The Signal Clone the Trump Admin Uses Was Hacked

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

Photo by Andy Feliciotti / Unsplash

Micah Lee

04 May 2025

> 💡 I wrote this article with Joseph Cox. You can read the original at 404 Media. Following 404 Media's lead, this post is behind a freewall. You can read the full post for free by subscribing.

A hacker has gained access to the Signal message archiving tool which Mike Waltz accidentally revealed to the world.

A hacker has breached and stolen customer data from TeleMessage, an obscure Israeli company that sells modified versions of Signal and other messaging apps to the U.S. government to archive messages, 404 Media has learned. The data stolen by the hacker contains the contents of some direct messages and group chats sent using its Signal clone, as well as modified versions of WhatsApp, Telegram, and WeChat. TeleMessage was recently the center of a wave of media coverage after Mike Waltz accidentally revealed he used the tool in a cabinet meeting with President Trump.

The hack shows that an app gathering messages of the highest ranking officials in the government—Waltz's chats on the app include recipients that appear to be Marco Rubio, Tulsi Gabbard, and JD Vance—contained serious vulnerabilities that allowed a hacker to trivially access the archived chats of some people who used the same tool. The hacker has not obtained the messages of cabinet members, Waltz, and people he spoke to, but the hack shows that the archived chat logs are not end-to-end encrypted between the modified version of the messaging app and

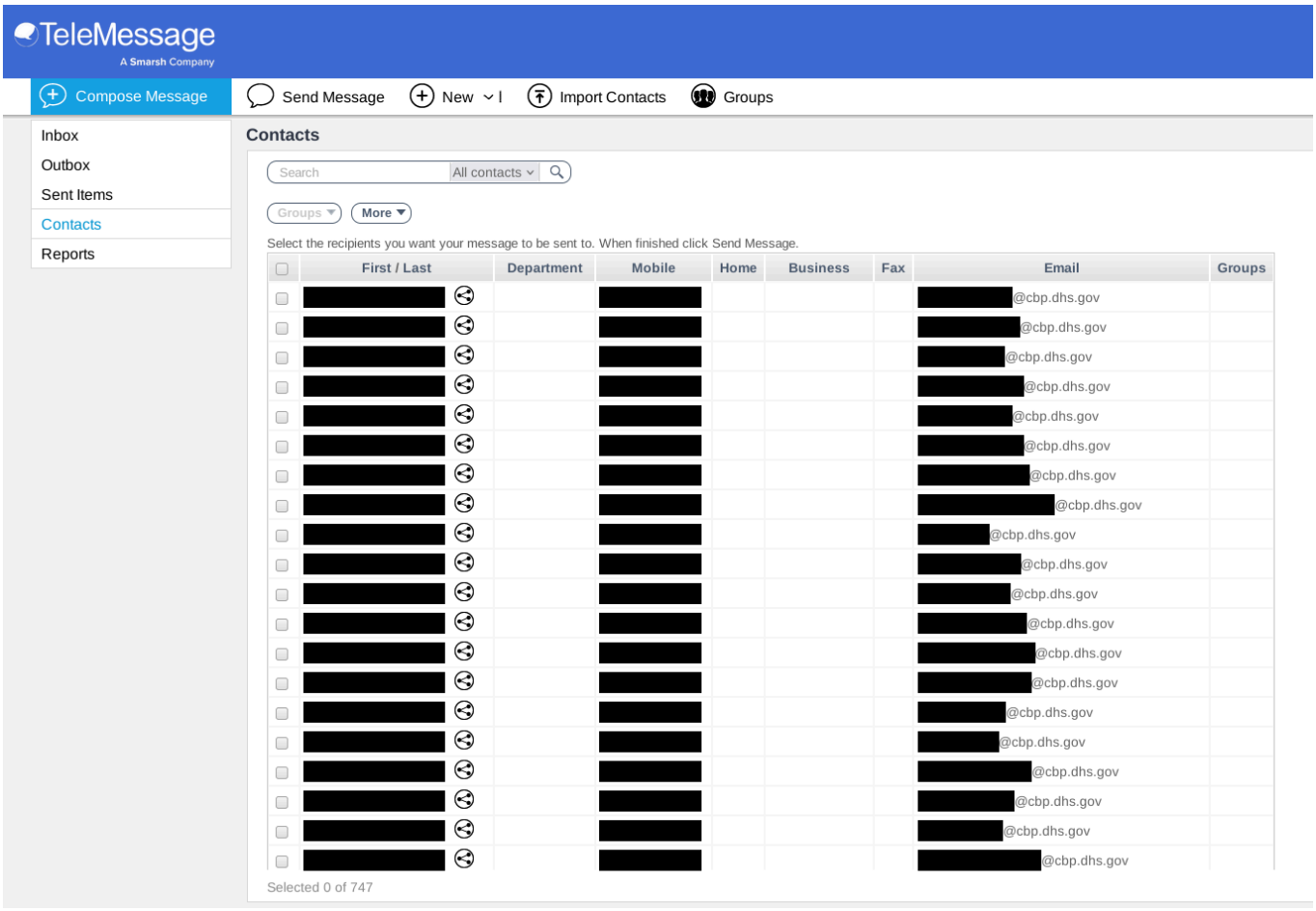
the ultimate archive destination controlled by the TeleMessage customer.

