Cruz campaign updates smartphone app to fix security flaws

March 11 2016, by Michael Biesecker And Jack Gillum

The campaign of Republican presidential candidate Ted Cruz updated its mobile app after an independent review found security flaws that could have allowed hackers to access personal data from users.

The computer-security firm Veracode performed audits of the "Cruz Crew" app and those released by other 2016 presidential contenders at the request of The Associated Press.

While AP was reporting on potential vulnerabilities with the Cruz app, a high-ranking Cruz staffer responsible for the security of the campaign's horde of personal data suffered a breach, giving a hacker access to a campaign email account. Last week, the hacker sent phishing emails to individuals with whom the official had been corresponding, including AP reporters.

The email appeared to be a message from the campaign that included a link to what appeared to be a folder on the Google Drive cloud service. Anyone who clicked the link was prompted to enter login information that gave the hacker access to the victim's email account and any data folders on Google's cloud.

"It's a virus. Don't click on it," Chris Wilson, Cruz's data and digital director, said when asked about the email sent to AP reporters from his account. "Wasn't paying attention and clicked on the stupid folder. ... It must have phished my sent items."

The AP reported last month that the "Cruz Crew" app is designed to gather detailed information from users' phones—tracking their physical movements and harvesting the names and contact information of friends who might want nothing to do with his campaign. That information and more is then fed into a vast database containing intimate details about nearly every adult in the United States to build psychological profiles that target individual voters determined to be likely Cruz supporters.

The campaign said the app's users voluntarily share their personal data, and how that information is collected and shared is detailed in legal disclosures available online.

Veracode concluded that the Cruz app—downloaded to more than 70,000 Apple and Android devices so far—had used poor computer code practices and had deployed weak encryption, potentially exposing personal data because it could be intercepted by eavesdroppers. The review further determined the app could also send text messages without the user's permission.

A Veracode senior project manager, Jonathan Mandell, said poor coding practices on the app "could lead to leaked information, or even exploitation."

After AP shared Veracode's report with Cruz's staff, the campaign worked with its app developer to address the vulnerabilities. AP waited to report the vulnerabilities in the app until the campaign had an opportunity to fix them.

Veracode confirmed last week that the updates resolved some issues with the Cruz app identified in its security audit but said the software still contains weakness that need to be fixed.

After the AP asked Veracode to review apps released by other 2016

presidential candidates, the firm found that code included in the app from Republican candidate John Kasich contained a serious vulnerability known as "SQL injection," which allows an attacker to manipulate information stored by the campaign. Kasich spokesman Rob Nichols said the campaign's staff reviewed Veracode's analysis and did not find it credible.

"Your firm doesn't understand our product," Nichols said. "They don't know what they don't know."

Asked for details of what the campaign felt was in error, Nichols replied: "I'm not a tech person."

Veracode found no suspect code in the "Field The Burn" app released by the campaign of Democrat Bernie Sanders. The campaigns of Republican Donald Trump and Democrat Hillary Clinton have not released their own apps.

Citation: Cruz campaign updates smartphone app to fix security flaws (2016, March 11) retrieved 10 April 2024 from
https://phys.org/news/2016-03-cruz-campaign-smartphone-app-flaws.html