by TeleMessage, a federal contractor that sold dangerously insecure communications software to the White House and other federal agencies.

May 6, 2025

https://www.wyden.senate.gov/imo/media/doc/doj_letter_telemessage.pdf



how shoddy its security practices really were and because its claims were false, at least two hackers were able to gain access to communications and other data from federal customers, including employees of CBP. TeleMessage must be held accountable for its apparent false statements to federal agencies and for its apparent violations of the cybersecurity requirements in federal contracts. I urge the DOJ to investigate whether TeleMessage violated the False Claims Act by selling insecure products to the federal government. Second, I urge you to launch an investigation into the counterintelligence threat posed by TeleMessage, to determine the extent to which foreign employees of the company have access to the messages of government users, whether the company has shared U.S. government communications with the Israeli government, and whether the Israeli government played any role in the product's dangerous design.

Thank you for your attention to this important matter. If you have any questions about this request, please contact Chris Soghoian in my office.

Sincerely,

Ron Wyden

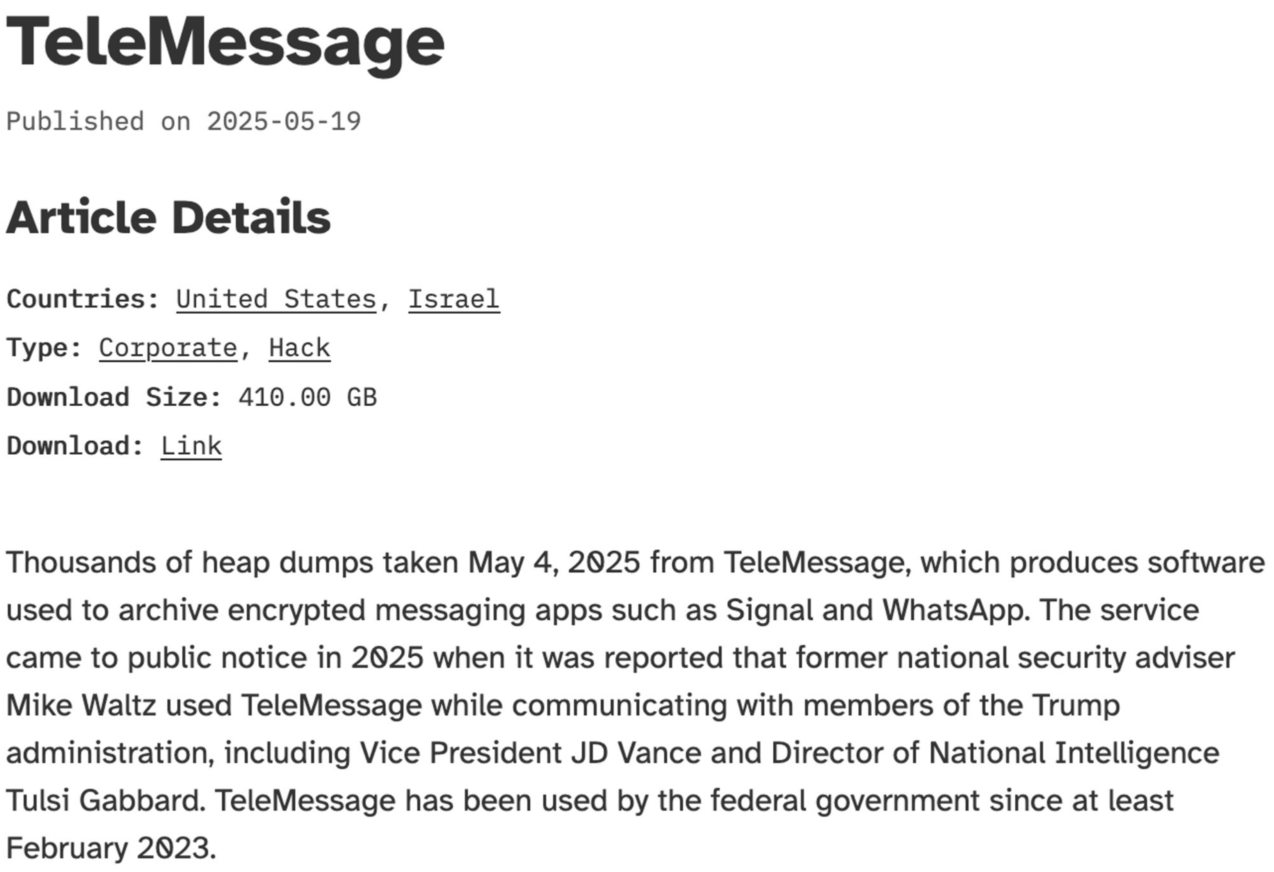
Ron Wyden
United States Senator

May 6, 2025

https://www.wyden.senate.gov/imo/media/doc/doj_letter_telemessage.pdf

Chapter 7: Drowning in Heap Dumps

Distributed Denial of Secrets



TeleMessage

Published on 2025-05-19

Article Details

Countries: United States, Israel

Type: Corporate, Hack

Download Size: 410.00 GB

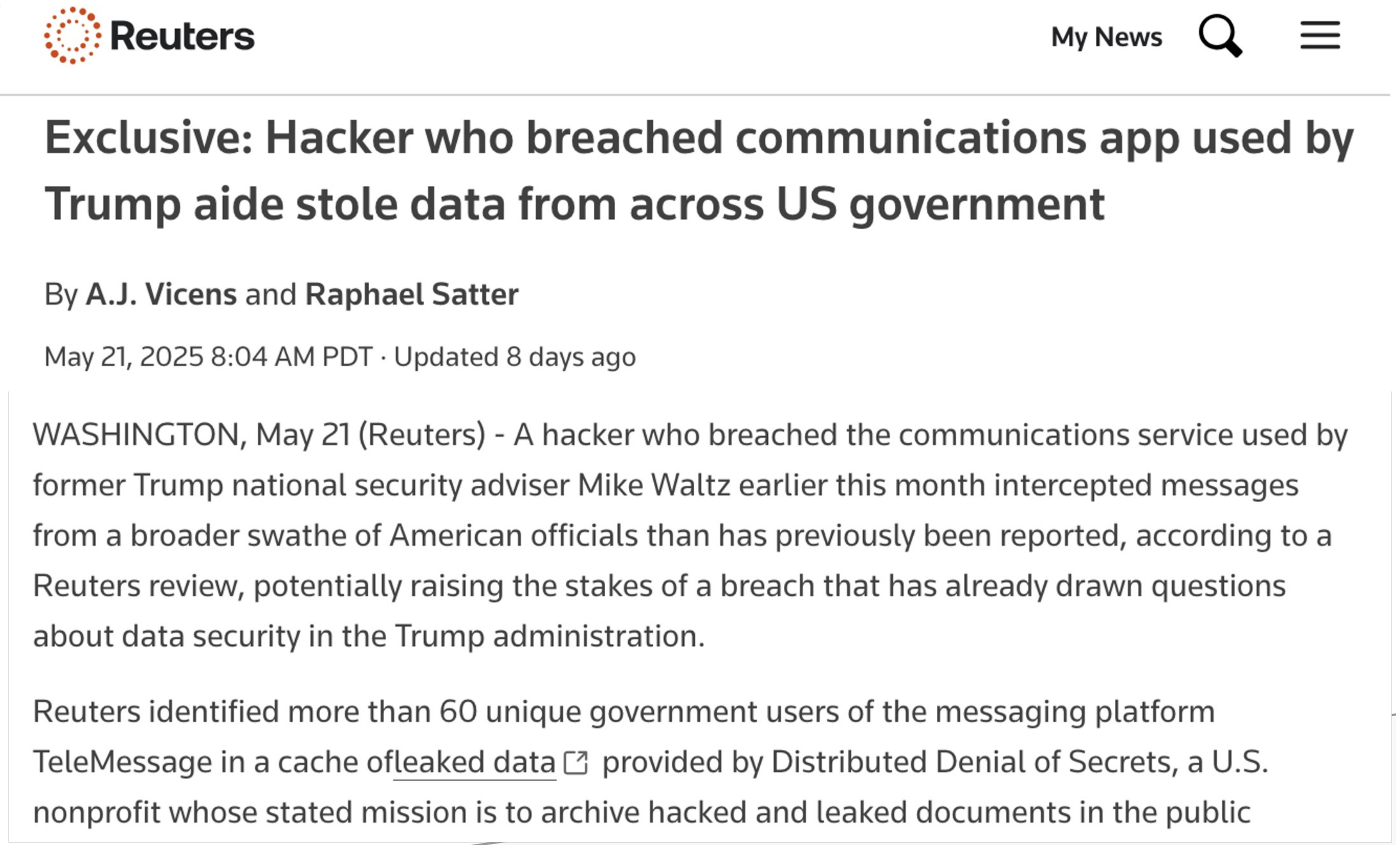
Download: Link

Thousands of heap dumps taken May 4, 2025 from TeleMessage, which produces software used to archive encrypted messaging apps such as Signal and WhatsApp. The service came to public notice in 2025 when it was reported that former national security adviser Mike Waltz used TeleMessage while communicating with members of the Trump administration, including Vice President JD Vance and Director of National Intelligence Tulsi Gabbard. TeleMessage has been used by the federal government since at least February 2023.

May 19, 2025

https://ddosecrets.com/article/telemessage

Chapter 7: Drowning in Heap Dumps



Exclusive: Hacker who breached communications app used by Trump aide stole data from across US government

By **A.J. Vicens** and **Raphael Satter**

May 21, 2025 8:04 AM PDT · Updated 8 days ago

WASHINGTON, May 21 (Reuters) - A hacker who breached the communications service used by former Trump national security adviser Mike Waltz earlier this month intercepted messages from a broader swathe of American officials than has previously been reported, according to a Reuters review, potentially raising the stakes of a breach that has already drawn questions about data security in the Trump administration.

