Detecting Scatter Swine: Insights into a Relentless Phishing Campaign

By Defensive Cyber Operations

Published: 2022-08-25 · Archived: 2026-04-05 12:36:08 UTC

Summary

- Twilio recently identified unauthorized access to information related to 163 Twilio customers, including Okta. Access was gained to internal Twilio systems, where data of some Okta customers was accessible to a threat actor (detailed below).
- Okta has determined that a small number of 1) Mobile phone numbers and 2) Associated SMS messages containing one-time passwords (“OTPs”) were accessible to the threat actor via the Twilio console.
- Okta has notified any customers where a phone number was visible in the console at the time the console was accessed.
- There are no actions necessary for customers at this time. Details regarding this access, our response, and best practices can be found below.

In recent months, a number of technology companies were subject to persistent phishing campaigns by a threat actor we refer to as “Scatter Swine”.

Okta’s Defensive Cyber Operations (DCO) has proactively notified these companies when we have observed phishing infrastructure deployed by this threat actor, among others. It is commonplace for DCO to detect Scatter Swine repeatedly targeting the same organizations with multiple phishing sites within a matter of hours.

On the evening of Sunday, August 7, 2022, Twilio disclosed that a number of Twilio customer accounts and internal applications were accessed in attacks that resulted from one or more of these phishing campaigns.

Okta offers customers a range of authenticators to choose from, including the use of SMS for the delivery of one-time codes. Twilio provides one of two services Okta leverages for customers that choose to use SMS as an authentication factor.

On August 8, 2022, Twilio provided an initial notification to Okta, to inform us that unspecified data relevant to Okta was accessed during Twilio’s incident.

Okta prioritized routing of SMS-based communications to an alternative provider while we worked with Twilio’s security team to understand the scope and impact of the incident.

The Twilio security team supported our investigation by subsequently providing internal system logs which we were able to use to correlate and identify the extent of the threat actor’s activity as it pertains to Okta customer

data.

Using these logs, Okta's Defensive Cyber Operations' analysis established that two categories of Okta-relevant mobile phone numbers and one-time passwords were viewable during the time in which the attacker had access to the Twilio console. A one-time passcode is valid for five minutes.

A **primary** category (see "Targeted Activity" below) are those mobile phone numbers the threat actor searched for directly in the Twilio console.

A **secondary** category (see "Incidental Exposure" below) are mobile phone numbers that can be considered 'incidental' to the specific actions or objectives of the threat actor.

Okta has notified customers with mobile phone numbers in both of the above categories.

Targeted Activity

The threat actor searched for 38 unique phone numbers in the Twilio console, nearly all of which can be linked to a single targeted organization.

A review of logs provided to us by Twilio revealed that the threat actor was seeking to expand their access. We assess that the threat actor used credentials (usernames and passwords) previously stolen in phishing campaigns to trigger SMS-based MFA challenges, and used access to Twilio systems to search for One Time Passwords sent in those challenges.

Incidental Exposure

The second category of exposed mobile phone numbers were incidental to this activity. Incidental, in this case, can be defined as phone numbers that may have been present in the Twilio portal during the threat actor's limited activity window. Okta's analysis reveals no indication that the threat actor targeted or used such mobile phone numbers.

The threat actor performed their searches using Twilio administrative portals that (by default) list the most recent 50 messages sent using Okta's Twilio account.

Okta usernames are not visible in Twilio logs.

The threat actor took no actions that indicated an intent to use access to this information, an observation we have verified via extensive investigation (described below).

Intrusion Analysis

After analyzing suspicious activity and identifying key TTPs used by the threat actor, Okta performed threat hunting across our platform logs during the time period that the threat actor was known to have had access to Twilio's systems. Some example threat hunting searches are provided below.

This exercise uncovered an event in which the threat actor successfully tested this technique against a single account unrelated to the primary target. The threat actor did not perform any additional actions once they had

validated this access, and returned to their prior activity.

Outside of this isolated event, there is no evidence that the threat actor successfully used this technique to expand the scope of its access outside of their primary target.

Tactics, Techniques and Procedures

Scatter Swine has directly targeted Okta via phishing campaigns on several occasions, but was unable to access accounts due to the strong authentication policies that protect access to our applications.

Okta Security has observed the following TTPs (tactics, techniques and procedures) employed by Scatter Swine:

- The threat actor makes use of infrastructure provided by Bitcoin-friendly provider Bitlaunch, providing servers from DigitalOcean, Vultr, and Linode.
- Preferred domain name registrars include Namecheap or Porkbun, both of which accept Bitcoin as payment.
- We have observed the threat actor delivering phishing lures in bulk to individuals in targeted organizations via text messages. We are aware of multiple instances where hundreds of messages were sent to employees and even to family members of employees.
- The threat actor likely harvests mobile phone numbers from commercially available data aggregation services that link phone numbers to employees at specific organizations.
- The threat actor calls targeted individuals and impersonates support trying to understand how authentication works. The accent of the threat actor appears to be North American, confident and clearly spoken.
- The threat actor’s targets have included technology companies, telecommunications providers and organizations and individuals linked to cryptocurrency.
- The threat actor predominately hosts self-contained, HTTP-based phishing infrastructure. Their sites do not use TLS certificates.
- If the threat actor successfully harvests user credentials during a SMishing (SMS phishing) campaign, attempts are made to authenticate using anonymizing proxy services. In this particular campaign the threat actor favored Mullvad VPN.
- The phishing kit used by the threat actor is designed to capture usernames, passwords and OTP factors. We have also observed the threat actor triggering multiple push notifications in an attempt to trick a target into allowing access to the account.
- The threat actor has been observed connecting to multiple users from the same Windows device.

