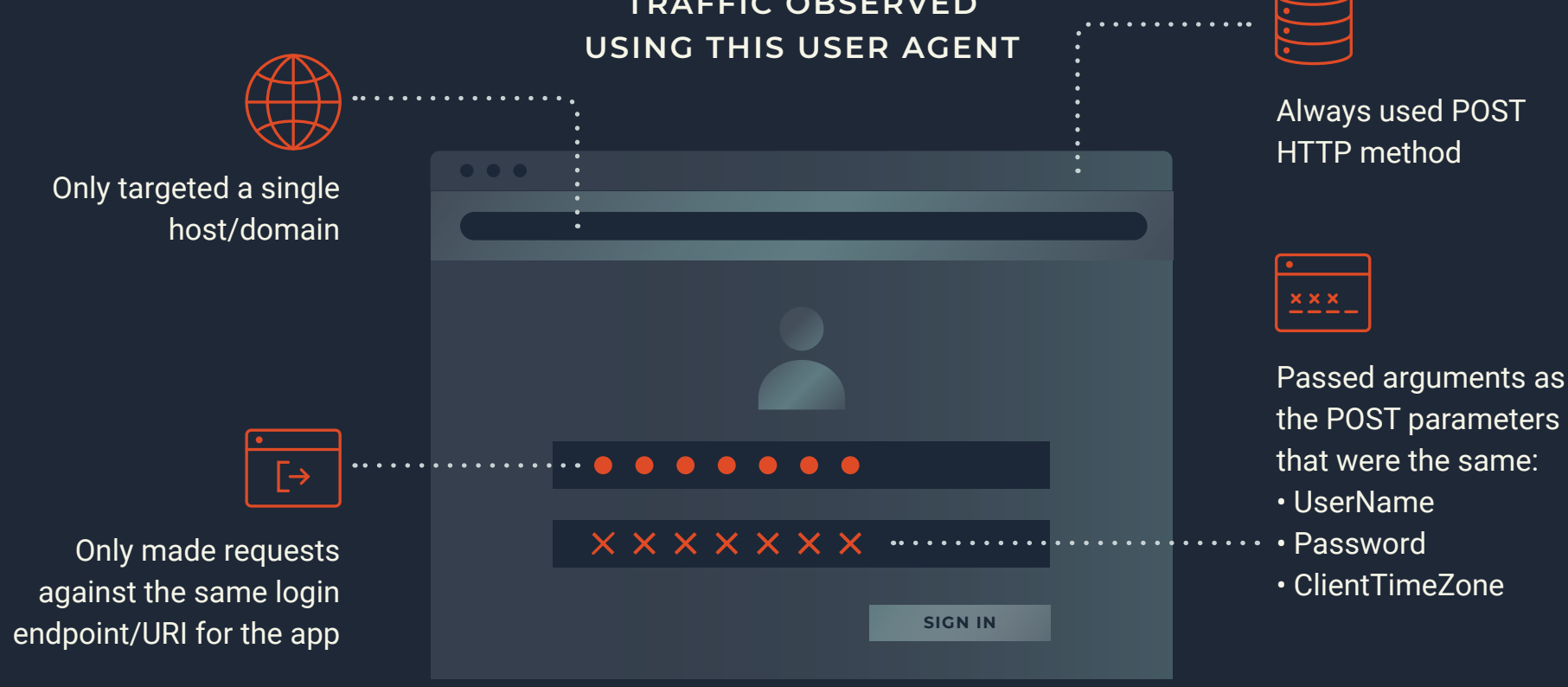


# Anatomy of a Distributed Credential Stuffing Attack

One of ThreatX's customers recently experienced a credential stuffing attack, illustrated below.