Reuters identified more than 60 unique government users of the messaging platform TeleMessage in a cache ofleaked data provided by Distributed Denial of Secrets, a U.S. nonprofit whose stated mission is to archive hacked and leaked documents in the public

May 21, 2025

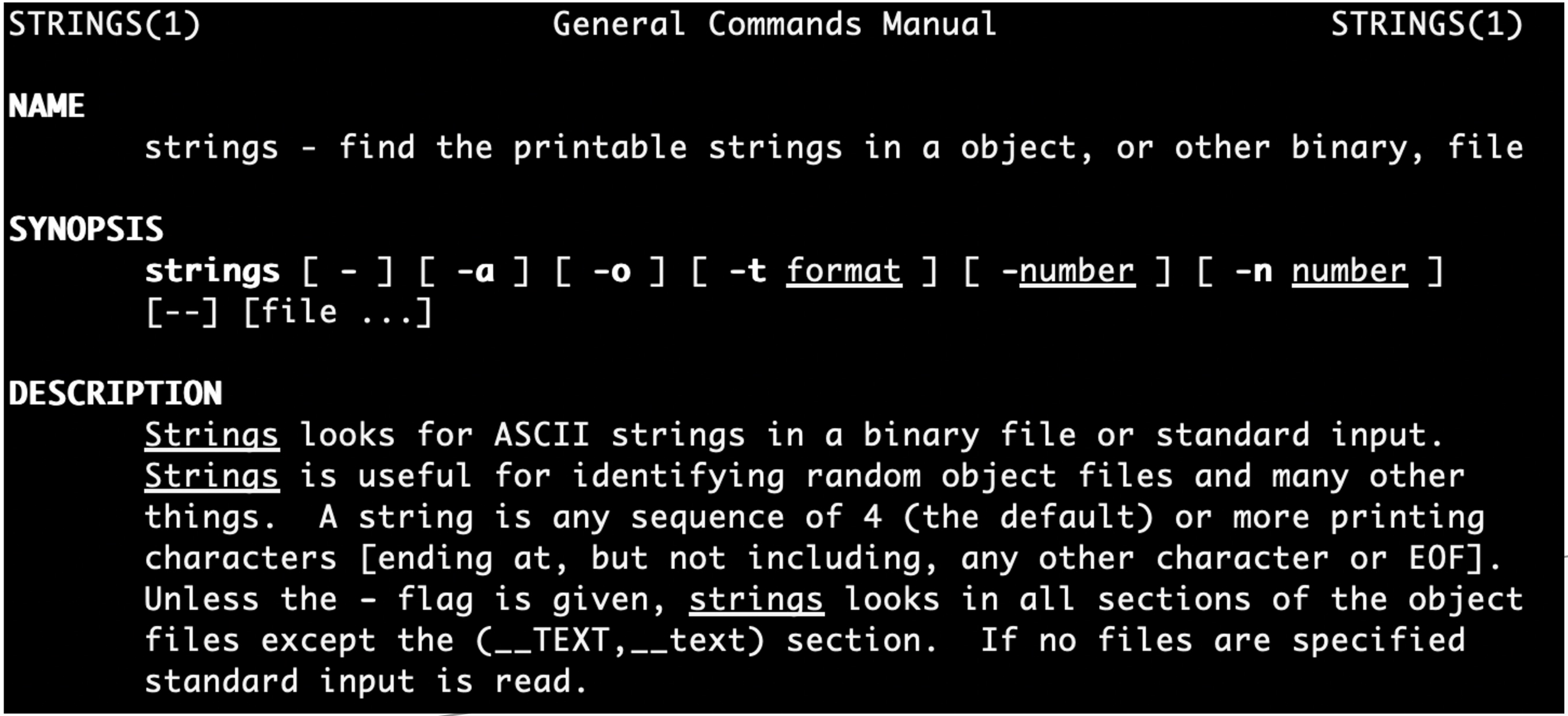
https://archive.ph/75Qwv

Chapter 7: Drowning in Heap Dumps

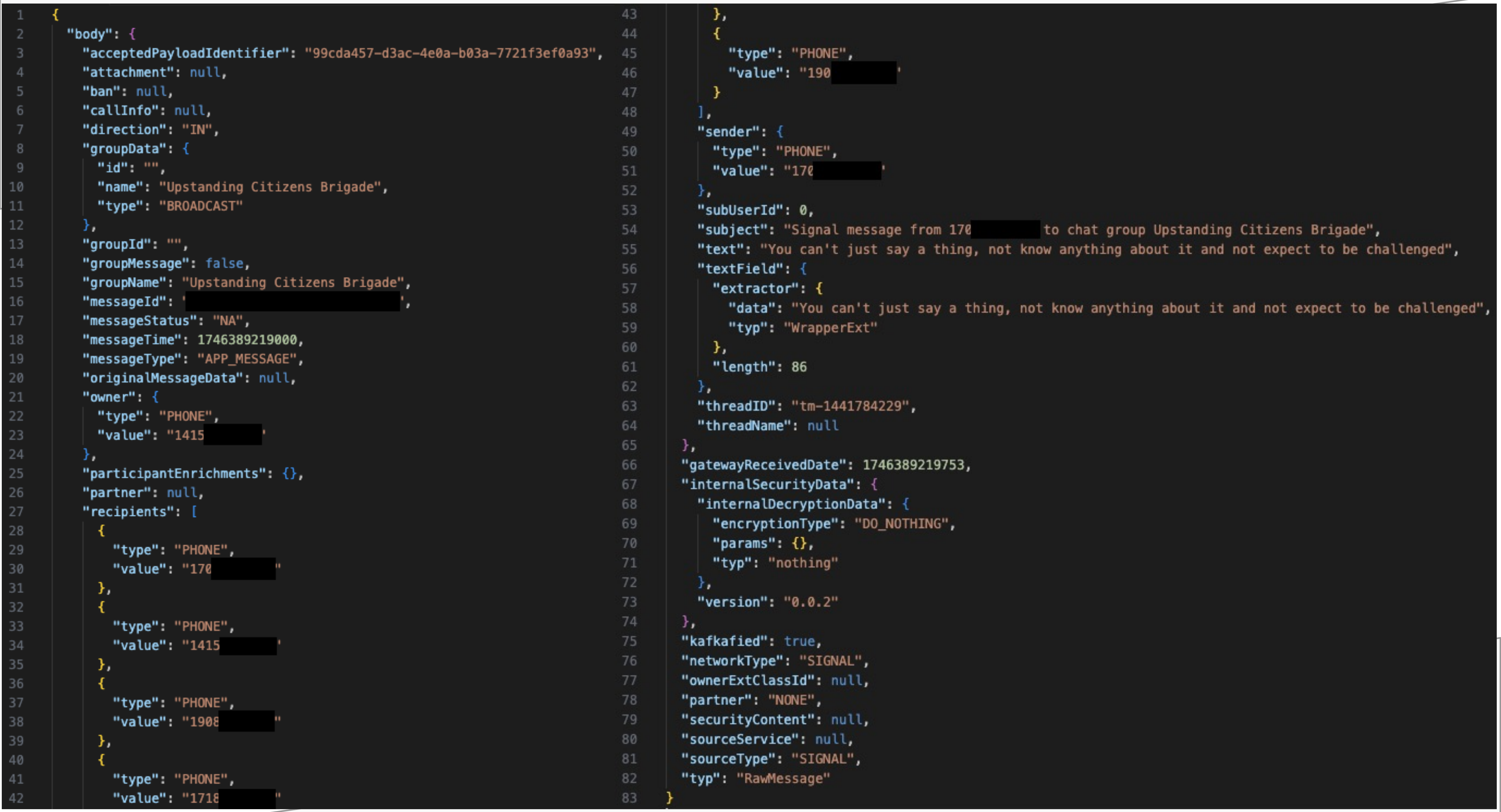
What is this data?

- 2,729 Java heap dumps, in HPROF format
- 130 MB to 291 MB each
- *Not* a copy of the data stored on the archive server
- Rather, fragments of data that happened to be in memory on Sunday, May 4, 2025

Chapter 7: Drowning in Heap Dumps



```
STRINGS(1)                General Commands Manual               STRINGS(1)

NAME
       strings - find the printable strings in a object, or other binary, file

SYNOPSIS
       strings [ - ] [ -a ] [ -o ] [ -t format ] [ -number ] [ -n number ]
       [--] [file ...]

DESCRIPTION
       Strings looks for ASCII strings in a binary file or standard input.
       Strings is useful for identifying random object files and many other
       things.  A string is any sequence of 4 (the default) or more printing
       characters [ending at, but not including, any other character or EOF].
       Unless the - flag is given, strings looks in all sections of the object
       files except the (__TEXT,__text) section.  If no files are specified
       standard input is read.
```

