

# FIVE

[ ADS Scanner ]

# MINUTE



## SECKC

# TOOL TALK

Aaron Crawford  
Insider Security Agency

# SeckC Tool Talk – June 11, 2019

01

## Pick ANY Tool

The sky is the limit so don't make any excuses, just pick a cool tool that you would like to share with others.

02

## Create a 5 Minute Talk

Break down the usage and tips into a quick start segment of sorts that can be presented in 5 minutes or less. Be sure to include and focus on the basics.

03

## Submit the Talk to SeckC

After you have created the talk, submit it to SeckC at? [www.seckc.org](http://www.seckc.org) so it can be selected for an upcoming SeckC meeting.

04

## Share the Fun

Present your favorite tool and its usage at a SeckC meeting. Make new friends by sharing information and discover a great and supportive starting place. Information wants to be free!



# SECKC



## What is a the ads.txt file?

The Authorized Digital Sellers file or ADS.TXT version 1.0.2 is a server side file that specifies a mechanism for publishers to list their authorized digital sellers, in order to fight against fraud and misrepresented domains. The most current version allows users to specify entities that they prohibit as well. This helps to expedite sales and avoid fraud.

<https://iabtechlab.com/ads-txt/>



## Location

The ADS.TXT file will ALWAYS be located on the site's root directory as dictated by IAB standards.  
EXAMPLE: <https://www.website.com/ads.txt>

## The Risk?

A centrally located list of approved third parties, subdomains, and your advertising partner identifications. In addition an automated attack vector for constructing botnets and malvertising attacks.

## The Approved Use?

Speed up approved advertisement placement and sales through whitelisting approved third parties and vendors.

# Recon Potential

What exactly can the ADS.TXT file give an attacker and a security assessment?





```
leads.tv, 8839, DIRECT, 13a9c4416d20cbe1
outbrain.com, 007d5bdae84ea9f865307ba5e95aa29dda, DIRECT # banner
outbrain.com, 00e41b90c34e6b3a580e675b4570b52f13, DIRECT # banner
beachfront.com, 2268, DIRECT, e2541279e8e2ca4d
pubmatic.com, 157628, DIRECT, 5d62403b186f2ace
districtm.io, 101707, DIRECT
districtm.io, 100269, DIRECT, 3fd707be9c4527c3
appnexus.com, 1908, RESELLER, f5ab79cb980f11d1
google.com, pub-9685734445476814, RESELLER, f08c47fec0942fa0
emxdgt.com, 975, DIRECT, 1e1d41537f7cad7f
appnexus.com, 1356, RESELLER, f5ab79cb980f11d1
google.com, pub-5995202563537249, RESELLER, f08c47fec0942fa0
contextweb.com, 561632, RESELLER
tremorhub.com, tv8k8-5qsvj, RESELLER, 1a4e959a1b50034a
freewheel.tv, 923041, DIRECT
freewheel.tv, 923201, RESELLER
advertising.com, 28238, RESELLER
adtech.com, 11628, RESELLER
google.com, pub-7082778644367489, DIRECT, f08c47fec0942fa0
pubmatic.com, 157184, DIRECT, 5d62403b186f2ace
pubmatic.com, 157916, DIRECT, 5d62403b186f2ace
spotxchange.com, 149668, RESELLER, 7842df1d2fe2db34
spotx.tv, 149668, RESELLER, 7842df1d2fe2db34
advertising.com, 12171, RESELLER
tremorhub.com, 51vtw, RESELLER, 1a4e959a1b50034a
google.com, pub-5405744859927315, RESELLER
lkqd.net, 464, RESELLER, 59c49fa9598a0117
lkqd.com, 464, RESELLER, 59c49fa9598a0117
freewheel.tv, 867601, RESELLER
freewheel.tv, 867617, RESELLER
google.com, pub-1719633316796094, DIRECT, f08c47fec0942fa0
rubiconproject.com, 16720, RESELLER, 0bfd66d529a55807
undertone.com, 3734, DIRECT
appnexus.com, 2234, RESELLER
openx.com, 537153564, RESELLER, 6a698e2ec38604c67
appnexus.com, 2764, RESELLER
rhythmonline.com, 4107953657, RESELLER
rubiconproject.com, 17712, DIRECT, 0bfd66d529a55807
loopme.com, 2680, RESELLER, 6c8d5f95897a5a3b
#
# CANADA
google.com, pub-1011508009856018, RESELLER, f08c47fec0942fa0
rubiconproject.com, 14904, RESELLER
#
# SUBDOMAINS
subdomain=healthination.cnn.com
subdomain=games.cnn.com
subdomain=inhealth.cnn.com
subdomain=lending.cnn.com
```



## Account ID for advertising

The file contains the Publisher ID is in the format of  
pub-0000000000000000

## Approved Third Parties

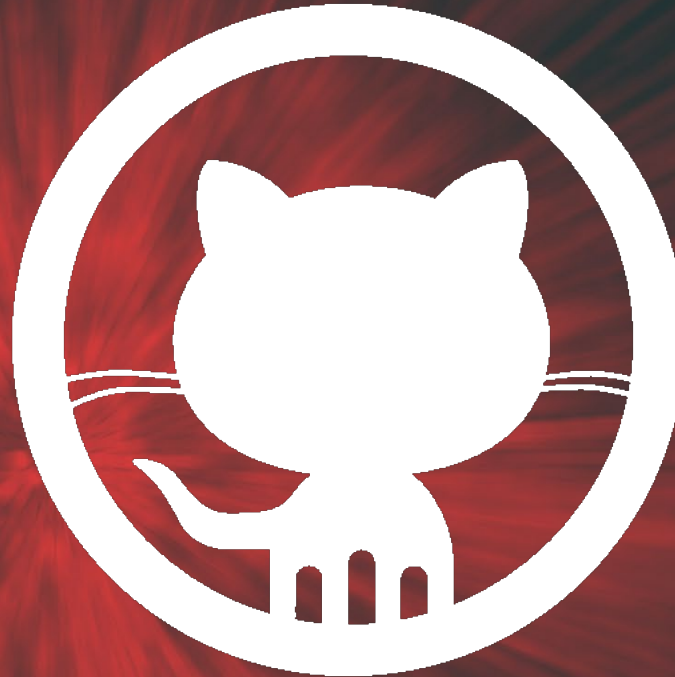
The ads.txt file is a target rich environment for social operations and attacks as this gives an exact list of approved third parties and vendors. These can be used for phishing or pretext phone calls. Automated scans and attacks can be done in addition.

## Subdomains

A rapid way of discovering subdomains is located in the file as formatted by its own section and the formatted designator of: "subdomain="

# Metasploit

To help automate the discovery and remediation of ADS.TXT issues I have created an unreleased Metasploit module.



<https://github.com/insideragency>



# Metasploit Module Demo

See how easy it is to use and how safe it is to integrate into an assessment.

Download the module and place it into the following system folder:

`$HOME/.msf/modules/auxiliary`





# — Where to go from here?

This talk has simply been the introduction to the concepts and ideas behind using the ads.txt file safely and ethically into your assessment process. For additional resources and questions please feel free to contact:

**Web:** [www.theinsideragency.com](http://www.theinsideragency.com)

**Resources:** [github.com/insideragency](https://github.com/insideragency)

**LinkedIn:** Insider Security Agency

**Twitter:** @Insider\_Agency

**Hashtags:** #SocialEngineeringTips #SocialOperator  
#LearnSocialEngineering #HackerHired #HackHunger

