

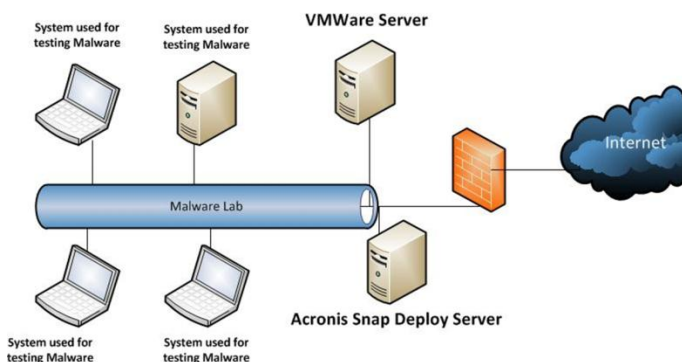
The Adometry Malware Lab is searching, tracking and reporting any suspicious behavior that is committing online fraud or harming advertisers' ad spend.

The Adometry Malware Lab installs and monitors the behavior of different types of malware which impact search results in the PPC/CPC, video, and display space. These results include HTTP captures and videos of the malware patterns.

The Adometry Malware Lab's main goals are to identify methods of attacks, bad actors, the size and scope of the problem, and gather intelligence for creating rules, reporting black hat IP addresses and those committing the fraud to authorities across the globe.

Overview of the Problem:

- CPC/PPC, Affiliate and Display fraud is a significant and growing problem for the online media industry.
- Fraudsters continue to use ever-more sophisticated means to generate and monetize fraudulent traffic.
- Malware is increasingly the vehicle of choice — allowing fraudsters to infect tens of millions of PC's.
- These "botnets" are then used to perpetrate highly distributed, low and high frequency attacks.
- This fraudulent traffic is immediately distributed and routed across and through multiple ad networks, making it very difficult to find and mitigate.
- Online media advertisers and marketers are unsuspectingly paying for this fraudulent traffic, grossly inflating their costs and decreasing the effectiveness of their media.



For more information on Adometry's Malware Lab please contact us at:



sales@adometry.com
866-512-5425

What is the Malware Lab?

- The lab utilizes our research, scientific methodology and expertise through various lists and sources to constantly identify new malware attacks and exploits.
- In the lab tech's purposefully and continuously infect an array of computer's set up with various malware algorithms, programs and software.
 - Using Virtual Machines and real systems that we infect and an anonymous internet connection to disguise our activity.
 - The lab leverages all leading system configurations (Windows, Mac OS, etc.) and user agents.
- Performing comprehensive automated testing against this series of infected machines and then records and tracks all aspects of fraudulently generated traffic.
- This allows the tech to see the entire audit trail of fraudulent activity — each and every touch point of the chain — with full visibility into how the fraud is perpetrated and monetized and report to all law enforcement and black list all IP's associated with the fraudulent activity.

Malware Lab Efforts and Deliverables:

- Dedicated, continuous and automated testing against an entire array of malware-infected machines.
 - For each client, the lab incorporates a specific campaign (top keywords and campaigns, by source of traffic, etc.) and traffic buying channels (PPC, Affiliate, Display).
- Fully categorized and researched specifics for each fraud example generated, with complete end-to-end reporting and definitive audit trails.
 - The lab provides all related details so that clients can identify bad actors, quantify the impact and take action (i.e. get refunds; filter and block traffic).
- Reports delivered weekly and experts within the staff are always available for consultative advice.

Customer Benefits:

- Quickly identify and eliminate sources of bad traffic.
- The lab generates irrefutable proof of fraudulent activity.
- Improve overall advertising results (either your own or the results of your clients) increasing media effectiveness and ROI.
- No implementation effort involved.