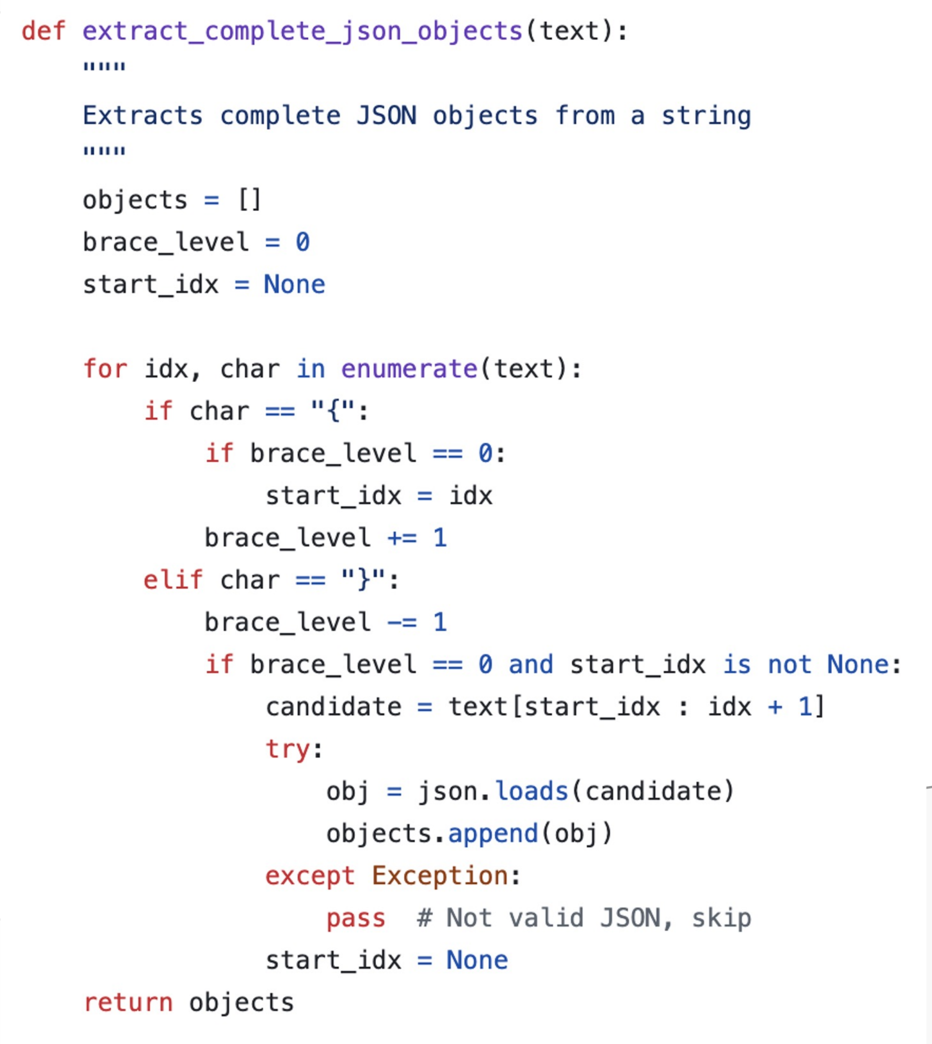


```
{
  "body": {
    "acceptedPayloadIdentifier": "99cda457-d3ac-4e0a-b03a-7721f3ef0a93",
    "attachment": null,
    "ban": null,
    "callInfo": null,
    "direction": "IN",
    "groupData": {
      "id": "",
      "name": "Upstanding Citizens Brigade",
      "type": "BROADCAST"
    },
    "groupId": "",
    "groupMessage": false,
    "groupName": "Upstanding Citizens Brigade",
    "messageId": "[redacted]",
    "messageStatus": "NA",
    "messageTime": 1746389219000,
    "messageType": "APP_MESSAGE",
    "originalMessageData": null,
    "owner": {
      "type": "PHONE",
      "value": "1415[redacted]"
    },
    "participantEnrichments": {},
    "partner": null,
    "recipients": [
      {
        "type": "PHONE",
        "value": "170[redacted]"
      },
      {
        "type": "PHONE",
        "value": "1415[redacted]"
      },
      {
        "type": "PHONE",
        "value": "1908[redacted]"
      },
      {
        "type": "PHONE",
        "value": "1718[redacted]"
      },
      {
        "type": "PHONE",
        "value": "190[redacted]"
      }
    ],
    "sender": {
      "type": "PHONE",
      "value": "170[redacted]"
    },
    "subUserId": 0,
    "subject": "Signal message from 170[redacted] to chat group Upstanding Citizens Brigade",
    "text": "You can't just say a thing, not know anything about it and not expect to be challenged",
    "textField": {
      "extractor": {
        "data": "You can't just say a thing, not know anything about it and not expect to be challenged",
        "typ": "WrapperExt"
      },
      "length": 86
    },
    "threadID": "tm-1441784229",
    "threadName": null
  },
  "gatewayReceivedDate": 1746389219753,
  "internalSecurityData": {
    "internalDecryptionData": {
      "encryptionType": "DO_NOTHING",
      "params": {},
      "typ": "nothing"
    },
    "version": "0.0.2"
  },
  "kafkafied": true,
  "networkType": "SIGNAL",
  "ownerExtClassId": null,
  "partner": "NONE",
  "securityContent": null,
  "sourceService": null,
  "sourceType": "SIGNAL",
  "typ": "RawMessage"
}
```

Chapter 7: Drowning in Heap Dumps

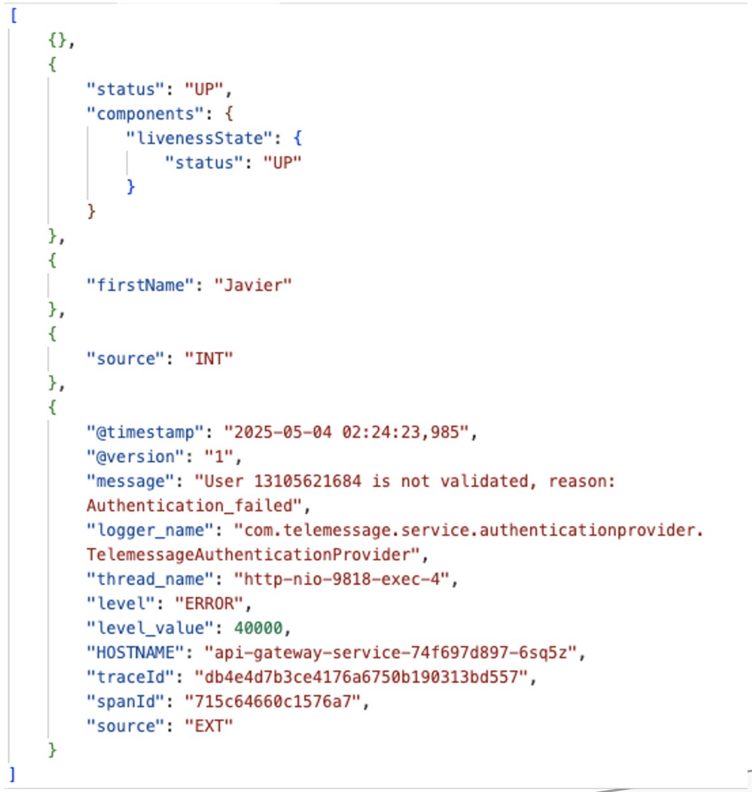
Grepping for known JSON objects works, *but what if I miss stuff?*

Solution: Extract every single complete JSON object from every single heap dump.



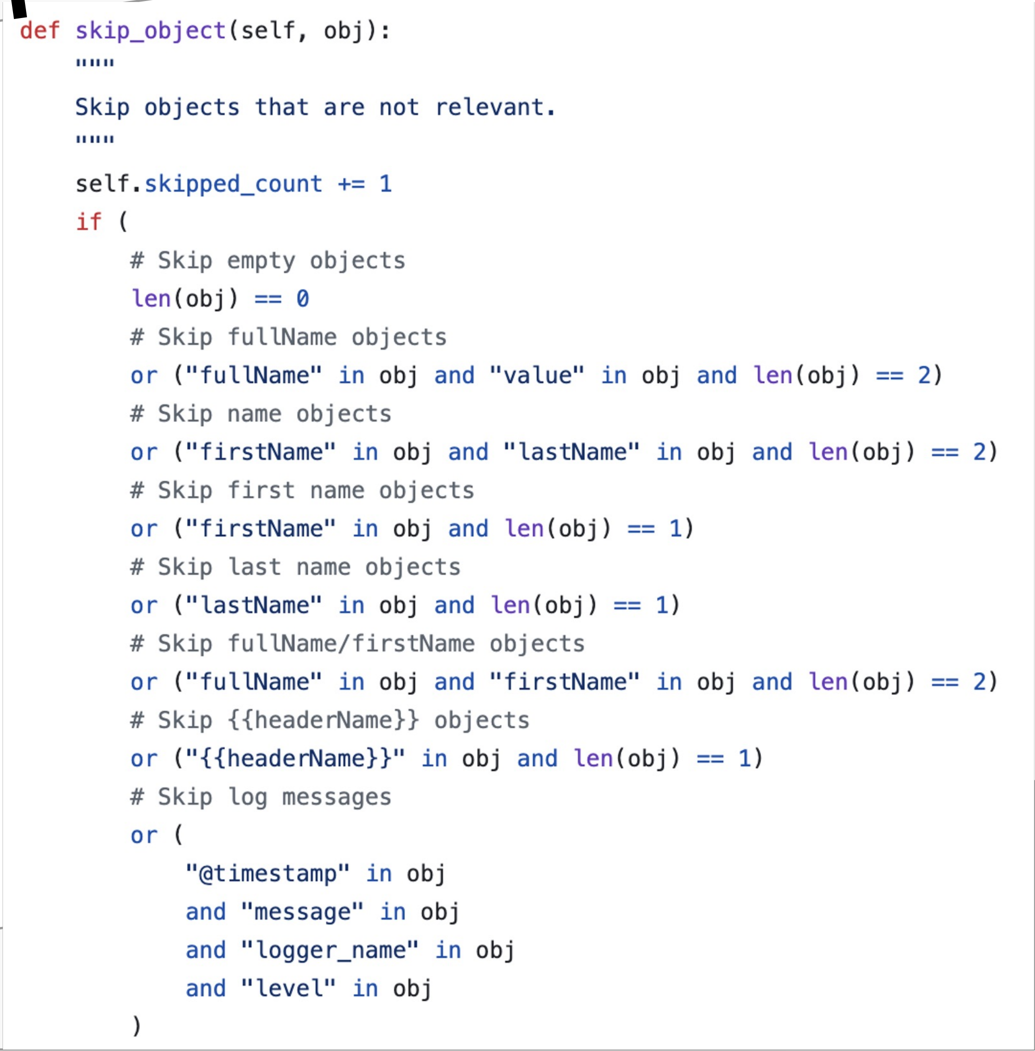
```
def extract_complete_json_objects(text):
    """
    Extracts complete JSON objects from a string
    """
    objects = []
    brace_level = 0
    start_idx = None

    for idx, char in enumerate(text):
        if char == "{":
            if brace_level == 0:
                start_idx = idx
            brace_level += 1
        elif char == "}":
            brace_level -= 1
            if brace_level == 0 and start_idx is not None:
                candidate = text[start_idx : idx + 1]
                try:
                    obj = json.loads(candidate)
                    objects.append(obj)
                except Exception:
                    pass  # Not valid JSON, skip
                start_idx = None
    return objects
```

