New Reconnaissance Vectors Through Web Marketing

Aaron Crawford
Insider Security Agency

INSIDER
SECURITY AGENCY

Aaron Crawford

whoami

INSIDER

SECURITY AGENCY

Not enough time here to explain.
Find me after this talk.

Twitter: @Insider_Agency

web: www.theinsideragency.com

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

Web Recon Briefing 05.03.2019

01 Getting Started

What is ADS.TXT?

02 Recon Potential

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

03 Security Scenarios

How can ADS.TXT risks be addressed and used to help clients?

04 Metasploit

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

INSIDER
SECURITY AGENCY

Getting Started

What is the ads.txt file? Where is it located and why is it needed?

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.

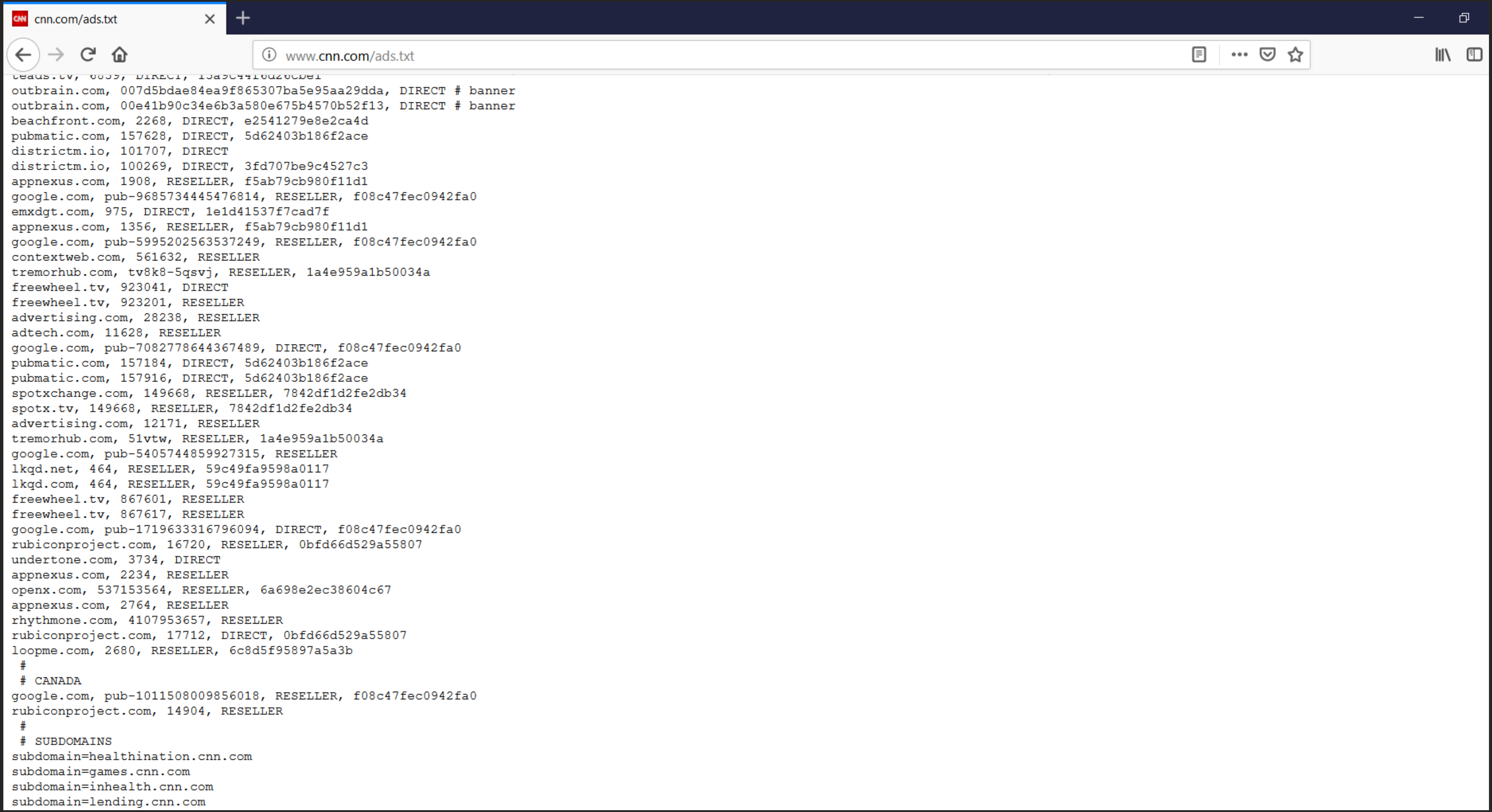
The Approved Use?

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?

INSIDER
SECURITY AGENCY



```
teads.tv, 6859, DIRECT, 15a9c44f6d26cbe1
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
rhythmone.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="

Security Scenarios

How can ADS.TXT risks be addressed and used to help clients?

INSIDER
SECURITY AGENCY

Web Application Firewall (WAF)

The file will always be located on the domain root, so add as many layers of non-intrusive defenses in place.

Communication & Assessments

Having a baseline for the acceptable risk and use fo the ads.txt file is key. Regular web site security assessments is key to ensuring that everything is up to date, patched and properly secured. In addition an approved communication plan for the ads.txt fille must be created to prevent social operations.

Continuous Monitoring

Use an IDS or other defensive monitoring protocols to allow for instant alert and monitoring of requests to the ads.txt file. Set a low threshold for monitoring.

Metasploit

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

Metasploit Module

A safe and benign Metasploit scanner module has been created for the ads.txt file and can locate up to class A subnet of instances. Locate the file faster without worry during your next assessment.

INSIDER

SECURITY AGENCY

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
LinkedIn: Insider Security Agency
Twitter: @Insider_Agency
Hashtags: #SocialEngineeringTips #SocialOperator #LearnSocialEngineering #HackerHired #HackHunger

INSIDER
SECURITY AGENCY