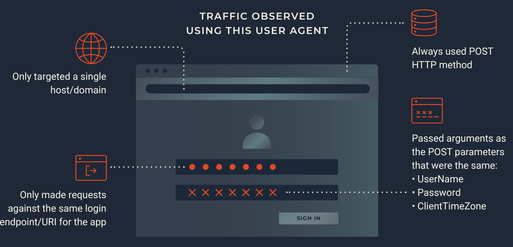
THREATX

Anatomy of a Distributed Credential Stuffing Attack

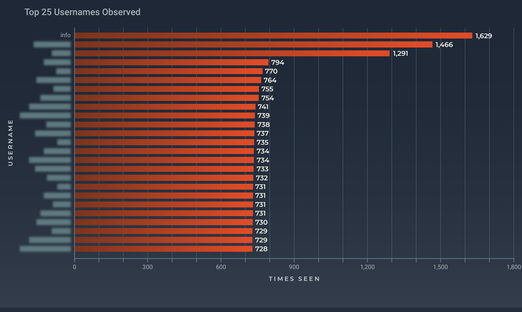
One of ThreatX's customers recently experienced a credential stuffing attack, illustrated below.

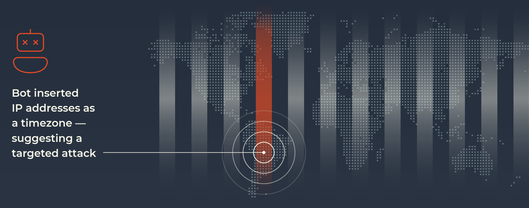
ThreatX identified suspicious traffic from various IP addresses using the following User-Agent header:

`gfdfgsdfgsgfdDSFSD3223`

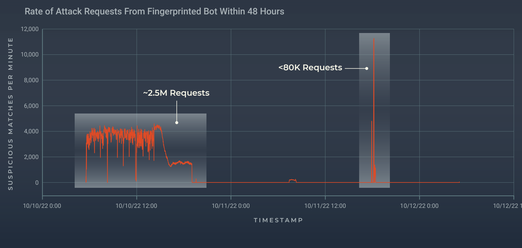


1.6m+ UNIQUE USERNAMES SEEN ACROSS ALL SUSPICIOUS REQUESTS





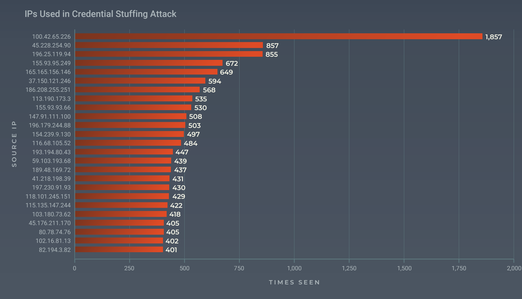
SUSPICIOUS USER AGENT SHOWS UP IN 2.5m+ requests



Attack bot's number of:

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

<1,000 OF SOURCE IPs FLAGGED AS COMPROMISED SERVERS



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

READ MORE →