Chapter 7: Drowning in Heap Dumps



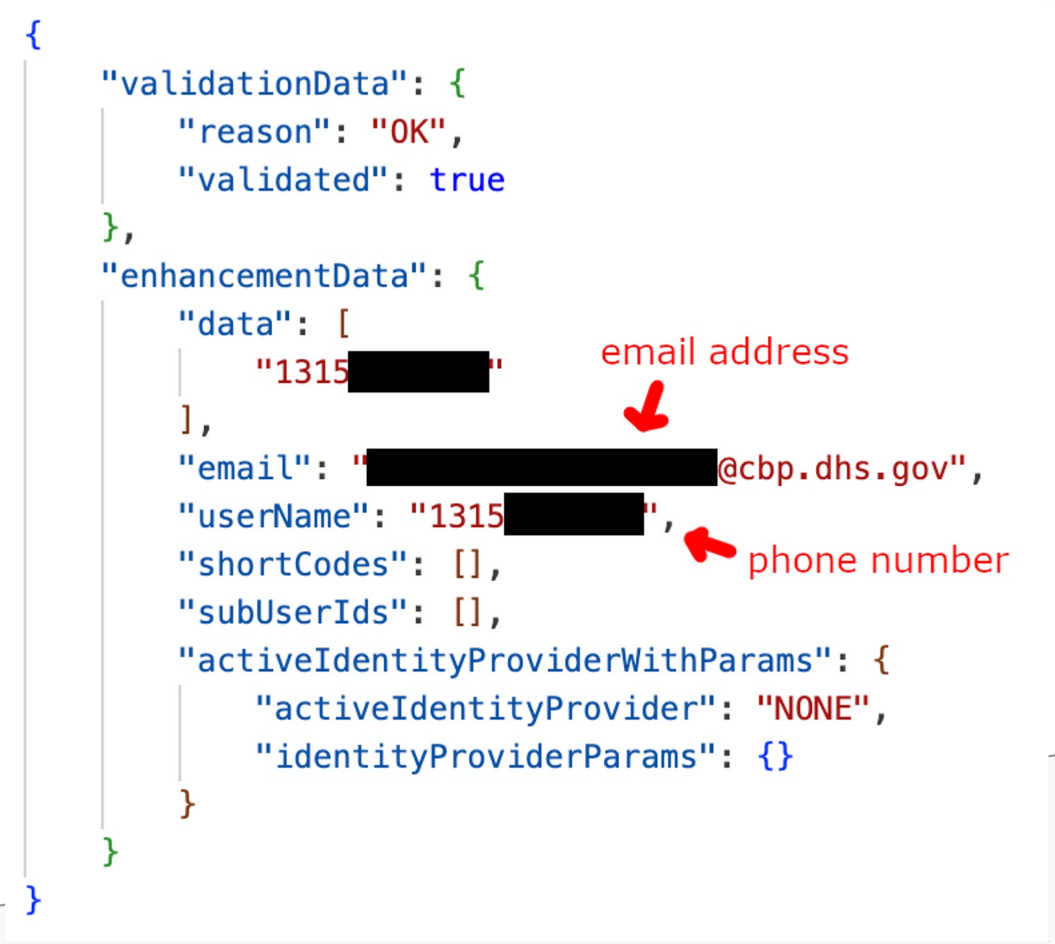
```
[
    {},
    {
        "status": "UP",
        "components": {
            "livenessState": {
                "status": "UP"
            }
        }
    },
    {
        "firstName": "Javier"
    },
    {
        "source": "INT"
    },
    {
        "@timestamp": "2025-05-04 02:24:23,985",
        "@version": "1",
        "message": "User 13105621684 is not validated, reason:
        Authentication_failed",
        "logger_name": "com.telemessage.service.authenticationprovider.
        TelemessageAuthenticationProvider",
        "thread_name": "http-nio-9818-exec-4",
        "level": "ERROR",
        "level_value": 40000,
        "HOSTNAME": "api-gateway-service-74f697d897-6sq5z",
        "traceId": "db4e4d7b3ce4176a6750b190313bd557",
        "spanId": "715c64660c1576a7",
        "source": "EXT"
    }
]
```

Example JSON objects this code skips



```python
def skip_object(self, obj):
    """
    Skip objects that are not relevant.
    """
    self.skipped_count += 1
    if (
        # Skip empty objects
        len(obj) == 0
        # Skip fullName objects
        or ("fullName" in obj and "value" in obj and len(obj) == 2)
        # Skip name objects
        or ("firstName" in obj and "lastName" in obj and len(obj) == 2)
        # Skip first name objects
        or ("firstName" in obj and len(obj) == 1)
        # Skip last name objects
        or ("lastName" in obj and len(obj) == 1)
        # Skip fullName/firstName objects
        or ("fullName" in obj and "firstName" in obj and len(obj) == 2)
        # Skip {{headerName}} objects
        or ("{{headerName}}" in obj and len(obj) == 1)
        # Skip log messages
        or (
            "@timestamp" in obj
            and "message" in obj
            and "logger_name" in obj
            and "level" in obj
        )
```

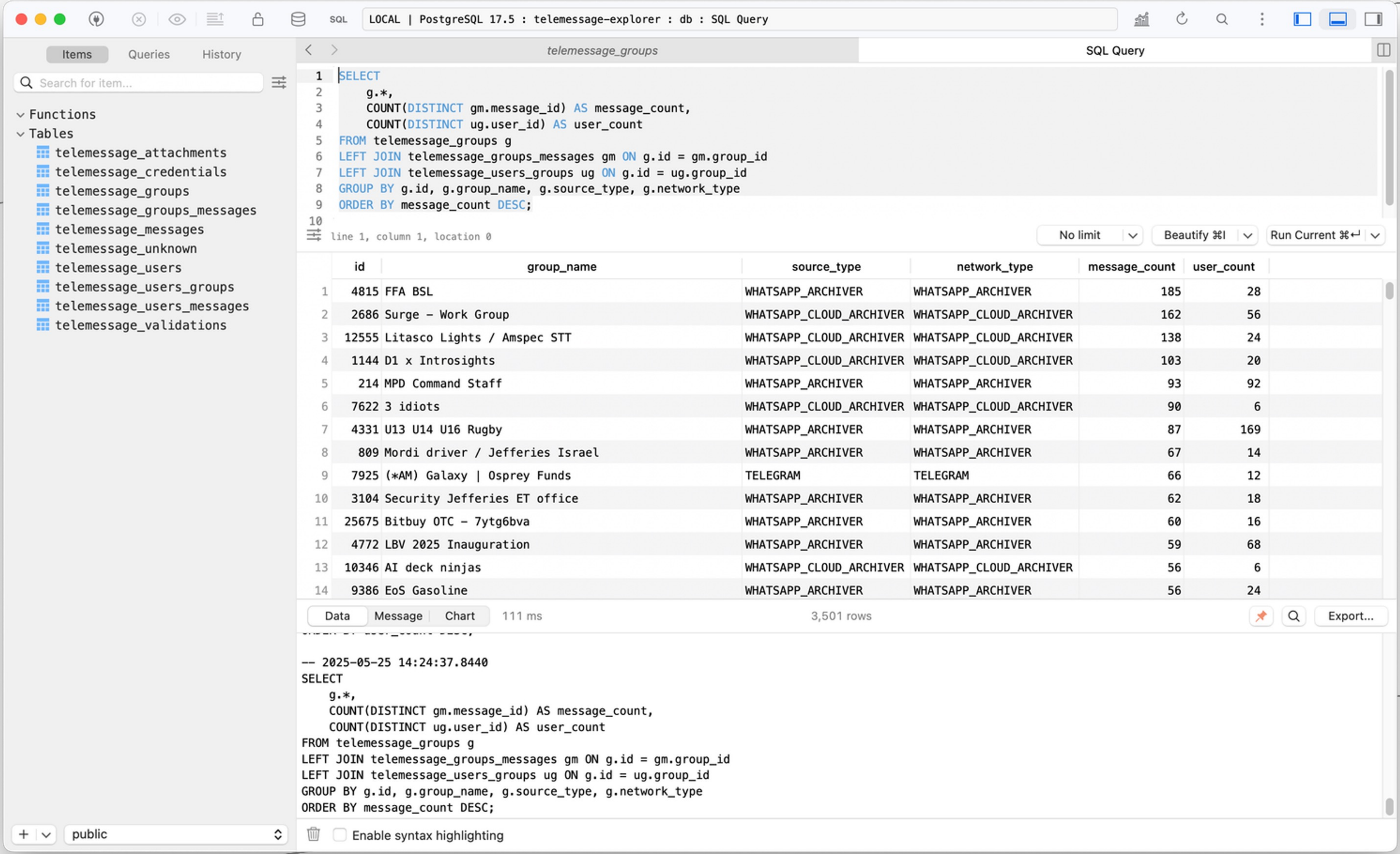
Chapter 7:
Drowning in Heap Dumps



```
{
    "validationData": {
        "reason": "OK",
        "validated": true
    },
    "enhancementData": {
        "data": [
            "1315[redacted]"
        ],
        "email": "[redacted]@cbp.dhs.gov",
        "userName": "1315[redacted]",
        "shortCodes": [],
        "subUserIds": [],
        "activeIdentityProviderWithParams": {
            "activeIdentityProvider": "NONE",
            "identityProviderParams": {}
        }
    }
}
```

email address

phone number

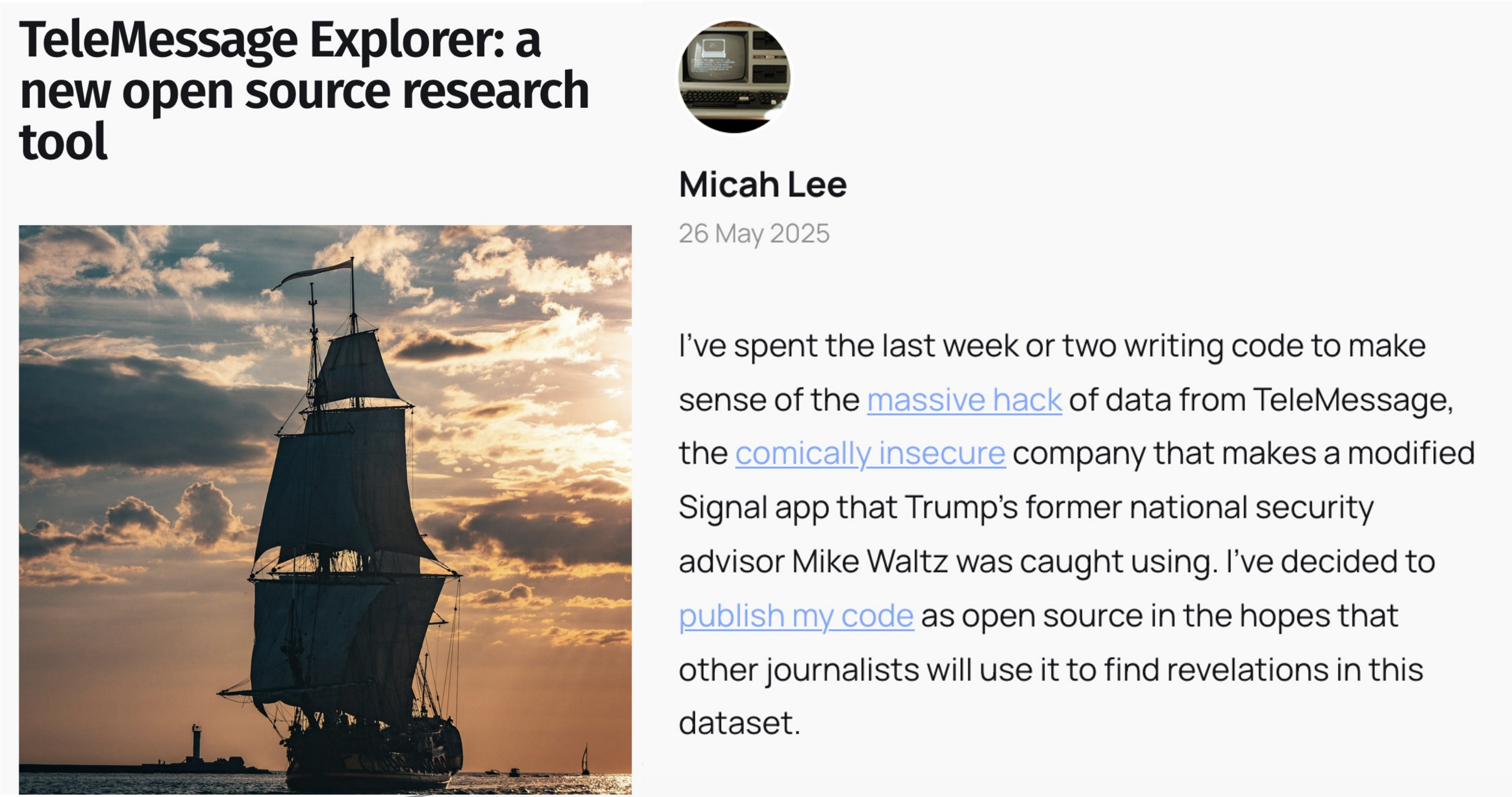


```sql
SELECT
    g.*,
    COUNT(DISTINCT gm.message_id) AS message_count,
    COUNT(DISTINCT ug.user_id) AS user_count
FROM telemessage_groups g
LEFT JOIN telemessage_groups_messages gm ON g.id = gm.group_id
LEFT JOIN telemessage_users_groups ug ON g.id = ug.group_id
GROUP BY g.id, g.group_name, g.source_type, g.network_type
ORDER BY message_count DESC;
```

