Early Analysis of the Twilio phishing attack-it is the tip of the iceberg.

silentpush.com/blog/analysis-of-the-twilio-phishing-attack

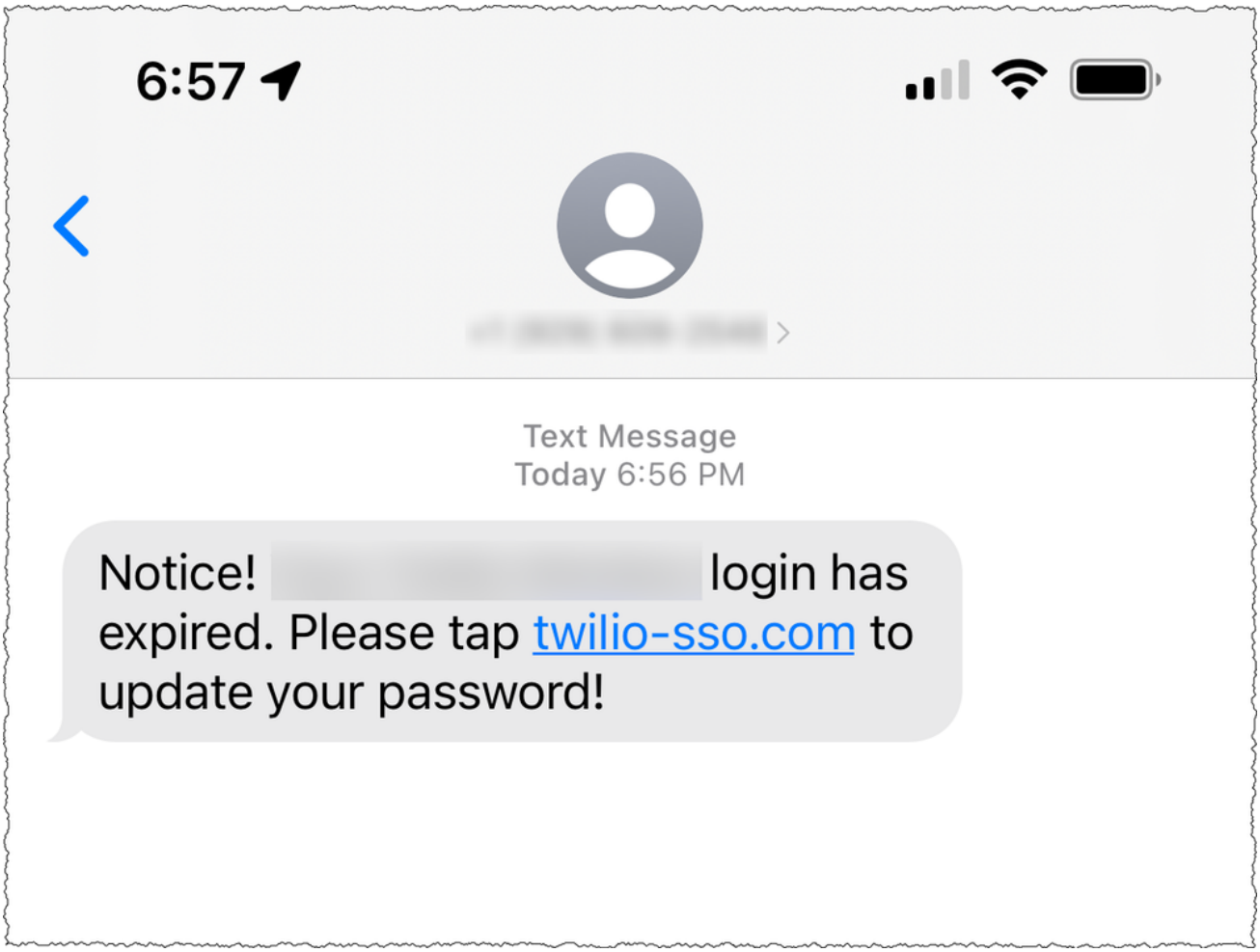
August 13, 2022

Aug 13
Written By The Team

What happened?

On August 4th, threat actors gained illicit access to customer information on the Twilio platform - a global UCaaS service with nearly 8,000 employees - following an SMS-based social engineering attack that fooled staff into providing login credentials, through a malicious access portal.

