Anti-abuse applications of IP

January 19, 2021

IETF PEARG Research Group Interim Meeting

Why are IPs important for anti-abuse use cases?

- IPs represent a *fairly** stable identifier of the origin of a request.
- Anti-abuse engines fundamentally rely on their ability to classify subpopulations of requests as good vs bad.
- The lack of IPs would make it (in multiple cases) impossible to identify such subpopulations and as a result it would gradually erode the trust and safety of the Internet.

** Abusers often rely on a) residential proxy networks, b) anonymous networks (e.g. Tor), and c) mobile carrier networks behind NATs that reduce the stability of IP addresses.*

Anti-abuse applications that heavily rely on IPs

Use Case	Examples	Why's it important?
Account Abuse	• Fake account creation • Credential stuffing or cracking • Account takeover	• User security and privacy is compromised when accounts are hijacked. • >360 breaches in the past five years, 3B accounts and 550M passwords leaked. • Credential stuffing costs up to an average of $US 6 million a year per company.
Engagement & Financial Fraud	• Engagement Fraud • Payment fraud • Synthetic identity fraud • Ransomware • Email spam	• Automated/fake engagement can amplify disinformation narratives. • Automated botnet activity is reportedly increasing. • For every dollar of fraud committed, U.S. retailers incur $3.13 of costs.
Ad Fraud	• Large botnets (e.g. Methbot, 3ve) • Malware on mobile devices (e.g. Terracotta) • Fake traffic on Roku devices (e.g. ICEBUCKET)	• Online advertising is the primary monetization mechanism for the Open Internet. • >$US 6b is lost every year due to different types of ad fraud. The revenue generated is used to further fund cybercriminal operations.
Child Abuse	• Geolocation of child sexual abuse victims • Identifying distributors of CSAM	• Some CSAM distributors are unsophisticated and do not use proxies. • NCMEC finds IP information useful, even with proxies.

Stable IPs establish trust for Account Recovery

Challenges of account ownerships are varied as a function of perceived risk. This reduces user friction and lockout while maintaining a high degree of friction for would-be hijackers.

The stability of the client IP (i.e. is this a long-used IP on which the user has passed challenges) is one important signal in this domain. We can leverage the fact that the user is on a stable IP to infer trust in key account recovery scenarios

IP as an entity for clustering and aggregation

IPs allow us to identify abusive clients and networks independent of cookies or accounts. This is useful for protecting:

- Accounts Creation (IPs as hotspots of sign-up activity)
- Account Ownership (IPs as hotspots of authentication activity)
- Contextual Integrity (IPs as hotspots of crawling)
- Low-latency interfaces (IPs as hubs for reputation)

Automated Datacenter Traffic

Scaled abuse often originates from datacenters, including so-called “bulletproof hosts” specializing in cybercrime. These are primarily tracked via IPs.

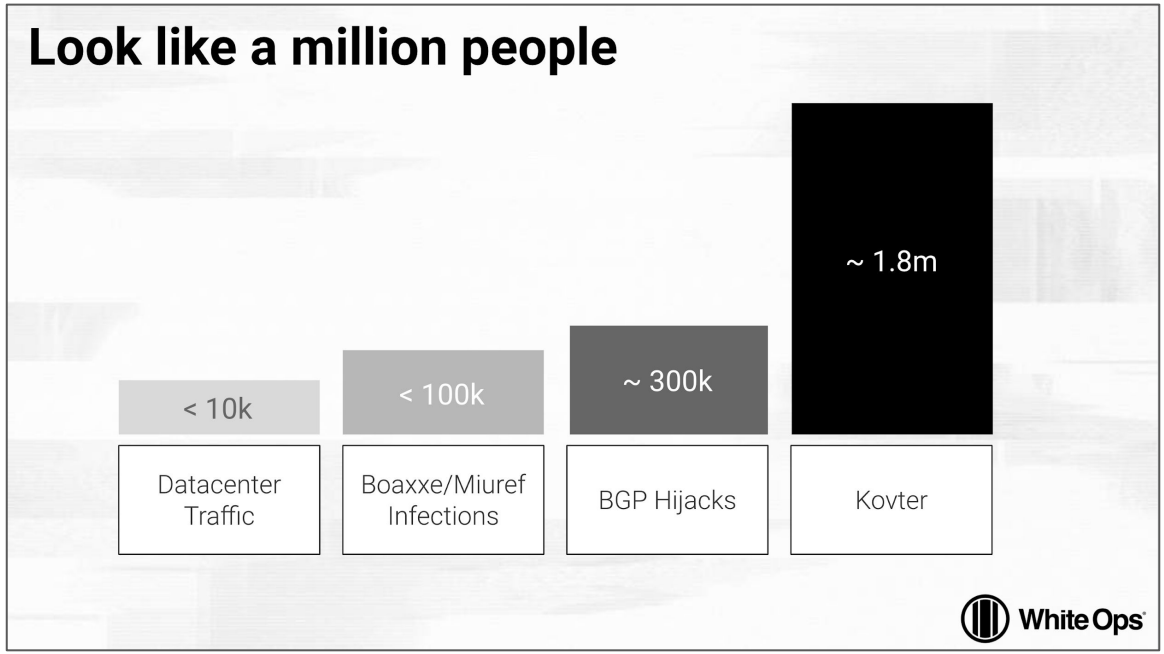
There exist several public lists[1] of datacenter IP addresses contributing traffic considered “not valid”, which allow companies without the scale or resources to do their own classification to protect themselves against unsavory datacenter traffic.