	id	group_name	source_type	network_type	message_count	user_count
1	4815	FFA BSL	WHATSAPP_ARCHIVER	WHATSAPP_ARCHIVER	185	28
2	2686	Surge – Work Group	WHATSAPP_CLOUD_ARCHIVER	WHATSAPP_CLOUD_ARCHIVER	162	56
3	12555	Litasco Lights / Amspec STT	WHATSAPP_CLOUD_ARCHIVER	WHATSAPP_CLOUD_ARCHIVER	138	24
4	1144	D1 x Introsights	WHATSAPP_CLOUD_ARCHIVER	WHATSAPP_CLOUD_ARCHIVER	103	20
5	214	MPD Command Staff	WHATSAPP_ARCHIVER	WHATSAPP_ARCHIVER	93	92
6	7622	3 idiots	WHATSAPP_CLOUD_ARCHIVER	WHATSAPP_CLOUD_ARCHIVER	90	6
7	4331	U13 U14 U16 Rugby	WHATSAPP_ARCHIVER	WHATSAPP_ARCHIVER	87	169
8	809	Mordi driver / Jefferies Israel	WHATSAPP_ARCHIVER	WHATSAPP_ARCHIVER	67	14
9	7925	(*AM) Galaxy | Osprey Funds	TELEGRAM	TELEGRAM	66	12
10	3104	Security Jefferies ET office	WHATSAPP_ARCHIVER	WHATSAPP_ARCHIVER	62	18
11	25675	Bitbuy OTC – 7ytg6bva	WHATSAPP_ARCHIVER	WHATSAPP_ARCHIVER	60	16
12	4772	LBV 2025 Inauguration	WHATSAPP_ARCHIVER	WHATSAPP_ARCHIVER	59	68
13	10346	AI deck ninjas	WHATSAPP_CLOUD_ARCHIVER	WHATSAPP_CLOUD_ARCHIVER	56	6
14	9386	EoS Gasoline	WHATSAPP_ARCHIVER	WHATSAPP_ARCHIVER	56	24

```
-- 2025-05-25 14:24:37.8440
SELECT
    g.*,
    COUNT(DISTINCT gm.message_id) AS message_count,
    COUNT(DISTINCT ug.user_id) AS user_count
FROM telemessage_groups g
LEFT JOIN telemessage_groups_messages gm ON g.id = gm.group_id
LEFT JOIN telemessage_users_groups ug ON g.id = ug.group_id
GROUP BY g.id, g.group_name, g.source_type, g.network_type
ORDER BY message_count DESC;
```

Chapter 8: TeleMessage Explorer



TeleMessage Explorer: a new open source research tool

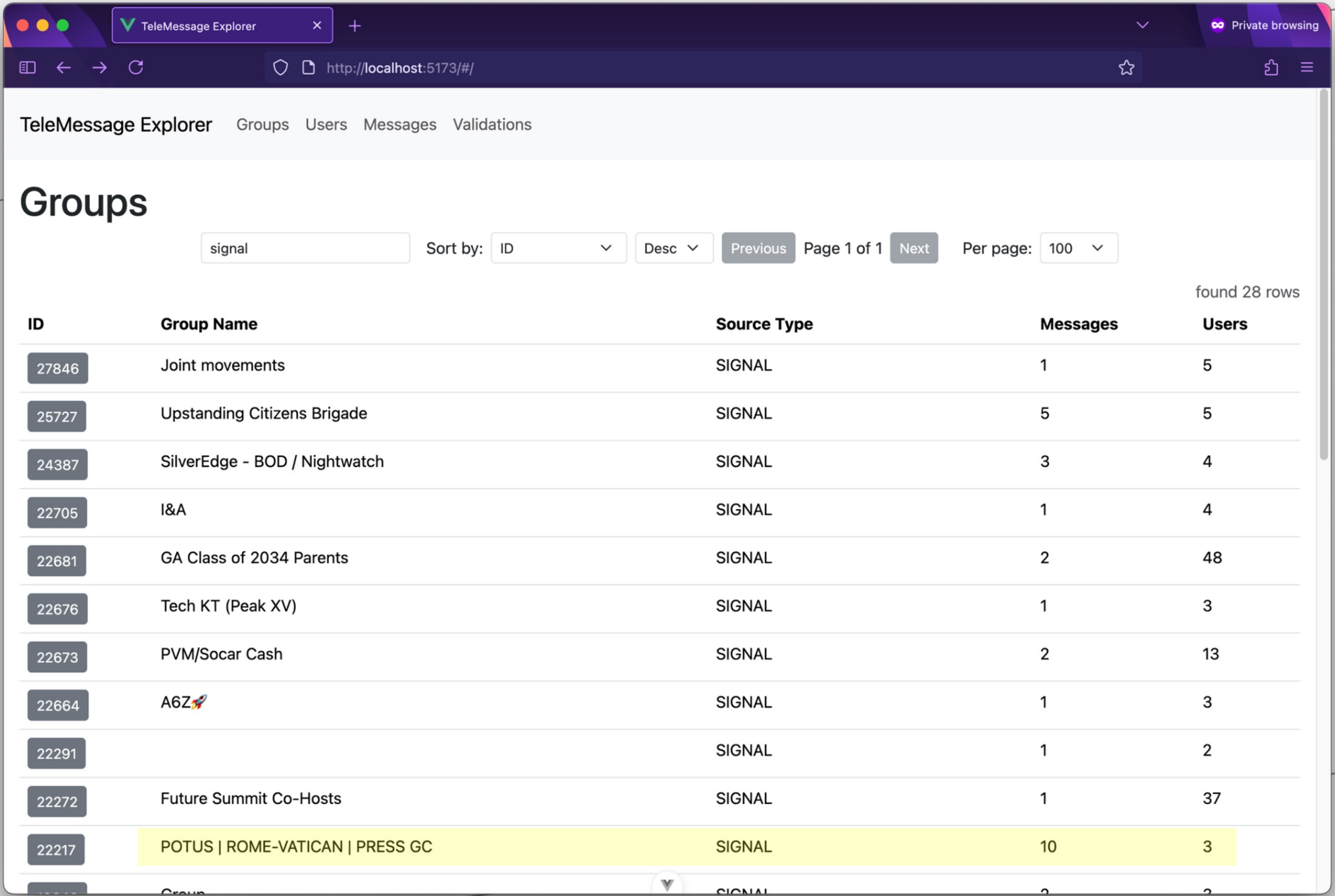
Micah Lee

26 May 2025

I’ve spent the last week or two writing code to make sense of the massive hack of data from TeleMessage, the comically insecure company that makes a modified Signal app that Trump’s former national security advisor Mike Waltz was caught using. I’ve decided to publish my code as open source in the hopes that other journalists will use it to find revelations in this dataset.