The threat actor registers domain names in common formats in order to socially engineer targets into entering their credentials into their phishing sites.

- {targeted organization}-corp.net
- {targeted organization}-help.com
- {targeted organization}-help.net
- {targeted organization}-helpdesk.com
- {targeted organization}-login.co
- {targeted organization}-mfa.com
- {targeted organization}-okta.co
- {targeted organization}-okta.com
- {targeted organization}-okta.net
- {targeted organization}-okta.org
- {targeted organization}-okta.us
- {targeted organization}-onelogin.com
- {targeted organization}-sso.com
- {targeted organization}-sso.net
- {targeted organization}-vpn.com
- {targeted organization}-vpn.net
- {targeted organization}-vpn.org
- okta-{targeted organization}.com

Stepping up your defenses

Based on our analysis of this intrusion, we recommend that customers embrace a “defense in depth” approach to protecting user accounts from phishing attacks.

- Use strong authenticators with the most phishing-resistant properties, such as FIDO2 WebAuthn platform and roaming authenticators and smart cards. Consider FastPass, Okta’s passwordless solution as a longer-term strategy to minimize exposure to credential-based attacks.
- Train users to identify indicators of suspicious emails, phishing sites and common social engineering techniques used by attackers. Okta customers can make it easy for users to report potential issues by configuring End User Notifications and Suspicious Activity Reporting.

- Authentication policies can be used to restrict user access to applications based on a range of customer-configurable prerequisites.
- Use Behavior Detection to act (via step-up authentication) or alert (via System Log) when a user's sign in behavior deviates from a previous pattern of activity. This threat actor is almost always attempting to authenticate from a new device and new IP that has no previous association with the user.
- Use Network Zones to deny or perform step-up authentication on requests from rarely-used networks and anonymizing proxies.
- Restrict access to applications to only those devices that are registered (with Okta FastPass) or devices managed by endpoint management tools, and
- Restrict access to the most sensitive applications and data using application-specific authentication policies. Require re-authentication "every time" a user signs into these resources.
- Protect administrative sessions: Take a "Zero Standing Privileges" approach to administrative access. Assign administrators Custom Admin Roles with the least permissions required for daily tasks, and require dual authorization for JIT (just-in-time) access to more privileged roles. Apply ASN and IP Session Binding (from Settings > Features) to all administrative apps to prevent the replay of stolen administrative sessions. Enable Protected Actions (under Settings > Features) to force re-authentication whenever an administrative user attempts to perform sensitive actions.
- Talk to your SaaS partners about support for Demonstrating Proof-of-Possession, Continuous Access Evaluation Profile (CAEP) and Universal Logout.

Searching Okta System Log for Scatter Swine TTPs

The following Okta System Log query searches for SMS events (authentication challenges, password resets or factor enrolment events) from new devices and network locations for a given user, filtered according to known TTPs discovered through the analysis of this campaign.

If customers are seeking to check which of these messages transited Twilio, add the following to the query:

and debugContext.debugData.smsProvider eq "TWILIO"

Customers using the Okta Add-On for Splunk can run a similar search using the following query:

Further Threat Hunting

Using the above TTPs, below is an example query for how you might hunt for potential account takeover attempts.

This is a starting point and should be adjusted for your environment. A filter for securityContext.isProxy eq "true" could reduce the scope of events to review.

Equally, consider that the threat actor is known to use VPS providers that accept Bitcoin as payment. Virtual Private Servers are not classified as proxies.

In the example below, we assume that:

- The threat actor was NOT using FIDO2/WebAuthn factors.
- The threat actor was using a Computer with a Windows Operating System.
- The threat actor made the request using a New Device and New IP for the target user.
- The threat actor often uses proxies or other anonymization services.

For further advice on searching Okta System Log for suspicious events, see this support article.

Change log:

1.2 - 03/08/2024

- Updated recommendations to include reauthentication frequency.
- Updated recommendations to include new features released as part of Okta Secure Identity Commitment: Protected Actions, ASN/IP Session Binding.

1.1 - 08/30/2022

- Detection Logic edited in System Log events to reflect that attributes in logOnlySecurityData are captured in a json format {"Key":"Value"}. Detections that evaluate behaviours (debugContext.debugData.behaviors) take the form of Key=Value and remain unchanged.

1.0 - 08/25/2022

- Original version published.
