Twilio Hit with Social Engineering Smishing Scheme

Article By

Linn F. Freedman
Robinson & Cole LLP
Data Privacy + Security Insider

Related Practices & Jurisdictions

- Communications, Media & Internet
- Administrative & Regulatory
- Corporate & Business Organizations
- All Federal

Thursday, August 11, 2022

We’ve explained smishing schemes before [view related posts]. Smishing is like phishing, but uses SMS texting to deliver malicious code to users’ phones, or tricks the user into visiting a malicious website to steal their credentials or money. Hence, the important tip is to be very wary of texts from unknown individuals urging you to click on links embedded within the text.

Smishing schemes can be sophisticated, which is how Twilio describes the successful smishing attack against it that was discovered on August 4, 2022. According to Wikipedia, Twilio “provides programmable communication tools for making and receiving phone calls, sending and receiving text messages, and performing other communication functions using its web service APIs.” It is ironic that Twilio, a communications platform, was hit with a smishing attack.

According to Twilio,

“One August 4, 2022, Twilio became aware of unauthorized access to information
related to a limited number of Twilio customer accounts through a sophisticated social engineering attack designed to steal employee credentials. This broad based attack against our employee base succeeded in fooling some employees into providing their credentials. The attackers then used the stolen credentials to gain access to some of our internal systems, where they were able to access certain customer data.

“More specifically, current and former employees recently reported receiving text messages purporting to be from our IT department. Typical text bodies suggested that the employee’s passwords had expired, or that their schedule had changed, and that they needed to log in to a URL the attacker controls. The URLs used words including “Twilio,” “Okta,” and “SSO” to try and trick users to click on a link taking them to a landing page that impersonated Twilio’s sign-in page. The text messages originated from U.S. carrier networks. We worked with the U.S. carriers to shut down the actors and worked with the hosting providers serving the malicious URLs to shut those accounts down. Additionally, the threat actors seemed to have sophisticated abilities to match employee names from sources with their phone numbers.”

The data of 125 customers was affected by the attack and Twilio is working directly with those customers.

Just after Twilio announced it had been affected by the smishing incident, Cloudfare publicly announced on August 9, 2022, that it, too, had been targeted by a similar attack. According to its website, Cloudfare “started as a simple application to find the source of email spam. From there it grew into a service that protects websites from all manner of attacks, while simultaneously optimizing performance.”

Cloudfare said it had been targeted by a similar smishing scheme and used the experience to educate others about the incident in its blog post: “The mechanics of a sophisticated phishing scam and how we stopped it.” Cloudfare acknowledged that “around the same time as Twilio was attacked, we saw an attack with very similar characteristics also targeting Cloudfare’s employees” and, while some of its employees fell for the messages, it used its own products to stop the attack. Albeit a bit self-serving, the point is that internet service providers (ISPs) and other communication providers were being targeted simultaneously with smishing attacks, which is obviously concerning.

Cloudfare states “This was a sophisticated attack targeting employees and systems in such a way that we believe most organizations would be likely to be breached. Given that the attacker is targeting multiple organizations, we wanted to share here a rundown of exactly what we saw in order to help other companies recognize and mitigate this attack.” Very helpful Cloudfare, and thank you for sharing details so other organizations can be aware of how the scheme works and put measures in place to prevent a similar attack. This is the value of information sharing. The breakdown of the attack by Cloudfare is excellent, and readers may wish to review it and use it as a tool for educating their users on smishing attacks and why they are often so successful.
Source URL: https://www.natlawreview.com/article/twilio-hit-social-engineering-smishing-scheme