May 26, 2025

https://micahflee.com/telemessage-explorer/

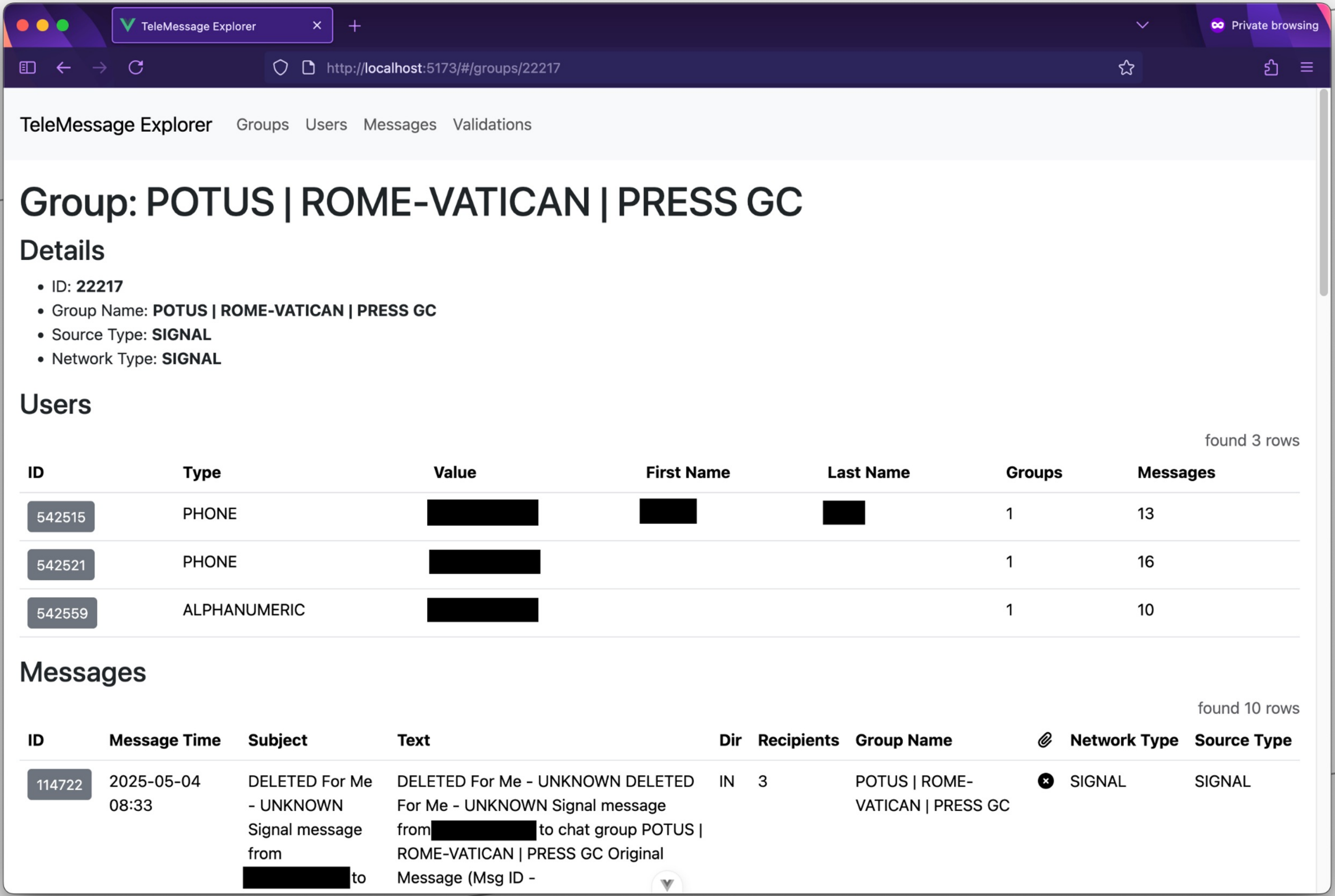


Groups

signal | Sort by: ID | Desc | Previous | Page 1 of 1 | Next | Per page: 100

found 28 rows

ID	Group Name	Source Type	Messages	Users
27846	Joint movements	SIGNAL	1	5
25727	Upstanding Citizens Brigade	SIGNAL	5	5
24387	SilverEdge - BOD / Nightwatch	SIGNAL	3	4
22705	I&A	SIGNAL	1	4
22681	GA Class of 2034 Parents	SIGNAL	2	48
22676	Tech KT (Peak XV)	SIGNAL	1	3
22673	PVM/Socar Cash	SIGNAL	2	13
22664	A6Z🚀	SIGNAL	1	3
22291		SIGNAL	1	2
22272	Future Summit Co-Hosts	SIGNAL	1	37
22217	POTUS | ROME-VATICAN | PRESS GC	SIGNAL	10	3



TeleMessage Explorer Groups Users Messages Validations

Group: POTUS | ROME-VATICAN | PRESS GC

Details

- ID: **22217**
- Group Name: **POTUS | ROME-VATICAN | PRESS GC**
- Source Type: **SIGNAL**
- Network Type: **SIGNAL**

Users

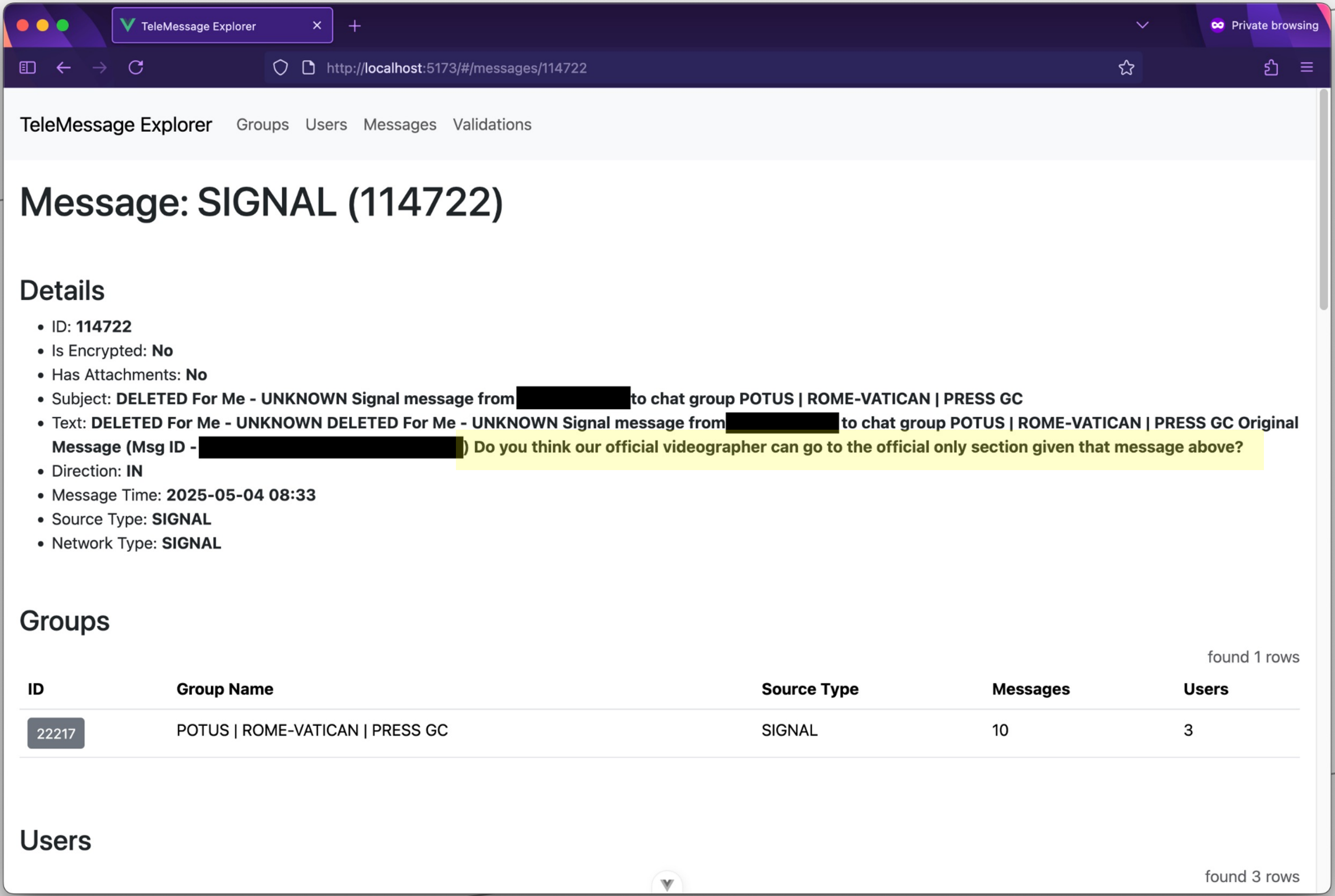
found 3 rows

ID	Type	Value	First Name	Last Name	Groups	Messages
542515	PHONE	[redacted]	[redacted]	[redacted]	1	13
542521	PHONE	[redacted]			1	16
542559	ALPHANUMERIC	[redacted]			1	10

Messages

found 10 rows

ID	Message Time	Subject	Text	Dir	Recipients	Group Name	📎	Network Type	Source Type
114722	2025-05-04 08:33	DELETED For Me - UNKNOWN Signal message from [redacted] to	DELETED For Me - UNKNOWN DELETED For Me - UNKNOWN Signal message from [redacted] to chat group POTUS | ROME-VATICAN | PRESS GC Original Message (Msg ID -	IN	3	POTUS | ROME-VATICAN | PRESS GC	⊗	SIGNAL	SIGNAL



TeleMessage Explorer Groups Users Messages Validations

Message: SIGNAL (114722)

Details

- ID: **114722**
- Is Encrypted: **No**
- Has Attachments: **No**
- Subject: **DELETED For Me - UNKNOWN Signal message from [redacted] to chat group POTUS | ROME-VATICAN | PRESS GC**
- Text: **DELETED For Me - UNKNOWN DELETED For Me - UNKNOWN Signal message from [redacted] to chat group POTUS | ROME-VATICAN | PRESS GC Original Message (Msg ID - [redacted]) Do you think our official videographer can go to the official only section given that message above?**
- Direction: **IN**
- Message Time: **2025-05-04 08:33**
- Source Type: **SIGNAL**
- Network Type: **SIGNAL**

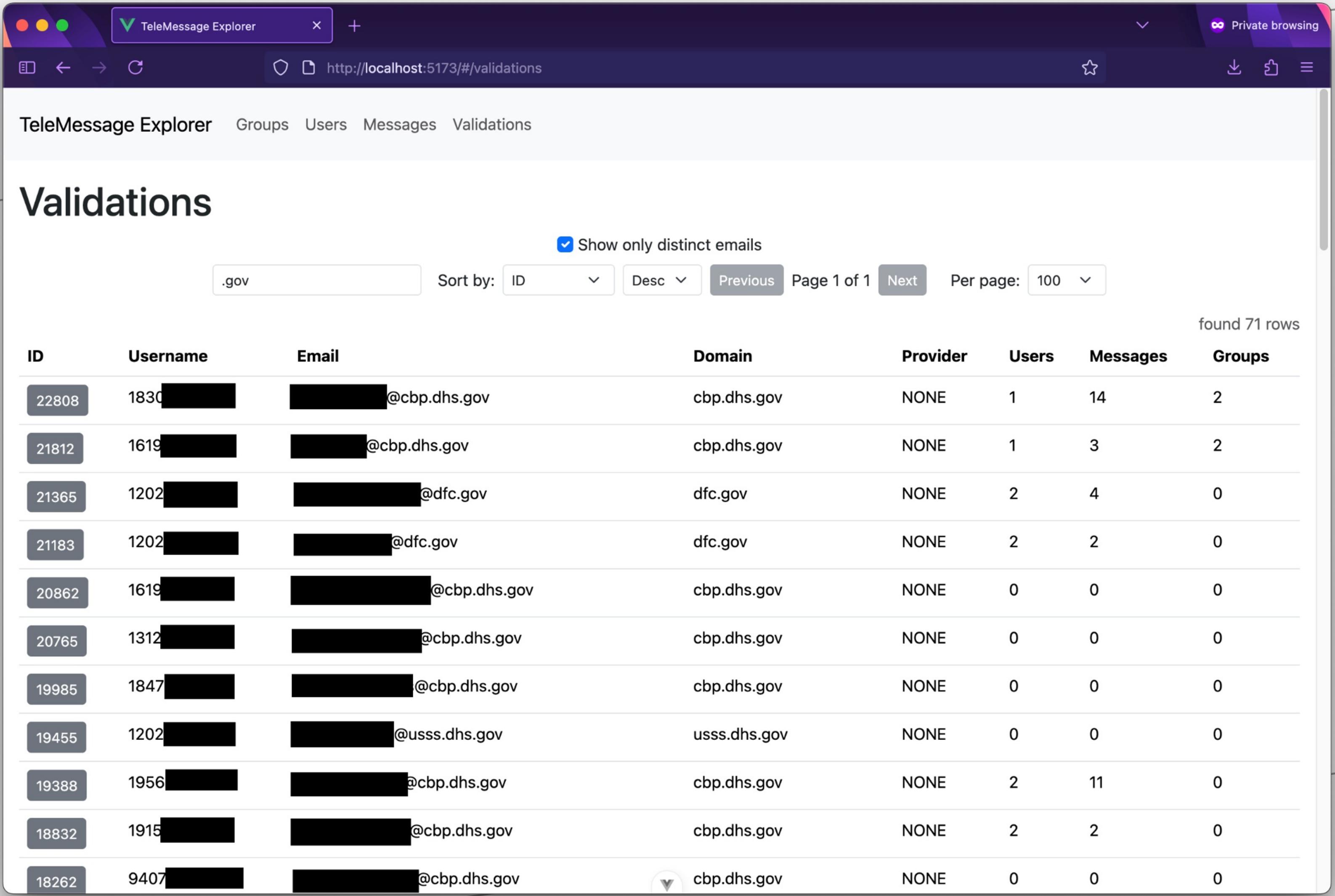
Groups

found 1 rows

ID	Group Name	Source Type	Messages	Users
22217	POTUS | ROME-VATICAN | PRESS GC	SIGNAL	10	3

