auth0

The State of Secure Identity

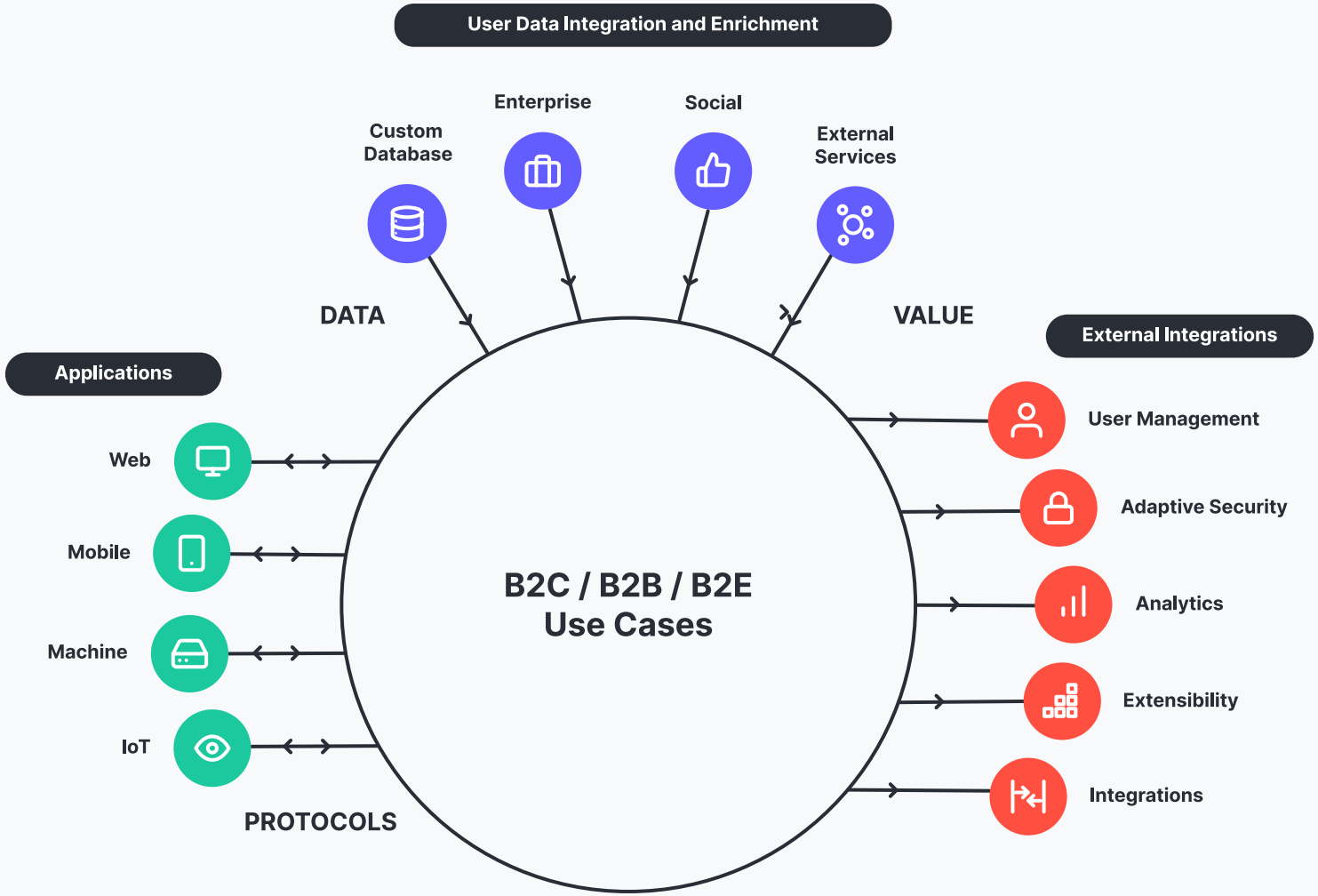
Published May 2021

Overview

Digital identities are already commonplace, controlling access to an assortment of online applications and services. However, security professionals often aren't given the time or resources to give identity the attention it deserves.

The report aims to increase the awareness of identity attacks and give security professionals data they can use to protect their organizations.

What is Identity-as-a-Service



Key Definitions

Bots

A bot is a computer program designed to perform tasks, such as logging into a website with a predefined list of username and passwords.

Account Takeover

A form of identity theft, where a malicious third party successfully gains access to a user's account credentials.

Common Attacks

- Credential stuffing
- Injection attacks
- Authentication bypass

Credential Stuffing

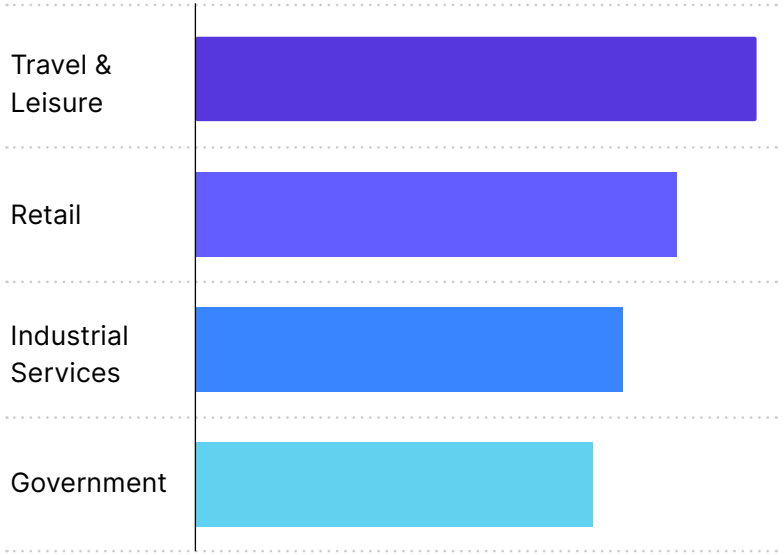
Automated attempts to compromise a large number of user accounts with stolen credentials.

Malicious Traffic

Authentication traffic that is consistent with that of an identity attack.

