Sign in

rsmudge / Malleable-C2-Profiles Public

Notifications Fork 425 Star 1.5k

Code Pull requests 1 Actions Projects Security Insights

Malleable-C2-Profiles / normal / onedrive_getonly.profile

bluscreenofjeff initial commit of new profiles 3f8f670 · 8 years ago

127 lines (100 loc) · 5.87 KB

Code Blame Raw

```
#
# OneDrive
#
# Author: @bluscreenofjeff
#

#set https cert info
https-certificate {
    set CN       "mail.live.com"; #Common Name
    set O        "Microsoft Corporation"; #Organization Name
    set C        "US"; #Country
    set L        "Redmond"; #Locality
    set OU       "Outlook EdgeProxyBAYJune2015"; #Organizational Unit Name
    set ST       "Washington"; #State or Province
    set validity "365"; #Number of days the cert is valid for
}

#default Beacon sleep duration and jitter
set sleeptime "60000";
set jitter    "20";

#default useragent for HTTP comms
set useragent "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko";

#IP address used to indicate no tasks are available to DNS Beacon
set dns_idle "8.8.4.4";
```

```

#Force a sleep prior to each individual DNS request. (in milliseconds)
set dns_sleep "0";

#Maximum length of hostname when uploading data over DNS (0-255)
set maxdns    "235";

http-get {

    set uri "/preload";

    client {
        parameter "manifest" "wac";
        header "Host" "onedrive.live.com";
        header "Accept" "text/html,application/xml;*/*;";
        header "Accept-Encoding" "gzip, deflate";

        #session metadata
        metadata {
            base64url;
            prepend "E=P:";
            append "=:PFzM9cj";
            header "Cookie";
        }

        #header "MicrosoftApplicationsTelemetryDeviceId" "9u2srx19-4gm0-3x2t-lf25-9ejwla1gvbsn;";

    }


    server {

        header "Cache-Control" "no-cache, no-store";
        header "Pragma" "no-cache";
        header "Content-Type" "text/html; charset=utf-8";
        header "Expires" "-1";
        header "Vary" "Accept-Encoding";
        header "Server" "Microsoft-IIS/8.5";
        header "Set-Cookie" "E=P:We/01nw8bIg=:oIbA04j2Itig4t8cWKNKrDaG/ZDZuMnyxXC+BkkNivU=:F; domai

        #Beacon's tasks
        output {
            netbios;
            prepend " <html xmlns=\"http://www.w3.org/1999/xhtml\"><head><title>Preload</title><scr
            append "u002ffiles\u002fonedrive-website-release-prod_master_20160928.003\u002fwac_s_ur
            print;
        }
    }
}

http-post {

    set uri "/sa";
    set verb "GET";

    client {

        header "Host" "onedrive.live.com";
        header "Accept" "text/html,application/xml;*/*;";
        header "Accept-Encoding" "gzip, deflate";

        #Beacon's responses
        output {
            base64url;
            prepend "E=P:";
            append "=:PFzM9cj";
            header "Cookie";
        }

        #session ID
        id {
            base64url;
            prepend "https://p.sfx.ms/sa.html?s=";
            header "Referer";
        }

    }

    server {

        header "Cache-Control" "no-cache, no-store";
        header "Pragma" "no-cache";
        header "Content-Type" "text/html; charset=utf-8";
        header "Expires" "-1";
        header "Vary" "Accept-Encoding";
        header "Server" "Microsoft-IIS/8.5";
        header "Set-Cookie" "E=P:We/01nw8bIg=:oItIbA04j2rDig4t8cWKNKaG/ZDZuMnyxXC+BkkNivU=:F; domai

        #empty
        output {
            print;
        }
        }
    }
}

#change the stager server
http-stager {
    server {
        header "Content-Type" "text/html; charset=utf-8";
    }
}
```