How to Block Anonymizing Services using Okta

By Moussa Diallo and Brett Winterford

Published: 2024-04-27 · Archived: 2026-04-05 14:25:23 UTC

Over the last month, Okta has observed an increase in the frequency and scale of credential stuffing attacks targeting online services, facilitated by the broad availability of residential proxy services, lists of previously stolen credentials (“combo lists”), and scripting tools.

- From March 18, 2024 through to April 16, 2024, Duo Security and Cisco Talos observed large-scale brute force attacks on multiple models of VPN devices.
- From April 19, 2024 through to April 26, 2024, Okta’s Identity Threat Research team observed a spike in credential stuffing activity against user accounts from what appears to be similar infrastructure.

In credential stuffing attacks, adversaries attempt to sign-in to online services using large lists of usernames and passwords obtained from previous data breaches of unrelated entities, or from phishing or malware campaigns.

All recent attacks we have observed share one feature in common: they rely on requests being routed through anonymizing services such as TOR. Millions of the requests were also routed through a variety of residential proxies.

What is the Tor Network?

Tor (The Onion Router) provides its users a method of sending requests to web sites in which the originating source IP address of the request is obscured. Tor relies on the relay of messages across an overlay network of “onion routers”, each of which can only observe the IP of the preceding node and the next node in the communication. While Tor has legitimate uses, it is routinely used to conceal the real IP address of attackers.

What are Residential Proxies?

Residential Proxies are networks of legitimate user devices that route traffic on behalf of a paid subscriber. Providers of residential proxies effectively rent access to route authentication requests through the computer, smartphone or router of a real user, and proxy traffic through the IP of these devices to anonymize the source of the traffic.

Residential Proxy providers don’t tend to advertise how they build these networks of real user devices. Sometimes a user device is enrolled in a proxy network because the user consciously chooses to download “proxyware” into their device in exchange for payment or something else of value. At other times, a user device is infected with malware without the user’s knowledge and becomes enrolled in what we would typically describe as a botnet. More recently, we have observed a large number of mobile devices used in proxy networks where the user has downloaded a mobile app developed using compromised SDKs (software development kits). Effectively, the

developers of these apps have consented to or have been tricked into using an SDK that enrolls the device of any user running the app in a residential proxy network.

The net sum of this activity is that most of the traffic in these credential stuffing attacks appear to originate from the mobile devices and browsers of everyday users, rather than from the IP space of VPS providers. For more information on residential proxy services, we recommend this informative summary by CERT Orange Cyberdefense and Sekoia.

Block it at the Edge

One of the key tenets of the Okta Secure Identity Commitment is to champion customer security best practices. We are committed to raising the bar for default security features in our platforms.

In February 2024, Okta released a well-timed capability into the Okta Platform that detects and blocks requests from anonymizing services.

Organizations that wish to deny access from specific anonymizers, and allowlist others, must first be licensed to use **Dynamic Zones**, which is included in the Adaptive MFA SKU).

Customers using Auth0 should consider the Attack Protection Suite, and consider the other recommendations in the table below.

Modern Defenses, Built into the Identity Platform

The unprecedented scale of these attacks has provided clear insights into the controls most effective against credential stuffing.

ThreatInsight, Okta's built-in control against high volume attacks, blocks requests from IPs involved in large scale credential based attacks prior to authentication.

The small percentage of customers where these suspicious requests proceeded to authentication shared similar configurations: The Org was nearly always running on the Okta Classic Engine, ThreatInsight was configured in Audit-only mode (not Log and Enforce mode), and Authentication policies permitted requests from anonymizing proxies.

Customers using Okta Identity Engine that (a) enabled ThreatInsight in log and enforce mode and (b) deny access requests from anonymizing proxies were protected from these opportunistic accounts. These basic features are available in all Okta SKUs. Upgrading to Okta Identity Engine is free, often highly automated, and provides access to a range of features including CAPTCHA challenges for risky sign-ins and passwordless authentication using Okta FastPass.

Broader Recommendations

We recommend Okta customers practice defense in depth to mitigate the risk of account takeovers from credential stuffing attacks.