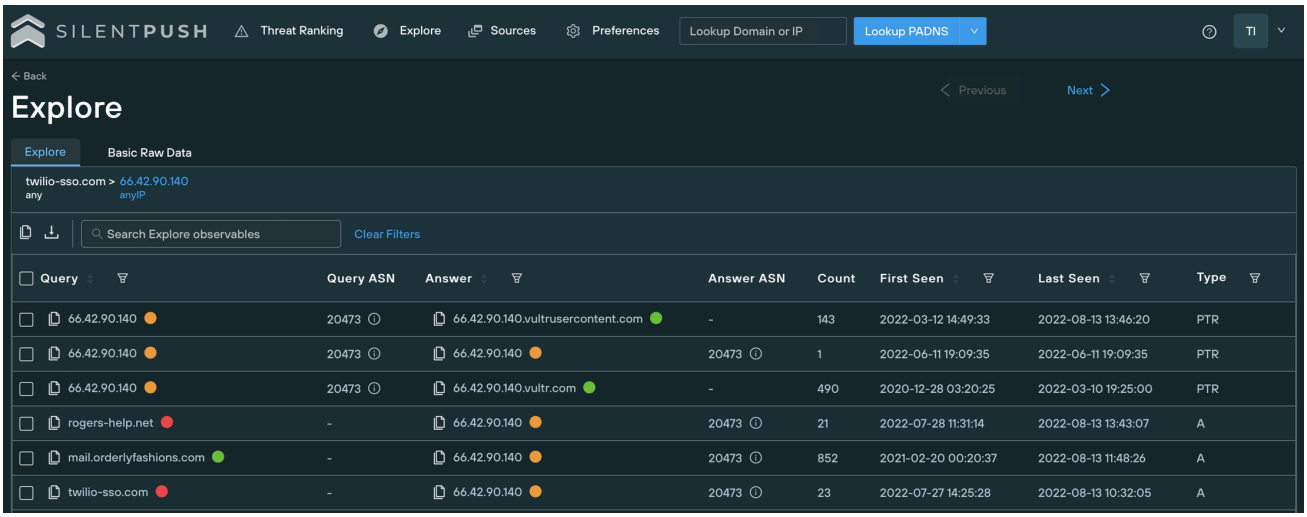
The attack vector was simple - employees received a text message asking them to renew their company credentials via what appeared to be at first glance a legitimate URL:



Original SMS message

Staff members followed the link - believing it to be genuine - and inputted their credentials, which enabled threat actors to harvest numerous sets of authentication details, providing them access to restricted customer records.

Twilio's response was admirable - they immediately consulted with similarly affected firms, cell carriers and the security community to mitigate any further damage - but threat actors resumed their assault by sending messages over alternate carriers, and used different hosting providers to facilitate access to compromised login portals.



