cyberscoop

As White House puts pressure on leakers, DC startup sees business opportunity

Chris Bing

February 28, 2017

A hazardous political landscape in Washington — underlined by a White House desperate to plug leaks — has spurred the use of encrypted messaging apps by federal employees. For software developers, this nervousness and anxiety translates into a very real opportunity.

In light of media reports noting the growing use of WhatsApp, Confide and Signal among government workers, some companies are now working to provide other options. One of those alternative platforms, Cloakroom — an insiders-only anonymous messaging app already notorious on Capitol Hill — released an update Friday to offer a secure communication channel to members of the defense community, founder Ted Henderson told CyberScoop.

The updated Cloakroom, Henderson said, is better equipped than its competitors to evade surveillance and other interception capabilities held by the U.S. government because it is the only secure messaging platform specifically developed from the ground up for the federal sector.

Henderson coded the expansion by tapping into an open-source, USA.gov-authored API directory for federal agencies. He then layered that information with Google's Geocoding API to add geographical context for the user experience. That allows usage of "geofences" to validate identity, Henderson said, making it a unique entrant to the niche messaging application market.

"Federal workers from 474 agencies and subagencies can use Cloakroom to anonymously share tips and intel with their colleagues and chat one-on-one with encryption so extreme even the NSA won't be able to listen in," Henderson wrote last week in a blog post.

Henderson later clarified that his company is in no way condoning the dissemination of classified or otherwise secret information. The app is free for individuals to use, but it has at least one paid sponsor, the libertarian Cato Institute, which uses the app to share its podcasts and other content.

Signing up as a member on Cloakroom requires a .gov or .mil email address unless — and only if — an individual is physical located within the geographic vicinity of a federal building. To login using the latter option, smartphone location services must be enabled. When originally registering with an email address, a confirmation message is sent with a code back to the user who then validates the token via the app.

Cloakroom's user interface is organized into three different communication channels, including a general forum where anyone can post messages, invite-only forums that select users can access and secure, end-to-end encrypted chatrooms. These chatrooms are encrypted using an open-source, AES256-GCM encryption library provided by Virgil Security.

It remains unclear whether the U.S. intelligence community, or any other foreign intelligence service for that matter, has the capability to break AES 256 encryption. With that being said, there a number of other avenues an attacker will likely take to compromise a smartphone app.

In broad strokes, Henderson said that Cloakroom is essentially secure because the company stores very little information on users.

Aliases are commonly employed by members, an email registration address is not mandatory for login purposes and the forums themselves are not archived. Content can be easily removed by users — for example, deletion of an account includes wiping all of the posts written by that handle.

Data storage controls have been and continue be a central aspect of the app's backend infrastructure, which was inherently designed, according to Henderson, to mitigate the risks associated with a potential warrant or cyberattack. Cloakroom relies on Google's Cloud Platform.

In the past, the U.S. intelligence community has maintained a working relationship with Google and other major tech firms in an effort to share information about threats relevant to national security.

Unlike Signal or WhatsApp, Cloakroom's push notifications are limited to forum discussions and do not include its encrypted chatrooms. This was done, Henderson said, to avoid sending any information in plaintext to Apple, Google or Microsoft's cloud-based push notification services. In the past, security researchers have uncovered privacy concerns in the way that company's engineer push notification services.

"To my knowledge, we've never been hacked. And no one has served me a warrant of any kind. But let's say they did, even if they did, I doubt it would do them much good," said Henderson, "what we have on our end isn't a lot. I made sure of that."