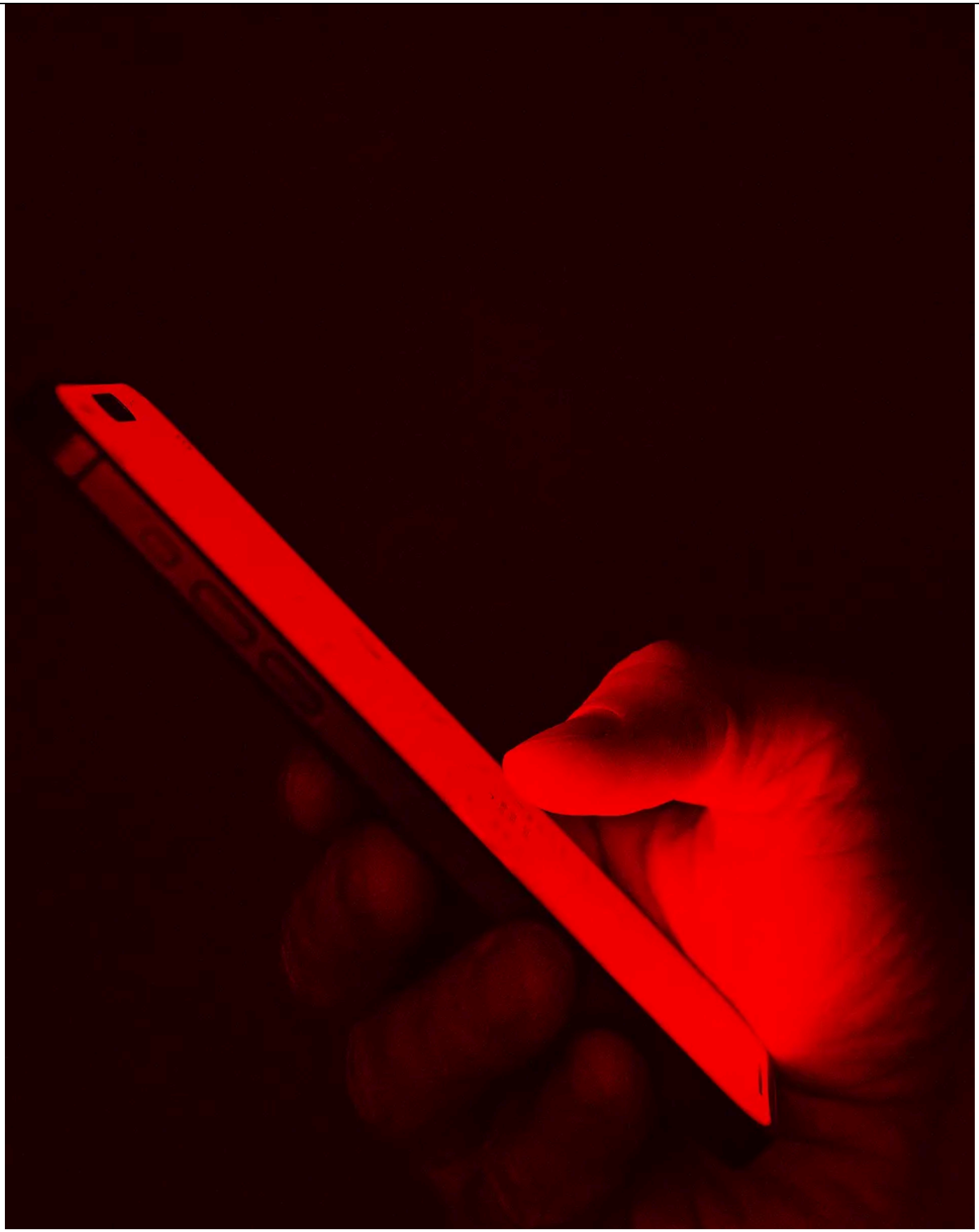
MICAH LEE SECURITY MAY 18, 2025 7:00 AM

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.



PHOTOGRAPH: GETTY IMAGES

SAVE THIS STORY

Listen to this story

00:00
1x
08:07

DURING A RECENT cabinet meeting, President Donald Trump's then national security adviser, Mike Waltz, must have been bored. Apparently unaware of the photographer behind him, he was caught clandestinely checking his Signal messages under the table.

Only he wasn't using the official Signal app, which is widely considered to be the gold standard of encrypted messaging apps. He was actually using a clone of Signal called TeleMessage Signal, or TM SGNL. This app, made by TeleMessage (which was recently acquired by Smarsh), works in almost exactly the same way as Signal, except that it also archives copies of all the messages passing through it, shattering all of its security guarantees.