Key Research Findings

Industries hit the most by Credential Stuffing Attacks



Food & Beverage sector is the most targeted (within Travel & Leisure)

39%

Of **IP addresses** associated with credential stuffing attacks are based in the United States

15%

Of **account registration** results in a failure

Industries that account for more than 50% of SQL injection attacks

Financial services leads in MFA adoption, followed by technology and industrial services

Most users choose email or SMS as their MFA factor, however, most applications with Auth0 MFA utilize time-based one-time passcode

Research Results

Report Contents

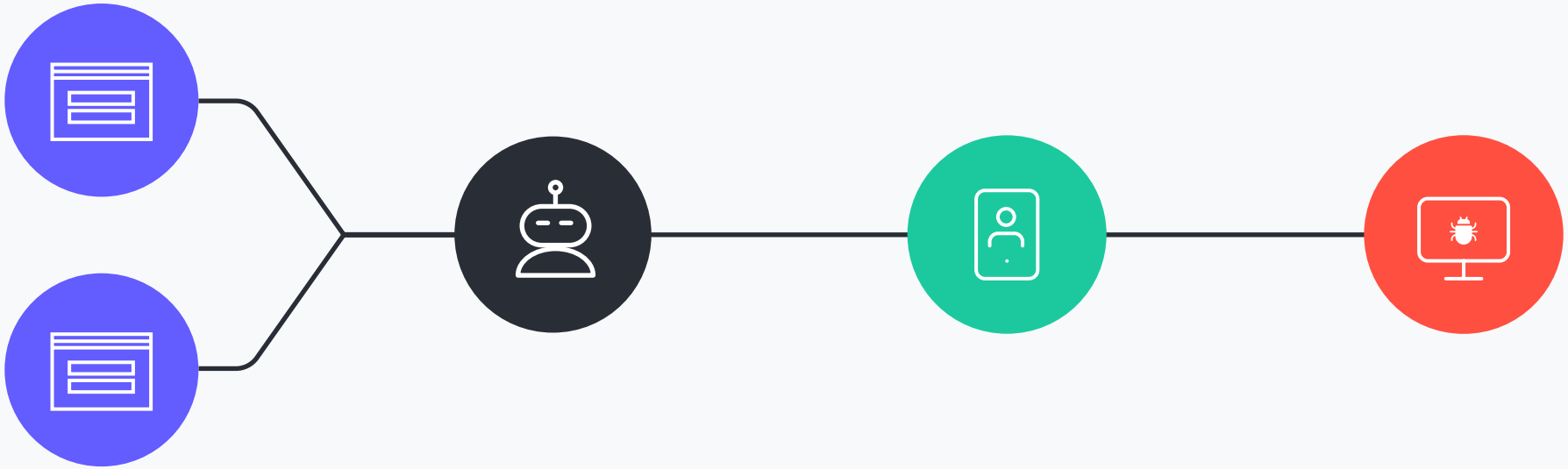
01.

CREDENTIAL STUFFING

Credential stuffing attacks are one of the biggest threats facing identity systems

Credential Stuffing

Credential stuffing attacks target users who reuse passwords.



For reference, here is the price criminals will pay...

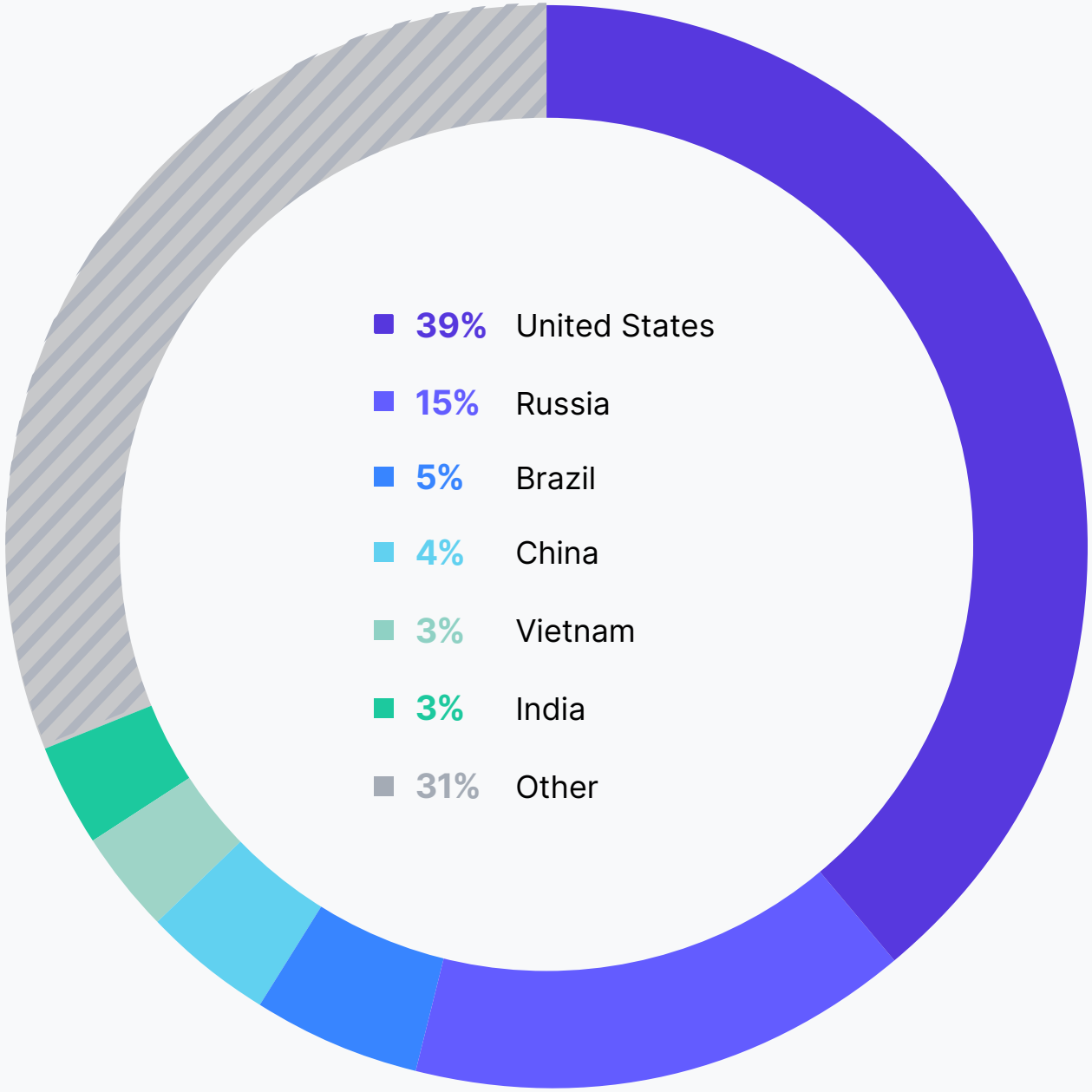
Credit card record	$14-$1000
Crypto account	$350-$810
Social media account	$2-$80
Netflix account	$44
Adobe creative cloud	$160
Private USA dentists database - 122k records	$50

Credential stuffing attacks accounted for 16.5% of login traffic on the Auth0 platform, with daily peaks reaching higher than 40%.

