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

While Reuters could not verify the entire contents of the TeleMessage trove, the news agency was able to establish that the phone numbers in the leaked data were correctly attributed to their owners.

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 of leaked data provided by Distributed Denial of Secrets, a U.S. nonprofit whose stated mission is to archive hacked and leaked documents in the public interest. The trove included material from disaster responders, customs officials, several U.S. diplomatic staffers, at least one White House staffer and members of the Secret Service. The messages reviewed by Reuters covered a roughly day-long period of time ending on May 4, and many of them were fragmentary. Once little known outside government and finance circles, TeleMessage drew media attention after an April 30 Reuters photograph showed Waltz checking TeleMessage's version of the privacy-focused app Signal during a cabinet meeting.

While Reuters could not verify the entire contents of the TeleMessage trove, in more than half a dozen cases the news agency was able to establish that the phone numbers in the leaked data were correctly attributed to their owners. One of the intercepted texts' recipients – an applicant for aid from the Federal Emergency Management Agency – confirmed to Reuters that the leaked message was authentic; a financial services firm whose messages were similarly intercepted also confirmed their authenticity. Based on its limited review, Reuters uncovered nothing that seemed clearly sensitive and did not uncover chats by Waltz or other cabinet officials. Some chats did seem to bear on the travel plans of senior government officials. One Signal group, "POTUS | ROME-VATICAN | PRESS GC," appeared to pertain to the logistics of an event at the Vatican. Another appeared to discuss U.S. officials' trip to Jordan.

Reuters reached out to all the individuals it could identify seeking comment; some confirmed their identities but most didn't respond or referred questions to their respective agencies. Reuters could not ascertain how TeleMessage had been used by each agency. The service – which takes versions of popular apps and allows their messages to be archived in line with government rules – has been suspended since May 5, when it went offline "out of an abundance of caution." TeleMessage's owner, the Portland, Oregon-based digital communications firm Smarsh, did not respond to requests for comments about the leaked data.

The White House said in a statement that it was "aware of the cyber security incident at Smarsh" but didn't offer comment on its use of the platform. The State Department didn't respond to messages. The Secret Service said TeleMessage products had been used "by a small subset of Secret Service employees" and that it was reviewing the situation. FEMA said in an email that it had "no evidence" that its information had been compromised. It didn't respond when sent copies of internal FEMA messages. A CBP spokesperson repeated a past statement noting that it had disabled TeleMessage and was investigating the breach.

METADATA RISK Federal contracting data shows that State and DHS have had contracts with TeleMessage in recent years, as has the Centers for Disease Control. A CDC spokesperson told Reuters in an email Monday that the agency piloted the software in 2024 to assess its potential for records management requirements “but found it did not fit our needs.” The status of the other contracts wasn’t clear. A week after that hack, the U.S. cyber defense agency CISA recommended that users “discontinue use of the product” barring any mitigating instructions about how to use the app from Smarsh.

Jake Williams, a former National Security Agency cyber specialist, said that, even if the intercepted text messages were innocuous, the wealth of metadata – the who and when of the leaked conversations and chat groups – posed a counterintelligence risk.

“Even if you don’t have the content, that is a top-tier intelligence access,” said Williams, now vice president of research and development at cybersecurity firm Hunter Strategy. Waltz’s prior use of Signal created a public furor when he accidentally added a prominent journalist to a Signal chat where he and other Trump cabinet officials were discussing air raids on Yemen in real time. Soon after, Waltz was ousted from his job, although not from the administration: Trump said he was nominating Waltz to be the next U.S. ambassador to the United Nations.

The circumstances surrounding Waltz’s use of TeleMessage haven’t been publicly disclosed and neither he nor the White House has responded to questions about the matter.