Data related to Customs and Border Protection (CBP), the cryptocurrency giant Coinbase, and other financial institutions are included in the hacked material, according to screenshots of messages and backend systems obtained by 404 Media.

The breach is hugely significant not just for those individual customers, but also for the U.S. government more widely. On Thursday, 404 Media was first to report that at the time U.S. National Security Advisor Waltz accidentally revealed he was using TeleMessage's modified version of Signal during the cabinet meeting. The use of that tool raised questions about what classification of information was being discussed across the app and how that data was being secured, and came after revelations top U.S. officials were using Signal to discuss active combat operations.

The hacker did not access all messages stored or collected by TeleMessage, but could have likely accessed more data if they decided to, underscoring the extreme risk posed by taking ordinarily secure end-to-end encrypted messaging apps such as Signal and adding an extra archiving feature to them.

"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.



Redacted screenshot from the hacker showing users with Customs and Border Protection email addresses

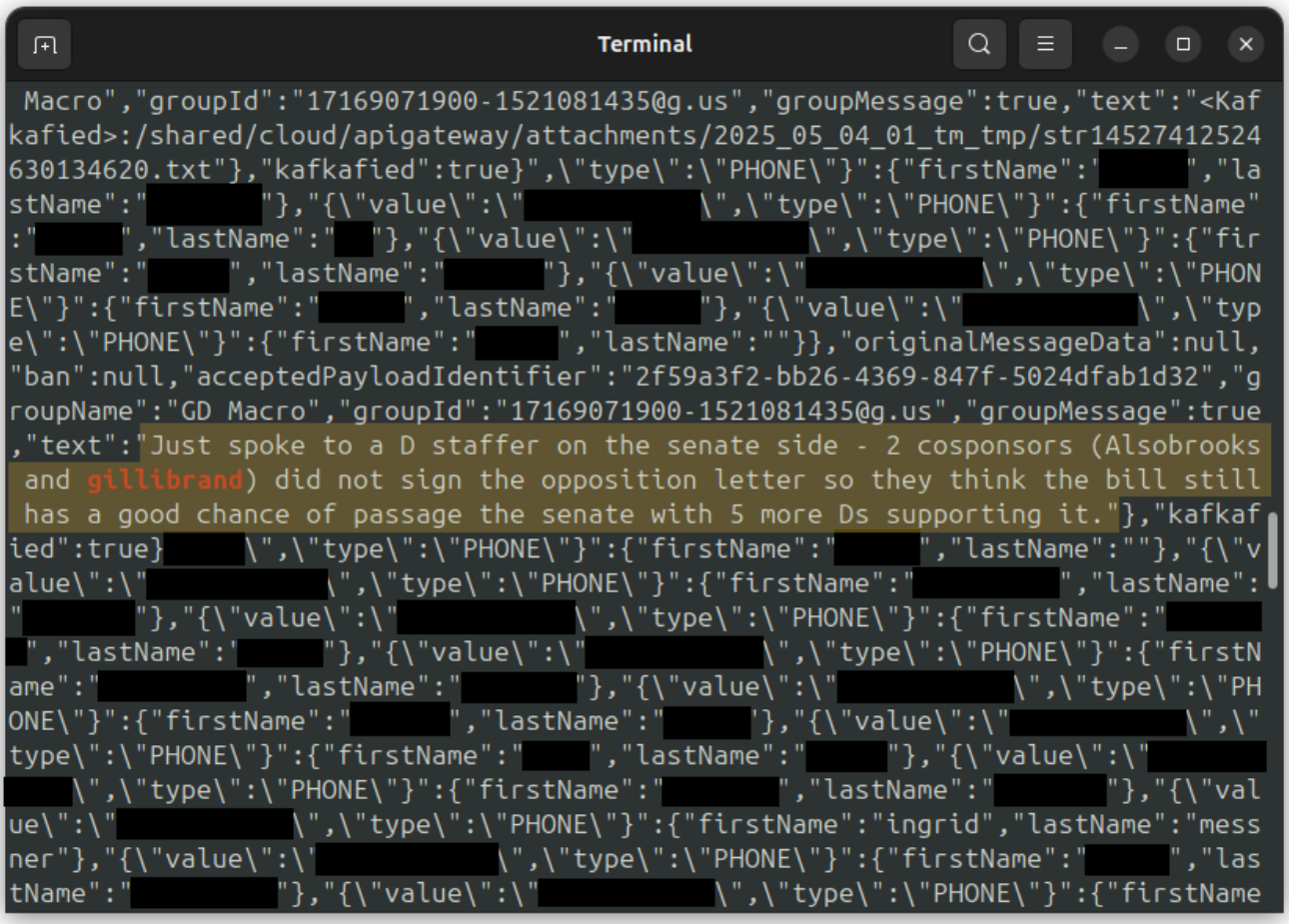
The data includes apparent message contents; the names and contact information for government officials; usernames and passwords for TeleMessage's backend panel; and indications of what agencies and companies might be TeleMessage customers. The data is not representative of all of TeleMessage's customers or the sorts of messages it covers; instead, it is snapshots of data passing through TeleMessage's servers at a point in time. The hacker was able to login to the TeleMessage backend panel using the usernames and passwords found in these snapshots.

A message sent to a group chat called "Upstanding Citizens Brigade" included in the hacked data says its "source type" is "Signal," indicating

