GUIDE

Signal Impacted by Twilio Social Engineering Attack

> **Incident:** Signal Impacted by Twilio Social Engineering Attack **Date:** 2022-08-08 | **Duration:** ~None hours | **Severity:** P1-high **Affected:** A small number of Signal users | **Systems:** Twilio's phone number verification services, Signal user registration/verification process **Root cause (summary):** Twilio employees fell victim to a sophisticated phishing attack, leading to the compromise of their credentials and unauthorized access to Twilio's internal support systems.

Timeline: Timeline not available from public sources.

Incident Summary

On August 8, 2022, Signal was notified by its third-party phone number verification provider, Twilio, about a security incident. Twilio had experienced a sophisticated social engineering attack, where malicious actors successfully phished several of its employees. This compromise granted the attackers unauthorized access to Twilio's internal support systems, which included access to customer data for a limited number of Twilio clients.

For Signal, this meant that the attackers gained access to Twilio's console used for phone number verification. This access allowed them to query information about Signal users' phone numbers and, critically, to re-register some Signal accounts to attacker-controlled devices. While the attackers could not access message history or contact lists due to Signal's end-to-end encryption, they could potentially send and receive messages from the compromised phone number if they successfully re-registered the account.

Upon notification, Signal immediately took steps to identify and notify potentially affected users, prompting them to re-register their accounts and enable a critical security feature known as Registration Lock. This incident underscores the inherent risks of supply chain dependencies, even for platforms designed with robust end-to-end encryption.

What Went Wrong: Root Cause

The core issue stemmed from a sophisticated social engineering attack targeting Twilio employees. The attackers successfully executed a phishing campaign, tricking employees into divulging their corporate credentials and multi-factor authentication (MFA) tokens. This compromise provided the attackers with unauthorized access to Twilio's internal systems.

Specifically, the attackers gained entry to Twilio's internal customer support tools. These tools are designed to manage and verify phone numbers for Twilio's client base, including Signal. The critical failure at Twilio was the insufficient protection against this type of credential compromise and subsequent unauthorized access to sensitive internal systems, which allowed the attackers to manipulate phone number verification processes for Signal users. The reliance of Signal's account registration flow on Twilio's SMS verification service meant that a breach in Twilio's security perimeter directly impacted Signal's user accounts.

Attack Vector Details

The attack against Twilio was a highly targeted and sophisticated phishing campaign. Based on Twilio's public statements, the sequence of events unfolded as follows:

1. **Initial Phishing:** Twilio employees received SMS messages impersonating Twilio's IT department. These messages contained links to malicious websites designed to mimic Twilio's internal login page.
2. **Credential Harvesting:** Employees who clicked these links were prompted to enter their corporate usernames, passwords, and multi-factor authentication (MFA) tokens. The attackers used a real-time phishing kit to capture these credentials and session tokens as they were entered.
3. **Unauthorized Access:** With the stolen credentials and MFA tokens, the attackers successfully bypassed Twilio's security measures and gained unauthorized access to Twilio's internal systems.
4. **Internal System Exploitation:** The attackers specifically accessed Twilio's internal support console. This console allowed them to view customer accounts and, crucially, to initiate actions related to phone number verification and re-registration for a subset of Twilio's customers, including Signal.

5. **Signal Account Compromise:** By leveraging their access to Twilio's systems, the attackers were able to query phone numbers associated with Signal accounts and initiate the re-registration process for those numbers onto devices under their control. This effectively allowed them to impersonate Signal users.

Impact and Blast Radius

The impact of the Twilio social engineering attack on Signal users was significant, albeit contained to a limited subset.

- **Affected Users:** Approximately 1,900 Signal users were potentially affected. Out of these, Signal confirmed that the attackers actively targeted and attempted to re-register the accounts of about 6 users.
- **Data Exposed:** For the affected users, the attackers could view their phone number, profile picture, and "About" information.
- **Account Takeover Potential:** The primary impact was the potential for account takeover. If an attacker successfully re-registered a user's phone number to their device, they could then send and receive Signal messages from that number. This could lead to impersonation, social engineering attacks against the user's contacts, and access to new messages.
- **Limitations:** Crucially, Signal's end-to-end encryption architecture prevented the attackers from accessing any past message history, contact lists, or other sensitive encrypted data. The compromise was limited to the registration process, not the encrypted communication itself.
- **Severity:** Classified as P1-high due to the direct potential for user account compromise and impersonation, which represents a severe privacy and security breach for those affected.

