JOINING FORCES TO TAKE DOWN THE HYDRA AD FRAUD BOTNET

tag
TRUSTWORTHY ACCOUNTABILITY GROUP

PROTECTED MEDIA

INTRODUCTION

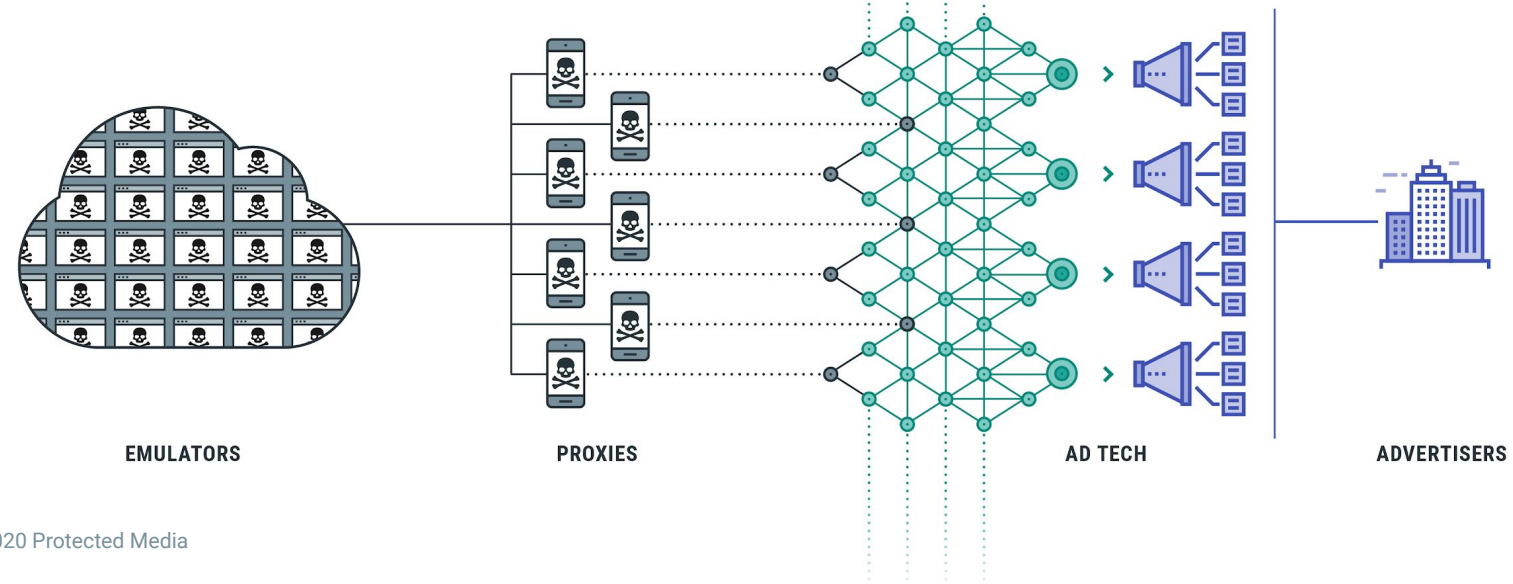
- “Hydra” is a technologically-advanced botnet, first identified and blocked by Protected Media during August 2019
- Up-to-date, Hydra’s orchestrated ad fraud operation has been involved in:
  - Defrauding advertising platforms of very large budgets
  - Stealing data off websites
  - Account takeovers
- The botnet’s fraudulent activities are growing in sophistication and scope. Hydra is continuously introducing quick cycles of new attack technology layers and evolving counter-cyber measures to avoid detection.