The most targeted organizations and the originating IP addresses of most credential stuffing attacks are in the United States of America.

Most Credential Stuffing Attacks are attributed to US-based IP addresses

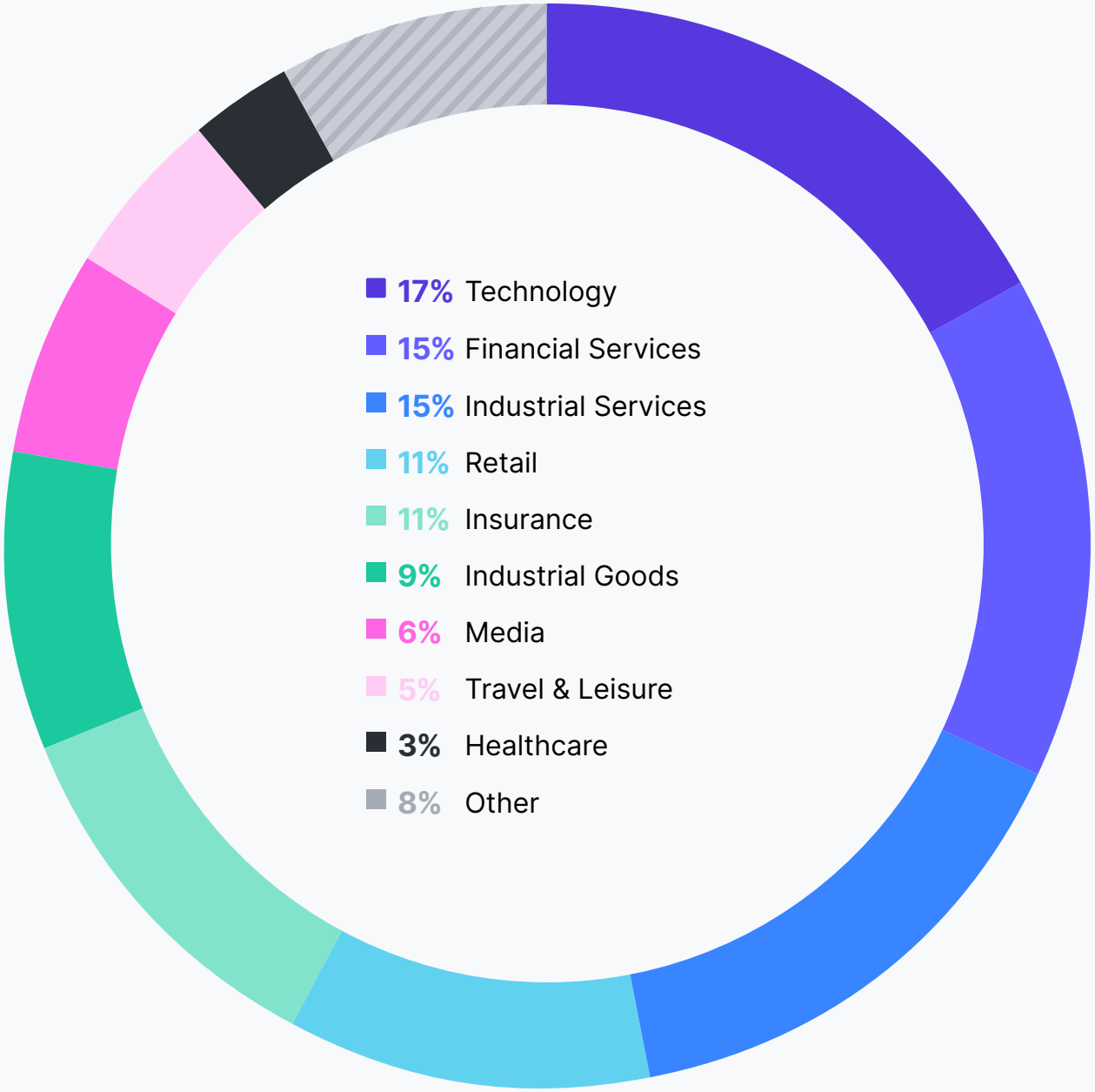
Geolocation of IP addresses associated with Credential Stuffing Attacks



What industries are attempting to thwart credential stuffing attacks via a risk-based CAPTCHA using Auth0 Bot Detection?

Bot detection is adopted most by technology, financial and industrial services, retail, and insurance

