Fake Diurnals

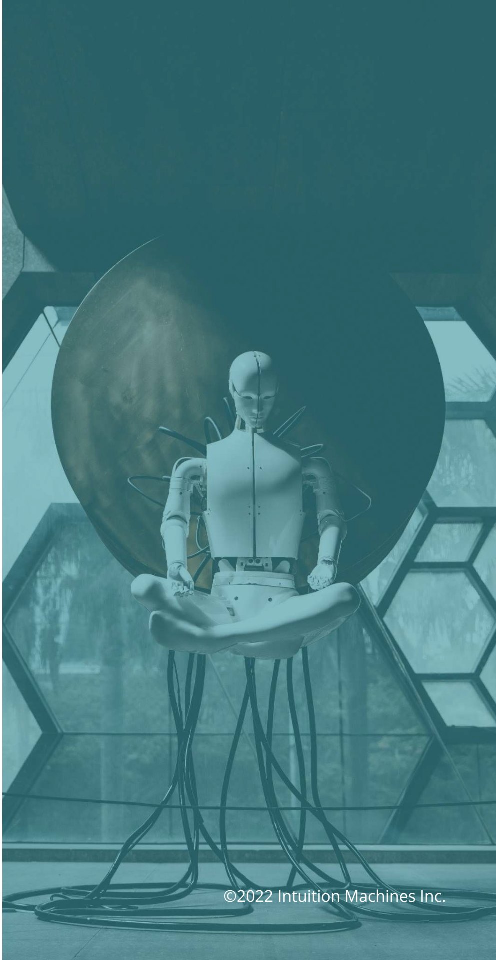
Malicious Threat Actors Hiding in Plain Sight

hCaptcha
for Enterprise

Introduction

As bot mitigation and fraud detection solutions have grown more sophisticated over the years, threat actors have been forced to evolve as they attempt to circumvent the latest technologies.

One popular bad actor tactic is to generate "low and slow" fake diurnal traffic. Using this tactic, bad actors attempt to evade detection by hiding within legitimate user traffic patterns.



Standard Human Traffic

To understand the concept of fake diurnals, it helps to examine what network traffic looks like when it originates from genuine humans.

Humans generally follow predictable patterns. Their traffic often mirrors the standard work, leisure, and sleep patterns of individuals around the world. As shown below in figure 1, regional human traffic typically increases dramatically in the morning and builds throughout the day, and then decreases in the late afternoon and evening.

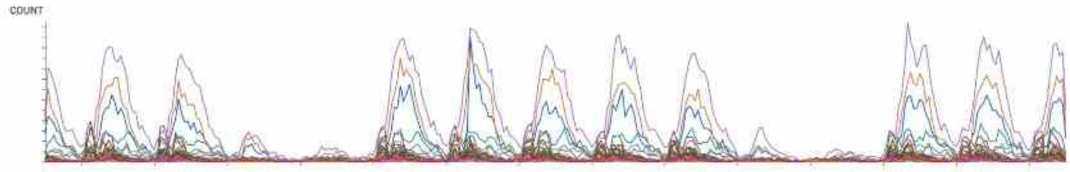


Figure 1: Legitimate human traffic follows a set pattern that is inextricably linked to human behavior relating to work, leisure, and sleeping habits.

Standard Human Traffic

Most online properties also see significantly lower volume over the weekend. Many industries may also experience a noticeable drop in volume mid-day when people are taking time for lunch. You can see this lunch-time pattern in Figure 1, and even more so in Figure 2.

Most human traffic reflects these daytime, or diurnal, patterns.

