



TWILIO SOCIAL ENGINEERING ATTACK

ZEROFOX INTELLIGENCE

F-2022-08-08b

Classification: TLP:WHITE

Criticality: Medium

Intelligence Requirements: Data Breach, PII, and Fraud

August 8, 2022



Scope Note

*ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were **identified prior to 1:00 PM (EDT) on August 8, 2022**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.*

Twilio Social Engineering Attack

Key Findings

- Enterprise software vendor Twilio confirmed today that hackers accessed an undisclosed amount of its customer data after an SMS phishing (smishing) campaign.
- Twilio began contacting users impacted by the attack.
- Nevertheless, ZeroFox Intelligence recommends that Twilio users change their account login credentials and enable two-factor authentication if possible.

Analyst Commentary

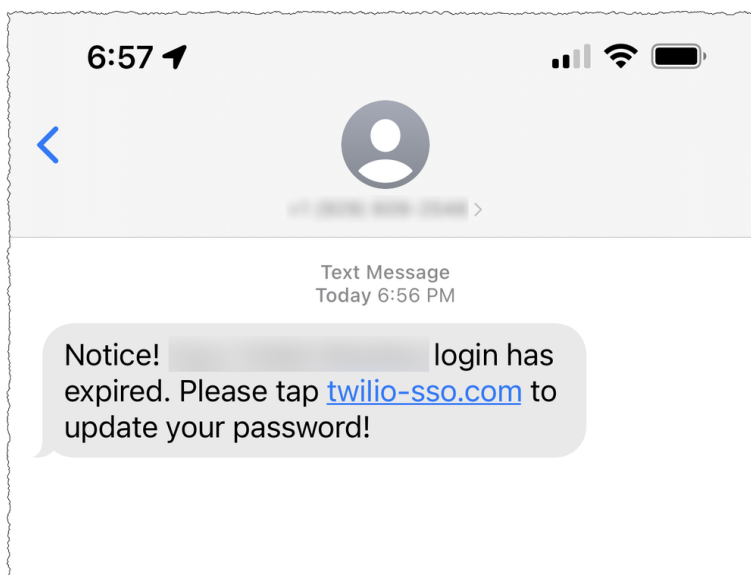
ZeroFox Intelligence is monitoring an incident involving Twilio, which confirmed that hackers accessed its customer data after a successful smishing campaign. Twilio announced publicly today that the campaign targeted current and former employees with fraudulent SMS messages claiming to be from Twilio's IT department and stating that the users' passwords had expired. The attackers were then able to use the stolen credentials to gain access to internal systems and, subsequently, to certain customer data. Twilio is contacting all affected customers as of this writing.

- The messages referenced “Okta” and “SSO” (Single Sign On) to entice the employees to click on a link guiding them to a fraudulent, threat-actor-controlled landing page that impersonated Twilio's sign in page.
- The credibility of the smishing messages was increased by matching employee names from sources with their phone numbers.

ZeroFox Intelligence notes the potential for some supply chain impact on downstream customers. Twilio provides communication tools for making and receiving calls, sending and receiving text messages, and other communication functions—including



SMS-based two-factor authentication. Twilio is known to work with political action committees and other U.S. government entities to communicate with constituents and donors. If threat actors discover a way to leverage Twilio's services to obtain authenticated sessions from downstream customers, multiple end users could be compromised for follow-on malicious activity.



Example of Malicious SMS Message Directed at Twilio Employees

Source: [hXXps://www.twilio\[.\]com/blog/august-2022-social-engineering-attack](https://www.twilio.com/blog/august-2022-social-engineering-attack)

Recommendations

- If not already enabled, turn on the compromised credentials rule for all relevant entities and ensure relevant emails are entered for those entities, or reach out to ask@zerofox.com for assistance.
- Alert employees to potential social engineering attacks, including smishing text messages relating to this campaign.
- In addition to enabling two-factor authentication, consider using a password manager as an additional protective measure against smishing.

Sources

1. [hXXps://www.twilio\[.\]com/blog/august-2022-social-engineering-attack](https://www.twilio.com/blog/august-2022-social-engineering-attack)
2. [hXXps://techcrunch\[.\]com/2022/08/08/twilio-breach-customer-data/](https://techcrunch.com/2022/08/08/twilio-breach-customer-data/)
3. [hXXps://www.cyberscoop\[.\]com/twilio-campaign-hack-text/](https://www.cyberscoop.com/twilio-campaign-hack-text/)



Appendix: Traffic Light Protocol for Information Dissemination

Red

WHEN SHOULD IT BE USED?

Sources may use TLP:

RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.

HOW MAY IT BE SHARED?

Recipients may NOT share TLP:

RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.

Amber

Sources may use TLP:

AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.

Recipients may ONLY share TLP:

AMBER information with members of their own organization and only as widely as necessary to act on that information.

Green

WHEN SHOULD IT BE USED?

Sources may use TLP:

GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.

HOW MAY IT BE SHARED?

Recipients may share TLP:

GREEN information with peers & partner organizations within their sector or community but not via publicly accessible channels.

White

Sources may use TLP:

WHITE when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.

Recipients may share TLP:

WHITE information without restriction, subject to copyright controls.