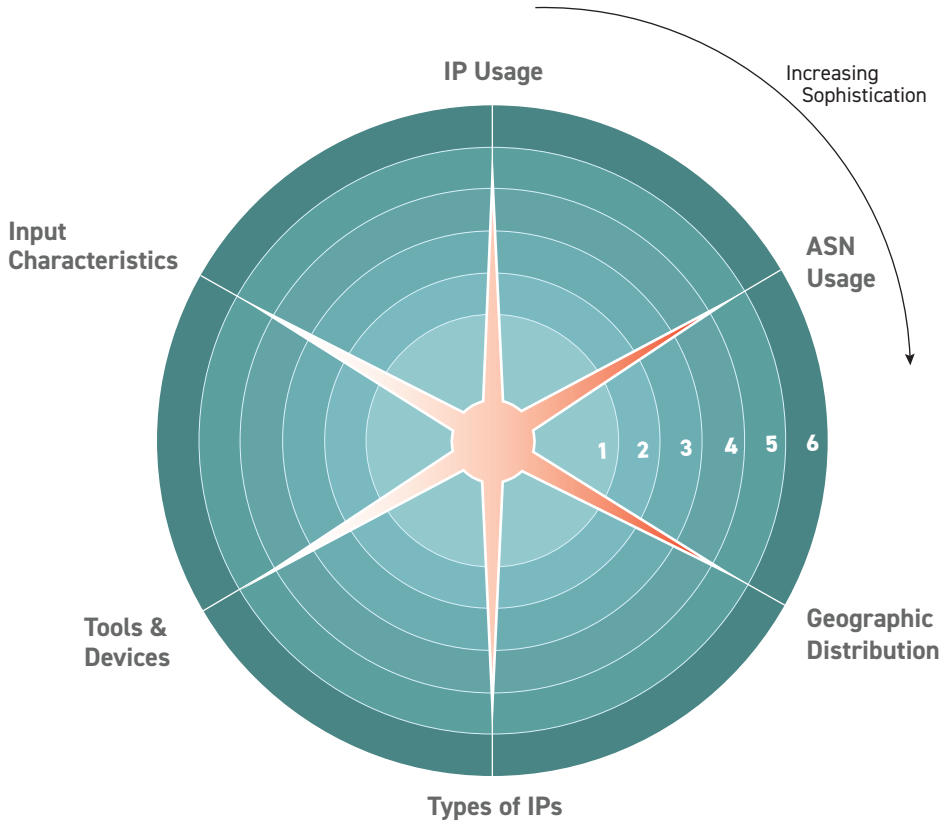
Imitation Attack Scale™

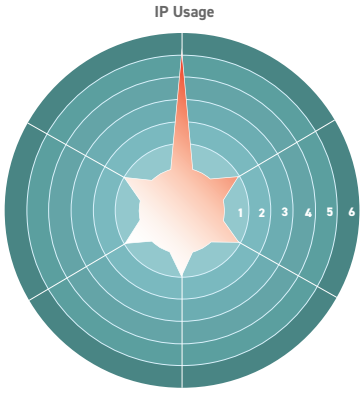
When bad actors first attack a website or mobile app, they typically launch unsophisticated attacks, as those are the cheapest and fastest. These attacks stand out from normal user traffic and are relatively easy to detect and prevent. As soon as attackers face any type of countermeasure deployed on the website or mobile app, they begin evolving their attack to more closely imitate normal human traffic, making it more difficult to deflect.

The more sophisticated the attack, the more closely it represents legitimate user traffic. Shape's Imitation Attack Scale measures the sophistication of an attack across network, client and behavioral characteristics. The framework uses the following attributes and is extensible to provide additional precision in measuring attack sophistication.

Network Characteristics - IP Usage, ASN Usage, Geographic Distribution, Types of IPs
Client Characteristics - Tools & Devices
Behavioral Characteristics - Input Characteristics

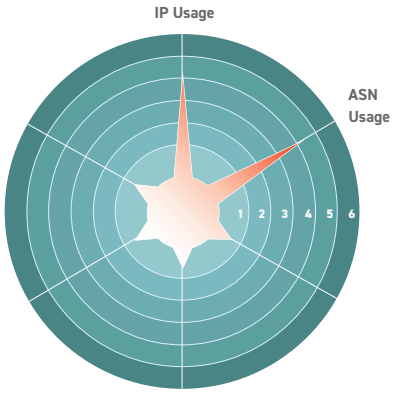


Note: The size of the center circle represents the potential volume of the attack



