On 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. We continue to notify and are working directly with customers who were affected by this incident. We are still early in our investigation, which is ongoing.

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.

We have heard from other companies that they, too, were subject to similar attacks, and have coordinated our response to the threat actors – including collaborating with carriers to stop the malicious messages, as well as their registrars and hosting providers to shut down the malicious URLs. Despite this response, the threat actors have continued to rotate through carriers and hosting providers to resume their attacks.

Based on these factors, we have reason to believe the threat actors are well-organized, sophisticated and methodical in their actions. We have not yet identified the specific threat actors at work here, but have liaised with law enforcement in our efforts. Socially engineered attacks are -- by their very nature -- complex, advanced, and built to challenge even the most advanced defenses.

Investigation Conclusion – October 27, 2022

This is our final update to this blog post describing a security incident involving an SMS phishing (or “smishing”) attack targeting Twilio employees, resulting in unauthorized access to some internal non-production systems. Twilio and a leading forensic firm conducted an extensive investigation into the incident, and we provided updates to our blog as information became available. The investigation has now concluded, and we’d like to share our findings.

Background

In mid-July 2022, malicious actors sent hundreds of smishing text messages to the mobile phones of current and former Twilio employees (the “Smishing Incident”). The malicious actors posed as Twilio IT or other administrators and urged users to click on what appeared to be password-reset and other links. The links led to fake Okta login pages for Twilio. These fake pages were hosted on domains created by the malicious actors, such as twilio-sso.com, twilio.net, twilio.org, sendgrid-okta.org, twilio-okta.net, and twilio-okta.com. Some Twilio employees entered their credentials on these fake pages. The malicious actors then used the credentials of these Twilio employees to access internal Twilio administrative tools and applications to access certain customer information, which we have detailed in previous blog posts on the incident.

Our investigation also led us to conclude that the same malicious actors likely were responsible for a brief security incident that occurred on June 29, 2022. In the June incident, a Twilio employee was socially engineered through voice phishing (or “vishing”) to provide their credentials, and the malicious actor was able to access customer contact information for a limited number of customers. The threat actor’s access was identified and eradicated within 12 hours. Customers whose information was impacted by the June Incident were notified on July 2, 2022.

Smishing incident findings

Our investigation into the Smishing Incident found the following:

* The last observed unauthorized activity in our environment was on August 9, 2022;
* 209 customers – out of a total customer base of over 270,000 – and 93 Authy end users – out of approximately 75 million total users – had accounts that were impacted by the incident; and
* There is no evidence that the malicious actors accessed Twilio customers’ console account credentials, authentication tokens, or API keys.

We have completed our outreach to customers who had affected accounts and worked with them to understand the impact.

Industry findings regarding widespread cyberattacks

Independent cybersecurity researchers examining worldwide cyber incidents have found that a wide-scale set of attacks have been launched against numerous technology companies, telecommunications providers, and cryptocurrency-related individuals and organizations. According to these researchers – who have dubbed the malicious actors “0ktapus” or “Scatter Swine” – the attacks involved (a) identifying the mobile phone numbers of employees at such organizations, (b) sending smishing texts or making voice phishing (“vishing”) phone calls to identified phone numbers to trick the employees into clicking on links that led to fake Okta, Azure, Duo and other login pages, (c) harvesting the employees’ credentials and one-time passwords (“OTPs”) through those fake pages, and (d) using those credentials to advance reconnaissance operations within the target networks in order to attempt user account takeovers and further smishing efforts targeting other organizations. The attack on Twilio employed similar tactics, techniques, and procedures.