Users

found 3 rows



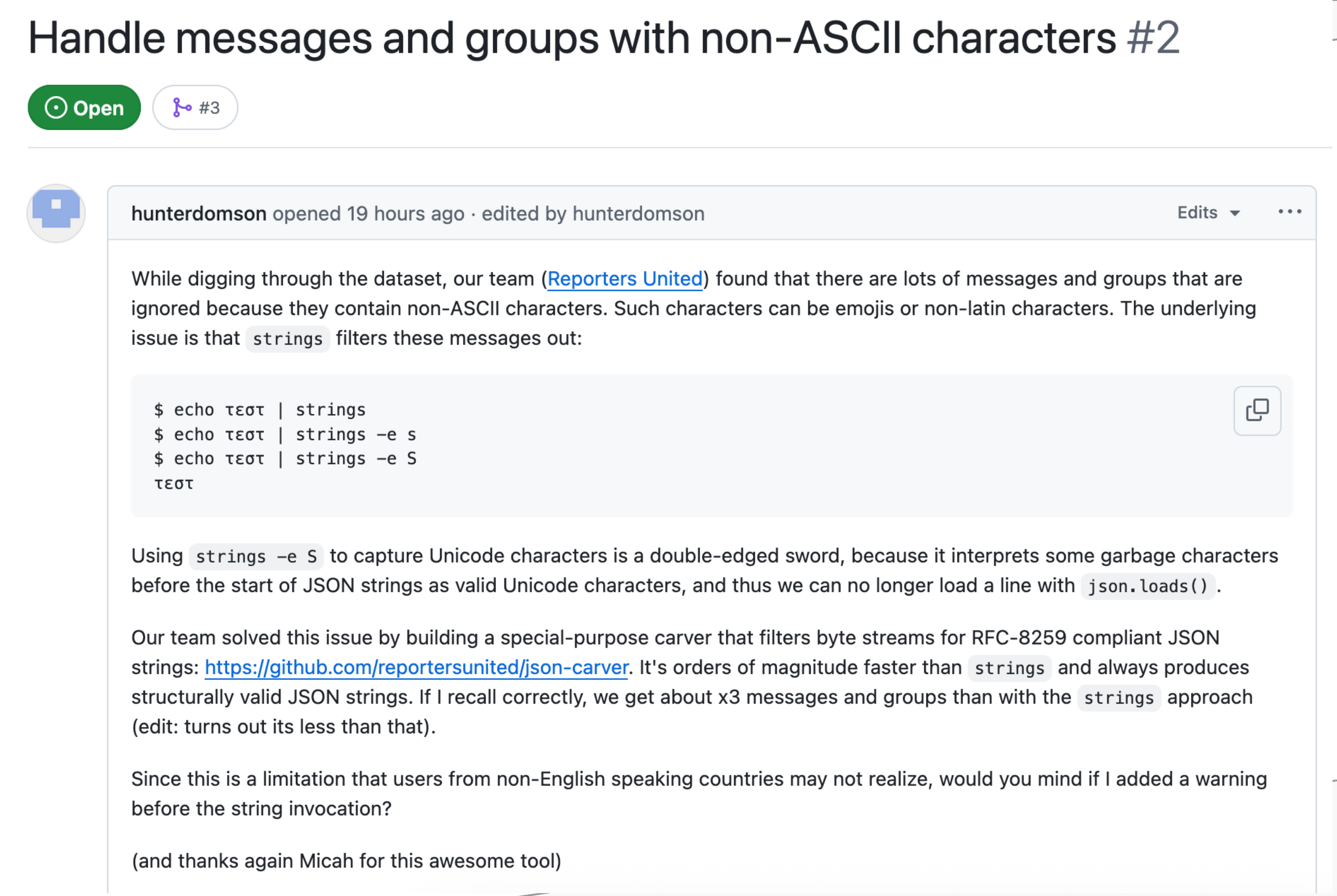
Validations

☑ Show only distinct emails

.gov Sort by: ID Desc Previous Page 1 of 1 Next Per page: 100

found 71 rows

ID	Username	Email	Domain	Provider	Users	Messages	Groups
22808	1830[redacted]	[redacted]@cbp.dhs.gov	cbp.dhs.gov	NONE	1	14	2
21812	1619[redacted]	[redacted]@cbp.dhs.gov	cbp.dhs.gov	NONE	1	3	2
21365	1202[redacted]	[redacted]@dfc.gov	dfc.gov	NONE	2	4	0
21183	1202[redacted]	[redacted]@dfc.gov	dfc.gov	NONE	2	2	0
20862	1619[redacted]	[redacted]@cbp.dhs.gov	cbp.dhs.gov	NONE	0	0	0
20765	1312[redacted]	[redacted]@cbp.dhs.gov	cbp.dhs.gov	NONE	0	0	0
19985	1847[redacted]	[redacted]@cbp.dhs.gov	cbp.dhs.gov	NONE	0	0	0
19455	1202[redacted]	[redacted]@usss.dhs.gov	usss.dhs.gov	NONE	0	0	0
19388	1956[redacted]	[redacted]@cbp.dhs.gov	cbp.dhs.gov	NONE	2	11	0
18832	1915[redacted]	[redacted]@cbp.dhs.gov	cbp.dhs.gov	NONE	2	2	0
18262	9407[redacted]	[redacted]@cbp.dhs.gov	cbp.dhs.gov	NONE	0	0	0



Handle messages and groups with non-ASCII characters #2

hunterdomson opened 19 hours ago · edited by hunterdomson

While digging through the dataset, our team (Reporters United) found that there are lots of messages and groups that are ignored because they contain non-ASCII characters. Such characters can be emojis or non-latin characters. The underlying issue is that `strings` filters these messages out:

```
$ echo τεστ | strings
$ echo τεστ | strings -e s
$ echo τεστ | strings -e S
τεστ
```

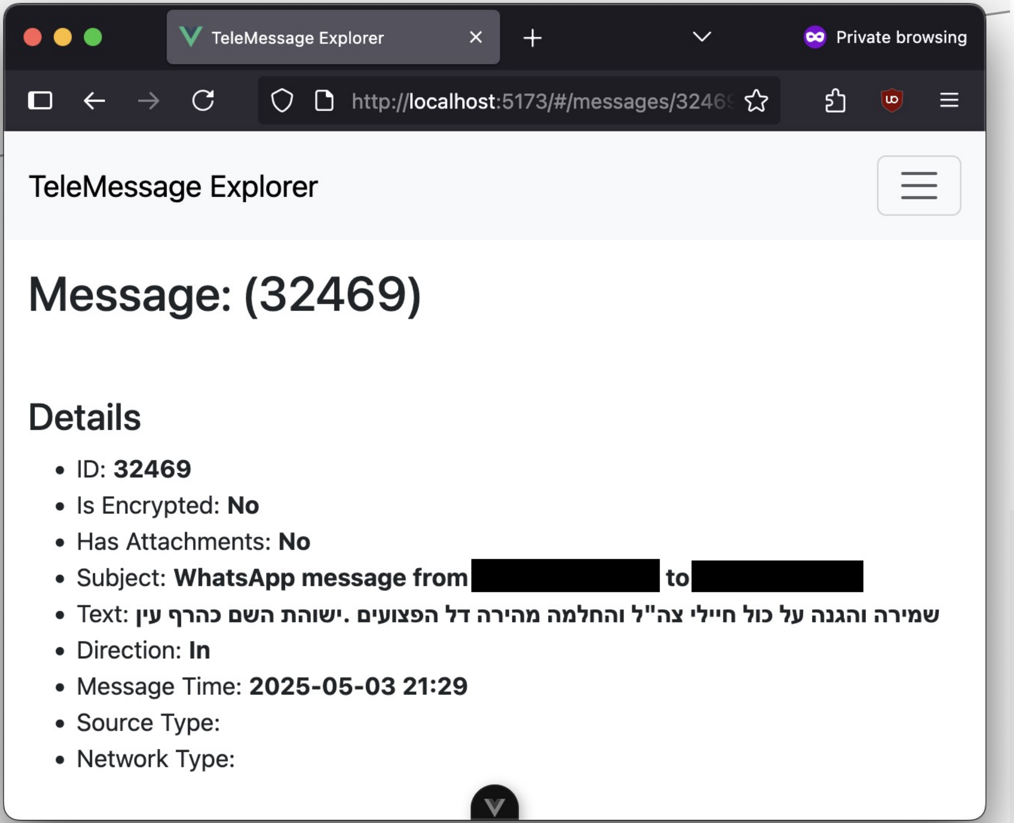
Using `strings -e S` to capture Unicode characters is a double-edged sword, because it interprets some garbage characters before the start of JSON strings as valid Unicode characters, and thus we can no longer load a line with `json.loads()`.

Our team solved this issue by building a special-purpose carver that filters byte streams for RFC-8259 compliant JSON strings: https://github.com/reportersunited/json-carver. It's orders of magnitude faster than `strings` and always produces structurally valid JSON strings. If I recall correctly, we get about x3 messages and groups than with the `strings` approach (edit: turns out its less than that).

Since this is a limitation that users from non-English speaking countries may not realize, would you mind if I added a warning before the string invocation?