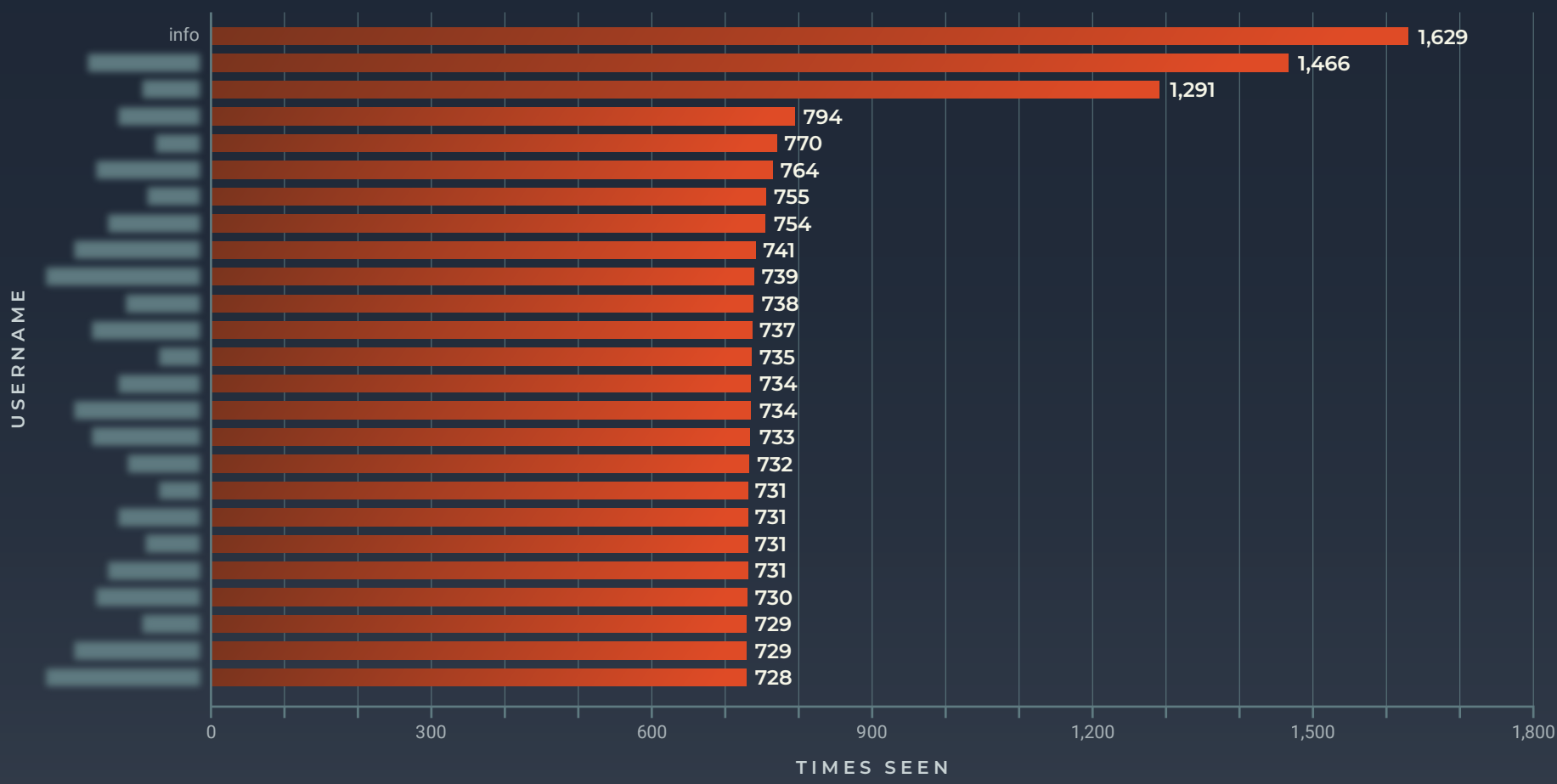
ThreatX identified suspicious traffic from various IP addresses using the following User-Agent header:

