rsmudge / **Malleable-C2-Profiles** Public

Notifications Fork 425 Star 1.5k

Code Pull requests 1 Actions Projects Security Insights

Files

2632378

Go to file

- APT
- crimeware
- normal
  - amazon.profile
  - bingsearch_getonly.profile
  - cnnvideo_getonly.profile
  - gmail.profile
  - googledrive_getonly.profile
  - microsoftupdate_getonly.profile
  - msnbcvideo_getonly.profile
  - ocsp.profile
  - onedrive_getonly.profile
  - pandora.profile
  - randomized.profile
  - reference.profile
  - rtmp.profile
  - safebrowsing.profile
  - webbug.profile
  - webbug_getonly.profile
  - wikipedia_getonly.profile

Malleable-C2-Profiles / normal / **amazon.profile**

HarmJ0y added author 5f84c04 · 10 years ago History

Code Blame 83 lines (63 loc) · 1.78 KB Raw

```
#
# Amazon browsing traffic profile
#
# Author: @harmj0y
#

set sleeptime "5000";
set jitter    "0";
set maxdns    "255";
set useragent "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko";

http-get {

    set uri "/s/ref=nb_sb_noss_1/167-3294888-0262949/field-keywords=books";

    client {

        header "Accept" "*/*";
        header "Host" "www.amazon.com";

        metadata {
            base64;
            prepend "session-token=";
            prepend "skin=noskin;";
            append "csm-hit=s-24KU11BB82RZSYGJ3BDK|1419899012996";
            header "Cookie";
        }
    }

    server {

        header "Server" "Server";
        header "x-amz-id-1" "THKUYEZKCKPGY5T42PZT";
        header "x-amz-id-2" "a21yZ2xrNDNtdGRsa212bGV3YW85amZuZW9ydG5rZmRuZ2tmZGl4aHRvND
        header "X-Frame-Options" "SAMEORIGIN";
        header "Content-Encoding" "gzip";

        output {
            print;
        }
    }
}

http-post {

    set uri "/N4215/adj/amzn.us.sr.aps";

    client {

        header "Accept" "*/*";
        header "Content-Type" "text/xml";
        header "X-Requested-With" "XMLHttpRequest";
        header "Host" "www.amazon.com";

        parameter "sz" "160x600";
        parameter "oe" "oe=ISO-8859-1;";

        id {
            parameter "sn";
        }

        parameter "s" "3717";
        parameter "dc_ref" "http%3A%2F%2Fwww.amazon.com";

        output {
            base64;
            print;
        }
    }

    server {

        header "Server" "Server";
        header "x-amz-id-1" "THK9YEZJCKPGY5T42OZT";
        header "x-amz-id-2" "a21JZ1xrNDNtdGRsa219bGV3YW85amZuZW9zdG5rZmRuZ2tmZGl4aHRvND
        header "X-Frame-Options" "SAMEORIGIN";
        header "x-ua-compatible" "IE=edge";

        output {
            print;
        }
    }
}
```