it came from TeleMessage's modified version of the messaging app. The message itself was a link to this tweet posted on Sunday which is a clip of an NBC Meet the Press interview with President Trump about his memecoin. The hacked data includes phone numbers that were part of the group chat.

One hacked message was sent to a group chat apparently associated with the crypto firm Galaxy Digital. One message said, "need 7 dems to get to 60.. would be very close" to the "GD Macro" group. Another message said, "Just spoke to a D staffer on the 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 supporting it."

This means a hacker was able to steal what appears to be active, timely discussion about the efforts behind passing a hugely important and controversial cryptocurrency bill; Saturday, Democratic lawmakers published a letter explaining they would oppose it. Bill cosponsors Maryland Sen. Angela Alsobrooks and New York Sen. Kirsten Gillibrand did not sign that letter.



The data includes real-time discussion about lobbying for a controversial cryptocurrency bill

One screenshot of the hacker's access to a TeleMessage panel lists the names, phone numbers, and email addresses of CBP officials. The screenshot says "select 0 of 747," indicating that there may be that many CBP officials included in the data. A similar screenshot shows the contact information of current and former Coinbase employees.

Another screenshot obtained by 404 Media mentions Scotiabank. Financial institutions might turn to a tool like TeleMessage to comply with regulations around keeping copies of business communications. Governments have legal requirements to preserve messages in a similar way.

Another screenshot indicates that the Intelligence Branch of the Washington D.C. Metropolitan Police may be using the tool.

The hacker was able to access data that the app captured intermittently for debugging purposes, and would not have been able to capture every single message or piece of data that passes through TeleMessage's service. However, the sample data they captured did contain fragments of live, unencrypted data passing through TeleMessage's production server on their way to getting archived.