Bot detection adoption by industry



In March 2021, Bot Detection was triggered 11,312,051 times

Travel and Retail are targeted the most by brute attacks activities

Top industries targeted by brute force attacks

01. Travel and Leisure

02. Retail

03. Government

04. Industrial Services

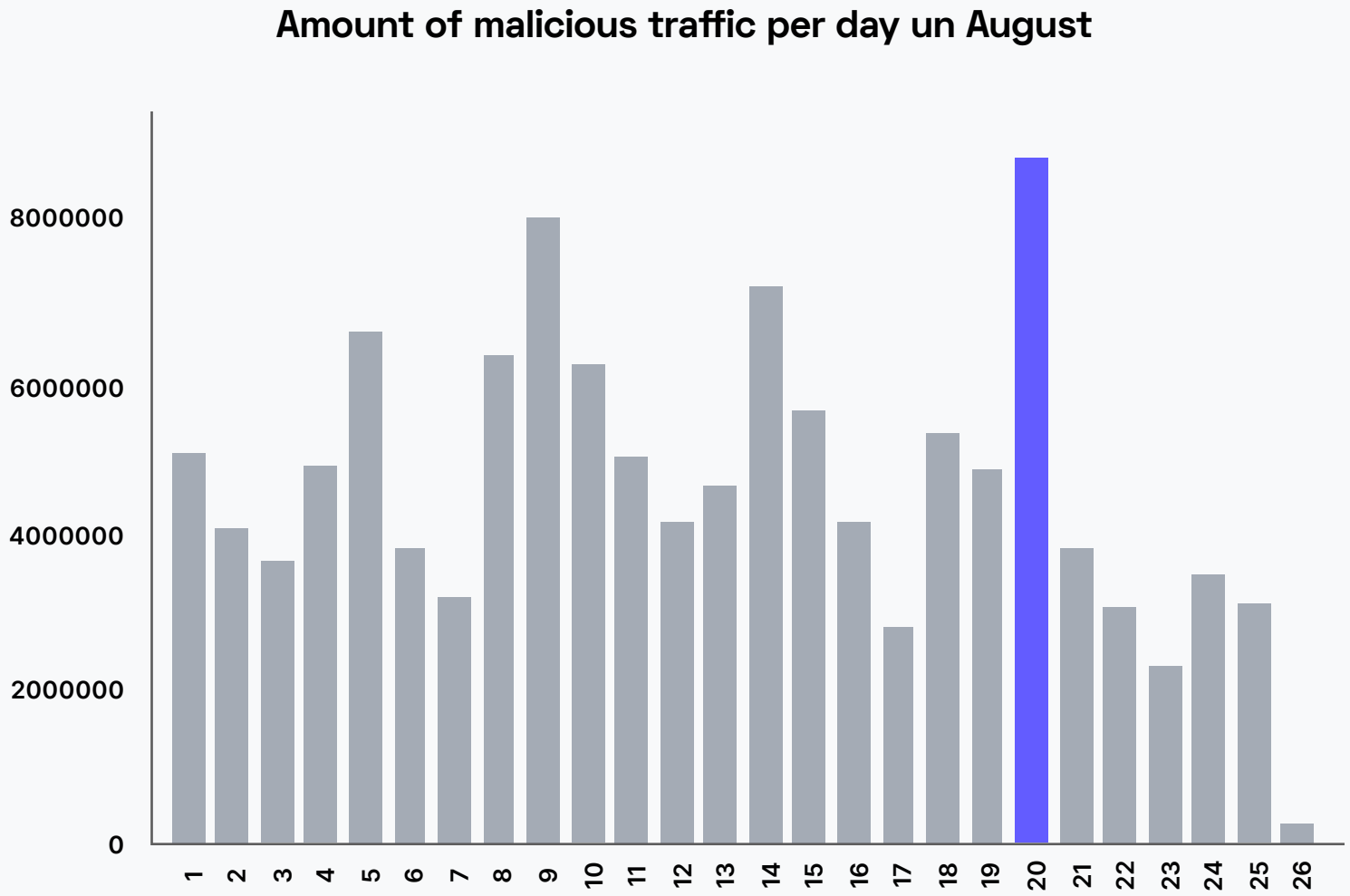
05. Technology

Within Travel and Leisure,
the Food and Beverage sector is the most targeted segment by attackers.

What does an attack look like
For one of the most targeted restaurants?

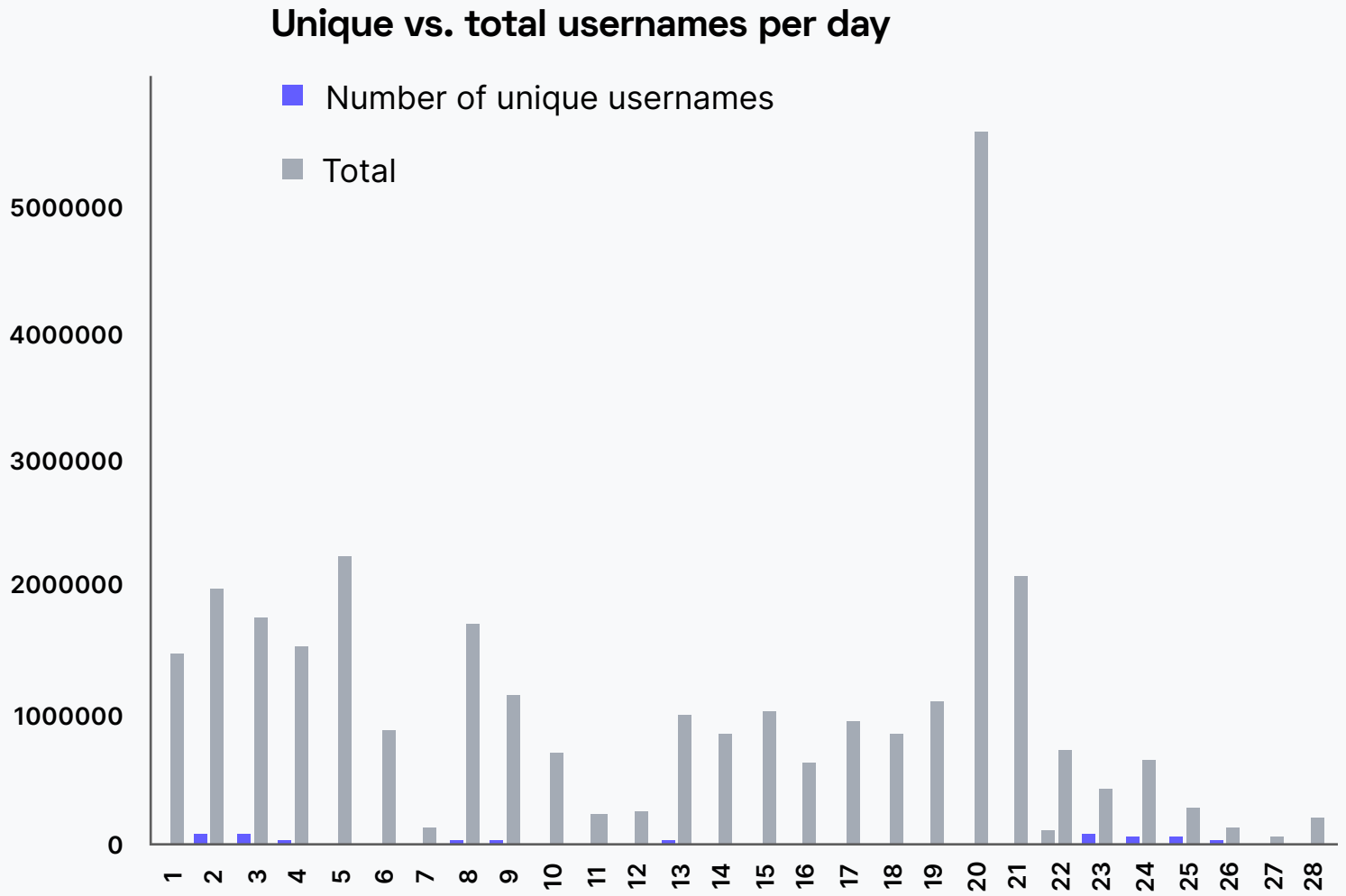
Daily spikes in malicious traffic

In particular, August 20 saw the largest amount of malicious traffic.



The same usernames are targeted over and over.