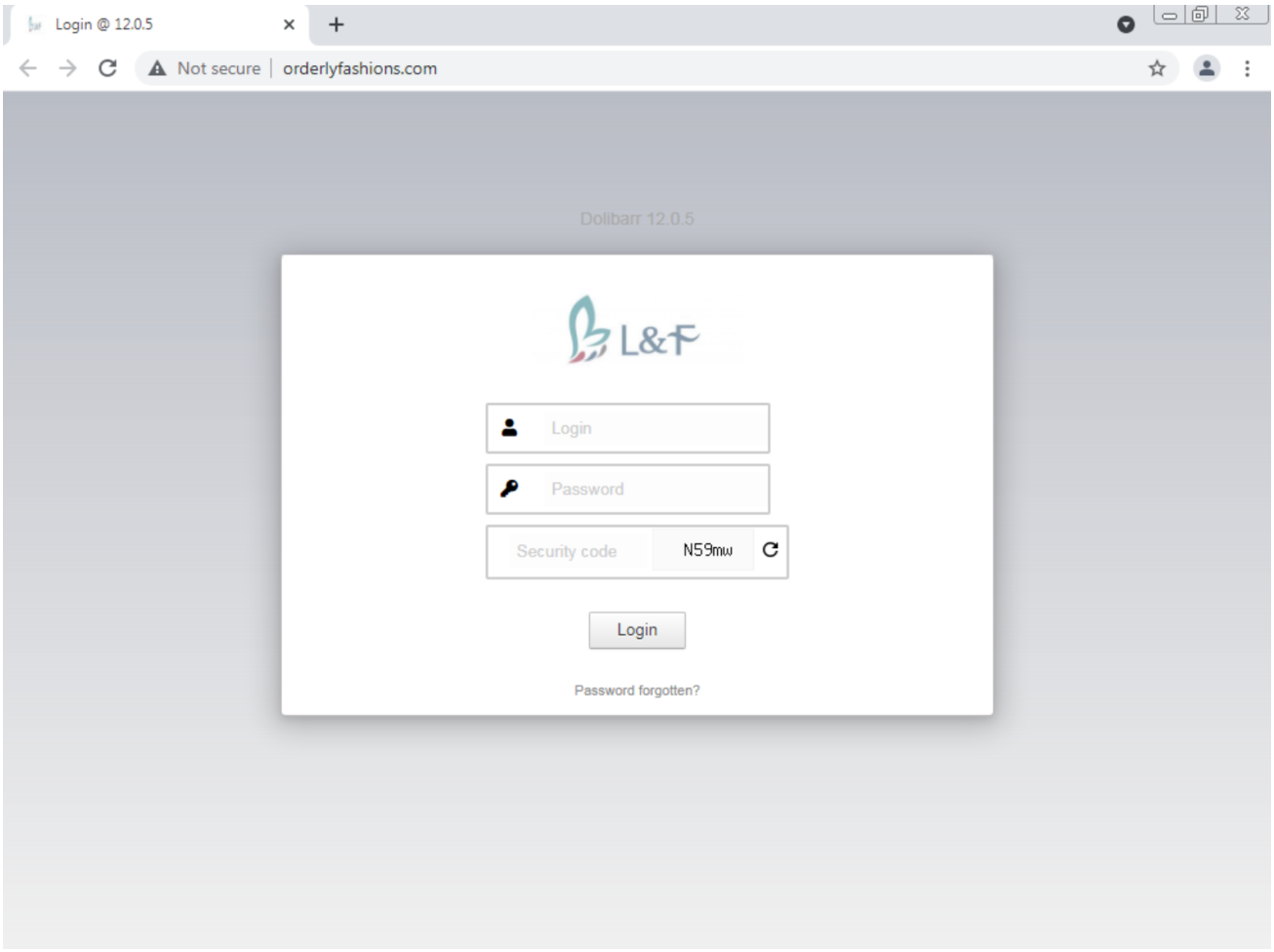
Linked phishing pages

Analysis of the attack

In any phishing attack, supplemental domain analysis is the key to both unlocking the attack vector, and protecting against further intrusions originating from the same IoC.

We analysed the DNS information of `twilio-sso[.]com`, and identified a subdomain of `orderlyfashions[.]com`, hosted on the same IP address as the original IoC.

The domain populates a website that displays a customised Dolibarr login page - an open source ERP and CRM platform:



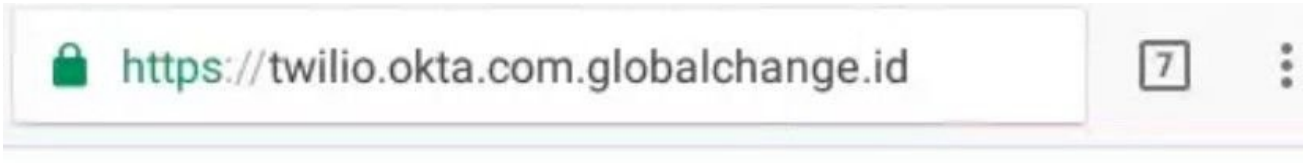
Malicious Dolibar login page

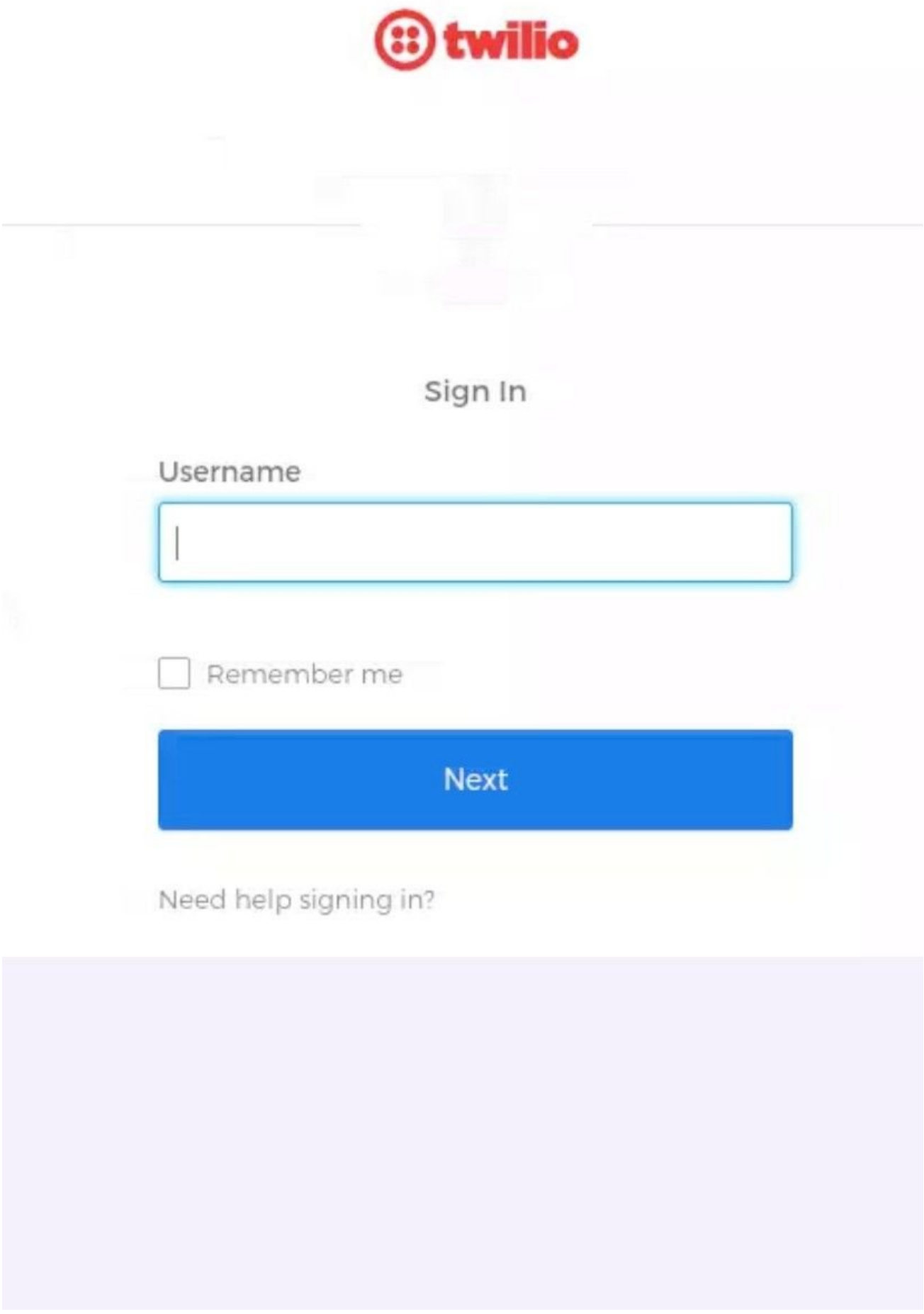
Upon further analysis, we uncovered several phishing domains targeting Twilio, all of which redirected to the same Dolibarr login page.