Two days after the photo of Waltz was published, an anonymous source told me that they had hacked TeleMessage. "I would say the whole process took about 15 to 20 minutes," the hacker said, as Joseph Cox and I reported in 404 Media. "It wasn't much effort at all." Representatives from TeleMessage and Smarsh did not respond to a request for comment.

The exploit that the hacker used was incredibly simple. At the time, we chose not to publish any details about it because it would be so easy for others to replicate. Since then, TeleMessage has temporarily suspended all services, which is now why WIRED can share exactly how this hack took place without risking anyone's private data.

“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.

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**.

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.

The hacker said they “knew from past experience that heap dumps from web servers” will include the “bodies” of http requests, they said, “and this may include credentials of users logging in.” And for TM SGNL, they did. By downloading a heap dump and then searching for “password,” the hacker could see usernames and passwords of random users.
They tried logging into **secure.telemessage.com** using a pair of these credentials and discovered that they had just hacked a user with an email address associated

customer.

After spending a few more minutes digging through the heap dump, the hacker also discovered plaintext chat logs. “I can read Coinbase internal chats, this is incredible,” the hacker said. (Coinbase did not respond to WIRED's request for comment, but did tell 404 Media that “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.”)

At this point, the hacker says they had spent 15 to 20 minutes poking at TeleMessage’s servers, and had already compromised one of their federal government customers, along with one of the world’s biggest cryptocurrency exchanges.

As I discovered from analyzing TM SGNL’s source code, TeleMessage apps—like the one running on Mike Waltz’s phone—uploaded unencrypted messages to **archive.telemessage.com** (I call this the archive server), which then forwards the messages to the customer’s final destination. This contradicts TeleMessage’s public marketing material, where they claimed TM SNGL uses “end-to-end encryption from the mobile phone through to the corporate archive.”

The archive server is programmed in Java and is built using Spring Boot, an open source framework for creating Java applications. Spring Boot includes a set of features called Actuator that helps developers monitor and debug their applications. One of these features is the heap dump endpoint, which is the URL the hacker used to download heap dumps.

According to Spring Boot Actuator’s documentation: “Since Endpoints may contain sensitive information, careful consideration should be given about when to expose them.” In the case of TeleMessage’s archive server, the heap dumps contained usernames, passwords, unencrypted chat logs, encryption keys, and other sensitive information.

unencrypted Signal messages, too.

A 2024 post on the cloud security company Wiz's blog lists "Exposed HeapDump file" as the number one common misconfiguration in Spring Boot Actuator. "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)," the author wrote. "Despite this improvement, developers often disable these security measures for diagnostic purposes when deploying applications to test environments, and this seemingly small configuration change may remain unnoticed and thereby persist when an application is pushed to production, inadvertently allowing attackers to obtain unauthorized access to critical data."

In a 2020 post on Walmart's Global Tech Blog, another developer gave a similar warning. "Apart from /health and /info, all actuator endpoints are risky to open to end users because they can expose application dumps, logs, configuration data and controls," the author wrote. "The actuator endpoints have security implications and SHOULD NEVER EVER be exposed in production environment."

The hacker's quick exploit of TeleMessage indicates that the archive server was badly misconfigured. It was either running an eight-year-old version of Spring Boot, or someone had manually configured it to expose the heap dump endpoint to the public internet.

This is why it took a hacker about 20 minutes of prodding before it cracked open, with sensitive data spilling out.

Despite this critical vulnerability and other security issues with TeleMessage's products—most notably, that the Israeli firm that builds the products can access all its customer's chat logs in plaintext—someone in the Trump administration deployed it to Mike Waltz's phone while he was serving as national security adviser.

You Might Also Like ...

- **In your inbox:** Upgrade your life with WIRED-tested gear
- The definitive story of Tesla takedown
- **Big Story:** AI chatbots and the humans who love them
- Snake venom, urine, and a quest to live forever
- **Special Edition:** The new era of work travel

Micah Lee is a coder, a security researcher, and an independent journalist. He develops open source privacy and security tools with the Lockdown Systems collective. He's the former director of information security for The Intercept, and the author of *Hacks, Leaks, and Revelations: The Art of Analyzing Hacked and Leaked* ... Read More

CONTRIBUTOR

TOPICS HACKS CYBERSECURITY DONALD TRUMP SECURITY VULNERABILITIES COINBASE SIGNAL