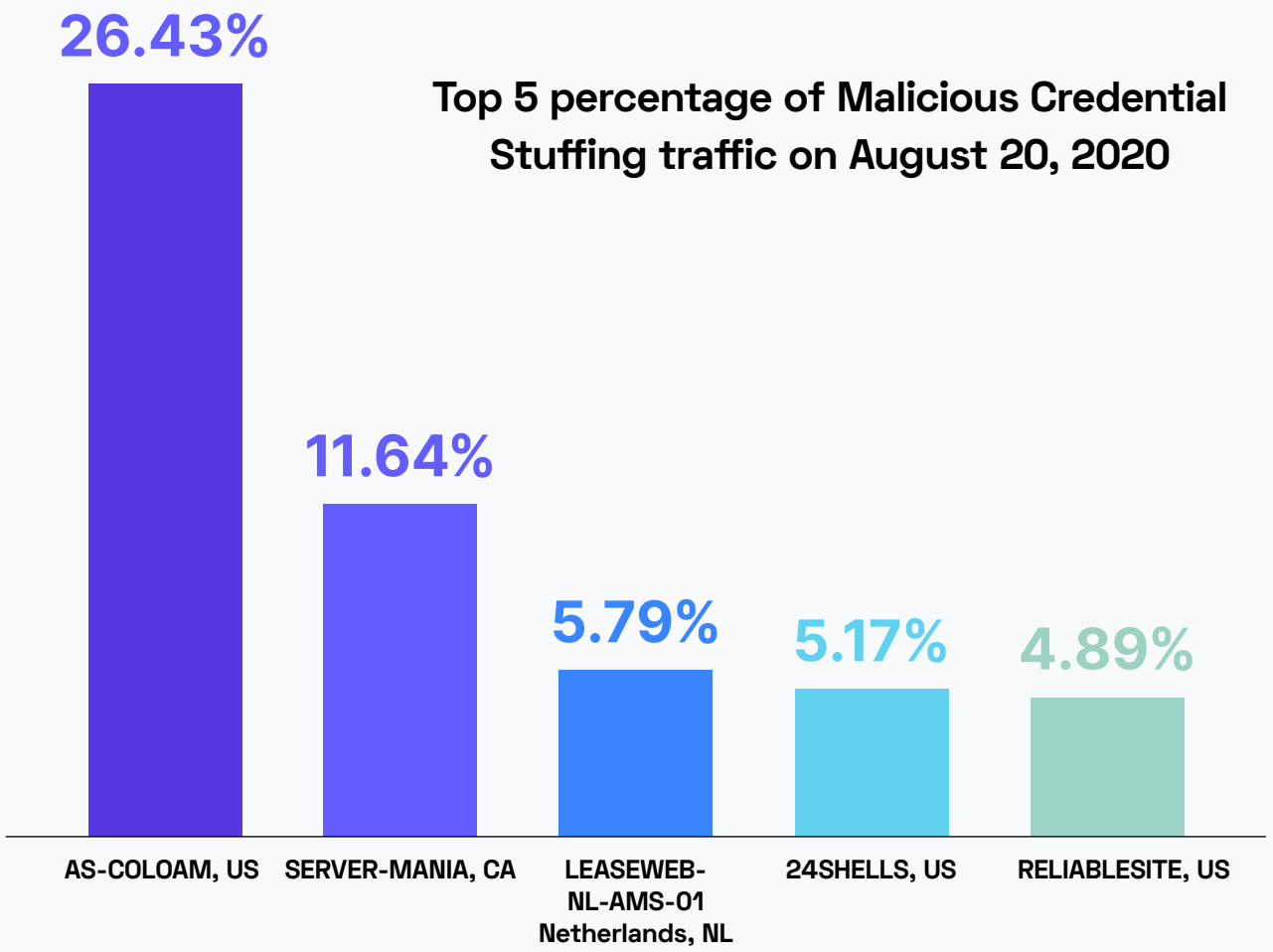
Large traffic volume with few unique usernames, indicating these usernames are being attacked.



Large amounts of traffic with a low number of unique username can be a sign of a credential stuffing or brute force attack.

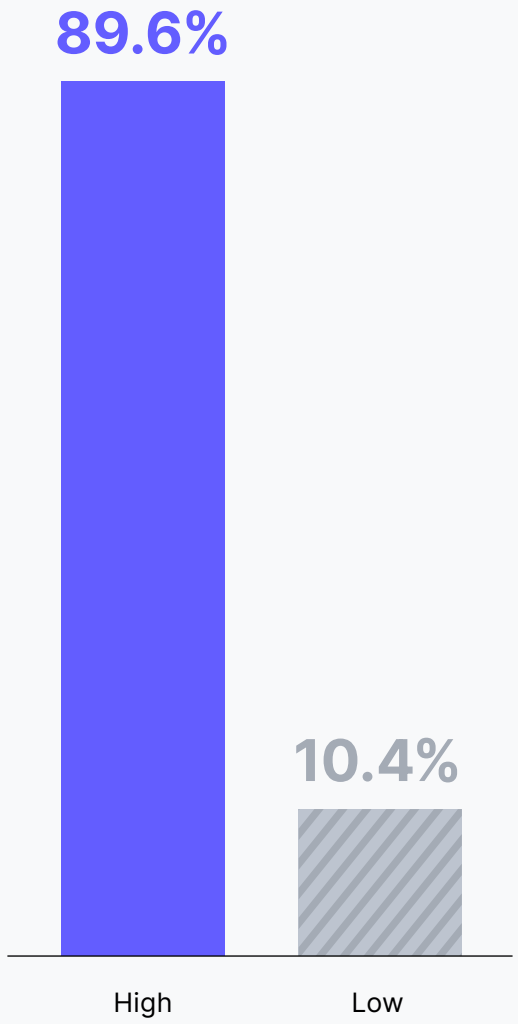
Where is it coming from?

Most of the malicious traffic is coming from the same colocation services, suggesting it is part of a single attack.



This attack is using a small number of colocation services, which allow customers to rent their hardware, launch their attacks.

Most requests are coming from IP address deemed “high risk,” which makes them detectable using IP reputation data



High and low risk correlating
Open Source Intelligence

This restaurant is experiencing a credential stuffing attack

Why is it being targeted?

It offers a rewards program that grants befenits to loyal customers.

Auth0 often see rewards programs targeted because they are rarely secured well and the benefits are easily motenizied.

“If you read the news, you hear more of these account takeover attacks and more usernames and passwords showing up from breaches at other companies exposing more and more data.”

- Scott Scherer, CIO at Jersey Mike’s, on protecting their digital customers from credential stuffing attacks

“If you read the news, you hear more of these account takeover attacks and more usernames and passwords showing up from breaches at other companies exposing more and more data.”

—Scott Scherer, CIO at Jersey Mike’s, on protecting their digital customers from credential stuffing attacks

02.