404 Media verified the hacked data in various ways. First, 404 Media phoned some of the numbers listed as belonging to CBP officials. In one case, a person who answered said their name was the same as the one included in the hacked data, then confirmed their affiliation with CBP when asked. The voicemail message for another number included the name of an alleged CBP official included in the data.

404 Media ran several phone numbers that appeared to be associated with employees at crypto firms Coinbase and Galaxy through a search tool called OSINT Industries, which confirmed that these phone numbers belonged to people who worked for these companies.

The server that the hacker compromised is hosted on Amazon AWS's cloud infrastructure in Northern Virginia. By reviewing the source code of TeleMessage's modified Signal app for Android, 404 Media confirmed that the app sends message data to this endpoint. 404 Media also made an HTTP request to this server to confirm that it is online.

TeleMessage came to the fore after a Reuters photographer took a photo in which Waltz was using his mobile phone. Zooming in on that

photo revealed he was using a modified version of Signal made by TeleMessage. The photograph came around a month after *The Atlantic* reported that top U.S. officials were using Signal to message one another about military operations. As part of that, Waltz accidentally added the editor-in-chief of the publication to the Signal group chat.

TeleMessage offers governments and companies a way to archive messages from end-to-end encrypted messaging apps such as Signal and WhatsApp. TeleMessage does this by making modified versions of those apps that send copies of messages to a remote server. A video from TeleMessage posted to YouTube claims that its 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.

It is not true that an archiving solution properly preserves the security offered by an end-to-end encrypted messaging app such as Signal. Ordinarily, only someone sending a Signal message and their intended recipient will be able to read the contents of the message. TeleMessage essentially adds a third party to that conversation by sending copies of those messages somewhere else for storage. If not stored securely, those copies could in turn be susceptible to monitoring or falling into the wrong hands.

That theoretical risk has now become very real.

A Signal spokesperson previously told 404 Media in email "We cannot guarantee the privacy or security properties of unofficial versions of

Signal."

White House deputy press secretary Anna Kelly previously told NBC News in an email: "As we have said many times, Signal is an approved app for government use and is loaded on government phones."

The hacker told 404 Media that they targeted TeleMessage because they were "just curious how secure it was." They did not want to disclose the issue to the company directly because they believed the company might "try their best to cover it up."

"If I could have found this in less than 30 minutes then anybody else could too. And who knows how long it's been vulnerable?" the hacker said.

404 Media is not explaining in detail how the hacker managed to obtain this data in case others may try to exploit the same vulnerability.

According to public procurement records, TeleMessage has contracts with a range of U.S. government agencies, including the State Department and Centers for Disease Control and Prevention.

Guy Levit, CEO of TeleMessage, directed a request for comment to a press representative of Smarsh, TeleMessage's parent company. That representative did not immediately respond to an email or voicemail.

Recently, after the wave of media coverage about Waltz's use of the tool, TeleMessage wiped its website. Before then it contained details on the services it offers, what its apps were capable of, and in some cases direct downloads for the archiving apps themselves.

A Coinbase spokesperson told 404 Media in an email “We are aware of reports that a third party communications tool widely used across the tech, banking, and other industries for archival and trade surveillance purposes has been breached. We are closely following these reports and assessing their impact on Coinbase. At this time, there is no evidence any sensitive Coinbase customer information was accessed or that any customer accounts are at risk, since Coinbase does not use this tool to share passwords, seed phrases, or other data needed to access accounts.”

Neither CBP, Coinbase, Scotiabank, Galaxy Digital, nor Washington D.C. Metropolitan Police responded to a request for comment.

Update: this piece has been updated to include a statement from Coinbase.

1 comment

PJ

Join the discussion

Add comment

H

Helaman · Yesterday

It is ridiculous how so many US government agencies started to use TeleMessage products without vetting them first (e.g. review of 3rd party security audits or perhaps a security audit directly by the NSA's or DoD's respective department). :o But of course it all fits perfectly with the government style of the current administration.

0 Reply

← Previous

Subscribe