THE HYDRA BOTNET: ANATOMY

1. Datacenter servers run Android emulators impersonating thousands of real Apps, creating +100M fake impressions/day

2. Fake traffic is streamed through 70K/day mobile residential IP, each creating thousands of ad impressions

3. Botnet impressions are sold over-and-over through multiple networks and exchanges and get diluted within real traffic

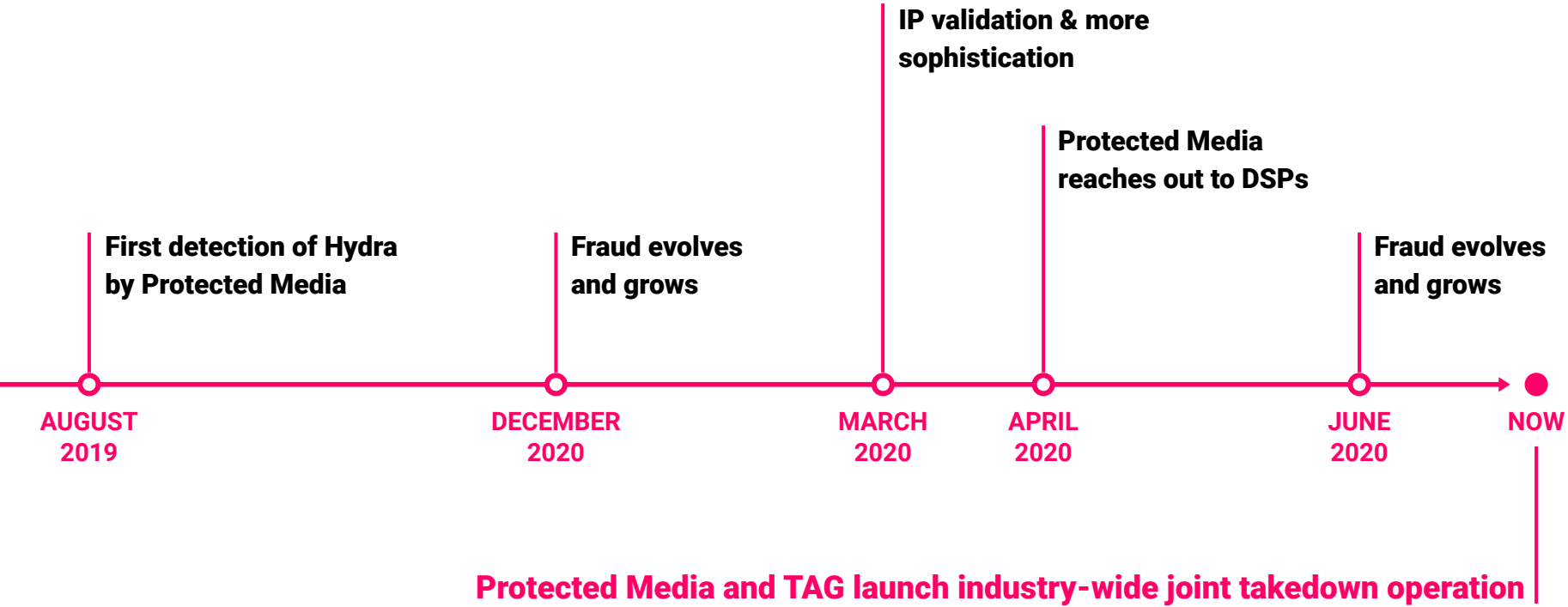


THE HYDRA BOTNET: MODE OF OPERATION

Hydra relies on advanced technologies and a profound understanding of advertising KPIs and methodologies to build an efficient and hard to detect fraud operation:

- By fragmenting its operation across over 8,000 apps, Hydra's impact is diluted in thousands of independently evaluated traffic streams. When fraud indications do surface, they appear insignificant.
- By selling traffic through dozens of networks, Hydra is protected by multiple tiers of commercial secrecy since no one wants their traffic investigated
- By selling programmatically and making up the apps Hydra maintains an agile operation: when bad traffic is detected and cut off, new traffic is served right away.
- By capping sales volume Hydra keeps a relatively low profile
- Connecting the dots requires advanced counter-fraud technologies and resources.

TIMELINE



AUGUST
2019

FIRST FRAUD IDENTIFICATION

- Protected Media detects IVT across multiple sources
- The operation is relatively easy to catch, and blends in with other prevalent fraud types
- Traffic is Mobile App
- Protected Media keeps tabs on the botnet during the following months

FRAUD EVOLVES AND GROWS

- Protected Media registers unique identifiers pointing at increased scope and sophistication of the operation
- A full investigation is launched
- Using 4 independent detection logics, Protected Media's researchers uncover advanced fraud patterns
- Counter-cyber measures are employed by the botnet to try and throw off Protected Media's investigation
- By connecting the attacks' components and patterns, Protected Media is able to expose the operation's magnitude
- Among other parameters, the botnet passed traffic through over a dozen ad-networks, who kept reselling it

IP VALIDATION & MORE SOPHISTICATION

- Protected Media secures the cooperation of major cybersecurity companies, to confirm the extent of the fraud
- Independent research confirms proxy IPs are malicious
- Further research also uncovers that the network escalated its detection avoidance technology by enabling Advanced Persistent Bots (APBS)
- These bots cycle through random IP addresses, enter through anonymous proxies and peer-to-peer networks, and are able to change their user agents
- They use a mix of technologies and methods to evade detection while maintaining persistence on target sites