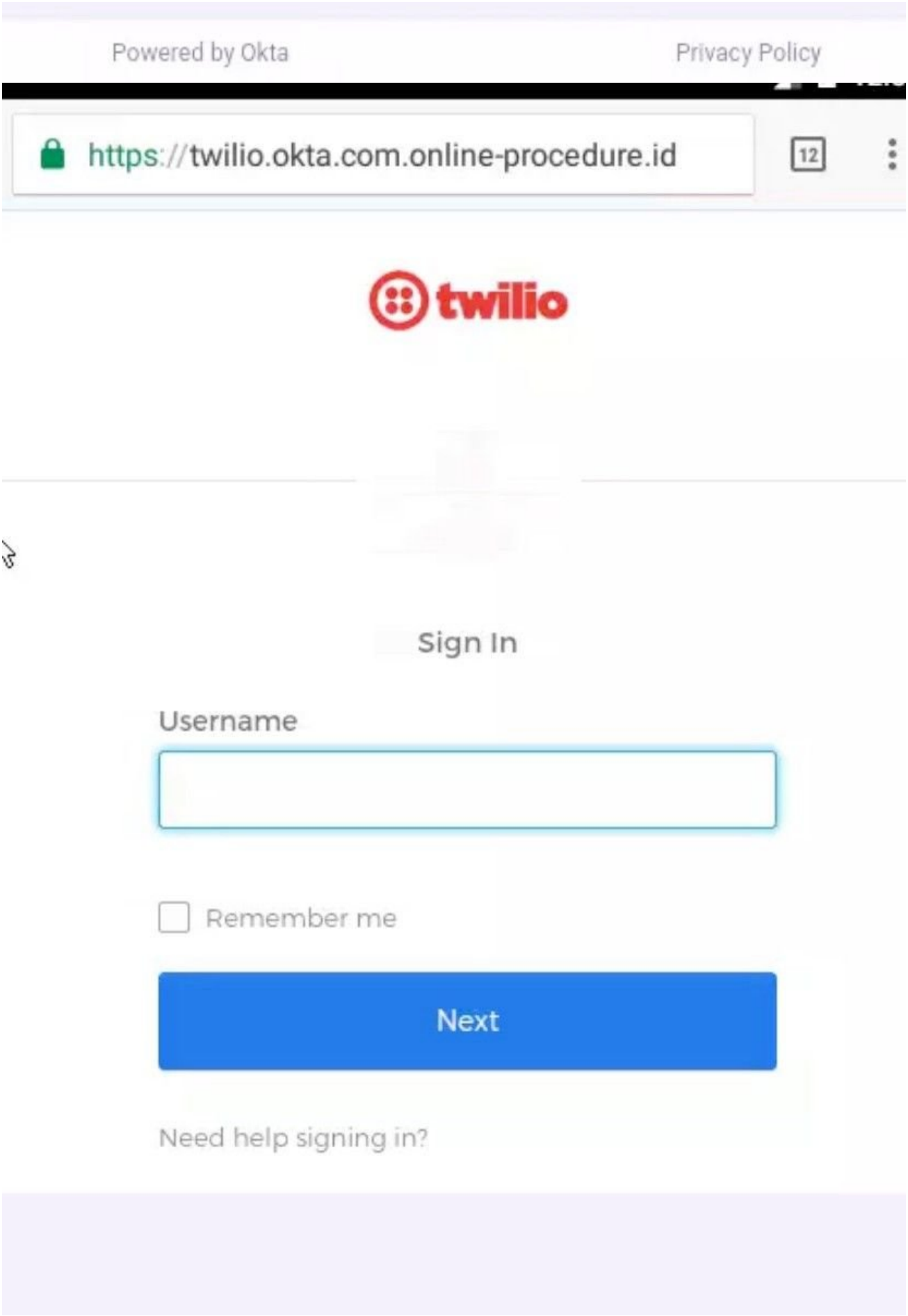
It is possible that threat actors were using a communal login portal - redirected from multiple domains - the purpose of which is unclear, but possibly as a central administration portal. The control panel could just be a skin to hide their phishing control panel or it may be that they used a vulnerability in the control panel to take over the infrastructure and launch their campaign from there. A number of things lead us to believe the former is the more likely scenario.