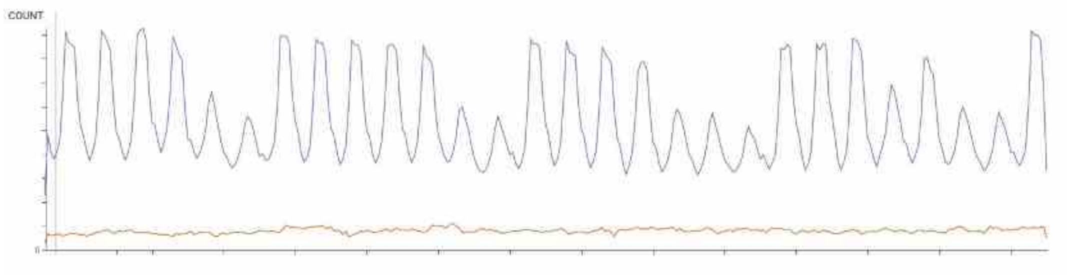
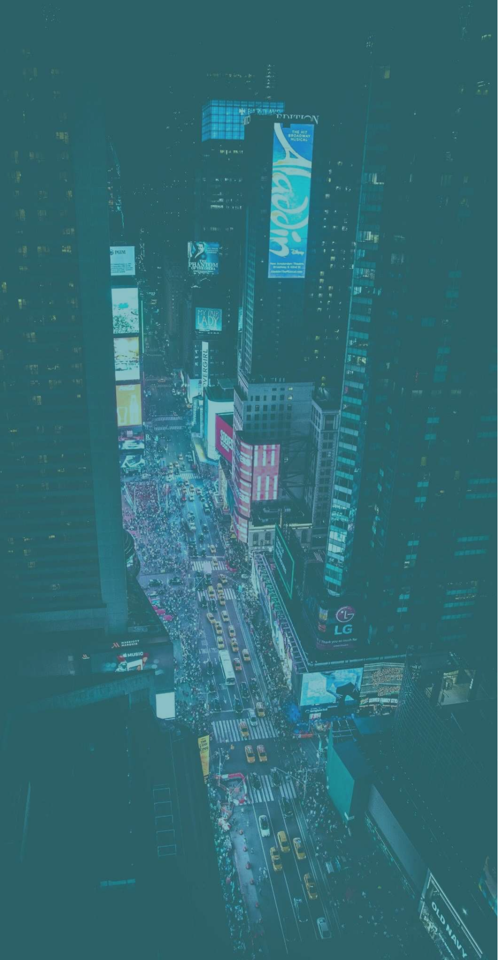


Figure 2: Human traffic ramps up in the morning, peaks in the afternoon, and then tapers off in the evening.



Changing Times

In the past, the distinctly diurnal patterns of human beings made it possible for fraud and security systems to identify malicious bots with relative ease.

Most automated attacks created network traffic that showed unnatural spikes throughout the day and night. These sharp spikes look quite different when compared to legitimate traffic. Malicious bot traffic might also generate traffic surges during weekends, holidays, or other times when humans are less likely to be online.

Changing Times

Fraud and SOC teams could quickly identify these anomalies and take immediate action. In the example illustrated in figure 3 below, the initial, large spike suspiciously begins precisely on the hour, and its shape strongly differs from human diurnal activities, flagging it instantly as possible malicious activity.

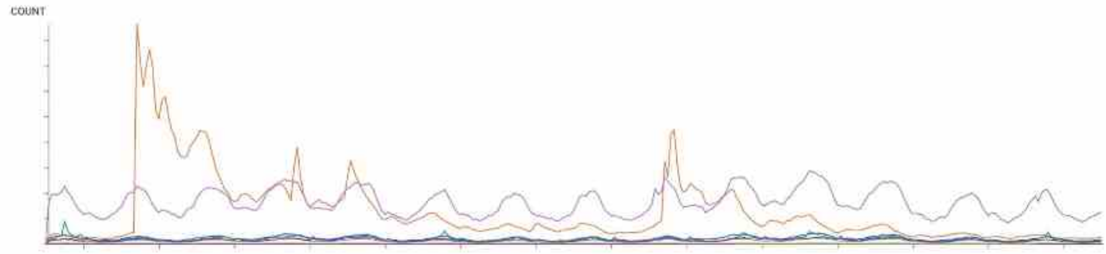


Figure 3: Pronounced anomalies, such as the sharp spikes could result from a sale, a promotional campaign, or some other genuine business event. They could also indicate an automated attack.

Putting a Stop to Fake Diurnals

As cyber criminals become more sophisticated, we are seeing a notable increase in the use of fake diurnals, resulting in bot traffic that, on the surface, looks like real human traffic patterns.

Take a look at Figure 4. The bot operator has used fake diurnal technology to better emulate human traffic.