PM REACHES OUT TO DSPs

- Protected Media undertakes Responsible Disclosure and informs major impacted platforms about the fraud
- Protected Media supplies over 100K IP addresses which were recently used by the botnet, as well as dedicated transaction/log-level data of each group's specific transactions, allowing them to use tens of thousands of their own transactions to research their exposure to the botnet
- Demand players use this data to positively identify the fraud
- Subsequently, these platforms limit purchase of the fraudulent traffic

OTHER DSPs FILL THE DEMAND GAP

- The void created by the reduced traffic is quickly filled
- Other DSPs, unaware of the fraud, start purchasing the fraudulent traffic
- The botnet is quickly restored to its previous volume
- In addition, Hydra is upping its ante by writing code to send Protected Media's code's results to their servers and employing a sophisticated technology to continuously update their mode of operation
- Protected Media joins forces with TAG for an industry-wide take down

TAG THREAT EXCHANGE

- Hydra is an advanced, proactive, large-scale fraud operation
- Taking it down completely will require a collaborative approach
- Protected Media joins forces with TAG and launches the Hydra Operations Center
- The Hydra Operations Center will provide technical help to adtech and media buyers who wish to identify and avoid the fraudulent traffic
- The Hydra Operations Center will cooperate with other security vendors who wish to participate in the takedown operation
- Over Q2 the number of fraudulent proxies has been reduced by half, signaling that up to date take down efforts are indeed working

A NEW KIND OF INDUSTRY RESPONSE

- No one is immune. Any platform, publisher and advertiser can be harmed by Hydra
- To take Hydra down the industry must engage in an orchestrated, cooperated action
- In order to succeed, it is vital that every player takes a stance
- TAG's and PM's Responsible Disclosure methodology protects the privacy of everyone involved, so that there's no exposure of "victims"

NEXT STEPS

- Through the TAG Threat Exchange, Protected Media will provide industry leaders the full scope of data needed to assess the damage
- The data, including the IP addresses which have been used by the botnet on specific dates, will allow organizations to self-asses and pick their response
- Under NDA, Protected Media will provide dedicated transaction/log-level data for authenticated platforms' specific transactions, allowing them to research tens of thousands of their own exposures to the botnet
- Protected Media will advise platforms in using this data to perform a de-facto take down by stopping funds to the botnet, thereby depriving it of oxygen

HYDRA TAKEDOWN METHODOLOGY

To facilitate a rapid and successful take down, Protected Media will publish IP addresses which have been used by the botnet by date (a file per day)

- IP address used by Hydra are real residential and mobile IPs
- The majority of traffic from these IPs on the days used by Hydra proxies are fraudulent
- However, there are some genuine activities from these IPs. The main reasons for this are:
    - IPs are allocated by the mobile operators and will be allocated to a legitimate user before or after being allocated and used by the botnet for fraud
    - IPs are used for various types of fraud and may be seen in ads outside of Hydra's activity, such as in account takeover

    This is NOT an IP Blacklist

WHAT YOU NEED TO DO NOW

- PM will provide a daily list of IPs for the past weeks and going forward
- When checking, run a cross between your daily impression IP log and the Hydra daily IPs. If there is a significant overlap within a traffic source, see if such an overlap happens on other days (before and after that day). If the overlap is consistent you are most likely buying Hydra traffic
- Hydra would most likely be diluted in traffic. The closer one is to the supply end, the higher the chances they'd see larger percentages of it in specific sources
- If you identify suspicious traffic you’re welcome to reach out to PM and we'll help you research further

ABOUT PROTECTED MEDIA

- Protected Media is a cyber-security based ad fraud detection and prevention technology provider
- Protected Media is a major player in the CTV space, using an advanced approach to identify and eliminate sophisticated ad fraud
- Whenever possible, Protected Media cooperates with law enforcement to fight fraud operations
- Protected Media advocates industry-wide cooperation and knowledge sharing to eliminate fraud and improve trust and reputation for all digital advertising players

Protected Media is MRC accredited for both general invalid traffic (GIVT) and sophisticated invalid traffic (SIVT) detection and filtration, across OTT, desktop, mobile web and in-app.

PROTECTED
MEDIA

CONTACT HYDRA OPERATION CENTER

slay-hydra@protected.media