INJECTION ATTACKS

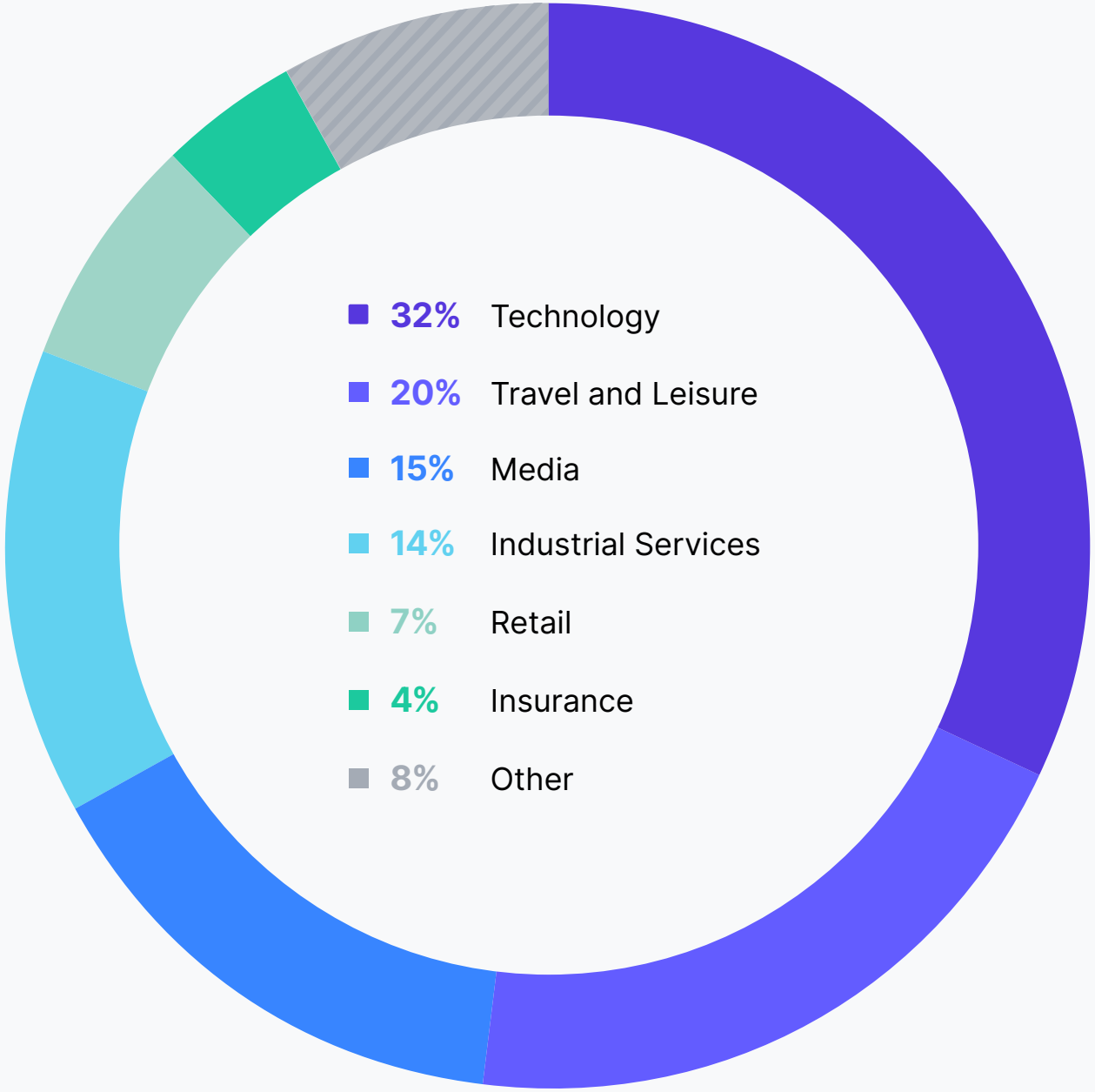
These attacks are high impact and often take advantage of vulnerable identity implementations

Injection attacks are the
top web application security risk
according to OWASP.

Injection Attacks

Injection attacks against identity systems use arbitrary code execution to bypass authentication.

Top industries targeted by SQL injection attacks in Q1 2021



03.

ACCOUNT CREATION ATTACKS

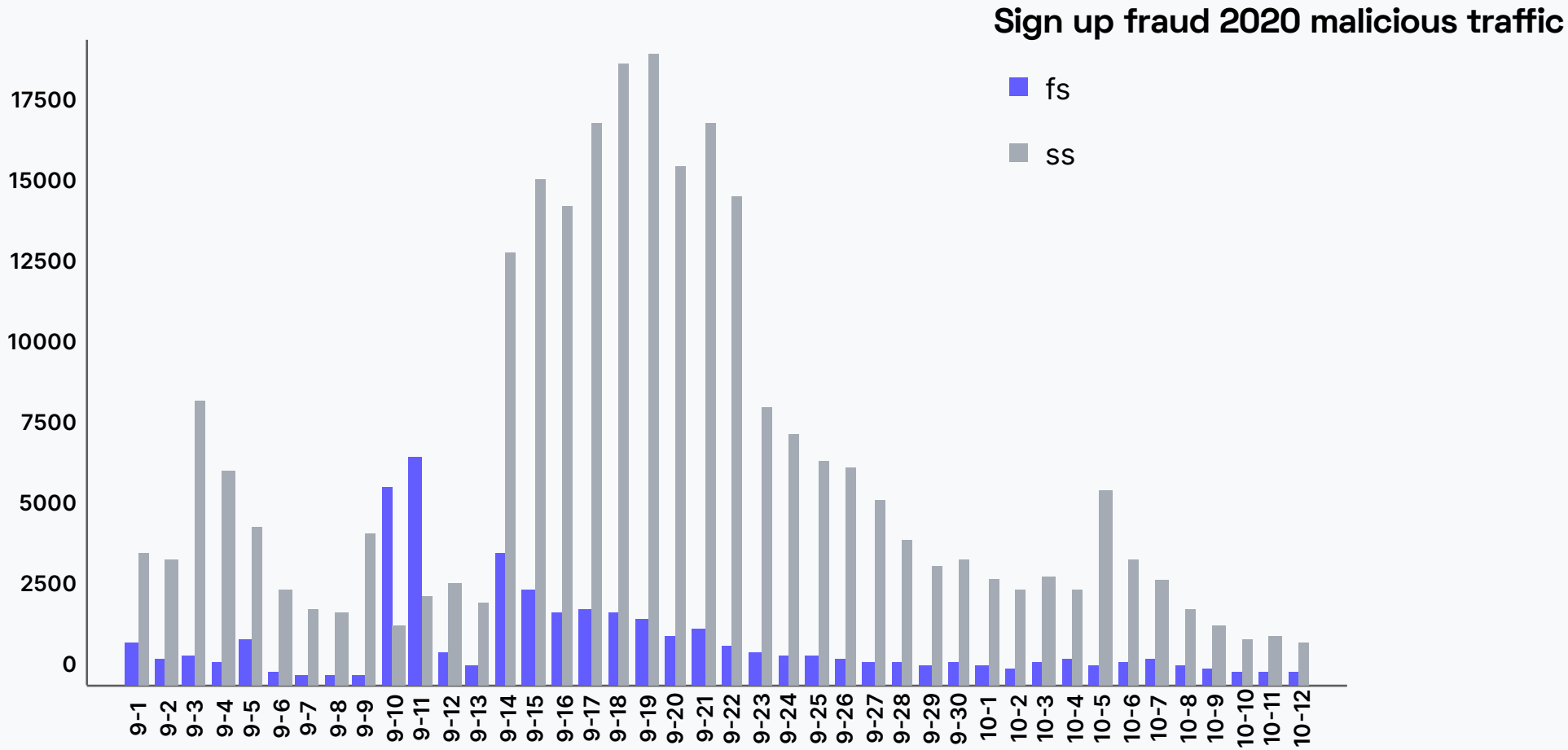
Attackers may create large numbers of fake accounts to take advantage of signup bonuses, spread misinformation, or to cause damage