	Recommendation	**Okta Workforce Identity and Customer Identity**	**Auth0**
1.	Embrace Passwordless	Require **Okta FastPass** and **FIDO2 WebAuthn**	Support **PassKeys** as a preferred sign-in method
2.	Prevent users from making poor password choices	Require 12 chars and no parts of username in **Password Policy** . Block passwords found in **common password list**	Enable **Breached Password Protection** or **Credential Guard** to prevent use of passwords known to have been breached in 3P sites
3.	Enforce MFA on sign-in	Require MFA in Global Session Policies	Require MFA for Password Authentication flows
4.	Deny requests from locations where your organization does not operate	Use **Network Zones** to block requests prior to authentication	Deny access by location using a WAF or via the Country-based Access Control **Action**
5.	Deny authentication requests from IPs with poor reputation	Deny requests made via anonymizing services via **Dynamic Network Zones** Configure **ThreatInsight** in	Use **Suspicious IP Throttling** to slow down login attempts from suspicious IPs Use **Bot Protection**

		log and enforce mode to deny attempts based on the volume and velocity of failed requests from an IP Require **CAPTCHA** challenges on high risk logins	to present CAPTCHA challenges to requests from suspicious IPs Use 3P **Auth0 Actions** integrations to check if an IP is associated with an anonymizing proxies
6.	Monitor for and respond to anomalous sign-in behavior	Enforce per-user **Account Lockout** . Exempt requests from devices that have successfully authenticated Monitor for **ThreatInsight** events and rate limit violations	Use **Brute-force Protection** to block and lockout accounts subject to persistent failed authentication requests Monitor for sign-in events using invalid usernames/non-existent users and/or previously breached passwords

TTPs used in Recent Attacks

Top 20 ASNs

Autonomous System Number	**Network Provider**
53667	FranTech Solutions
62744	Quintex Alliance Consulting
60729	Stiftung Erneuerbare Freiheit

1101	SURF B.V.
210558	1337 Services GmbH
197540	netcup GmbH
16276	OVH SAS
60404	Liteserver
210644	AEZA INTERNATIONAL LTD
399532	Universal Layer LLC
200651	FlokiNET ehf
44925	1984 ehf
51396	Pfcloud UG
4224	The Calyx Institute
51852	Private Layer INC
56655	TerraHost AS
36352	HostPapa
208323	Foundation for Applied Privacy

63949	Akamai Connected Cloud
41281	KeFF Networks Ltd

User Agent

Mozilla/5.0 (Windows NT 10.0; rv:102.0) Gecko/20100101 Firefox/102.0

Relevant System Log Queries: The Okta Platform

Event	System Log Query
ThreatInsight has Detected Access Requests from IPs Associated with Suspicious Behavior	eventType eq "security.threat.detected"
Suspected Brute Force Attack (T1110.001)	eventType eq "security.threat.detected" AND outcome.reason eq "Login failures"
Suspected Credential Stuffing Attack (T1110.004)	eventType eq "security.threat.detected" AND outcome.reason co "Login failures with high unknown users count"
Suspected Password Spray Attack (T1110.003)	eventType eq "security.threat.detected" AND outcome.reason co "Password Spray"
Targeted Brute Force Attack against a Specific Org	eventType eq "security.attack.start"

Relevant System Log Queries: The Auth0 Platform

Event	Log Query

Failed login request	f
Failed login: Invalid username/email address	fu
Failed login: Invalid password	fp
Login attempt from a known leaked password	pwd_leak
Signup (registration) attempt from a leaked password	signup_pwd_leak
IP address blocked: excessive failed login or registration requests without a successful login	limit_mu
User account lockout: excessive failed login requests per time period from the same IP address	limit_sul
IP address blocked: excessive failed login attempts to a single user account	limit_wc

Brett Winterford is Vice President of Okta Threat Intelligence. Okta Threat Intelligence delivers timely, highly relevant and actionable insights about the threat environment, with a focus on identity-based threats. Brett was previously the regional Chief Security Officer for Okta in the Asia Pacific and Japan, and advised business and technology leaders in the region on all things identity.
Prior to Okta, Brett held a senior security leadership role at Symantec, and helmed security research, awareness and education at Commonwealth Bank. Brett is also an award-winning journalist, editor-in-chief of iTnews Australia and a contributor to the Risky Business podcast and newsletter, to ZDNet, the Australian Financial Review and the Sydney Morning Herald.