Wherever we found the login page, once we'd analysed the IP addresses which used to host it, we found even more SSO phishing pages.

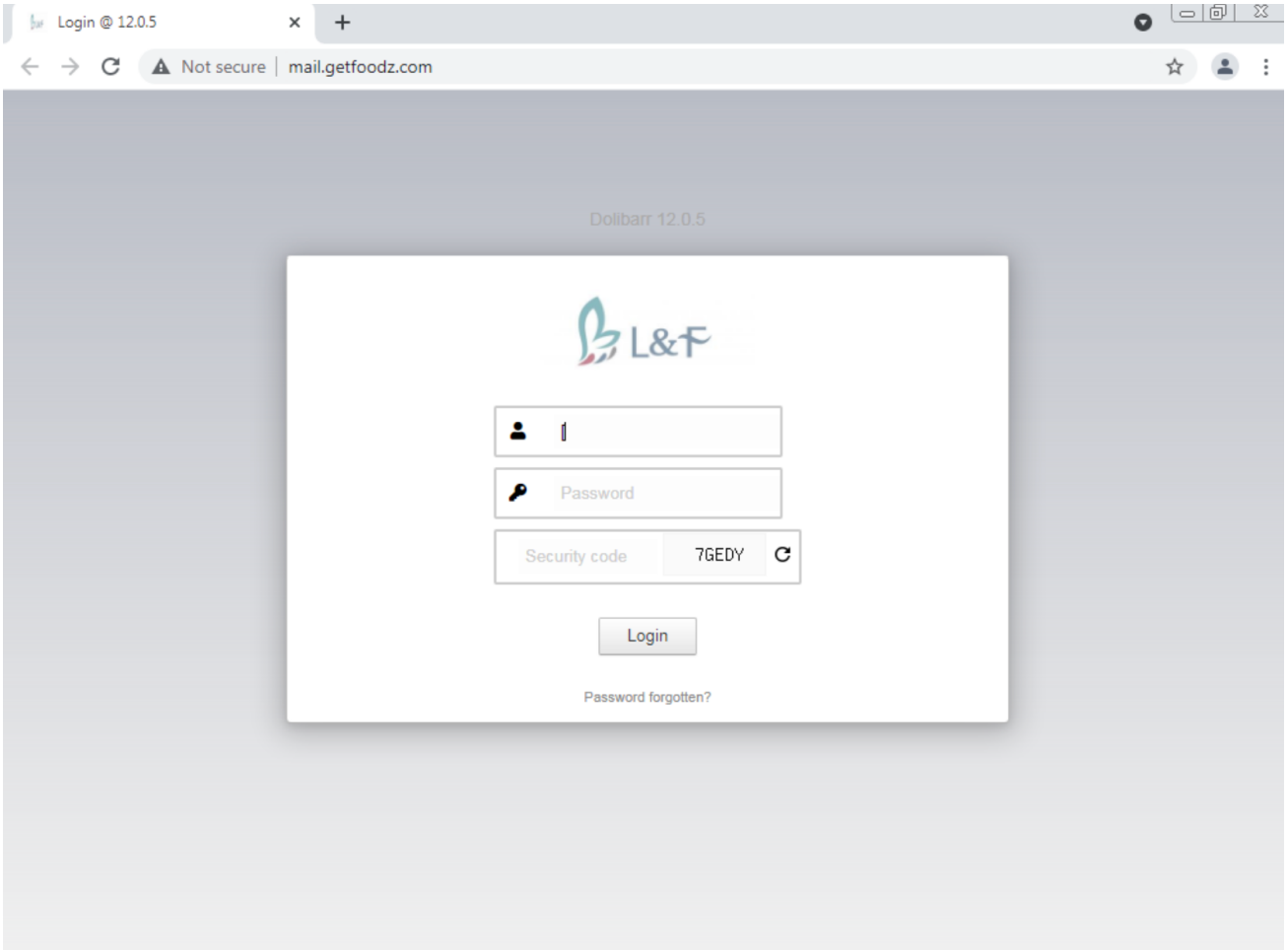
Here's a few domains that we uncovered by following an IP chain that originated with the Dolibarr panel:



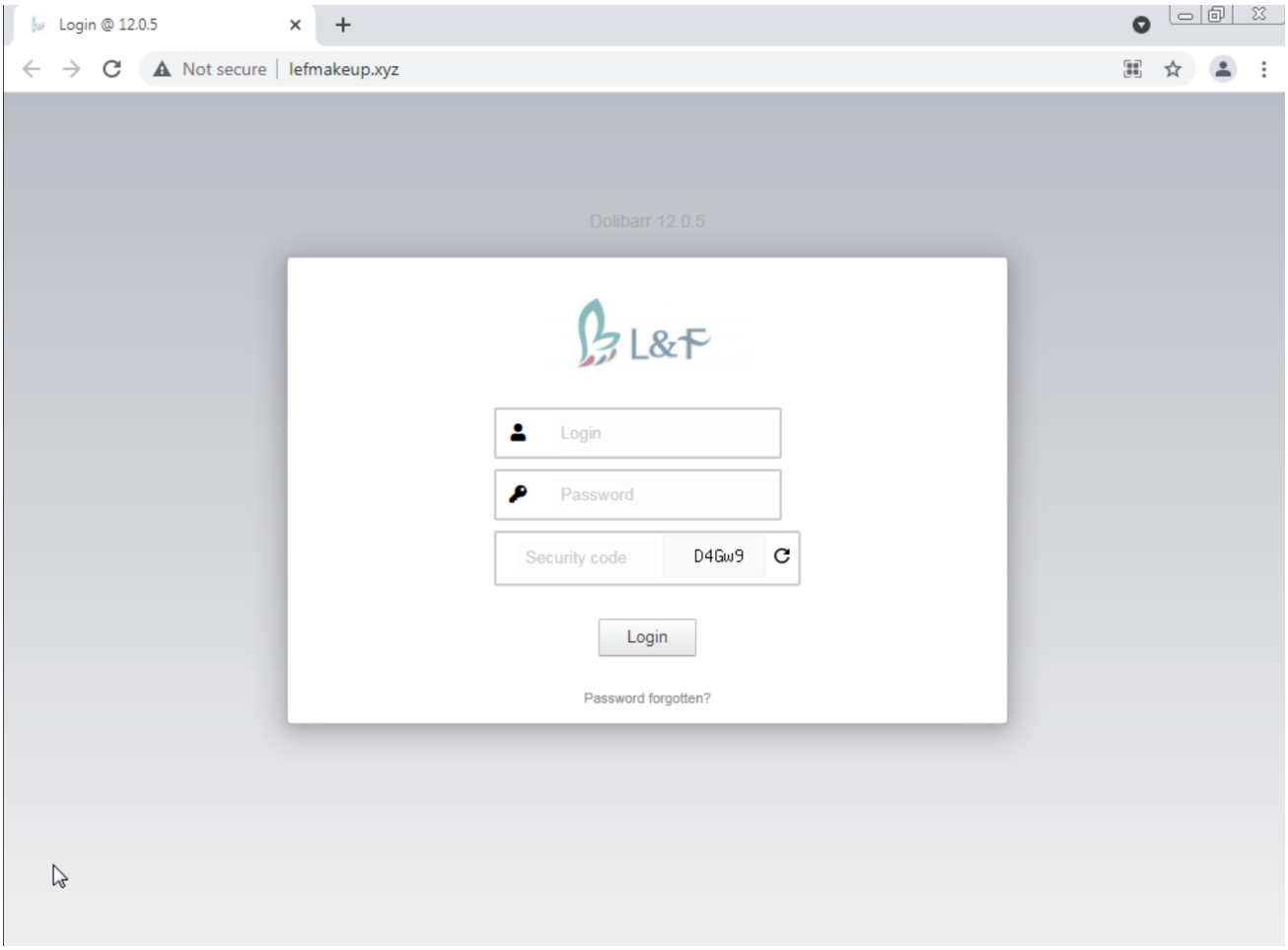

twilio
Sign In
Username
Remember me
Next
Need help signing in?


Powered by Okta
Privacy Policy
https://twilio.okta.com.online-procedure.id
12
twilio
Sign In
Username
Remember me
Next
Need help signing in?

It didn't stop there. Once we'd set about mapping out the threat actors DNS infrastructure, we discovered numerous other websites with the same portal attached to them:



Domain - mail.getfoodz[.]com



Domain - lefmakeup[.]xyz

-sso and -okta domains targeting other companies

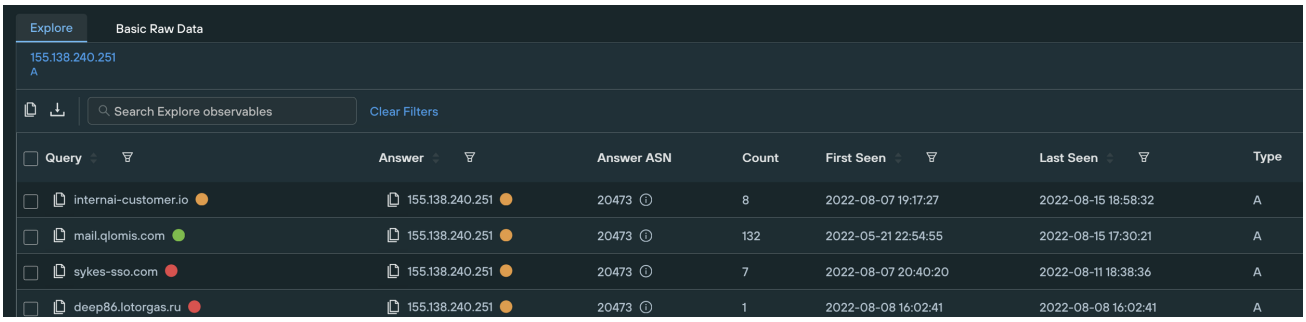
Threat actors cast their nets far and wide. Social engineering is a numbers game - the more users they can get in front of, the more chance they have of harvesting authentication data.

This particular threat actor also created phishing targeting other companies - Accenture, Microsoft, Manpowergroup, Sykes, Telus, TTEC, iQor, and Rogers Communication.

After we'd consolidated our results, a pattern started to emerge - all of the above organisations provide some sort of **communication service** (UCaaS, VOIP, messaging etc.) and most of them facilitate a service that allows companies to communicate with their customer base, and vice versa.

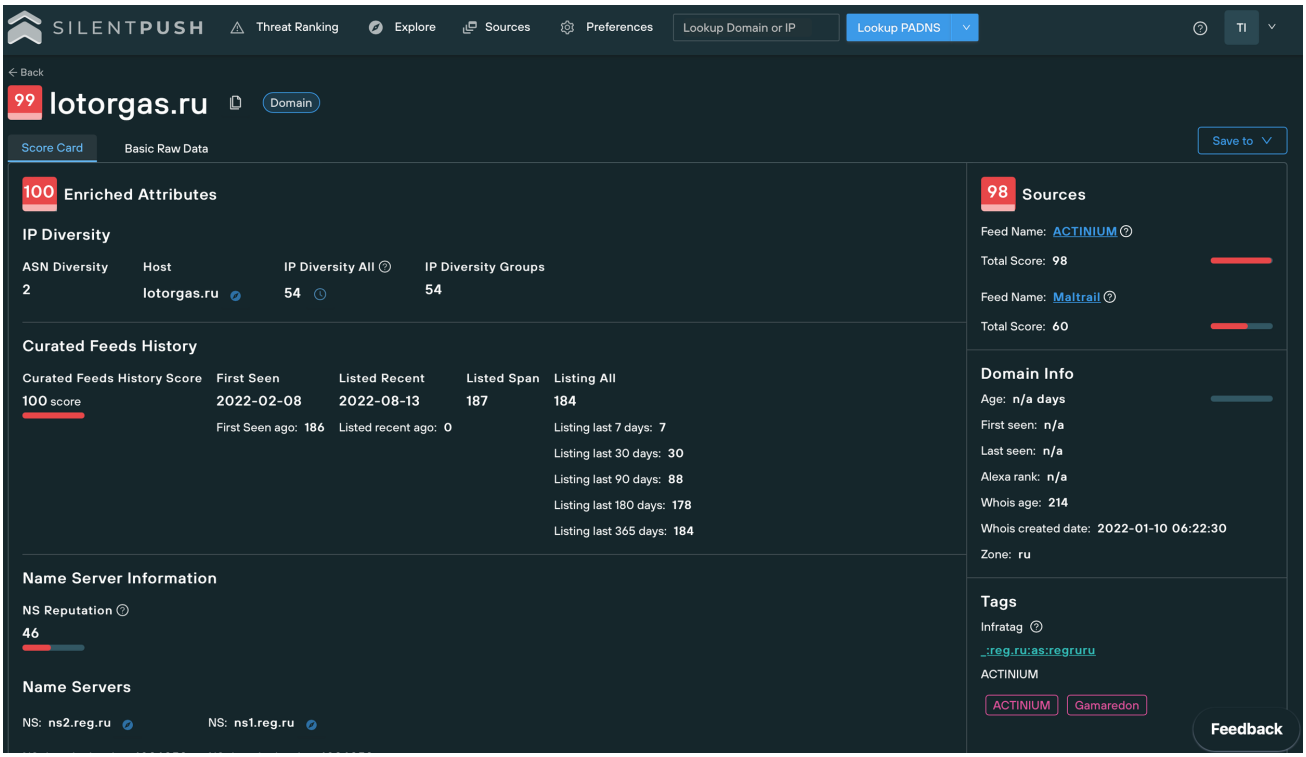
This particular group of threat actors clearly think that online SSO portals are less likely to be questioned than other forms of cloud-based authentication, and for good reason - information is a commodity, and SSO login information commands top dollar.