Account Creation Attacks

Account creation attacks involve creating a large number of fake sign ups. Attackers may do this for a variety of reasons from taking advantage of sign-up bonuses, causing damage, or spreading misinformation.

Roughly 15% of all registration attempts result in failure. Much of this is driven by threat actors creating puppet accounts.

A large spike in failed sign-up attempts indicates the beginning of an attack.



Failed a sign up attempts are relatively rare. A spike in failed sign ups could be a sign of account creation attack.

The attack is originating from all over the world. There is very little pattern, suggesting it is a manual, non-automated attack.

These new accounts were mostly created using free email services, which make it easy for attackers to create a large number of email addresses.

Top email services used in the attack

01. Gmail.com

02. 163.com

03. Hotmail.com

04. Mail.ru

05. Yahoo.com

This particular customer offered free cryptocurrency with sign ups.

It is likely this account creation attack was used to gather as much of that free cryptocurrency to turn a profit.

04.

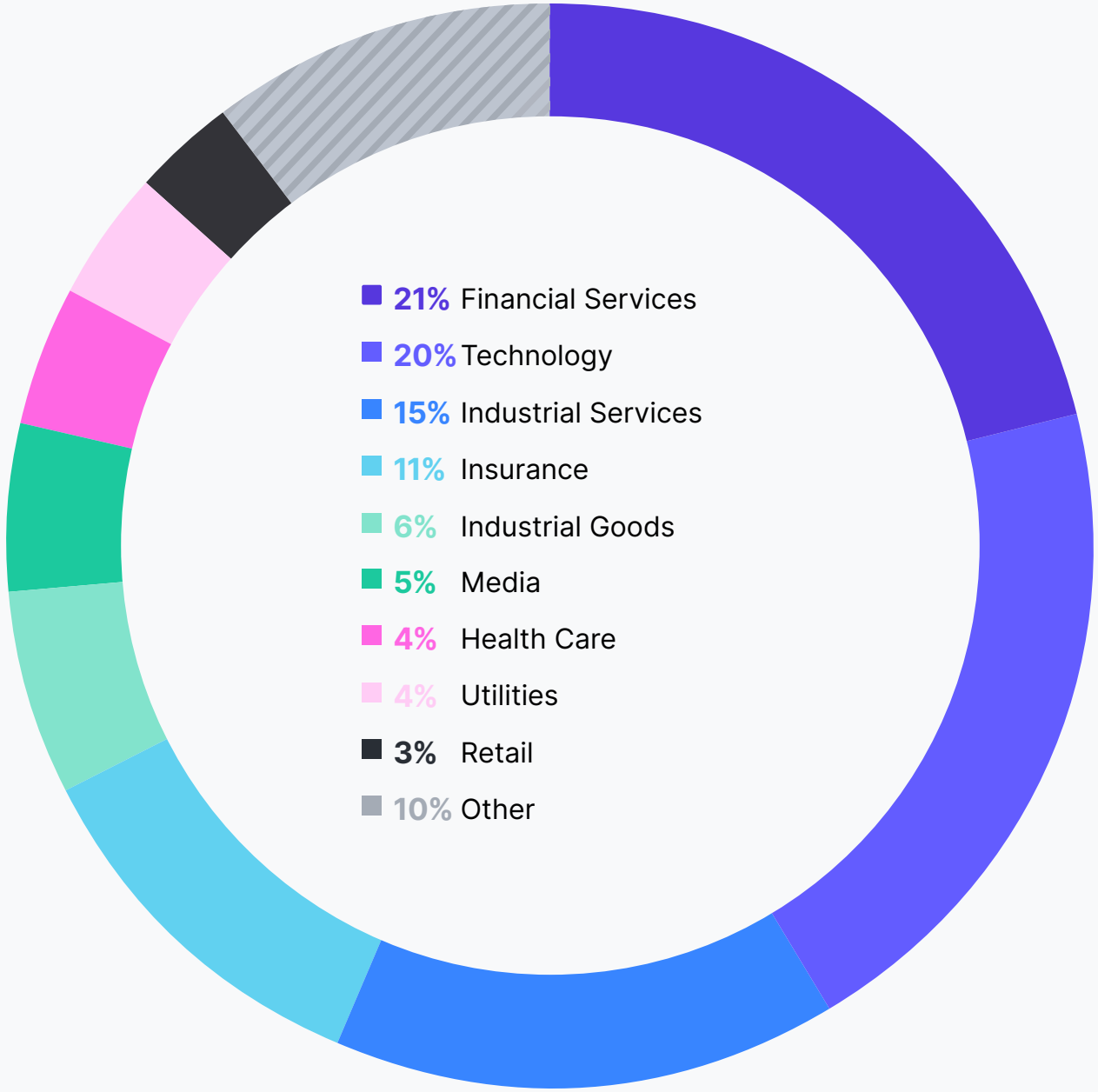
MULTIFACTOR AUTHENTICATION

MFA is one of the most effective defenses against attacks

Multifactor Authentication is one of the best defenses against account takovers.