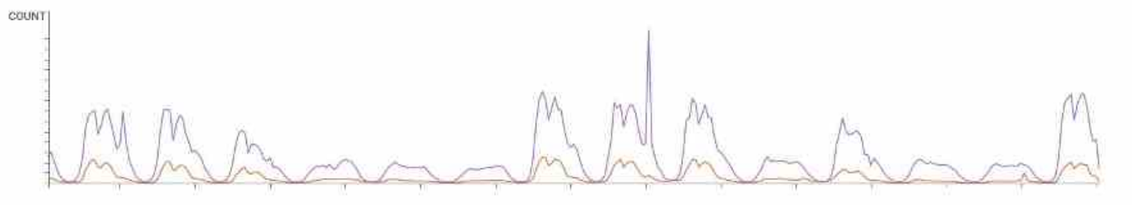


Figure 4: *Malicious bot traffic (in orange) uses fake diurnal patterns to look very similar to genuine traffic.*

Putting a Stop to Fake Diurnals

Because today's fake diurnals blend in with authentic human traffic more effectively than in the past, solutions must be more sophisticated and use:

Fine-Grained Time Series Analytics: Advanced traffic behavior analytics that are capable of fine-grained pattern detection, isolation, monitoring, and drift analysis.

Behavioral Threat Intelligence: Sophisticated, large-scale global threat intelligence that's continuously learning from humans, bots, botnets, clickfarms, and operators.

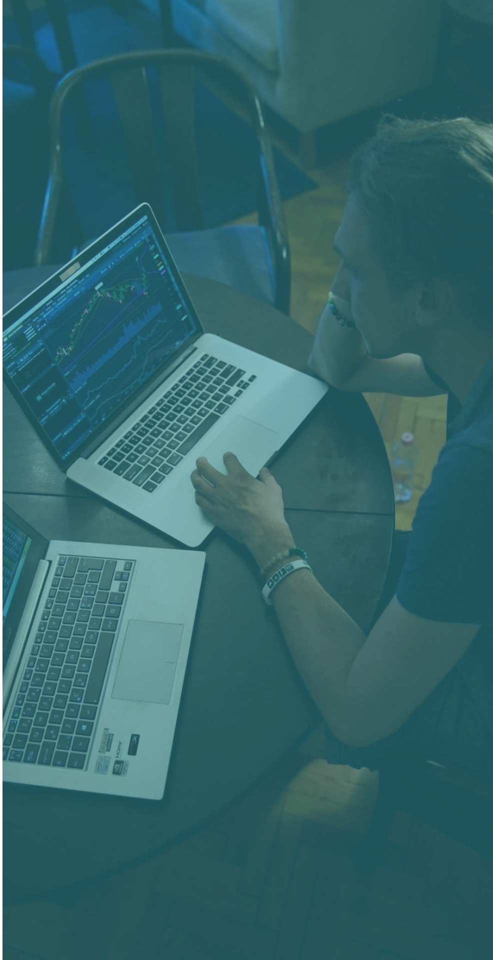
Specialized Machine Learning: Advanced ML that's been specially trained to detect and react to the emergence and increased sophistication of bot behavior designed to mimic broad human behavior.

Putting a Stop to Fake Diurnals

Highly Accurate Humanity Verification: Bot detection and mitigation needs to not just accurately spot suspicious requests, but confirm suspicions with low human friction.

After-The-Fact Learning and Alerting: The capability to automatically identify and group seemingly separate events that are part of a coordinated single attack – even if those events have already occurred.

Specifically Trained SOC Team: Fraud and security analysts that are familiar with sophisticated bots, and how to detect and isolate them can be helpful in priming learning nets to detect new sophisticated behaviors.



Summary

Bad actors are constantly refining their skills and tooling in an effort to stay ahead of the tactics and solutions employed by their targets. The use of fake diurnal traffic patterns is yet another strategy threat actors are now using to make it more difficult for organizations to detect and mitigate these sophisticated attacks.

With the correct resources and tools, combined with a strong security culture that stays ahead of new attacks, organizations can effectively protect themselves from this and other emerging threat vectors.

About hCaptcha

hCaptcha offers the most advanced machine-learning driven bot detection available, including industry-unique edge learning that puts privacy first.

hCaptcha Enterprise is an ideal solution to help organizations stay ahead of even the most sophisticated threat actors while maintaining low user friction. Click here to learn more.