(and thanks again Micah for this awesome tool)

https://github.com/micahflee/telemessage-explorer/issues/2

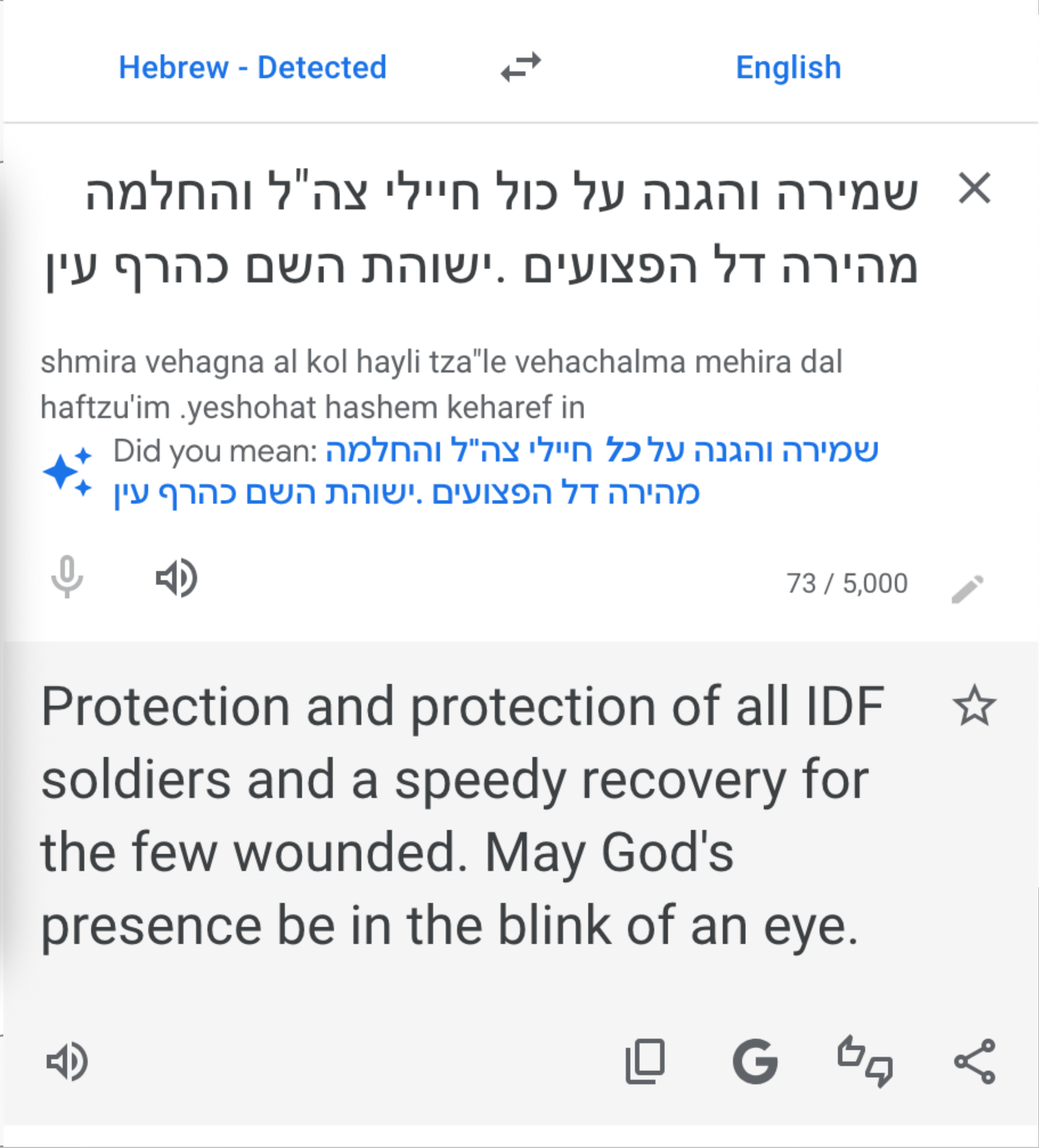


TeleMessage Explorer

Message: (32469)

Details

- ID: **32469**
- Is Encrypted: **No**
- Has Attachments: **No**
- Subject: **WhatsApp message from [redacted] to [redacted]**
- Text: **שמירה והגנה על כול חיילי צה"ל והחלמה מהירה דל הפצועים .ישוהת השם כהרף עין**
- Direction: **In**
- Message Time: **2025-05-03 21:29**
- Source Type:
- Network Type:



שמירה והגנה על כול חיילי צה"ל והחלמה מהירה דל הפצועים .ישוהת השם כהרף עין

shmira vehagna al kol hayli tza"le vehachalma mehira dal haftzu'im .yeshohat hashem keharef in

Did you mean: שמירה והגנה על כל חיילי צה"ל והחלמה מהירה דל הפצועים .ישוהת השם כהרף עין

Protection and protection of all IDF soldiers and a speedy recovery for the few wounded. May God's presence be in the blink of an eye.

Chapter 8: TeleMessage Explorer

“

WhatsApp message on May 4, 2025
from **Sam Altman**, CEO of OpenAI
to **Brad Gerstner**, CEO of Altimeter Capital

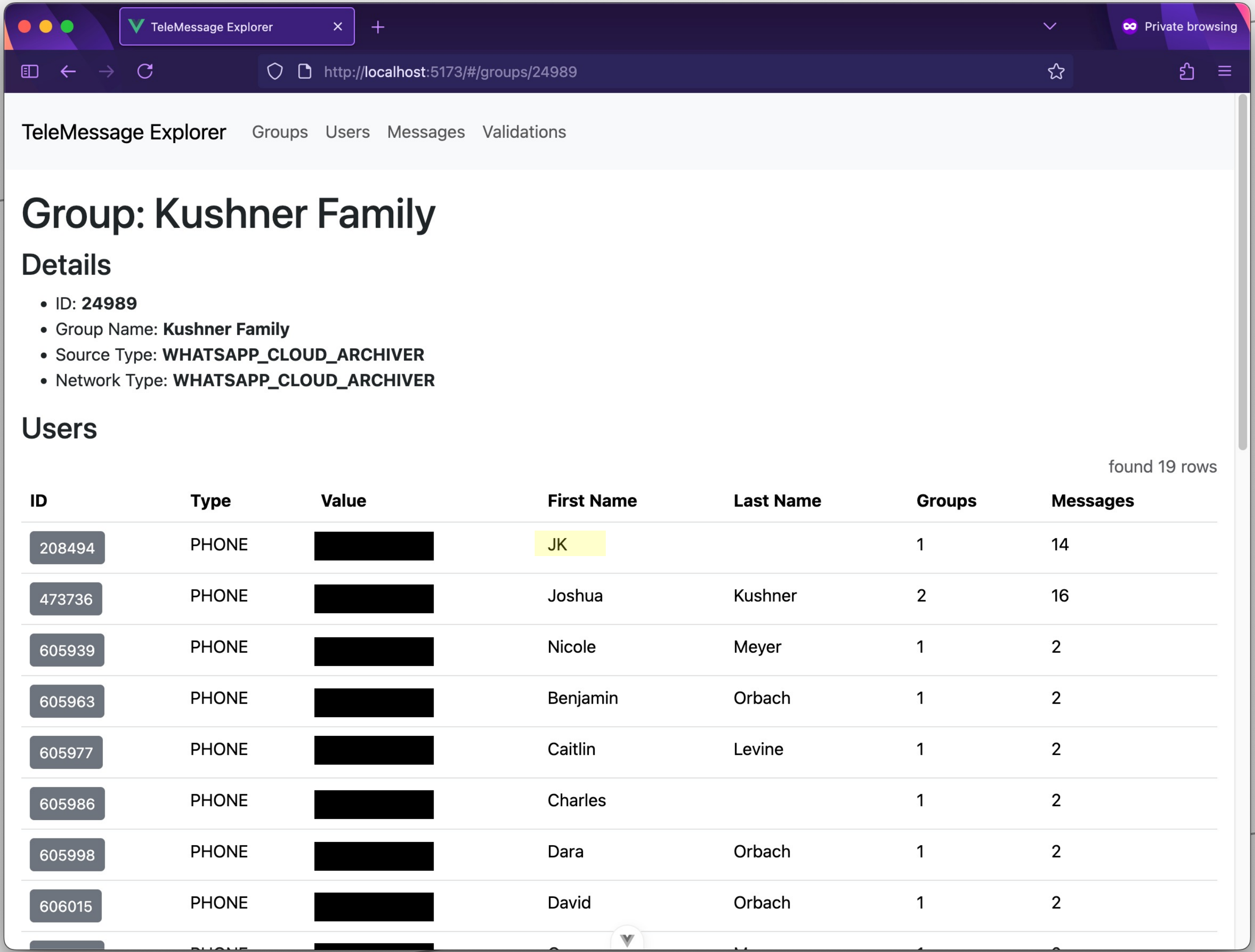
great! what are you hearing specifically in DC about it?

”

Chapter 8: TeleMessage Explorer

WhatsApp message on May 4, 2025
from **Sriram Krishnan**, Trump’s Senior White House Policy Advisor on AI
to **Jared Kushner**, husband of Donald Trump’s daughter Ivanka

> “would love to catch up on all things UAE. working with David a lot on what we are doing with UAE”



Group: Kushner Family

Details

- ID: **24989**
- Group Name: **Kushner Family**
- Source Type: **WHATSAPP_CLOUD_ARCHIVER**
- Network Type: **WHATSAPP_CLOUD_ARCHIVER**

Users

found 19 rows

ID	Type	Value	First Name	Last Name	Groups	Messages
208494	PHONE	[redacted]	JK		1	14
473736	PHONE	[redacted]	Joshua	Kushner	2	16
605939	PHONE	[redacted]	Nicole	Meyer	1	2
605963	PHONE	[redacted]	Benjamin	Orbach	1	2
605977	PHONE	[redacted]	Caitlin	Levine	1	2
605986	PHONE	[redacted]	Charles		1	2
605998	PHONE	[redacted]	Dara	Orbach	1	2
606015	PHONE	[redacted]	David	Orbach	1	2

Chapter 9: Clean OPSEC

👊🇺🇸🔥

I’m Micah Lee.

https://micahflee.com

micah@micahflee.com

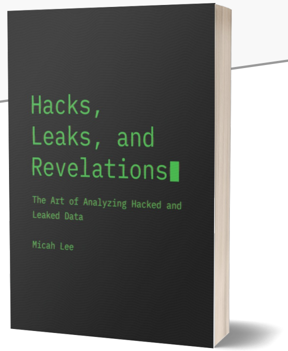
micah.01

@micahflee.com

@micahflee@infosec.exchange

THE END

… to be continued?



Hacks, Leaks, and Revelations: The Art of Analyzing Hacked and Leaked Data
I’m doing a book signing with No Starch Press on Sunday in the vendor area!