Financial services and technology lead in MFA adoption

MFA adoption by industry



Time-based OTP and SMS are the leading types of MFA offered in applications

Top MFA types by application count

01. Time-based one-time password
02. SMS
03. Recovery code
04. Push notification
05. Email
06. WebAuthn
07. Voice

However, users are mostly enrolled email or text message MFA

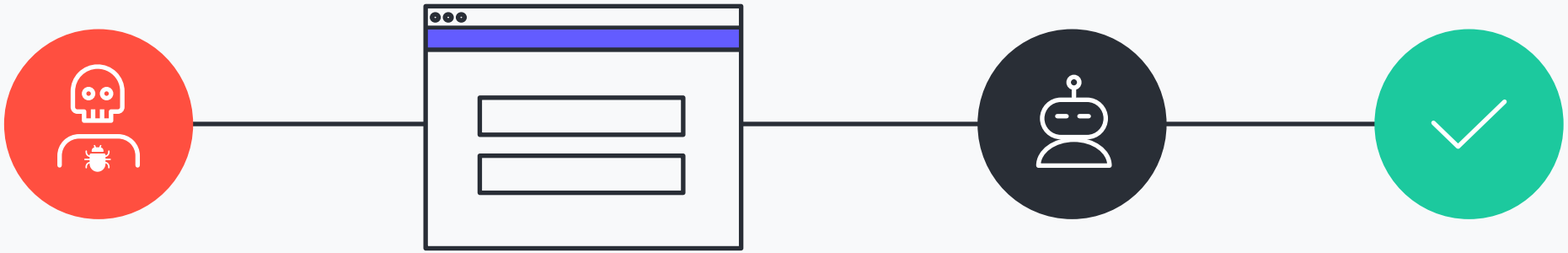
Top MFA types by user count

01. Email
02. SMS
03. Time-based one-time password
04. Push notification
05. Recovery code
06. Voice
07. WebAuthn

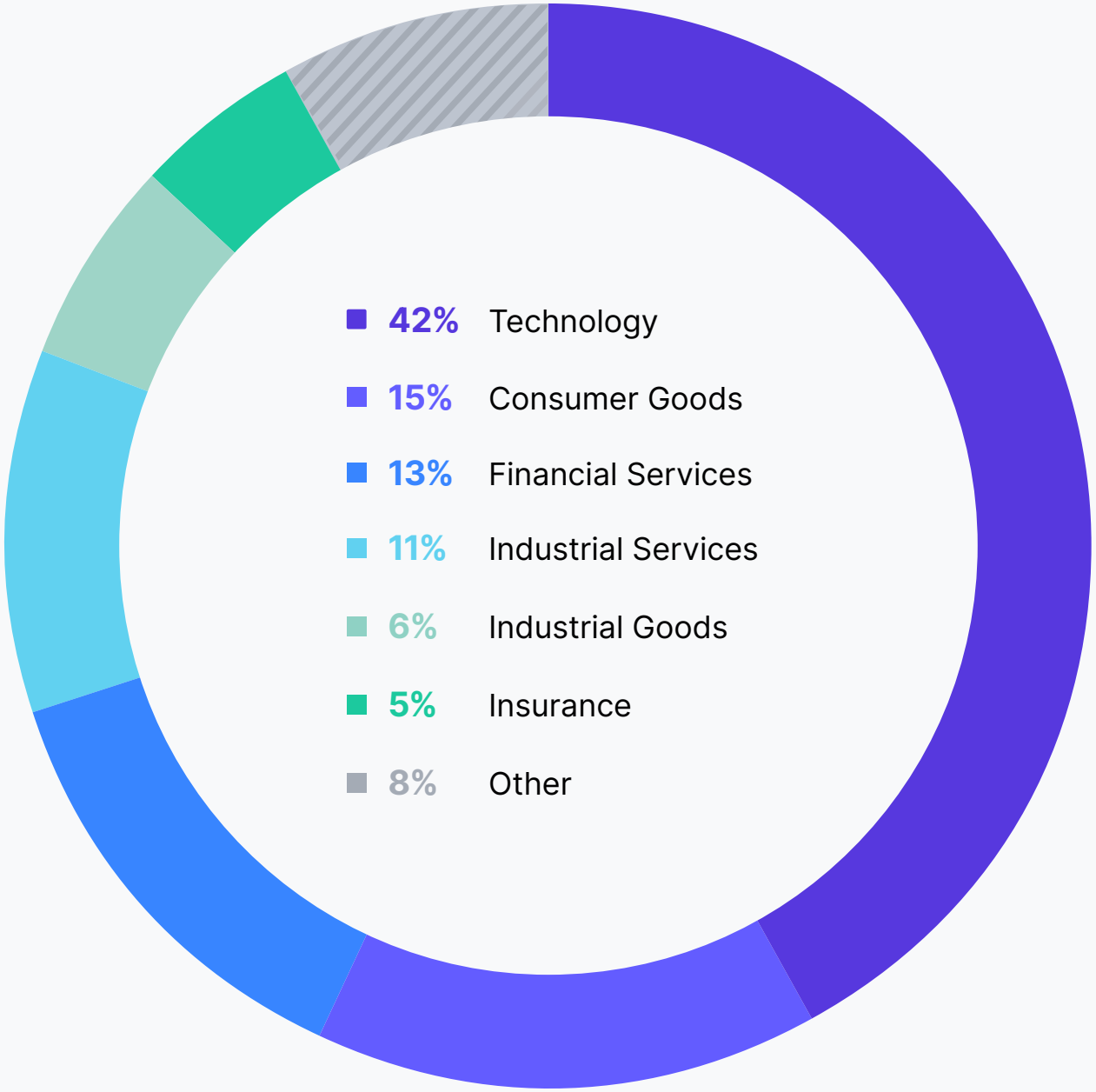
MFA often protects high-value accounts and could be targeted in MFA bypass attacks.

MFA Bypass Attacks

MFA bypass attacks involve the attacker circumventing MFA challenges, such as by brute forcing the one-time passcode.



The tech industry experiences the most MFA brute force attempts



In the first four months of 2021, Auth0 observed 87,526 MFA bypass attempts.

Auth0 provides a platform to authenticate, authorize, and secure access for applications, devices, and users. Security and application teams rely on Auth0's simplicity, extensibility, and expertise to make identity work for everyone. Safeguarding more than 4.5 billion login transactions each month, Auth0 secures identities so innovators can innovate, and empowers global enterprises to deliver trusted, superior digital experiences to their customers around the world.

For more information, visit **auth0.com** or follow **@auth0** on Twitter.