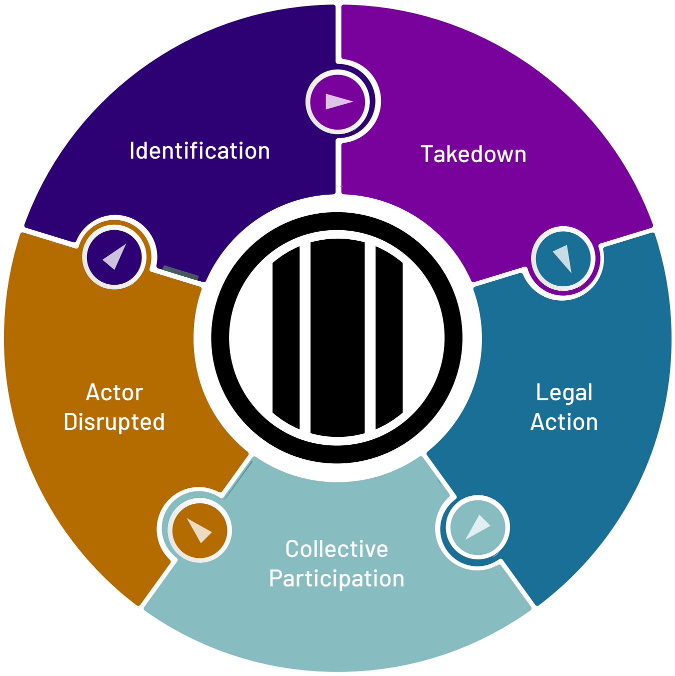
SATORI THREAT INTELLIGENCE AND RESEARCH TEAM

HUMAN's Satori team uncovers, reverse engineers, and takes down bot-driven threats to advertising, marketing, and cybersecurity.

A key pillar in HUMAN's mission to defeat bot-driven cybercrime is our ability to proactively find and disarm threats before they begin to impact our customers and partners. The Satori Threat Intelligence and Research Team is the group tasked with shining a light into the dark corners of the internet to find cybercriminals' plans and develop strategies to defend against them.



Satori helps customers with incident investigation and response for attribution and takedowns

Along with our partners in The Human Collective and major internet platforms like Roku, Facebook, and Google, HUMAN's Satori team participates in takedown efforts with law enforcement when the fraudsters behind the schemes are identified.

HUMAN's Satori team has disrupted several notable schemes:

Methbot

300 MILLION At its zenith, the Methbot operation was "watching" 300 million video ads a day. And as video advertising carries a significantly higher cost than traditional banner or social ads, this adds up fast.

6,000 More than 6,000 premium publishers were spoofed in this operation.

10 The ringleader of the Methbot scheme was recently sentenced to 10 years in prison and restitution fines of more than $3.5 million.

3ve

700,000 The 3ve botnet had more than 700,000 active infections at a time during its operation.

3 BILLION More than 3 billion ad requests every day were attributable to the 3ve botnet.

20+ The industry group built to disrupt—and take down—the 3ve botnet and scheme was composed of more than 20 organizations, including Google, Facebook, Amazon, and the FBI.

ICEBUCKET

28% At its height, the ICEBUCKET scheme accounted for 28% of all connected TV traffic passing through the Human Verification Engine.

1.9 BILLION Nearly two billion pre-bid ad requests were associated with the ICEBUCKET operation every day before its disruption.

2 MILLION More than two million people in 30 countries were spoofed or faked during ICEBUCKET.

PARETO

6,000 The PARETO operators spoofed more than 6,000 CTV apps as part of their scheme.

1 MILLION PARETO operated chiefly through a botnet of nearly one million infected Android phones.

650 MILLION Across its mobile and CTV-centric botnet, the PARETO operation made more than 650 million fraudulent bid requests a day.

About HUMAN

HUMAN is a cybersecurity company that safeguards 500+ customers from sophisticated bot attacks, fraud and account abuse. We leverage modern defense—internet visibility, network effect, and disruptions—to enable our customers to increase ROI and trust while decreasing end-user friction, data contamination, and cybersecurity exposure. Today we verify the humanity of more than 15 trillion interactions per week across advertising, marketing, ecommerce, government, education and enterprise security, putting us in a position to win against cybercriminals. Protect your digital business with HUMAN. To Know Who's Real, visit www.humansecurity.com.