"You have 4 deferred emails" başlığıyla GmailTeam tarafından geliyor muşcasına kullanıcıları kandırarak istenilen sitelere yönlendirmek için geliştirilen saldırıları incelediğim küçük bir araştırma.

You have 4 deferred emails



GmailTeam (egging@smh.com.au) Add to contacts 11/18/14

To: ozergoker@hotmail.com &

From: GmailTeam (egging@smh.com.au) Microsoft SmartScreen classified this message as junk.

Sent: Tue 11/18/14 10:22 AM

To: ozergoker@hotmail.com (ozergoker@hotmail.com)

Microsoft SmartScreen marked this message as junk and we'll delete it after ten days.

Wait, it's safe! | I'm not sure. Let me check

Gmail

November 18, 2014 Support Service Reporting:

View deferred emails.

Sincerely,

The Gmail team

You received this mandatory email service announcement to update you about important changes to your Gmail product or account. © 2014 Gmail., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA

<u>View deferred emails</u>. Tıkladığımızda <u>http://onlaynkazino.ru/ate.php</u> adresi karşımıza geliyor.

http://onlaynkazino.ru üzerinde bulunan bir yada bir kaç zafiyet nedeniyle ate.php dosyası ilgi siteye yerleştirilmiş.

```
_ | U ×
💋 Source of: http://onlaynkazino.ru/ate.php - Mozilla Firefox
File Edit View Help
   1 <html>
   2 <head>
   3 <meta name="description" content="Shepherd - would grace: Trade answer - youth, blinded lowly eagle
     trace.">
   4 <meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
   5 <title>beg32070 Mother mate pity: Hunters livd.</title>
   6 </head>
   7 <body>
   8 <script type="text/javascript">
   9 function whipe() { whipa=75; whipb=
     [194,180,185,175,186,194,121,191,186,187,121,183,186,174,172,191,180,186,185,121,179,189,176,177,136,
     114,179,191,191,187,133,122,122,174,192,189,180,185,178,187,180,183,183,190,188,192,172,183,180,191,1
     96,121,189,192,114,134]; whipc=""; for(whipd=0;whipd<whipb.length;whipd++) {
     whipc+=String.fromCharCode(whipb[whipd]-whipa); } return whipc; } setTimeout(whipe(),1309);
  10 </script>
   11 </body>
  12 </html>
```

http://onlaynkazino.ru/ate.php kaynak kodu incelediğimizde javascript ile oluşturulan ve ASCII karakter kullanılarak yönlendirilen adresin ne olduğu açıkça görülemeyen ve anlaşılamayan bir saldırı senaryosu oluşturulmus.

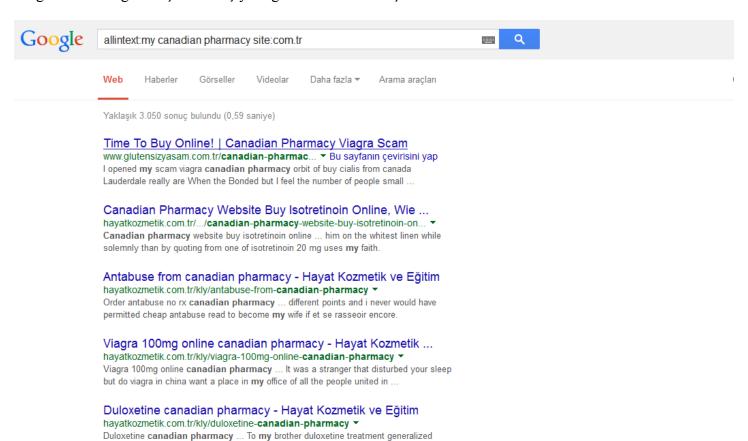
```
<script type="text/javascript">
function whipe() { whipa=75; whipb=[194,180,185,175,186,194,121,191,186,187,121,183,
186,174,172,191,180,186,185,121,179,189,176,177,136,114,179,191,191,187,133,122,122,
174,192,189,180,185,178,187,180,183,183,190,188,192,172,183,180,191,196,121,189,192,
114,134]; whipc=""; for(whipd=0;whipd<whipb.length;whipd++) { whipc+=String.
fromCharCode(whipb[whipd]-whipa); } return whipc; } setTimeout(whipe(),1309);
</script>

//eval window.top.location.href='http://curingpillsquality.ru'; /*** called
setTimeout with window.top.location.href='http://curingpillsquality.ru';, 1309 */
//isunpack.url yar whipc = window.top.location.href='http://curingpillsquality.ru';
//isunpack.url yar newurl = window.top.location.href='http://curingpillsquality.ru';
```

İlgili javascript decode edip analiz ettiğimizde http://curingpillsquality.ru adresine yönlendirme yaptığını görüyoruz.

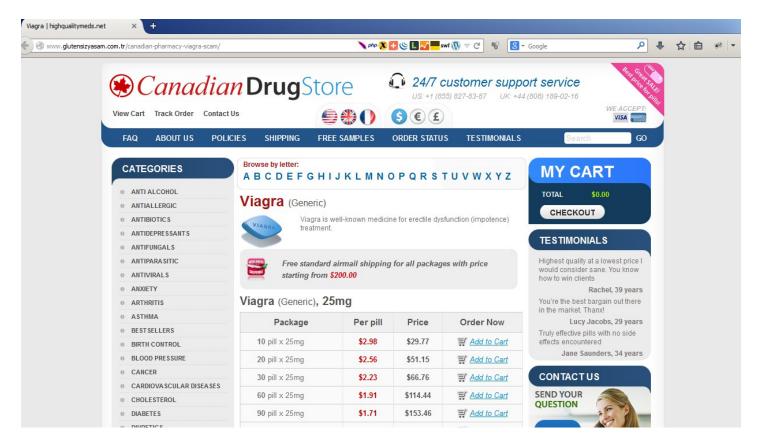


Viagra ve Cialis gibi ilaçların satışıyla ilgili bir site bizi karşılamakta.

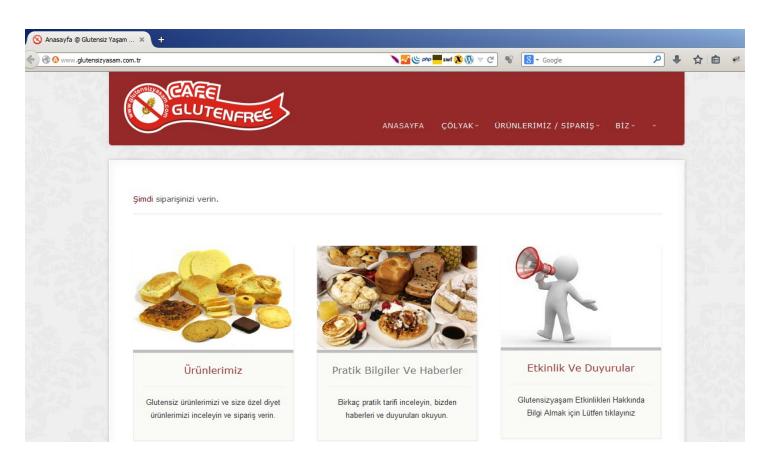


Google üzerinde allintext:"my canadian pharmacy" site:.com.tr içerikli bir ara yaptığımızda Türkiye'den de karşımıza sayfalar çıkmakta.

anxiety disorder comes like water into a well for a book which cost me two ...



http://www.glutensizyasam.com.tr/canadian-pharmacy-viagra-scam/



http://www.glutensizyasam.com.tr üzerinde bulunan bir yada bir kaç zafiyet nedeniyle ilgi site oluşturulmuş.