Signal's Response

Upon receiving notification from Twilio, Signal initiated a rapid and targeted response to mitigate the impact and protect its users:

1. **Immediate Identification:** Signal engineers quickly worked to identify all user accounts potentially affected by the Twilio breach. This involved correlating data from Twilio's notification with Signal's internal records.

2. **User Notification:** Signal proactively notified all 1,900 potentially affected users directly through the Signal app. These notifications explained the incident, its potential implications, and the steps users needed to take.
3. **Account Re-registration Prompt:** For users whose accounts were identified as potentially compromised or targeted, Signal prompted them to re-register their Signal app. This action would invalidate any attacker-controlled device attempting to use their number.
4. **Emphasis on Registration Lock:** Signal strongly encouraged all users, particularly those affected, to enable "Registration Lock." This feature adds an additional layer of security by requiring the Signal PIN to be entered whenever a user attempts to register their phone number with Signal on a new device. This effectively prevents unauthorized re-registration attempts, even if an attacker gains control of the SMS verification process.
5. **Internal Review and Hardening:** While not explicitly detailed, it is standard practice for Signal to review its integration points with third-party vendors and assess potential hardening measures to reduce similar risks in the future. This likely included evaluating alternative verification methods or implementing stricter controls around Twilio's API usage.

Systemic Lessons for Secure Communication Platforms

This incident provides critical systemic lessons for any platform, especially those dealing with sensitive communications and relying on third-party services.

1. **Supply Chain Security is Paramount:** Even with robust end-to-end encryption, the security of a platform is only as strong as its weakest link. Third-party dependencies, like SMS verification providers, represent significant attack surfaces. Platforms must conduct thorough security assessments of all critical vendors and have contingency plans for vendor breaches.
2. **Multi-Factor Authentication (MFA) is Not a Panacea:** The Twilio incident demonstrated that even with MFA in place, sophisticated phishing techniques can bypass it by capturing MFA tokens in real-time. Organizations must move beyond basic MFA to stronger forms like FIDO2/WebAuthn hardware keys, which are phishing-resistant.

3. **Layered Security for Critical Operations:** Internal tools and systems that can affect customer accounts (e.g., support consoles, administrative interfaces) must have extremely stringent access controls, anomaly detection, and audit logging. Access should be based on the principle of least privilege, and critical actions should require multiple approvals.
4. **User-Empowering Security Features:** Signal's "Registration Lock" feature proved to be a vital defense against this type of attack. Platforms should empower users with security features that can mitigate risks even when external dependencies are compromised. These features should be easy to understand and enable.
5. **Employee Security Training Must Evolve:** Phishing attacks are constantly evolving. Employee security training needs to go beyond basic awareness to include recognition of sophisticated social engineering tactics, including those designed to bypass MFA. Regular simulated phishing exercises are crucial.

User Education

The Twilio incident highlights the importance of user vigilance and the effective use of available security features. For Signal users, and users of any secure communication platform, the following educational points are critical:

- **Enable Registration Lock (Signal PIN):** This is the single most important action Signal users can take to protect against account takeover attempts. By setting a Signal PIN and enabling Registration Lock, you prevent anyone from registering your phone number to a new device without knowing your PIN, even if they intercept SMS verification codes.
- **Be Skeptical of Unsolicited Messages:** Exercise extreme caution with links received via SMS, especially those claiming to be from your service provider or IT department. Always verify the sender and the legitimacy of the request through an official channel (e.g., directly visiting the company's official website, not clicking a link).
- **Use Strong, Unique Passwords and MFA:** While this incident targeted a third-party, general account security best practices remain crucial. Use strong, unique passwords for all your online accounts and enable MFA wherever possible.

- **Understand Platform Limitations:** While Signal provides excellent end-to-end encryption for message content, the initial registration process often relies on external systems like SMS. Understanding these dependencies helps users appreciate the importance of features like Registration Lock.
- **Stay Informed:** Pay attention to security notifications from your service providers. They are designed to help you protect your account.

> 📌 **Key Engineering Lesson:** Organizations must implement robust multi-factor authentication, comprehensive employee security training, and strong supply chain security practices to mitigate the risk of sophisticated social engineering attacks targeting critical third-party dependencies.