TECHNICAL SERVICE BULLETIN (TSB)

Fantasy Sports Websites

WHAT IS THE HARM?

ComSifter®
protect web users now!

TSB Date: October 23, 2015

IN THIS DOCUMENT

SUMMARY

Fantasy sports websites causing potential harm by using HTTPS for secure traffic and not employing a model to determine if users of the site are at least 18-years-old.

DESCRIPTION

Recently, two (2) major fantasy sports sites have garnered national attention. The websites are designed to allow users to create a mock sports team in a variety of genres that then compete against other users' mock sports team. In general, the mock team with the highest points wins the bet—with a variety of betting and winning methods.

The domains of concern are:

- fanduel.com
- draftkings.com

Issue

Typically, Comsift does not involve itself with what we consider "adult activities," but these sites have garnered our attention. Not only do the websites require a credit card to participate, but the sites have minimal or nonexistent methods to verify that the user is over 18-years-old. Because the website are basically handling financial transactions, the websites have been designed and programmed to use HTTPS (port 443) to secure those transactions.

RESOLUTION

Blacklist

Comsift is taking these sites seriously, and have added the sites to our blacklist. Typically, such gambling-oriented sites would be added to the gambling CSPhrase and Filter groups of the blacklist, allowing you, the end user, to decide if gambling sites are permitted on your network. In this case, we have decided to add the domains to the pornography group, which affects all filters and is permanently enabled.

Proxy

If the web browsers on your network have proxy enabled (ComSifter IP address and port 8080), then no further action is necessary, as the ComSifter will be able to see the request to access these domains and automatically deny access to the sites.

If proxy is not enabled, the ComSifter will see the request for access to port 443 (HTTPS)—instead of port 8080 when proxy is enabled—and allow the session to continue. Because the session is secure (encrypted), the ComSifter will not be able to see which domains are being accessed and cannot utilize the blacklist or the CSPhrase technology to filter or deny the request. A more thorough discussion of the pros and cons of proxy and deployment on the local network can be found in the white paper *Transparent v. Proxy Mode*.

http://comsift.com/white-papers/wp_20130101_transparent-v-proxy-mode.pdf

Comsift, Inc. | 1646 Elderberry Way, San Jose, CA 95125-4507 | 866-875-1254 | info@comsift.com | www.comsift.com