"HIDING IN THE WEB" THE GROWING THREAT OF LOCATION FRAUD

David Briggs - Chairman



1. Ge(o)nesis...





UIGEA



UIGEA defines "unlawful Internet gambling" as "to place, receive, or otherwise knowingly transmit a bet or wager by any means which involves the use, at least in part, of the Internet where such bet or wager is unlawful under any applicable Federal or State law in the State or Tribal lands in which the bet or wager is initiated, received, or otherwise made."



US iGaming Licensed Geolocation Compliance Service Provider



Tested and Verified by





250 million devices

GEOGUARD LOCATION CONFIDENCE

European Division of GeoComply



10 million transactions/day









Verify Accuracy & Integrity: 350 Checks



2. So what..?



What's The Big Deal About Geolocation?







- 884 datacenters offering anonymized web hosting
- **11,202** sets of distinct IP ranges
- 296,293,554 individual IP's held by DataCenters



- 160,604,000 (and counting!) IP v4 address held by data centers/VPN's
- 4,294,967,296 (4.29 billion) IPV4 addresses
- 340,282,366,920,938,463,463,374,607,431,768,211,456 (2¹²⁸ ≈ 3x10³⁸) IPV6 addresses



Credential-Stuffing Attacks Take Enterprise Systems By Storm

Automated credential-stuffing attempts makes up 90% of enterprise login traffic.

Billions of online credentials freshly stolen in 2016 are fueling a practice of automated login hacks that are overwhelming legitimate human-login traffic on enterprise Web properties.



3. Case Studies





Google Searches @ Launch of Pokemon GO





Fig 8: The availability of live (and otherwise unavailable/paid) sports is a major draw for sections of the public



Premier League can now block illegal Kodi football live streams

Sky, BT, Virgin Media and TalkTalk will have to block customers' access to games accessed through third-party add-ons

Aatif Sulleyman | Friday 10 March 2017 12:17 GMT | 🖵 1 comment





Click to follow The Independent Tech



4. Can you close the door to VPN's/VM's?



Multi-faceted threats require a multi-faceted response



Closing the open door to malicious Data Center connections is just an API away...



Content Delivery

The final phase exports only the actionable data into a consumable format for customers. This might include file-based databases that can be updated periodically, or a WebService-API if additional protections beyond VPNs and proxies are desired.

Intelligent Filtering

Given that not all data sources are of equal quality or reliability, each source is given an internal confidence rating to score the probability that an observed threat gathered from a given source truly represents a credible attempt to spoof location.

Exploratory Investigation

Fraud Specialists identify, profile and establish credible risks, which then our fraud engineers develop ways to nullify the effectiveness of the fraud.

Third-Party Sources

Open data sources are evaluated, assigned a confidence rating, and incorporated into the data set along with risks identified in the first two phases.

Real-time Analytics

Mining Data Information identified by GeoGuard's Fraud Specialists from embedded native applications sitting on hundreds of millions of devices worldwide is filtered through various manual

and automated processes.

GeoGuard's proprietary set of real-time analytics scripts monitor internet traffic to detect signs of location spoofing services and automatically react to and adjust to changing IP ranges from location countering threats.

GEOGUARD LOCATION CONFIDENCE