gfdfgsdfgsgfdDSFSD3223

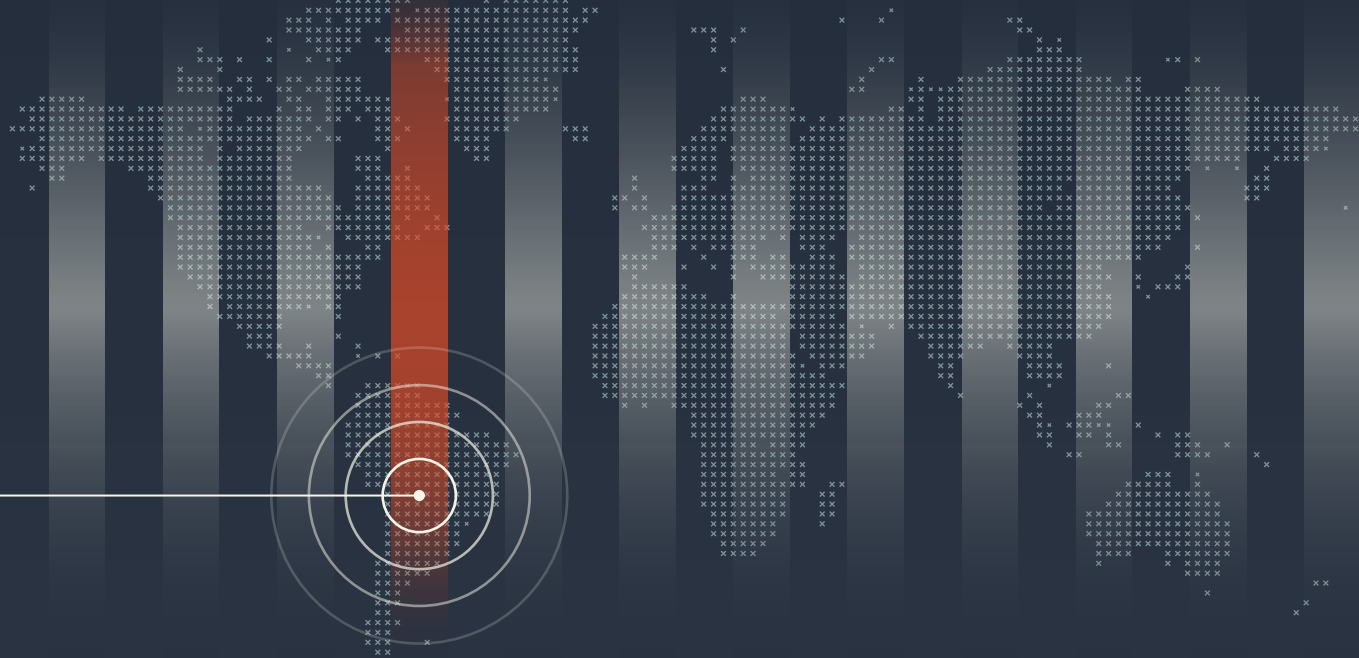


**1.6m+** UNIQUE USERNAMES SEEN ACROSS ALL SUSPICIOUS REQUESTS

Top 25 Usernames Observed

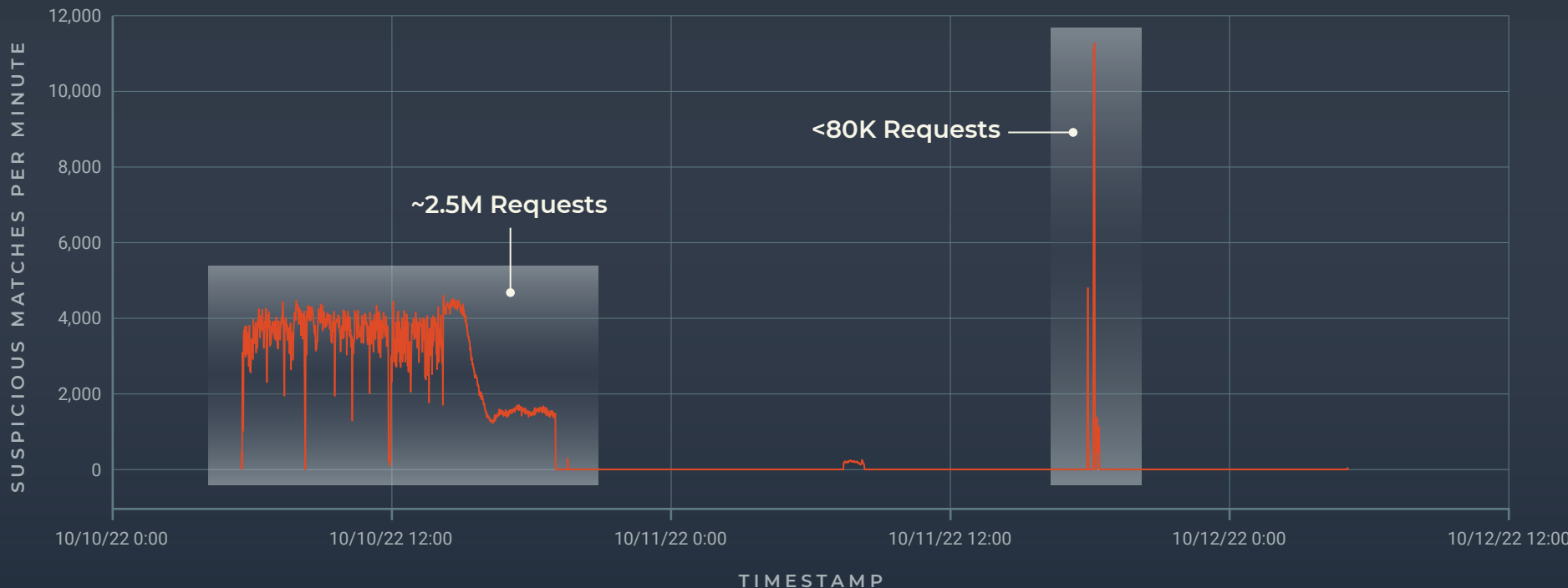


Bot inserted IP addresses as a timezone — suggesting a targeted attack



SUSPICIOUS USER AGENT SHOWS UP IN **2.5m+** requests

Rate of Attack Requests From Fingerprinted Bot Within 48 Hours

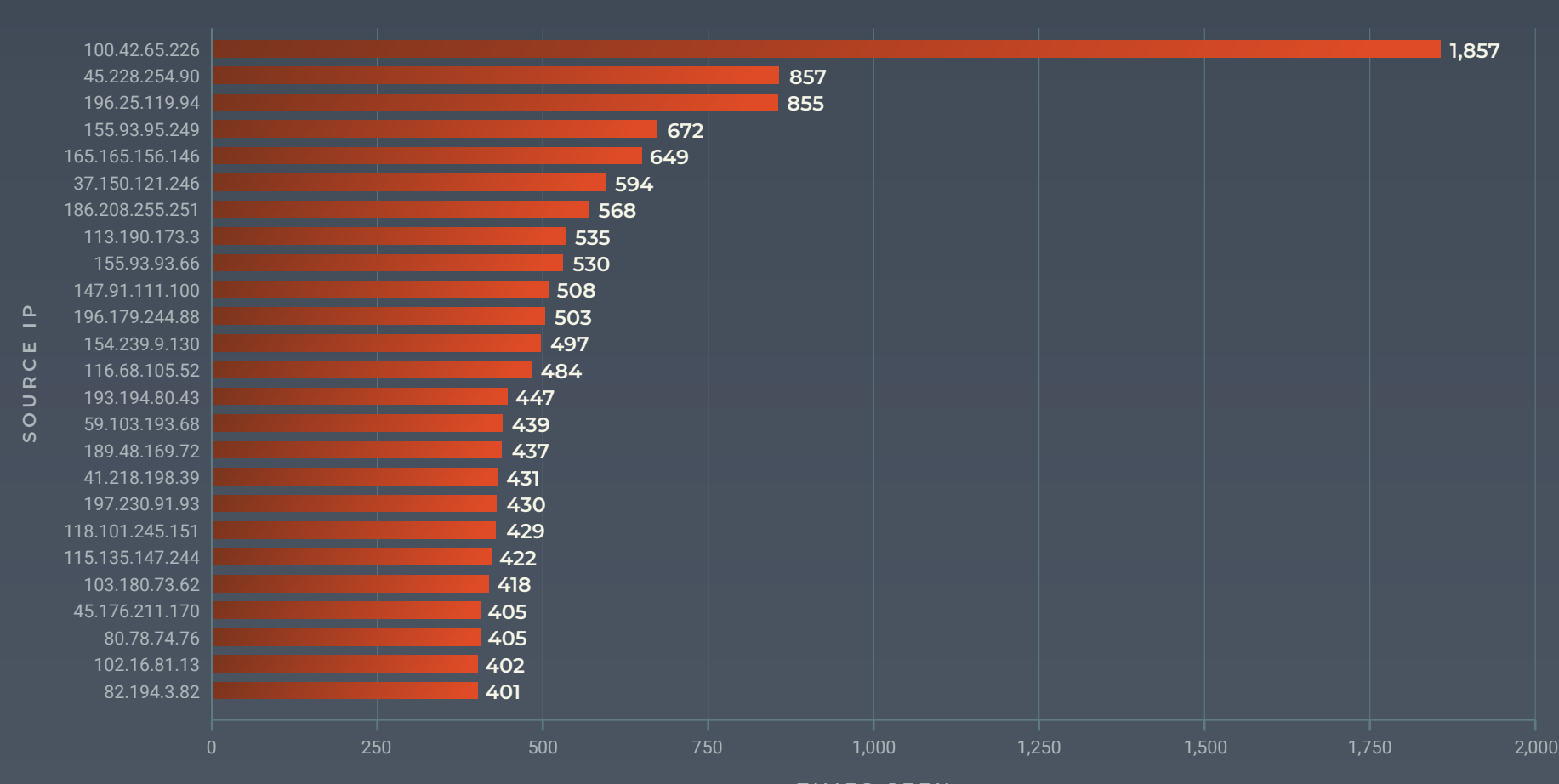


Attack bot's number of:

- UNIQUE IP ADDRESSES: **86,266**
- COUNTRIES: **176**
- ASNs/ASOs: **5,021**

**<1,000** OF SOURCE IPs FLAGGED AS COMPROMISED SERVERS

IPs Used in Credential Stuffing Attack



Get more details on this attack in the ThreatX Labs research report, *Anatomy of a Targeted Credential Stuffing Attack*.

[READ MORE →](#)



ThreatX is managed API and application protection that lets you secure them with confidence, not complexity. It blocks botnets and advanced attacks in real time, letting enterprises keep attackers at bay without lifting a finger. Trusted by companies in every industry across the globe, ThreatX profiles attackers and blocks advanced risks to protect APIs and applications 24/7. Learn more at [www.threatx.com](http://www.threatx.com).