WOMBLE BOND DICKINSON

August 8, 2023

Womble Bond Dickinson (US) LLP

50 California Street, Suite 2750
San Francisco, CA 94111

Via E-mail: Stephen.Smith@cooley.com

Stephen Smith
Cooley LLP
1299 Pennsylvania Avenue, NW
Suite 700
Washington, DC 20004-2400

Chris E. Mammen
Partner
D: 415-765-6267
E-mail: Chris.Mammen@wbd-us.com

Re: Arkose Labs, Inc. Patents

Dear Mr. Smith,

I am writing to you again on behalf of Arkose Labs, and to follow up on my March 1, 2023, letter relating to Arkose Lab's patents. We have not received any response to that letter.

In addition to the patents identified in my previous correspondence, we wish to draw your attention to the following additional patents, also owned by Arkose.

U.S. Patent No. 7,373,510

Claim 1 states:

> 1. A method for preventing robots from browsing a Web site beyond a welcome page, said method in said Web site comprising the steps of:
>
> receiving an initial request from an undefined originator and responding to said initial request with a challenge that prompts a response from said undefined originator; and
>
> receiving a response from said undefined originator and checking said response to determine whether said challenge is fulfilled; and
>
> if said challenge is fulfilled:
>
> processing any further requests; and
>
> if said challenge is not fulfilled:
>
> stopping processing of any further requests, wherein said step of stopping processing of said further requests includes the further step of:
>
> dropping or redirecting a TCP connection established with said undefined originator
>
> logging a source IP address of said undefined originator and starting a timer,

Womble Bond Dickinson (US) LLP is a member of Womble Bond Dickinson (International) Limited, which consists of independent and autonomous law firms providing services in the US, the UK, and elsewhere around the world. Each Womble Bond Dickinson entity is a separate legal entity and is not responsible for the acts or omissions of, nor can bind or obligate, another Womble Bond Dickinson entity. Womble Bond Dickinson (International) Limited does not practice law. Please see www.womblebonddickinson.com/us/legal-notice for further details.

further including steps upon receiving a new request of:

checking whether a source IP address of said new request matches said logged source IP address; and

if said source IP address matches said logged source IP address:

checking whether said timer has expired and, if said timer is expired, resetting said logged IP address; and

proceeding normally with said new request; and

if said timer is not expired, dropping or redirecting said TCP connection;

if said source IP address does not match said logged source IP address, proceeding normally with said new request and executing all the above steps with each newly received request.

U.S. Patent No. 10,147,049

Claim 1 states:

1. A method, comprising:

for a system or application used by a plurality of users, providing an access to a memory device storing user data samples for all users of the plurality of users;

selecting a target user from among the plurality of users; and

using a processor on a computer and using data samples for the target user and data samples for other users of the plurality of users, generating a normal sample data set and an abnormal (anomalous) sample data set to serve as a training data set for training a model for an anomaly detection monitor for the target user such that the data samples of the target user are used to derive a normal sample data set for the training set and the data samples of other users are used to derive an abnormal sample data set for the training set.

U.S. Patent No. 11,227,232

Claim 1 states:

1. A method, comprising:

for a system or an application used by a plurality of users, providing an access to a memory device storing user data samples of a usage of the system or the application for all users of the plurality of users;

selecting a target user from among the plurality of users, using a processor on a computer, the data samples of the target user forming a cluster of data points in a data space;

using the processor to take data samples for the target user to generate a normal sample data set as training data set for training a model for an anomaly detection monitor for the target user; and

using a local outlier factor (LOF) function to generate an abnormal sample data set for training the anomaly detection monitor for the target user.

U.S. Patent No. 10,938,845

Claim 1 states:

1. A method for detecting user behavior deviation in an enterprise network, comprising:

defining a set of user groups based on user attribute information received from a user directory of the enterprise;

receiving from an application security events for a collection of users whose user attribute information is used to define the set of user groups, and generating a set of training data;

training a machine learning system using the set of training data set to generate a set of clusters in a model of user behavior by: (i) transforming the set of training data to generate transformed training data, (ii) applying a clustering model to the transformed training data to derive a set of learned groupings, and (iii) computing measures of distance between the set of learned groupings and the set of user groups, wherein a cluster is a learned user group that corresponds to a defined user group in the set of user groups; and

comparing a behavior of a user against the model to detect a deviation from an expected behavior for the user as represented by one of the clusters.

As we have previously stated, Arkose believes that DataDome will require a license to one or more of these patents for its CAPTCHA service.

Please respond to this letter within 30 days, by September 8, 2023, to discuss DataDome's willingness to enter into a license to practice these and other Arkose patents.

Best regards,

Womble Bond Dickinson (US) LLP

Chris Mammen
Partner