Some of the malicious -sso and -okta domains we discovered were hosted on infrastructure also used by the ACTINIUM group within the same time frame - threat actors that the Ukrainian Government have publicly linked to the Russian Federal Security Service.



Time overlap of campaign with Actinium group on the same infarstructure.

With the right security tools and search methodologies in place, threat sources aren't particularly difficult to uncover. As an example `sykes-sso[.]com` is hosted on `155.138.240[.]251`. The same IP that contains several subdomains of `lotorgas[.]ru` - a well-known part of ACTINIUM's DNS infrastructure.



lotorgas[.]ru - part of the ACTINIUM threat feed

Twilio was just one of many targeted organizations. There are numerous mini campaigns here targeting different types of organization. Each category of target gives the attacker potential access to many other organizations. For example, one set of targets are Business Process Outsourcing companies like Arise. Another is transactional email companies like Sendgrid and Mailchimp.

We reveal some of the IOCs associated with these campaigns below. We are still tracking more of this infrastructure in different categories of targeted organization. For a comprehensive live feed, subscribe to the service.

How Silent Push helps companies prevent phishing attacks

Silent Push's proprietary scanning software maps out the Internet's entire IPv4 infrastructure, every day - all 4,294,967,296 addresses - allowing us to provide an up-to-date assessment of risk levels and malicious activity at any given time. We also re-resollve all DNS every day and make behavior attributes from the changes.

We have the most complete view of the entire internet every day and its changes.

Public DNS infrastructure gives you your first insight into all manner of attack vectors - not just SMS phishing and SSO spoofing.

Organizations need to monitor the larger extended attack surface for infrastructure targeting them and take up-front blocking action on it to prevent attackers finding ways in.

Our platform features a detection-focused analytics engine that provides organizations with a top-down view of changes to their infrastructure, any domains of interest and critical DNS variables - including NS and AS records - that keeps them one step ahead of threat actors, and ensures they don't end up on the wrong end of a global news report.

We will provide you with daily threats that are targeting your organization.

Reference information

URLS with a compromised Dolibarr control panel

`orderlyfashions[.]com`

`mail.getfoodz[.]com`

`lefmakeup[.]xyz`

`*.orderlyfashions[.]com`

`*.getfoodz[.]com`

`*.lefmakeup[.]xyz`

Phishing domains related to the same control panel

`twilio.okta-access[.]com`

`twilio.okta-teams[.]com`

`twilio.okta.com-helpdesk[.]id`

`twilio.okta.com-oauth2[.]id`

`twilio.okta.com-portal[.]id`

`twilio.okta.com-workspace[.]id`

`twilio.okta.com.globalchange[.]id`

`twilio.okta.com.online-procedure[.]id`

`twilio.okta.com.system-revamp[.]id`

`twilio.okta.system-revamp[.]id`

`twilio.oktaportals[.]com`

`twilio.oktaservice[.]com`

`twilio.oktasignin[.]com`

`twilio.oktaworkspace[.]com`

`www.twilio.okta.com-update[.]online`

`www.twilio.okta.com.globalchange[.]id`

`www.twilio.okta.com.online-procedure[.]id`

`www.twilio.okta.com.system-revamp[.]id`

`www.twilio.okta.system-revamp[.]id`

Phishing domains targeting other companies

`accenture-sso[.]com`

`arise-okta[.]com`

`att-sso[.]com`

`bandwith-okta[.]com`

`coin-base-okta[.]com`

`concentrix-sso[.]com`

`iqor-duo[.]com`

`iqor-duo[.]net`

`iqor-sso[.]net`

mailchimp-help[.]com

`manpowergroup-sso[.]com`

`microsoft-sso[.]net`

`rogers-sso[.]com`

`rogers-help[.]net`

`sitel-sso[.]com`

`sykes-sso[.]com`

`t-mobile-okta[.]net`

`t-mobile-okta[.]org`

`t-mobile-sso[.]net`

`teleperformance-ssovcom`

`telus-sso[.]com`

`tmo-sso[.]com`

`transcom-sso[.]com`

`ttec-sso[.]com`

`twiiio-okta[.]com`

`twiiio-sso[.]com`

Linked IP addresses

`143.198.156[.]234`

`146.190.42[.]89`

`146.190.44[.]66`

`147.182.201[.]149`

`149.248.62[.]54`

`155.138.240[.]251`

`161.35.119[.]80`

`164.92.122[.]3`

`167.172.131[.]89`

`167.99.221[.]10`

`45.32.212[.]77`

`45.32.66[.]165`

`45.63.39[.]151`

`45.76.80[.]199`

`66.42.91[.]138`

`66.42.90[.]140`

`185.173.37[.]140`

`77.232.40[.]101`

`185.244.181[.]186`

`64.52.80[.]26`

`45.61.136[.]168`

`185.173.38[.]46`

Name *
Thank you!

The Team