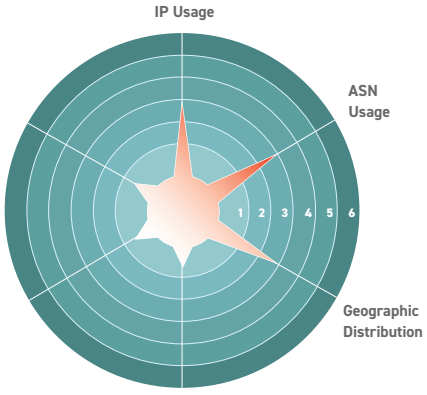
1 IP Usage

The first way to disguise an attack is to typically increase the number of IP addresses used to launch the attack. Attackers begin with this step to bypass IP-based rate limits.



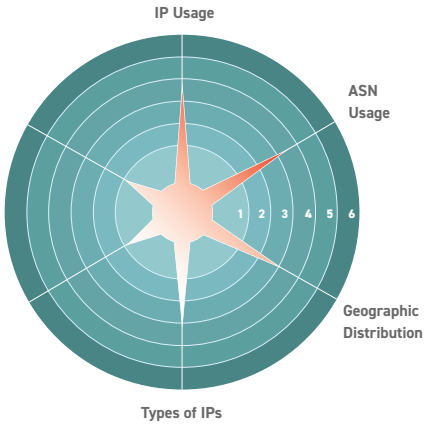
2 ASN Usage

If decreasing the transaction to IP ratio is not successful, the attacker may start using new ASNs from other providers. An ASN is the ID for major blocks of the internet. For example, AS13385 is an ASN associated with Comcast.



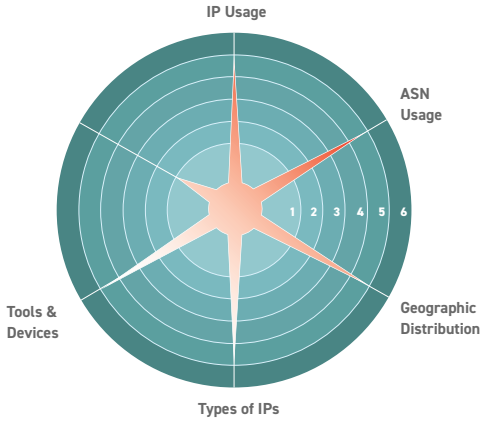
3 Geographic Distribution

If still unsuccessful, an attacker may look more closely at which countries the attack's IP addresses are associated with. For example, if attacking a Mexican bank, the attacker will want to use primarily IP addresses originating from Mexico.



4 Types of IPs

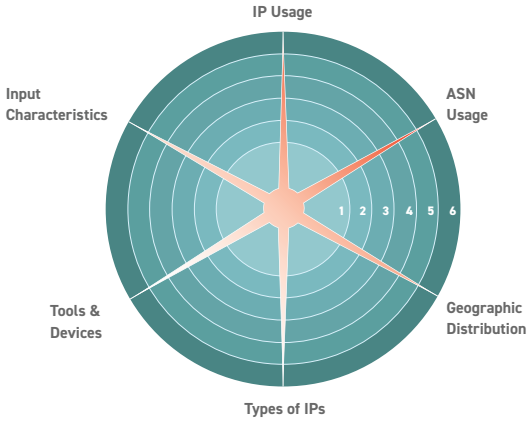
If an attacker believes they are using IP addresses from the right geographies and at a normal rate, they could alter the types of IP addresses that they are using. For example, rather than using IP addresses from open proxies or hosted IPs, which are more likely to be blacklisted, they can start leveraging botnets through legitimate residential and business IPs.



5 Tools & Devices

If improving the network characteristics of their attack is still unsuccessful, an attacker can attempt to utilize tools and devices that will make their transactions appear more legitimate. For example, a first step would be to use something like a headless browser, which can execute JavaScript, thereby circumventing simple JavaScript-based defenses.

Note: Introducing more complex tooling increases the time and cost to execute an attack, causing the volume of the attack to decrease (as represented by the size of the center circle).



6 Input Characteristics

The final dimension of sophistication is to actually imitate human behavior, by introducing characteristics such as mouse movements or keystrokes. Attackers incorporate these behaviors into their attacks by using tools like Selenium, which can record and replay a real interaction.