[1] example: https://www.tagtoday.net/fraud#dcip

3ve Botnet - Preventing abuse from infected devices

One recent example was the 3ve botnet takedown. White Ops and Google referred the case to the FBI - leading to several arrests and coordinated takedown of one of the largest botnets we've ever seen generating ad fraud activity.

IPs were the main indicator White Ops used to track and block the 3ve activity. It was also the main indicator used to collaborate with the law enforcement and the rest of the cross industry group that took down 3ve.



IP space used by the 3ve operation

Child abuse enforcement

NCMEC is a hub for the reporting of child sexual abuse material (CSAM), and allows internet service providers to collaborate with global law enforcement to bring child sexual abusers to justice. The strength of this collaboration has enabled us to disrupt child sex trafficking on multiple occasions. IPs are one critical part of this, along with other re-identifiable client properties.

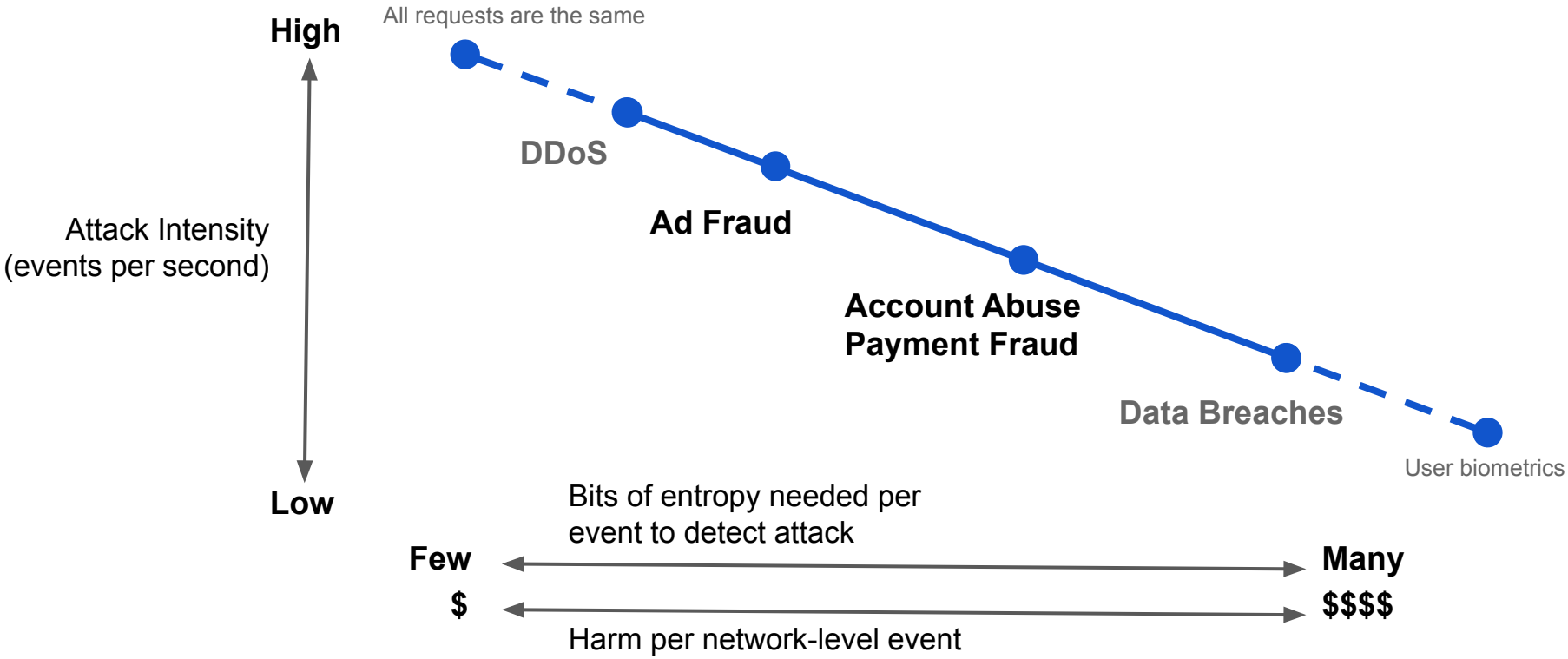
Over 25M images reviewed by NCMEC annually (source). Over 1,400 companies registered to make reports to NCMEC.

Takeaways

- IP addresses are fundamental in preventing abuse of TCP/IP networks. Anonymizing the sources of network traffic without addressing anti-abuse use cases will empower cybercriminals of all stripes.
- This abuse is detrimental to privacy (e.g. account takeover), trust (e.g. fake accounts + engagement), and commerce (e.g ad fraud + transaction fraud).
- Goal: Protecting user privacy while maintaining security/anti-abuse capabilities should be a core tenet of the Privacy Sandbox.

Appendix

Anti-abuse and Privacy



IP Size estimation

- Suppose we want to build an invalid traffic filter on an IP over some time period and filter if it generates too much activity
  - If we treat all IPs equally, then:
    - Low Thresholds ⇒ high false positives for IPs with many users
    - High Thresholds ⇒ high false negative rate for IPs sending little traffic
- Instead, we can adjust the thresholds based on the number of users behind an IP, which we call **IP Size**
- Built an IP Size Estimation pipeline that builds statistical models for IP size estimation based on aggregated log files.